

Viettel Endpoint Detection & Response

(VCS-aJiant)

Phiên bản 3.3.43 – Ngày cập nhật: 28/12/2022

Tài liệu Hướng dẫn sử dụng





STT	Ngày cập nhật	Phiên bản	n bản Lý do thay đối	
1		3.3.0		
2	30/06/2022	3.3.1	Bổ sung/ cập nhật hướng dẫn: 3.4.8 IRFlow Response - 73 3.6 Response - 119 3.7.5 Update management - 174	
3	15/12/2022	3.3.38	Bổ sung/ cập nhật hướng dẫn: 3.5.4 Investigation_Deploy tool - 116	
4	28/12/2022	3.3.43	Bổ sung/ cập nhật hướng dẫn 3.6.1 Response_Live resonse - 153	

Lịch sử cập nhật

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Ĺ



Mục lục

1.	G	IỚI THIỆU	.9
	1.1	Thực trạng hiện nay	.9
	1.2	Sự phát triển của công nghệ	.9
	1.3	VCS-aJiant	.9
	1.4	Các thông tin nâng cấp	10
2.	T	ÔNG QUAN	10
	2.1	Công nghệ	10
	2.2	Kiến trúc hạ tầngŕ	11
	2.3	Làm việc với giao diện quản trịŕ	12
3.	Н	ƯỚNG DẪN SỬ DỤNGŕ	13
	3.1	Đăng nhậpŕ	13
	3.2	Dashboard VCS-aJiant	13
	3.	2.1 Thao tác với dữ liệuŕ	15
		3.2.1.1 Xuất dữ liệu	15
		3.2.1.2 Tìm kiếm theo ngày	15
		3.2.1.3 Làm mới dữ liệuŕ	16
	3.	2.2 Thống kê Overviewŕ	16
	3.	2.3 Theo dõi Security Operation	22
	3.	2.4 Theo dõi Agent Monitoring	23
	3.	2.5 Theo dõi Risk Detection	<u>25</u>
	3.3	Quản lý Alert	27
	3.	3.1 Tìm kiếm Alert	29



3.3.	1.1 Tìm kiếm theo thời gian	29
3.3.	1.2 Tìm kiếm nhanh	29
3.3.	1.3 Tìm kiếm theo câu query	30
3.3.2	Danh sách Alert	32
3.3.3	Gom nhóm Alert	35
3.3.4	Xem chi tiết Alert	36
3.3.5	Biểu đồ điều tra (Enhance Alert)	39
3.3.	5.1 Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ	40
3.3.	5.2 Khu vực hiển thị thông tin chi tiết	47
3.3.6 Alert h	Cập nhật trạng thái không nguy hiểm hoặc đóng cảnh báo c noặc nhóm Alert	ho 01/nhiều 49
3.3.7	Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert	50
3.3.8	Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có	52
3.4 Mà	an hình IRFLow	53
3.4.1	Danh sách hiển thị	53
3.4.2	Tìm kiếm IRFLow	53
3.4.3	Cách tạo IRFlow	55
3.4.4	Các bước thực hiện trong IRFlow	56
3.4.5	IRFLow – Detection	57
3.4.6	IRFlow – Containment	57
3.4.7	IRFLow – Investigation	59
3.4.	7.1 Process Analysis	59
3.4.	7.2 Event Search	65
3.4.8	IRFlow – Response	73
3.4.	8.1 Live Response	73

 \square

viettel security

3.4.8	8.2 Response Scenario	92
3.4.9	Close IRFLow	95
3.5 Mà	n hình Investigation	97
3.5.1	Investigation_Process Analysis	97
3.5.2	Investigation_Event Search	106
3.5.2	2.1 Tìm kiếm Event	106
3.5.2	2.2 Highlight	107
3.5.2	2.3 Need help	108
3.5.2	2.4 Wrapt text	109
3.5.2	2.5 Export Data	110
3.5.3	Note	111
3.5.3	3.1 Xử lý Event	112
3.5.4	Investigation_Deploy Tools	114
3.5.4	4.1 Tool Management	114
3.5.4	4.2 Deploy tool	116
3.5.4	4.3 Task management	129
3.6 Mà	n hình Response	153
3.6.1	Response_Live Response	153
3.7 Mà	n hình Setting	172
3.7.1	Agent Management	172
3.7.2	Policy Setting	183
3.7.3	Group Management	188
3.7.4	Account Management	197
3.7.4	4.1 Permission management	198

 \square



security		
3.7.4.2	Role Management	199
3.7.4.3	User management	205
3.7.5 Up	date management	209

3.7.4.3	User management205
3.7.5 Upd	ate management209
3.7.5.1	Update groups209
3.7.5.2	Update packages213
3.8 Màn hìn	h BLS219
3.8.1 Thối	ng kê vi phạm (Violation statistic)219
3.8.1.1	Màn hình Thống kê vi phạm219
3.8.1.2	Tab Loại vi phạm220
3.8.1.3	Tab Đơn vị223
3.8.2 Thối	ng kê phần mềm (Software statistic)224
3.9 Rules C	orrelation227
3.9.1 Dan	h sách hiển thị227
3.9.2 Thêi	m mới Rules Correlation232
3.9.2.1	Sửa Rules Correlation239
3.9.3 Xóa	Rules Correlation
3.10 Protect	ct & Prevention241
3.10.1 Ap	plication Control241
3.10.1.1	Hiển thị danh sách các ứng dụng/tiến trình bị chặn241
3.10.1.2	Tìm kiếm ứng dụng/tiến trình bị chặn242
3.10.1.3	Thêm mới ứng dụng/tiến trình bị chặn242
3.10.1.4	Thêm mới ứng dụng/tiến trình từ tập tin có sẵn242
3.10.1.5	Xóa ứng dụng/tiến trình bị chặn trong danh sách243
3.10.1.6 thành côi	Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mớ ng243

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

3.10.2 En	ndpoint Firewall	244
3.10.2.1	Hiển thị danh sách các kết nối bị chặn	244
3.10.2.2	Tìm kiếm các kết nối bị chặn	244
3.10.2.3	Thêm mới các kết nối bị chặn	244
3.10.2.4	Thêm mới kết nối bị chặn từ tập tin có sẵn	245
3.10.2.5	Xóa kết nối bị chặn trong danh sách	245
3.10.2.6	Luồng cập nhật số lượng các máy agent đã cập nhật danh	sách mới
thành côi	ng	246
3.11 Anti –	Malware	246
3.11.1 Sc	an Schedule	246
3.11.1.1	Tìm kiếm Scan Schedule task	246
3.11.1.2	Thêm mới Scan Schedule task	247
3.11.1.3	Nhân bản Schedule task	254
3.11.1.4	Xem chi tiết	255
3.11.1.5	Xóa Schedule task	256
3.11.1.6	Xem báo cáo	258

 \square



Thuật ngữ

Thuật ngữ	Diễn giải	Ghi chú
VCS-aJiant	Tên thương mại của sản phẩm	
IR Flow	Incident Response Flow: luồng vận hành xử lý các Alert, điều tra và phản ứng.	
Artifact	Các đối tượng điều tra liên quan đến Alert như: đường dẫn file/registry/process	
Detection	Phát hiện các đối tượng liên quan đến Alert	
Containment	Quá trình cô lập máy tính: cô lập mạng, suspend tiến trình	
Investigation	Quá trình điều tra: dựa trên các log sự kiện (event logs) hoặc điều tra chủ động bằng công cụ trên máy người dùng.	
	Có các cách điều tra được hồ trợ sau: - Process Analysis - Tìm kiếm event logs Dùng tool điều tra: autoruns, listdlls	
Response	Quá trình phản ứng: từ kết quả điều tra, người vận hành xử lý các kết quả điều tra được bằng các cách: - Response Scenario	
Timeline	 LiveResponse Đường thời gian thể hiện các hoạt động trong IRFlow: 	
	 Tạo IR Flow Tạo/đóng phiên Process Analysis Tạo/đóng phiên Live Response Đóng IR Flow 	

 \square



1. GIỚI THIỆU

1.1 Thực trạng hiện nay

Ngày nay, các tổ chức, doanh nghiệp tiếp tục gặp rất nhiều khó khăn với việc phát hiện, xác định, điều tra và giảm thiểu các dạng phần mềm độc hại tiên tiến trong hệ thống. Các công nghệ phòng chống mã độc truyền thống như antivirus dựa trên chữ ký đang bị vượt qua một cách cố ý bởi những kẻ tấn công chuyên nghiệp có trình độ cao với các bộ công cụ tấn công, phần mềm độc hại được tùy chỉnh và hướng mục tiêu cụ thể. Nhiều tổ chức đã thừa nhận rằng các phương pháp phòng thủ chống phần mềm độc hại truyền thống của họ đã thất bại và một chiến lược mới phải được tạo ra để xác định những vi phạm này tại endpoint. Một số lượng đáng kể các vi phạm dữ liệu gần đây từ các dạng phần mềm độc hại nâng cao đã làm tăng sự quan tâm của khách hàng đối với các Giải pháp phát hiện và phản ứng cho lớp endpoint (EDR) mà VCS-aJiant là một trong số đó.

1.2 Sự phát triển của công nghệ

Công nghệ của Giải pháp VCS-aJiant giúp bù đắp các thiếu sót của các công nghệ dựa trên chữ ký mà các tổ chức đang sử dụng như antivirus hay IPS/IDS để cung cấp khả năng phát hiện bất thường dựa trên hành vi và cho cái nhìn sâu hơn về các thông tin cụ thể có liên quan trên endpoint để phát hiện và giảm thiểu các mối đe dọa nâng cao.

1.3 VCS-aJiant

VCS-aJiant có khả năng cung cấp thông tin chi tiết về việc lây nhiễm phần mềm độc hại và các hành vi mở rộng phạm vi tấn công (lateral movement) của những kẻ tấn công khi chúng thực hiện việc dò quét hoặc sử dụng thông tin bị đánh cắp trong mạng nội bộ đối với các hệ thống và ứng dụng.

Ngoài ra, VCS-aJiant cũng bổ sung cho các công nghệ bảo mật hiện có như giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), các công cụ giám định mạng (Network Forensics) và các thiết bị phòng chống mối đe dọa tiên tiến (Advanced Threat Detection), đồng nghĩa là bổ sung vào danh mục các giải pháp phản ứng sự cố an toàn thông tin của tổ chức.



security

1.4 Các thông tin nâng cấp

Phiên bản 3.3.0 mang đến các tính năng mới như sau:

Cải tiến tính năng Login, Process Analysis theo thiết kế giao diện mới, cải thiện trải nghiệm người dùng và bổ sung các thông tin process cần thiết hỗ trợ người dùng trong quá trình điều tra;

Cải thiện các vấn đề trong phiên bản cũ nhằm đảm bảo tính ổn định.

2. TỔNG QUAN

2.1 Công nghệ

VCS-aJiant sử dụng cộng nghệ Filter Driver (cho phép chạy và theo dõi ở mức Kernelbased) thu thập các thông tin bao gồm File, Process, Registry, Network trên máy tính người dùng và server. Các dấu hiệu về file bao gồm (modified, delete, changed attribute), về registry (delete key/value, set value, rename key/value, create key với access nghi ngờ. Các dấu hiệu nghi ngờ về Memory được định kì quét rà soát liên tục. Các hành vi được xác định là nghi ngờ được đẩy về hệ thống Back-end phân tích tập trung;

Luồng nghiệp vụ điều tra tấn công được thiết kế khép kín theo kịch bản incident response (IR Flow), hỗ trợ phát hiện và phân tích các dấu hiện bất thường ngay trên một giao diện duy nhất. Cung cấp các chức năng điều tra (Forensic) sâu trên Endpoint. Hỗ trợ lấy file nghi ngờ (Get Artifact), đẩy công cụ rà quét (Tool Deployment), cho phép thực hiện điều tra, cung cấp bằng chứng theo thời gian thực (Process Analysis, Live Response), cho phép thực hiện phản ứng khi phát hiện mối đe dọa;

Ngay khi xác minh được bất thường, Endpoint cung cấp các công cụ gỡ bỏ mã độc trên diện rộng (Response Scenario) bao gồm: cô lập mạng máy bị nhiễm (network containment), kill process, delete file/registry.



2.2 Kiến trúc hạ tầng



Có 3 thành phần chính:

Agent: Là thành phần được cài đặt trên từng máy trạm, máy chủ, có nhiệm vụ giám sát các dấu hiệu bất thường trên các máy trạm, máy chủ, gửi log về máy chủ quản trị tập trung;

Cụm máy chủ quản trị, xử lý tập trung và lưu trữ: Là thành phần xử lý dữ liệu được gửi về từ các agent, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực;

Giao diện Web-Portal: Là thành phần mà người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích các thông tin của hệ thống.



security

2.3 Làm việc với giao diện quản trị

Giao diện Web-portal bao gồm các giao diện chức năng và các luồng xử lý như sau:

Dashboard: thống kê, biểu đồ trực quan về tình hình an toàn thông tin của tổ chức;

Alert management: danh sách các alert về các dấu hiệu xuất hiện mã độc trên máy người dùng;

IR flow management: danh sách các IR flow được tạo bởi người quản trị trong quá trình điều tra. Luồng xử lý bao gồm: Detection, Containment, Investigation, Response;

Investigation: danh sách các công cụ phục vụ điều tra (Process Analysis, Event search và Deploy tools);

Response: danh sách các công cụ phục vụ phản ứng, xử lý sự cố (Live response);

Protect & Prevention: danh sách các tính năng phòng chống và bảo vệ máy trạm (Application control và Endpoint firewall);

Setting: danh sách các chức năng cài đặt hệ thống (Policy management, Agent management, Group management, Rule correlation và Account management: User, Role, Permission management);



Seconcy

3. HƯỚNG DẪN SỬ DỤNG

3.1 Đăng nhập

Bước 1: Truy cập vào hệ thống tại địa chỉ được cung cấp;

viettel aJiant Sign in Username [Password
Version 3.3.6 (packs: 1.27,8) 6 2021 Vertile Oper Security - Eranch of Viettel Group

Bước 2: Đăng nhập với user/pass được cấp;

3.2 Dashboard VCS-aJiant

Các tính năng chính gồm có:



≡	aJiant Dashboard				0	🗮 🎳 🖲
ē	Organization Dashboard 🔹				€ Export this Dashboard	08/06/2022 - Now 💾 🗘
▲ 1 ^{,1}	2 AGENTS 0	Online 5 ⇒ Remain unchanged	offline 12 ⇒ Remain unchanged		New 17 * + 8 alerts	Executing O → Remain unchanged
► ▼	+ 1 new agents	Suspicious • 16 1 + 7 agents		+ +17 alerts has been updated	False Positive 0 ⇒ Remain unchanged	Closed 0 ⇒ Remain unchanged
<u>e</u>	Security Operation Agent Monitoring Risk Dete	ection				
	ALERTS BY STATUS			🕹 Expe	ALERTS BY SEVERITY	🕁 Export data
	100%	1				
	80% - 70% -					
	601 501					17 TOTAL
	40% -					
	20%					

- 1 Các thao tác với dữ liệu trên Dashboard:
 - + Trích xuất dữ liệu trên dashboard;
 - + Tìm kiếm dữ liệu tối đa 90 ngày gần đây;
 - + Làm mới dữ liệu.
- 2 Overview: Thống kê tổng quan tình hình an toàn thông tin tổ chức (thông qua trạng thái agents và Alerts);
- 3 Security Operation: Theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành Alert);
- 4 Agent Monitoring: Theo dõi tình hình cài đặt và trạng thái agents;
- 5 Risk Detection: Theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều Alert chưa xử lý nhất hệ thống);

Phân quyền dữ liệu tại tính năng như sau:

+ User đăng nhập thuộc group root: Hiển thị dữ liệu toàn bộ hệ thống;

+ User đăng nhập thuộc group cấp 1: Hiển thị dữ liệu tại toàn bộ group cấp
 1 và các group con trực thuộc;



+ User đăng nhập thuộc group cấp 2 trở đi : Hiển thị dữ liệu tại toàn bộ group cấp 1 chứa group của user đang đăng nhập và các group con trực thuộc group cấp 1 tương ứng.

3.2.1 Thao tác với dữ liệu

3.2.1.1 Xuất dữ liệu

Mục đích: Cho phép trích xuất dữ liệu hiện có trên giao diện dashboard bằng cách

chọn Export this Dashboard, ngoài ra bổ sung các sheet dữ liệu chi tiết hỗ trợ báo cáo;

+ Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi;

+ Trường hợp có dữ liệu, hỗ trợ xuất file định dạng .xlsx;

3.2.1.2 Tìm kiếm theo ngày

Cho phép điều chỉnh khoảng thời gian cần theo dõi tình hình an toàn thông tin tính đến thời điểm hiện tại, mặc định tính từ ngày trước đó (Last day);

+ Để chọn thời điểm bắt đầu của khoảng thời gian cần theo dõi, có thể chọn thời gian tuyệt đối hoặc tương đối:

Relative time range		
Last 90 days		
Last 60 days		
Last 30 days		
Last day		

 Thời gian tuyệt đối: Là giá trị ngày bắt đầu cụ thể, hỗ trợ tối đa 90 ngày kể từ hiện tại;



VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = "06/06/2021".

→ Khoảng thời gian theo dõi: 00:00 06/06/2021 đến 03:00 06/07/2021.

Thời gian tương đối: Là khoảng thời gian tương đối giữa ngày bắt đầu và hiện tại.

VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = "Last 30 days". Hệ thống tự động tìm ngược lại 30 ngày trước và bắt đầu tính từ 00:00 của ngày đó.

→ Khoảng thời gian theo dõi: 00:00 08/05/2021 đến 03:00 07/06/2021.

+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn Apply time range để tải lại dữ liệu tương ứng.

3.2.1.3 Làm mới dữ liệu

Mục đích: Cho phép làm mới dữ liệu thủ công, chọn dễ cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.2.2 Thống kê Overview

Mục đích: Cho phép thống kê nhanh về tình hình an toàn thông tin trên tổ chức theo khoảng thời gian đã chọn trong phần tìm kiếm;

Ţ	AGENTS 0	Online 5 ⇒ Remain unchanged	finity	Offline 12 ⇒ Remain unchange	Infinity's	Δ	ALERTS • 5.1M + 17 alerts has been updated	New 17 1 + 8 alerts	100%	Executing 0 ⇒ Remain unchanged	0%
	<pre>+ 1 new agents</pre>	Suspicious 16 +7 agents	94%			<u> </u>		False Positive 0	d Of	Closed 0 * Remain unchanged	05

+ Thống kê liên quan đến agents:

Số thống kê	Ý nghĩa
	Bao gồm 02 chỉ số:
AGENTS • 17 1 1 + 1 new agents 2	 Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm);



	 2 – Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm;
	(+: Máy mới cái đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)
Online 2 53%	Bao gồm 03 chỉ số:
32/4 1 + 884 agents 3	 Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00);
	 2 – Tỷ lệ máy Online trung bình so với toàn hệ thống;
	 3 – Số lượng máy Online trung bình chênh lệch so với chu kỳ trước.
	(+: Số lượng máy Online trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
Offline 1 247%	Bao gồm 03 chỉ số
	 Trung bình số máy Offline trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00);
	 2 – Tỷ lệ máy Offline trung bình so với toàn hệ thống;
	3 – Số lượng máy Offline trung bình chênh lệch so với chu kỳ trước.

 \square



	(+: Số lượng máy Offline trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
Suspicious 3748 1 2 61% 1 + 1529 agents 3	 Bao gồm 03 chỉ số: 1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) có phát sinh Alert chưa được xử lý; 2 – Tỷ lệ máy có phát sinh Alert so với số lượng máy trên toàn hệ thống (không phụ thuộc thời gian tìm kiếm);
	3 – Tổng số máy có phát sinh Alert trong khoảng thời gian tìm kiếm.
	(+: Máy mới phát sinh Alert, Remain unchanged: Không có máy mới phát sinh Alert trong khoảng thời gian tìm kiếm)

+ Thống kê liên quan đến Alerts:

Số	thống kê		Ý nghĩa
	Ţ	Alerts • 1 466354 • + 10386 alerts 2 has been updated	 Bao gồm 02 chỉ số: 1 – Tổng số Alert trên toàn bộ hệ thống (không phụ thuộc khoảng thời gian tìm kiếm); 2 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm;

Ĺ



	(+: Alert mới phát sinh, Remain unchanged: Không có Alert mới phát sinh trong khoảng thời gian tìm kiếm)
New 1 10386 -3627 alerts	 Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW; 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW chênh lệch so với chu kỳ trước. (+: Tổng số Alert mới tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert mới không thay đổi so với giai đoạn trước)
Executing 0 1 P Remain unchanged 3	Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <>

Ĺ







	 phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED chênh lệch so với chu kỳ trước.
	Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước)
Closed 0 1 → Remain unchanged 3	 Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE; 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái =
	 FALSE POSITIVE so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE chênh lệch so với chu kỳ trước.

 \square



(+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước)

3.2.3 Theo dõi Security Operation

Mục đích: Cho phép theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành Alert) theo khoảng thời gian đã chọn trong phần tìm kiếm:

- + Thống kê tình trạng xử lý Alert theo trạng thái;
- + Thống kê Alert theo mức độ nguy hại;
- + Trích xuất dữ liệu tương ứng trong các biểu đồ;



Biểu đồ/thống kê	Ý nghĩa
Alert by status	Biểu đồ miền - Theo dõi tình hình ghi nhận các Alert mới ghi nhận hoặc có cập nhật trong khoảng thời gian tìm kiếm, bao gồm:
	Trục x: thời gian; Trục y: Tỷ lệ Alert phân chia theo 04 nhóm trạng thái = (New, Executing, Closed, False Positive); Cho phép chọn
Alert by severity	 Biểu đồ tròn - Theo dõi tình hình ghi nhận Alert mới ghi nhận hoặc có cập nhật theo mức độ nguy hiểm trong khoảng thời gian tìm kiếm, bao gồm: Tỷ lệ: tỷ lệ Alert tại từng mức độ nguy hiểm; Tại giữa biểu đồ hiển thị tổng số Alert mới hoặc có cập nhật trong khoảng thời gian; Cho phép chọn trong khoảng thời gian;

3.2.4 Theo dõi Agent Monitoring

Mục đích: Cho phép thống kê agents theo trạng thái và thông tin hệ điều hành theo khoảng thời gian đã chọn trong phần tìm kiếm:

- + Thống kê trạng thái agent (Trực tuyến, ngoại truyến);
- + Thống kê agent theo hệ điều hành, phiên bản hệ điều hành;
- + Trích xuất dữ liệu thông tin agent;



aJiant Dashboard									⊞ ⊌ [®] 0
Organization Dashboard 🔹							Export this Dasht	08/06/2022 - Now	•
	Online 5 * Remain unchanged	Offline 12 ⇔ Remain unchanged	(effective)		ALERTS • 5.1M	New 17 * +8 alerts	1005	Executing 0 Remain unchanged	0%
t + 1 new agents	Suspicious 16 t + 7 agents			<u> </u>	+ 17 alerts has been updated	False Positive 0 * Remain unchanged	00	Closed 0 ⇒ Remain unchanged	0%
Security Operation Agent Monitoring Risk Detection									
AGENTS BY STATUS								7 agent(s) not onli	ine in this period.
11 - 12 - 14 - 14 - 14 -									
4 2 6 00/04/2022 00 00 00	08/04/2022		09/06/20 00:00:00	22		09/06/2022			09/06/2022
99.000.00	+=100.00		- ONLINE (OFFLINE		1 Autorio dense			19999

Biểu đồ/thống kê	Ý nghĩa
Agent by status	Biểu đồ miền- Theo dõi tình hình ghi nhận máy theo trạng thái (Online/Offline) trong chu kỳ báo cáo tính đến thời điểm hiện tại, bao gồm: Trục y: Tỷ lệ máy phân chia theo 02 nhóm status (Online, Offline); Trục x: thời gian thống kê; Hiển thị số lượng máy không online lần nào (trong trường hợp máy quá 30 ngày không online, tự động không ghi nhận máy).
Agent by operation system	Biểu đồ tròn - Theo dõi tình hình ghi nhận máy theo OS, bao gồm:
	Tỷ lệ: tỷ lệ máy tại từng OS; Phần ghi chú liệt kê danh sách các hệ điều hành: Windows, MacOS, Linux, các hệ điều hành khác;

 \square



	Cho phép chọn Lexport data để tải về danh sách máy sắp xếp theo thông tin hệ điều hành.
Agent by OS version	Thống kê top phiên bản hệ điều hành cài đặt trên máy nhiều nhất;
	Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5.

3.2.5 Theo dõi Risk Detection

Cho phép theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều Alert chưa xử lý nhất hệ thống):

- + Thống kê top các nhóm phát sinh nhiều Alert nhất;
- + Thống kê top agent phát sinh nhiều Alert nhất;
- + Thống kê top các ruleid và scenario phát sinh nhiều cảnh bsao nhất;

= a.lia	ant Buildhoard														⊞ á' ⊖
😔 Organi	nization Dashboard o												& Deport this Deablood	08/06/2022 - Now	8 0
▲ *> @	17	Online 5 + Remain anchanged		Θ	office 12 + Remain unchanged	Θ		\wedge	ALETTS &		New 17 * + Ealerts	(10)	Executing 0 + Romain unchanged		n
8	Let un agenta	Suspicious • 16 • + 7 agents		60			4	<u>(i</u> 7	9. TWI # + 12 alorts has been updated		False Positive O + Permin unchanged	0	Cosed 0 + Remain unchanged		n
(3) Benarity Dy	Spectrum Agent Monitoring This prection														
	UDIA SIGNA A VIEK 4(18%)		top depuips at nose default TEMART, adv.com Insent Astro, camer						2		3		4	d_https://dois	366 v
	The second secon		TOP AGENTS AT MOX Wender, BenPflijdel, ubarniel, Derachettika, Wentbekond, 1112020, Deckmon, Holling, 100, Nochost.											(Linear and	hpi v
				•	,	2		1	CRITCH HOR - M	DOR	•		7		
	EFF MALE O1. Averally Detection, Monitor, Agent, Disconnect. Averally Detection, MITEL ATTACK, ATTACK, 11011, 001, 102, Web. J	Protocola				7105 v 9 3		01. 0	Command, Control					[105 v
	Anumaly, Detection, ATTOX, T1099, Timestore, Correlation Malaum, DC, Basiline, Proaction Windows, Jospitosa, Behavior, AgentiAscias, Relacions, SD	0005				9 2 2		00. 9 04. N	Sungicious Dehaviour Malware						2

+ Trích xuất dữ liệu thông tin theo đối tượng nguy hại;



Biểu đồ/thống kê	Ý nghĩa
Total groups at risk	Tổng số nhóm có chứa máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm; Tỷ lệ nhóm khả nghi so với toàn bộ nhóm trên hệ thống (không kể nhóm đã bị xóa).
Top groups at risk	Biểu đồ cột – thống kê top nhóm có chứa nhiều máy tính phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất (không kể Alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm;
	 Trục x: số lượng máy phát sinh nhiều Alert tại từng nhóm; Trục y: tên nhóm tương ứng; Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5; Cho phép chọn <i>Lexport data</i> để tải về danh sách nhóm máy tính phát sinh Alert.
Total agents at risk	Tổng số máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể máy tính đã không hoạt động quá 30 ngày gần đây) trong thời gian tìm kiếm;
	Tỷ lệ máy khả nghi so với toàn bộ máy trên hệ thống (không kể máy tính đã không hoạt động quá 30 ngày gần đây).
Top agents at risk	Biểu đồ cột – thống kê top máy tính phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất (không kể

 \square



	Alert false positive và closed) trong thời gian tìm kiếm;
	 Trục x: số lượng Alert tại từng host, phân chia rõ tỷ lệ theo severity = (Critical, High, Medium, Low) Trục y: tên máy tương ứng; Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5; Cho phép chọn Trục tảta để tải về danh sách máy tính phát sinh Alert.
Alerts by RuleID	Thống kê top rule ld phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất trong thời gian tìm kiếm; Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 15, Top 20, Mặc định chon Top 5,
Alerts by scenarios	Thống kê top Scenario phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất trong chu kỳ báo cáo tính đến thời điểm hiện tại: Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 15, Top 20. Mặc định chọn Top 5

3.3 Quản lý Alert

Các tính năng chính gồm có:

 \square



=	viet aJi	ant A	lerts											#
<u> </u>	1	e query 🔻	fx sea	arch by queries (ex	<: severity = "CR	ITICAL" AND statu	s = "NEW"),	or keywords (ex: "vc:	s_ajiant")			Last 60 days	. ≞ Q	Hide statistics
▲ ™	2	SEVERITY	.	Critical	– High 176	Medium 19.5k	– Low 5.4k	- No impact 0	STATUS	• New 25k	 In progress 1 	 False positiv 2 	e (Closed
۵ (۵	Show	ing 50 of 25.03	30 result(s)	11/04/2022 10:16:06 -	10/06/2022 10:16:06							🛃 Export	🏉 Group rows b	y ••• More
		Severity	Status	Timestamp create	Host name	Scenario	Object	Rule id			Description			Scan Action
		LOW	• New	06/06/2022 09:03:17	ANM-HUNGTX	Execution	C:\Progr	Anomaly_Detection_ATTCK	_T1204_002_User_Execut	tion_Malicious_File	Detect attack technique [T1204_002]	Jser Execution: Mal	icious_File on A	N/A
~		MEDIUM	New	06/06/2022 09:03:17	ANM-HUNGTX	Execution	C:\Progr	Anomaly Detection_MITRE	ATT&CK_ATTCK_T1204_0	02_User_Execution	Detect attack technique [T1204_002]	Jser Execution: Mal	cious_File on A	N/A
Ē <u>.</u>		LOW	• New	06/06/2022 09:03:03	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
(m)		LOW	• New	06/06/2022 08:48:59	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
÷		LOW	• New	06/06/2022 08:22:03	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 08:02:14	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	initialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 07:56:25	VCS-HALTT	Execution	C:\Progr	Anomaly_Detection_ATTCK	_T1204_002_User_Execut	tion_Malicious_File	Detect attack technique [T1204_002] U	Jser Execution: Mal	cious_File on V	N/A
		MEDIUM	New	06/06/2022 07:56:25	VCS-HALTT	Execution	C:\Progr	Anomaly Detection_MITRE	ATT&CK_ATTCK_T1204_0	002_User_Execution	Detect attack technique [T1204_002] U	Jser Execution: Mal	cious_File on V	N/A
		LOW	New	06/06/2022 07:50:22	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	 New 	06/06/2022 07:39:01	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 07:29:10	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 07:19:01	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 07:07:00	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 06:58:54	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	 New 	06/06/2022 06:36:55	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	 New 	06/06/2022 06:26:55	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	promise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	 New 	06/06/2022 06:17:02	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 06:06:55	ANM-TRUONGL	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_I	InitialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 05:56:55	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A
		LOW	New	06/06/2022 05:46:57	ANM-TRUONGL.	Initial Access	C:\Windo	Windows_MITRE_ATT&CK_	InitialAccess_DriveByCom	npromise_T1189	Detect process C:\Program Files\Goo	gle\Chrome\Applica	tion\chrome.ex	N/A 🖌
	- 0		• New	86/86/2022 05236-54	ANM TRUONOL	Initial Access	C:Windo	Windows MITRE ATTROX	initialAccess DriveByCom	promiac T1109	Detect process 01Program Files\000	de) Ohrome' Apolicy	tion/chrome.cx	N/A

1 – Tìm kiếm dữ liệu theo truy vấn và thời gian:

+ Tìm kiếm dữ liệu theo câu lệnh truy vấn và sử dụng các câu lệnh truy vấn đã lưu;

+ Tìm kiếm dữ liệu theo thời gian.

- 2 Tìm kiếm nhanh;
- 3 Danh sách Alert và các thao tác với Alert:
 - + Xem danh sách Alert;
 - + Gom nhóm Alert;
 - + Xem tóm tắt Alert;
 - + Xem chi tiết 01 Alert;
 - + Xem biểu đồ điều tra (Investigation Graph);
 - + Đánh dấu không nguy hiểm (Set False Positive) cho 01/nhiều Alert;
 - + Tạo IR flow từ 01/nhiều Alert;
 - + Thêm 01/nhiều Alert vào IR flow;

Phân quyền dữ liệu tại tính năng như sau:

viettel

+ User đăng nhập thuộc group root: Hiển thị tất cả Alert trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị tất cả Alert thuộc group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Alert thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Alert thuộc group của user đang login;

3.3.1 Tìm kiếm Alert

Mục đích: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn đã lưu hoặc tìm kiếm nhanh để tìm kiếm Alert theo thời gian phát sinh Alert.

3.3.1.1 Tìm kiếm theo thời gian

Mặc định khi vừa truy cập vào hệ thống, tìm kiếm Alert theo 7 ngày gần đây; Mục đích: Cho phép thay đổi giá trị thời gian bằng cách chọn thời gian tuyệt đối hoặc thời gian tương đối:

+ Thời gian tuyệt đối: Là giá trị thời gian bắt đầu – thời gian kết thúc cụ thể, cho phép nhập hoặc chọn từ lịch, hỗ trợ định dạng ngày/tháng/năm giờ:phút:giây;

+ Thời gian tương đối: Là khoảng thời gian tương đối giữa thời gian bắt đầu và thời gian hiện tại;

VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = "Last 30 days".
Hệ thống tự động tìm ngược lại 30 ngày trước và bắt đầu tính từ 03:00 giờ của ngày đó.

→ Khoảng thời gian theo dõi: 03:00 08/05/2021 đến 03:00 07/06/2021.

3.3.1.2 Tìm kiếm nhanh

Mục đích: Hỗ trợ tìm kiếm Alert nhanh theo các trường:

- + Time: thời gian phát sinh Alert;
- + Status: trạng thái của Alert;
- + Severity: mức độ nguy hại của Alert;

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- + Scenario: kich bån sinh ra Alert;
- + Assigned to: người được phân công xử lý Alert;

3.3.1.3 Tìm kiếm theo câu query



- 1 Sử dụng câu query đã lưu trước đó để tìm kiếm;
- 2 Nhập câu query để tìm kiếm;

(*) Sử dụng câu query đã lưu trước đó để tìm kiếm

- **Bước 1:** Chọn query đã lưu trước đó tại combobox Use saved query *;
- Bước 2: Xem lại nội dung câu query trước khi chọn bằng cách chọn 💌;
- **Bước 3:** Trường hợp muốn xóa câu query cũ, di chuột qua bản ghi muốn xóa và chọn **a**;
- **Bước 4:** Click vào bản ghi muốn sử dụng để truy vấn, nội dung query cũ được hiển thị tại ô nhập query;

Use saved query $*$ fx host_name = "ADMIN-PC"	
Q Search name	
auto test 2 🔻	
host_name = "ADMIN-PC"	
testauto ►	111
test ▶	111
Hello >	1
test20 ⊳	
test15 ⊨	
test13 ⊨	
test12 ⊳	
-test ▶	

→ Trường hợp muốn thêm mới/chỉnh sửa nội dung câu query, có thể cập nhật

ngay tại ô nhập query và chọn

^{Save query} để lưu lại.





Lưu ý: nút save query chỉ hiển thị khi câu lệnh query đúng cấu trúc.

(*) Nhập câu query để tìm kiếm:

Bước 1: Nhập vào textbox Search câu query với format như sau:

<ten_truờng> <toán tử> "<value>" AND/OR <ten_trường> <toán tử> "<value>".....

Trong đó:

- + <tên_ trường> là các giá trị sau:
 - severity: độ nghiêm trọng của Alert
 - Alert_id: mã Alert
 - status: trạng thái của Alert
 - group: nhóm của sự kiện sinh Alert
 - hostname: Tên của máy trạm
 - scenario: kich bản sinh ra Alert dựa theo MITRE ATT&CK
 - ir_flow_name: tên IR flow mà Alert thuộc IR flow đó
 - assignee: người được phân công xử lý Alert
 - signature_id: mã sự kiện phát sinh Alert
 - rule_id: mã bộ luật phát sinh Alert
 - description: mô tả thông tin ngữ cảnh phát sinh Alert
- + <toán tử> là các giá trị:
 - = : tìm chính xác giá trị là value
 - != : tìm giá trị khác với value
 - ~: tìm giá trị like với value
 - AND/OR: toán tử kết hợp để kết hợp 2 câu query.



Bước 2: Click nút "Search".

+ Trường hợp không có kết quả phù hợp, hệ thống sẽ hiển thị thông báo:
 No data;

+ Trường hợp có kết quả phù hợp, hệ thống hiển thị mặc định 50 bản ghi theo thứ tự giảm dần theo thời gian. Để xem nhiều bản ghi hơn thực hiện scroll dữ liệu xuống cuối trang, hệ thống sẽ load 50 bản ghi tiếp theo;

+ Trường hợp câu query đúng cấu trúc và muốn lưu lại để sử dụng cho các lần tiếp theo, chọn save query và nhập tên gợi nhớ cho query:

2011 Hompaul	OTATIO		
Save query			>
Name			
search Alert list from alert_id			
Query			
alert_id ~ "20220609"			
			,
Set as default query			_
		Cancel	Sa

<u>*Lưu ý*</u>: nút ^{save query} chỉ hiển thị khi câu lệnh query đúng cấu trúc.

3.3.2 Danh sách Alert

Mục đích: Hiển thị danh sách Alert trong hệ thống;

Cho phép xem danh sách các Alert đáp ứng điều kiện tìm kiếm

save query 🔻 f	x alert_id ~ '	20220609"								Last 24 hours	Hide statis
REVEDITY	- Critical	- High	- Medium	- Low	— N	lo impact	STATIC	• New	 In progress 	False positive	Closed
OLAFULLI	0	2	0	0		0	STATUS	2	0	0	0
wing 2 of 2 result(s)	09/06/2022 09:06	27 - 10/06/2022 00/06/27								Export 1	coup rows by
owing 2 of 2 result(s)	09/06/2022 09:06 Severity	27 - 10/06/2022 09:06:27	Status	s ,	Ajiant event id	Agent id		Time	stamp create Target comm	上 Export 🛛 🔮 G	Group rows by •••• N Description Action
Wing 2 of 2 result(s) Host name ubuntu18	09/06/2022 09:06 Severity HIGH	27 - 10/06/2022 09:06:27 Alert id 20220609_173832_55307826	Statu: 7_618098_ • Net	s 4	Ajiant event id	Agent id D8EACAB11D	A9F0A3F0F65575E9E9C3	Time 313DC61A83B 09/04	stamp create Target comm 5/2022 17:38:31 N/A	Export () and andline Hash sha1 N/A	Group rows by •••• N Description Action Computer ubu

Bước 1: Chọn ^{View column} để lựa chọn các trường muốn hiển thị trên danh sách Alert:



Q Search field	
Selected	
 Target commandline 	Hash sha1
Alert id	 Host name
Agent id	 Timestamp create
Severity	Status
 Description 	 Ajiant event id
Others	
File hash sha1	Scan result
Malware type	Malware name
Classify	Assignee
Ir flow name	 Target process path md5

Tại đây có thể tìm kiếm trường thông tin theo tên trường, hỗ trợ chọn/bỏ chọn tất cả các trường;

Bước 2: Trên danh sách hỗ trợ các thao tác như sau:

+ Sắp xếp theo dữ liệu tại từng cột:

VD: Để sắp xếp dữ liệu theo trường thời gian tạo, click lần thứ nhất tại tên trường để sắp xếp theo thời gian tạo tăng dần Timestamp create, click lần thứ hai để sắp xếp theo thời gian tạo giảm dần Timestamp create, click lần thứ ba để bỏ sắp xếp, quay lại trạng thái ban đầu Timestamp create;

+ Kéo thả trường thông tin đến vị trí mong muốn:

	SEVERITY	- Critical O	High 2	- Medium 0	– Low O	 No impact 0 	STATUS	• New 2	• In pr C	ogress @ F)	alse positive O	• Close	ed
Show	ng 2 of 2 result(s)	09/06/2022 09	:06:27 - 10/06/2022 09:06:27							<u>ب</u> الح	port 🌔 G	roup rows by	••• More
	Host name	Severity	Alert id	Status	Ajiant ever	nt id Agent id			Timestamp create	Target commandline	Hash sha1	Description	Action
	ubuntu18	HIGH	20220609_173832_55307826	57_618098 • New	500	D8EACAB11	DA9F0A3F0F65575E9E9	C313DC61A83B	09/06/2022 17:38:31	N/A	N/A	Computer ubu	
	localhost.localdo	HIGH	20220609_113824_26780358	4_564214 • New	500	31F6FA3729	44D72C2DC854E155A63	170CE9686AD	09/06/2022 11:38:23	N/A	N/A	Computer loca	
	1. Chọn cộ tin muốn	ột (trường thôn 1 thay đổi vị trí	g	2. Kéo thầ	tới vị tri mong muốn								

+ Click 01 lần để xem thông tin chi tiết hoặc chọn ^{•••} và chọn "View detail", chi tiết xem trong <u>3.3.4 Xem chi tiết Alert</u>



+ Chọn và chọn "Update status" để cập nhật trạng thái cho Alert (Update status to "False Positive" hoặc Update status to "Close", xem trường hợp đánh dấu 01 Alert trong

+ Chọn và chọn "Add to IR Flow" để đưa Alert vào IR flow, xem trường hợp đưa 01 Alert vào IR flow đã tồn tại trong <u>3.3.8 Thêm 01/nhiều Alert hoặc nhóm</u> <u>Alert vào IR flow đã có</u> hoặc vào IR flow mới trong <u>3.3.6 Tạo IR flow từ 01/nhiều Alert</u> <u>hoặc nhóm Alert</u>

+ <u>Chọn</u> dễ xem lý do đánh dấu không nguy hiểm tại các Alert đang ở trạng thái "FALSE POSITIVE"..

Bước 1: Sau khi đã thao tác trên các bản ghi xong, cho phép chọn 01 hoặc nhiều bản ghi bằng cách click chọn □ tại đầu mỗi Alert để tiếp tục thao tác, hỗ trợ các thao tác sau:

SEVERITY	- Critical O	- High 2	- Medium 0	- Low O	 No impact 0 	STATUS	• New 2	 In progress 0 	 False positive O 	e Close O	ed
Showing 2 of 2 result(i) 09/06/2022 09:06	:27 - 10/06/2022 09:06:27							Export ب	Group rows by	••• More
Selected 2 alert(s)	🖌 Update status	Add to IRFlow	🕁 Export data Clea	r selection							
 Host name 	Severity O	Agent id		Status	Ajiant event id	Alert id	Times	tamp create Target co	mmandline Hash sh	a1 Description	Action
ubuntu18	HIGH	D8EACAB11DA9F0A3F0F	65575E9E9C313DC61A83	B • New	500	20220609_173832_5530 8	178267_61809 09/06	/2022 17:38:31 N/A	N/A	Computer ubur	
 localhost.locale main 	lo HIGH	31F6FA372944D72C2DC8	354E155A63170CE9686AE	• New	500	20220609_113824_2678 4	03584_56421 09/06	/2022 11:38:23 N/A	N/A	Computer loca	

Bước 2: Chọn [™] Add to IRFlow</sup> để thêm Alert vừa chọn vào IR flow để xử lý.

Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ Alert được chọn đều ở trạng thái = "NEW", nếu có ít nhất một Alert đang ở trạng thái khác "NEW", Hệ thống ẩn đi các

thao tác ^{Selected 1 alert(s)} **Update status ™** Add to IRFlow **▲** Export data Clear selection . Chi tiết xem trong trường hợp đưa 01 Alert vào IR flow mới trong <u>3.3.6 Tạo IR flow từ 01/nhiều Alert</u> <u>hoặc nhóm Alert</u> hoặc thêm vào IR flow đã tồn tại trong <u>3.3.7 Thêm 01/nhiều Alert</u> <u>hoặc nhóm Alert vào IR flow đã có</u>

+ Chọn dể cập nhật trạng thái của Alert:



Update status to:		
False Positive		~
Comment		
Write something		
		/i
	Cancel	

Chọn Update Status to "False Positive" để đánh dấu không nguy hiểm

cho Alert;

• Chọn Update Status to "Close" để đóng Alert;

Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ Alert được chọn đều ở trạng thái = "NEW", nếu có ít nhất một Alert đang ở trạng thái khác "NEW", thao tác sẽ bị ẩn đi . Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 Alert trong <u>3.3.5 Đánh</u> dấu không nguy hiểm cho 01/nhiều Alert hoặc nhóm Alert

+ Chọn ^{± Export data} để trích xuất các Alert đang được chọn.

3.3.3 Gom nhóm Alert

Mục đích: Cho phép gom nhóm các Alert theo 01 hoặc nhiều tiêu chí: hostname, scenario, group, ruleid;

Bước 1: Sau khi tìm kiếm có thể gom nhóm Alert lại, chọn ^{Group rows by...} để lựa chọn các tiêu chí muốn sử dụng làm tiêu chí gom nhóm Alert;

Q Search field	
 Target commandline 	 File hash sha1
Hash sha1	Scan result
 Malware type 	 Malware name
Classify	Assignee
Ir flow name	 Target process path md5
Net flag	 Net source ip
Service target path sha1	 File path request file id
 Target domain name 	Group
	Cancel Apply

Hỗ trợ tìm kiếm theo tên tiêu chí và lựa chọn 01 hoặc nhiều tiêu chí đê gom nhóm.



Bước 2: Chọn dễ áp dụng.

Những Alert có cùng các tiêu chí đã chọn và có cùng trạng thái và đang ở cùng IR flow (nếu có) sẽ được gom lại 1 dòng trong danh sách kết quả.

Showing 7 group(s) of 390 result(s) 11/05/2022 09:53:31 - 10/06/2022 09:53:31	Change fields for grouping▼ Ungroup	••• More
Fields	Number of alerts	Action
target_commandline: N/A ajiant_event_id: N/A	189	
target_commandline: N/A ajlant_event_id: 3	7	
target_commandline: N/A ajiant_event_id: 11	155	
target_commandline: N/A ajiant_event_id: 13	2	₽Q.
target_commandline: N/A ajiant_event_id: 23	1	
target_commandline: N/A ajiant_event_id: 400	1	
target_commandline: N/A ajiant_event_id: 500	35	

Trong đó:

- + Các trường được sử dụng làm tiêu chí gom nhóm sẽ được bôi đậm;
- + Hiển thị số lượng các Alert được gom nhóm tại tiêu chí đã chọn.
- **Bước 3:** Để bỏ gom nhóm, thực hiện tương tự nhưng không chọn tiêu chí nào và chọn "Apply";

Q Search field	
Selected	
 Target commandline 	 Ajiant event id
Others	
File hash sha1	Hash sha1
 Scan result 	 Malware type
 Malware name 	Classify
Assignee	Ir flow name
 Target process path md5 	 Net flag
Net source ip	 Service target path sha1
	Cancel Apply

3.3.4 Xem chi tiết Alert

Mục đích: Cho phép xem thông tin chi tiết Alert, hỗ trợ tự động làm đa dạng thông tin bằng cách tự động thu thập thông tin các sự kiện liên quan đến Alert vừa phát sinh, cung cấp biểu đồ trực quan để xem nhanh mối quan hệ giữa các đối tượng có trong Alert;


High 20220609_173832_553078267_618098 First seen: 09/06/2022 17:38:31 · Last update: 09/06/2022 17:38:31		2 State of the IRFlow Endet events ★ Enhance Alert 🖬 Update status 💌 🗙
● GROUP default		Li HOST NAME Ubuntu18
Detail Raw data		3
Description	Source event logs	
Computer ubuntu18 was disconnected at least 30 days	This section defines source event li	st of this alert, which creates and contains more context information for this alert.
Rule ID <u>Anomaly Detection_Monitor_Agent_Disconnect</u>	1 result(s)	Show columns
	SystemTimeStamp Ever	nt ID Description
	09/06/2022 17:38:30 500	Agent was disconnected
	Advanced	^
	Host	
	This information is about suspiciou	s host.
	Client id	D8EACAB11DA9F0A3F0F65575E9E9C313DC61A83B
	Hostname	ubuntu18
	Network Connection	
	This information is about suspiciou	is network connection.
	MAC	00.0c:29.fb:19.eb
	Others	
	These other information provides m	nore context about this alert collected by VCS-aJiant.
	Create time	09/06/2022 17:38:30
	Log provider name	AdvanceCollector
	Source log	mixed
	Sub category	Monitor
	Description	Computer ubuntu18 was disconnected at least 30 days

1 – Nhóm thông tin chung của Alert, trong đó:

2 –

+ Status: Hiển thị trạng thái của Alert (New, In Progress, False Positive, Closed);

+ Severity: Phân loại Alert theo mức độ nguy hại (Critical, High, Medium, Low);

- + Alert_id: Hiển thị thông tin id của Alert;
- + First seen: Thời gian Alert được tạo;
- + Last seen: Thời gian gần nhất Alert được cập nhật;
- 3 Nhóm các thao tác với Alert

+ Chọn dễ đưa Alert vào IR flow, xem trường hợp đưa 01 Alert vào IR flow đã tồn tại trong <u>3.3.7 Thêm 01/nhiều Alert hoặc nhóm Alert vào IR flow đã có</u> hoặc vào IR flow mới trong <u>3.3.6 Tao IR flow từ 01/nhiều Alert hoặc nhóm Alert</u>

tte	el ity	
+	Chọn ^{dupdete status} để d	cập nhật trạng thái của Alert:
		Update status to:
		False Positive 🗸
		Comment
		Write something
		Cancel Update status

Chọn Update Status to "False Positive" để đánh dấu không nguy hiểm cho Alert;

• Chọn Update Status to "Close" để đóng Alert;

Lưu ý: Thao tác này chỉ áp dụng khi Alert được chọn ở trạng thái = "NEW", thao tác sẽ bị ẩn đi. Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 Alert trong <u>3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều Alert hoặc nhóm Alert;</u>

+ Chọn ^{■ enterent} để chuyển đến tính năng Event Search với thời gian mặc định là 04 tiếng trước và sau thời gian phát sinh Alert;

+ Chọn 🔽 để xem logs hoạt động liên quan đến Alert;

💷 khaith und	date status into Closed
22/04/2022 18:0	07:01
In progress	
🗄 khaitb add	ded the alert into the IR Flow <u>IRF_Demo</u>
22/04/2022 17:4	48:52
New	
VCS-aJiar	nt created the alert.
2/04/2022 17-	35:48

- 4 Tab các thông tin liên quan đến Alert:
 - + Tab Detail: Cho phép hiển thị toàn bộ thông tin chi tiết liên quan tới Alert;



Detail Raw data					
Description ^	Source event logs	2 ^			
Detect attack technique T1562.004: Disable or Modify System	No tracked events!				
files\dell\supportassistagent\bin\supportassistagent.exe (PID =	Advanced ^				
Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe") is	File				
creating child process with path = C:\windows\system32\netsh.exe (commandline = "netsh.exe"	This file is impacted (created/modified/deleted/executed) suspiciously.				
http delete ssicert ipport=0.0.0.0:5700, PID = 9732) to the disable firewall.	Target process path	Signed C:\windows\system32\netsh.exe			
Rule ID <u>Anomaly_Detection_ATTCK_T1562_004_Disa</u>	Source process path	Source process path Unknown C\program files\dell\supportassistagent\bin\supportassistagent.exe			
	Process				
	This source/target process has suspicious behaviours.				
	Target process path	Signed C:\windows\system32\netsh.exe			
	Source commandline	Unknown "C:\Program Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe"			
	Target commandline	Unknown "netsh.exe" http delete sslcert ipport=0.0.0.0:5700			
	Source process path	Unknown C:\program files\dell\supportassistagent\bin\supportassistagent.exe			
	Host				
	This information is about suspicio	us host.			
	Client id	9C4C8D5F62C98BE5918732E0D8D91DCD01121CD2			
	Ip dcn	10.61.188.2			
	MAC Address	a8:6b:ad:71:14:2b,1a:6b:ad:71:14:2b,2a:6b:ad:71:14:2b,00:50:56:c0:00:01,00:50:56:c0:00:08,48:4d:7e:ba:be:53			
	Others	_			
	These other information provides r	nore context about this alert collected by VCS-aJiant.			

• Khung thông tin (1) Description: Cho phép hiển thị thông tin mô tả chi tiết Alert và RuleID;

- Khung thông tin (2):
 - Source event logs: Ghi lại Source event logs liên quan đến Alert (nếu có);
 - Advance: Thông tin nâng cao liên quan đến Alert bao gồm: File, Process, Host, Others, ...

3.3.5 Biểu đồ điều tra (Enhance Alert)

Mục đích: Cho phép hiển thị mối quan hệ của các đối tượng trong Alert, xem chi tiết các đối tượng và hỗ trợ điều tra loang dựa trên tập các sự kiện thu thập được trong hệ thống.



🖩 Unknown 📲 Clean 🧧 Su	spicious 📕 Malicious	Host detail		×
		General		
FILÈ SÉRVICE		HOST NAME	Win7x64_MayaoHai	
		HOSTID	fe2a4ba0-b348-4a43-bd26-79995feb57e9	
Band Report of the second seco		STATUS	Offline	
a the second second		SET UP VERSION	N/A	
ULEY CNIS 21/05/2021 14:24:23		GROUP	default	
OUTERT ON'S WIDTY 664, Mayao Haj		UPDATE GROUP	release	
		POLICY	full_features	
224.99.28.3		IP DCN	10.61.188.2	
		OS	windows	
	_	FIRST PING	12/05/2021 16:02:02	
	-	LAST PING	26/05/2021 14:23:17	
1	Q	Platform		~
	Q	CPUs		~
	۲	Network Interfaces		~
1	井	Default Gateway		2

- 1 Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ
- 2 Khu vực hiển thị thông tin chi tiết các đối đượng trên biểu đồ

3.3.5.1 Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ

Cho phép hiển thị trực quan các đối tượng trong Alert phục vụ xem thông tin và điều tra;

Mặc định khi vừa truy cập, biểu đồ hiển thị thông tin liên quan đến máy gốc phát sinh Alert, cụ thể như sau:



Trong biểu đồ luôn có 01 máy được cắm cờ [™] để đánh dấu máy gốc phát sinh Alert, mặc định tại mỗi máy luôn đi kèm các đối tượng có quan hệ trực tiếp máy gốc trong vòng 01 ngày kể từ thời điểm phát sinh Alert, danh sách các đối tượng bao gồm:



NETWORK	DEFAULT					
USER	O DEFAULT					
REGISTRY	DEFAULT	KEY	VALUE			
FILE	DEFAULT	DOC	EXCEL EXCEL	POWERPOIN	т	
		<%> .ASP	.JS	 .PHP	SCPT	VBS .VBS
HOST	ě.	SERVICE	¢°	PROCESS	C.	
SCHEDULED TASK	Ľ _o	DNS QUERY	DNS	WMI	ф wMi	

Mỗi đối tượng bao gồm các trạng thái như sau: ^{Clean} Suspicious Malicious Giữa các đối tượng, hiển thị mối quan hệ bao gồm:

+ Relationship: Mối quan hệ định nghĩa theo các sự kiện phát sinh trong vòng 01 ngày từ thời điểm phát sinh Alert (trong đó tên mối quan hệ nằm phía trên

mũi tên nối liên 02 đối tượng)

+ Reference: Mối quan hệ tham chiếu, là các đối tượng khác ghi nhận được trong sự kiện chính phát sinh ra đối tượng (được thể hiện bởi nét đứt và không có tên quan hệ cụ thể)

Ví dụ:





Các thao tác hỗ trợ hiển thị biểu đồ bao gồm:

Thao tác hỗ trợ hiển thị	Ý nghĩa
	Cho phép ẩn/hiện các thông tin trên biểu đồ:
Hide reference i Hide relationship name	+ Reference: Khi chọn, cho phép ẩn/hiện thông tin tham chiếu bao gồm mũi tên nét đứt và đối tượng tham chiếu tại tất cả các đối tượng hiện có trên biểu đồ;
	+ Relationship name: Khi chọn, cho phép ẩn/hiện thông tin tên mối quan hệ phía trên tất cả các mũi tên nét liền hiện có trên biểu đồ
Q	Cho phép zoom in/zoom out biểu đồ tương ứng tại vị trí đang trỏ chuột
Q	Ngoài ra có thể lăn chuột tại vị trí muốn zoom in/out để thao tác nhanh



•	Cho phép quay lại vị trí trung tâm của biểu đồ (máy gốc)
ί	Cho phép mở rộng màn hình tối đa để xem biểu đồ và thao tác trên biểu đồ

Ví dụ một biểu đồ mặc định như sau:



+ Trường hợp tại mỗi loại đối tượng có nhiều hơn 01 đối tượng trực thuộc, các đối tượng sẽ được tự động nhóm lại.

+ Hover để xem thống kê nhanh tại từng nhóm đối tượng như sau:



Từ đây, muốn điều tra loang tiếp các đối tượng thực hiện các bước như sau:
 Bước 1: Click chọn nhóm đối tượng muốn xem, hiển thị giao diện như sau:



Obje	Objects in this group network					
Q	Search object					٩
🗹 Uni	known (48) 🛛 Clean (1	25) Z Malicious (87)				View column 🔻
Selecte	ed 1/20 node(s) 🛛 🔍 Show	on graph Clear selection				
	STATUS	DOMAIN ADDRESS	IP	LOCAL PORT	PROCESS NAME	ACTION
	Clean	ocsp.verisign.com	240.100.28.3	N/A	SYSTEM	R
	Clean	crl4.digicert.com	80.105.28.3	N/A	SYSTEM	۳Q
	Clean	crl.microsoft.com	16.87.28.3	N/A	SYSTEM	۳Q
	Malicious	www.microsoft.com	96.103.28.3	N/A	SYSTEM	R
	Clean	ocsp.digicert.com	240.94.28.3	N/A	SYSTEM	R
	Clean	crl.verisign.com	224.91.28.3	N/A	SYSTEM	R
	Malicious	www.msftncsi.com	0.96.28.3	N/A	SYSTEM	R
	Clean	csc3-2010-crl.verisign.com	112.89.28.3	N/A	SYSTEM	R
	Clean	ocsp.globalsign.com	48.88.28.3	N/A	SYSTEM	R
	Clean	crl4.digicert.com	80.105.28.3	N/A	SYSTEM	đ
Show	ring 20/260 result(s)					

+ Cho phép lọc các đối tượng trong nhóm theo trạng thái • UNHOWN • Clean • SUSPICIONS • MAILCOUS hoặc tìm kiếm nhanh bằng cách nhập nhập dữ liệu muốn tìm kiếm trong tất cả các trường;

+ Khi đã chọn được đối tượng phù hợp, chọn <a> dể hiển thị 01 đối tượng lên biểu đồ hoặc chọn <a> show on graph dể chọn tối đa 20 đối tượng lên biểu đồ;

<u>Lưu ý</u>: Nếu đối tượng được mở rộng là một máy tính, mặc định khi hiển thị đối tượng, cũng tự động hiển thị các đối tượng các quan hệ trực tiếp đến máy tính trong vòng 01 ngày kể từ thời điểm phát sinh Alert



Page | 44



Bước 2: Sau khi đã hiển thị các đối tượng cần điều tra trên biểu đồ, các thao tác hỗ trợ mở rộng/thu gọn bao gồm:

+ Tại máy gốc/máy tính thường: Hỗ trợ thu gọn các đối tượng về trạng thái mặc định khi hiển thị máy (Chỉ bao gồm các đối tượng có quan hệ trực tiếp với máy, mỗi loại đối tượng nếu nhiều hơn 01 đối tượng, hiển thị dạng nhóm) bằng cách chọn chuột phải tại đối tượng, sau đó chọn "Group child-level objects";



+ Tại các đối tượng khác: Hỗ trợ thu gọn bằng cách nhóm lại theo loại đối tượng và loại quan hệ với các đối tượng cùng cấp bằng cách chọn chuột phải tại đối tượng, sau đó chọn "Group same-level objects";

æ	
0.96	Group same-level objects
	Unpin
_	

+ Tại đối tượng là tiến trình (process) cho phép mở rộng để điều tra loang bằng cách chọn chuột phải tại đối tượng,

+ Trường hợp không thể tiếp tục loang, hiển thị:

1	No more objects to add Unpin
	Unpin

+ Trường hợp có thể loang, chọn "Add more objects..."





maii	Add more objects Unpin	
------	---------------------------	--

Hiển thị giao diện cho phép chọn đối tượng muốn loang đến

Show more object			10				×		
Files	1	Create Key Delete Value	Set Value				2		
Network Process	5	Q Search object							
Registry	3	Malicious (3)					View column 🔻		
		STATUS	DOMAIN ADDRESS 🚔	IP ♣	LOCAL PORT 🛱	PROCESS NAME	ACTION		
		Malicious	N/A	127.0.0.1	1588	main.exe	ବ୍ଦି		
		Malicious	N/A	127.0.0.1	6668	main.exe	ଟ୍ଦି		
		Malicious	N/A	0.0.0.0	0	main.exe	ලේ		
							3		
1		Showing 1/1 result(s)							

- 1 Chọn loại đối tượng;
- 2 Chọn loại quan hệ từ tiến trình tới đối tượng;
- 3 Chọn trực tiếp đối tượng muốn hiển thị. Hỗ trợ tìm kiếm theo trạng thái độc/sạch của đối tượng hoặc tìm kiếm theo nội dung có tại các trường thông tin của đối tượng.

+ Chọn vercourne để lựa chọn các trường thông tin hiển thị hoặc dùng tính năng ⁺ để sắp xếp thông tin trong danh sách

+ Khi đã chọn được đối tượng phù hợp, chọn <a>

 lên biểu đồ hoặc chọn <a>

 (<a>show on graph

 để chọn tối đa 20 đối tượng lên biểu đồ;

+ Tại đối tượng là tiến trình (process), khi có các đối tượng đang được mở rộng cho phép thu gọn lại bằng cách chọn chuột phải tại đối tượng;



Collapse all Unpin	mai	Add more objects
Unpin		Collapse all
		Unpin

+ Mặc định tại biểu đồ, các đối tượng tự động chạy và giữ khoảng cách với nhau khi bị di chuyển. Trường hợp dùng chuột chọn và kéo thả các đối tượng, sau khi bỏ chuột đối tượng tự động được Pin vào vị trí mới. Để hủy thao tác Pin, chọn Unpin

0	
Add more objects	
Collapse all	
Unpin	

3.3.5.2 Khu vực hiển thị thông tin chi tiết

Là tính năng bổ sung của biểu đồ, cho phép hiển thị thông tin chi tiết của các thành phần trong biểu đồ (bao gồm các đối tượng và mối quan hệ trong biểu đồ);



Host detail		×
General		
HOST NAME	Win7x64_MayaoHai	3 Сору
HOST ID	fe2a4ba0-b348-4a43-bd26-79995feb57e9	
STATUS	Offline	
SET UP VERSION	N/A	
GROUP	default	
UPDATE GROUP	release	
POLICY	full_features	
IP DCN	10.61.188.2	
OS	windows	
FIRST PING	12/05/2021 16:02:02	
LAST PING	26/05/2021 14:23:17	1
Platform		~
CPUs		~
Network Interfaces		~
Default Gateway		2 ~

- Nhóm thông tin chung: Bao gồm các thông tin chung/thông tin định danh của đối tượng, mặc định luôn hiển thị khi vừa truy cập;
- 2 Nhóm thông tin chi tiết: Bao gồm các thông tin chi tiết của đối tượng,
 được phân thành các nhóm thông tin khác nhau, mặc định các nhóm thông tin này sẽ được đóng lại, chọn č để mở rộng và hiển thị nhóm thông tin.
 - + Thao tác Copy hỗ trợ sao chép nội dung trường thông tin

Lưu ý: Một số trường thông tin định danh đối tượng cho phép link nhanh để tra cứu trong Event Search hoặc Agent Management.



Process detail	×
General	
PROCESS ID	1432
PROCESS NAME	main.exe
MD5	1e092a44d44c29ef8d6bfc3a74f34b73
SHA26	1941d3f261033344b22c5e9cf246e5683c17d450ac87d0af6f 3ed7a52f431bb6
PROCESS PATH	C:\users\admin\desktop\taodataloang\main.exe
FILE COMPANY	N/A
FILE DESCRIPTION	N/A
FILE VERSION	N/A
FILE PRODUCT	N/A
USER NAME	admin
COMMANDLINE	.\main.exe
INTEGRITY LEVEL	HIGH

3.3.6 Cập nhật trạng thái không nguy hiểm hoặc đóng cảnh báo cho 01/nhiều Alert hoặc nhóm Alert

Mục đích: Cho phép đánh dấu Alert là không nguy hiểm;

Bước 1: Chọn 01/nhiều Alert muốn đánh dấu không nguy hiểm;

Bước 2: Chọn dể cập nhật trạng thái của Alert:

False Positive		~
Comment		
Add to False Positive		
		/
	Cancel	Update status



Bước 3: Chọn Update Status to "False Positive";

Bước 4: Nhập lý do đánh dấu không nguy hiểm và:

 Chọn " Update status" để xác nhận đánh dấu không nguy hiểm cho Alert;

Chọn "Cancel" để xác nhận hủy thao tác đánh dấu không nguy hiểm cho Alert;

Chọn Update Status to "Close" để đóng Alert;

Bước 1: Chọn 01/nhiều Alert muốn đóng (Closed);

Bước 2: Chọn dễ cập nhật trạng thái của Alert:

Closed		~
Comment		
done		

Bước 3: Chọn Update Status to "Closed";

- Bước 4: Nhập lý do đóng Alert và:
 - Chọn " Update status" để xác nhận đóng Alert;
 - Chọn "Cancel" để xác nhận hủy thao tác đóng Alert;

3.3.7 Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert

Bước 1: Lựa chọn 01/nhiều Alert để tạo IRFLow và chọn "Add to IR Flow";



	Showin	ig 4 of 4 repult(s) 09/06/2022 11:50	00 - 10/06/2022 11:50:00					🕁 Export 🕕 Group rows by	··· More
	Sele	cted 2 alert(s)	🖌 Update status	Add to IRFlow	🛃 Export data 🛛 🔾	clear selection				
0	-	Severity	Status	Timestamp create	Host name	Scenario	Object	Rule id	Description	Action
٩		LOW	New	10/06/2022 07:34:15	DESKTOP-R2GBJE	Suspicious Behavio	C:\Windo	Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005	Detect process [C:\Windows\System32\svchost.exe] (PID: [1096]) i	it
		LOW	New	09/06/2022 18:09:26	DESKTOP-R2GBJE	Suspicious Behavio	C:\Windo_	Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005	Detect process [C:\Windows\System32\svchost.exe] (PID: [1096]) i	t :
		HIGH	• New	09/06/2022 17:38:31	ubuntu18	N/A	N/A	Anomaly Detection_Monitor_Agent_Disconnect	Computer ubuntu18 was disconnected at least 30 days	
L		LOW	New	09/06/2022 15:05:02	DESKTOP-R2GBJE	Suspicious Behavio	C:\Windo	Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005	Detect process [C:\Windows\System32\svchost.exe] (PID: [1096]) in	1

Bước 2: Nhập các thông tin và tạo IRFLow:

New IR Flow		×
R Flow name		
new_critical_IRFlow		
Assignee(s)		
. root ×		• •
Note (optional)		
Write something		
List of alerts		
List of alerts	Host name	Action
List of alerts Alert ID 20220606_18134_278220	Host name 796_546256	Action
List of alerts Alert ID 20220606_18134_278220 20220606_18153_440049	Host name 796_546256 062_394732	Action
List of alerts Alert ID 20220606_18134_278220 20220606_18153_440049	Host name 796_546256 062_394732	Action
List of alerts Alert ID 20220606_18134_278220 20220606_18153_440049	Host name 796_546256 062_394732	Action
List of alerts Alert ID 20220606_18134_278220 20220606_18153_440049	Host name 796_546256 062_394732	Action

Dữ liệu hiển thị trong Combobox Assigned to bao gồm:

- + User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị tên User đang login;

+ User đăng nhập thuộc group cha: Hiển thị tất cả tên User thuộc group con của user đang login và user đang login;



+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tên User đang login;

Bước 3: Sau khi thêm 1 hoặc nhiều Alert vào luồng xử lý IR flow, có thể hoàn tác trong 10s:

+ Để hoàn tác: chọn "Cancel" trong 10 s;

+ Để tạo ngay IR flow và chuyển sang màn hình IR flow chọn tên IR flow vừa tạo: chọn "Add to IR Flow";

3.3.8 Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có

Tương tự như 3.3.5 nhưng không chọn "Add new IRFlow" mà chọn IR flow đã có từ danh sách chọn;

Q Search IR Flow	New IR Flow
na test	
win7edr	
winedr	
asd1	
S	
ZXC	
12123	

Hệ thống hiển thị popup Xác nhận thao tác thêm 1 hoặc nhiều Alerts vào luồng xử lý IRFLow có sẵn trong hệ thống:





3.4 Màn hình IRFLow

3.4.1 Danh sách hiển thị

Mục đích: Cho phép hiển thị danh sách IRFlow trong hệ thống theo phân quyền người dùng:

+ User đăng nhập thuộc group root: Hiển thị tất cả IRFlow trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị tất cả IRFlow được assign cho user đang login;

+ User đăng nhập thuộc group cha: Hiển thị tất cả IRFlow được assign cho user đang login và các user thuộc group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả IRFlow được assign cho user đang login;

3.4.2 Tìm kiếm IRFLow

Mục đích: Cho phép tìm kiếm được những bản ghi IRFlow theo phân quyền người dùng đăng nhập;

Tương tự chức năng tìm kiếm ở màn hình Alert, màn hình IRFLow hỗ trợ tìm kiếm theo query như sau:

=	aJiant IR Flow							# 0
2 •	IR Flow management assignee != 'anhm' AND status = 'NEW'	1) Last 60 day	g Guidelines					
P±	10 result(s) 14/04/2022 09:29:50 -		+ Create					
۲	TIME	* NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE		ACTION
-	09/06/2022 18:05:32	test66	New	root	root			Ð ()
6	09/06/2022 15:25:52	win7edr	New	root	root) ()
	30/05/2022 11:08:58	phula_test_0530	New	root	root) ÷
÷	04/05/2022 11:08:43	test_tnn4	New	root	test_tnn) ÷
E7	04/05/2022 11:08:22	test_tnn3	New	root	test_tnn) (j
Q	04/05/2022 11:08:03	test_tnn2	New	root	test_tnn) (j
	04/05/2022 11:07:42	test_tnn_1	New	root	test_tnn			÷ 0
	04/05/2022 11:03:20	test1	New	root	anhvn	tạo luông		→ ○
	29/04/2022 10:29:09	testttt	New	anhvn	anhvn			→ ○
	27/04/2022 13:51:00	test_test	New	root	admin) (j
	Showing 10/10 result(s)							

Bước 1: Nhập vào textbox Search câu query với format như sau:

<ten_truờng> <toán tử> "<value>" AND/OR <ten_trường> <toán tử> "<value>".....





Trong đó:

- + <tên_ trường> là các giá trị sau:
 - assignee: người được phân công xử lý Alert;
 - created_by: tài khoản tạo IRFLow;
 - name: Tên của IRFLow;
 - notation: lưu ý của IRFlow;
 - status: trạng thái của IRFlow;
- + <toán_tử> là các giá trị sau:
 - = : tìm chính xác giá trị là value;
 - != : tìm giá trị khác với value;
 - ~: tìm giá trị like với value;
 - AND/OR: toán tử kết hợp để kết hợp 2 câu query.
- **Bước 2:** Chọn khoảng thời gian tìm kiếm bằng cách click vào nút "Date & Time" và chọn khoảng thời gian tùy ý. Nếu không chọn mặc định là Last 7 days;

Bước 3: Click on "Search"

Ngoài ra hỗ trợ tìm kiếm theo lịch sử tìm kiếm

=	aJiant IR Flow										
r.	IR Flow management									uidelines	
A	sssgree - "admir" 👩									Q	
101	Q assignee = "anhin" OR assignee = "anhin" AND Last 60 days								_	_	
Ŧ	Q assignee I= "anhvn" AND status I= "HEW" AND Last 60 days								+ Create		
۲	Q assignee is "anihun" AND status = "IEW" AND Last 60 days								ACTION		
5	Clear history search									0	
										0	
	09/06/2022 18:05:32	test66	New	root	root			÷	<u>با</u>	0	
÷.	09/06/2022 15:25:52	win7edr	New	root	root				<u>ه</u>	0	
EA	30/05/2022 11:08:58	phula_test_0530	New	root	root			4	<u>ه</u>	0	
ē	04/05/2022 11:08:43	test_tnn4	New	root	test_tnn	ZX		1) (0	
	04/05/2022 11:08:22	test_tnn3	New	root	test_tnn	ff		1) (0	
	04/05/2022 11:08:03	test_tnn2	New	root	test_tnn	def		e))	0	
	04/05/2022 11:07:42	test_tnn_1	New	root	test_tnn	abc		4	<u>،</u> ا	0	
	04/05/2022 11:03:20	test1	New	root	anhvn	tạo luông		12	•	0	
	29/04/2022 10:29:09	testttt	New	anhvn	anhvn			12) (0	
	27/04/2022 13:51:00	test_test	New	root	admin	sfds		10) (0	
	Showing 12/12 result(s)										

Để vào xem thông tin chi tiết 1 IRFlow và thực hiện các hành động điều tra, xử lý người dùng chọn "IRFLow Detail":



≡	aJiant IR Flow						₩ 0
e	IR Flow management	Ø Guidelines					
▲	assignee = "admin" OR assignee = "anhvn"	A) Last 60 days					
۴±	13 result(s) 14/04/2022 09:41:32 - 13/	x6/2022 09:41:32					+ Create
۲	тіме *	NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE	ACTION
-	13/06/2022 09:41:52	chuyen	New	root	chuyennt		
6	13/06/2022 09:36:11	new_chuyennt2	Closed	root	root, chuyennt		0
S	13/06/2022 09:34:10	chuyennt2	Closed	root	root		View detail
_	09/06/2022 18:05:32	test66	New	root	root		to e

3.4.3 Cách tạo IRFlow

Bước 1: Click vào "Create";

=	aJiant IR Flow						8		
e B	IR Flow management								
▲	assignee - 'admin' OR assignee - 'admin'								
Έ	13 result(s) 14/04/2022 09:41:	:32 - 13/06/2022 09:41:32					+ Create		
۹	TIME	♥ NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE	ACTION		
_	13/06/2022 09:41:52	chuyen	New	root	chuyennt		Ð ()		
6	13/06/2022 09:36:11	new_chuyennt2	Closed	root	root, chuyennt		0		
S	13/06/2022 09:34:10	chuyennt2	Closed	root	root		View detail		
-	09/06/2022 18:05:32	test66	New	root	root		Ð 0		

Bước 2: Hệ thống hiển thị Popup form Create New IRFlow, nhập thông tin hợp lệ;

Dữ liệu hiển thị trong Combobox Assigned to:

- + User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị tên User đang login;

+ User đăng nhập thuộc group cha: Hiển thị tất cả tên User thuộc group con của user đang login và user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tên User đang login;



Create New IR Flow		×
IR flow name	Type IR flow name	
Assigned to	Choose assignees	
First note	Type first note	
	Cancel	

Bước 3:

+ Người dùng chọn nút "Create", Hệ thống ghi nhận IRFlow vừa tạo và hiển thị trên màn hình danh sách IRFlow;

+ Người dùng chọn nút "Cancel", Hệ thống hủy thao tác thêm mới IRFlow vừa tạo và quay về màn hình danh sách IRFlow;

3.4.4 Các bước thực hiện trong IRFlow

Sau khi tạo IRFlow từ các Alert hoặc đưa các Alert vào IRFlow, người vận hành sẽ vào trang IRFlow để thực hiện các hành động sau:

+ Xem các thông tin để điều tra: danh sách Alert, máy tính có Alert, các đối tượng liên quan (file/registry/process);

+ Cô lập các máy phát sinh Alert: cô lập mạng, cô lập tiến trình;

+ Điều tra và phát hiện các đối tượng liên quan đến Alert (artifacts);

+ Phản ứng: xử lý các kết quả đã điều tra. Ví dụ: kill tiến trình mã độc, xóa file mã độc, xóa các registry do mã độc sinh ra ...

+ Kết thúc điều tra: đóng IRFlow, dừng cô lập máy, đóng các phiên ProcessAnalysis và LiveResponse;



3.4.5 IRFLow – Detection

Mục đích: Tab Detection cho phép hiển thị các đối tượng liên quan đến Alert như:

- + Danh sách máy tính có Alert;
- + Danh sách Alert;
- + Danh sách artifacts được phát hiện trong quá trình điều tra (investigation);

		Detection	Containment	Investigation	Response		
Original detection							
Agent DESKTOP-HHN2B1Q							
Alert							
TIME	GROUP		HOSTNAME		SCENARI	10	SEVERITY
07:00:00 14/01/2019	no_group		DESKTOP-HHN2B1Q		Executi	on	High
07:00:00 14/01/2019	no_group		DESKTOP-HHN2B1Q		Executi	on	High
07:00:00 14/01/2019	no_group		DESKTOP-HHN2B1Q		Initial A	locess	High
Additional detection							
Aritfacts							
TIME	AGENT ID		OBJECT			FROM	REFERENCE
07:25:05 14/01/2019	9D76E75C81645C6B88E18B46961C5D75C8154752		c:\Users\Test\Desktop\demo.exe			WIN_EVENT_LOG	plq3SWgBTy9idpUvVJ-d
07:25:05 14/01/2019	9D76E75C81645C6B88E18B46961C5D75C8154752		HKLM\SOFTWARE\Microsoft\Wind	ows\CurrentVersion\Run\demo		WIN_EVENT_LOG	plq3SWgBTy9idpUvVJ-d

Các đối tượng thuộc phần "Original Detection": là các Alert (Alert) và máy tính (Agent) ban đầu khi IRFlow được tạo;

Còn các đối tượng thuộc phần "Additional Detection": là các Alert, máy tính, artifacts được thêm vào ở bước điều tra (Investigation);

Ý nghĩa một số trường trên màn hình detection:

- + Time: thời gian thêm agent/artifact vào màn hình detection;
- + Object: đường dẫn file/registry của artifact;
- + From: nguồn phát sinh artifact (Event log hoặc Process Analysis);
- + Reference: ID của event log hoặc ID của phiên kết nối Process Analysis;

3.4.6 IRFlow – Containment

Mục đích: Tab Containment cho phép thực hiện cô lập 1 hay nhiều máy tính có trong tab Detection hoặc Suspend tiến trình thuộc Alert nằm trong IRFlow; Các trạng thái của Containment:

+ NOT APPLIED: chưa gửi lệnh xuống Agent;





- + APPLYING: đang gửi lệnh xuống agent;
- + APPLIED: đã gửi lệnh cô lập thành công;
- + STOPPING: đang gửi lệnh dừng cô lập;
- + STOPPED: đã gửi lệnh dừng cô lập thành công;

Bước 1: lựa chọn hình thức điều tra: cô lập mạng hoặc suspend tiến trình sau đó chọn "Next Step";

=	viette aJia	nt IR flow detail						* 0
<u>e</u>	View de	tail - chuyen R flow list						
▲ ∓≟	TIMELINE	e de Create						Close IR flow
۵		<u>i</u>	Detection	Containment	Ŕ	Investigation	Response	
•	1	Rule setting Choose one rule setting to continue next step						2 Next step
Ē		Network containment						
ē		Process containment						
	- 2	Deploy to agent						
		Agent list Choose agent(s) in list below and click move right button to add to apply agent list		»	Agent apply list			
		edr-ubuntu-18 Agent_Ud-ASTETISTNBSB1710081CS77871818544477682	test_group3	NOT APPLIED .	<c Save</c 			

Lưu ý: sau khi nhập Path/PID thì phải ấn Enter để lưu lại cấu hình. Có thể suspend cùng lúc nhiều tiến trình.

Bước 2: chọn danh sách Agent cần cô lập và chọn "Start" để bắt đầu cô lập:

- 2	Deploy to agent		4	
	Agent list (1 agent(s) selected) Choose agent(s) in list below and click move right button to add to appl	ely agent list	»	Agent apply list
	ubuntu Agent_id: 0E1CBE9249C350CDF763F217005A55F1F1F51A59 admin	NOT APPLIED .	«	
	Vin11-EDR Agent_id: 7AA3E83246091499665913553ABCF74003FEA16A default	NOT APPLIED	Save	
1			- e	

Bước 3: Để dừng việc cô lập click "Stop" hoặc chọn agent ở "Agent apply list" và chuyển về danh sách "Agent list";



Trong trường hợp người quản trị không chủ động dừng việc cô lập trên Portal thì sau thời gian mặc định (24h) thì Agent cũng tự động gỡ cô lập dưới Agent.

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



3.4.7 IRFLow – Investigation

3.4.7.1 Process Analysis

a. Xem thông tin process

Mục đích: là quá trình phân tích các tiến trình trên máy người dung có trong tab Detection theo thời gian thực nhằm tìm kiếm các dấu hiệu bất thường;

Bước 1: Chọn agent để kết nối, sau đó click "Start". Danh sách Agent là các Agent trong IRFLow;







Lưu ý:

+ Thời gian timeout tạo kết nối là 60s. Hết 60s không kết nối được Agent thì cần kết nối lại;

+ Tại 1 thời điểm trong 1 IRFLow chỉ có thể tạo 1 kết nối tới Agent. Trong trường hợp có tài khoản khác đang kết nối với Agent trong cùng IRFLow thì sẽ thông báo lỗi:



+ Tại thời điểm kết nối, nếu Agent offline. Hệ thống sẽ hiển thị popup thông báo Agent đang ở trạng thái Offline:





Bước 2: Click "Refresh" để lấy danh sách process mới nhất dưới Agent:



Bước 3: Lựa chọn process trong list process để xem thông tin chi tiết:

	aJiant IR flow detail			25	0					
r.	View detail - IR_HuyenPK	w detail - IR_HuyenPK								
▲ ₹	TIMELINE			Enter your license to access the full features of VCS-aJiant.	low					
±	Create Containment Agent (1)									
⊛ ⊡		Detection	Investigation	Response						
◙	Process analysis	Q Event Search	Tools	Investigation result						
Ē,	SELECT Choose agent to connect PROCES	S smss.exe • Normal	Alert Refresh Agent ii Agent ii	nformation ST O STARTED O DURATION STATE N.0.15(52)009011 16:52 30/05/2022 00:01/25 Duration						
0		DISLESS	A PRO STATE STATE	CESS INFORMATION LOADED MODULES FILE HANDLE KEY HANDLE SYSTEM Incrosoft Corporation NLAME Microsoft Corporation NLAME Microsoft System 32 (smss. exe CUMIndows/System32 (smss. exe CULINE VsystemRoot/System32 (smss. exe 4 16742790895960690237a5143cedec8b 887/b3db5d931389a737891e16d70691355959da03e9ec0fffe6095/ 264	E 61837fa					

- 1 Chọn agent và chọn process;
- 2 Hiển thị thông tin cây process, mặc định hiển thị 1 cấp cha và 1 cấp con. Cho phép mở thêm/thu nhỏ các cấp khi click vào process trong cây. Process được focus trong cây sẽ hiển thị icon khác so với process không được focus;
- 3 Hiển thị thông tin process được focus trong cây bao gồm thông tin trên các tab: Process info, Modules (loaded dll), File handles, Key handles, Thread List, Section handles, Network Connection;

Bước 4: Để lấy thông tin mới nhất của process, click icon Refresh trên mỗi tab



Agent information				
BIN-0JSI63088	C STAF SNI 16:5	ETED (52 20/06/2022 (DURATION 00:01:35	STATE Running
PROCESS INFORMA	TION Ġ	LOADED MODULES	FILE HANDLE	KEY HANDLE
USER	SYSTEM			
COMPANYNAME	Microsoft	Corporation		
PRODUCTNAME	Microsoft	® Windows® Operating	g System	
FILEVERSION	6.1.7600.1	6385		
PROCESSPATH	C:\Window	vs\System32\smss.ex	e	
COMMANDLINE	\SystemRo	oot\System32\smss.e	xe	
PPID	4			
MD5	16742790	895960690237a5143c	edec8b	
SHA256	88f7b3db5	5d931389a737891e16	d7069135959da03	Be9ec0fffe609561837fa
PID	264			

Lưu ý:

+ Khi chuyển tab con trong Investigation như Event Search, Tools, Investigation Result thì phiên kết nối với Agent được giữ và không cần kết nối lại;

+ Khi chuyển tab khác như Detection, Containment, Response hay Alert, Setting.... Hoặc F5, Logout... thì cần phải tạo lại kết nối với Agent;

+ Phiên kết nối Process Analysis trong IRFLow chỉ đóng khi quản trị đóng IRFLow. Tức là nếu chưa đóng IRFLow thì mỗi lần vào IRFLow và kết nối với Agent thì ID của phiên kết nối ko thay đổi;

b. Marking/Get artifact

Chức năng Marking artifact cho phép đánh dấu các artifact cần theo dõi. Có thể marking các dữ liệu sau:

- + Process Info: ProcessPath;
- + Loaded module: Path;
- + File Handle: Path;
- + Key Handle: Key path, Value;

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Đánh dấu thông tin trong Process:

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút "Marking artifact";

Agent infor	rmation JSI63088NI	© STARTED 16:52 20/06/2022	OU:06:57	STATE Runn	ing
PROCESS	S INFORMATION	LOADED MODULES 😋	FILE HANDLE	KEY HANDLE	THREAD LIS
NAME	PATH	MD	5	SHA256	COMPANY NAME
smss.exe	📙 \System	Root\m32\smss.ex 🏥	I	نال	1
ntdll.dll	📙 C:\Windo	ws\S32\ntdll.dll 📗	ed60c95c805dbae	🕒 c <mark>3</mark> Marking artifa	act I Get artifa

Bước 2: Click vào nút "Accept", có thể chỉnh sửa đường dẫn file khi click vào icon "edit":

A	Agent informa	tion					
	WIN-0JSI	53088NI	STARTED 16:52 20/06/20	22 [©]	00:09:32		state Running
-	PROCESS INF	ORMATION	LOADED MODULE	s 🖸	FILE HANDLE	KEY HAND	LE THREAD LIS
NA	ME	PATH		MD5		SHA256	COMPANY NAME
sm	iss.exe	🍈 \System	nRoot\m32\smss.e	ex 🂼		()	
ntd	lll.dll	C:\Wind	dows\S32\ntdll.dll	📑 ed60	c95c805dbae	🕒 d35574d2cd	42b4eMicrosoft C
M	1arking arti	fact				Cancel	Accept
P	ATH						
n	tdll.dll						
С	:\Windows\S\	/STEM32\nt	dll.dll				

+ Trường hợp chọn bản ghi có Agent chưa tồn tại trong Detection sẽ có thêm check box Add Agent to IRFlow. Khi thực hiện Accept thì Agent tương ứng sẽ được add vào Detection.

Sau khi marking thành công, hiển thị thông báo. Click vào nút "View all artifacts in Investigation Result" để chuyển đến màn hình Investigation Result. Artifact được marking sẽ hiển thị trên màn hình này:



	٩ge	nt information					
	Ð	HOST MACOS_BICHPT3	G	STARTED 09:51 21/06/2022	OURATION 00:02:43	STATE Running	
4	F	PROCESS INFORMATIO	ON C	LOADED MODULES	FILE HANDLE	KEY HANDLE	THREAD LIS
US	ER		🍺 root				
Ma	rke	ed artifact	- / 301	namona		View in inves	tigation resu
М	05		🌔 00ad	l6b735d11f2220b014b	fcc0253daf		
SH	A2	56	1 2714	40ca9818992d11d7fe	58e26f0515fcfafb7d	d43c35f1eef3fbc53c6	6a9a5
ST	ATE		🎒 Ss				
PI	D		1 🌐				

		<u>- Detection</u> Conta	inment 🥳 Investigation	Response	
¢	Process analysis	Q Event Search		🗗 Tools	D investigation result
~	Marked artifact				
	TIME	OBJECT			
	20/06/2022 16:28:14	C:\Program Files\Ajiant\propre\VESProPre.ex	ce		Added to IRFlow 🗸
	20/06/2022 17:27:53	C:\Windows\System32\cmd.exe			<u>10</u> >
Got artifact	20/06/2022 17:28:28	C:\Program Files\Ajiant\AgentInfo.exe	<u>10</u> >		
	20/06/2022 17:28:44	C:\Program Files\Microsoft VS Code\Code.ex	<u>10</u> >		
	20/06/2022 17:30:39	HKU\S-1-5-21-657600163-1704432705-42179	by [11 <u>10</u> >		
Tools result	20/06/2022 17:57:24	HKLM\System\CurrentControlSet\Services\E	ventLog\VEDR		<u>10</u> ;
	L				

Chức năng Get Artifact cho phép lấy thông tin file/registry dưới Agent phục vụ cho việc điều tra;

Chọn 1 bản ghi và hover vào bản ghi đó. Click nút "Get artifact" > Lựa chọn loại artifact (File/Registry) > Click "Accept". Sau đó kiểm tra kết quả thực hiện Get artifact trên màn hình Investigation Result;

	Agent information								
	MACOS_BICHPT3		09:59 21/06/2022		00:00:44			state Running	
•	PROCESS INFORMATION	9	LOADED MODULES	FILE HA	NDLE	KEY HANDLE		THREAD LIST	SECT
U	SER [root						1	
P	ROCESSPATH	/sbin/la	unchd				Marki	ng artifact	Get artifac
С	OMMANDLINE	/sbin/la	unchd						վեղ
N	105 🚺	00ad6b	735d11f2220b014bf	cc0253daf					0
S	HA256	271440	ca9818992d11d7fe5	8e26f0515f	cfafb7dd43	3c35f1eef3fbo	:53c66	a9a5	
S	TATE [Ss							
P	ID 🚺	1							
_									





3.4.7.2 Event Search

Đây là quá trình tìm kiếm các đối tượng dựa vào event logs. Khác với các tab khác trong IRFLow chỉ hiển thị thông tin các Agent được add vào IRFLow thì ở tab này hiển thị toàn bộ event của tất cả Agent trong hệ thống.

a.	Tìm	kiếm	Event

~			Detection	E Contai	nment W Investigation	ATTA K ^C A Response		
				100/1	-0 -			
1	Proce	ess analysis				Tools		Investigation result
Ē.	Search EventD - '1'							2 3 2 3 2 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
ø	POPULAR							View column
	OTHERS	AGENTID		EVENTID	COMPUTER	LOGTYPE	SYSTEMTIMESTAMP	TIMESTAMP
	AgentID	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:21:47	20/06/2022 17:19:34
	Channel	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:21:01	20/06/2022 17:19:34
	Computer	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:21:01	20/05/2022 17:19:34
	EventID	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:20:36	20/05/2022 17:19:34
	LogType	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:20:36	20/06/2022 17:19:34
	Platform	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:20:35	20/06/2022 17:19:34
	ProcessID	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:20:35	20/06/2022 17:19:34
	ThreadD	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:20:35	20/06/2022 17:19:34
	client_id	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:19:47	20/06/2022 17:17:34
	event_id_meaning	1B0A66FD56ED04C2C6D557DDFDB79A6F5040FCOC		1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:18:51	20/06/2022 17:17:46
	event_log_id	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC		1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:18:48	20/06/2022 17:17:46
	file_company	180A66FD56EDD4C2C6D557DDFD879A6F5040FCCC		1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:18:48	20/06/2022 17:17:46
	file_description	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039		1	WIN-0JSI63088NI	EventLog	20/06/2022 17:18:19	20/06/2022 17:15:34
	file_hash_md5	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCOC		1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:18:12	20/06/2022 17:17:46
	file hash sha1	180A66FD56EDD4C2C6D557DDFD879A6F5040FCCC		1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:18:12	20/06/2022 17:17:46

Bước 3: Nhập vào textbox Search câu query với format như sau: <tên_trường> <toán tử> "<value>" AND/OR <tên_trường> <toán tử> "<value>"..... Trong đó:

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: wvw.viettelcybersecurity.com



- + <tên_ trường> là các giá trị sau:
 - AgentID: ID của agent;
 - EventID: ID của event;
 - Computer: Tên của computer;
 - LogType: Loại log;
 - Channel: Channel của event;
- + <toán_tử> là các giá trị sau:
 - = : tìm chính xác giá trị là value;
 - != : tìm giá trị khác với value;
 - ~: tìm giá trị like với value;
 - AND/OR: toán tử kết hợp để kết hợp 2 câu query;
- **Bước 4:** Chọn khoảng thời gian tìm kiếm bằng cách click vào nút "Date & Time" và chọn thời gian tùy ý. Nếu không chọn thời gian thì hệ thống chọn mặc định là Last 7 days;

Bước 5: Click on Search:

+ Trường hợp không có kết quả phù hợp, hệ thống sẽ hiển thị thông báo: No data;

+ Trường hợp có kết quả phù hợp, hệ thống hiển thị mặc định 50 bản ghi theo thứ tự giảm dần theo thời gian với 5 cột hiển thị mặc định bao gồm: AgentID, EventID, Computer, LogType, Channel;

b. Xử lý Event

Mục đích: Hỗ trợ người dùng thao tác và xử lý các Event; Marking artifact: Đánh dấu artifact



ž I			Detection	Containment	investigation	Response				
0	Process :	analysis	Q Event Search			📑 Tools		🗋 Investigatio	on result	
£λ	Search Search								Last 7 days	٩
ē	POPULAR	E 109.901 results 13/06/2022 17:06:52 - 20/06/2022 17:06:52						V	ew column	
	OTHERS	AGENTID	E	VENTID (COMPUTER	LOGTYPE	SYSTEMTIMESTAMP	TIMESTAMP		
	AgentiD	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	1	1	WIN-0JSI63088NI	EventLog	20/06/2022 17:06:00	20/06/2022 17:03	1:34	
	Channel	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	1	L I	WIN-OUSI63088NI	EventLog	20/06/2022 17:06:00	20/06/2022 17:03	134	
	Computer	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	1	1 1	WIN-OJSI63088NI	EventLog	20/06/2022 17:05:47	20/06/2022 17:03	1:34	Marking antifect(a)
	EventID	B6BE59BC53C7E4BFCE2CFC1821AFA623F737C039	1	L I	WIN-0JSI63C88NI	EventLog	20/06/2022 17:05:33	20/06/2022 17:03	134	Get artifact
	LogType	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	1	L 1	WIN-OJSI63088NI	EventLog	20/06/2022 17:05:33	20/06/2022 17:03	134	
	Platform	B6BE59BC53C7E4BFCE2CFC1821AFA623F737C039	1	L 1	WIN-0JSI63088NI	EventLog	20/06/2022 17:05:32	20/06/2022 17:03	134	
	ProcessID	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	1	L 1	WIN-OJSI63088NI	EventLog	20/06/2022 17:05:32	20/06/2022 17:03	1:34	
	ThreadD	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	1	L 1	WIN-0JSI63088NI	EventLog	20/06/2022 17:05:32	20/06/2022 17:03	1:34	
	client_id	B6BE59BC53C7E4BFCE2CFC1821AFA623F737C039	1	10 1	WIN-0JSI63088NI	EventLog	20/06/2022 17:05:32	20/06/2022 17:03	1:34	
	event_id_meaning	1B0A66FD56EDD4C2C6D557DDFD879A6F5040FCCC	1	12 1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:04:41	20/06/2022 17:04	804	
	event_log_id	1B0A66FD56EDD4C2C6D557DDFDB79A6FS040FCCC	1	12 1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:04:41	20/06/2022 17:04	104	
	file_company	1B0A66FD56EDD4C2C6D557DDFD879A6F5040FCCC	1	L I	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:04:27	20/06/2022 17:04	004	
	file description	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	1	12 1	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:04:27	20/06/2022 17:04	004	

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút "Marking artifact". Trên màn hình sẽ hiển thị popup như sau:

€ ⊡			Detection	Containment	investigation	Response			
0	ŝ	3 Process analysis	Q, EventSearch			Tools		Investigation result	
Ē.	Search Search							Last 7 days	٩
۹	POPULAR	109.901 results 13/06/2022 17:	96:52 - 20/06/2022 17:06:52					View column	
	OTHERS	AGENTID		EVENTID	COMPUTER	LOGTYPE	SYSTEMTIMESTAMP	TIMESTAMP	
	AgentID	B6BE598C53C7E4BFCE2CFC1821AFA623F7	17C039	1	WIN-OJSI63088NI	EventLog	20/06/2022 17:06:00	20/06/2022 17:03:34	
	Channel	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	1	WIN-0JSI63088NI	EventLog	20/06/2022 17:06:00	20/06/2022 17:03:34	
	Computer	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	1	WIN-0JSI63088NI	EventLog	20/06/2022 17:05:47	20/06/2022 17:03:34	
	EventID	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	1	WIN-OJSI63088NI	EventLog	Marking Artifact(S)		
	LogType	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	1	WIN-0JSI63088NI	EventLog			
	Platform	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	1	WIN-OJSI63088NI	EventLog	04704		
	ProcessID	B6BE598C53C7E4BFCE2CFC1821AFA623F7	17C039	1	WIN-0JSI63088NI	EventLog	PAIN		
	ThreadID	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	1	WIN-0JSI63088NI	EventLog			
	client_id	B6BE598C53C7E4BFCE2CFC1821AFA623F7	37C039	10	WIN-OJSI63088NI	EventLog	C:/Windows\System32\cmd.exe 🖉		
	event_id_meaning	1B0A66FD56EDD4C2C6D557D0FDB79A6F5	HOFCOC	12	DESKTOP-R2GBJEF	EventLog			
	event_log_id	1B0A66FD56EDD4C2C6D557D0FDB79A6F5	HOFCCC	<u>12</u>	DESKTOP-R2GBJEF	EventLog	C:/Windows\System32\schtasks.exe 🤌		
	file_company	1B0A66FD56EDD4C2C6D557D0FD879A6F5	HOFCCC	1	DESKTOP-R2GBJEF	EventLog	🗌 schtasks.exe 🤌		
	file_description	1B0A66FD56EDD4C2C6D557D0FDB79A6F5	HOFCCC	12	DESKTOP-R2GBJEF	EventLog			
	file hash md5	1B0A66FD56EDD4C2C6D557DDFDB79A6F5	HOFCCC	11	DESKTOP-R2GBJEF	EventLog	Cancel Accept	Add Agent To IR Flow	
	file hash sha1	1B0A66FD56EDD4C2C6D557DDFDB79A6F5	HOFCCC	11	DESKTOP-R2GBJEF	EventLog			
	file hash sha256	1B0A66FD56EDD4C2C6D557D0FDB79A6F5	HOFCCC	11	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:04:25	20/06/2022 17:04:04	
	file and at	1B0A66FD56EDD4C2C6D557D0FDB79A6F5	HOFCCC	11	DESKTOP-R2GBJEF	EventLog	20/06/2022 17:04:25	20/06/2022 17:04:04	

Bước 2: Chọn 1 hoặc nhiều path thực hiện đánh dấu Artifact:



- + Chọn nút "Accept" để xác nhận yêu cầu đánh dấu Artifact;
- + Chọn nút "Cancel" để xác nhận hủy bỏ yêu cầu đánh dấu Artifact;

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Get artifact: thực hiện get file/registry dưới Agent lên server để phục vụ cho quá trình điều tra;

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút "Get artifact" Trên màn hình sẽ hiển thị popup như sau:

@ [Agent S	<u> </u>	etection	investigation				
0		(ĝ) Process analysis	Q, Event I	arth .	📑 Tools			investigation result	
£λ	Search teach							D Last 7 days	1 a
æ	POPULAR	≡ 110.377 results 13/06/3	022 17-80-83 - 20/06/2022 17:40-83					View column	
	07HERS	SVSTSMTMRSTAMP	TRACTIONP	AGENTIE		EVENTED	COMPOSED	1007194	
	AgentID	20/06/2022 17:39:47	20/06/2022 17:37:34	B6BE598C53C7E4BFCE2CFC1821AFA623F7	370039	1	WIN-0JSI63088NI	EventLog	
	Channel	20/06/2022 17:38:49	20/06/2022 17:37:46	180A66FD56EDD4C2C6D557DDFD879A6F5	DADFOCC	1	DESKTOP-R2GBJEF	EventLog	
	Computer	20/06/2022 17:38:50	20/06/2022 17:37:46	180A66FD56EDD4C2C6D557DDFD879A6F5	DAGFODD	12	DESKTOP-R2GBJEF	EventLog	
	EventID	20/06/2022 17:38:49	20/06/2022 17:37:46	1B0A66FD56EDD4C2C6D557DDFDB79A6F5	D40FCCC	1	DESKTOP-R2GBJEF	EventLog	
	LogType	20/06/2022 17:38:50	20/06/2022 17:37:46	1BDA66FDS6EDD4C2C6D557DDFDB79A6FS	DADECCC	12	DESKTOP-R2GBJEF	EventLog	Marking
	Platform	20/06/2022 17:38:52	20/06/2022 17:37:46	180A66FD56EDD4C2C6D557DDFD879A6F5	DADFOCC	1	DESKTOP-R2GBJEF	EventLog	Get artifact
	ProcessID	20/06/2022 17:38:43	20/06/2022 17:37:46	180A66FD56EDD4C2C6D557DDFDB79A6F5	DesFOCC	1	DESKTOP-R2GBJEF	EventLog	

Bước 2: Chọn artifact sau đó chọn loại artifact (File/Registry) và click "Accept"

Khi marking artifact thành công màn hình sẽ hiển thị thông báo. Click vào "View in investigation result" để chuyển đến màn hình Investigation Result. Kết quả của việc Get artifact sẽ hiển thị trên tab này:

e i			Detection Containment	investigation	
Ø		(§) Process analysis	Q Event Search	🖓 Tools	
e2	~	Marked artifact			
(a)	Marked artifact	TIME	OBJECT		
-		20/06/2022 16:28:14	C:\Program Files\Ajiant\propre\VESProPre.exe		Added to IRFlow 🗸
	ك	20/06/2022 17:27:53	C:\Windows\System32\cmd.exe		<u>a</u> >
	Got artifact	20/06/2022 17:28:28	C:\Program Files\Ajiant\AgentInfo.exe		<u>a</u> >
		20/06/2022 17:28:44	C:\Program Files\Microsoft VS Code\Code.exe		2 >
	8	20/06/2022 17:30:39	HKU\S-1-5-21-657600163-1704432705-4217905726-1001\Software\Microsoft\SystemC	ertificates\Root\Certificates has been added or deleted by [11092]	<u>a</u> >
	Tools result				

c. Deploy Tools

Mục đích: là quá trình đẩy tool xuống dưới Agent lấy thông tin để điều tra. Thông tin một số tool có sẵn trên hệ thống:

- + Với agent Windows:
 - Listdlls: lấy thông tin các processs và dll đang được load lên;
 - Autorunsc: lấy thông tin các tiến trình, dịch vụ khởi động cùng hệ thống;
- + Với agent Linux:
 - ListService: lấy danh sách service dưới máy agent;

+ Luồng thực hiện chức năng này như sau: Thực hiện lựa chọn tool > Chọn agent > click "Deploy tools";



Để lựa chọn tool thích hợp có 2 cách sau:

+ Cách 1: Click vào textbox search tool > click tool cần deploy > click "Choose tool":



+ Cách 2: Click vào textbox search tool > click "See all tools" => hiện ra màn hình danh sách tool đầy đủ >Tìm kiếm và lựa chọn tool cần deploy > click "Add tool";



53 Process and	atysis
Add tool 2 Multi select agents online	
Tools	Ag
Q Type to search tool Add Tool	
(WINDOWS	-
Bichpt3_Hello.exe	
C Vv1outputhelio Hash: e01659c0e481ab4a66bbb29eb0e	
W get services x64 bet	
Vbat I Hash: ees04se73ffa5e5er9e6/4787ff68e06d3815	
🐴 LINUX	
linux_sleep_5s.sh	
Vlinuxscript Hash: 39348d52223cafdb1c5dc44272069e	
phula_tool_test.sh	
C V1234 Hash: 392436691f2d139c1a28625feb0308a11a	
ngocanh testtool.sh	
☐ V1.1 Hash: 6aff1115fcbe132cb90218faace5092fb22ad	
linux olf with param	
Welf Hards h05hd704646561b102755961ade61dec2991	
⊔ hbc_tool_ls.sh	
U V1 Hash: ebfdec641529d4b59a54e18f8b0e9730f85939	
Dbgview.exe	
V1 Hash: 77a8060d1629183e457fdbc2f34143a5070bd	
Bichpt3_Hello (1).exe	
C Vtool windows Hash: e01659c0e481ab4a66bbb29eb0e	
B MACOS	
pnula_tool_test_macos.sh	
 v1ada Hash: atstaboppeac1b6879d1ae5549b622d002 	

+ Sau bước tìm kiếm tool thực hiện chọn agent và click "Deploy tools"

Page | 70



	$\frac{1}{2} \left(\frac{1}{2} \right)^{\frac{1}{2}}$ Detection	Containment	Investigation	Response	
Process analysis	Q Even	t Search		🖸 Tools	Investigation result
Add tool Add tool Multi select agents online	S Click Deploy Tool button to				
Tools	Agents Type to search by query	Q			
Q Type to search tool Add Tool	HOSTNAME YUN-0JSI63088NI	M 🗑 TOOLS 🦉			STATUS Online
Bichpt3_Hello.exe Wioutputhelio (Hash: e01659c0et81ab4a66bb329eb0ea886317#5e4ab					
∧ Linux					
ngocanh_testtool.sh V1.1 Hash: 6alf1115fcbe132cb90218fasce5092fb22ad70c					
Bichpt3_Hello (1).exe Vtool windows Hash: e01659c0e481ab4a66bbb29eb0ead86317e5e4ab					
∧ MacOS					
Deploy Tools					

+ Sau khi deploy tool thì xem kết quả ở tab Investigation Result, tab Tools

Result

5	View detail - IR_Huy ← Back to IR flow list	enPK							
∎ _µ ,,,	TIMELINE	te Containment Agent: (s)	Tool Deployed Successfull Agent: (1)	y Tool Deployed Successfully To Agent: (s)	ol Deployed Successfully Agent: (s)				Description → Description
•				Detection	Containment	Investigation	Response		
Ø		Process analysis		Q Event Sear	ch		Tools	• • •	Investigation result
Ē	\checkmark	Tools result							
ē	Marked artifact	 Ngocanh_testtool.Sh 	Agents (1)	Success (0/1)					
		 Bichpt3_Hello (1).Exe 	e Agents (1)	Success (0/1)					
	Got artifact	 Bichpt3_Hello.Exe 	Agents (1)	Success (1/1)					
	B								
	Tools result								
									0

d. Investigation result

Đây là màn hình hiển thị thông tin kết quả Deploy tool, Marking/Get Artifact ở 3 tab: Process Analysis, Event search, Tools:

+ Tab "Got Artifact": kết quả thực hiện lệnh Get Artifact;



Page | 71



- + Tab "Tool Results": kết quả thực hiện lệnh Deploy tools;
- + Tab "Marked Artifact": các artifact đã marking;

Trong tab "Got Artifact" và "Tool Results", có thể thực hiện các hành động sau:

+ Xem nội dung chi tiết của artifact đã lấy hoặc kết quả chạy tool dưới agent. Nếu dữ liệu là text thì có thể xem trực tiếp trên giao diện, nếu dữ liệu là file thực thi (.exe) thì cần download về máy local để kiểm tra;

+ Download artifact hoặc kết quả chạy tool. Có 2 cách Download: click icon "Download" trên giao diện hoặc click icon "Detail" > click icon "Download" trên màn hình này;

		<u></u> Detection	Containment	Investigation	Response		
	183 Process analysis	Q Event Search			Tools	🗋 Investiga	ation result
×	Got artifact						
Marked artifact	 MACOS_BICHPT3 Agents (1) 	Success (1/1)					
	TIME TYPE OF	JJECT				STATUS	ACTION
Got artifact	10:06 21/06/2022 FILE /sb	sin/launchd				Success Do	wnioad
							0
<i>E</i>							
Tools result							

Trong Tab Marked artifact, lựa chọn artifact để thêm vào màn hình Detection, Chọn 1 artifact và click "Add to detection":

		<u>- Detection</u> Containment	Investigation	Response	
	Process analysis	Q Event Search		Tools	Investigation result
\sim	Marked artifact				
Marked artifact	TIME	OBJECT			
	20/06/2022 16:28:14	C:\Program Files\Ajiant\propre\VESProPre.exe			Added to IRFlow 🗸
\checkmark	20/06/2022 17:27:53	C:\Windows\System32\cmd.exe			Add to detection
Got artifact	20/06/2022 17:28:28	C:\Program Files\Ajiant\AgentInfo.exe			x (7 <u>8</u>
	20/06/2022 17:28:44	C:\Program Files\Microsoft VS Code\Code.exe			<u>0</u> ×
æ	20/06/2022 17:30:39	HKU\S-1-5-21-657600163-1704432705-4217905726-1001\Software	Microsoft\SystemCertificates\	Root\Certificates has been added or deleted by [11	092] <u>친</u> ×
Tools result	20/06/2022 17:57:24	HKLM\System\CurrentControlSet\Services\EventLog\VEDR			<u>1</u> ×

Chọn nhiều artifact và click "Add to detection":


		<u>Detection</u>	Containment Investigation	Response	
	Process analysis	Q Event Search		Tools	Investigation result
~	Marked artifact	2			
Marked artifact	Selected (2)	Add to detection			Reset C
		OBJECT			
*	20/06/2022 16:28:14	C:\Program Files\Ajiant\propre\VESProPre.exe			Added to IRFlow 🗸
Got artifact	20/06/2022 17:27:53	C:\Windows\System32\cmd.exe			
	20/06/2022 17:28:28	C:\Program Files\Ajiant\AgentInfo.exe			
e	20/06/2022 17:28:44	C:\Program Files\Microsoft VS Code\Code.exe			
Tools result	20/06/2022 17:30:39	HKU\S-1-5-21-657600163-1704432705-42179057	726-1001\Software\Microsoft\SystemCertificates\	Root\Certificates has been added or deleted by	/ [11092]
	20/06/2022 17:57:24	HKLM\System\CurrentControlSet\Services\Event	tLog\VEDR		

	Process analysis	Q Event Search	🖓 Tools	Investigation result
~	Marked artifact			
Marked artifact	Added artifacts to detection			View all artifacts in Detection phase
	20/06/2022 16:28:14	C:\Program Files\Ajiant\propre\VESProPre.exe		Added to IRFlow 🗸
	20/06/2022 17:27:53	C:\Windows\System32\cmd.exe		Added to IRFlow 🗸
Got artifact	20/06/2022 17:28:28	C:\Program Files\Ajiant\AgentInfo.exe		Added to IRFlow 🗸
	20/06/2022 17:28:44	C:\Program Files\Microsoft VS Code\Code.exe		Added to IRFlow 🗸
8	20/06/2022 17:30:39	HKU\S-1-5-21-657600163-1704432705-4217905726-1001\Software	Microsoft\SystemCertificates\Root\Certificates has been added or deleted by [1109	2] <u>친</u> ×
Tools result	20/06/2022 17:57:24	${\sf HKLM} \ System \ Current Control Set \ Services \ Event \ Log \ VEDR$		<u>n</u> ×

Sau khi add thành công sẽ hiện thông báo thành công, click vào "View all artifacts in Detection phase" chuyển đến màn hình Detection. Các artifact được thêm vào mục Additional detection trên màn hình Detection:

	le ^r	Detection	Containment 🦉	Investigation	Response				
Original detection									
Agent WIN-0JSI63088NI MACO	IS_BICHPT3								
Aritfacts									
TIME	AGENT ID		OBJECT			FROM		REFERENCE	
20/06/2022 16:28:14	B6BE598C53C7E4BFCE2CFC1821AFA623F737	rC039	C:\Program Files	\Ajiant\propre\VESProPre.	exe	PROCESS_ANALYS	SIS	58583AD0	
Additional detection									
Alert									
TIME	GROUP	HOSTNAME	SCENARIO	SEVERI	ITY				
08/06/2022 16:37:55	TENANT_edr.com	MACOS_BICHPT3		<span< td=""><td>class="severity-item high">High</td><td></td><td></td><td></td><td>× 🛈</td></span<>	class="severity-item high">High				× 🛈
Aritfacts									
TIME	AGENT ID	OBJECT				FROM	REFERENCE		
20/06/2022 17:27:53	B6BE598C53C7E4BFCE2CFC1821AFA623F737C039	C:\Windows\System3	2\cmd.exe			EVENT_LOG			×
20/06/2022 17:28:28	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Program Files\Ajia	nt\Agentinfo.exe			EVENT_LOG			×
20/06/2022 17-20-44	10034440544003040557006087034650306000	C1Droorom Eilon Mio	month VC Code) Code ave			EVENT LOO			×
									D

3.4.8 IRFlow – Response

3.4.8.1 *Live Response*

Chức năng Live response cung cấp khả năng xử lý một tập các command từ xa theo phiên làm việc nhằm cho biết các thông tin hoặc xử lý yêu cầu trên host; Các bước thực hiện chức năng Live Response trong IRFlow:

Bước 1: Click tab "IRFlow";





Bước 2: Click đúp vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Live Response);

	aJiant IR Flow								# 0
Ę	IR Flow management								Guidelines
A	Type to search queries						Last 7 d	ays	Q
$\mathbf{H}^{\mathbf{q}}$	3 result(s) 14/06/2022 10:42:25 - 2	1/06/2022 10:42:25							+ Create
۲	TIME	 NAME 	STATUS	CREATED BY	ASSIGNED TO	NOTE			CTION
_	21/06/2022 09:50:14	IR_huyenpk1	New	root_test	root_test			Ð	0
<u>}-</u>	20/06/2022 16:28:14	IR_HuyenPK	New	root_test	root_test			Ð	0
•	16/06/2022 14:25:35	centos6	New	root_test	root_test			Ð	0
-	Showing 3/3 result(s)								
Eγ									
ē									

Bước 3: Click tab con Response:

- <u>`</u> Detection Con	ainment 🥳 Investigation	Response 2				
			Response scenario			
- 						
AGENT ID	REMOTE	SESSION RANGE				
3 MACOS_BICHPT3(0784013009	1BBF3A0FBBD21E5DB771	~				
-						
	Start					
	Objection Example 0 control AGENTID MACCOS_BICHPT3(67640T3009PF)	Detection Image: Containment Image: Ima	Meterion Containment Westigation Meterion (Containment) Image: Containment Image: Containment Image: Containment) Containment)<			

Bước 4: Chọn Agent và khoảng thời gian cần thực hiện (5 phút/ 15 phút/ 1 giờ/ 3 giờ) Live Response và bấm nút "Start Live Response";

Danh sách Agent hiển thị trong combobox là tất cả các Agent hiển thị trong tab Detection;

Sau đó, người dùng cần chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là "connecting";





Bước 5: Khi kết nối thành công, hệ thống hiển thị 1 bản ghi bên Remote session list và màn hình console có thông tin của kết nối và hiển thị trạng thái "running".

	Create	Containment Agent (1)								
				<u>Detection</u>	Containment	1 investigation	on Respon	158		
			Dve response					Response scenario		
Remote session	list			+ Add new remote	Agent ID: 1B0A66FD56ED	D4C2C6D557DDFDB79A6F50	MOFCCC			
STATUS	AGENT ID		START TIME	END TIME	DESKTOP-R2GBJEF	O	ITARITED 10:59:35 21/06/2022	COUNTDOWN 00:13:10	TIME TO LIVE 15m	
• Norsey-					-iist -iist -iist-sername Lips 	List over- opt List of vice-rease chere console chere console d-he methods d-he m	est espile din markin argunt est est est est est est est est est es			• Rumin
					 Attachment log 					
					FILE NAME			TIME CREATED	DIRECTORY	
					LZID			2022-06-21104:01:16Z	U.	ت گ
										0

(Remote Session List: hiển thị danh sách các phiên live response đã được thực hiện của IRFlow)

Lưu ý: Mỗi agent tại một thời điểm chỉ có 1 phiên Live response làm việc.

Người dùng có thể thực hiện các lệnh tại màn hình console như sau:



STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath></dirpath>	Thay đổi thư mục làm việc hiện tại
		cd hoặc cd	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
		dir [drive:][path][filename] [/A[[:]attributes]] [/O[[:]sortorder]] [/T[[:]timefield]] [/L] [/Q] [/R] [/S] [/X]	Liệt kê các file/ các thư mục con trong thư mục hiện thời
3	dir	 /A:[-] attributes Displays files with specified attributes. Attributes: D Directories R Read-only files H Hidden files A Files ready for archiving S System files L Reparse Points 	
		/L Lower-case filename	
		/O:[-]sortorderList by files insorted order.sortorder	



STT	Các lệnh	Tham số	Mô tả
		N By name (alphabetic)	
		S By size (smallest first)	
		E By extension (alphabetic)	
		D By date/time (oldest first)	
		G Group directories first	
		- Prefix to reverse order	
		Ex: dir /O:N;	
		/T:timefield Choose which time field displayed	
		timefield	
		C Creation	
		M MFT Creation	
		A Last Access	
		W Last Written	
		Ví dụ: dir /T:A	
		- Prefix to exclude attribute	
		Ví dụ: dir /A:D-AH	
		/Q Display the owner of the file.	
		VI dụ: dir /Q	
		/R Display alternate data streams of the file.	
		Ví dụ: dir /R	



STT	Các lệnh	Tham số	Mô tả
		/S Displays files in specified directory and all subdirectories. Ví dụ: dir /S	
		 /X This displays the short names generated for non-8dot3 file names. Ví dụ: dir /X 	
		delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"</path>	Xóa 1 file
4	delete	delete -folder <folderpath> ví dụ: delete -folder temp\axvers</folderpath>	Xóa 1 thư mục
		delete –all <folderpath> ví dụ: delete –all c:\temp</folderpath>	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<sourcepath> <destpath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"</destpath></sourcepath>	Cho phép di chuyển file/ folder



STT	Các lệnh	Tham số	Mô tả
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5="" sha1="" ="" <br="">sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe</filepath></type:>	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	dump		Cho phép dump tiến trình. Nếu bạn bỏ qua đường dẫn tệp kết xuất, nó sẽ mặc định là <processname> _ <datetime> .dmp</datetime></processname>
		-process -pid <processid> [-f <destpath>] dump process by process id Ví dụ: dump -process -pid 452 -f "C:\Users\Evil_dumped.dmp"</destpath></processid>	Dump process bởi Process id
		-process-name <processname>[-f<destpath>]dumpprocess by process nameVí dụ: dump -process -nameEvil.exe-f"C:\Users\Evil_dumped.dmp"</destpath></processname>	Dump process bởi Process name



STT	Các lệnh	Tham số	Mô tả
		-process -path <processpath> [-f <destpath>] dump process by process path Ví dụ: dump -process -path "C:\Users\Evil_exe" -f "C:\Users\Evil_dumped.dmp"</destpath></processpath>	Dump process bởi Process Path
9	get	<filepath></filepath>	Upload 1 file từ host lên server
10	put	<url><folderpath></folderpath></url>	Download 1 file tới máy host
11	mkdir	<dir name=""></dir>	Tạo 1 thư mục
			Các lệnh liên quan đến Registry
12	reg	query <keyname>-v<valuename>ví dụ:reg-query"HKLM\Software\abc xyz"-v"run path""</valuename></keyname>	Truy vấn dữ liệu value của 1 key
		query <keyname> -s ví dụ: reg-query "HKLM\Software\abc xyz" -s</keyname>	Truy vấn tất cả các subkey và value và data
		add <keyname></keyname>	Thêm 1 key



STT	Các lệnh	Tham số	Mô tả
		ví dụ: reg-add "HKLM\software\abc xyz"	
		add <keyname> -v <valuename> -t <type> -d <data> ví dụ:</data></type></valuename></keyname>	Thêm 1 value
		reg-add "HKLM\software\abc xyz" -v "run path" -t REG_SZ - d "c:\temp\bin.exe"	
		delete <keyname> ví dụ: reg -delete HKU\S-1-5-21- 3791698801-2327923109- 636705026- 2080\Software\Test</keyname>	Xóa 1 key và tất cả các subkey và value
		delete <keyname> -v <valuename></valuename></keyname>	Xóa 1 giá trị của key
		import <filename></filename>	Import 1 file .reg
		export <keyname> <filename></filename></keyname>	Export 1 file .reg
			Các lệnh liên quan đến process
13	process	-t <processid></processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình



STT	Các lệnh	Tham số	Mô tả	
		-s <processid></processid>	Tạm dừng 1 tiến trình	
		-r <processid></processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó	
		-l -a	Liệt kê toàn bộ các process của tất cả các user	
	-I -u <username></username>		Liệt kê các process của 1 user	
			Các lệnh liên quan đến service	
14	service	-query	Liệt kê các service đang chạy trên máy host	
		-start <servicename></servicename>	Start 1 service	
		-stop <servicename></servicename>	Stop 1 service	
		-uninstall <service_name> uninstall service</service_name>	Gỡ cài đặt service	
		-listdrivers list drivers on host, example: service - listdrivers	List danh sách drivers trên host	
15	usor	-list	Liệt kê các user trên máy	
15	usei	-sid <username></username>	Lấy sid của username	
16	grep	grep -t <text> <param/> <command/></text>	Hỗ trợ tìm kiếm theo từ hoặc chuỗi từ kết quả đầu ra được theo lệnh command truyền vào	



STT	Các lệnh	Tham số	Mô tả
17	cls		Xóa màn hình console
18	help		Lệnh help
19	Clear		Làm sạch console
20	Close		Đóng session

+ Ubuntu: Thực hiện các câu lệnh sau:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath></dirpath>	Thay đổi thư mục làm việc hiện tại
		cd hoặc cd	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
3	dir	dir list file / subfolder in current folder	Liệt kê các file/ các thư mục con trong thư mục hiện thời
4	delete	delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"</path>	Xóa 1 file
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers</folderpath>	Xóa 1 thư mục

Ĺ



STT	Các lệnh	Tham số	Mô tả
		delete –all <folderpath> ví dụ: delete –all c:\temp</folderpath>	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<sourcepath> <destpath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"</destpath></sourcepath>	Cho phép di chuyển file/ folder
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5="" sha1="" ="" <br="">sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe</filepath></type:>	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath></filepath>	Upload 1 file từ host lên server
9	put	<url><folderpath></folderpath></url>	Download 1 file tới máy host
10	mkdir	<dir name=""></dir>	Tạo 1 thư mục
			Các lệnh liên quan đến process
11	process	-t <processid></processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình



STT	Các lệnh	Tham số	Mô tả
		-s <processid></processid>	Tạm dừng 1 tiến trình
		-r <processid></processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-l -u <username></username>	Liệt kê các process của 1 user
		-e -s <imagepath> -c <cmd> execute a non GUI process as system Ví dụ: process -e -s /tmp/run</cmd></imagepath>	
		-e-u <username> <imagepath> -c <cmd> execute a non GUI process as a user Ví dụ: process -e -u Alex /tmp/run</cmd></imagepath></username>	
		-d <processid> -o <imagepath> generate core file of running program, ví dụ: process -d 231 -o /tmp/core_file</imagepath></processid>	
12	service		Các lệnh liên quan đến service



STT	Các lệnh	Tham số	Mô tả
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename></servicename>	Start 1 service
		-stop <servicename></servicename>	Stop 1 service
		-uninstall <service_name> uninstall service</service_name>	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service - listdrivers	List danh sách drivers trên host
13	usor	-list	Liệt kê các user trên máy
15	user	-sid <username></username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console

+ MACOS:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath></dirpath>	Thay đổi thư mục làm việc hiện tại
		cd hoặc cd	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc



STT	Các lệnh	Tham số	Mô tả		
3	dir	dir list file / subfolder in current folder	Liệt kê các file/ các thư mục con trong thư mục hiện thời		
4		delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"</path>	Xóa 1 file		
	delete	delete -folder <folderpath> ví dụ: delete -folder temp\axvers</folderpath>	Xóa 1 thư mục		
		delete –all <folderpath> ví dụ: delete –all c:\temp</folderpath>	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)		
5	mv	<sourcepath> <destpath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"</destpath></sourcepath>	Cho phép di chuyển file/ folder		
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Hiển thị dữ liệu trong file (giới hạn kích thước file)		
7	Hash	hash <type: md5="" sha1="" ="" <br="">sha256> <filepath> -f get file hash</filepath></type:>	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác		



STT	Các lệnh	Tham số	Mô tả
		ví dụ: example: hash md5 c:\test\run.exe	
8	get	<filepath></filepath>	Upload 1 file từ host lên server
9	put	<url><folderpath></folderpath></url>	Download 1 file tới máy host
10	mkdir	<dir name=""></dir>	Tạo 1 thư mục
			Các lệnh liên quan đến process
11	process	-t <processid></processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid></processid>	Tạm dừng 1 tiến trình
		-r <processid></processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-l -u <username></username>	Liệt kê các process của 1 user
		-e -s <imagepath> -c <cmd> execute a non GUI process as system Ví du: process -e -s /tmp/run</cmd></imagepath>	
		-e-u <username> <imagepath> -c <cmd></cmd></imagepath></username>	



STT	Các lệnh	Tham số	Mô tả
		execute a non GUI process as a user Ví dụ: process -e -u Alex /tmp/run	
			Các lệnh liên quan đến service
12	service	-query	Liệt kê các service đang chạy trên máy host
		-start <servicename></servicename>	Start 1 service
		-stop <servicename></servicename>	Stop 1 service
		-uninstall <service_name> uninstall service</service_name>	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service - listdrivers	List danh sách drivers trên host
13	user	-list	Liệt kê các user trên máy
	usei	-sid <username></username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console

Một số lưu ý khi làm việc với các lệnh trên màn hình console: Lệnh get <filepath>:



Ví dụ: get procexp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình Attachment Log ở phía dưới góc bên phải của màn hình. Người dùng được phép tải file về trình duyệt hoặc xóa file đã lấy về server.

fainment Agent (3)			
	12mg 2		
<u></u>	Jetection 🔛 Containment 😪 Investigation 🦉	Response	
		Ch. Resource scenario	
Add	w remote	W Insperior Astrono	
+ sess	Adem ID: TBUADDEDD4C2C0D55/DDFDB/9A0F5040FCCC	() COUNTROWN	TIMETOLIVE
START TIME END TIME	DESKTOP-R2GBJEF 10:59:35 21/06/202	22 00:11:39	15m
	-list unremane list unre norman cali unremane list unremane bala cameration cameration close cameration of the second close cameration of the second creation of		
	3011/12/34 213 dba #Hery1-Leilin 302/12/34 214 m-ba Bub Tell. dati 302/12/34 218 m-ba Bub Tell. dati 302/12/34 218 m-ba Bub Tell. dati 302/12/34 219 m-ba Bub Tell. dati 302/12/31 140 m-ba Program Files 302/12/31 219 m-ba Program Files 302/12/31 210 m-ba Program Files 302/12/31 210 m-ba 240 Program Files 302/22/31 210 m-ba 240 Program Files 302/22/31 210 m-ba 240 Program Files 302/22/32 120 m-ba 240 Program Files <td>tings 9)</td> <td></td>	tings 9)	
	C:>		
	FILE NAME	TIME CREATED DIRECTORY	
	t.zip	2022-06-21T04:01:16Z C:	
	FLE NAME 120	TIME CREATED EXECUTORY 2002.06-21104.01:16Z C:	

Bước 6: Phiên làm việc của Live Response kết thúc khi:

Thời gian của phiên hết hiệu lực: Khi trường "Duration" bằng thời gian với trường "Time To Live";

P.H		Create	Containment							_	
			Agent: (1)								
۲					Detection	Containment	Investigation	Besponse			
1					<u>All</u> betterion			non nesponse			
₽				Dive response					Response scenario		
-	Remote session lis	t			+ Add new remote	Agent ID: 1B0A66FD56EDD4C	2C6D557DDFDB79A6F5040FC0	c			
Εà	STATUS	AGENT ID		START TIME	END TIME	HOSTNAME DESKTOP-R2GBJEF	STARTEI 10:59:3	5 21/06/2022	© DURATION 00:15:00	TIME TO LIVE 15m	
ē	 Stopped 	1B0A66FD5	6EDD4C2C6D557DDFD	10:59:35 21/06/2022	11:14:35 21/06/2022	Time Modify (GMT+0) Attr	s Size (bytes) Name				
						2021/02/4 2213/6 2022/02/11 11:00 2022/02/11 11:00 2022/02/11 11:00 2022/02/11 11:00 2022/02/11 12:00 2022/02/11 22:00 1 2022/02/12 22:00 1 2022/02/13 22:00 1 2022/02/14 22:07 1 2022/02/15 22:07 1 2022/02/15 22:07 1 2022/02/15 22:07 1 2022/02/15 22:07 1 2022/02/15 22:07 1 2022/02/15 21:07 1 2022/02/15 21:07 1 2022/02/15 21:07 1 2022/02/15 21:07 1 2022/02/15 21:07 1 2022/02/15 21:07 1 2022/02/15 21:07 1 2022/	si Biccrit Biccri Biccri Biccrit Biccrit Biccrit Biccrit Biccrit Biccrit Bi	.Bin det 5. 5.95 Files Files tab tab tab tab tab tab tab tab tab tab	MC CREATED 222 06 21104 01:16Z	exectory C	● Stopp ↓

Người dùng chủ động yêu cầu đóng kết nối bằng lệnh "close";





Khi mất kết nối với agent, server thực hiện ping/pong failed trên 3 lần;

=	aJiant IR flow detail								# 0
5	View detail - huyen_test ← Back to IR flow list								
A ™	TIMELINE								 Close IR flow
) (<u>- Detection</u>	Containment	1 Investigation	Response			
•		🔁 Liven	sponse				Response scenario		
	Remote session list		+ Add new remote session	Agent ID: 33772DD1DC10F04	5300FB156D3F58B30DFBC5374				
Εà	STATUS AGENT ID	START TIME	END TIME	Win10x64bichpt3	STARTED 09:50:55	29/06/2022	ODURATION 00:01:06	TIME TO LIVE 5m	
ē	Stopped 33772DD1DC10F	045300FB156D3F 09:50:55 29/06/2	022 09:52:01 29/06/2022	-е -s <⊥мауераки> -с	cuiu> execute as	system, exampte: proce	ess -e -s c:\winnows\run.exe		
	• Stoper	4.20.005570.040.	000 00108.002	service 	Query sorriscs into service into uncertaint into u	t, example: service -U ::: :: :: :: :: :: :: : : : : : : : :	istérivers		

Ngoài ra, người dùng có thể click nút "+ Add New Remote" để tạo 1 phiên live response mới:

Page | 91



	Create Containment							
			Detection	Containment	K Investigation	Response		
		Elve response					Response scenario	
Remote session list			+ Add new remote	Agent ID: 180A66FD56EDD4	4C2C6D557DDFD879A6F5040FCC	C		
STATUS	AGENT ID	START TIME	END TIME	HOSTNAME DESKTOP-R2GBJEF	STARTER 11:21:3	3 21/06/2022	C DURATION 00:00:08	TIME TO LIVE
Stopped	180A66FD56EDD4C2C6D557DDFD.	. 11:21:33 21/06/2022	11:21:41 21/06/2022			(*) (*****		
Stopped	180A66FD56EDD4C2C6D557DDFD.	. 10:59:35 21/06/2022	11:14:35 21/06/2022			2 - NEG_ENTANG 3 - REG_BUARY 4 - REG_DWORD_LITTLE_ENDIAN 5 - REG_DWORD_BIG_ENDIAN 6 - REG_LINK 7 - REG_MILTI_SZ 9 - REG_EVLL_RESOURCE_LIST 9 - REG_FULL_RESOURCE_DESCR:	Fire form binary 32 - bit number(sa 32 - bit number Symbolic Link(unic Pultiple Unicode s Resource list in th IPTOR Resource list in th	area strag with environment value references ne as REG_DMORD) ode) the resource map he resource map
		Add new remote	session				NDIAN 64 - bit numbe	r -t 1 -d "c:\tem\bin.eve"
		Agent Id			Remote sess	ion range	value, 791698801-7377923109-1	636705026-2080\Software\Test
		DESKTOP-R2GE	UEF(1B0A66FD56EDD4C2C6D5570	DDFDB79A6F5040FCCC)	5 minutes	~	2	
				Cancel	ate 🚹		oad 123 D:malware.dll	
				-s apresestab -s apresestab -1 a -1 - -1 - 	internal control of the product a list proc list proc list proc list proc list proc apparts - <-code apparts	na agginant practice claume a process sess of all users sess of all users sess which hand module a site of the process -e a note, example; process -e st, example; service -listeri	-s crivindevirum-see -a Alex crivindevirum-see vers	
				[Tuesday, 21-Jun-22 94:2	21:41 UTC] agent closed			e Sto
				 Attachment log 				0

3.4.8.2 Response Scenario

Chức năng Response scenario cung cấp khả năng cài đặt một kịch bản Response và thực hiện phản ứng trên một hoặc nhiều Agent;

Các bước thực hiện chức năng Response Scenario trong IRFlow:

Bước 1: Click tab IRFlow:

	aJiant IR Flow							# 0
E.	IR Flow management							Guidelines
A	Type to search queries						Last 7 days	Q
${\rm E}_{\rm H}$	3 result(s) 14/06/2022 10:42:25 - 21/06/202	2 10:42:25						+ Create
۲	TIME	NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE	1	ACTION
_	21/06/2022 09:50:14	IR_huyenpk1	New	root_test	root_test			Ð ()
6-	20/06/2022 16:28:14	IR_HuyenPK	New	root_test	root_test			Ð 0
•	16/06/2022 14:25:35	centos6	New	root_test	root_test			Ð ()
Ē	Showing 3/3 result(s)							
ē								

Bước 2: Click duplicate vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Response Scenario);

Lưu ý: Để thực hiện được các kịch bản phản ứng thì người quản trị phải add sẵn các Artifact ở phần Detection như hình dưới:





Bước 3: Click Response Tab >> Response Scenario:

5	View de ← Backto IB	etail - IR_huyenpk1 R flow list										
▲ ™	TIMELINE	Create Co	ntainment Agent: (1)									Close IR flow
۵				<u>- <u>)</u> Detection</u>	Containment	Ŕ	Investigation	Resp	onse			
◙			Live respon	ise					🗘 Resp	ponse scenario		
Ē.	- 0	Add action to artifacts (Choose artifact(s)	have same type to add action! Drag and I	Drop artifact(s) in table to change position)							+ Add artifacts	Save & Next
ē		Containment integration										
		OBJECT								TYPE	ACTIONS	
		C:\Windows\explorer.exe								Add type		
		C:\Windows\System32\vm.	saservice.exe							Add type		
	2	Deploy to agents										
		Agent list Choose ONLINE agent(s)	in list below and click >> button to add	I to apply agent list			Agent apply list C	lick deploy button to a	apply rule for agent list b	elow		Deploy
		MACOS_BICHPT3 Agent_Id: 0784013009F188F3A0F88021E	ID87717ED5AE10C	Offline o								
		DESKTOP-R2GBJEF Agent_Id: 180A66FD56EDD4C2C6D557DDF	DB79A6F5040FCCC	Online 🔹								

Bước 4: Thực hiện các cấu hình chi tiết: Add action to Artifact

Click nút Add artifacts from detection phase để bắt đầu thêm artifacts vào kịch bản phản ứng; Danh sách Artifact hiển thị từ tab Detection:

Ο	Artifacts from detection (4 artifact(s) selected)		Ari	tifacts added to response		
 	C:\Windows\system32\SnippingTool.exe					
~	C:\Windows\regedit.exe	»				
~	C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe					
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profile s\[4034A037-3505-4974-804E-75BD40A59C0A}\DateLastConnected					

Click nút Ddể chuyển sang phần các artifact trong kịch bản phản ứng:

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



d artifacts to response Artifacts from detection	Artifacts added to response
	C:\Windows\system32\SnippingTool.exe
	C:\Windows\regedit.exe
	C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profile s\[4034A037-3505-4974-804E-75BD40A59C0A]\DateLastConnected
	Cancel Sav

Click "Save" để lưu lại danh sách Artifact đã chọn hoặc "Cancel" để hủy bỏ thao tác chọn trên:

0	Add action to artifact (Choose antifacts have same type to add action! Drag and Drag artifact in table to change position)										
	Containment Integration										
	OBJECT THE	ACTIONS									
	C:\Windows\system32\ShippingTool.exe	Add Type	×								
	C:\WindowsJregedit.exe	Add Type	×								
	CiUsesi\nhand4/ppDatalLocalTempIprocesp64.exe	Add Type	×								
	HKLMSOFTWARE/Microsoft/Windows NTi/CurrentVersion/NetworkList/Profiles/[40344037-33054974-804E-75B040A59C0A]/DateLastConnected	Add Type	×								

Lựa chọn Type cho các Artifact. Hệ thống hỗ trợ gán từng type và action cho từng Artifact hoặc 1 type/action cho nhiều Artifact. Có 3 type: File, Process, Registry. Mỗi Type lại có 1 action riêng;

1	Add action to artifact (Choose artifacts have same type to add action) Drag and Drop artifact in table to change position)		+ Add artifacts	Save & Next Step
	Containment Integration			
	□ oa.#cr	TYPE	ACTIONS	
	C:\Windows\system32\SnippingTooLexe	PROCESS	Terminate	×
	C:\Windows\regadit.exe	PROCESS	Suspend	×
	Cr[Lisers]nhandl4[AppData]Local[Temp]procexp64.exe	FILE	Delete	×
	HKLM(SOFTWARE)Microsoft(Windows NTiCurrentVersion)NetworkList(Profiles)(40344037-3505-4974-804E-758D40A59C0A)(DateLastConnected	REGISTRY	Delete	×

Sau khi hoàn tất phần gán Type và Action, Click Save & Next Step để lưu và chuyển sang bước tiếp hoặc Click + Add artifacts để tiếp tục thêm Artifact;

Deploy to Agent: Danh sách Agent được lấy từ tab Detection;

Tích chọn Agent đang online trong List Agent của IRFlow để thực hiện chuyển sang List các agent thực hiện kịch bản phản ứng;

2	Deploy to agent				
Agent list (1 agent(s) selected) Choose ONLINE agent in list below and click >> button to add to apply agent list			»	Agent apply list Click Deploy button to apply rule for agent list below	Deploy
	nhandt4-PC Agent_id: 806F788659F80650C6285	Online •	«		

Click Deploy; Tích chọn Agent để Deploy;

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



0	Deploy to agent		34-		
	Agent list Choose ONLINE agent in list below and click->> button to add to apply agent list	-	Agent apply list (1 sgent(s) selected) Click Deploy button to apply rule for a	> Deploy	
		*	Nandt4-PC Agent_d-B057785594EC77628887009866594B043005285	Online 🔹	

Bấm nút Deploy

Sau khi bấm nút Deploy, có các trạng thái:

Deploying:

	2	Deploy to agent					
		Agent list Choose ONLINE agent in list below and click >> button to add to apply agent list		•	Agent apply list (1 agent(s) selected) Click Deploy button to apply rule for agent list below		► Deploy
			«	e	nhandt4-PC Agent_id:80EF7B3ES9EECT762888TCC98885SF8D65DC6285	Online 🔹	17:54:39 24/05/2019 deploying •
L							

Successed

2	Deploy to agent				
	Agent list Choose OVE.INE agent in list below and click >> button to add to apply agent list	10	Agent apply list Click Deploy button to apply rule for agent list below		Deploy
			nhandt4-PC Agent_d.B0EF7838396EC77628887CC988855F8D83DC6285	Online •	17:56:49 24/05/2019 successed

Click vào chi tiết để xem kết quả triển khai kịch bản

D	eploy result				×
	Object	Туре	Action	Result	
	C:\Windows\system32\SnippingTool.exe	PROCESS	Terminate	successed	
	C:\Windows\regedit.exe	PROCESS	Suspend	Error: Incorrect function.	
	C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe	FILE	Delete	Error: The request is not supported.	
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{4034A037-350	REGISTRY	Delete	successed	

3.4.9 Close IRFLow

Đóng IRFLow sau khi đã điều tra và xử lý xong;

Để thực hiện close IRFlow click "Close IRFlow" trên màn hình danh sách IRFLow;

≡	aJiant IR Flow								# 0	
Ē.	IR Flow management									
A	Type to search queries									
${\rm F}^{\rm H}_{\rm H}$	6 result(s) 14/06/2022 11.33.23-21/06/2022 11.33.23									
۲	TIME	▼ NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE		ACT	ION	
—	21/06/2022 10:45:23	qqqqqqqqqqwe	New	root_test	root_test		Close	R flow	0	
6-	21/06/2022 10:43:48	wwewqqqqqq	New	root_test	root_test			×.	0	
◙	21/06/2022 10:43:39	999999	New	root_test	root_test			€	0	
_	21/06/2022 09:50:14	IR_huyenpk1	New	root_test	root_test			€	0	
U <u>à</u>	20/06/2022 16:28:14	IR_HuyenPK	New	root_test	root_test			€	0	
¢.	16/06/2022 14:25:35	centos6	New	root_test	root_test			€	0	
-	Showing 6/6 result(s)									





Hoặc click "Close IRFlow" trên timeline ở bất cứ pha nào trong IRFlow: Detection, Containment, Investigation, Response;

	View detail - IR ← Back to IR flow list	Lhuyenpk1						
₽ ₽±		00 Create	Containment Agent: (1)					Close IR flow
X				- <u>`</u> Detection	Containment	Nvestigation	Response	

Nếu khi chọn close IRFLow mà có các tác vụ chưa thực hiện xong như: Containment, Live Response, Response Scenario, Deploy tool... thì sẽ hiện thông báo hỏi người dùng;

≡	aJiant IR Flow	N						* 0
Ţ,	IR Flow management	L2					(Guidelines
A	Type to search queries						Last 7 days	Q
$\mu^{\rm H}$	6 result(s) 14/06/2022 11:33:23	- 21/06/2022 11:33:23						- Create
۲	TIME	* NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE	AC	TION
	21/06/2022 10:45:23	qqqqqqqqqqwe	New	root_test	root_test		1	0
<u>6-</u>	21/06/2022 10:43:48	wwewqqqqqq	New	root_test	root_test		Ð	0
◙	21/06/2022 10:43:39	qqqqqq	New			×	Ð	0
÷	21/06/2022 09:50:14	IR_huyenpk1	New				9	0
Шà	20/06/2022 16:28:14	IR_HuyenPK	New				9	0
ē	16/06/2022 14:25:35	centos6	New	Cannot	close IR flow		9	0
	Showing 6/6 result(s)							
				1. ProcessAnalysis ph 2. LiveResponse phas 3. Containment phase Are you sure you v Cance	hase is pending ! se is pending ! e is pending ! want to force close IR flow el Accept			

Khi người dùng chọn Ok thì sẽ đóng tất cả các kết nối tới Agent trong Irflow; Khi vào IRFLow đã closed chỉ xem được thông tin ở 2 tab Detection và Investigation Result, các tab khác chức năng sẽ bị disable hoặc không hiển thị dữ liệu;

=	viette aJia	nt IR flow detail					₩ 0
3.	View de ← Backtol	etail - centos6 🔒					
A ₽ [±]	TIMELINE	OB Create Close IR Flow					• •
) ()			Detection	Containment	W Investigation	Response	
Ð	0	Rule setting Choose one rule setting to continue next step			-		
Ē.							
ē	- 2	Deploy to agent					
		Agent list Choose agent(s) in list below and click move right button to add to	apply agent list		>> Agent apply list		
		Win10x64bichpt3 Agent_id:33772D010C10F043300F8156D3F56830DF8C5374	default	NOT APPLIED .			



	aJiant IR flow detail	I						× 0
Ę	View detail - centos6							
▲ -	TIMELINE 00	0						
н (Create	Close IR Flow						
Š			Detection	Containment	Investigation	Response		
₽	tột Proc	ess analysis	Q Event Sea	rch		Tools	2	Investigation result
Ē,								
ē				i i i				
				Ľ	D			
				IRFlow	is closed			
				Go to page investigat	ion result to view data !			
	viettel							
=	aJiant IR flow detai	1						× 0
Ę.	View detail - centos6							
4 3. 	TIMELINE 00	Close IP Flow						
÷	Cleate	Close in From						
			Detection	Containment	Investigation	Response		
Ø	Proce	ess analysis	Q Event Sea	rch		Tools	ג 🔪	Investigation result
Ē	v - 1	larked artifact						
Ø	Marked artifact	TIME 16/06/2022 14:25:35	OBJECT C:\Windows\System32\	svchost.exe				Added to IRFlow
	Ł							
	Got artifact							
	8							
	Tools result							

3.5 Màn hình Investigation

Màn hình Investigation gồm một số tab nhỏ là Process Analysis, Event Search, Deploy Tools. Về mặt hoạt động thì 2 chức năng này không khác nhiều so với trong IRFLow. Có 1 số điểm khác sẽ được trình bày cụ thể dưới đây

3.5.1 Investigation_Process Analysis

- Mục đích: Chức năng cho phép người dùng tạo kết nối và kiểm tra hiện trạng process dưới máy người dùng. Trong đó:



_		
► ■	aJiant Investigation / Process analysis	
Ş		
A		
- -		
		>_
D		Process Analysis
₽		Choose an online agent for analyzing running processes, then click 'Connect' to start the session.
*		Choose agent 🗸
Ēλ		
ē		Q search agent
		DESKTOP-RZGBJEF (180A66FD56ED04C2C60557D0FDB79A6F

Danh sách máy người dùng:

+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

 + User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;

Bước 1: Tìm kiếm và chọn Agent kết nối (Lưu ý để đảm bao có thể kết nối, danh sách chỉ hiển thị các máy đang Online);

>_	
Process Analysis	
Choose an online agent for analyzing runnir	ng processes, then click
Connect to start the session.	
Choose agent	~
Choose agent	~

Chọn 01 máy và click nút "Connect" để thực hiện kết nối (kết nối có thể mất tối đa 60 giây)



Process Analysis Choose an online agent for analyzing running processes, then click
'Connect' to start the session.
DESKTOP-R2GBJEF V
Connect
Process Analysis
Choose an online agent for analyzing running processes, then click 'Connect' to start the session.
DESKTOP-R2GBJEF V
Connecting
Connecting to agent (expire in 00:56)
Cancel connection

Bước 2: Xem danh sách tiến trình đang hoạt động tại máy người dùng

DESKTOP-R2GBJEF (180A66FD56EDD4C2)	C6D557DDFDB79A6F5040FCC	CONNECTED TIME 21/06/2022 11:45:40	DURATION 00:00:18	STATUS Running	Change	e agent Stop con
Q Type to search						्र
118 result(s) Last updated: : 21/06/2022 11:45	5:57			Show verified signature 🕥 💿 View sil artifac	ts (0) 💎 Filter by signature	Show colum
Name	PID	Path	User name	Command line	Signature	Action
▼ explorer.exe	5048	C:\Windows\explorer.exe	test	C:\Windows\Explorer.EXE	Microsoft Windows	
SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	test	"C:\Windows\System32\SecurityHealthSystray.exe"	N/A	
vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	test	"C:\Windows\System32\vm3dservice.exe" -u	VMware, Inc.	
vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	test	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n	vm VMware, Inc.	
OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.e	xe test	"C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDriv	e.e Microsoft Corporation	
mmc.exe	6132	C:\Windows\System32\mmc.exe	test	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\	per N/A	
▼ cmd.exe	3212	C:\Users\test\Desktop\New folder\cmd.exe	test	"C:\Users\test\Desktop\New folder\cmd.exe"	N/A	
conhost.exe	9252	C:\Windows\System32\conhost.exe	test	\??\C:\Windows\system32\conhost.exe 0x4	N/A	
▼ Code.exe	11092	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"	Microsoft Corporation	
Code.exe	3284	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"type=gpu-	-pro_Microsoft Corporation	
▼ Code.exe	13300	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"type=rend	lereMicrosoft Corporation	
Code.exe	9228	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"reporter-u	rl= Microsoft Corporation	
Code.exe	5008	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"nolazyin	nsp Microsoft Corporation	
Code.exe	13328	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"type=utilit	ty Microsoft Corporation	
Code.exe	4896	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"type=rend	lereMicrosoft Corporation	
chrome.exe	8308	C:\Program Files (x86)\Google\Chrome\Application\chrome.e	xe test	C:\Program Files (x86)\Google\Chrome\Application\chrom	ie.e Google LLC	
abreese eve	6664	C:\Program Files (x86)\Google\Chrome\Application\chrome	xe test	"C:\Program Files (x86)\Google\Chrome\Application\chrom	e e Google LLC	

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

Trong đó giao diện chia làm các nhóm thông tin:

- 1 Nhóm thông tin liên quan đến kết nối, bao gồm: Máy đang kết nối, thời gian tạo kết nối, thời lượng kết nối tính đến hiện tại, trạng thá kết nối
- 2 Nhóm thông tin hỗ trợ tìm kiếm/làm mới và lọc dữ liệu tại danh sách, bao gồm các thao tác:

Cho phép tìm kiếm theo từ khóa của dữ liệu đang hiển thị trong tất cả các trường trên danh sách;

Prefresh : Cho phép làm mới dữ liệu (vẫn giữ lại các điều kiện tìm kiếm và điều kiện lọc đang sử dụng, chỉ lấy dữ liệu mới nhất từ máy người dùng để hiển thị);

^{show verified signature} : Cho phép bật/tắt việc lấy thông tin chữ ký số cho các tiến trình. Trong trường hợp bật cấu hình này, cho phép lọc dữ liệu tiến trình theo chữ ký số:



Các trạng thái chữ ký số sẽ quy định màu của bản ghi tương ứng

Type to search						Q O Refree
116 result(s) Last updated: : 21/05/2022 11:50:01				Show verified signature	Filter by signature	I Show columns
Name	PID	Path	User name	Command line	Signature	Action
svchost.exe	3360	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	Microsoft Windows Publisher	
svchost.exe	3680	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p	Microsoft Windows Publisher	
SecurityHealthService.exe	6076	C:\Windows\System32\SecurityHealthService.exe	SYSTEM	"C:\Windows\System32\SecurityHealthSystray.exe"	Microsoft Windows Publisher	
svchost.exe	8084	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\System32\svchost.exe -k netsvcs -p	Microsoft Windows Publisher	
VESSvc.exe	14380	C:\Program Files\Ajiant\VESSvc.exe	SYSTEM	"C:\Program Files\Ajiant\VESSvc.exe"	N/A	
VESConfigurationManager.exe	3500	C:\Program Files\Ajiant\VESConfigurationManager.exe	SYSTEM	"C:\Program Files\Ajiant\VESConfigurationManager.exe"	N/A	
VESConnectionManager.exe	8628	C:\Program Files\Ajiant\VESConnectionManager.exe	SYSTEM	"C:\Program Files\Ajiant\VESConnectionManager.exe"	N/A	
VESUpdater.exe	11864	C:\Program Files\Ajiant\VESUpdater.exe	SYSTEM	"C:\Program Files\Ajiant\VESUpdater.exe"	N/A	
VESResponse.exe	18852	C:\Program Files\Ajiant\response\VESResponse.exe	SYSTEM	"C:\Program Files\Ajiant\response\VESResponse.exe"	Viettel Group	
VESProPre.exe	16604	C:\Program Files\Ajiant\propre\VESProPre.exe	SYSTEM	"C:\Program Files\Ajiant\propre\VESProPre.exe"	N/A	
SecurityNotify.exe	7640	C:\Program Files\Ajiant\propre\BLS\SecurityNotify.exe	test	"C:\Program Files\Ajiant\propre\BLS\SecurityNotify.exe" -ppid .	Viettel Group	
VESAutoScan.exe	16592	C:\Program Files\Ajiant\autoscan\VESAutoScan.exe	SYSTEM	"C:\Program Files\Ajiant\autoscan\VESAutoScan.exe"	Viettel Group	
VESCollector.exe	18304	C:\Program Files\Ajiant\collector\VESCollector.exe	SYSTEM	"C:\Program Files\Ajiant\collector\VESCollector.exe"	N/A	
svchost.exe	2656	C:\Windows\System32\svchost.exe	SYSTEM	"C:\Windows\regedit.exe"	Microsoft Windows Publisher	
TrustedInstaller.exe	3908	C:\Windows\System32\wermgr.exe	SYSTEM	C:\Windows\system32\wermgr.exe -upload	Microsoft Windows	
lsass.exe	800	C:\Windows\System32\lsass.exe	SYSTEM	C:\Windows\system32\lsass.exe	Microsoft Windows Publisher	
fontdrvhost.exe	940	C:\Windows\System32\fontdrvhost.exe	UMFD-0	"fontdrvhost.exe"	Microsoft Windows	

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Verified: Xanh có chữ ký số và còn hạn;
- Not verified: Đỏ không có chữ ký số hoặc chữ ký hết hạn;
- N/A: Trắng không tìm thấy thông tin chữ ký số;

show columns T: Cho phép điều chỉnh trường hiển thị trên danh sách tiến trình.

Trên danh sách ngoài trường "Name" luôn hiển thị cố định, các trường còn lại đều có thể tùy chọn hiển thị hoặc không hiển thị.



Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



3 – Danh sách tiến trình, hiển thị dữ liệu tiến trình hiện tại trên máy người dùng với các trường thông tin đã chọn trong phần Show column. Tại mỗi bản ghi, click đúp để xem chi tiết tiến trình;

≡	aJiant Investigation / Process analy	sis			•	0
₽ ▲	HOST NAME DESKTOP-R2GBJEF (180A66FD56EDD4C2C	26D557DDFDB79A6F5040Fi	CCC) 21/06/2022 11:45:40	Process detail Loaded modules File handles Keyhandles Threads Sections Network connections	~	×
۰t	Q Type to search			Q Type to search	9	•
3	117 result(s) Last updated ::21/06/2022 11:50 Name	.01 PID	Path	14 result(s) Path VREGISTRY/USER(S-1-5-21-657600163-1704432705-4217905726-1001_Classes/Local Settings/Software/Microsoft	Ac	tion:
	▼ explorer.exe	5048	C:\Windows\explorer.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes\Local Settings		
	SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes		
¥	vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes		
阆	vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes		
	OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.ex	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NIs\Sorting\Versions		
ē	mmc.exe	6132	C:\Windows\System32\mmc.exe	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NIs\Sorting\Ids		
	♥ cmd.exe	3212	C:\Users\test\Desktop\New folder\cmd.exe	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\(D65231B0-B2F1-4857-A4CF	E	
	conhost.exe	9252	C:\Windows\System32\conhost.exe	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\(7C5A40EF-A0FB-4BFC-874/	A	
	♥ Code.exe	11092	C:\Program Files\Microsoft VS Code\Code.exe	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744	£	
	Code.exe	3284	C:\Program Files\Microsoft VS Code\Code.exe	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options		
	▼ Code.exe	13300	C:\Program Files\Microsoft VS Code\Code.exe	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Ole		
	Code.exe	9228	C:\Program Files\Microsoft VS Code\Code.exe	\REGISTRY\MACHINE		
	Code.exe	5008	C:\Program Files\Microsoft VS Code\Code.exe	\REGISTRY\MACHINE		
	Code.exe	13328	C:\Program Files\Microsoft VS Code\Code.exe			
	Code.exe	4896	C:\Program Files\Microsoft VS Code\Code.exe			
		8308	C:\Program Files (x86)\Google\Chrome\Application\chrome.ex			
	chrome.exe	6664	C:\Program Files (x86)\Google\Chrome\Application\chrome.ex			
		20222				

Chi tiết tiến trình được chia thành các tabs, với mỗi tab, danh sách thông tin tương ứng được hiển thị.

Bước 3: Marking artifact

Tương tự như chức năng Process Analysis trong IRFlow ở màn hình này cũng cung cấp việc đánh dấu các artifact để phục vụ cho việc điều tra;

Người dùng có thể chọn tiến trình từ ngoài danh sách để mark:

≡	aJiant Investigation / Process analysis						* 0
₽ •	HOST NAME DESKTOP-R2GBJEF (180A66FD56EDD4C2C60)	57DDFDB79A6F5040FCC0	CONNECTED TIME 21/06/2022 11:45:40	DURATION 00:11:01	status Running	Change age	nt Stop connect
۶t	Q Type to search						C Refresh
٩	117 result(s) Last updated: : 21/06/2022 11:50:01				Show verified signature	(0) V Filter by signature	Show columns
>-	Name	PID	Path	User name	Command line	Signature	Action
◙	▼ explorer.exe	5048	C:\Windows\explorer.exe	test	C:\Windows\Explorer.EXE	Microsoft Windows	, A Q
	SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	test	"C:\Windows\System32\SecurityHealthSystray.exe"	Microsoft Windows	Mark artifact
*	vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	test	"C:\Windows\System32\vm3dservice.exe" -u	VMware, Inc.	
Ē	vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	test	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vn	m VMware, Inc.	
	OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive	exe test	"C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.	e Microsoft Corporation	
ē	mmc.exe	6132	C:\Windows\System32\mmc.exe	test	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\pe	er Microsoft Windows	
	▼ cmd.exe	3212	C:\Users\test\Desktop\New folder\cmd.exe	test	"C:\Users\test\Desktop\New folder\cmd.exe"	Microsoft Windows	

Hoặc mark các đối tượng khả nghi trong chi tiết tiến trình:



	aJiant Investigation / Process anal	ysis			4 0
₽ ▲	HOST NAME DESKTOP-R2GBJEF (180A66FD56EDD4C2	2C6D557DDFDB79A6F5040F	CONNECTED TIME	Process detail Loaded modules File handles Keyhandles Threads Sections Network connections	~ ×
₽±	Q Type to search			Q Type to search	Q 0
۲	117 result(s) Last updated: : 21/06/2022 11:50	0:01		14 result(s) Path	Action
5	Name	PID	Path	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes\Local Settings\Software\Microsoft	
	▼ explorer.exe	5048	C:\Windows\explorer.exe	\REGISTRY\USER\S-1-5:21-657600163-1704432705-4217905726-1001_Classes\Local Settings	27,3478
	SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes	A
*	vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes	Mark artifact
Ē	vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	\REGISTRY\USER\S-1-5-21-657600163-1704432705-4217905726-1001_Classes	
-A	OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive ex	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NIs\Sorting\Versions	
ē	mmc.exe	6132	C:\Windows\System32\mmc.exe	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NIs\Sorting\\ds	
				\BEGISTEV\M4CHINE\S0ETWARE\Microsoft\Windows\Current\Jersion\Evolorer\EolderDescriptions\JD65231BD.R2E1.4857	AACE.

Với mỗi đối tượng được chọn, lựa chọn "Mark with edit" – đánh dấu trực tiếp nội dung hiện tại. Hoặc người dùng có thể chỉnh sửa nội dung đối tượng trước khi đánh dấu

=	aJiant Investigation / Process analysis							* 0
₽ •	HOST NAME DESKTOP-R2GBJEF (180A66FD56EDD4C2C6D5	S7DDFDB79A6F5040FCCC)	CONNECTED TIME 21/06/2022 11:45:40	DURATION 00:11:58	•	STATUS Running	Change ag	ent Stop connect
₽±	Q Type to search							Q O Refresh
۲	117 result(s) Last updated: : 21/06/2022 11:50:01				Show verified signature	O View all artifacts (t	Filter by signature	I Show columns
	Name	PID	Path	User name	Command line		Signature	Action
•	▼ explorer.exe	5048	C:\Windows\explorer.exe	test	C:\Windows\Explorer.EXE		Microsoft Windows	Ad
2	SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	test	"C:\Windows\System3 Path	list		
*	vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	test	°C:\Windows\System3			2
暾	vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	test	"C:\Program Files\VM	\windows\System32\svcnost.ex	e Edit and mark artifact	M N
-4	OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.ex	e test	"C:\Users\test\AppDat	\Windows\Explorer.EXE		
ē	mmc.exe	6132	C:\Windows\System32\mmc.exe	test	"C:\Windows\system3	\windows\explorer.exe		
	▼ cmd.exe	3212	C:\Users\test\Desktop\New folder\cmd.exe	test	C:\Users\test\Desktop\New fo	ider\cmd.exe"	Microsoft Windows	
	conhost.exe	9252	C:\Windows\System32\conhost.exe	test	\??\C:\Windows\system32\cor	host.exe 0x4	Microsoft Windows	

Sau khi đánh dấu, có thể xem lại danh sách bằng cách click eview all artifacts (1)

Lưu ý: Nút này chỉ hiển thị khi có ít nhất 01 artifact được đánh dấu.

≡	viet a Ji	iant Investigation / Process ar	analysis								0
ية •		HOST NAME DESKTOP-R2GBJEF (180A66FD56EDD- CONTROL CONTROL C	D4C2C6D5570	DDFDB79A6F5D40FCCC)	CONNECTED TIME 21/06/2022 11:45:40	DURATION 00:13:59		STATUS Running		Change ager	11 Stop connect
н,	Q	Type to search									C Refresh
3	1	17 result(s) Last updated: : 21/06/2022 1	11:50:01				Show verified signatu	re 🛑 📕	O View all artifacts (1)	Filter by signature	Show columns
> -		Name	Mark	ed Artifacts					×	nature	Action
		 explorer.exe 	man	and Andraoto						rosoft Windows	
		SecurityHealthSystray.exe	1 result	lt(s)						rosoft Windows	
*		vm3dservice.exe		Time	Agent ID	Object	From	Reference	Action	ware, Inc.	
兪		vmtoolsd.exe		21/06/2022 11:59:51	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\svchost.exe	PROCESS_ANALY	705964A9		ware, Inc.	
-4		OneDrive.exe								rosoft Corporation	
ē		mmc.exe								rosoft Windows	
		▼ cmd.exe								rosoft Windows	
		conhost.exe								rosoft Windows	
		▼ Code.exe								rosoft Corporation	
		Code.exe								rosoft Corporation	
		▼ Code.exe								rosoft Corporation	
		Code.exe			· ·				Sack to top	rosoft Corporation	

Bước 4: Thêm artifact vào IRFLow:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 103



Trên tab Marked artifact, click "Add to IRFLow" trên 1 bản ghi hoặc chọn nhiều artifact ở chế độ multi select và click "Add to IRFLow":

Ma	rked Artifacts			onor	- remed blandtar	×
1 re	sult(s)					
	Time	Agent ID	Object	From	Reference	Action
	27/06/2022 13:53:30	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\smss.exe	PROCESS_ANALY	0465D157	¥ ×
						Madd to IR Flow rienc
						Back to top
Ma	rked Artifacts					×

Sele	ected 2 artifact(s)	ع اسا	Add to IR Flow				
	Time O	9	Agent ID	Object	From	Reference	Acti
	27/06/2022 13:53:30		1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\smss.exe	PROCESS_ANALY	0465D157	
	27/06/2022 13:56:04		1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\csrss.exe	PROCESS_ANALY	0465D157	

Lựa chọn IRFlow đã tạo sẵn hoặc tạo mới IRFLow:



- 4 Danh sách IRFlow đã tạo sẵn:
 - + User đăng nhập thuộc group root: Hiển thị tất cả IRFlow trong hệ thống;



+ User đăng nhập thuộc group default: Hiển thị tất cả IRFlow được assign cho user đang login;

+ User đăng nhập thuộc group cha: Hiển thị tất cả IRFlow được assign cho user đang login và các user thuộc group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả IRFlow được assign cho user đang login;

Add to IR Flo	W			×
IR Flow name	huyen_test			
Assignee(s)	root_test			
List of artifacts				
C:\Windows\Syst	tem32\csrss.exe			
C:\Windows\Syst	tem32\smss.exe			
			Cancel	Add to IR Flow

Danh sách assigned to khi tạo mới 1 IRFlow:

- + User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị tên User đang login;

+ User đăng nhập thuộc group cha: Hiển thị tất cả tên User thuộc group con của user đang login và user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tên User đang login;

Nếu chọn để add vào 1 IRFlow đã tồn tại thì khi chuyển đến màn hình Detection artifact đó sẽ được thêm vào phần Additional detection;

Nếu chọn để add vào 1 IRFlow mới thì khi chuyển đến màn hình Detection artifact đó sẽ được thêm vào phần Original detection;



_									
≡	aJiant IR flow detail	l.							* 0
E,	View detail - huyen_test								
▲ ī≟	TIMELINE 00 Create								Close IR flow
€			Detection	Containment	Investigation	Response			
•	Original detection								
Ē	Agent DESKTOP-R2GBJEF								
ě	Alert								
	TIME	GROUP	HOSTNAME		SCENARIO		SEVERITY		
	23/06/2022 18:13:21	default	DESKTOP-R2GBJEF		Command, Control		Medium	View alert	
	Additional detection								
	Aritfacts								
	TIME	AGENT ID	OBJECT				FROM	REFERENCE	
	27/06/2022 14:17:37	180A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\syste	m32\svchost.exe			PROCESS_ANALYSIS	4F8DBE9A	×
									0

Lưu ý: Dữ liệu artifacts sẽ không bị mất đi nếu chuyển kết nối đến các máy khác nhau hoặc khi máy hiện tại mất kết nối, trường hợp người dùng tải lại trang hoặc điều hướng đến trang khác, hệ thống yêu cầu xác nhận:

Reload site?		
Changes you made may not be saved.		
	Reload	Cancel

3.5.2 Investigation_Event Search

3.5.2.1 Tìm kiếm Event

Chức năng này tương tự trong Event Search của IRFLow:

Bước 1: Nhập câu query >Chọn khoảng thời gian > Click nút "Search":



aJiant IR flow detail								# 0
View detail - huyen_test								
THELINE								⇒ Ə Ciose IR flow
Create								
		:	Detection	investigation	19 Pesponse			
8 Pc	ocess enelysis	Q tven	Search		Teols			[] investigation result
Search AgentO + "180A66F056ED04C2C6055720	OFD87944/S0K0FCCC'							1) Last 7 days
POPULAR	■ 64.025 results 20/06/2022 14/25/44-27/06/202	22 14:25:44						View column
OTHERS	SYSTEMTIMESTAMP	TIMESTAMP	AGENTID			EVENTE	COMPUTER	LOGTWRE
AgentiD	27/06/2022 14:23:34	27/06/2022 14:22:56	180A66FD56EDE4C2C6D557DDFDB79A6	6F5040FCCC		4624	DESKTOP-R2GBJEF	EventLog
Channel	27/06/2022 14:18:32	27/06/2022 14:18:56	180A66FD 56EDD4C2C6D 557DDFD879A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
Computer	27/06/2022 14:13:30	27/06/2022 14:12:56	180A66FD56EDD4C2C6D557DDFDB79A6	6F5040FCOC		4624	DESKTOP-R2GBJEF	EventLog
EventiD	27/06/2022 14:08:28	27/06/2022 14:08:56	180A66FD56EDD4C2C6D557DDFDB79A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
EventRecordID	27/06/2022 14:03:25	27/06/2022 14:02:56	180A66FD56EDD4C2C6D557DDFD879A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
Guid	27/06/2022 13:58:23	27/06/2022 13:58:56	180A66FD56EDD4C2C6D557DDFDB79A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
Keywords	27/36/2022 13:53:21	27/06/2022 13:52:56	180A66FD56EDD4C2C6D557DDFD879A6	6F5040FCCC		4624	DESKTOP-R2GBJEF	EventLog
Level	27/06/2022 13:48:18	27/06/2022 13:48:56	180A66FD 56EDD4C2C6D 557DDFD879A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
LogType	27/36/2022 13:43:36	27/06/2022 13:42.56	180A66FD56EDD4C2C6D557DDFD879A6	6F5040FCCC		70.40	DESKTOP-R2GBJEF	EventLog
Opcode	27/06/2022 13:43:35	27/06/2022 13:42:56	180A66FD 56EDD 4C2C6D 557DDFD879A6	SF5840FCOC		7040	DESKTOP-R2GBJEF	EventLog
Platform	27/36/2022 13:43:35	27/06/2022 13:42:56	1BDA66FD 56EDD4C2C6D 557DDFDB79A6	SF5040FCCC		70.40	DESKTOP-R2GBJEF	EventLog
Tesk	27/06/2022 13:42:43	27/06/2022 13:42:56	180A66FD 56EDD 4C2C6D 557DDFD879A6	SF5840FCOC		7040	DESKTOP-R2GBJEF	EventLog
Version	27/06/2022 13:42:43	27/06/2022 13:42:56	180A66FD56EDB4C2C6D557DDFD879A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
authentication_packaga_name	27/06/2022 13:42:42	27/06/2022 13:42:56	180A66FD 56EDD 4C2C6D 557DDFD879A6	SF5840FCOC		4624	DESKTOP-R2GBJEF	EventLog
client id	27/06/2022 13:38:14	27/06/2022 13:36:56	180A66FD 56EDD4C2C6D 557DDFD879A6	SF5040FCCC		4624	DESKTOP-R2GBJEF	EventLog
duter	27/06/2022 13:33:11	27/06/2022 13:32:56	180A66FD 56EDD-4C2C6D 557DDFD879A6	SF5040FC00		4624	DESKTOP-R2GBJEF	EventLog
elevated token	27/06/2022 13:28:09	27/06/2022 13:26:56	180A66FD 56EDD4C2C6D 557DDFD879A6	SF5040FCCC		4624	DESKTOP-R2GBJEF	EventLog
event id mension	27/36/2022 13:23:07	27/06/2022 13:22:56	180A66FD56EDD4C2C6D557DDFD879A6	SF5840FC00		<u>4624</u>	DESKTOP-R2GBJEF	EventLog
over its id	27/06/2022 13:18:05	27/06/2022 13:16:56	180A66FD56EDD4C2C6D557DDFD879A6	SF5840FCCC		4624	DESKTOP-R2GBJEF	EventLog
0000	27/36/2022 13:13:02	27/06/2022 13:12:56	180A66FD56EDD4C2C6D557DDFD879A6	SF5840FC00		4624	DESKTOP-R2GBJEF	EventLog
battame	27/06/2022 13:08:00	27/06/2022 13:06:56	180A66FD56EDD4C2C6D557DDFD879A6	SF5840FCCC		46.24	DESKTOP-R2GBJEF	EventLog
imperation level	27/36/2022 13:02:58	27/06/2022 13:02:56	180A64FD 56EDD4C2C6D 557DDFD879A	MFSD40FCCC		<u>4624</u>	DESKTOP-R2GBJEF	EventLog
an personation () even	27/06/2022 12:57:55	27/06/2022 12:56:56	180A66FD56EDD4C2C6D557DDFD879A6	SF5040FCCC		4624	DESKTOP-R2GBJEF	EventLog

Bước 2: Thêm các trường tìm kiếm vào câu query với trường Popular và Others bằng cách chọn queries "=" hoặc "#" tại Add to search:

0			Detection	Containment 🥳 Investigation	Response		
0	() Pro	oess enelysis	Q Event Search		Toola		🗋 Investigation result
E)	Search Search						G Last 7 days
(B)	POPULAR	130.031 results 26/06/2022 14:30:67 - 27/06/2022 14:30:67					View column
	OTHERS	ADNTD	EVENTIO	COMPUTER	LOGTYPE	SYSTEMTIMESTAMP	TIMESTAMP
	AgentiD ^	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 14:23:34	27/06/2022 14:22:56
	1BDAMAFD56EDD4C206D557(Add to search	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 14:18:32	27/06/2022 14:18:56
	(50)	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 14:13:30	27/06/2022 14:12:56
	Channel	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 14:08:28	27/06/2022 14:08:56
	Computer	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4524	DESKTOP-R2GBJEF	EventLog	27/06/2022 14:03:25	27/06/2022 14:02:56
	EventiD	180A66FD56EDD4C2C6D557DDFD879A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:58:23	27/06/2022 13:58:56
	EventRecordD	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:53:21	27/06/2022 13:52:56
	Guid	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	4628	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:48:18	27/06/2022 13:48:56
	Keyworda	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	2040	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:43:36	27/06/2022 13:42:56
	Level	1B0A66FD56ED04C2C6D557DDFD879A6F5040FCCC	2040	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:43:35	27/06/2022 12:42:56
	LogType	1BDA66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	2040	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:43:35	27/06/2022 13:42:56
	Opende	1B0A66FD56ED04C2C6D557DDFD879A6F5040FCCC	2040	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:42:43	27/06/2022 12:42:56
	Platform	180A66FD56E804C2C60557D0FD879A6F5040FCCC	4624	DESKTOP-R2GBJEF	EventLog	27/06/2022 13:42:43	27/06/2022 13:42:56

3.5.2.2 Highlight

Mục đích: Cho phép thêm 01 hoặc nhiều highlight để rà soát đồng thời tại một thời điểm (không giới hạn số lượng tối đa), khi thực hiện search hoặc sort thì mọi highlight đã tạo sẽ bị clear;

Các bước thự hiện:

- **Bước 1:** ND chọn Investigation >> Chọn tab Event search;
- **Bước 2:** Màn hình hiển thị danh sách event, Chọn nút "Find and highlight", HT hiển thị poup Find in table;
- **Bước 3:** Nhập vào từ khóa đánh dấu, lựa chọn màu đánh dấu và xác nhận thao tác:

Chọn nút "Add highlight", để xác nhận từ khóa đánh dấu;

Page | 107



Chọn nút "Cancel", để hủy thao tác đánh dấu từ khóa tìm kiếm;

$f\!x$ Search by queries (ex: sever	ity = "CRITICAL" AND status = "	NEW"), or keywords (ex: "	vcs_ajiant")		Last 15 minutes 📋 📿	Show gra
Showing 36 of 36 result(s) 27/06/2022	14:43:38 - 27/06/2022 14:58:38			<	> View artifacts (3) Find and highlight	··· More
Systemtimestamp	Computer	Process path	Description		Add highlight Cancel	Action
27/06/2022 07:51:40	aJiant-automationAPI-1	N/A	Process [5612] C:\Windows\System32\cmd.exe has been created by 36 result(s)			
27/06/2022 07:51:42	aJiant-automationAPI-1	N/A	Process [7848] C:\Windows\System32\cmd.exe has been created by [10008] C:\Progra	am _ N/A	1	
27/06/2022 07:51:42	aJiant-automationAPI-1	N/A	Process [2376] C:\Windows\System32\SecEdit.exe has been created by [7848] C:\Win	do N/A	1	
27/06/2022 07:51:40	aJiant-automationAPI-1	N/A	Process [10480] C:\Windows\System32\more.com has been created by [5612] C:\Windows	do N/A	1	
27/06/2022 07:51:40	aJiant-automationAPI-1	N/A	Process [10144] C:\Windows\System32\wbem\WMIC.exe has been created by [5612]	C:\ N/A	1	
27/06/2022 14:50:43	Win7x86TestEDR	N/A	Process [11356] C:\Windows\System32\more.com has been created by [14300] C:\Windows	nd N/A	1	
27/06/2022 14:50:44	Win7x86TestEDR	N/A	Process [10496] C:\Windows\System32\SecEdit.exe has been created by [13056] C:\W	/inN/A	1	
27/06/2022 14:50:42	Win7x86TestEDR	N/A	Process [1968] C:\Windows\System32\wbem\WMIC.exe has been created by [14300]	C:\ N/A	1	
27/06/2022 14:50:44	Win7x86TestEDR	N/A	Process [13056] C:\Windows\System32\cmd.exe has been created by [5252] C:\Progr	am N/A	1	
27/06/2022 14:50:42	Win7x86TestEDR	N/A	Process [14300] C:\Windows\System32\cmd.exe has been created by [4804] C:\Progr	am N/A	1	
27/06/2022 14:47:55	Win7x86TestEDR	N/A	Process [9496] C:\Program Files\Google\Update\GoogleUpdate.exe has been created	by [N/A	1	
27/06/2022 14:48:51	Win7x86TestEDR	N/A	Process [9456] C:\Program Files\Google\Update\GoogleUpdate.exe has been created	by [N/A	1	
27/06/2022 07:47:36	aJiant-automationAPI-1	N/A	Process [9684] C:\Windows\System32\ROUTE.EXE has been created by [4160] C:\Prog	gra N/A	1	
27/06/2022 14:45:41	Win7x86TestEDR	N/A	Process [3600] C:\Windows\System32\cmd.exe has been created by [5252] C:\Program	m F N/A	1	
27/06/2022 14:45:42	Win7x86TestEDR	N/A	Process [3944] C:\Windows\System32\SecEdit.exe has been created by [3600] C:\Win	do N/A	1	
27/06/2022 14:45:40	Win7x86TestEDR	N/A	Process [13324] C:\Windows\System32\cmd.exe has been created by [10884] C:\Prog	ira N/A	1	
27/06/2022 14:45:40	Win7x86TestEDR	N/A	Process [7124] C:\Windows\System32\wbem\WMIC.exe has been created by [13324]	C:\ N/A	1	
27/06/2022 14:45:40	Win7x86TestEDR	N/A	Process [13348] C:\Windows\System32\more.com has been created by [13324] C:\Windows	nd N/A	1	
27/06/2022 07:45:57	aJiant-automationAPI-1	N/A	Process [14204] C:\Program Files\Viettel\Update\GoogleUpdate.exe has been created	by _ N/A	1	
					0	Jackt 🖌

3.5.2.3 Need help

- Mục đích: tra thông tin event, ý nghĩa trường;
- Các bước thực hiện:
- **Bước 1:** ND chọn Investigation >> Chọn tab Event search;
- Bước 2: Tại màn hình Event Search, chọn "More";
- **Bước 3:** HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Export, Need help, Chọn "Need help?";
- **Bước 4:** HT hiển thị popup Help with Event Search, cho phép tra cứu thông tin, ý nghĩa các trường trong Event Search.


≡	viettet aJiant Investigation / Event search		Help with Event Search $ imes$
ल्म			About events About fields
Ŧ	fx Search by queries (ex: severity = "CRITICAL" AND status = "NEW"), or keywords (ex: "vcs_ajiant")		How to use event_id for investigation?
A			Q Search by Event ID or description
Ptt	Showing 50 of 264.107 result(s) 27/06/2022 14:52:15 - 27/06/2022 15.07:15		Event ID: 0
٢	Source process path	Time stamp	N/A
_	C:\Windows\System32\services.exe	27/06/2022 15:07:00	Event ID: 1
•	C:\Windows\System32\services.exe	27/06/2022 15:07:00	New process has been created
	C:\Windows\System32\services.exe	27/06/2022 15:07:00	Event ID: 2
_	C:\Windows\System32\services.exe	27/06/2022 15:07:00	Process changed a file creation time
Uλ	C:\Windows\System32\services.exe	27/06/2022 15:07:00	Event ID: 3
ø	C:\Windows\System32\services.exe	27/06/2022 15:07:00	Process created TCP/UDP connections on the machine
	N/A	27/06/2022 15:07:00	Fund the d
	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	27/06/2022 15:07:00	Sysmon service state changed
	C:\windows\system32\cmd.exe	27/06/2022 15:07:00	
	C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00	Event ID: 5 Process terminated
	C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:00	Process terminated
	C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:00	Event ID: 6
	C:\Users\admin\AppData\Local\JetBrains\IntelliJ IDEA Community Edition 2020.3.2\jbr\bin\java.exe	27/06/2022 15:07:00	Driver loaded on the system
	C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00	Event ID: 7
	C:\Windows\System32\svchost.exe	27/06/2022 15:07:00	Image loaded in a specific process
	N/A	27/06/2022 15:07:00	Event ID: 8
	C:\windows\system32\taskhost.exe	27/06/2022 15:07:00	Process created a thread in another process
	C:\program files\windowsapps\microsoft.microsoftofficehub_18.2008.12711.0_x648wekyb3d8bbwe\localbridge.exe	27/06/2022 15:07:00	Event ID: 9
	C:\Program Files\Microsoft Office\Office16\EXCEL.EXE	27/06/2022 15:07:00	Process opened for raw read/write access of the disks and volumes
	C:\program files\microsoft office\office16\winword.exe	27/06/2022 15:07:00	Event ID: 30
		Process opened and	
		P	

3.5.2.4 Wrapt text

Mục đích: Có thể hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút "wrap text";

Các bước thực hiện:

- Bước 1: Tại màn hình Event Search, chọn "More";
- **Bước 2:** HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Export, Need help, Chọn "Wrapt text?";
- **Bước 3:** HT thay đổi thông tin hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút "Wrap text";



≡	viettel a Jiant Investigation / Event search			# 0
2 •	fx Search by queries (ex: severity = "CRITICAL" AND status = "NEH"), or keywords (ex: "vcs_sjiant")		Last 15 minutes	Show graph
τŧ	Showing 50 of 264.107 result(s) 27/06/2022 14:52:15 - 27/06/2022 15:07:15	View artifacts	Find and highlight	··· More
۲	Source process path Time stamp			Action
5	C:\Windows\System32\services.exe 27/06/2022.15:07:00			
	C:\Windows\System32\services.exe 27/06/2022.15:07:00			
č	C:\Windows\System32\services.exe 27/06/2022 15:07:00			
¢λ	C:\Windows\System32\services.exe 27/06/2022.15.07.00			
ē	C1Windows\System32\services.exe 27/06/2022.15.07.00			
	C:\Windows\System32\services.exe 27/06/2022 15:07:00			
	N/A 27/06/2022 15:07:00			
	C1Windows\SysW0W64\WindowsPowerShellv1.0\powershell.exe 27/06/2022 15:07:00			
	C1windows1system321cmd.exe 27/06/2022.15:07:00			
	C:\Program Files\Google\Chrome\Application\chrome.exe 27/06/2022 15:07:00			
	C1program files (x86)\viettel\securityagent\worker.exe 27/06/2022 15.07.00			
	C1program files (x86)\viettel\securityagent\worker.exe 27/06/2022 15:07:00			
	C:\Users\admin\AppData\Local\JetBrains\IntellU IDEA Community Edition 2020.3.2\jbr\bin\java.exe 27/06/2022 15:07:00			
	C:\Program Files\Google\Chrome\Application\chrome.exe 27/06/2022 15:07:00			
	C:\Windows\System32\svchost.exe 27/06/2022 15:07:00			
	N/A 27/06/2022 15:07:00			_
			O B	ackt 🖌

3.5.2.5 Export Data

Mục đích: Cho phép tải xuống dữ liệu liên quan đến Event trong hệ thống Các bước thực hiện:

- Bước 1: Tại màn hình Event Search, chọn "More";
- Bước 2: HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Export, Need help, Chon "Export"
- Bước 3: HT hiển thị Popup lọc thông tin Data Event, Chọn các tham số lọc theo điều kiện có sẵn trong hệ thống: Chọn các trường thông tin, Định dạng file export, Số dòng và xác nhận thao tác;

Chọn nút "Export", để xác nhận thao tác tải Data Event;

Chọn nút "Cancel", để hủy thao tác;



Export data		×
Choose fields to export Search Virtual account File signature expried Net extra data Task content Net extradata length Src Authentication package name Dns query status User home directory Severity	Selected fields Source process path Time stamp User logon hours Process Id	File type CSV JSON Autore of rows to export Thomber of rows exceeding 200000 can affect system performance, and it may take a while to system performance, and it may take a while to 20000 20000 D0000 <li< th=""></li<>
Add all fields	Clear all selection	Cancel Export

3.5.3 Note

Mục đích: Hiển thị ở tất cả các màn hình, khi di chuyển đến các màn hình thì nội dung không thay đổi, có thể di chuyển được nút "Note";

Các bước thực hiện:

Bước 1: Tại màn hình Event Search, chọn icon **4**;

Bước 2: HT hiển thị note ở tất cả các màn hình, khi di chuyển đến các màn hình thì nội dung không thay đổi, có thể di chuyển được nút "Note".

A General by superior (and superior - 1007770111 AND status - 100701) as by superior (and first side status)				曲		oh
X Search by queries (ex: severity = "CHITICAL" AND status = "NEW"), or Keywords (ex: "vcs_a]iant")				ast 15 minutes	Q	Sho
Showing 50 of 264.107 result(s) 27/06/2022 14:52:15 - 27/06/2022 15:07:15			View artifacts	Eind and highlig	t •	
Source process path	Time stamp					Act
C:\Windows\System32\services.exe	27/06/2022 15:07:00					
C:\Windows\System32\services.exe	27/06/2022 15:07:00					
C:\Windows\System32\services.exe	27/06/2022 15:07:00					
C:\Windows\System32\services.exe	27/06/2022 15:07:00					
C:\Windows\System32\services.exe	27/06/2022 15:07: My no	ote		Sa	re as	>
C:\Windows\System32\services.exe	27/06/2022 15:07: Note ever	rything you found in here.				
N/A	27/06/2022 15:07:					
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	27/06/2022 15:07:					
C:\windows\system32\cmd.exe	27/06/2022 15:07:					
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:					
C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:					
C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:					
C:\Users\admin\AppData\Local\JetBrains\IntelliJ IDEA Community Edition 2020.3.2\jbr\bin\java.exe	27/06/2022 15:07:					
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:					
C:\Windows\System32\svchost.exe	27/06/2022 15:07.					
N/A	27/06/2022 15:07					



3.5.3.1 Xử lý Event

Marking artifact: Đánh dấu artifact;

Showing 50 of 1	120 result(s) 17/06/2022 10:14:38 -	17/06/2022 10:29:38					Find and highlight	••• More
Event id	Time stamp	File path	Target process path	File signature	Source process path	File signed	Hash md5	Action
1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\Trusted Installer.exe	Microsoft Windows	C:\Windows\System32\services.exe	true	N/A	Mark artife
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.c om	Microsoft Windows	C:\Windows\System32\cmd.exe	true	N/A	
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\Isass.e xe	Sysinternals	C:\Users\admin\AppData\Local\Temp\procexp - Copy64.exe	true	N/A	
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\SecEdi t.exe	Microsoft Windows	C:\Windows\System32\cmd.exe	true	N/A	
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\cmd.e xe	Microsoft Windows	C:\Program Files\Ajiant\propre\BLS\BlsUtils.exe	true	N/A	
3	17/06/2022 10:28:31	N/A	N/A	N/A	C:\windows\system32\sychost.exe	N/A	N/A	

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút icon "Marking artifact". Trên màn hình sẽ hiển thị popup như sau:



- + ND có thể thực hiện chỉnh sửa và đánh dấu bằng cách:
 - Chọn icon 🗳 Edit and mark artifact;
 - Edit đường dẫn (thông tin cần đánh dấu);
 - Chọn icon Complete and Mark để kết thúc thao tác Edit and mark

artifact;

Event id	Time stamp	File path	Target process path	File signature	Source process path	File signed	Hash md5	Ac
1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\Trusted	Microsoft Windows	C:\Windows\System32\services.exe	true	N/A	
			Installer.exe			C:\Windows\servicing\TrustedInstaller.exe		
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.c om	Microsoft Windows	C:\Windows\System32\cmd.exe	Trustedinstaller.exe		0
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.e xe	Sysinternals	C:\Users\admin\AppData\Local\Temp\pr	C:\Windows\System32\services.exe	Edit and mark ar	ufact D
Showing 50 of 12	0 result(s) 17/06/2022 10:14:38 -	17/06/2022 10:29:38	land f fa T land an			View artifacts	Find and highlight	
Showing 50 of 12 Event id	0 result(s) 17/06/2022 10:14:38 - Time stamp	17/06/2022 10:29:38 File path	Target process path	File signature	Source process path	 View artifacts File signed 	Find and highlight Hash md5	••• h Ac
Showing 50 of 12 Event id	0 result(s) 17/06/2022 10:14:38 - Time stamp 17/06/2022 10:28:31	17/06/2022 10:29:38 File path N/A	Target process path C:\Windows\servicing\Trusted	File signature	Source process path C:\Windows\System32\services.exe	View artifacts File signed true	Find and highlight Hash md5 N/A	N Ac
Showing 50 of 12 Event id	D result(s) 17/06/2022 10:14:38- Time stamp 17/06/2022 10:28:31	17/06/2022 10:29:38 File path N/A	Target process path C:\Windows\servicing\Trusted Installer.exe	File signature Microsoft Windows	Source process path C:\Windows\System32\services.exe	View artificts File signed true C:\Windows\servicing\Trustedinstaller.exe	Find and highlight Hash md5 N/A	N Ac Q
Showing 50 of 12 Event id 1	0 result(s) 17/06/2022 10:14:38- Time stamp 17/06/2022 10:28:31 17/06/2022 10:28:31	17/06/2022 10:29:38 File path N/A N/A	Target process path C:\Windows\servicing\Trusted Installer.exe C:\Windows\System32\more.c om	File signature Microsoft Windows Microsoft Windows	Source process path C:\Windows\System32\services.exe C.\Windows\System32\cmd.exe	View artifacts File signed true C:\Windows\servicing\Trustedinstaller.exe Trustedinstaller.exe	Find and highlight Hash md5 N/A	N Ac Q
Showing 50 of 12 Event id 1	D result(s) 17/06/2022 10:14:38 - Time stamp 17/06/2022 10:28:31 17/06/2022 10:28:31	17/06/2022 10:29:38 File path N/A N/A	Target process path C:Windowsiservicing\Trusted Installer.exe C:Windows/System32\more.c own C:Windows/System32\lass.e	File signature Microsoft Windows Microsoft Windows Sysintemals	Source process path C:\Windows\System32\services.exe C:\Windows\System32\cmd.exe C:\Uiers\udmini4optata\Local\TempLpr	View artifacts File signed true C:Windows\servicing\Trustedinstaller.exe Trustedinstaller.exe C:Windows\System32\services.exe	Find and highlight Hash md5 N/A Complete and	۰۰۰ N Act

Viettel Cyber Security



+ ND chỉ đánh dấu Mark Artifact:

н ^л	Showing 50 of 1	20 result(s) 17/06/2022 10:14:38 - 1		View artifacts Find and highlight		••• More				
۵	Event id	Time stamp	File path	Target process path	File signature	Source process path		File signed	Hash md5	Action
E	4624	17/06/2022 10:28:49	N/A	N/A	N/A	C:\Windows\System32\services.exe		N/A	N/A	
Ø	10	17/06/2022 10:28:31	N/A	C:\Windows\system32\Jsass.e xe	Sysinternals	$\label{eq:c:Users} C:\label{eq:c:Users} C:$		true	N/A	•
¥	1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\Trusted	Microsoft Windows	C:\Windows\System32\services.exe		true	N/A	□ ●
÷				Installer.exe			C:\Windows\servicing\T	rustedInstaller.exe		
ι <u>ά</u>	1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.c om	Microsoft Windows	C:\Windows\System32\cmd.exe	TrustedInstaller.exe			
ē	10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.e	Sysinternals	C:\Users\admin\AppData\Local\Temp\p	C:\Windows\System32\	services.exe	Mark witho	ut edit

Hoặc chọn icon Cancel để bỏ đánh dấu marking artifact:

3	20/06/2022 11:32:03	N/A	N/A	N/A	C:\program files (x86)\google\chrome\app	lication\chrome.exe	N/A	N/A	×	
1	20/06/2022 11:32:03	N/A	C:\Windows\System32\wbem	Microsoft Windows	C:\Windows\System32\cmd.exe		true	N/A	A	0
10	20/06/2022 11:32:03	N/A	C:\Windows\system32\lsass.e	Microsoft Corporation	C:\Users\test\Desktop\SysinternalsSuite\g	C:\Windows\System32\cmd.exe				
1	20/06/2022 11:32:03	N/A	C:\Windows\System32\cmd.e	Microsoft Windows	C:\Program Files\Ajiant\propre\BLS\BlsUti	e. (minden o toyotem o 2 tem a. ene			Linemark antifact	
1	20/06/2022 11:32:03	N/A	C:\Program Files\Ajiant\propr	Viettel Group	C:\Program Files\Ajiant\propre\VESProPre	C:\Windows\system32\wbem\wmi	c.exe		orman artifact	
1	20/06/2022 11:32:03	N/A	C:\Windows\servicing\Trusted	Microsoft Windows	C:\Windows\System32\services.exe	C:\Windows\System32\wbem\en-L	JS\csv			
13	20/06/2022 11:32:03	N/A	N/A	N/A	C:\Windows\System32\cmd.exe	WMIC.exe				
3	20/06/2022 11:32:03	N/A	N/A	N/A	C:\Program Files (x86)\Google\Chrome\Ag	C:\Windows\System32\whem\WM	IC exe			
11	20/06/2022 11:32:03	C:\Users\test\AppDa	. N/A	N/A	C:\Windows\System32\cmd.exe					

Bước 2: Khi marking artifact thành công màn hình sẽ hiển thị thông báo:

<i>S</i>	Artifact(s) marked successfully!	
	Ignore	View artifacts	

ND chọn nút "View artifacts" để chuyển đến màn hình danh sách Artifacts:

	Time	Agent ID	Object	From	Action
	20/06/2022 11:36:59	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Program Files\Ajiant\recovery\VESRecoveryHandler.exe	EVENT_LOG	
	20/06/2022 11:38:23	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\program files (x86)\google\chrome\application\chrome	EVENT_LOG	
	20/06/2022 11:39:09	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\cmd.exe	EVENT_LOG	
	20/06/2022 11:39:14	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\system32\wbem\wmic.exe	EVENT_LOG	
	20/06/2022 11:45:08	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\wbem\en-US\csv	EVENT_LOG	
	20/06/2022 11:48:10	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	HKLM\System\CurrentControlSet\Services\EventLog\VEDR	EVENT_LOG	
resu	t(s)				A Back to top

Xem thông tin chi tiết event: ND chọn 1 bản ghi bất kỳ và hover vào bản ghi đó, click vào icon "Xem chi tiết" ¹:



Event detail Detail Raw data	:
Q Search by field name o	r value
Description	Registry object HKLM\System\CurrentControlSet\Services\EventLog\VEDR has been added or deleted by [13552] C:\Program Files\Ajiant\recovery\VESRecoveryHandler.exe
Event id	12
Time stamp	20/06/2022 11:34:03
Source process path	(Verify this field) C:\Program Files\Ajiant\recovery\VESRecoveryHandler.exe
Agent id	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC
Channel	AdvanceCollector/Operational
Computer	DESKTOP-R2GBJEF
Log type	EventLog
Platform	windows
Systemtimestamp	20/06/2022 11:35:01
Thread id	0
Client id	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC
Event ID meaning	Registry object added or deleted
Event log id	20220620_j6fo928cku9svi39ruikpb3tpebgg167
Group	default
Hostname	DESKTOP-R2GBJEF
Log channel name	AdvanceCollector/Operational
Log provider name	AdvanceCollector
Reg desired access	3
Reg event type	CreateKey
Reg target object	HKLM\System\CurrentControlSet\Services\EventLog\VEDR
Signature id	12

3.5.4 Investigation_Deploy Tools

Mục đích: chức năng cho phép deploy (triển khai) các tools (công cụ) phục vụ điều tra, xử lý sự cố an toàn thông tin từ Portal xuống các Agents.

3.5.4.1 Tool Management

Mục đích: quản lý toàn bộ tool của hệ thống, người sử dụng có thể thêm/ xóa tool ở màn hình này. Các tính năng ở màn hình này gồm có:

+ Hiển thị danh sách tool cùng các thông tin chi tiết của tool: Tên, Parameter, Version, Architecture, Upload User, Platform, Output, Thời gian upload;

+ Tìm kiếm tool: Tìm kiếm theo tên tool



+ Upload tool: upload tool chạy trên agent Windows, MacOS và Linux có dung lượng tối đa 100MB;

≡	viettel aJiant	Investigation / Deploy Tool								# 0
Ę.	Tool manage	ement Task management								
A	Q Search too	ol								Q
pH Ø	Showing 50	of 170 result(s)							Show only my tool	oad tool
		Tool OutputFile_Linux_Params Upload by root_lest at 14/12/2022 18:825 Version fail Architecture x86 Output hohoho.b.t Parameter N/A	THE STREET	Tool OutputFolder_Linux_Params Upload by reat_test at 14/12/2022 18:28:48 Version 1 Architecture x64 Output Test Parameter N/A	-	etf Uplo Uplo Arch Outp Para	I OutputFile_Linux_Params ad by root_test at 14/12/2022 18:27:35 ion 1 litecture x64 uut hohoho.txt umeter N/A		Tool StdOut_Linux_LongTime Upload by reeLest at 14/12/2022 18:26:59 Version 1 Architecture x64 Output StdOut Parameter N/A	-
Q		OutputFolder.ps1 Upload by root_best at 14/12/2022 18:26:02 Version 1 Architecture N/A Output Test Parameter N/A	•••	OutputFile.ps1 Upload by root_best at 14/12/2022 18.25.48 Version 1 Architecture N/A Output hohoho.txt Parameter N/A		Stdi Upio Vers Arch Outp Para	Out.ps1 aid by reot.text N/A umeter N/A	-	Tool StdOut, x64, Params.exe Upload by rod_Vest at 14/12/2022 18:24.08 Version 1 Architecture x64 Output StdOut Parameter N/A	-
		Tool StdOut_x86_Params.exe Upload by root_test at 14/12/2022 18/23.55 Version 1 Architecture x86 Output StdOut Parameter N/A	 Q	Tool StdOut_Linux_Params Upload by root_bet at: 14/12/2022 18:23:25 Version 1 Architecture X64 Output StdOut Parameter N/A		Uplos Vers Arch Outp Para	I StdOut_OSX_Params ad by reet_lest at 14/12/2022 18/23/05 ilon 1 illecture x64 out StdOut imeter N/A		Tool OutputFolder_x64_Params.exe upload by rect_test at 14/12/022 16/22.37 Version 1 Architecture x64 Output Test Parameter N/A	
		Tool OutputFolder_x86_Params.exe		Tool OutputFolder_OSX_Params		— Тоо	I OutputFile_x64_Params.exe	-	Tool OutputFile_x86_Params.exe Activate Windows Go to Settings to activate Wind	Back to top

Với tính năng Upload tool thao tác theo các bước sau:

Click vào "Upload tool" > Chọn đường dẫn đến tool cần upload hoặc kéo thả tool vào giao diện > Nhập thông tin vào popup Tool info > click **Upload tool**:

Jiant	investigatio	T/ Depidy 1001										-
Tool mana	gement	Task management										
Q Search to	loc											
Showing 50	0 of 170 result(s)									Show only my tool	Upload
	Tool Output	File_Linux_Params lest at 14/12/2022 18:38:25		Tool Output	Folder_Linux_Params test at 14/12/2022 18:28:48			Tool Output	File_Linux_Params est at 14/12/2022 18:27:35		Tool StdOut_Linux_LongTime Upload by root_test at 14/12/2022 18/26/59	
۵	Version Architecture	fail x86	A	Version Architecture	1 x64		A	Version Architecture	1 x64	A	Version 1 Architecture x64	
	Output Parameter	hohoho.bd N/A		Output Parameter	Test N/A			Output Parameter	hohoho.bxt N/A		Output StdOut Parameter N/A	
					Upload tool			×				
exe	Upload by root_	r.ps1 lest at 14/12/2022 18:26:02	 exe	Upload by roo	2 En Choose file	/lax file size is s executable fil	100 MB, supp e	orted file types	at 14/12/2022 18:25:18	 -	Tool StdOut_x64_Params.exe Upload by root_test at 14/12/2022 18:24:08	
	Version Architecture	1 N/A		Architecture	N/A	-		Architecture	N/A		Version 1 Architecture x64	
	Output	Test		Output	hohoho.txt			Output	StdOut		Output StdOut	
	Parameter	N/A		Parameter	N/A.			Parameter	N/A		Parameter N/A	
	Tool StdOut	_x86_Params.exe		Tool StdOut	_Linux_Params test at 14/12/2022 18 23 25			Tool StdOut	OSX_Params	 exe	Tool OutputFolder_x64_Params.exe	
	Version	1	A	Version	1		ui.	Version	1		Version 1	
	Architecture	x86		Architecture	x64			Architecture	x64		Architecture x64	
	Parameter	N/A		Parameter	N/A			Parameter	N/A		Parameter N/A	
0	Tool Output	Folder_x86_Params.exe		Tool Output	Folder_OSX_Params			Tool Output	file_x64_Params.exe		Tool OutputFile_x86_Params.exe	

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Với tính năng xóa tool, chọn icon 💻 tại tool cần xóa > chọn Delete

≡	viettel aJiant	Investigation / Deploy Tool						# 0
Ę.	Tool mana	agement Task management						
A	Q Search t	tool						Q
₽ ^H	Showing 5	60 of 170 result(s)					Show only my tool	oad tool
► ₩	्म	Tool OutputFile_Linux_Params Upload by root_best at 14/12/2022 18:88:25 Version fall Architecture x86 Output hoboho txt Parameter N/A	 R	Tool OutputFolder_Linux_Params Upload by reot_text at 14/12/2022 18:28:48 Version 1 Architecture x64 Output Test Parameter N/A	2 Deploy this to Delete	Tool OutputFile_Linux_Params Upload by root_test at 14/12/2022 1827.35 of Prohtecture x64 Output hohoho.txt Parameter N/A	 Tool StdOut_Linux_LongTime Upload by reat_itest at 14/12/2022 18/26/59 Wersion 1 Architecture K64 Output StdOut Parameter N/A	-
هم ۲		OutputFolder.ps1 Upload by root_test at 14/12/2022 18:26:02 Version 1 Architecture N/A Output Test Parameter N/A	•••	OutputFile.ps1 Upload by root.text at 14/12/2022 18:25:48 Version 1 Architecture N/A Output hohoho.txt Parameter N/A		StdOut_ps1 Upload by root_lest at 14/12/2022 18:25:18 Version 1 Architecture N/A Output StdOut Parameter N/A	 Tool StdOut_x64_Params.exe Upload by mod_lest at 14/12/2022 18:24:08 Version 1 Average the stdout Version StdOut Parameter N/A	
		Tool StdOut_x86_Params.exe Upload by root_set at 14/12/2022 18:23 55 Version 1 Architecture x66 Output StdOut Parameter N/A	 8	Tool StdOut_Linux_Params Upload by root_tent at 14/12/2022 18:23:25 Version 1 Architecture x64 Output StdOut Parameter N/A	•	Tool StdOut_OSX_Params Upload by root_letal at 14/12/2022 18 23 85 Version 1 Architecture x64 Output StdOut Parameter N/A	 Tool OutputFolder_y64_Params.exe Upload by mot_leaf at 1/(1/2)022 18:22:37 Version 1 Version 1 Version 1 Output 764 Output 76st Parameter N/A	
		Tool OutputFolder_x86_Params.exe		Tool OutputFolder_OSX_Params		Tool OutputFile_x64_Params.exe	 Tool OutputFile_x86_Params.exe Activate Windows Go to Settings to activate Window	Back to top

3.5.4.2 **Deploy tool**

Mục đích: Cấu hình thông tin deploy tool dưới agent Điều kiện:

+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default:

+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;

Các bước thực hiện Deploy tool tại màn hình Tab Tool management:

Bước 3: Sau khi lựa chọn tool, chọn icon icon tại bản ghi tool cần deploy > chọn Deploy this tool, man hinh Create new task hiển thị:



≡	aJiant Investigation / Deploy Too	l		# 0
<u>_</u>	Tool management Task manag	Create new task	×	
▲ ⁷ ±	Q Search task Showing 50 of 1664 result(s)	Information Please fill out all the information of this task. Task name Task deploy tool Linux(Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups Edit Choose apentify or groups Edit	Show only my schedule New task
	Task name Author t276 root_t t275 root_t task mac root_t	Description About your task	Number of agent(s) run in each time Edit All selected agent(s) Run this task	Upcoming agents Action N/A N/A N/A N/A
Î <u>⊾</u> ₽	Task 888668 root_t 1274 root_t 1273 root_t	Tool to deploy Tool OutputFolder_Linux_Params	Trigger Edit Trigger Start time Expired time Immediately At the time this _ N/A	N/A N/A N/A
	retry 8 root_t t272 root_t retry 6 root_t Task event abrile root_t	Tool parameters (optional) Parameters for this tool Tool output	Advanced C Delete output after run tool I the task failed to run, retry up to:	N/A N/A N/A
	task dijent abdus 10001 task fff root_t ddf root_t fdf root_t	Folder V Test	1 time(s) within 3 hour(s) v every 30 minute(s) Cancel the task if the tool can not return output report from agent after: 30 minute(s)	N/A N/A N/A
	im 23 root_t daily 23 root_t daily 22 root_t im 22 root_t			N/A N/A N/A
	zsdsd root_t		Cancel Create	N/A Activate Windows Co to setting to activat Q Back to top

- **Bước 4:** Thực hiện nhập các thông tin task để deploy tool: Task name, Description, Tool parameters, Tool output;
- **Bước 5:** Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

Lựa chọn **All agent(s)**: chọn tất cả các agent(s) trong phạm vi quản lý của user đang đăng nhập để thực hiện deploy;

Lựa chọn agents or groups thực hiện deploy – Choose agent(s) or group(s):

Information Please fill out all the information of Task name	this task.	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit.					
Task deploy tool Linux		Choose agent(s) or group(s)					
About your task		Number of agent(s) run in each time					
Tool to deploy Tool OutputFolder_Linux_Para Tool parameters (optional) Parameters for this tool	 All agents (total 50 agents) Choose agent(s) or group(s) 	2 Edit mation of selected agent(s) will be showing here.					
Tool output Folder V Test		Cancel Save minute(s) > Cancel the task if the tool can not return output report from agent after: 30 minute(s) >					

+ Chọn Add agent(s):

viettel

security

≡	aJiant Investigation	n / Deploy To	bl			* (3
<u> </u>	Tool management	Task manaç	Create new task			×	
▲ 1 ⁴	Q Search task	(\$)	Information Please fill out all the information of this task Task name Task deploy tool Linux		Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups Choose agent(s) or group(s)	e Show only my schedule New task	۶.
•	Task name	Autho	Description		Number of agent(s) run in each time	upcoming agents Action	
	1276	root_t	About your task		Edit	N/A	
	t275	root_t	Edit a	ssignees	×	N/A	
*	Task 99969	root_t		agents (total 50 agents)		N/A	
Ēλ	1056 000000	root	Tool to deploy	oose agent(s) or group(s)	2		
	1274	root					
<u>e</u>	1273	root	Tool OutputFolder_Linux_Para		3 Add acont(c)	N/A	
_	101 y 0	root	Tool parameters (optional)		mation of selected age. Add amun(s)	N/A	
_	retry 6	root t	Parameters for this tool		Hen Broth 2)	N/A	
_	Task agent abods	root t	Tool output		Cancel Save	N/A	
_	task fff	root_t	Folder		minute(s) ~	N/A	
_	ddf	root_t			Cancel the task if the tool can not return output report from agent after: 30 minute(e) set	N/A	
_	fðf	root_t			Cancer the task in the tool can not return output report non agent alter. 30 minute(s) *	N/A	
	im 23	root_t				N/A	
	daily 23	root_t				N/A	
	daily 22	root_t				N/A	
	im 22	root_t				N/A	
	zsdsd	root_t			Cancel	N/A	
			_			Go to Settings to activate Windows	

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi **T**: (+84) 971 360 360 **E**: vcs.sales@viettel.com.vn | **W**: www.viettelcybersecurity.com 

• Tìm kiếm Agent: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent

≡	aJiant Investigation / Deplo	/ Tool	* 0
(*1) (1)	Tool management Task ma	Create new task X	
▲ 1 ² H ◎	Q Search task Showing 50 of 1664 result(s)	Information Agents or groups Please fill out all the s Task name Task deploy tool tar fix Computer Name ~ "ubu" Selected (2)	C Show only my schedule.
¥k ⊲	1276 ro- 1275 ro- 1275 ro- 1275 ro-	U About your task U U Edit 10 result(s) In a gent ID Computer name IP Address Group Status	N/A N/A N/A
Ē.▲ ®	Tail NESSOR ro 1274 ro 1273 ro 1273 ro retry 8 ro 1272 ro retry 6 ro Task agent abcds ro daff ro daff ro daff ro daff ro daff ro daff/23 ro daff/23 ro	Tool to deploy 	N/A N/A
	im 22 ro zsdsd ro	Cancel Create	N/A NA Activate Windows Go to Settings to activate Windows

Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều
 Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung Selected > chọn
 Cancel để hủy thao tác thêm Agent để deploy hoặc chọn nút Add để xác nhận danh sách Agent(s):

=	aJiant Investigation	/ Deploy To	ol										* 0
	Tool management Ta	ask manaç	Create new task								×		
A	Q Search task		Information			Agents or groups							۹
÷Ξ		_	Task name	Add	agent(s)				\times	ang or them, o	aick the		
0	Showing 50 of 1664 result(s))	Task deploy tool Lin	fx	ComputerName ~ "ubu"				9 Q		Edit	Show only my schedule	G New task
>-	Task name	Autho	Description	Select	ted (2)							Upcoming agents	Action
_	t276	root_t	About your task	ub	untu × ubuntu18 ×				• ~		Edit	N/A	
~	t275	root_t										N/A	
ЩĽ	task mac	root_t		10 res	sult(s)							N/A	
-	Task 888868	root_t			Agent ID	Computer name	IP Address	Group	Status		Edit	N/A	
$\mathbb{F}_{\underline{A}}$	t274	root_t	Tool to deploy		27CFD9DA7A0394EA7CC955.	_ ubuntu	127.0.0.1, 192.168.12.	global	 Offline 			N/A	
¢	t273	root_t	Tool OutputFolder_L		2F1EB4A7D7FD84483EC743	ubuntu-2004	127.0.0.1, 10.0.2.15, 1	anhnn_test	 Online 			N/A	
	retry 8	root_t	Tool parameters (onti		60AA2618E17825BADCD191	ubuntu18	127.0.0.1, 192.168.25.	group_ubuntu	 Offline 			N/A	
	t272	root_t	Tool parameters (ope		A303D982A258A6328267D0	ubuntu	127.0.0.1, 192.168.74	anhnn_test	Offline			N/A	
	retry 6	root_t	Parameters for this		BB5933621EB880749E6AA6	ubuntu18	127.0.0.1, 192.168.74	thanhnm18_test	 Offline 			N/A	
	Task agent abcds	root_t	Tool output		BE56627FA3FEE2B1ECBBE5	bichpt3-ubuntu	127.0.0.1, 192.168.25.	group_ubuntu	Offline			N/A	
	task fff	root_t	Folder 🗸		C68C5DFCFA883C928D7CAE.	huyenpt_ubuntu18	127.0.0.1, 192.168.74.	thanhnm18_test	 Offline 	ute(s) 🗸		N/A	
	ddf	root_t			E414646EFAF694E531F810A.	thanhnm18-ubuntu18-test	127.0.0.1, 192.168.12.	global	 Offline 	minute(s) 🗸	N/A	
	fðf	root_t										N/A	
	im 23	root_t						< 1	2)			N/A	
	daily 23	root_t										N/A	
	daily 22	root_t						Cancel	Add			N/A	
	im 22	root_t										N/A	
	zsdsd	root_t	_							Cancel	Create	N/A Activate Windows Go to Settings to activate	e Windows.
													4

Viettel Cyber Security



Hover vào các Agent(s) đã chọn > Chọn icon dể thực hiện loại
 bỏ Agent(s) khỏi danh sách đã chọn



Chọn Cancel để hủy hoặc chọn Save để lưu thông tin các Agent(s)
 đã chọn để deploy:

=	aJiant Investigation / De	ploy To	ol											# 0
2	Tool management Task I	manaç	Create new task									×		
▲ F#	Q Search task Showing 50 of 1664 result(s) Task name 1276	Authe	Information Please fill out all the information Task name Task deploy tool Linux Description About your task.	of this task. Edit assignees		Agents Settings respect Selecte Choose	s or groups s for assignees an ive buttons to edit d agents or group e agent(s) or group	d triggering for s	r this task are set b	y default. To d	change anything of them, click th Edit Edit	e	Show only my schedule O Upcoming agents N/A	New task Action
♥ 兼 Ē⊾	1275 task mac Task 888868 1274	root_t root_t root_t	Tool to deploy	 All agents (total 50 a Choose agent(s) or 	agents) group(s)		•	Add agent/gro	Import from	n list v	Edit		N/A N/A N/A	
2	1273 retry 8 1272 retry 6	root_t root_t root_t root_t	Tool OutputFolder_Linux_Para Tool parameters (optional) Parameters for this tool	2 agent(s) Agent ID (0 056DC579B568 k 07718463D55E k	Computer r HuyenPT-W virtual_ager	name /in10x64 nt_maintn	IP Address 192.168.74.128, 127.0.0.1, 172.1	Group edr_team maitest	Status Offline Offline	Action			N/A N/A N/A N/A	
	Task agent abods task fff ddf fdf im 23 daily 23	root_t root_t root_t root_t root_t root_t	Tool output Folder V Test	-					Cancel	Save	r: 30 minute(s) ~		N/A N/A N/A N/A N/A	
	daily 22 im 22 zsdsd	root_t root_t root_t									Cancel	ate	N/A N/A Activate Windows Go to Settings to activate Wind	rok te top

+ Chọn Add group(s):

Viettel Cyber Security



≡	aJiant Investigation / Dep	Tool		* 0
<u> </u>	Tool management Task m	Create new task	×	
▲ ^{pH} ⊙	Search task Showing 50 of 1664 result(s) Task name 1276 1275 1	Information Please fill out all the information of this task. Task mee Task deploy tool Linux Description About your task Edit accimpage	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups Edit Choose agent(s) or group(s) Edit Number of agent(s) run in each time Edit	Show only my schedule Typeoming agents Action N/A NA
×# 🔂 💁	task mac a Task 88868 a t274 a t273 a t272 a retry 8 a task agent abods a task fff a	Tool to deploy Tool outputFolder_Linux_Pars Tool outputFolder_Linux_Pars Tool outputFolder_Linux_Pars Tool output Parameters (optional) Parameters for this tool Tool output Folder V Tex	Is So agents) (s) or group(s) Information of selected Add agent(s) Cancel Sove minute(s) ~	NA N/A N/A N/A N/A N/A N/A N/A
	daf f fdf e im 23 de daily 23 e im 22 e zadad e		Cancel the task if the tool can not return output report from agent after: 30 minute(s) Cancel Cancel	N/A N/A N/A N/A N/A N/A N/A Activate: Windows So to settings to activate Windows

• Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:

\equiv	aJiant Investiga	tion / Deploy To	ol								# 0
(*1) (1)	Tool management	Task manaç	Create new task	Add group	(s)		×		×		
A	Q Search task		Information	Qt			© Q.	authing of them	click the		Q
P ⁴			Task name	• NOTE: In thi	s interface, users belonging to the parer	nt group have full control over all the child gro	oups of their parent gr <u>See more ≥≥</u>				
۲		ult(s)	Task deploy tool Linux		Group	Location	Action		Edit	Show only my schedule	New task
D -1	Task name	Authc	Description	□ 💑	TENANT_viettel.com.vn					Upcoming agents	Action
	t276	root_t	About your task	🗆 💑	anhnn_test	admin			Edit	N/A	
	t275	root_t		- 😪	cnctest	TENANT_nsm.com/anhvn				N/A	
*	task mac	root_t		□ 💑	default					N/A	
~	Task 888868	root_t		□ 💑	edr_team	viettel/khoi_phu_thuoc/vcs_ann	n		Edit	N/A	
ΕÅ	t274	root_t	Tool to deploy			H < 1	2 3 4 5 ≻ ▶	ed time		N/A	
٢	t273	root_t	Tool OutputFolder_Linu			_				N/A	
	retry 8	root_t	Tool parameters (optional	Selected						N/A	
	t272	root_t		No group(s)						N/A	
	retry 6	root_t	Parameters for this tool	Group	Location		Action			N/A	
	Task agent abcds	root_t	Tool output							N/A	
	task fff	root_t	Folder 🗸 T					minute(s) 🗸		N/A	
	ddf	root_t				(\mathbf{X})		0 minut	e(s) 🗸	N/A	
	fðf	root_t				\sim				N/A	
	im 23	root_t				NO DATA TO SHOW				N/A	
	daily 23	root_t								N/A	
	daily 22	root_t								N/A	
	im 22	root_t								N/A	
	zsdsd	root_t					Cancel Save	Cancel		N/A	
				_						Activate Windows	

 Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung Selected > chọn Cancel để hủy thao tác thêm group(s) để deploy hoặc chọn nút Save để xác nhận danh sách group(s):

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



≡	aJiant Investigation / Deploy T	ool		# 0
(**) 	Tool management Task management	Create new task	Add group(s) X X	
▲ "±	Q Search task	Information Please fill out all the infor Task name	Q t Q Q NOTE in this interface, uses belonging to the parent group have full control over all the child groups of their parent grup. Sea more are nything of them, click the	<u>م</u>
0	Showing 50 of 1664 result(s)	Task deploy tool Linux	Group Location Action	Show only my schedule • New task
	Task name Author 1276 root_J 1275 root_J 1276 root_J Task 88866 root_J 1274 root_J 1273 root_J	Description About your task Tool to deploy	0 0 12 0 MM - finite.com/ min 0 </th <th>Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/A</th>	Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/A
ş	retry 8 root_1 1272 root_1 retry 6 root_1 Task agent abcds root_1	Tool Output voter_Linu Tool parameters (optiona Parameters for this too Tool output	Selected 2 group(s) Group Location Action Contest TENANT_nsm.com/anlwn	N/A N/A N/A
	task fff root.d ddf root.d fdf root.d im 23 root.d daily 23 root.d daily 22 root.d	Folder V	Gefault ninute(s) √ minute(s) minute(s) √ minute(s) minute(s) minute(s) minute(s) minute(s) minute(s) minute(s)	N/A N/A N/A N/A N/A
	root_1		Cancel Seve Cancel Create	N/A Activate Windows Go to Settings to activate Windows

Hover vào các group(s) đã chọn > Chọn icon dể thực hiện loại
 bỏ group(s) khỏi danh sách đã chọn

≡	viettel aJiant Investigation / De	eploy To	ol						# 0
Ţ.	Tool management Task	(manaç	Create new task				×		
▲ ₽±	Q Search task		Information Please fill out all the information Task name	of this task.		Q			
0	Showing 50 of 1664 result(s)		Task deploy tool Linux		Selected agents or groups		Edit	Show only my schedule	New task
۶.	Task name	Autho	Description	Edit assignees		×		Upcoming agents	Action
◙	t276 t275	root_t	About your task	 All agents (total 50 agents) 			Edit	N/A N/A	
₩	task mac	root_t		Choose agent(s) or group(s)				N/A	
÷	Task 888868	root_t		0(-)	G Add agent/	group Import from list V	Edit	N/A	
ЦŸ	1274	root_t	Tool to deploy	3 group(s) Group	Location	Action	Expired time	N/A	
ģ	t273	root_t	Tool OutputFolder_Linux_Para	TENANT_nsm.com	N/A	â	N/A	N/A	
_	retry 8	root_t	Tool parameters (optional)	S congne	TENANT_edr.com			N/A	
_	t272	root_t	Parameters for this tool	S default	N/A			N/A	
_	retry 6	root_t						N/A	
_	Task agent abcds	root_t	Tool output			< 1 >	minute(e) >	N/A	
_	task fff	root_t	Folder 🗸 Test				Timute(o)	N/A	
_	646	root_t				Cancel Save	er: 30 minute(s) V	N/A	
_	im 22	root t						N/A	
_	daily 23	root t						N/A	
	daily 22	root						N/A	
	im 22	root_t						N/A	
	zsdsd	root_t					Annual Constant	N/A	
			_	_	_		Cancel Create	Activate Windows Go to Settings to activate Win	4

 Chọn Cancel để hủy hoặc Chọn Save các group(s) đã chọn để deploy:



Tool management	Task manag	Create new task					×		
Q Search task Showing 50 of 1664 result	(s)	Information Please fill out all the information Task name Task deploy tool Linux	of this task.	Agents or groups Settings for assignees and triggerin respective buttons to edit. Selected agents or groups	ig for this task are set by default. T	o change anything of them,	click the Edit	Show only my schedule	New ta
Task name	Authc	Description	Edit assignees		×			Upcoming agents	Actio
t276 t275 task mac	root_t root_t root_t	About your task	 All agents (total 50 agents) Choose agent(s) or group(s) 	Add agen	t/group Import from list▼	(Edit	N/A N/A N/A	
Task 888868	root_t	Tool to deploy	3 group(s)				Edit	N/A	
+272	root t		Group	Location	Action	Expired time		N/A	
1273	root	Tool OutputFolder_Linux_Para	TENANT_nsm.com	N/A	۵.	N/A		N/A	
1070	TOOL	Tool parameters (optional)	🛃 congnc	TENANT_edr.com				N/A	
1272	root	Parameters for this tool	🛃 default	N/A				N/A	
Task agent abode	root t	Tool output			 1 			N/A	
task fff	root t					minute(s) 🗸		N/A	
ddf	root t	Polder V Test			Cancel	m 20 minute	(0) + 4	N/A	
fdf	root t					a. 30 minute	(5)	N/A	
im 23	root_t							N/A	
daily 23	root_t							N/A	
daily 22	root_t							N/A	
im 22	root_t							N/A	
zsdsd	root_t					Canaal	Create	N/A	
						Cancel	Create		

+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn Import from list

- Chọn **Download sample file** để lấy form danh sách file agent(s) mẫu;
- Nhập thông tin agent(s) > chọn Import from .CSV để thực hiện tải lên

danh sách agent(s)

≡	aJiant Investigation /	Deploy To	l		* 0
	Tool management Ta	sk manag	Create new task	×	
land the second	Q Search task		Information Please fill out all the information of this task. Task name Task deploy tool Linux Description	Agents or groups Settings for assignces and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups Choose agent(s) or group(s)	Show only my schedule New task
P	Task name	Autho	Description	Number of agent(s) run in each time	Opcoming agents Action
	t276	root_t	About your task	Edit	N/A
<u> </u>	task mac	root t	Edit assignees	×	N/A
*	Task 888868	root t	 All agents (total 50 agen 	ts)	N/A
ĒΔ	1274	root_t	Choose agent(s) or grou	p(s) Expired time	N/A
តា	t273	root_t	Tool OutputFolder Linux Para	Add agent/group Import from list▼ N/A	N/A
Ť	retry 8	root_t	Taal assessmenters (antianal)	Information of selected agent(e) will be showing Import from .CSV 3	N/A
	t272	root_t	Tool parameters (optional)	Download sample file	N/A
	retry 6	root_t	Parameters for this tool	2	N/A
	Task agent abcds	root_t	Tool output	Cancel Save	N/A
	task fff	root_t	Folder V Test	minute(s) V	N/A
	ddf	root_t		Cancel the task if the tool can not return output report from agent after: 30 minute(s) ~	N/A
	fðf	root_t			N/A
	im 23	root_t			N/A
	daily 23	root_t			N/A
	daily 22	root_t			N/A
	im 22	root_t			N/A
	zsdsd	root_t		Cancel Create	N/A Activate Windows Go to Settings to activate Windows top
					4

Viettel Cyber Security



Bước 6: Cấu hình số lượng agent deploy tool mỗi lần:

+ All Agent: Cho phép deploy toàn bộ agent(s) người dùng đã chọn



+ Cấu hình số lượng agent mỗi lần deploy:

Tool management	Task manaç	Create new task		×
Q Search task Showing 50 of 1664 resul	it(s) Authc	Information Please fill out all the information of this task. Task name Task deploy tool Linux Description	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click th respective buttons to exit. Selected agents or groups Choose agent(s) or group(s)	he Show only my schedule New Upcoming agents Act
1276 1275	root_t	About your task	Number of agent(s) run in each time All selected agent(s) Edit	N/A N/A N/A
Task 888868 1274	root_t	Tool to deploy Choose n	mber of agents X Edit umber of agents you want to run in each time: Expired time Expired time Expired time	N/A N/A
t273 retry 8 t272 retry 6	root_t root_t root_t	Tool OutputFolder_Linux_Params 2 0 90 Tool parameters (optional) Parameters for this tool	agent(s) every 3 hour(s) v until finished	N/A N/A N/A
Task agent abcds task fff	root_t	Tool output Folder	1 time(s) within 3 hour(s) v every 30 minute(s) v	N/A N/A
ddf fdf im 23	root_t		Cancel the task if the tool can not return output report from agent after: 30 minute(s) ~	N/A N/A
daily 23 daily 22	root_t			N/A N/A
im 22 zsdsd	root_t		Cancel	N/A N/A

Bước 7: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

Viettel Cyber Security



+ Chọn **Run immediately** để thực hiện cấu hình thời gian deploy tool **ngay lập tức** (sau khi tạo task thành công)

	aJiant Investigation / C	Deploy To	ol			* 0
<u>r</u>	Tool management Tas	ik manaç	Create new task		×	
 ↓[#] Ø I 	Q Search task Showing 50 of 1664 result(s) Task name 1275	Authe root_t	Information Please fill out all the information of this task: Task deploy tool Linux Description About your task		Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttoms to edit. Selected agents or groups Edit Choose agent(s) or group(s) Edit Number of agent(s) run in each time Edit	Show only my schedule Upcoming agents Action N/A N/A N/A
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	taak mac Task 88800 1274 1273 retry 8 1272 retry 6 Task agent abcds taak fff	t_toon t_toon t_toon t_toon t_toon t_toon t_toon t_toon	Tool to deploy Tool OutputFolder,Linux,Params Tool parameters (optional) Parameters for this tool Tool output Polder V Test	Edit trigger When this task is creat © Run immediately © Run on a schedule	ed: Expired time vsk is cre_ N/A Cancel Swy 1 time(s) within 3 hour(s) ~ every 30 minute(s) ~	N/A N/A N/A N/A N/A N/A N/A N/A
	ddf fdf im 23 daily 23 daily 22 im 22 zodid	t_toon t_toon t_toon t_toon t_toon t_toon t_toon			Cancel the task if the tool can not return output report from agent after: 30 minute(a) ~	N/A N/A N/A N/A N/A N/A N/A N/A Activate Windows Go to Setting to solvate Windows

+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo lập lịch:

- Chọn schedule One time:
 - Cho phép lập lịch deploy tool một lần;
 - Cấu hình thời gian bắt đầu:

and the second se	X		Create new task		
	groups assignees and triggering for this task are set by default. To change anything of them, click the uttons to edit.	f this task.	Information Please fill out all the information of this ta Task name		Q Search lask
Show only my schedule	Edit		Task deploy tool Linux		Showing 50 of 1664 result(s)
Upcoming agents Act	nt(s) or group(s)		Description	Autho	Task name
NZA	Edit		About your task	root_t	t276
N/A	×	Edit trigger		root_t	t275
N/A	0	When this task is creat		root_t	task mac
N/A	Edit	2 Run on a schedule		root_t	Task 888868
N/A	Expired time		Tool to deploy	root_t	t274
N/A	ask is cre N/A	One time	Tool OutputFolder_Linux_Params	root_t	1273
N/A		Start time	Tool assumptions (antional)	root	retry 8
N/A		15/12/2022 - 00:	(Contraction of the second sec	root_t	t272 a
N/A			Parameters for this tool	1001_1	retry 6
N/A	5 Company (1997)		Tool output	root_t	Task agent abcds
N/A	Cancel Save ery 30 minute(s) ~		Folder 🗸 Test	root_t	task fff
N/A	the task if the tool can not return output report from agent after: 30 minute(s) \sim	the second se		root_t	ddf
N/A				root	fdf
N/A				root_t	im 23
N/A				root_t	daily 23
N/A				root	daily 22
N/A				root	im 22
N/A	Cancel			root_t	zsdsd

Viettel Cyber Security



- Chọn schedule **Daily**:
 - Cho phép lập lịch deploy tool hàng ngày;
 - o Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:

≡	aJiant Investigation / De	eploy Too	bi				* 9
Ţ	Tool management Task	manaç	Create new task			;	<
▲ "±	Q Search task	1	Information Please fill out all the information of this Task name	task.	Agents or groups Settings for assignces and triggering for this task are set b respective buttons to edit.	y default. To change anything of them, click the	Q
0	Task name	Autho	Task deploy tool Linux Description	Edit trigger	×	Edit	Upcoming agents Action
₩ ₩	1276 1275 task mac	t_toor t_toor t_toor	About your task	When this task is creat 2 Run immediately Run on a schedule Daily	led:	Edit	N/A N/A N/A
Ēλ	Task 888868	root	Tool to deploy	Recur		Expired time	N/A N/A
9	1273 retry 8 1272		Tool OutputFolder_Linux_Params Tool parameters (optional) Parameters for this tool	Start time	00:00 th	ask is cre N/A	N/A N/A N/A
	Task agent abcds task fff	root	Tool output	Expire in	15/12/2022-00:00 🛗	ery 30 minute(s) ~	N/A N/A
	ddf fdf im 23	root_t			Cancel	agent after: 30 minute(s) ~	N/A N/A
	daily 23 daily 22	root_t					N/A N/A
	im 22 zsdsd	root_t				Cancel	N/A N/A
				_			Go to Settings to activate Windows

- Chọn schedule **Weekly**:
 - Cho phép lập lịch deploy tool hàng tuần;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:



≡	aJiant Investigation / Deple	y Tool	* 0
<u>_</u>	Tool management Task ma	Create new task X	
∎ ^T ±	Q Search task	Information Agents or groups Please fill out all the information of this task. Settings for assignces and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Task name Task name	٩
۲	Showing 50 of 1664 result(s)	Task deploy tool Linux Edit trigger X	Show only my schedule
).).	Task name Au	the Description When this task is created:	Upcoming agents Action
_	t276 ro	ALI About your task.	N/A
	t275 ro	CL 2 O Run on a schedule	N/A
پلا	task mac ro	AL Weekly	N/A
	Task 888868 ro	Edit	N/A
E7	t274 ro	n_1 Tool to deploy Recur this task every 1 4 week(s) on: Expired time	N/A
ø	t273 ro	at. Tool OutputFolder_Linux_Params ask is cre N/A	N/A
	retry 8 ro	Tool parameters (optional)	N/A
	t272 ro	til Start time	N/A
	retry 6 ro	15/12/2022 - 00:00:00 B	N/A
	Task agent abcds ro		N/A
	task fff ro	t Folder V Test	N/A
	ddf ro	agent after: 30 minute(s) ~	N/A
	fđf ro	Cancel Save	N/A
	im 23 ro	AJ	N/A
	daily 23 ro	U C	N/A
	daily 22 ro	u la	N/A
	im 22 ro	0	N/A
	zsdsd ro	Cancel Create	N/A
			Go to Settings to activate Windows
			4

- Chọn schedule Monthly:
 - Cho phép lập lịch deploy tool hàng tháng;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:

Tool management Ta	sk maha(Create new task				>	<	
Q Search task		Information		Agents or groups				
		Please fill out all the information of this t	ask.	Settings for assignees and triggering for th	is task are set by default. To chan	ge anything of them, click the		
		Task name	Edit trigger		×	_	-	
Showing 50 of 1664 result(s)		Task deploy tool Linux	When this task is crea	ited:		Edit	Snow only my schedule	C New t
Task name	Autho	Description	 Run immediately 				Upcoming agents	Acti
1276	root_t	About your task	- ² O Run on a schedul	le		Edit	N/A	
t275	root_t		Monthly				N/A	
task mac	root_t		Recur				N/A	
Task 888868	root_t		Recur this task in	these months:		Edit	N/A	
t274	root_t	Tool to deploy	May August	× October ×	0 ¥ E	xpired time	N/A	
t273	root_t	Tool OutputFolder_Linux_Params	at these days:		ask is cre N	/A	N/A	
retry 8	root_t	Tool parameters (optional)		and the second	5		N/A	
t272	root_t	Parameters for this tool	9 10 2 10	5 X 30 X Last day or month X	0		N/A	
retry 6	root_t	Parameters for this tool	Start time				N/A	
Task agent abcds	root_t	Tool output	15/12/2022 - 00	0:00:00	t	minuta(a) a s	N/A	
task fff	root_t	Folder 🗸 Test	- Custor In	45-40-6000 00-0000 #	ery 50	minute(s) 🗸	N/A	
ddf	root_t		Expire in	13/12/2022 00:00:00	n agent after:	30 minute(s) V	N/A	
tđi	root_t				8		N/A	
Im 23	root			Can	cel Save		N/A	
daily 22	root t		-		_		N/A	
im 22	root t						N/A	
zerled	root t						N/A	
						Cancel Create	Activate Mindows	

Viettel Cyber Security



Bước 8: Cấu hình thông tin nâng cao cho task

+ **Delete tool after run tool** cho phép xóa tool output sau khi run tool và trả kết quả về BE thành công;

+ **If the task failed to run, retry upto** khi task deploy thất bại,cho phép cấu hình thông tin retry task (deploy lại task)

≡	aJiant Investigation / Deploy 1	001		* 0
	Tool management Task mana	Create new task	×	
▲ ¹⁺ 0 : ▼ * @	Q Search task	Information Please fill out all the information of this task. Task name Task deploy tool Linux Description About your task Tool to deploy	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttoms to exit. Selected agents or groups Edit All agents (total 50 agents) Edit Number of agent(s) run in each time Edit All selected agent(s) Edit Run this task Edit Trigger Edit Trigger Edit	Show only my schedule Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/A N/A
Q	1273 root. refty 8 root. 1272 root. refty 6 root. Task agent abcds root. ddf root. ddf root. fdf root. dally 23 root. dally 23 root. dally 23 root. zddsd root.	Tool OutputFolder_Linux_Params Tool parameters (optional) Parameters for this tool Tool output Folder Test	On day(s) 9, 10, 16, 30 and last day of May 15/12/2022 15:00:00 23/12/2022 00:00:00 Advanced 9 Delete output after run tool 1 time(s) within 3 hour(s) v every 3 minute(s) v Cancel the task if the tool can not return output report from agent after: 30 minute(s) v	N/A M/A M/A N/A N/A

+ Cancel the task if the tool can not return output report from agent after cho phép hủy task nếu task không thể chạy sau thời gian cấu hình của người dùng:



Tool management Task n	K Create new task		×	
Q Search task	Information Agents or group Please fill out all the information of this task. Settings for assigner spectree buttom Task name Settings for assigner spectree buttom Task deploy tool Linux All agents (not agents) About your task Number of agent, all all setted agents Image: Setting for agent agents Settings for assigner spectree buttom Setting for agent agents All agents (not agent) About your task Number of agent, all setted agent Task task Run this task	58 nees and triggering for this task are set by default. To change anything of the to edit. (a groups 0 agents) (b) run in each time (c)	m, click the Edit Edit	Show only my schedule New Upcoming agents Act N/A N/A
Task 88866 r Task 88866 r 1274 r 1273 r retry 8 r 1272 r retry 6 r Task agent abcds r task fff r ddf r	Tool to deploy Tool to deploy Tool QuputFolder_Linux_Params Tool parameters (optional) Parameters for this tool Tool output Folder Test Cancel the task fail Tuble	Start time Expired time 6, 30 and last day of May 15/12/2022 15:00:00 23/12/2022 00:00 after run tool	Edit D0	N/A N/A N/A N/A N/A N/A N/A N/A
fdf r Im 23 r daily 23 r Im 22 r zsdsd r		Cance	Create	N/A N/A N/A N/A N/A

Bước 9: Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

3.5.4.3 Task management

e. Danh sách task

Mục đích: Hiển thị danh sách task lập lịch deploy tool;

Các trường thông tin hiển thị: Task name, Author, Created time, Description, Number of agent(s), Trigger, Next run time, Status, Upcoming agents



≡	aJiant Investigation	n / Deploy Tool								# 0
	Tool management	Task managemer	nt							
-										
A	Q Search task									Q
P ⁴										
0	Showing 50 of 1664 result	(s)							Show only my schedule	New task
> -	Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
	t276	root_test	14/12/2022 18:39:11	N/A	1	Immediately	N/A	Finished	N/A	
•	t275	root_test	14/12/2022 18:36:21	N/A	1	Immediately	N/A	Finished	N/A	
i	task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	 Finished 	N/A	
÷	Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
Ľ <u>à</u>	t274	root_test	14/12/2022 17:47:06	N/A	1	Immediately	N/A	Finished	N/A	
ē	t273	root_test	14/12/2022 17:42:13	N/A	1	Immediately	N/A	 Finished 	N/A	
	retry 8	root_test	14/12/2022 17:13:17	N/A	1	Immediately	N/A	 Stopped 	N/A	
	t272	root_test	14/12/2022 17:11:03	N/A	1	Immediately	N/A	Finished	N/A	
	retry 6	root_test	14/12/2022 17:00:09	N/A	1	Immediately	N/A	Finished	N/A	
	Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	 Stopped 	N/A	
	task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	 Finished 	N/A	
	ddf	root_test	14/12/2022 15:55:04	N/A	1	Immediately	N/A	 Finished 	N/A	
	fðf	root_test	14/12/2022 15:51:54	N/A	1	Immediately	N/A	 Finished 	N/A	
	im 23	root_test	14/12/2022 15:21:05	N/A	5	Immediately	N/A	Finished	N/A	
	daily 23	root_test	14/12/2022 14:52:23	N/A	5	At 14/12/2022 - 15:00:00	N/A	Finished	N/A	
	daily 22	root_test	14/12/2022 14:48:31	N/A	5	At 14/12/2022 - 14:55:00	N/A	Finished	N/A	
	im 22	root_test	14/12/2022 14:47:24	N/A	5	Immediately	N/A	 Finished 	N/A	
	zsdsd	root_test	14/12/2022 14:06:55	N/A	5	Immediately	N/A	 Finished 	N/A	
									Activate Windows Go to Settings to activate	

f. Tìm kiếm task

Mục đích: Cho phép tìm kiếm task theo tên task;

Các bước thực hiện: Nhập vào từ khóa tìm kiếm > chọn nút **Search** hoặc kết thúc nhập từ khóa > nhấn enter. HT thực hiện tìm kiếm thông in Agent liên quan đến từ khóa tìm kiếm có trong hệ thống:

aJiant	n / Deploy Tool								4
Tool management	Task manageme	ent							
Q task								2	8
Showing 50 of 285 result(s)							Show only my schedule	+ New
Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Act
Task r7	root_test	15/12/2022 14:46:17	N/A	2	Immediately	N/A	Finished	N/A	
Task ró	root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	Finished	N/A	
Task r5	root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	• In Progress	N/A	
Task f4	root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	Finished	N/A	
Task r3	root_test	15/12/2022 14:21:01	N/A	2	Immediately	N/A	Finished	N/A	
Task r2	root_test	15/12/2022 14:20:29	N/A	2	Immediately	N/A	Finished	N/A	
Task r1	root_test	15/12/2022 14:12:22	N/A	2	Immediately	N/A	Finished	N/A	
Task r	root_test	15/12/2022 14:10:12	N/A	2	Immediately	N/A	 Finished 	N/A	
Task 8988	root_test	15/12/2022 09:32:14	N/A	1	Immediately	N/A	Finished	N/A	
task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	 Stopped 	N/A	
task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	Finished	N/A	
Task retry a	root_test	14/12/2022 11:21:36	N/A	1	Immediately	N/A	Finished	N/A	
Task rep dgf	root_test	13/12/2022 18:09:43	N/A	5	Immediately	N/A	Finished	N/A	
Task 90	root_test	13/12/2022 18:09:21	N/A	5	Immediately	N/A	 Stopped 	N/A	
Task test report 89	root_test	13/12/2022 18:01:38	N/A	5	Immediately	N/A	Finished	N/A	
Task test repm 9	root_test	13/12/2022 17:54:48	N/A	5	Immediately	N/A	Finished	N/A	

Page | 130



g. Tạo task

(Chức năng tương tự như mục 3.5.4.2. Deploy tool)

Mục đích: Cấu hình thông tin deploy tool dưới agent Điều kiện:

+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;

Các bước thực hiện deploy tool tại tab Task management:

Bước 10: Sau khi lựa chọn tool, chọn icon icon tại bản ghi tool cần deploy > chọn **Deploy this tool**, màn hình Create new task hiển thị:



a Jiant Investigation / Deploy	Tool		
Tool management Task man	Create new task	×	
Task name Aut 1276 100 1275 100 1275 100 1275 100 1273 100 1274 100 1273 100 1274 100 1273 100 1274 100 1272 100 1272 100 1272 100 1274 100 1273 100 retry 8 100 1272 100 1273 100 retry 6 100 134k agent abcds 100 145k fff 100 16f 100 16g 100 102 100 103 100	Information Please fill out all the information of this task. Task name Task deploy tool Linux Description About your task Tool to deploy Tool OutputFolder_Linux_Params Tool parameters (optional) Parameters for this tool Tool output Folder Folder Test	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the reserve buttons to edit. Selected agents or groups Edit Choose agent(s) or group(s) Edit Mumber of agent(s) run in each time Edit All exicted agent(s) Edit Trigger Edit Trigger Edit Trigger At the time this – N/A Advanced In the task failed to run, retry up to: 1 time(s) within 3 four(s) ~ every 30 minute(s) ~ 1 time(s) within 3 four(s) ~ every 30 minute(s) ~	Show only my schedule Upcoming agents Action N/A
im 22 roo zsdsd roo		Cancel Create	N/A N/A Activate Windows @ Back to t

- **Bước 11:** Thực hiện nhập các thông tin task để deploy tool: Task name, Tool to deploy, Description, Tool parameters, Tool output;
- **Bước 12:** Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

Lựa chọn **All agent(s)**: chọn tất cả các agent(s) trong phạm vi quản lý của user đang đăng nhập để thực hiện deploy;

Lựa chọn agents or groups thực hiện deploy – Choose agent(s) or group(s):

Information Please fill out all the information of Task name	this task.	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit.
Task deploy tool Linux		Selected agents or groups Edit Choose agent(s) or group(s) Edit
About your task		Number of agent(s) run in each time
Tool to deploy Tool OutputFolder_Linux_Para Tool parameters (optional) Parameters for this tool	 All agents (total 50 agents) Choose agent(s) or group(s) 	2 Edit mation of selected agent(s) will be showing here.
Tool output Folder V Test		Cancel Save minute(s) > Cancel the task if the tool can not return output report from agent after: 30 minute(s) >

+ Chọn Add agent(s):

viettel

security

≡	aJiant Investigation / D	eploy To	ol			# 0
<u>_</u>	Tool management Tas	k manaç	Create new task			×
▲ ^{p±}	Q Search task Showing 50 of 1664 result(s)		Information Please fill out all the information of this tas Task name	k.	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttoms to edit.	Show only my schedule New task
	Task name	Autho	Description		Choose agent(s) or group(s)	Upcoming agents Action
Ø	t276 t275	root_t	About your task Edit	assignees	Nomber of agent(s) run in each time	N/A N/A
兼	task mac Task 888868	root_t	O AI	agents (total 50 agents) loose agent(s) or group(s)	Z	N/A N/A
ē.	t274 t273	root_t	Tool to deploy Tool OutputFolder_Linux_Para		Add agent/group Import from list	N/A N/A
	retry 8 t272	root_t	Tool parameters (optional) Parameters for this tool		rmation of selected by Add agent(s) Add group(s)	N/A N/A
	Task agent abcds	root_t	Tool output		Cancel Save minute(s) v	N/A N/A
	ddf fdf	root_t	lest		$\hfill \Box$ Cancel the task if the tool can not return output report from agent after: 30 minute(s) \backsim	N/A
	im 23 daily 23	root_t				N/A N/A
	daily 22 im 22	root_t				N/A N/A
	zsdsd	root_t			Cancel Creat	te Activate Windows
						4

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

• Tìm kiếm Agent: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent

\equiv	aJiant Investigation /	Deploy To	ol										# 0
<u>_</u>	Tool management Tas	sk manaç	Create new task								×		
A	Q Search task		Information			Agents or groups							Q
P ₂ ±			Please fill out all the in Task name	Add	l agent(s)			1	×	ning of them,	click the		
0	Showing 50 of 1664 result(s)		Task deploy tool Lin	fx	ComputerName ~ "ubu"				9 Q		Edit	Show only my schedule	New task
).).	Task name	Authc	Description	Selec	ted (2)							Upcoming agents	Action
	t276	root_t	About your task	u	ountu × ubuntu18 ×				• ~	ſ	Edit	N/A	
~	t275	root_t										N/A	
э.	task mac	root_t		10 re	sult(s)							N/A	
~	Task 888868	root_t			Agent ID	Computer name	IP Address	Group	Status	ſ	Edit	N/A	
Γ <u>λ</u>	t274	root_t	Tool to deploy	~	27CFD9DA7A0394EA7CC955	. ubuntu	127.0.0.1, 192.168.12.	global	 Offline 			N/A	
ø	t273	root_t	Tool OutputFolder_I		2F1EB4A7D7FD84483EC743	ubuntu-2004	127.0.0.1, 10.0.2.15, 1.	anhnn_test	 Online 			N/A	
	retry 8	root_t	Tool parameters (onti	~	60AA2618E17825BADCD191	ubuntu18	127.0.0.1, 192.168.25.	group_ubuntu	 Offline 			N/A	
	t272	root_t	root parameters (opn		A303D982A258A6328267D0	ubuntu	127.0.0.1, 192.168.74.	anhnn_test	 Offline 			N/A	
	retry 6	root_t	Parameters for this		BB5933621EB880749E6AA6	ubuntu18	127.0.0.1, 192.168.74.	thanhnm18_test	 Offline 			N/A	
	Task agent abcds	root_t	Tool output		BE56627FA3FEE2B1ECBBE5	bichpt3-ubuntu	127.0.0.1, 192.168.25.	group_ubuntu	 Offline 			N/A	
	task fff	root_t	Folder 🗸		C68C5DFCFA883C928D7CAE.	huyenpt_ubuntu18	127.0.0.1, 192.168.74.	_ thanhnm18_test	 Offline 	ute(s) 🗸		N/A	
	ddf	root_t			E414646EFAF694E531F810A	thanhnm18-ubuntu18-test	127.0.0.1, 192.168.12	global	 Offline 	minute	:(s) 🗸	N/A	
	fðf	root_t							2 .			N/A	
	im 23	root_t							- /			N/A	
	daily 23	root_t						Canaal				N/A	
	daily 22	root_t						Cancel	Add			N/A	
	im 22	root_t						_				N/A	
	zsdsd	root_t								Cancel	Create	N/A Activate Windows Go to Settings to active	te Windows.
													4

Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều
 Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung Selected > chọn
 Cancel để hủy thao tác thêm Agent để deploy hoặc chọn nút Add để xác nhận danh sách Agent(s):

=	aJiant Investigati	on / Deploy Too	ol									# 0
<u>_</u>	Tool management	Task manaş	Create new task							×		
A	Q Search task		Information			Agents or groups						٩
≂±		_	Please fill out all the in	Add	agent(s)				×	ing of them, click the		
0	Showing 50 of 1664 resul	lt(s)	Task deploy tool Lin	fx	ComputerName ~ "ubu"				8 Q	Edit	Show only my schedule	New task
5-1	Task name	Autho	Description	Select	ted (2)						Upcoming agents	Action
	t276	root_t	About your task	ub	untu × ubuntu18 ×				• ~	Edit	N/A	
~	t275	root_t									N/A	
ž.	task mac	root_t		10 res	ult(s)						N/A	
	Task 888868	root_t	1	•	Agent ID	Computer name	IP Address	Group	Status	Edit	N/A	
à	t274	root_t	Tool to deploy		27CFD9DA7A0394EA7CC955	ubuntu	127.0.0.1, 192.168.12.	_ global	 Offline 		N/A	
ē.	t273	root_t	Tool OutputFolder_L		2F1EB4A7D7FD84483EC743	ubuntu-2004	127.0.0.1, 10.0.2.15, 1.	anhnn_test	 Online 		N/A	
	retry 8	root_t	Tool parameters (onti		60AA2618E17825BADCD191	ubuntu18	127.0.0.1, 192.168.25.	. group_ubuntu	 Offline 		N/A	
_	t272	root_t	Toor parameters (oper		A303D982A258A6328267D0	ubuntu	127.0.0.1, 192.168.74.	anhnn_test	Offline		N/A	
	retry 6	root_t	Parameters for this		BB5933621EB880749E6AA6	ubuntu18	127.0.0.1, 192.168.74.	_ thanhnm18_test	 Offline 		N/A	
	Task agent abcds	root_t	Tool output		BE56627FA3FEE2B1ECBBE5	bichpt3-ubuntu	127.0.0.1, 192.168.25.	. group_ubuntu	Offline		N/A	
_	task fff	root_t	Folder 🗸		C68C5DFCFA883C928D7CAE.	huyenpt_ubuntu18	127.0.0.1, 192.168.74.	thanhnm18_test	 Offline 	ute(s) V	N/A	
_	ddf	root_t			E414646EFAF694E531F810A	thanhnm18-ubuntu18-test	127.0.0.1, 192.168.12.	. global	 Offline 	minute(s) ~	N/A	
	fðf	root_t									N/A	
	im 23	root_t						× •	, ,		N/A	
	daily 23	root_t							2		N/A	
	daily 22	root_t						Cancel	Add		N/A	
	im 22	root_t									N/A	
	zsdsd	root_t								Cancel	N/A Activate Windows Go to Settings to activate	
												4

Viettel Cyber Security



Hover vào các Agent(s) đã chọn > Chọn icon dể để thực hiện loại
 bỏ Agent(s) khỏi danh sách đã chọn:



Chọn Cancel để hủy hoặc chọn Save để lưu thông tin các Agent(s)
 đã chọn để deploy:

\equiv	aJiant Investigation / D	eploy To	ol											* 0
Ţ.	Tool management Task	c manaç	Create new task									×		
▲ _{F±}	Q Search task		Information Please fill out all the information	of this task.		Agent Setting respec	ts or groups gs for assignees an tive buttons to edit	d triggering for	this task are set by	/ default. To	change anything of them, click th	e		Q
•	Showing 50 of 1664 result(s)		Task deploy tool Linux			Selecto Choos	ed agents or group	s (<i>S)</i>			Edit		Show only my schedule	O New task
.⊥ Vi	Task name 1276 1275 task mac	Authorization Au	Description About your task	Edit assignees All agents (total 50 Choose agent(s) or 	agents) group(s)					×	Edit]	Upcoming agents N/A N/A N/A	Action
r A	Task 888868 t274 t273	root_t root_t root_t	Tool to deploy	2 agent(s) Agent ID	Computer r	name	IP Address	Add agent/gro Group	Import from Status	n list▼ Action	Edit		N/A N/A N/A	
	retry 8 t272 retry 6	root_t root_t root_t	Tool parameters (optional) Parameters for this tool	056DC579B568 07718463D55E	HuyenPT-W virtual_age	/in10x64 nt_maintn.	192.168.74.128 127.0.0.1, 172.1	edr_team maitest	Offline Offline	•			N/A N/A N/A	
	Task agent abcds task fff ddf	root_t	Folder V Test						Cancel	Save	minute(s) ~ er: 30 minute(s) ~		N/A N/A N/A	
	im 23 daily 23	root_t											N/A N/A	
	daily 22 im 22 zsdsd	root_t root_t									Cancel Cre		N/A N/A N/A	
			_										Go to Settings to activate	

+ Chọn Add group(s):

Viettel Cyber Security



≡	aJiant Investigation / Dep	Tool		* 0
<u> </u>	Tool management Task m	Create new task	×	
▲ ^{pH} ⊙	Shewing 50 of 1664 result(s) Task name 1275 12	Information Please fill out all the information of this task. Task mee Task deploy tool Linux Description About your task Edit accimpage	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups Edit Choose agent(s) or group(s) Edit Number of agent(s) run in each time Edit	Show only my schedule Typeoming agents Action N/A NA
×# 🔂 💀	task mac a Task 88868 a t274 a t273 a retry 8 a t272 a retry 6 a task agent abcds a	Tool to deploy Tool outputFolder_Linux_Pars Tool outputFolder_Linux_Pars Tool outputFolder_Linux_Pars Tool output Parameters (optional) Parameters for this tool Tool output Folder V Tex	Is So agents) (s) or group(s) Information of selected Add agent(s) Cancel Sove minute(s) ~	NA N/A N/A N/A N/A N/A N/A N/A
	daf f fdf e im 23 o daily 23 e im 22 e zadad e		Cancel the task if the tool can not return output report from agent after: 30 minute(s) Cancel Cancel	N/A N/A N/A N/A N/A N/A N/A Activate: Windows So to settings to activate Windows

• Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:

\equiv	aJiant Investiga	tion / Deploy To	ol								# 0
<u>h</u>	Tool management	Task manaç	Create new task	Add group(s)		×	1	×		
A	Q Search task		Information	Qt			8 Q				Q
"≟			Please fill out all the infon Task name	NOTE: In this in	iterface, users belonging to the parent	t group have full control over all the child group	ps of their parent gr See more >>	2 mything of them	, click the		
0	Showing 50 of 1664 res	ult(s)	Task deploy tool Linux	Gr	oup	Location	Action		Edit	Show only my schedule	New task
D -1	Task name	Authc	Description	🗆 👷 TE	NANT_viettel.com.vn					Upcoming agents	Action
	t276	root_t	About your task	🗆 💑 ani	hnn_test	admin			Edit	N/A	
	t275	root_t		🗆 🖧 cn	ctest	TENANT_nsm.com/anhvn				N/A	
×.	task mac	root_t		🗆 🖧 de	fault					N/A	
	Task 888868	root_t		🗆 💑 ed	r_team	viettel/khoi_phu_thuoc/vcs_anm			Edit	N/A	
ΕÅ	t274	root_t	Tool to deploy			I4 < 1	2 3 4 5 ≻ ▶	ed time		N/A	
٢	t273	root_t	Tool OutputFolder_Linu:			-				N/A	
	retry 8	root_t	Tool parameters (optiona	Selected						N/A	
	t272	root_t		No group(s)						N/A	
	retry 6	root_t	Parameters for this too	Group	Location		Action			N/A	
	Task agent abcds	root_t	Tool output							N/A	
	task fff	root_t	Folder 🗸 T					minute(s) 🗸		N/A	
	ddf	root_t				\mathbf{X}		0 minut	e(s) 🗸	N/A	
	fðf	root_t				\sim				N/A	
	im 23	root_t				NO DATA TO SHOW				N/A	
	daily 23	root_t								N/A	
	daily 22	root_t								N/A	
	im 22	root_t								N/A	
	zsdsd	root_t					Cancel Save	Cancel		N/A Activate Windows	

 Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung Selected > chọn Cancel để hủy thao tác thêm group(s) để deploy hoặc chọn nút Save để xác nhận danh sách group(s):

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



≡	aJiant Investigation / Deploy T	ool		# 0
(**) 	Tool management Task management	Create new task	Add group(s) X X	
▲ "±	Q Search task	Information Please fill out all the infor Task name	Q t Q Q NOTE in this interface, uses belonging to the parent group have full control over all the child groups of their parent grup. Sea more are nything of them, click the	<u>م</u>
0	Showing 50 of 1664 result(s)	Task deploy tool Linux	Group Location Action	Show only my schedule • New task
	Task name Author 1276 root_J 1275 root_J 1276 root_J Task 88866 root_J 1274 root_J 1273 root_J	Description About your task Tool to deploy	0 0 12 0 MM - finite.com/ min 0 </th <th>Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/A</th>	Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/A
ş	retry 8 root_1 1272 root_1 retry 6 root_1 Task agent abcds root_1	Tool Output voter_Linu Tool parameters (optiona Parameters for this too Tool output	Selected 2 group(s) Group Location Action Contest TENANT_nsm.com/anlwn	N/A N/A N/A
	task fff root.d ddf root.d fdf root.d im 23 root.d daily 23 root.d daily 22 root.d	Folder V		N/A N/A N/A N/A N/A
	root_1		Cancel Seve Cancel Create	N/A Activate Windows Go to Settings to activate Windows

Hover vào các group(s) đã chọn > Chọn icon dể thực hiện loại
 bỏ group(s) khỏi danh sách đã chọn

≡	aJiant Investigation / De	eploy To	ol							* 0
<u>_</u>	Tool management Task	: manaç	Create new task					×		
▲ 1 ^{,14}	Q Search task Showing 50 of 1664 result(s)	I	Information Please fill out all the information Task name Task deploy tool Linux	of this task.	Agents or groups Settings for assignees and triggering respective buttons to edit. Selected agents or groups Choose agent(c) or groups	for this task are set by default. To a	change anything of them, click t	the	Show only my schedule	Rew task
).	Task name	Authc	Description	Edit assignees		×			Upcoming agents	Action
₩	t276 t275 task mac	root_t root_t root_t	About your task	 All agents (total 50 agents) Choose agent(s) or group(s) 	Add agent.	/group Import from list▼	Edit		N/A N/A N/A	
Ē	1274	root_t	Tool to deploy	3 group(s)			Edit		N/A	
ø	t273	root_t	Tool OutputFolder_Linux_Para	Group	Location N/A	Action	N/A		N/A	
	+272	root_t	Tool parameters (optional)	🖧 congnc	TENANT_edr.com				N/A	
	retry 6	root_t	Parameters for this tool	🖧 default	N/A				N/A	
	Task agent abcds	root_t	Tool output			< 1 >			N/A	
	task fff	root_t	Folder 🗸 Test				minute(s) V		N/A	
	ddf	root_t				Cancel Save	er: 30 minute(s) ~		N/A	
	fdf	root_t							N/A	
	im 23	root_t							N/A	
	daily 23	root_t							N/A	
	daily 22	root_t							N/A	
	im 22	root_t							N/A	
	zsdsd	root_t	_				Cancel	reate	Activate Windows Go to Settings to activate	Milleovie top

 Chọn Cancel để hủy hoặc Chọn Save các group(s) đã chọn để deploy:



Tool management	Task manag	Create new task					×		
Q Search task Showing 50 of 1664 result	(s)	Information Please fill out all the information Task name Task deploy tool Linux	of this task.	Agents or groups Settings for assignees and triggerin respective buttons to edit. Selected agents or groups	ig for this task are set by default. T	o change anything of them,	click the Edit	Show only my schedule	New ta
Task name	Authc	Description	Edit assignees		×			Upcoming agents	Actio
t276 t275 task mac	root_t root_t root_t	About your task	 All agents (total 50 agents) Choose agent(s) or group(s) 	Add agen	Ngroup Import from list	(Edit	N/A N/A N/A	
Task 888868	root_t	Tool to deploy	3 group(s)				Edit	N/A	
+272	root t		Group	Location	Action	Expired time		N/A	
1273	root	Tool OutputFolder_Linux_Para	TENANT_nsm.com	N/A	۵.	N/A		N/A	
1070	TOOL	Tool parameters (optional)	🛃 congnc	TENANT_edr.com				N/A	
1272	root	Parameters for this tool	🛃 default	N/A				N/A	
Task agent abode	root t	Tool output			 1 			N/A	
task fff	root t					minute(s) 🗸		N/A	
ddf	root t	Polder V Test			Cancel	m 20 minute	(0) + 4	N/A	
fdf	root t					a. 30 minute	(5)	N/A	
im 23	root_t							N/A	
daily 23	root_t							N/A	
daily 22	root_t							N/A	
im 22	root_t							N/A	
zsdsd	root_t					Canaal	Create	N/A	
						Cancel	Create		

+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn Import from list

- Chọn **Download sample file** để lấy form danh sách file agent(s) mẫu;
- Nhập thông tin agent(s) > chọn Import from .CSV để thực hiện tải lên

danh sách agent(s)

International data in the internation of the task. International data in the internation of the task. International data in the internation of the task. International data internation of the task. Internation of the internation	≡	viettel aJiant Investigation / Deploy To	0	* 0
 Control totals Control totals<td></td><td>Tool management Task manag</td><td>Create new task X</td><td></td>		Tool management Task manag	Create new task X	
daily 22 rot1 N/A im 22 rot1 NA zsdrd rot1 Cancel Centerl N/A	🔺 1 ^H 🧿 I 🕑 🧍 🔂	Task name Aufter 1275 1004.1 1275 1004.1 1275 1004.1 1275 1004.1 1274 1004.1 1273 1004.1 1273 1004.1 1273 1004.1 1273 1004.1 1273 1004.1 1271 1004.1 1272 1004.1 1271 1004.1 1272 1004.1 1273 1004.1 1274 1004.1 1275 1004.1 1272 1004.1 1273 1004.1 1274 1004.1 1275 1004.1 1272 1004.1 1284 agent abcds 1004.1 1294 1004.1 1294 1004.1 1294 1004.1 1294 1004.1 1294 1004.1 1294 1004.1 1294 1004.1	Information Take affel out lative Tak deploy tool Linux Tak deploy tool Linux Description Address of genetic of group(s) Choice agent(s) of group(s) Description Address of genetic of group(s) Choice agent(s) of group(s) Description Address of genetic of group(s) Choice agent(s) of group(s) Choice agent(s) or group(s) Choice agent (s) or group(s) <td>Show only my schedule Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/</td>	Show only my schedule Upcoming agents Action N/A N/A N/A N/A N/A N/A N/A N/
Go to Settings to		im 22 root_ zsdsd root_1	Cancel Create	N/A Activate Windows Go to Settings to activate Windows

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Bước 13: Cấu hình số lượng agent deploy tool mỗi lần:

+ All Agent: Cho phép deploy toàn bộ agent(s) người dùng đã chọn



+ Cấu hình số lượng agent mỗi lần deploy:

aJiant	on / Deploy Too		
Tool management	Task manaç	Create new task	×
Q Search task		Information Agents or groups Please fill out all the information of this task. Settings for assignees and triggering for this task are set by default. To change respective buttons to edit. Task name Task name	ge anything of them, click the
Showing 50 of 1664 resul	lt(s)	Task deploy tool Linux Choose agent(s) or groups Choose agent(s) or group(s)	Edit Show only my schedule
Task name	Autho	Description	Upcoming agents
t276	root_t	About your task Number of agent(s) run in each time	Edit N/A
t275	root_t	All selected agent(s)	N/A
task mac	root_t	Edit number of agente	N/A
Task 888868	root_t		Edit N/A
t274	root_t	Tool to deploy Choose number of agents you want to run in each time:	xpired time N/A
t273	root_t	Tool OutputFolder_Linux_Params ask is cre N	I/A N/A
retry 8	root_t	2 9 9 agent(s) every 3 hour(s) ✓ until finished	N/A
t272	root_t		N/A
retry 6	root_t	Parameters for this tool Save	N/A
Task agent abcds	root_t	Tool output	N/A
task fff	root_t	Folder V Test 0 1 time(s) within 3 hour(s) V every 30	minute(s) V N/A
ddf	root_t	Cancel the task if the tool can not return output report from agent after:	30 minute(s) ~ N/A
fðf	root_t		N/A
im 23	root_t		N/A
daily 23	root_t		N/A
daily 22	root_t		N/A
im 22	root_t		N/A
zsdsd	root_t		Cancel Create N/A
			Activate Windows

Bước 14: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



+ Chọn **Run immediately** để thực hiện cấu hình thời gian deploy tool **ngay lập tức** (sau khi tạo task thành công)

	aJiant Investigation / C	Deploy To	ol			÷ 0
<u>r</u>	Tool management Tas	ik manaç	Create new task		×	
 ↓[#] Ø I 	Q Search task Showing 50 of 1664 result(s) Task name 1276 1275	Authe root_t	Information Please fill out all the information of this task. Task name Task deploy tool Linux Description About your task		Agents or groups Settings for assignees and tiggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups Choose agent(s) or group(s) Number of agent(s) run in each time All selected agent(s)	Show only my schedule Upcoming agents Action N/A St/A
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	task mac Task 88808 1274 1273 retry 8 1272 retry 6 Task sgent abcds task fff	t_toon t_toon t_toon t_toon t_toon t_toon t_toon t_toon	Tool to deploy Tool OutputFolder_Linux_Params Tool parameters (optional) Parameters for this tool Tool output Polder Test	Edit trigger When this task is creat	d: Expired time ask is cre_ N/A Cancel Swy 1 time(s) within 3 hour(s) ~ every 30 minute(s) ~	N/A N/A N/A N/A N/A N/A N/A
	ddf fdf im 23 daily 23 daily 22 im 22 zodsd	t_toon t_toon t_toon t_toon t_toon t_toon t_toon			Cancel the task if the tool can not return output report from agent after: 30 minute(s) v Cancel Cancel	N/A N/A N/A N/A N/A N/A Activate Windows Co to Settings to activate Windows

+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo lập lịch:

- Chọn schedule One time:
 - Cho phép lập lịch deploy tool một lần;
 - Cấu hình thời gian bắt đầu:

Tool management Ta	sk manaç	Create new task			>	<	
Q Search task		Information Please fill out all the information of this tas Task name	ik.	Agents or groups Settings for assignees and triggering for this task are set by respective buttons to edit.	default. To change anything of them, click the		
Showing 50 of 1664 result(s)		Task deploy tool Linux		Selected agents or groups	Edit	Show only my schedule	O New ta
Task name	Autho	Description		choose agent(s) or group(s)		Upcoming agents	Acti
t276	root_t	About your task		Number of scant/e) run in each time	Edit	N/A	
t275	root_t		Edit trigger	×		N/A	
task mac	t_toor		When this task is created	t.	1	N/A	
Task 888868	root_t		2 Run immediately		Edit	N/A	
1274	root_t	Tool to deploy	Ruir on a schedule	U	Expired time	N/A	
1273	root_t	Tool OutputFolder_Linux_Params	One time	~	ask is creN/A	N/A	
retry 8	root_t	Tool parameters (optional)	Start time			N/A	
t272	root_t		15/12/2022 - 00:00	:00 🖬		N/A	
retry 6	root_t	Parameters for this tool	L			N/A	
Task agent abcds	t_toor	Tool output				N/A	
task fff	root_t	Folder 🗸 Test		Cancel Save	ery 30 minute(s) ~	N/A	
ddf	root_t			Cancel the task if the tool can not return output report f	rom agent after: 30 minute(s) ~	N/A	
fðf	root_t					N/A	
im 23	root_t					N/A	
daily 23	root					N/A	
daily 22	root					N/A	
im 22	root					N/A	
zsdad	root_t				Cancel	N/A Activate Windows	Otron

Viettel Cyber Security



- Chọn schedule **Daily**:
 - Cho phép lập lịch deploy tool hàng ngày;
 - o Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:

aJiant Investiga	ation / Deploy To	ol				* 0
Tool management	Task manaç	Create new task				×
Q Search tank Showing 50 of 1664 res	sulti(s)	Information Please fill out all the information of this Task name	task.	Agents or groups Settings for assignees and triggering for this task are se respective buttons to edit. Selected agents or groups	et by default. To change anything of them, click t	he Shrw oply my schedule A New Last
Task name	Autho	Task deploy tool Linux Description	Edit trigger		×	Upcoming agents Action
	t_toor t_toor t_toor	About your task	When this task is creat Run immediately Run on a schedule	ed:		N/A N/A N/A
Task 888868	Lioon	Tool to deploy	Recur	4	Expired time	N/A N/A
e 12/3 retry 8 1272	Loon Loon Loon	Tool OutputFolder_Linux_Params Tool parameters (optional) Parameters for this tool	Start time	00:00 t	askis cre_ N/A	N/A N/A N/A
Task agent abcds task fff	root_t	Tool output	Expire in	15/12/2022-00:00:00	ery 30 minute(s) ~	N/A N/A
ddf fdf im 23	root_t root_t root_t			Cancel Sav	agent after: 30 minute(s) ~	N/A N/A
daily 23 daily 22	roor_t					N/A N/A
im 22 zsdsd	root_t				Cancel	eute N/A Activate Windows
25USU C	100(_1	_	_		Cancel	Activate Windows Go to Settings to activate Window

- Chọn schedule **Weekly**:
 - Cho phép lập lịch deploy tool hàng tuần;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:



≡	aJiant Investigation / Dep	yy Tool	* 0
	Tool management Task m	Treate new task	
A	Q Search task	Information Agents or groups	Q
Р		Please fill out all the information of this task. Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit.	
0	Showing 50 of 1664 result(s)	Task deploy tool Linux Edit trigger X	Show only my schedule • New task
)-	Task name A	the Description When this task is created:	Upcoming agents Action
	t276 r	About your task O Run immediately	N/A
	t275 n	ot_t	N/A
×.	task mac n	ot Weekly	N/A
	Task 888868 n	Edit	N/A
Ε <u>λ</u>	1274 n	Tool to deploy Recur this task every 1 deveck(s) on:	N/A
ø	t273 r	ot.1 Tool OutputFolder_Linux_Params	N/A
	retry 8 re	Tool parameters (optional)	N/A
	t272 n	otul Start time	N/A
	retry 6 n	Parameters for this tool 15/12/2022 - 00:00:00	N/A
	Task agent abcds	Tool output	N/A
	task fff n	of J Folder V Test	N/A
	ddf r	otagent after: 30 minute(s) ~	N/A
	fðf n	Cancel Save	N/A
	im 23 n		N/A
	daily 23 r		N/A
	daily 22 r	au	N/A
	im 22 n	ou	N/A
	zsdsd n	Cancel Create	N/A
			Go to Settings to activate Windows
			4

- Chọn schedule Monthly:
 - Cho phép lập lịch deploy tool hàng tháng;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:

	Task midhaç	Create new task					×	
Q Search task		Information		Agents or groups				
		Please fill out all the information of this t	ask.	Settings for assignees and triggering for t	this task are set by de	fault. To change anything of them, click the		
		Task name	Edit trigger		×			
Showing 50 of 1664 result	(s)	Task deploy tool Linux	When this task is creat	ted		Edit	Show only my schedule	New
Task name	Autho	Description	 Run immediately 				Upcoming agents	Acti
1276	root t	About your took	2 💿 Run on a schedule	e .		Edit	N/A	
t275	root_t		Monthly			Lon	N/A	
task mac	root_t		Recur				N/A	
Task 888868	root_t		Recur this task in t	hese months:		Edit	N/A	
t274	root_t	Tool to deploy	4 Ma	X October X	0 ¥	Expired time	N/A	
t273	root_t	Tool OutputFolder_Linux_Params	at these days:			ask is cre N/A	N/A	
retry 8	root_t	Tool parameters (ontional)	at triese days.		5		N/A	
t272	root_t		9 × 10 × 16	× 30 × Last day of month ×	° ~		N/A	
retry 6	root_t	Parameters for this tool	Start time				N/A	
Task agent abcds	root_t	Tool output	15/12/2022 - 00:	:00:00	6 団		N/A	
task fff	root_t	Folder 🗸 Test			-	very 30 minute(s) V	N/A	
ddf	root_t		Expire in	15/12/2022 - 00:00:00		magent after: 30 minute(s) ~	N/A	
fðf	root_t				8		N/A	
im 23	root_t			Ca	ncel Save		N/A	
daily 23	root_t				_		N/A	
daily 22	root_t						N/A	
im 22	root_t						N/A	
zsdsd	root_t					Cancel Creat	te Activato Minda	

Viettel Cyber Security



Bước 15: Cấu hình thông tin nâng cao cho task

+ **Delete tool after run tool** cho phép xóa tool output sau khi run tool và trả kết quả về BE thành công;

+ If the task failed to run, retry upto khi task deploy thất bại,cho phép cấu hình thông tin retry task (deploy lại task)

≡	aJiant Investigation / Deploy 1	001		* 0
	Tool management Task mana	Create new task	×	
▲ 1-1 0 V	Search task. Showing 50 of 1664 result(s) Task name Auth t276 root. t275 root. task mac root. Task 88868 root. t274 root.	Information Please fill out all the information of this task. Task name Task deploy tool Linux Description About your task Tool to deploy	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttoms to exit. Selected agents or groups Edit All agents (otal 50 agents) Edit All egents (otal 50 agents) Edit All egents (otal 50 agents) Edit Trigger Edit Trigger Edit	Q Show only my schedule Q N/A N/A N/A N/A N/A N/A N/A N/A
Q	1273 root. refty 8 root. 1272 root. refty 6 root. refty 6 root. task agent abcds root. ddf root. ddf root. idf root. daily 23 root. im 22 root. im 22 root. zidsd root.	Tool OutputFolder_Linux_Params Tool parameters (optional) Parameters for this tool Tool output Folder Test	On day(s) 9, 10, 16, 30 and last day of May 15/12/2022 15:00:00 23/12/2022 00:00:00 Advanced 9 Delete output after run tool 1 time(s) within 3 hour(s) v every 30 minute(s) v 2 Cancel the task if the tool can not return output report from agent after: 30 minute(s) v Cancel the task if the tool can not return output report from agent after: 30 minute(s) v	NA NA NA NA NA NA NA NA NA NA NA NA

+ Cancel the task if the tool can not return output report from agent after cho phép hủy task nếu task không thể chạy sau thời gian cấu hình của người dùng:



aJiant Investigation	n / Deploy Too			\$
Tool management	Task manaç	Create new task	×	
Q Search task		Information Please fill out all the information of this task.	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the resence huttrops to ordi	
Showing 50 of 1664 result	(s)	Task name Task deploy tool Linux	Selected agents or groups Edit	Show only my schedule
Task name	Autho	Description	Number of agent(s) run in each time	Upcoming agents Action
t275	root_t	Parona your asona.	All selected agent(s)	N/A
Task 888868	root_t	Teal to dealer:	Trigger Edit	N/A
t274 t273	root_t	Tool OutputFolder_Linux_Params	Trigger Start time Expired time On day(s) 9, 10, 16, 30 and last day of May 15/12/2022 15:00:00 23/12/2022 00:00:00	N/A N/A
retry 8 1272	root_t	Tool parameters (optional)	Advanced	N/A N/A
retry 6 Task agent abcds	root_t	Tool output	Denete output after run tool If the task failed to run, retry up to:	N/A N/A
task fff ddf	root_t	Folder V Test	Cancel the task if the tool can not return output report from agent after: Cancel the task if the tool can not return output report from agent after: So minute(s)	N/A N/A
fðf Im 23	root_t			N/A N/A
daily 23 daily 22	root_t			N/A N/A
im 22 zsdsd	root_t		Cancel Crente	N/A N/A
				Go to Settings to activate Mindows

Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

h. Nhân bản task (Duplicate task)

Mục đích: Cho phép nhân bản task (sao chép task), tự động điền các giá trị như task gốc ngoại trừ trường Task name (Yêu cầu người dùng nhập/ sửa lại tên tasks); Các bước thực hiện:

Bước 16: Tại màn hình danh sách tool, hover vào tool cần nhân bản (duplicate)

> chọn 👘 > chọn duplicate this task


	aJiant	eploy Tool								# 0
2	Tool management Task	managemer	nt							
A	Q task									<u>୍</u> ଷ ପ
÷										
9	Showing 50 of 285 result(s)								Show only my schedule	New task
≻-	Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
	Task r7	root_test	15/12/2022 14:46:17	N/A	2	Immediately	N/A	• Finished	N/A	<u> </u>
<i>,</i>	Task r6	root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	 Finished 	N/A View report	
i.	Task r5	root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	• In Progress	N/A View detail	2
	Task f4	root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	 Finished 	N/A Duplicate this t	ask
à	Task r3	root_test	15/12/2022 14:21:01	N/A	2	Immediately	N/A	Finished	N/A	
p	Task r2	root_test	15/12/2022 14:20:29	N/A	2	Immediately	N/A	Finished	N/A	
	Task r1	root_test	15/12/2022 14:12:22	N/A	2	Immediately	N/A	Finished	N/A	
	Task r	root_test	15/12/2022 14:10:12	N/A	2	Immediately	N/A	Finished	N/A	
	Task 8988	root_test	15/12/2022 09:32:14	N/A	1	Immediately	N/A	 Finished 	N/A	
	task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
	Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
	Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	 Stopped 	N/A	
	task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	Finished	N/A	
	Task retry a	root_test	14/12/2022 11:21:36	N/A	1	Immediately	N/A	 Finished 	N/A	
	Task rep dgf	root_test	13/12/2022 18:09:43	N/A	5	Immediately	N/A	Finished	N/A	
	Task 90	root_test	13/12/2022 18:09:21	N/A	5	Immediately	N/A	 Stopped 	N/A	
	Task test report 89	root_test	13/12/2022 18:01:38	N/A	5	Immediately	N/A	Finished	N/A	
	Task test repm 9	root_test	13/12/2022 17:54:48	N/A	5	Immediately	N/A	Finished	N/A	_
									Activate Windows Go to Settings to activate	nindowię top

Bước 17: Nhập thông tin Task name và kiểm tra/ cập nhật thông tin task > Chọn Create để hoàn thiện cấu hình hoặc chọn Cancel để hủy thao tác nhân bản task

≡	aJiant Investigation / Deploy To	lool		* 0
Ţ	Tool management Task manag	Duplicate task	×	
3; 🛥 µ ^H 👩 🗄 💽 🕷 🖆 🗗	Q. task Showing S0 of 285 result(s) Task name Author Task r3 rooL.1 Task r3 rooL.1 Task r2 rooL.1 Task r2 rooL.1	Information Plesse fill out all the information of this task. Task name Task duplicate 1 Description About your task Tool to deploy Tool OutputFolder_Linux_Params Tool parameters (optional)	Agents or groups Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit. Selected agents or groups 2 agent(s) Agent ID Computer name IP Address Group Status Action SA4E6A6001F4 redhat_tester 192.168.6.41,19 maitest225 Online CB03FC002664 centos7_test_hostna 192.168.6.118,1 maitest225 Online Computer name All selected agent(s) run in each time Litter All selected agent(s) Edit Run this task Edit	Show only my schedule New task Upcoming agents Action N/A
	Task r root_t	Parameters for this tool	Trigger Edit	N/A
	Task 8988 root_t task mac root t	Tool output	Trigger Start time Expired time	N/A N/A
	Task 888868 root_t	File V Downloads/test.txt	immediately At the time this task is creN/A	N/A
	Task agent abcds root_t		Advanced	N/A
	task fff root_t		Delete output after run tool	N/A
	Task retry a root_t		If the task failed to run, retry up to:	N/A
	Task rep dgf root_t		1 time(s) within 3 hour(s) \checkmark every 30 minute(s) \checkmark	N/A
	Task 90 root_t		\Box Cancel the task if the tool can not return output report from agent after: 30 minute(s) \sim	N/A
	Task test report 89 root_t			N/A
	Task test repm 9 root_f		Cancel	N/A Activate Windows Go to Settings to activate Reack to top

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



i. Danh sách Upcoming Agents

Mục đích: Cho phép hiển thị danh sách Agents sắp được deploy tool;

Các bước thực hiện: Tại màn hình danh sách task > Chọn Danh sách Upcoming agents.

j. Stop/ Start task

Mục đích: Cho phép Stop/ Restart task (Dừng deploy task hoặc deploy lại task đã tạm dừng).

Các bước thực hiện tạm dừng task: Tại màn hình danh sách task, hover vào task cần tạm dừng > Chọn icon <a>Im để tạm dừng task:

viettel										
aJiant	Investigation / I	Deploy Tool								4
Tool mana	gement Tas	k managemer	nt							
Q task										8
Showing 10	00 of 290 result(s)								Show only my schedule	New task
Task name	e	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task r7		root_test	15/12/2022 14:46:17	N/A	2	Immediately	N/A	Finished	N/A	
Task r6		root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	Finished	N/A	
Task r5		root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	• In Progress	N/A	
Task f4		root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	• Finished	N/A	Stop this task
Task r3		root_test	15/12/2022 14:21:01	N/A	2	Immediately	N/A	• Finished	N/A	
Task r2		root_test	15/12/2022 14:20:29	N/A	2	Immediately	N/A	Finished	N/A	
Task r1		root_test	15/12/2022 14:12:22	N/A	2	Immediately	N/A	Finished	N/A	
Task r		root_test	15/12/2022 14:10:12	N/A	2	Immediately	N/A	Finished	N/A	
Task 8988		root_test	15/12/2022 09:32:14	N/A	1	Immediately	N/A	Finished	N/A	
task mac		root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	 Finished 	N/A	
Task 8888	68	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	 Finished 	N/A	
Task agent	t abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	 Stopped 	N/A	
task fff		root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	 Finished 	N/A	
Task retry	a	root_test	14/12/2022 11:21:36	N/A	1	Immediately	N/A	Finished	N/A	
Task rep d	gf	root_test	13/12/2022 18:09:43	N/A	5	Immediately	N/A	Finished	N/A	
Task 90		root_test	13/12/2022 18:09:21	N/A	5	Immediately	N/A	 Stopped 	N/A	
Task test r	report 89	root_test	13/12/2022 18:01:38	N/A	5	Immediately	N/A	 Finished 	N/A	
Task test r	repm 9	root_test	13/12/2022 17:54:48	N/A	5	Immediately	N/A	 Finished 	N/A	
										Windows to top
										4

Các bước thực hiện deploy lại task (đã tạm dừng – Stopped): Tại màn hình danh sách task, hover vào task cần deploy lại > Chọn icon **b** để deploy lại task:



aJiant	1 / Deploy Tool								*
Tool management	Task managemer	nt							
Q task									8
Showing 100 of 290 result(s)							Show only my schedule	New tas
Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task immediately 989	root_test	07/12/2022 14:49:13	N/A	1	Immediately	N/A	 Stopped 	N/A	
Task 8955455	root_test	07/12/2022 13:55:58	N/A	1	Immediately	N/A	Finished	N/A	
Task Monthly MacOS	root_test	06/12/2022 18:25:02	N/A	1	On day(s) 7, 8, 9, 10, 11, 12, 13, 14, 15, 18 of Nove	07/11/2023 09:00:00	In Progress	N/A	
Task weekly MacOs	root_test	06/12/2022 18:23:59	N/A	1	On Mondays, Tuesdays, Wednesdays, Thursdays,	16/12/2022 09:00:00	In Progress	N/A	
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	1	Every 1 day(s) at 09:00:00	16/12/2022 09:00:00	 In Progress 	N/A	
Task 7647657465	root_test	06/12/2022 17:57:36	N/A	1	Immediately	N/A	Finished	N/A	
new task 8	root_test	06/12/2022 17:56:16	N/A	1	Immediately	N/A	Finished	N/A	
new task 6	root_test	06/12/2022 17:50:15	N/A	1	Immediately	N/A	Finished	N/A	
new task 4	root_test	06/12/2022 17:43:13	N/A	1	Immediately	N/A	Finished	N/A	
Task macosvb 1	root_test	06/12/2022 16:41:35	N/A	1	Immediately	N/A	 Stopped 	N/A	
Task monthly dài	root_test	06/12/2022 15:18:38	N/A	1	On day(s) 7, 8, 9, 10, 11, 12 of December at 09:00:	N/A	 Stopped 	N/A	•
Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	N/A	Finished	N/A	Run this ta
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:0	19/12/2022 12:00:00	• In Progress	N/A	-
Task 787878f	root_test	06/12/2022 11:11:58	N/A	1	Immediately	N/A	Finished	N/A	
New task 1	root_test	06/12/2022 11:11:42	Description	48	Immediately	N/A	Finished	N/A	
Task test retry 132	root_test	06/12/2022 10:49:15	N/A	1	Immediately	N/A	Finished	N/A	
Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	N/A	• Finished	N/A	
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:0	19/12/2022 12:00:00	• In Progress	N/A	
								Activate Windows Go to Settings to activat	G Back to to

k. Chi tiết task (Detail task)

Mục đích: Cho phép xem thông tin chi tiết task;

Các bước thực hiện: Tại màn hình danh sách task, hover vào task cần xem chi tiết > Chọn View detail:

	viettel aJiant	Deploy Tool					View task detail				×
r.	Tool management Ta	sk manageme	ent				General				
	-						Name	Task immediately 989			
A	Q task						Description	N/A			
÷						_	Tool to deploy	Bichpt3_Hello.exe			
	Chowing 100 of 200 result(a)						Parameters	N/A			
9	showing too of 250 result(s)						Output type	none			
	Task name	Author	Created time	Description	Number of agent(s)	Trigger	Output path	N/A			
	Task immediately 989	root_test	07/12/2022 14:49:13	N/A	1	Immediately	Agents & groups				
	Task 8955455	root_test	07/12/2022 13:55:58	N/A	Immediately	Assignees					
÷.	Task Monthly MacOS	root_test	06/12/2022 18:25:02	N/A	1	On day(s) 7, 8, 9, 10, 1	1 agent(s)				
	Task weekly MacOs	root_test	06/12/2022 18:23:59	N/A	1	On Mondays, Tuesday	Agent ID	Computer name	IP Address	Group	Status
2	Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	1	Every 1 day(s) at 09:0	97617AC1A609458E	Maingocwinx64	192.168.74.128	maitest225	Online
តា	Task 7647657465	root_test	06/12/2022 17:57:36	N/A	1	Immediately					< 🔳 >
	new task 8	root_test	06/12/2022 17:56:16	N/A	1	Immediately	Number of agent(a) run	in each time			
	new task 6	root_test	06/12/2022 17:50:15	N/A	1	Immediately	All choosing agent(s)	in each unie			
	new task 4	root_test	06/12/2022 17:43:13	N/A	1	Immediately	Run this task				
	Task macosvb 1	root_test	06/12/2022 16:41:35	N/A	1	Immediately	Tringer				
	Task monthly dài	root_test	06/12/2022 15:18:38	N/A	1	On day(s) 7, 8, 9, 10, 1	ingger				
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	Trigger		Start time	Expired tim	e
	New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednes	Ininediately		At the time this task is c	eated. N/A	
	Task 787878f	root_test	06/12/2022 11:11:58	N/A	1	Immediately	Advance				
	New task 1	root_test	06/12/2022 11:11:42	Description	48	Immediately	Retry	None			
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A	1	Immediately	Timeout	None			
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A	1	Immediately					
	New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednes					
									A G	ctivate Window o to Settings to activ	/S rate Windows.

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



I. Xem báo cáo (View tool result)

Mục đích: Xem kết quả báo cáo deploy tool;

Các bước thực hiện: Tại màn hình danh sách task, hover vào task cần xem chi tiết > Chọn **View report**:

aJiant	t Investigation / D	eploy Tool			View repo	rt - New task 2					لى Downloa	d all outputs 🛛 🗗 Get report	rt
Tool ma	inagement Task	managemer	nt		14/12/2022	- 12:00:00	fx Search by	agent					(
Q task					Total agents Success	51 1	Showing 50 of 51 re	esults					
					12/12/2022	- 12:00:00	Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Actio
Showing	g 100 of 290 result(s)				Total agents	49	97EB9873A6807	Win7x86-A-PC	10.0.2.15	N/A	Failed	Architecture invalided (Tool: :	
					Success	2	A23B7D0C7455D	thanhnm18-test	192.168.121	0	• Failed	Failed to get output(tool outp	P
Task na	ime aakhi MacOr	Author	Created time	Description			97617AC1A6094	Maingocwinx64	192.168.74.1	0	Success	N/A	
Took M	acOC daily 1	root test	06/12/2022 10:23:39	N/A	07/12/2022	- 12:00:00	A86963E7A5830	Win10x64-A-PC	10.0.2.15	0	• Failed	Failed to get output(tool outp	P
Tools 76	47657465	root_test	06/12/2022 18:23:17	N/A	Total agents Success	49	50EF37015E7D1	DSTest-PC	192.168.56.1,	N/A	• Failed	Unknown error	
IBSK /C		root_test	06/12/2022 17:57:56	N/A			524B30C4C568F	EDR-TEST02	192.168.133	N/A	• Failed	Unknown error	
new tas	sk o	root_test	06/12/2022 17:50:16	N/A			056DC579B5681	HuyenPT-Win10x	192.168.74.1	N/A	• Failed	Unknown error	
new tas	ak 0	Toot_test	06/12/2022 17:30:15	N/A			12B680FA5B469	Win7x86	192.168.74.1	N/A	• Failed	Unknown error	
new tas	JK 4	root_test	06/12/2022 17:43:13	N/A			AE36AD62DEA59.	BichPT3	192.168.255	N/A	 Expired 	Task time expired	
Task m	acosvo 1	root_test	06/12/2022 16:41:35	N/A			180A66FD56EDD	DESKTOP-R2GBJ_	192.168.198	N/A	Expired	Task time expired	
Task m	onthiy dai	root_test	06/12/2022 15:18:38	N/A			C81D5366CED36	HuvenPT-Win7x86	192.168.74.1	N/A	 Expired 	Task time expired	
Task ad		root_test	06/12/2022 13:58:21	N/A			1B2D5EC3C7611	HuvenPT-Win7x64	192.168.74.1	N/A	• Expired	Task time expired	
New ta:	SK Z	root_test	06/12/2022 11:14:48	Description			97FA4D29AA9AF	BichPT3 7x86	192 168 255	N/A	Expired	Task time expired	
Task /a	18/8/8	root_test	06/12/2022 11:11:58	N/A			A855552ED3C7E	thanhnm18.w10x	102 168 121	N/A	Expired	Task time expired	
New ta:	sk 1	root_test	06/12/2022 11:11:42	Description			5059670844535	HusenDT-Win10x	102 168 74 1	N/A	• Expired	Task time expired	
Task te	st retry 132	root_test	06/12/2022 10:49:15	N/A			501 007 00 A4231	Richard Min107.	102 168 255	11/15	• Expired	Task time expired	
Task at	WIND	root_test	06/12/2022 13:58:21	N/A			P2440178E0709	bionpio_Wintore_	192.100.200	10/15	- Copied	Task time expliced	
New ta:	SK 2	root_test	06/12/2022 11:14:48	Description			3C7764CA3D8D8	Dau-Pu	10.0.2.15	N/A	• cxpired	rask ume expired	
Task 78	378781	root_test	06/12/2022 11:11:58	N/A			EA4B8A259CC45	x64_ptbich	192.168.255	N/A	Expired	Task time expired	
New ta:	sk 1	root_test	06/12/2022 11:11:42	Description			AC736D6DD5A3	Win10x86	192.168.74.1	N/A	 Expired 	Task time expired	
Task te	st retry 132	root_test	06/12/2022 10:49:15	N/A			E1A2D22E765E5	thanhnm18-test-7_	192.168.121	N/A	 Expired 	Task time expired	
							EF0C1A62F117F	thanhnm18-w7x64	192.168.121	N/A	ExpiredActive	Task time expired	

- + Tìm kiếm kết quả deploy tool theo các câu lệnh truy vấn:
 - Mục đích: Cho phép tìm kiếm kết quả deploy tool theo câu lệnh truy

vấn;

 Các bước thực hiện: Nhập vào câu lệnh truy vấn tìm kiếm > tích chọn nút Search hoặc kết thúc nhập từ khóa > nhấn enter. HT thực hiện tìm kiếm thông tin kết quả liên quan đến từ khóa tìm kiếm có trong hệ thống



≡	aJiant Investigation	1 / Deploy Tool			View repo	rt - New 1	task 2					Downloa 🕁	d all outputs	Get report	i X
Ţ,	Tool management	Task manageme	nt		14/12/2022	- 12:00:00		fx ComputerNa	me ~ "mai"					-0-	2 2 2
A	Q task				Success	1		Showing 12 of 12 r	esults						
5 <u>+</u>	Showing 100 of 290 result(s	s)			12/12/2022	- 12:00:00		Agent ID 8E03ADB705FF8	Computer name virtual_agent_mai	IP Address 172.17.0.2	Tool exit code	Status • Failed	Message Platform inva	alided (Tool: wind	Action d.
Q					Success	2		A6ED648CC1C17	virtual_agent_mai	172.17.0.5	N/A	Failed	Platform inva	alided (Tool: wine	1.
D-	Task name	Author	Created time	Description				AA037D044FF8C	virtual_agent_mai	172.17.0.11	N/A	• Falleu	Platforminva	anded (100). White	
	Task Weekly MdcUs	TOOLLIEST	06/12/2022 18:23:39	N/A	07/12/2022	- 12:00:00		210352BC56C0B	macOS-Mais-Mac	192.168.74.1	N/A	 Failed 	Platform inva	alided (Tool: wind	1
Ť	Task MacOS daily I	root_test	06/12/2022 18:23:17	N/A	Total agents	49		71BC4C742BB32	virtual_agent_mai	172.17.0.4	N/A	 Failed 	Platform inva	alided (Tool: wind	1
	Task /04/05/405	root_test	06/12/2022 17:57:36	N/A	0000000	0		E450A71CC08FD	virtual_agent_mai	172.17.0.3	N/A	 Failed 	Platform inva	alided (Tool: wind	£
<u>_</u>	new task 8	root_test	06/12/2022 17:56:16	N/A				3CAD1ACA8489	virtual_agent_mai	172.17.0.7	N/A	 Failed 	Platform inva	alided (Tool: wind	1
Ľà	new task 6	root_test	06/12/2022 17:50:15	N/A				07718463D55E5	virtual_agent_mai	172.17.0.10	N/A	 Failed 	Platform inva	alided (Tool: wind	1
ø	new task 4	new task 4 root_test 06/12/2022 17:43:13 N/A						6C648D7431177	virtual_agent_mai	172.17.0.9	N/A	 Failed 	Platform inva	alided (Tool: wind	3.
	Task macosvb 1	root_test	06/12/2022 16:41:35	N/A				556075243054B	virtual_agent_mai.	2.17.0.8	N/A	 Failed 	Platform inva	alided (Tool: wind	d.
	Task monthly dài	root_test	06/12/2022 15:18:38	N/A				6DBE442BB0298	virtual_agent_mai_	172.17.0.6	N/A	 Failed 	Platform inva	alided (Tool: wind	d.
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A				97617AC1A6094	Maingocwinx64	192.168.74.1	0	Success	N/A		
	New task 2	root_test	06/12/2022 11:14:48	Description											
	Task 787878f	root_test	06/12/2022 11:11:58	N/A											
	New task 1	root_test	06/12/2022 11:11:42	Description											
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A											
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A											
	New task 2	root_test	06/12/2022 11:14:48	Description											
	Task 787878f	root_test	06/12/2022 11:11:58	N/A											
	New task 1	root_test	06/12/2022 11:11:42	Description											
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A											
												Acti Go to	vate Windo Settings to ac	OWS tivate Windows	
								A The tool results is	going to be deleted auto	matically after 2 m	onths for saving reso	ources		O B	1 00

- + Tải xuống toàn bộ kết quả deploy tool (theo lập lịch task):
 - Mục đích: Cho phép tải xuống toàn bộ kết quả deploy tool (theo lập lịch

task);

• Các bước thực hiện: Tại màn hình View report, chọn nút Download all

output

≡	aJiant Investigation	/ Deploy Tool			View repo	ort - New t	ask 2					Downlos 🕁	ad all outputs 🕞 Get repo	art X
, L	Tool management T	ask manageme	nt		14/12/2022	- 12:00:00	•••	fx ComputerNa	me ~ "mai"					0 Q
A	Q task				Success	1		Showing 12 of 12 r	esults					
۴t					10/10/0000	10.00.00		Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
	Showing 100 of 290 result(s	5)			Tatal agente	- 12:00:00		8E03ADB705FF8	virtual_agent_mai.	. 172.17.0.2	N/A	 Failed 	Platform invalided (Tool: wi	nd.
					Success	2		A6ED648CC1C17	virtual_agent_mai.	. 172.17.0.5	N/A	 Failed 	Platform invalided (Tool: wi	nd.
<u>6-</u>	Task name	Author	Created time	Description				AA657D644FF8C	virtual_agent_mai.	. 172.17.0.11	N/A	 Failed 	Platform invalided (Tool: wi	nd.
_	Task weekly MacOs	root_test	06/12/2022 18:23:59	N/A	07/12/2022	- 12:00:00		210352BC56C0B	macOS-Mais-Mac.	. 192.168.74.1.	N/A	Failed	Platform invalided (Tool: wi	nd.
◙	Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	Total agents	49		71BC4C742BB32	virtual_agent_mai.	. 172.17.0.4	N/A	Failed	Platform invalided (Tool: wi	nd.
秦	Task 7647657465	root_test	06/12/2022 17:57:36	N/A	Success	0		E450A71CC08FD	virtual_agent_mai.	. 172.17.0.3	N/A	• Failed	Platform invalided (Tool: wi	nd.
~	new task 8	root_test	06/12/2022 17:56:16	N/A				3CAD1ACA8489	virtual_agent_mai.	. 172.17.0.7	N/A	• Failed	Platform invalided (Tool: wi	nd.
Ē	new task 6	N/A				07718463D55E5	virtual_agent_mai.	172.17.0.10	N/A	• Failed	Platform invalided (Tool: wi	nd.		
Ø	new task 4	N/A				6C648D7431177	virtual_agent_mai.	. 172.17.0.9	N/A	• Failed	Platform invalided (Tool: wi	nd.		
-	Task macosvb 1	root_test	06/12/2022 16:41:35	N/A				556075243054B	virtual_agent_mai.	2.17.0.8	N/A	• Failed	Platform invalided (Tool: wi	nd.
	Task monthly dài	root_test	06/12/2022 15:18:38	N/A				6DBE442BB0298	virtual_agent_mai.	. 172.17.0.6	N/A	• Failed	Platform invalided (Tool: wi	ind.
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A				97617AC1A6094	Maingocwinx64	192.168.74.1.	0	 Success 	N/A	
	New task 2	root_test	06/12/2022 11:14:48	Description										
	Task 787878f	root_test	06/12/2022 11:11:58	N/A										
	New task 1	root_test	06/12/2022 11:11:42	Description										
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A										
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A										
	New task 2	root_test	06/12/2022 11:14:48	Description										
	Task 787878f	root_test	06/12/2022 11:11:58	N/A										
	New task 1 root_test 06/12/2022 11:11:42 Description													
	Task test retry 132 root_test 06/12/2022 10:49:15 N/A													
										Acti Go tr	ivate Windows o Settings to activate Window	15		
								A The tool results is	going to be deleted auto	matically after 2 m	onths for saving reso	urces	6	м _{гор}

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- + Get all report:
 - Mục đích: Cho phép download tất cả danh sách báo cáo kết quả deploy

tool.

• Các bước thực hiện: Tại màn hình View report, chọn nút Get report:

≡	aJiant Investigation	n / Deploy Tool			View repo	rt - New 1	task 2					Downloa 🕁	ad all outputs 🕞 Get rep	ort X
Ţ.	Tool management	Task manageme	nt		14/12/2022	- 12:00:00		fx ComputerNa	me ~ "mai"					8 Q
A	Q task				Success	1		Showing 12 of 12 n	esults		-			
۲ţ					12/12/2022	- 12:00:00		Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
ົ	Showing 100 of 290 result(s	s)			Total agents	49		8E03ADB705FF8	virtual_agent_mai_	. 172.17.0.2	N/A	 Failed 	Platform invalided (Tool: w	.nd.
					Success	2		A6ED648CC1C17	. virtual_agent_mai	. 172.17.0.5	N/A	 Failed 	Platform invalided (Tool: w	.nd.
)-	Task name	Author	Created time	Description				AA657D644FF8C	virtual_agent_mai_	. 172.17.0.11	N/A	 Failed 	Platform invalided (Tool: w	ind.
	Task weekly MacOs	root_test	06/12/2022 18:23:59	N/A	07/12/2022	- 12:00:00		210352BC56C0B	macOS-Mais-Mac.	. 192.168.74.1.	N/A	 Failed 	Platform invalided (Tool: w	ind.
~	Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	Total agents	49		71BC4C742BB32	virtual_agent_mai_	172.17.0.4	N/A	 Failed 	Platform invalided (Tool: w	ind.
兼	Task 7647657465	root_test	06/12/2022 17:57:36	N/A	Success	0		E450A71CC08FD	virtual_agent_mai_	172.17.0.3	N/A	 Failed 	Platform invalided (Tool: w	ind.
	new task 8	root_test	06/12/2022 17:56:16	N/A				3CAD1ACA8489	virtual_agent_mai	172.17.0.7	N/A	 Failed 	Platform invalided (Tool: w	ind.
EΔ	new task 6	root_test	N/A				07718463D55E5	virtual_agent_mai	172.17.0.10	N/A	 Failed 	Platform invalided (Tool: w	ind.	
ø	new task 4	root_test	06/12/2022 17:43:13	N/A				6C648D7431177	virtual_agent_mai	172.17.0.9	N/A	• Failed	Platform invalided (Tool: w	ind.
	Task macosvb 1	root_test	06/12/2022 16:41:35	N/A				556075243054B	virtual_agent_mai.	2.17.0.8	N/A	• Failed	Platform invalided (Tool: w	ind.
	Task monthly dài	root_test	06/12/2022 15:18:38	N/A				6DBE442BB0298	virtual_agent_mai_	. 172.17.0.6	N/A	 Failed 	Platform invalided (Tool: w	ind.
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A				97617AC1A6094	Maingocwinx64	192.168.74.1.	0	Success	N/A	
	New task 2	root_test	06/12/2022 11:14:48	Description										
	Task 787878f	root_test	06/12/2022 11:11:58	N/A										
	New task 1	root_test	06/12/2022 11:11:42	Description										
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A										
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A										
	New task 2	root_test	06/12/2022 11:14:48	Description										
	Task 787878f	root_test	06/12/2022 11:11:58	N/A										
	New task 1	root_test	06/12/2022 11:11:42	Description										
	Task test retry 132	Task test retry 132 root_test 06/12/2022 10:49:15 N/A												
												Acti Go tr	ivate Windows • Settings to activate Windo	ws
								A The tool results is	going to be deleted auto	matically after 2 m	onths for saving reso	urces	0	s 🖆 pp

+ Download output của từng lần lập lịch:

• Mục đích: Cho phép download tất cả danh sách báo cáo kết quả deploy tool tại từng lần lập lịch;

• Các bước thực hiện: Tại màn hình View report, chọn icon ^{•••} bản ghi lập lịch mà người dùng muốn download outputs > Chọn **Download outputs**



Ţ.	Tool management Tas	k manageme					-						anociputa	6 Gerreport	· ^
	Q task		nt	_	14/12/2022 Total agents Success	51	Downlos	fx Computer ad outputs	2 ~ "mai" results					0	٩
р.H. (О	Showing 100 of 290 result(s)	Author	Occupied time	Description	12/12/2022 Total agents Success	- 12:00:00 49 2		8E03ADB705FF8. A6ED648CC1C17.	Computer name virtual_agent_mai virtual_agent_mai virtual_agent_mai.	IP Address 172.17.0.2 172.17.0.5	Tool exit code N/A N/A N/A	Status • Failed • Failed	Message Platform invali Platform invali	ded (Tool: wind. ded (Tool: wind. ded (Tool: wind.	Action
⊳ ♥	Task Marte Task Weekly MacOs Task MacOS daily 1 Task 7647657465	root_test root_test root_test	06/12/2022 18:23:59 06/12/2022 18:23:17 06/12/2022 17:57:36	N/A N/A N/A	07/12/2022 Total agents Success	- 12:00:00 49 0	•••	210352BC56C0B. 71BC4C742BB32. E450A71CC08FD.	macOS-Mais-Mac. virtual_agent_mai. virtual_agent_mai.	. 192.168.74.1 172.17.0.4 . 172.17.0.3	N/A N/A N/A	 Failed Failed Failed 	Platform invali Platform invali Platform invali	ded (Tool: wind. ded (Tool: wind. ded (Tool: wind.	
ē.	new task 8 new task 6 new task 4 Task macosyb 1	root_test root_test root_test	06/12/2022 17:56:16 06/12/2022 17:50:15 06/12/2022 17:43:13 06/12/2022 16:41:35	N/A N/A N/A				3CAD1ACA8489 07718463D55E5 6C648D7431177	virtual_agent_mai. virtual_agent_mai. virtual_agent_mai.	. 172.17.0.7 . 172.17.0.10 . 172.17.0.9	N/A N/A N/A	Failed Failed Failed	Platform invali Platform invali Platform invali	ded (Tool: wind. ded (Tool: wind. ded (Tool: wind.	
	Task monthly dåi Task abfbvfvf New task 2	root_test root_test root_test	06/12/2022 15:18:38 06/12/2022 13:58:21 06/12/2022 11:14:48	N/A N/A Description				5560752430548 6DBE442BB0298. 97617AC1A6094	virtual_agent_mai. virtual_agent_mai. Maingocwinx64	172.17.0.8 172.17.0.6 192.168.74.1	N/A N/A 0	 Failed Failed Success 	Platform invali Platform invali N/A	ded (Tool: wind. ded (Tool: wind.	
	Task 787878f New task 1 Task test retry 132	root_test root_test root_test	06/12/2022 11:11:58 06/12/2022 11:11:42 06/12/2022 10:49:15	N/A Description N/A											
	Task abfbyfyf New task 2 Task 787878f New task 1	root_test root_test root_test root_test	06/12/2022 13:58:21 06/12/2022 11:14:48 06/12/2022 11:11:58 06/12/2022 11:11:42	N/A Description N/A Description											
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A				The tool resulter in	noing to be deleted aver	matically after 3 m	withe for soving read	Activ Go to	vate Windov Settings to acti	NS vate Windows	4

+ Download báo cáo của từng lần lập lịch:

• Mục đích: Cho phép download tất cả danh sách thống kê báo cáo kết quả deploy tool tại từng lần lập lịch (định dạng .csv)

Các bước thực hiện: Tại màn hình View report, chọn icon bản ghi
 lập lịch mà người dùng muốn download báo cáo > Chọn Get report



≡	aJiant Investigation	/ Deploy Tool			View repo	rt - New	task 2					Downloa 🕁	d all outputs	Get report	×
<u> </u>	Tool management Ta	ask manageme	nt		14/12/2022 Total agents	- 12:00:00		fx ComputerNa ad outputs	me ~ "mai"					0	Q
▲ p ⁴ O t O ★ 0.4 0	Q task Showing 100 of 290 result(s) Task name Task weekly MacOs Task MacOs daily 1 Task 7647057465 new task 8 new task 4 Task macOsyb 1 Task abtov/rf New task 4 Task macOsyb 1 Task abtov/rf New task 1 Task test retry 132 Task abtov/rf New task 1 Task test retry 132 Task test retry 132 Task test retry 132	Author root_test	Created time 06/12/2022 18:23:59 06/12/2022 18:23:59 06/12/2022 17:50:15 06/12/2022 17:50:15 06/12/2022 17:50:15 06/12/2022 17:50:15 06/12/2022 18:38 06/12/2022 11:14:83 06/12/2022 11:14:82 06/12/2022 11:14:82	Description N/A N/A N/A N/A N/A N/A N/A N/A N/A Description N/A Description N/A Description N/A Description N/A Description N/A	12/12/2022 Success 12/12/2022 Total agents Success 07/12/2022 Total agents Success	51 1 1 2 2 - 12:00:00 49 2 - 12:00:00 49 0	Downlend	d outputs rt 2 BE03AD8705FF8. A6ED048C01017. AA6570644F780. 2103528C56008. 716C4C7428B32. E450A71CC08FD. 3CAD1AC8489 0771464305585 6C648D7431177. 6D8E442800298 97617AC1A6094	computer name virtual_agent_mal. virtual_agent_mal. virtual_agent_mal. virtual_agent_mal. virtual_agent_mal. virtual_agent_mal. virtual_agent_mal. virtual_agent_mal. Maingocwinx64	IP Address 172.17.0.2 172.17.0.5 172.17.0.1 172.17.0.3 172.17.0.3 172.17.0.3 172.17.0.4 172.17.0.4 172.17.0.6 172.17.0.6 172.17.0.6	Tool exit code N/A N/A	Status • Falted • Fa	Message Platform inva Platform inva	Ilided (Tool: wind Ilided (Tool: wind	Action
								A The tool results is	going to be deleted auto	matically after <mark>2 m</mark>	onths for saving reso	nurces		O B	ep 🖌

- + View tool outputs của từng agent:
 - Mục đích: Cho phép người dùng xem tool outputs của từng agent
 - Các bước thực hiện: Tại màn hình View report, hover vào bản ghi cần

xem báo cáo (có trạng thái Success) > chọn icon 🔤 > Chọn View tool output

≡	aJiant Investigation	n / Deploy Tool			View repo	ort - New t	ask 2					Downloa 🕁	d all outputs 🗗 Get r	eport X
	Tool management	Task manageme	nt		14/12/2022	- 12:00:00		fx ComputerNa	me ~ "mai"					8 Q
A	Q task				Success	1		Showing 12 of 12 re	sults					
۲H					12/12/2022	- 12:00:00		Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
	Showing 100 of 290 result((s)			Total anente	10		8E03ADB705FF8	virtual_agent_mai	172.17.0.2	N/A	 Failed 	Platform invalided (Tool:	wind.
					Success	2		A6ED648CC1C17	virtual_agent_mai	172.17.0.5	N/A	 Failed 	Platform invalided (Tool:	wind.
	Task name	Author	Created time	Description				AA657D644FF8C	virtual_agent_mai	172.17.0.11	N/A	Failed	Platform invalided (Tool:	wind.
_	Task weekly MacOs	root_test	06/12/2022 18:23:59	N/A	07/12/2022	- 12:00:00		210352BC56C0B	macOS-Mais-Mac	192.168.74.1	N/A	 Failed 	Platform invalided (Tool:	wind.
≥	Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	Total agents	49		71BC4C742BB32	virtual_agent_mai	172.17.0.4	N/A	 Failed 	Platform invalided (Tool:	wind.
善	Task 7647657465	root_test	06/12/2022 17:57:36	N/A	Success	0		E450A71CC08FD	virtual_agent_mai	172.17.0.3	N/A	Failed	Platform invalided (Tool:	wind.
~	new task 8	root_test	06/12/2022 17:56:16	N/A				3CAD1ACA8489	virtual_agent_mai	172.17.0.7	N/A	Failed	Platform invalided (Tool:	wind.
Ē	new task 6	root_test	06/12/2022 17:50:15	N/A				07718463D55E5	virtual_agent_mai	172.17.0.10	N/A	• Failed	Platform invalided (Tool:	wind.
ত	new task 4	root_test	06/12/2022 17:43:13	N/A				6C648D7431177	virtual_agent_mai	172.17.0.9	N/A	 Failed 	Platform invalided (Tool:	wind.
Ē	Task macosvb 1	root_test	06/12/2022 16:41:35	N/A				556075243054B	virtual_agent_mai	172.17.0.8	N/A	 Failed 	Platform invalided (Tool:	wind.
	Task monthly dái	root_test	06/12/2022 15:18:38	N/A				6DBE442BB0298	virtual_agent_mai	172.17.0.6	N/A	Failed	Platform invalided (Tool:	View tool output
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A				97617AC1A6094	Maingocwinx64	192.168.74.1	0	Success	N/A	± 0
	New task 2	root_test	06/12/2022 11:14:48	Description										
	Task 787878f	root_test	06/12/2022 11:11:58	N/A										
	New task 1	root_test	06/12/2022 11:11:42	Description										
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A										
	Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A										
	New task 2	root_test	06/12/2022 11:14:48	Description										
	Task 787878f	root_test	06/12/2022 11:11:58	N/A										
	New task 1	root_test	06/12/2022 11:11:42	Description										
	Task test retry 132	root_test	06/12/2022 10:49:15	N/A										
					1							Acti Go to	vate Windows Settings to activate Windows	dows.
								A The tool results is g	noing to be deleted auto	matically after 2 m	onths for saving reso	urces	(р 🖆 ор

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- + Download báo cáo kết quả deploy tool từng agent:
 - Mục đích: Cho phép download báo cáo kết quả deploy tool từng agent;
 - Các bước thực hiện: Tại màn hình view report, hover vào bản ghi agent

cần xem báo cáo (có trạng thái Success) > chọn icon -> Chọn **Download output**

												,
Tool management	Task manageme	nt:		14/12/2022 -	- 12:00:00	fx Search by	agent					Q
Q task				Total agents Success	51	Showing 50 of 51 m	esults					
				10/10/2020	10.00.00	Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
Showing 100 of 290 resul	t(s)			Total anente	49	97EB9873A6807	Win7x86-A-PC	10.0.2.15	N/A	• Failed	Architecture invalided (To	ool: :
			S	Success	2	A23B7D0C7455D	thanhnm18-test	192.168.121	0	• Failed	Failed to get output(to D	ownload outpu
Task name	Author	Created time	Description			97617AC1A6094	Maingocwinx64	192.168.74.1	0	Success	N/A	
Task weekly MacOs	root_test	06/12/2022 18:23:59	N/A	07/12/2022 -	- 12:00:00 49 0	486963F745830	Win10x64-A-PC	10.0.2.15	0	Failed	Failed to get output(tool	outr
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	Total agents		50EE37015E701	DSTect-PC	102 168 56 1	N/A	• Failed	Unknown error	hart
Task 7647657465	root_test	06/12/2022 17:57:36	N/A	Success		524P20C4C568E	EDD.TECTO2	102 168 122	N/A	• Failed	Unknown error	
new task 8	root_test	06/12/2022 17:56:16	N/A			054D0570D5403	EDR-TESTUZ	192.100.133	11/5	• Failed	Unknown en or	
new task 6	root_test	06/12/2022 17:50:15	N/A			0300037983081	HuyenP1-winT0x	192.108.74.1	N/A	• Falled	Unknown erfor	
new task 4	root_test	06/12/2022 17:43:13	N/A			12B080FA5B409	win/x80	192.108.74.1	N/A	• Falled	Unknown error	
Task macosvb 1	root_test	06/12/2022 16:41:35	N/A			AE36AD62DEA59	BichP13	192.168.255	N/A	 Expired 	Task time expired	
Task monthly dài	root_test	06/12/2022 15:18:38	N/A			1B0A66FD56EDD	DESKTOP-R2GBJ_	192.168.198	N/A	 Expired 	Task time expired	
Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A			C81D5366CED36	HuyenPT-Win7x86	192.168.74.1	N/A	 Expired 	Task time expired	
New task 2	root_test	06/12/2022 11:14:48	Description			1B2D5EC3C7611	HuyenPT-Win7x64	192.168.74.1	N/A	 Expired 	Task time expired	
Task 787878f	root_test	06/12/2022 11:11:58	N/A			97EA4D29AA9AF	BichPT3_7x86	192.168.255	N/A	 Expired 	Task time expired	
New task 1	root_test	06/12/2022 11:11:42	Description			AB55552ED3C7F	thanhnm18-w10x	192.168.121	N/A	 Expired 	Task time expired	
Task test retry 132	root_test	06/12/2022 10:49:15	N/A			5DF867D8A4E3F	HuyenPT-Win10x	192.168.74.1	N/A	 Expired 	Task time expired	
Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A			F2AA317BE8769	Blchpt3_Win10Te	192.168.255	N/A	 Expired 	Task time expired	
New task 2	root_test	06/12/2022 11:14:48	Description			3C7764CA3D8D8.	bao-PC	10.0.2.15	N/A	 Expired 	Task time expired	_
Task 787878f	root_test	06/12/2022 11:11:58	N/A			EA4B8A259CC45	x64_ptbich	192.168.255	N/A	 Expired 	Task time expired	
New task 1	root_test	06/12/2022 11:11:42	Description			AC736D6DD5A3	Win10x86	192.168.74.1	N/A	Expired	Task time expired	
Task test retry 132	root_test	06/12/2022 10:49:15	N/A			E1A2D22E765E5	thanhnm18-test-7	192.168.121	N/A	Expired	Task time expired	
						EF0C1A62F117F_	thanhnm18-w7x64	192.168.121	N/A	• ExpiredActiv	Task time expired	
										Go to	Settinos to activate Wind	rows.

3.6 Màn hình Response

3.6.1 Response_Live Response

Mục đích: Chức năng Live response cung cấp khả năng xử lý một tập các command từ xa theo phiên làm việc nhằm cho biết các thông tin hoặc xử lý yêu cầu trên host; Các bước thực hiện chức năng Live Response:

Bước 1: Click tab "Response" và chọn "Live Response";



Viettel aJiant Response / Live response	÷ 0
e	
A	
	>_
	Live response
	Choose as online agent for a live response, then click Connect to start the session.
	DESKTOP-R2Q8JEF V Is minutes
9	Connect
	46

Bước 2: Thực hiện tạo mới 1 phiên live response Chọn Agent: Hiển thị danh sách các agent:

+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;

Người dùng chỉ thực hiện được Live Response với những agent đang có trạng thái online:

	Q	Search agent	
-	• Di	SKTOP-R2GBJEF (1B0A66FD56EDD4C2C6D557DDFDB79A6F	

+ Chon Duration: có các khoảng thời gian 5 phút, 15 phút, 1 giờ, 3 giờ;





+ Click nút "Connect":

	>_		
Live response			
Choose an online agent for start the session.	a live response,	then click 'Conne	ct' to
Agent		Duration	2
DESKTOP-R2GBJEF	~	15 minutes	Q
	Connect		
		(3

Bước 3: Chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là "connecting":

Choose an online agent for a live response, then click 'Connect' to start the session.				
Agent		Duration		
DESKTOP-R2GBJEF	~	5 minutes	Ŏ	
Connecting to agent (expire in 00:58)				
Cancel connection				

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@vietteLcom.vn | W: www.viettelcybersecurity.com



Bước 4: Khi kết nối thành công, người dùng được phép thực hiện các lệnh ở màn hình console và trạng thái của phiên Live response "running";

Lưu ý: Mỗi agent tại một thời điểm chỉ có 1 phiên Live response làm việc.

=	aJiant Response / Live response						# 0
¢	HOST NAME DESKTOP-R2GBJEF	CONNECTED TIME 27/06/2022 - 03:46:51	TIME TO RESPOND S minutes	DURATION 00:04:17	status Running	Change agent Stop connect	
- ₁ ,t ⊕ ≥	-ddicte chepanae) -+ conlorance -+ ctyp -ddicte chepanae) ddicte chepanae) ddicte chepanae) dalcte che	<pre>d datab AM subs. status. B2, B3 = 184 2 = 280, CONNE 52 3 = 280, CONNE 52 3 = 280, CONNE 52 5 = 280, CONNE 141, EXCEDING 5 = 280, CONNE 140, CONNE 140, CONNE 5 = 280, CONNE 140, CONNE 140, CONNE 140, CONNE 5 = 280, CONNE 140, CONNE 140, CONNE 140, CONNE 5 = 280, CONNE 140, CONNE 140, CONNE 140, CONNE 5 = 280, CONNE 140, CONNE 140, CONNE 140, CONNE 5 = 280, CONNE 140, CONNE 140,</pre>	Unicode mal terminated a Unicode mal terminated a Unicode mal terminated a Unicode mal terminated a Unicode Male and Alexandro Statistics and Alexandro Resource list in the terminate Resource list in the terminate Male and Alexandro Male and Alexandro Male and Alexandro Male and Alexandro Male and Alexandro Alexandro Alexandro Male and Alexandro Alexandro Male and Alexandro Alexandro Male and Alexandro Alexandro Male and Alexandro Alexandro Male and Alexandro Alexandro Male and Alexandro Ale	rring Fring with environment variable refere RES_INHED) Guarde map Guarde description d "c:tramplic.exe" a226-2000/Software/test	8083)		
		terilate a proces, semple: proces will be a process, semple: proce dilpate a case semitive into fail and a process, semple: proce resume a process into process of all laters into process of all laters exercises a super, example: process - exercises a super, example: process - exercises a super, example: process - exercises a super, example: process - exercises and the service and the service into the service - listering as	t 103 ar -wildd 123 Drmslware.dll boware -∂ ciwinddwe'rµn,ese -a lies erwinddwe'rµn,ese erg				
	Recharge Close session						6

Lưu ý: Người dùng có thể thực hiện câu lệnh kết nối tới container bằng cách thực hiện các lệnh màn hình console container

ajia	ant Response / Live Response						# 0
₽ ▲	HOST NAME ubuntu-docker	CONNECTED TIME 28/12/2022 - 10:09:05	 TIME TO RESPOND 15 minutes 	DURATION 00:13:06	STATUS Running	Change agent Stop connect	
μ [#] (W (W (W (W (W (W) (W) (W) (W) (W) (W) (Hemote session started.** Rednesday, 28-Dec-22 03:09:14 Rednesday, 28-Dec-22 03:09:14 Ventainer -1 PRTAINER ID Hadde	4 UTC] Agent Connected 4 UTC] Agent info: Linux OS CCREAND CREATED STATUS *Dash* 6 days ago Up 6 de "bash* 6 days ago Up 6 de	PORTS NAMES ys silly_saha ys magical_blackby				
Th DA (2) co co co di de ww vi ha	<pre>se operation completed succes whelp sticle hjiant live Response C d. change to ps ed change to ps ed change to ps ed change to ps of the second s</pre>	Safully. Commandline surrent working dir arent dir arent dir arent dir arent dir autorial dir subfolger in ournet folder undreider in folder dietes a file diet dietes afile diet dietes afile in folder thuy bates diete - file "trup/ru dietes afile in folder dietes afile in folder dietes afile in folder thuy arente in er the subfolger example: diete - folder thuy arente dietes afile in en diet arente dietes afile in folder teres of the subfolger example: we "trup/cless folder die bit of file ai nample: we "trup/cless file folger her file hand limited 4000	o host n* mot delete folder older n.so* */tmp/evil.so* see 10 of file size			Activate Windows On 10 Settings to actuate	• Windows

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Người dùng có thể thực hiện các lệnh tại màn hình console như sau:

+ Window: thực hiện các câu lệnh sau:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath></dirpath>	Thay đổi thư mục làm việc hiện tại
		cd hoặc cd	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
		dir [drive:][path][filename] [/A[[:]attributes]] [/O[[:]sortorder]] [/T[[:]timefield]] [/L] [/Q] [/R] [/S] [/X]	Liệt kê các file/ các thư mục con trong thư mục hiện thời
3	dir	 /A:[-] attributes Displays files with specified attributes. Attributes: D Directories R Read-only files H Hidden files A Files ready for archiving S System files L Reparse Points 	
		/L Lower-case filename	

Ĺ



STT	Các lệnh	Tham số	Mô tả
		/O:[-]sortorder List by files in sorted order.	
		sortorder	
		N By name (alphabetic)	
		S By size (smallest first)	
		E By extension (alphabetic)	
		D By date/time (oldest first)	
		G Group directories first	
		- Prefix to reverse order	
		Ex: dir /O:N;	
		/T:timefield Choose which time field displayed	
		timefield	
		C Creation	
		M MFT Creation	
		A Last Access	
		W Last Written	
		Ví dụ: dir /T:A	
		- Prefix to exclude attribute	
		Ví dụ: dir /A:D-AH	
		/Q Display the owner of the file.	
		Ví dụ: dir /Q	



STT	Các lệnh	Tham số	Mô tả
		/R Display alternate data streams of the file.Ví dụ: dir /R	
		/S Displays files in specified directory and all subdirectories. Ví dụ: dir /S	
		 /X This displays the short names generated for non-8dot3 file names. Ví dụ: dir /X 	
		delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"</path>	Xóa 1 file
4	delete	delete -folder <folderpath> ví dụ: delete -folder temp\axvers</folderpath>	Xóa 1 thư mục
		delete –all <folderpath> ví dụ: delete –all c:\temp</folderpath>	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<sourcepath> <destpath> move (rename) file / folder</destpath></sourcepath>	Cho phép di chuyển file/ folder



STT	Các lệnh	Tham số	Mô tả
		Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5="" sha1="" ="" <br="">sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe</filepath></type:>	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	dump		Cho phép dump tiến trình. Nếu bạn bỏ qua đường dẫn tệp kết xuất, nó sẽ mặc định là <processname> _ <datetime> .dmp</datetime></processname>
		-process -pid <processid> [-f <destpath>] dump process by process id Ví dụ: dump -process -pid 452 -f "C:\Users\Evil_dumped.dmp"</destpath></processid>	Dump process bởi Process id
		-process-name <processname>[-f<destpath>]dumpprocess by process name</destpath></processname>	Dump process bởi Process name



STT	Các lệnh	Tham số	Mô tả
		Ví dụ: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp"	
		-process-path <processpath>[-f<destpath>]dumpprocess by process pathVí dụ: dump -process -path"C:\Users\Evil.exe" -f"C:\Users\Evil_dumped.dmp"</destpath></processpath>	Dump process bởi Process Path
9	get	<filepath></filepath>	Upload 1 file từ host lên server
10	put	<url><folderpath></folderpath></url>	Download 1 file tới máy host
11	mkdir	<dir name=""></dir>	Tạo 1 thư mục
			Các lệnh liên quan đến Registry
12	reg	query <keyname> -v <valuename> ví dụ: reg-query "HKLM\Software\abc xyz" -v "run path" query <keyname> -s ví dụ:</keyname></valuename></keyname>	Truy vấn dữ liệu value của 1 key Truy vấn tất cả các subkey và value và data

 \square



STT	Các lệnh	Tham số	Mô tả
		reg-query "HKLM\Software\abc xyz" -s	
		add <keyname> ví dụ: reg-add "HKLM\software\abc xyz"</keyname>	Thêm 1 key
		add <keyname> -v <valuename> -t <type> -d <data></data></type></valuename></keyname>	Thâm 1 value
		reg-add "HKLM\software\abc xyz" -v "run path" -t REG_SZ - d "c:\temp\bin.exe"	
		delete <keyname> ví dụ: reg -delete HKU\S-1-5-21- 3791698801-2327923109- 636705026- 2080\Software\Test</keyname>	Xóa 1 key và tất cả các subkey và value
		delete <keyname> -v <valuename></valuename></keyname>	Xóa 1 giá trị của key
		import <filename></filename>	Import 1 file .reg
		export <keyname> <filename></filename></keyname>	Export 1 file .reg



STT	Các lệnh	Tham số	Mô tả
			Các lệnh liên quan đến process
		-t <processid></processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid></processid>	Tạm dừng 1 tiến trình
13	process	-r <processid></processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-I -u <username></username>	Liệt kê các process của 1 user
	service		Các lệnh liên quan đến service
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename></servicename>	Start 1 service
14		-stop <servicename></servicename>	Stop 1 service
		-uninstall <service_name> uninstall service</service_name>	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service - listdrivers	List danh sách drivers trên host
15	USAr	-list	Liệt kê các user trên máy
15	usei	-sid <username></username>	Lấy sid của username



STT	Các lệnh	Tham số	Mô tả
16	grep	grep -t <text> <param/> <command/></text>	Hỗ trợ tìm kiếm theo từ hoặc chuỗi từ kết quả đầu ra được theo lệnh command truyền vào
17	cls		Xóa màn hình console
18	help		Lệnh help
19	Clear		Làm sạch console
20	Close		Đóng session
		-	Liệt kê danh sách container
21	container	-a <container id=""></container>	Kết nối tới từng container
		-d	Thoát kết nối container

+ Ubuntu: Thực hiện các câu lệnh sau:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath></dirpath>	Thay đổi thư mục làm việc hiện tại
		cd hoặc cd	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
3	dir	dir list file / subfolder in current folder	Liệt kê các file/ các thư mục con trong thư mục hiện thời
4	delete	delete -file <path></path>	Xóa 1 file



STT	Các lệnh	Tham số	Mô tả
		ví dụ: delete -file "c:\temp\run path.exe"	
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers</folderpath>	Xóa 1 thư mục
		delete –all <folderpath> ví dụ: delete –all c:\temp</folderpath>	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<sourcepath> <destpath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"</destpath></sourcepath>	Cho phép di chuyển file/ folder
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5="" sha1="" ="" <br="">sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe</filepath></type:>	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath></filepath>	Upload 1 file từ host lên server



	inani so	Mo ta
put	<url><folderpath></folderpath></url>	Download 1 file tới máy host
mkdir	<dir name=""></dir>	Tạo 1 thư mục
	-t <processid></processid>	Các lệnh liên quan đến process Tắt 1 tiến trình đang chạy theo ID tiến trình
	-s <processid></processid>	Tạm dừng 1 tiến trình
process	-r <processid></processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
	-l -a	Liệt kê toàn bộ các process của tất cả các user
	-I -u <username></username>	Liệt kê các process của 1 user
	-e -s <imagepath> -c <cmd> execute a non GUI process as system</cmd></imagepath>	
	Ví dụ: process -e -s /tmp/run	
	-e-u <username> <imagepath> -c <cmd> execute a non GUI process as a user Ví dụ: process -e -u Alex</cmd></imagepath></username>	
	put	put <url><folderpath>mkdir<dir name="">mkdir-dir name>-t <processid>-t-t <processid>-s-s <processid>-r-r <processid>-r-l -a-l -a-l -u <username>-e -s <imagepath> -c <cmd><md><md><md><md><md><md><md><md><md><</md></md></md></md></md></md></md></md></md></cmd></imagepath></username></processid></processid></processid></processid></dir></folderpath></url>

 \square



STT	Các lệnh	Tham số	Mô tả
		-d <processid> -o <imagepath> generate core file of running program, ví dụ: process -d 231 -o /tmp/core_file</imagepath></processid>	
			Các lệnh liên quan đến service
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename></servicename>	Start 1 service
12	service	-stop <servicename></servicename>	Stop 1 service
		-uninstall <service_name> uninstall service</service_name>	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service - listdrivers	List danh sách drivers trên host
13	usor	-list	Liệt kê các user trên máy
10	usei	-sid <username></username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console
21	container	-	Liệt kê danh sách container
21		-a <container id=""></container>	Kết nối tới từng container



STT	Các lệnh	Tham số	Mô tả
		-d	Thoát kết nối container

+ MACOS:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath></dirpath>	Thay đổi thư mục làm việc hiện tại
		cd hoặc cd	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
3	dir	dir list file / subfolder in current folder	Liệt kê các file/ các thư mục con trong thư mục hiện thời
4	delete	delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"</path>	Xóa 1 file
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers</folderpath>	Xóa 1 thư mục
		delete –all <folderpath> ví dụ: delete –all c:\temp</folderpath>	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)



STT	Các lệnh	Tham số	Mô tả
5	mv	<sourcepath> <destpath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"</destpath></sourcepath>	Cho phép di chuyển file/ folder
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5="" sha1="" ="" <br="">sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe</filepath></type:>	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath></filepath>	Upload 1 file từ host lên server
9	put	<url><folderpath></folderpath></url>	Download 1 file tới máy host
10	mkdir	<dir name=""></dir>	Tạo 1 thư mục
11	process		Các lệnh liên quan đến process
		-t <processid></processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid></processid>	Tạm dừng 1 tiến trình



STT	Các lệnh	Tham số	Mô tả
		-r <processid></processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-I -u <username></username>	Liệt kê các process của 1 user
		-e -s <imagepath> -c <cmd> execute a non GUI process as system Ví du: process -e -s /tmp/run</cmd></imagepath>	
		-e-u <username> <imagepath> -c <cmd> execute a non GUI process as a user Ví dụ: process -e -u Alex /tmp/run</cmd></imagepath></username>	
			Các lệnh liên quan đến service
12	service	-query	Liệt kê các service đang chạy trên máy host
		-start <servicename></servicename>	Start 1 service
		-stop <servicename></servicename>	Stop 1 service
		-uninstall <service_name> uninstall service</service_name>	Gỡ cài đặt service



STT	Các lệnh	Tham số	Mô tả
		-listdrivers list drivers on host, example: service - listdrivers	List danh sách drivers trên host
13	user	-list	Liệt kê các user trên máy
		-sid <username></username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console

Một số lưu ý khi làm việc với các lệnh trên màn hình console:

+ Lệnh Clear: Sau khi thực hiện lệnh clear thì hệ thống sẽ hỗ trợ người dùng download toàn bộ log đã thực hiện trên màn hình console trước đấy, bằng thao tác click vào link "here";

+ Lệnh get <filepath>: ví dụ: get procexp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình Attachment Log ở phía dưới góc bên phải của màn hình. Người dùng được phép tải file về trình duyệt hoặc xóa file đã lấy về server.

Bước 5: Phiên làm việc của Live Response kết thúc khi:

+ Thời gian của phiên hết hiệu lực: Khi trường "Duration" bằng thời gian với trường "Time To Live";

Page | 171



▲ ™±	HOST NAME DESKTOP-R2GBJEF	CONNECTED TIME 27/06/2022 - 03:46:51	 TIME TO RESPOND 5 minutes 	DURATION 00:00:01	Status Stopped	Connect to agent
0 I D # 6	-delete (keynaac) -delete (keynaac) -v (valuenaac) -siport (tilenaec)	3 - BES_BINAN 4 - BES_BINAN 4 - BES_BINAN 5 - BES_BINAN 5 - BES_BINAN 7 - BES_BINAN 7 - BES_BINAN 7 - BES_BINAN 7 - BES_BINAN 8 - BES_BINAN 8 - BES_BINAN 8 - BES_BINAN 8 - BES_BINAN 8 - BES_BINAN 8 - BES_BINAN 1 - BES_BINAN 9 - BES_BINAN 1 - BES_BINAN 9 - BES_BINAN 1 - BES_BINAN 9 - BES_BINAN 1 - BES_BINAN 9 - BE	Free form binary 32 - bit mumber(same a 32 - bit mumber Symbolic link(muncode) Multiple bindood strice Multiple bindood strice 151 151 151 151 151 151 151 15	a REG_INARES) I pr securce map andmain description -d "clivesp(bill.exe" 500026-2000;dofuser=itars		
Ĭ	"Adjoint trepment valuement" process - disposation - disposatio	waptic w sey to a tray take terminate a process, example: process -t will part is cash example: process -t will part is cash meanling integer & process rangend a process rangend a process integrocess of a user integrocess of a user integrocess of a user integrocess of a user integrocess of a user integroces a system, example: process entrice execute a system, example: process entrice execute a super, example: process	9213 222 minised 223 Dimisivere.ell1 Sewarte e civaladowi non.ese allos civaladowi non.ese			
	-linddrivers list de user list discusses -sid cusermane get sid of userman clear clear connole bip command help clove clove session C:> C:> Jonnaky, 27-Jun-22 08:50:23 UTC; Session t	re samost, excepter service -listdrive	19			

- + Người dùng chủ động yêu cầu đóng kết nối bằng lệnh "close";
- + Khi mất kết nối với agent, server thực hiện ping/pong failed trên 3 lần.



3.7 Màn hình Setting

3.7.1 Agent Management

Mục đích: Chức năng Agent Management hỗ trợ người quản trị quản lý các agent đã cài đặt bao gồm:

+ Xem danh sách các agent và các thông tin chung;





- + Xem chi tiết của Agent;
- + Chọn nhanh các agent và thiết lập một số cài đặt (policy, update group);

≡	viette aJia	Setting / Agent	Management								🗰 🤷 🕅
E	Agent r	management									Guidelines
A	Type to :	search by queries								First Ping 📋	Last Ping 📋 🛛 🔍
μt	3 result((s)								📩 Vie	v column
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING		FIRST PING	IP DCN	POLICY	VERSION
_		Localhost.Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58		05/04/2022 14:49:51	10.61.188.2	phula_test	
<u>}-</u>		Ubuntu18	 Offline 	Default	Test	09/06/2022 17:24:22		07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8 5
◙		N/A	Offline	N/A	N/A	N/A		N/A	N/A	N/A	
Ē.	Display 3	/3 result					0				
ē											

Hệ thống hỗ trợ thực hiện các tính năng:

1 – Xem danh sách các agent đã được cài đặt trên hệ thống:

+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;

+ Mỗi agent được hiển thị các thông tin chung gồm: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, PlatForm, PlatForm Version, Architecture, DNS, Version.

2 – Hỗ trợ chức năng tìm kiếm Agent theo AgentID, ComputerName, OS, Architecture, Platform, Policy, IPDCN, Online, Update Group, Group ID, IP, Mac, Version. Với mỗi tiêu chí tìm kiếm thì hỗ trợ các toán tử tìm kiếm "=", "!=", "~";



≡	viet aJ	tel iant Setting / Agent Management			*	<mark>ы[°] О</mark>
Ţ,	Agen	t management			0	Guidelines
A	Agen	tID = "03D31B3FE60E83372C6EA3F8D5737FA19DBA5988" AND		First Ping	Last Ping 📋	Q
	۲	AgentID	Agent ID			
Ę	۵	ComputerName	۷ 🛎	liew column	~	
۹	00	OS	POLICY	VERSION		
5-	Ø	Architecture	Agent Architecture	phula_test	220	
	O D	Platform	Agent Platform	N/A	0.0.0	
č	O	Policy	Applied Policy			
Ē.	۲	IPDCN	IP DCN			
ē						

Ví dụ về các câu tìm kiếm:

+ Tìm kiếm với điều kiện "=":

≡	viett aJia	el Bot Setting / Agen	t Management										*	6 a
E	Agent	management												3 Guidelines
A	Policy = 'phula,test'												Last Ping	⊒
Ť±	1 resul	t(s)										🛃 Vie	ew column	~
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING		FIRST PING		IP DCN	POLICY		VERSION	
_		Localhost.Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58		05/04/2022 14:49:51		10.61.188.2	phula_test			
<u>>-</u>	Display	1/1 result												
₽														
Ē														
٥														

+ Tìm kiếm với điều kiện "!=":

≡	vietti aJia	Setting / Agent	t Management							*	a . U
1 1 1	Agent	management								0	Guidelines
A	Policy !	= "phula_test"							First Ping	Last Ping 📋	Q
۶.	2 result	t(s)							🛓 Vie	w column	~
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION	
_		Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8	
<u>}-</u>		N/A	 Offline 	N/A	N/A	N/A	N/A	N/A	N/A		
◙	Display 2	2/2 result									
Ē											
ē											

+ Tìm kiếm với điều kiện "~":

Ĺ



≡	vietti aJia	el ant Setting / Agen	t Management								*	6
Ę	Agent	management									(Guidelines
A	Compu	uterName ~ "ubun"							First Ping		Last Ping 📋	Q
P#	1 result	t(s)								🛃 Vi	ew column	~
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY		VERSION	
		Ubuntu18	 Offline 	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_f	eatures	3.3.8	
D	Display	1/1 result										
Ē												
9												

+ Tìm kiếm theo tiêu chí kết hợp AND:

=	vieti aji	ant Setting / Age	ent Management								*	6 6
	Agent	t management									0	Guidelines
A	Comp	uterName "ubun" AND Policy =	"anhnn_fuil_features"						First Ping		Last Ping 📋	Q
F ₇ #	1 resu	it(s)							4	±	View column	~
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY		VERSION	
		Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_fea	atures	3.3.8	
. D	Display	1/1 result										

+ Tìm kiếm theo tiêu chí kết hợp OR:

≡	viette aJia	Setting / Agent	Management							*	0
<u>N</u>	Agent	management								8	Guidelines
A	Policy =	"anhnn_full_features" OR Policy =	"phula_test"		First Ping	Last Ping 📋	Q				
P#	2 result	(8)							خ View	v column	~
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION	
_		Localhost.Localdomain	 Offline 	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test		
<u></u>		Ubuntu18	 Offline 	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8	
◙	Display 2	2/2 result									
Ē.											
ē											

3 – Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Policy

≡	vie aJ	liant Setting / Agen	t Management							*	6 °
Solution	Ager	nt management								0	Guidelines
A	Тург	to search by queries							First Ping	Last Ping	Q
₽±	3 res	ult(s)							🛃 Vie	w column	~
۲	Sele	cted (2) Set Policy Mo	ve to group 📓 Set update group	Cancel							
_		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION	
		Localhost.Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test		
D		Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8	
		N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A		
Ē.	Displa	y 3/3 result									
Ō											

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Ĺ



- + Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;
- + Thực hiện Set Policy:
 - Chon Policy:

≡	viettel aJiant	Setting / Agent Management						💥 🎍 🕅
5	Agent manager	nent						Guidelines
A	Type to search by qu	eries					First Ping	Last Ping 📋 🔍
P,#	3 result(s)						📩 View	column ~
۲	Selected (2)	Set Policy Move to group Set update group Cancel						
_	NAME	Policies	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
<u></u>	Localhe	Select an Option	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
◙	Ubuntu		Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8
	<u>N/A</u>		N/A	N/A	N/A	N/A	N/A	
ĒΔ	Display 3/3 result	default						
ৰ		full_features						
Ψ.		full_features_khaitb						
		phula_test						
		full_features_v2						
		anhnn_full_features						
		Full_AV						
		full fosturae macor						

- Xác nhận thao tác bằng cách chọn nút "Set policy";
- Xác nhận hủy thao tác bằng cách chọn nút "Cancel".
- 4 View Column: Cấu hình hiển thị các cột theo mong muốn.



5 – Xem chi tiết 1 agent bằng việc click duplicate chuột vào 1 row bất kỳ



Hệ thống hỗ trợ người dùng thiết lập Policy, Update Group và Move to group cho Agent 1 cách nhanh chóng.

+ User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị Group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Group thuộc user đang login và các user thuộc group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc user đang login;

Tab General info

+ Hệ thống hiển thị các thông tin chung về agent gồm: Các thông tin chung, CPUs, Network Interfaces, Default Gateway, DNS Server;

=	aJiant Setting / Agen	t Management			Offline Agent I Agent ID 31F6FA372944	ocalhost.localdomain b72C2DC854E155A63170CE	9686AD				î Uninstall 🗙
E.	Agent management				First ping: 05/04/2022 1	4:49:51 Last ping: 09/06/2	1022 10:43:58				
A	Type to search by gueries				Agent properties						
- ₅₋	2				Set Policy		Set update group	N	Nove to group		
-	3 result(s)				phula_test	~	phula_test	~	default	~ s	ave changes
۲	NAME	STATUS	GROUP	UPDATE GROUP							
	Localhost Localdomain	Offline	Default	Phula_test	About this agent						
<u>e-</u>]	Ubuntu18	offline	Default	Test	< General info	Installation Files Versio	n Installed Certificates	Scheduled Tasks	Disks & partitions	Environment variable	s Installed softs >
	<u>N/A</u>	Offline	N/A	N/A		installation rines renate	in monined our infeaters	ouncourse rasks	e entres a particione	citrionnent fundole	a matured some -
	Display 3/3 result				General info			Networ	rk Interfaces		
Ēλ					Host Name	localhost.localdoma	in	IP v4	127	.0.0.1	
1					Host ID	015a4d56-e545-241	a-e66b-14410ce8c348	IP v6	::1		
					Setup Version	N/A		MAC	N/A		
					Operating System	linux		Name	lo		
					Platform	redhat		IP v4	192	168 121 132	
					Platform Version	8.2		IP v6	fe80	1-437e.dc7a:2765:34ad	
					Platform Family	rhel		MAC	00-0	lc-29:e8:c3:48	
					Architecture	amd64		Name	eos	160	
					Physical Memory	1,843,832					
					CPUs			Default	1 Gateway		
					Cores	1		192.16	8.121.2		
					mhz	1992.001000		DNS Se	erver		
					Model Name	Intel(R) Core(TM) 17	-10700T CPU @ 2.00GHz	192.16	8.121.2		
					Vendor ID	GenuineIntel					

Installation Files Version

+ Thống kê tất cả các file cài agent, bao gồm các thông tin: Tên folder chứa file cài, File name, Version;

+ Hỗ trợ search nhanh theo File name, Version vào text box search



Page | 177



≡	aJiant Setting / Agen	t Management			Offline Agent localhost.localdomain Agent ID 31F6FA372944D72C2DC854E155A63170CE968	660 thistal
Ę.	Agent management				First ping: 05/04/2022 14:49:51 Last ping: 09/06/2022	2 10:43:58
A	Type to search by queries				Agent properties	
-					Set Policy Set	t update group Move to group
Ē	3 result(s)				phula_test ~	phula_test V default V Save changes
۲	NAME	STATUS	GROUP	UPDATE GROUP		
_	Localhost.Localdomain	Offline	Default	Phula_test	About this agent	
٥.	Ubuntu18	Offline	Default	Test	General info Installation Files Version	Installed Certificates Scheduled Tasks Disks & partitions Environment variables Installed softw >
◙		Offline	N/A	N/A		
<u> </u>	Display 3/3 result				Search by file name or version	Q
Ľ <u>à</u>					ajiant	VESUpdater
٩					···· response	VERSION 3.3.0
					collector	VESSvc
					drivers	VERSION 3.3.0
						RWorker
						VERSION 3.3.0
						VESConfigurationManager VERSION 3.3.0
						Agentinfo VERSION 3.3.0
						VESConnectionManager VERSION 3.3.0

Installed Certificates

+ Thống kê tất cả các certificate trên máy cài agent, bao gồm các thông tin: Danh sách certificates trên máy, Issused by, Issused to, Expiration date, Status;

+ Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn ⁽¹⁾, hiển thị màn hình như sau:

rtificate	
FRIENDLY_NAME	Microsoft Root Certificate Authority
ISSUER	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
KEY_USAGE	Digital Signature, Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing (c6)
SIGNATURE_ALGORITHM	sha1RSA
STATUS	R
SUBJECT	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
VALID_FROM	10/05/2001 06:19:22

Scheduled Tasks



+ Thống kê tất cả scheduled tasks trên máy cài agent, bao gồm các thông tin: Danh sách các scheduled tasks, Name, Status, Trigger, Next time run, Last time run, Author, Created;

+ Chọn ^{show} hoặc ^{Hide} để tùy chỉnh việc hiển thị thông tin bổ sung cho từng task;

+ Hover vào task và chọn 🕡 để xem thông tin đầy đủ của task dưới dạng xml

KML Detail	>
xml version="1.0" encoding="LITE-16"?	
Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">	
<registrationinfo></registrationinfo>	
<date>2021_03_09T18:36:49 6502882</date>	
<authors administrators="" authors<="" cs="" td=""><td></td></authors>	
<triangere></triangere>	
<principale></principale>	
<principal id="Author"></principal>	
< sprid>S-1.5-21-3942219608-2782901308-3935319899-500 corld	
< ogonTyne> nteractiveToken ogonTyne	
<punt eactprivilence<="" evels<="" evelst="" punt="" td=""><td></td></punt>	
<sattings></sattings>	
<multipleinstancespolicy>IgnoreNew</multipleinstancespolicy>	
<disallowstartifonbatteries>true</disallowstartifonbatteries>	
<stanlfcaingonbatterios>true</stanlfcaingonbatterios>	
<a>AllowHardTorminatoStruck/AllowHardTorminatoS	
<start whenavailable="">false</start>	
<stattwiteinavallablezialses p="" stattwiteinavallablez<=""></stattwiteinavallablezialses>	
<pre></pre>	
<td></td>	
<stopontaleend>true</stopontaleend>	
<restantonidie>taise</restantonidie>	
	LEXPORT to XML

.xml

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 179



Disks & partitions

+ Thống kê tất cả disks & partitions trên máy cài agent, bao gồm các thông tin: Danh sách Disks, Partition, Volume name, Serial, Drive type, File system, Capacity, Available

+ Chọn ^ hoặc Y để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.

≡	viettet aJiant Setting / Agent Management						Online Agent DESKTOP-R2GBJEF Agent to 1804A64504820442004055064769144650482004				×	
4	Agent	management				First ping: 09/06/2022 11:28:00 Last ping: 29/06/2022 18:28:58						
	Type to search by queries						Agent properties					
-								Set Doliny Set undete arroup Move to arroup				
ŧ	9	result(s)				full features hash	v miana	V default	Y Construction			
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	TOT_TEGISTES_Down	* Telease	derault	Save changes		
, a		Bichot3-Centos7	Offline	Default	Release	28/06/2022 16:35:13	About this agent					
		DESKTOP-R2GBJEF	Online	Default	Release	29/06/2022 18:23:58	(Disks & contribution			
		Win10x64bichpt3	© Offline	Default	Release	29/06/2022 17:36:14	General info Installation Fil	les Version Installed Certificates Sched	aled Tasks Disks & partitions	Environment variables Installed a	oftv *	
Ľ.		Bichpt3-Ubuntu18	Offline	Default	Release	29/06/2022 17:35:26	VMware Virtual NVMe Disk				^	
Ē		WIN-T5BK3MCL9I0	Offline	Default	Release	28/06/2022 11:38:23	Partition	C:				
		Anhnn19-Centos7	© Offline	Default	Release	29/06/2022 14:11:30	Volume Name					
		Centos6	Offline	Default	Release	29/06/2022 17:38:15	Serial	629825D5				
		Win7x64-A-PC	Offline	Group_bichpt3	Release	28/06/2022 15:38:25	Drive Type	Fixed				
		N/A	© Offline	N/A	N/A	N/A	File System	NTFS				
	Display 9/9 result						Capacity	50553 MB				
							Available	25128 MB				
											^	
							Partition	D:				
							Volume Name	ESD-ISO				
							Serial	DD15656F				
							Drive Type	CDRom				
							File System	UDF				
							Capacity	4071 MB				
							Available	0 MB				

Environment variables

+ Thống kê tất cả environment variables trên máy cài agent, bao gồm các thông tin: Danh sách system và users, tên biến, giá trị trực thuộc system hoặc user;

+ Chọn ^ hoặc Y để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.


≡	viettet aJiant Setting / Agent Management					Online Agent DESKTOP-R20BJEF Agent ID TROMMTDBAEDWICKDSTDOFERTMANSSARFOCC				
2	Agent	management					First ping: 09/06/2022 11:28:00 Last ping: 29/06/	/2022 18:23:58		
A	Type to	search by queries					Agent properties			
							Set Policy	Set update group	Move to group	
È	9	9 result(s)				full_features_baolt ~	release ~	default	Save changes	
۲		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING				
_		Bichpt3-Centos7	Offline	Default	Release	28/06/2022 16:35:13	About this agent			
		DESKTOP-R2GBJEF	Online	Default	Release	29/06/2022 18:23:58	Constallation Files Versi	on Installed Certificates Scheduled To	ska Diska & partitiona Environme	t variables Installed softy >
		Win10x64bichpt3	Offline	Default	Release	29/06/2022 17:36:14		on materies certificates orthogened re		
		Bichpt3-Ubuntu18	© Offline	Default	Release	29/06/2022 17:35:26	System			^
Εà		WIN-T5BK3MCL9I0	Offline	Default	Release	28/06/2022 11:38:23	ComSpec			
٥		Anhnn19-Centos7	Offline	Default	Release	29/06/2022 14:11:30	%SystemRoot%\system32\cmd.exe			
		Centos6	© Offline	Default	Release	29/06/2022 17:38:15	DriverData			
		Win7x64-A-PC	© Offline	Group_bichpt3	Release	28/06/2022 15:38:25	C:\Windows\System32\Drivers\DriverData			
		<u>N/A</u>	© Offline	N/A	N/A	N/A	OS NERGENIA NT			
						Testimute Control of Control Partnet Partnet Part	F, WSHLMSC	h signanus mount y vez anno y		

Tab Installed Software

+ Thống kê tất cả phần mềm đã cài trong agent bao gồm thông tin: Tên phần mềm, version cài, ngày cài;

+ Hỗ trợ search nhanh phần mềm Antivirus đã cài hoặc nhập tên phần mềm vào text box search;

Tab Required Software

+ Thống kê tất cả phần mềm bắt buộc đã cài hoặc chưa cài trong agent bao gồm thông tin: Tên phần mềm, version cài, trạng thái cài;

+ Hỗ trợ search nhanh phần mềm bắt buộc chưa cài đặt trên máy hoặc nhập tên phần mềm vào text box search.

Tab User list

+ Thống kê tất cả User đăng nhập trong agent bao gồm thông tin: Tên user, active, administrator

6 – Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Move to group

+ Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;



≡	vie a.	Setting / Agen	t Management							*	• 0
Ę	Agent management								Guidelines		
A	Тур	e to search by queries							First Ping	Last Ping	Q
۴	3 result(s)								v		
۲	Sel	ected (2) Set Policy Mov	ve to group Set update group	Cancel							
_		NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION	
<u>}-</u>		Localhost.Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test		
D		Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8	
		N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A		
E	Displ	ay 3/3 result									
ē											

+ Thực hiện Move to group:

Danh sách Group trong combobox Move to group:

- User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
- User đăng nhập thuộc group default: Hiển thị Group default;

 User đăng nhập thuộc group cha: Hiển thị tất cả Group thuộc user đang login và các user thuộc group con tương ứng;

• User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc user đang login;

- + Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Set update group:
 - Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;

≡	Viettel a Jiant Setting / Agent Management 🗟 🖞 🕘								3		
E.	Agent management								es		
A	Type to search by quartes								Last Ping 📋 🔍		
P.H	3 res	ult(s)	•						📩 Viev	v column 🗸 🗸	
۲	Sele	cted (2) Set Policy Mov	e to group Set update group	Cancel							
_	0	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION	
<u>►</u>		Localhost.Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test		
◙		Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8	
	0	N/A	 Offline 	N/A	N/A	N/A	N/A	N/A	N/A		
₽ <u>⊾</u>	Displa	ay 3/3 result									
ē											

• Thực hiện Set update group;

Lưu ý:

+ Move to group: Chuyển agent vào các group có trong màn hình Group management;



+ Update group: chuyển agent vào các group lưu trữ các file chạy dưới Agent, mỗi group có các file chạy khác nhau được định nghĩa trong server.

3.7.2 Policy Setting

Mục đích: Hỗ trợ người dùng quản lý danh sách các chính sách thiết lập cho các Agent;

Màn hình giao diện khi người dùng truy nhập vào Setting >> Policy Setting:

aJiant Setting / Pol	icy Setting							王 中。
Policy management							Guidelines	2 + Crea
POLICY NAME	¥	NUMBER OF AGENTS	¥	CREATED TIME	UPDATED TIME	APPLIED TIME	STATUS	Y 3
default		0		28/01/2019 14:11:52	03/12/2020 11:42:43	03/12/2020 11:42:50	Applied	1
full_features		0		09/12/2021 10:20:00	26/05/2022 14:14:25	08/06/2022 13:54:08	Applied	Ø Ü
rull_features_khaitb		0		13/01/2022 13:49:13	13/01/2022 14:15:50	13/01/2022 14:15:53	 Applied 	Ø Û
phula_test		1		14/01/2022 13:17:12	31/03/2022 13:07:30	31/03/2022 13:07:35	Applied	10 1
full_features_v2		0		17/01/2022 14:29:12	08/06/2022 16:02:34	08/06/2022 16:02:37	Applied	a
anhnn_full_features		1		08/02/2022 15:51:36	08/06/2022 16:19:12	08/06/2022 16:19:14	Applied	Ø 0
Full_AV		0		01/03/2022 14:36:25	20/05/2022 15:02:30	20/05/2022 15:02:34	Applied	a ū
full_features_macos		0		11/03/2022 18:22:01	18/03/2022 11:29:29	18/03/2022 11:29:32	Applied	a ū
full_features_anhnn		0		15/03/2022 15:14:32	25/05/2022 17:50:28	25/05/2022 17:50:31	Applied	Ø Ü
		9		17/03/2022 15:12:01	09/06/2022 15:32:37	09/06/2022 15:32:40	Applied	a ū

- 1 Hiển thị danh sách các Policy đã được tạo trên hệ thống. Mỗi 1 policy gồm các thông tin: Tên, số lượng Agent được áp chính sách, Thời gian tạo, thời gian cập nhật, Thời gian áp chính sách, trạng thái (có 2 trạng thái: Applied và Not Applied);
- 2 Tạo mới một chính sách: Click vào nút "Create" hệ thống hiển thị Popup tạo mới chính sách như sau:



Lưu ý: khi tạo mới: Tên Policy không được trùng với các Policy đã tạo trước đó.

Sau khi tạo mới policy thành công hệ thống sẽ hiển thị màn hình chi tiết của 1 policy:



Policy configuration tree			Cancel Save configuration
AGENT	SERVICE LIST	PLUGIN LIST	MODULE LIST
	ConfigurationManager ConnectionManager Updater Drivers Collector	E WindowsEventLog E Antikeylogger © F ProcessAnalysis F PeriodicScan E AdvanceCollector	EventSubcriber EventSubcry EventChannel Ø SysmonConfig
·	e Response	ti LiveResponse ti Containment ti ResponseScenario	
	0 Protection&Prevention	ti ApplicationControl EndpointFirewall E BtsPlugin 3 ti NacAuPlugin	
	E AutoScan =	AviraEngine PerformanceControl	
Configuration guidelines			
- change mode of policy tree configuration: Press In edit mode. Press shock buschesk butten to a	edit configuration button to edit		
After completed editting: Press save configurati	ion button to save configuration or cancel button to comeback previous configura-	ation	

Mỗi 1 policy tạo xong thường có 3 core service mặc định: ConfigurationManager, ConnectionManager, Updater. Lưu ý 3 service này không được phép xóa khỏi hệ thống. Các bước để cấu hình cho 1 policy:

Bước 1: Click nút Edit Config để thay đổi cây Policy

Bước 2: Khi ở trong chế độ Edit, người dùng được phép Check/Uncheck để Add/Remote các service khác:



Bước 3: Sau khi hoàn thành chế độ edit:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



• Người dùng nhấn nút "Save config" để lưu các thay đổi;

Người dùng nhấn nút "Cancel" để hủy thao tác cập nhật Policy và hệ thống quay lại cấu hình trước đấy.

Bước 4: Click icon ³ để thực hiện cấu hình chi tiết cho từng module/Plugin của các Service.

WindowsEventLog: cấu hình các nguồn log lấy dưới Agent:

EventSubcriber: chỉ định các kênh lấy log

Yêu cầu dữ liệu:

+ Trường **event_filter** (lọc theo Event ID): các string con cách nhau dấu phẩy (,);

```
VD: "4": loc các event có eventID = 4
```

"-689": loc các event có eventID # 689

- + Trường providers các string con cách nhau dấu chấm phẩy (;);
- + Các trường bắt buộc phải điền: subs_type, channel;
- + Channel: nguồn log;
- + sub_type:
 - PUSH: khi có event mới → gọi hàm của VCS-aJiant để xử lý;
 - POLLING: VCS-aJiant sau 1 khoảng thời gian chủ động lấy log;
 - PULL: VCS-aJiant chủ động lấy log sau 1 khoảng thời gian;

Sau khi cấu hình xong cần Save lại:

Event subscriber configuration					Clear Save
SUBSCRIBER TYPE	CHANNEL	EVENT FILTER	LEVEL	PROVIDERS	
Click to select 🗸 🗸	Type to	Multi value separated by ,	Select 🗸	Multi value separated by ;	Create
PULL	System	7040	information		ŵ
PULL	System	7040,7045			ŵ
PULL	Security	4624,4625,4698,4699,4700,4701,4702,4697,4738, 4720,4785,4787,5136,5137,5138,5139,5141			ũ
PULL	AdvanceCollector/Operational				ŵ
PULL	ApplicationControl/Operational				ů
PULL	EndpointFirewall/Operational				ŵ
PULL	VEDR	300			Û



+ EventPolicy: Thiết lập policy để enable/disable 1 số loại log mà hệ thống mặc định chưa có;

• Yêu cầu: có ít nhất 1 trường được chọn

Eve	nt policy configuration	
AUD	IT POLICIES	GROUP POLICIES
	Account Logon	Powershell 1
	Account Management	Process Create Command Line
	Detail Tracking	

+ EventChannel: cấu hình chi tiết 1 số nguồn log:

• Retention: có lưu log xoay vòng hay không (Nếu chọn Rentention thì khi file log đầy có log mới sẽ ghi đè lên log cũ nhất);

- Log file path: đường dẫn file log;
- Log file size: kích thước file log;
- Yêu cầu: tất cả dữ liệu đều phải điền;

Event channel configuration				Cite. Save
CHANNEL	LOGROTATE	LOG FILE PATH	LOG FILE SIZE (BYTES)	
Type to	0	Type to	Note: max 52428800(50118) min 10485760(10118)	Create
Chanel		16hffha16	10485760	

+ SysmonConfig: enable/disable sysmon tool trên Agent để lấy log sysmon: Microsoft-Windows-Sysmon/Operational;

s	ysmon	config	guration			Create Save
c	urrent o	onfig				
-	Param	S	-accepteula	Description	disable sysmon	
	#	N0.	PARAMS	DESCRIPTION		#
	0	1	-accepteula	disable sysmon		0 🖬

• Antikeylogger: là một SelfRun Plugin của VCS-aJiant, có nhiệm vụ định kỳ quét toàn bộ máy để tìm ra KeyLogger đang chạy trên máy nếu có;

- Scan setting: cấu hình các loại KeyLogger cần quét;
- Yêu cầu:
 - Scan cycle: min là 1 phút, max là 180 phút;





• Chọn ít nhất 1 loại Keylogger;

+ Whitelist setting: cấu hình whitelist 1 số phần mềm theo đường dẫn của file trên ổ đĩa hoặc theo chữ ký số (cert) của file chạy key logger

- Yêu cầu: điền đầy đủ các trường;
- Sau khi nhập xong cần "Save" lại cấu hình:

White list setting c						
WLTYPE	SCAN TYPE	DATA				
Select 🗸	Select 🗸	Type to	Add new			
WhiteListCer	RawInput	Microsoft Corporation	ũ			
WhiteListPath	HookMessage	C:\users\win 10 64\desktop\unikey40rc2-1101-win64\unikeynt.exe	ū			

+ Self defend: Bổ sung cơ chế chống unintall cho Self Defense;

• Yêu cầu: Lựa chọn Chọn Drivers > Tích chọn Self Defense để bật tính năng Self Defense hoặc bỏ chọn để tắt > chọn Save > chọn Apply Policy;



• Sau khi cập nhật thay đổi xong cần "Save" lại cấu hình:

Bước 5: Click nút Apply Policy để thiết lập Policy vừa được cấu hình cho Agent:

+ Clone chính sách mới: Click vào nút a hệ thống sao chép toàn bộ chi tiết của policy được clone ngoại trừ tên policy.



Clone from test_sample	policy: e	
NAME OF PO	LICY	
Enter name	e of policy	
Cannot edit name Create	of policy after create policy	

+ Xóa chính sách: Click vào nút ^{li} hệ thống hiển thị pop up để người dùng đưa ra quyết định xóa hay không?

Delete Policy		×
	Do you want to delete policy: 0503_test1	
	Cancel Accept	

+ Trường hợp Policy đã có agent được áp, sau khi xóa hệ thống tự động gán "default policy" cho các agent đó;

Delete Policy	×
Do you want to delete policy: <i>hieupc4</i> This policy has been assigned to agent(s). If this policy is deleted, agent(s) will be reset default policy!	to
Cancel Accept	

+ Khi click đúp vào từng bản ghi hệ thống sẽ chuyển tiếp tới trang chi tiết của 1 policy để người dùng xem/ thay đổi cấu hình cho Policy.

3.7.3 Group Management

Cấu hình luật để tự động chuyển policy và chuyển nhóm cho các agent nếu thỏa mãn luật trên Portal, giảm thời gian chuyển policy và chuyển nhóm cho từng agent và đồng bộ policy cho các agent thỏa mãn luật đã cấu hình.

Các tính năng chính trên màn hình này bao gồm:

- + Quản lý nhóm theo cây;
- + Tìm kiếm nhóm;
- + Thêm mới nhóm:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 188



• Tạo luật tự động chuyển nhóm cho agent;

• Tùy chọn cách thức chuyển nhóm (All existing agents, New agents only, All existing and new agents) và gán policy (gán ngay, không gán);

- + Theo dõi các agent thuộc nhóm, tổng số agent thuộc nhóm;
- + Chỉnh sửa nhóm;
- + Xóa nhóm, xóa agent thuộc nhóm;
- 1 Quản lý nhóm theo cây:
 - + User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
 - + User đăng nhập thuộc group default: Hiển thị group default;

+ User đăng nhập thuộc group cha: Hiển thị Group thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc group của user đang login;

Danh sách nhóm hiển thị theo dạng cây bao gồm các nhóm gốc và mỗi nhóm gốc gồm các nhóm con cấp 1, cấp 2...

Mỗi nhóm gồm tên nhóm, thông tin cấu hình của nhóm (rule, policy, apply to), và danh sách agent thuộc nhóm.

Các rule của nhóm là độc lập giữa các nhóm (không có kế thừa cha con). Việc quản lý nhóm theo cây để quản lý dễ dàng hơn khi số lượng agent lớn và có sự phân cấp về quản lý agent theo công ty, phòng, ban...

Khi user thuộc group con, chọn group cha sẽ không nhìn thấy popup group detail

2 – Tìm kiếm nhóm

+ Cách 1: Click vào textbox Search > hiện danh sách các nhóm của tương ứng với user đang login có thể scroll được > Chọn nhóm trong danh sách hiện ra;

+ Cách 2: Click vào textbox Search > nhập ký tự tìm kiếm vào textbox > hệ thống tự động tìm kiếm các bản ghi chứa ký tự nhập vào > Chọn 1 bản ghi phù hợp trong danh sách gợi ý hoặc click Search hoặc Enter sẽ hiện danh sách các bản ghi thỏa mãn;



	viettel aJiant	Setting / Group Man	agement						# 0
Ę	Group managem	ent				Ø Guidelines	vcs_anm		×
A	Type group name to se	arch			٩	Create	Detail information	Agent list	User list
τ_{\pm}	🗅 viettel	>	khoi_phu_thuoc	> 🗅 vcs_an	m				
۲							Rule		0
53							Moving agent to this group if All following condi	tions matched :	
							IP_DCN 10.61.188.2/32		
÷							Policy	Update group	
e <u>r</u>							beta_vcs ~	beta	~
÷							Apply policy immediately when rule matched		
							Apply to Applying to existing agents may take a while, you can che New agents only	ck later.	
								Apply	

Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.

+ Tab thông tin chi tiết hiển thị là Detail, dữ liệu của group đó là Rule, Policy, Apply to;

+ Khi chọn tab Agent list thì dữ liệu thông tin các agent match với group đó.

+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 2 option: Go to group và Delete group.

+ Nếu chọn Go to group thì đưa user đến vị trí của group đó trên cây;

+ Nếu chọn Delete group thì hiển thị popup confirm xóa group.

Khi click vào menu góc phải mỗi ản ghi cũng hiển thị 2 option: Go to group và Delete group.

3 – Thêm mới nhóm:

+ User đăng nhập thuộc group root: Có thể them mới tất cả Group trong;

+ User đăng nhập thuộc group default: Không thể thêm mới;

+ User đăng nhập thuộc group cha: có thể thêm mới group con tương ứng của group thuộc user đang login;



+ User đăng nhập thuộc group một hoặc nhiều con: có thể them mới group con tương ứng của group thuộc user đang login;

Bước 1: Lựa chọn vị trí nhóm sẽ tạo

+ Nếu tạo mới nhóm ở danh sách nhóm gốc, click nút "Add new" góc phải màn hình hoặc hover vào cuối danh sách nhóm gốc trên màn hình, click Add new ;

≡	aJiant	Setting / Group Man	agement						# 0
<u>en</u>	Group manageme	ent				Guidelines	vcs_anm		×
•	Type group name to see	irch				Q Create	Detail information	Agent list	User list
	🗅 viettel	>	khoi_phu_thuoc	>	C vcs_anm				
۲							Rule		D
							Moving agent to this group if All Y	ollowing conditions matched :	
							IP_DCN 10.61.188.2/32		
¢۵.							Policy	Update group	
Ø							beta_vcs	∨ beta	~
							Apply policy immediately when rule matched		
							Apply to		
							Applying to existing agents may take a whi	le, you can check later.	
								Apply	

+ Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2... thì click vào nhóm cha sau đó click "Create" trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click "Create";

Bước 2: Nhập tên nhóm và cấu hình luật;

Lưu ý: tên và luật cấu hình không được trùng với tên và luật đã có.

- + Nếu chọn toán tử "All": luật thỏa mãn khi cả 2 trường được thỏa mãn;
- + Nếu chọn toán tử "Any": luật thỏa mãn khi 1 trong 2 hoặc cả 2 trường thỏa mãn;



2000 C	Group managemen Type group name to searc ettel	it h				0			
▲ r±	Type group name to search	h				Guideliner	EDR_group		
F#	ettel	>			2	Create	Detail information	Agent list	User list
			▶ Wol_phu_thusc	C vojanni			Detail Information Rule Moving agent to this group if All following co p following co Add rule Apply policy immediately when rule matched Apply to All existing and new agents	Agent list dtions matched : Update group	User list

Bước 3: Lựa chọn policy và loại agent sẽ apply policy nếu thỏa mãn rule:

Sau khi click Apply kiểm tra agent được chuyển nhóm trong tab Agent list: danh sách agent thỏa mãn luật và được chuyển nhóm sang nhóm vừa thêm. Tùy thuộc vào lựa chọn ở phần "Apply to" để chuyển nhóm cho các agent trong hệ thống:

+ All existing agents: chuyển nhóm cho tất cả agent đang tồn tại trong hệ thống, các agent cài mới sau khi apply nếu có khớp luật cũng KHÔNG chuyển nhóm;

+ New agents only: chỉ chuyển nhóm cho các agent cài mới sau khi Apply, các agent đang tồn tại trên hệ thống nếu khớp luật cũng KHÔNG chuyển nhóm;

+ All existing and new agents: chuyển nhóm cho tất cả agent đang tồn tại trong hệ thống và agent cài mới sau khi apply nếu khớp luật;

Lưu ý:

+ Nếu chọn checkbox "Apply policy now when rule matched", sau đó click "Apply" thì với các agent được lựa chọn Apply sẽ kiểm tra các giá trị nếu khớp với luật đã cấu hình sẽ chuyển policy cho agent sang policy đã chọn ở mục "Policy", đồng thời chuyển nhóm;

Trong trường hợp ko chọn checkbox trên thì sau khi Apply, các agent được chọn Apply chuyển nhóm nhưng không chuyển policy, tức là agent giữ nguyên policy trong



khi chuyển sang nhóm có policy khác; với các agent cài mới nếu khớp luật thì chuyển nhóm và được áp policy "**default**" do không chọn checkbox > áp policy mặc định;

+ Nếu agent mới khớp luật của nhiều nhóm sẽ ưu tiên chuyển vào nhóm được tạo mới nhất, không tính thời gian sửa nhóm.

- 4 Sửa nhóm: có thể lựa chọn sửa 1 hoặc 2 hoặc cả 3 thành phần trong một nhóm: Rule, Policy, Apply to
 - + User đăng nhập thuộc group root: Có thể sửa tất cả group trong hệ thống;
 - + User đăng nhập thuộc group default: Không được sửa group default;

+ User đăng nhập thuộc group cha: Có thể sửa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả group thuộc user đang login;

+ Để sửa Rule (luật) của nhóm, click vào icon Edit > Chỉnh sửa luật của nhóm sau đó click Save > Sau đó có thể chỉnh sửa ở mục "Policy" và "Apply to" rồi click Apply;

vcs_anm		×
Detail information	Agent list	User list
Rule Moving agent to this group if All	following conditions matched :	Edit 🤌
Policy	Update group	
beta_vcs	∽ beta	~
Apply to	hile wu can check later	
New agents only	V	



vcs_anm			×
Detail information	Ag	ent list	User list
Rule			Cancel Save
Moving agent to this group if All v fol	llowing conditions	matched :	
IP DCN • 10.61.188.2/3	2		
Add rule			
Policy		Update group	
beta_vcs	~	beta	~
Apply policy immediately when rule matched			
Apply to			
New agents only	~		
		Apply	

Lưu ý:

+ Trường hợp sửa các thành phần của nhóm (Rule, Policy hoặc Apply to) sau đó ko click Apply thì nội dung chỉnh sửa đã được lưu lại, nhưng không cập nhật Agent list. Với các Agent cài mới thì xử lý như sau:

 Chuyển nhóm: phụ thuộc Agent mới có được chọn ở mục "Apply to" hay không, nếu được chọn sẽ kiểm tra phía Agent, khớp luật của nhóm sẽ được chuyển vào nhóm;

 Apply policy: policy của agent phụ thuộc việc chọn checkbox "Apply policy now when rule matched", nếu checkbox được chọn thì sẽ apply policy của nhóm, nếu không được chọn sẽ áp policy "default" do không chọn checkbox sẽ áp policy mặc định.

+ Trường hợp sửa xong các thành phần của nhóm rồi click Apply thì nội dung chỉnh sửa được lưu lại, đồng thời nếu có lựa chọn "All existing agents" trong

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 194



phần "Apply to" thì thực hiện quét thông tin toàn bộ agent trong hệ thống và chuyển nhóm cho agent, sau đó cập nhật Agent list.

Đối với Agent mới xử lý tương tự như trên.

- 5 Xóa nhóm hoặc xóa agent khỏi nhóm:
 - + User đăng nhập thuộc group root: Có thể xóa tất cả group trong hệ thống;
 - + User đăng nhập thuộc group default: Không được xóa group default;

+ User đăng nhập thuộc group cha: Có thể xóa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể xóa tất cả group thuộc user đang login;

Để xóa nhóm click vào nhóm cần xóa, click "Delete" sau đó click "OK" trên màn hình confirm. Sau khi xóa 1 nhóm thì các agent thuộc nhóm sẽ chuyển về nhóm mặc định, nhóm "default", policy giữ nguyên;

≡	viettel aJiant	Setting / Group Man	nagement							ŧ	8 0
ē.	Group managem	ent				2 Suidelines	huyenpk_group				×
A	Type group name to see	arch				Q Delete Creste	Detail informa	ition	Agent list	User list	
-7 <u>+</u>	🗅 admin	>	🗅 new_grou	p >	huyenpk_group						
۲	🗅 default		test_wild	ard			Rule				0
	🗅 global		hbc_serv	r			Moving agent to this gro	up if All V following conditi	ons matched :		
			auto_test	>			IP_DCN	123.123.12.31/241			
•			no_group	>			Palicy		Undate group		
¢λ			C chuyen_t	ist >	1 Delete		×		opuate group		
ē								~			~
					Are you sure you w	ant to delete group : huyenpk_gro	oup?	y when rule machieu			
						3					
						Cancel Delete	ager	nts may take a while, you can checi	k later.		
							All existing and new a	gents ~			
									Apply		



Để xóa Agent khỏi nhóm thì click vào tab Agent list, click icon "x" để xóa agent khỏi nhóm. Sau khi xóa agent khỏi nhóm thì agent được chuyển về nhóm mặc định: "default", policy giữ nguyên

vcs_anm					
Detail information		Agent list		User list	
50/279 agent(s)		Search agent			
AGENT ID	HOSTNAM	IE GROUP	STATUS	POLICY	#
4AE8D11BFB5037899FD20F5CEDF	ANM-HOANGNI	D31 vcs_anm	• Offline	full_features_with_autoscan_selfdefense	×
\1B37DBD39D0F632D9F7BEFBE421	ANM-SANGLV11	1 vcs_anm	• Offline	full_features_with_autoscan_selfdefense	×
75E895D48390F5C642FC57AD62C	ANM-THONGNE	D7 vcs_anm	• Offline	full_features_with_autoscan_selfdefense	×
(F8AF3B15A9A343F992D3596EBA3	ANM-HOABT21	vcs_anm	• Offline	full_features_with_autoscan_selfdefense	×
2FA6F1E3E016C748600CAF0C1A7	ubunbu-18	vcs_anm	• Offline	full_features_3.3.0	×
SCA1E94EC4C99ACE5EDB202FD7E	ANM-ANHNN19	o vcs_anm	• Offline	full_features_with_autoscan_selfdefense	×
9ACE6C4888F8E1F04428BC8BDD1	IS-LANNT	vcs_anm	• Offline	beta_vcs	×
343E35A30D5CC8EFC65AC7A83EB1	ANM-THANGNM	M14 vcs_anm	• Offline	full_features_with_autoscan	×
A04CF97FF6250F800308CE68352	ANM-DUCDH8	vcs_anm	• Offline	full_features_with_autoscan_selfdefense	×

Lưu ý: trường hợp xóa một nhóm cha:

+ Xóa tất cả nhóm con;

+ Chuyển tất cả agent của nhóm cha và các nhóm con về nhóm mặc định: "default";

- + Giữ nguyên policy của các agent trong nhóm cha và con;
- 6 Thêm mới user vào group



aJiar	nt	s	etting /	Group Management								* 0
Group ma	anager	nen	ŭ.					G uidelines	admin			×
Type p	Add u	iser	to gro	oup						Cancel Save	× srlist	Alphante seaser
-		Use	r avai	lable to add to group			User i	group			us ictive	* *
0			NO.	USERNAME	FULLNAME	EMAIL	. N). USERNAME	FULLNAME	EMAIL	tive	×
-	2		1	admin		t	0.1	iml_edr	iml_edr	iml_edr@ajiant.com	tive	×
-			2	alert_viewer	alert_viewer	alert_viewer@ajiant.com	□ 2	is_toanbd	is_toanbd@adf.com	is_toanbd@adf.com	tive	×
		ò	3	anhbd25		t1	3	khaitb	Trần Bá Khai	khaitb@viettel.com.vn		
			4	anhnn		anhnn@gmail.com	. 4	thanhln9	thanhIn9	thanhIn9@viettel.com.vn		
			5	anhnn19		tba						
			6	anhyn		anhvn@gmail.com						
			7	autotest151	fullname	clint.kris@yahoo.com						
			8	autotest281	fullname	marjory.ritchie@hotmail.com						
			9	autotest289	fullname	alec.stamm@gmail.com						
			10	autotest35	fullname	alica.lueilwitz@gmail.com						
		D,	11	autotest362	fullname	mao.huel@hotmail.com						
			12	autotest419	fullname	rachael.pouros@hotmail.com						
			13	autotest457	fullname	clyde.grady@gmail.com						
			14	autotest5	fullname	mckinley.ratke@gmail.com						

Danh sách user:

- + User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login:

=	aJiant Setting / C	Group Man	agemen	at								
2	Group management					Guidelines	test	t_wildcard				
	Type group name to search					Q Delete Create		Detail information	1	Agent list	User list	
	🗅 admin	>		new_group			3 ut	ser(s)		Type to filter user		1
	C default		D	test_wildcard			NO.	USERNAME	FULLNAME	EMAIL	STATUS	
	🗅 global			hbc_server			1	anhvn	anhvn	anhvn@gmail.com	Active	
				auto_test	>		2	autotest107	fullname	jackie.anderson@yahoo.com	 Active 	
				no_group	>		3	autotest11	fullname	sondra.trantow@yahoo.com	 Active 	
				chuyen_test	>							

3.7.4 Account Management

Quản lý các tài khoản, quyền, nhóm quyền của hệ thống Portal

Page | 197



3.7.4.1 *Permission management*

Quản lý các quyền truy cập vào tài nguyên (API) của hệ thống. 1 permission là quyền truy cập vào 1 tài nguyên xác định (API) của hệ thống; Các chức năng chính trên màn hình này:

- + Quản lý các permission;
- + Tìm kiếm permission;
- + Xóa permission;
- 1 Quản lý các permission: hiển thị toàn bộ các permission của hệ thống. Trong trường hợp xóa permission trên màn hình này, khi thực hiện các chức năng trên portal mà bị thiếu permission thì sẽ tự động thêm permission đã xóa trên màn hình quản lý Permission
- 2 Tìm kiếm permission: nhập ký tự tìm kiếm vào texbox Search > click
 Enter hoặc nút "Search" => hiển thị danh sách permission thỏa mãn

≡	aJi	ant Setting / Account Management / Permission Management			* 0
ē.	Permis	ision management			Guidelines
A	Type pe	ermission name to search		•	2 Q
÷	56 resu	ult(s)			
۲	NO.	PERMISSION NAME	DESCRIPTION	ROLE LIST	ACTION
_	1	agent_management_manage		manage_agent_management, manage_containment, manage_deploy_tool, root	0 Î
<u>>-</u>	2	agent_management_read		liennt_test, manage_investigation_result, root, view_agent_management,View	0 11
9	3	agent_policy_manage		manage_policy_management, root	0 û
	4	agent_policy_read		liennt_test, root, view_policy_management	0 Û
Ēà	5	agent_read			0 Ü
ē	6	alert_read			0 û
	7	alert_manager		manage_alert, root	0 Î
	8	alerts_read		root, view_alert	0 11
	9	appctrl_handler_manage		manage_appctrl_handler, root	0 D
	10	appctrl_handler_read		root, view_appctrl_handler	0 11
	11	artifact_handler_manage		$manage_event_search, manage_investigation_result, manage_process_analysis, root$	0 11
	12	artifact_handler_read		root, view_investigation_result, view_irflow, view_process_analysis	0 Î
	13	artifact_manage		manage_detection, root	0
	14	containment_manage		manage_containment, manage_irflow, root	0 11
	15	containment_read		root, view_containment, view_irflow	0 11
	16	correlation_manage			0 Ü
	17	correlation_read			0 û
	18	dashboard_read		default, root	0 Î
	19	deploy_tool_handler_manage		manage_deploy_tool, manage_investigation_tool, manage_irflow, root	0 Ü
	20	deploy_tool_handler_read		$manage_investigation_result, root, view_deploy_tool, view_investigation_result, View_in$	0 Û
	21	endpointfw_handler_manage		liennt_test, manage_endpointfw_handler, root	0 Î
	Showing	(25/56 result(s)			

3 – Xóa permission: click icon "Delete" > click "OK" trên màn hình confirm là xóa thành công:



=	aJiant	Setting / Account Management / Permission Management				# 0
<u>e</u> 1	Permission mana	agement				Guidelines
A	Type permission name	to search				Q
ц.	56 result(s)					
a	NO. PERMISSION N	IAME	DESCRIPTION	ROLE UIST		ACTION
	1 agent_mana	agement_manage		manage_a	gent_management, manage_containment, manage_deploy_tool, root	0 0
	2 agent_mana	igement_read		liennt_test	0 10	
	3 agent_polic	y_manage		manage_p	0 11	
	4 agent_polic	y_read		liennt_test	0 11	
EX	5 agent_read		Delete	×		0 1
ē	6 alert_read		Delete			0 11
	7 alert_manag	ger			ert, root	0
	8 alerts_read		Are you sure you want to delete permission : agent_read ?		ilert	0 11
	9 appctrl_han	dler_manage			pctrl_handler, root	0 11
	10 appctrl_han	dler_read	Cancel Delete 2		ippctrl_handler	0 11
	11 artifact_han	dler_manage			ent_search, manage_investigation_result, manage_process_analysis, root	0 11
	12 artifact_han	idler_read		root, view_	investigation_result, view_irflow, view_process_analysis	0 11
	13 artifact_mar	nage		manage_d	etection, root	0 11
	14 containmen	t_manage		manage_c	ontainment, manage_irflow, root	0 11
	15 containmen	t_read		root, view_	containment, view_irflow	0 11
	16 correlation_	manage				0 11
	17 correlation_	read				0 11
	18 dashboard_	read		default, roi	x	0
	19 deploy_tool	_handler_manage		manage_d	eploy_tool, manage_investigation_tool, manage_inflow, root	0
	20 deploy_tool	_handler_read		manage_in	vestigation_result, root, view_deploy_tool, view_investigation_result,View	0 11
	21 endpointfw	_handler_manage		liennt_test	, manage_endpointfw_handler, root	0 11
	Showing 25/56 result	(5)				

3.7.4.2 Role Management

Quản lý các role (nhóm quyền hay nhóm permission) của hệ thống; Các chức năng trên màn hình này bao gồm:

- + Quản lý danh sách role:
 - User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống;
 - User đăng nhập thuộc Role default: Hiển thị Role default;

 User đăng nhập thuộc Role cha: Hiển thị tất cả Role thuộc của user đang login và group con tương ứng;

User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login;

- + Tìm kiếm role;
- + Thêm mới role;
- + Xóa role.
- 1 Quản lý danh sách role: quản lý danh sách role theo dạng cây. Có 2 role
 ở gốc mặc định đã tạo sẵn: role "default" và "root"

Page | 199



+ Role "default": User có quyền "default" chỉ có quyền truy cập vào Portal, không có quyền xem dữ liệu hoặc thao tác chức năng;

+ Role "root": bao gồm toàn bộ các role của hệ thống, User có role "root" có toàn bộ quyền sử dụng tất cả chức năng trên Portal;

+ Click vào 1 role sẽ hiển thị thông tin chi tiết của role. Một role sẽ bao gồm các thông tin: tên role, danh sách các permission, danh sách User (tài khoản) chứa role, role cha hoặc danh sách role con (nếu có)

2 – Tìm kiếm role

+ Cách 1: Click vào textbox Search > hiển thị danh sách các role trong hệ thống và có thể scroll được danh sách role > Lựa chọn role trong danh sách hiện ra

+ Cách 2: Click vào textbox Search > Nhập ký tự tìm kiếm vào textbox > Hệ thống lọc ra các role chứa ký tự tìm kiếm > chọn role trong danh sách đã lọc hoặc click Enter hoặc click nút "Search"

≡	viettel aJiant	Setting / Account Management / Role Management		× 0
ē.	Role Managemer	it	 @ Guidelines	root ×
A	Type role name to sear	ch	Create role	Detail information User list
,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,	For enangement	nagement andler Imanage_deploy_tool manage_deploy_tool manage_detection manage_event_search manage_group_management manage_group_management manage_lowestigation_result	Costerior	root x Detail information User list Detail information User list Rede detail information Rute root (root) Dorson Detection Detail information Permission list read containment_read containment_manage agent_management_manage agent_management_read agent_management_manage agent_policy_read agent_management_manage agent_manage agent_mana
		manage_investigation_tool manage_inflow manage_inflow		update_group_manage appcrti_handier_read appcrti_handier_manage endpointhv_handier_read endpointhv_handier_manage violation_statistic_handier_read software_statistic_handier_read software_read patch_statistic_handier_read patch_read proxy_read proxy_manage alter_read enhance_alter_mad databload_read correlation_manage correlation_read
		manage_priv(epponte manage_permission_management manage_process_analysis		

- Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.
 - Tab thông tin chi tiết hiển thị là Detail, dữ liệu của role bao gồm thông tin role và các permission của role đó;



o Khi chọn tab User list là danh sách User chứa role;

+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị Go to role. Click vào "Go to role" đưa về danh sách role dạng cây ban đầu;

+ Khi click vào menu góc phải mỗi bản ghi cũng hiển thị option: Go to role;

3 – Thêm mới role:

+ User đăng nhập thuộc group root: Có thể them mới tất cả role trong các cây dữ liệu;

+ User đăng nhập thuộc group default: Không thể thêm mới;

+ User đăng nhập thuộc group cha: Có thể thêm mới role con tương ứng của group thuộc user đang login, không thể them mới role cùng cấp;

+ User đăng nhập thuộc group một hoặc nhiều con: có thể them mới group con tương ứng của group thuộc user đang login.

Bước 1: Có các cách tạo mới role như sau:

Click vào 1 role sau đó hover vào cuối danh sách role chọn "Add new" để tạo role cùng cấp với role đã chọn

Click "Add new" trên màn hình để tạo role con của role đã chọn

Chuột phải vào 1 cột trong cây chọn "Add new role"

Sau đó nhập tên role không trùng với tên role đã tồn tại trong hệ thống.



=	aJiant Setting / Account Ma	nagement / Role Management		÷	0
	Role Management Type role name to search	۵ ۵	Guidelines Create role	root	×
		view_containment view_deficion_tool view_deficition view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_endpointdw_handler view_investigation_result view_investigation_tool view_investigation_tool view_view_intow view_view_intow view_view_point_management view_response_conario view_response_conario view_rupdate_group view_rupdate_group view_rupdate_group	0	Declar information Definit INME mot (root) DOUMN mot (root) DOUMN mot (root) DESCRIPTION mot roote Permission list mot (root) agent_management_manage agent_policy_manage Inst_met_manage agent_policy_manage inflow_manage agent_policy_manage inflow_manage agent_management_read agent_management_manage agent_policy_manage inflow_manage response_scenario_manage agent_management_manage agent_policy_manage agent_management_manage agent_policy_manage agent_scenario_manage agent_policy_manage agent_scenario_manage agent_read group_manage group_manage group_manage goop_read user_read antst_read group_manage apert_handle_manage update_manage user_read group_manage apert_handle_read approx_tol_handler_manage apert_handler_manage update_manage update_read <t< th=""><th>0</th></t<>	0

Bước 2: Click icon Edit để thêm thông tin permission cho role > Lựa chọn permission để thêm vào role > click Save:

- + User đăng nhập thuộc group root: Có thể sửa tất cả role trong hệ thống;
- + User đăng nhập thuộc group default: Không được sửa role default;

+ User đăng nhập thuộc group cha: Có thể sửa tất cả role thuộc đang login và role con role ;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả role thuộc user đang login;

Lưu ý: danh sách permission của role con là tập con của role cha. Tức là khi muốn lựa chọn permission gán cho role con thì role đó phải thuộc danh sách permission của role cha.



view_irflow			×
Detail ir	nformation	User	list
Role detail information			0
NAME	view_irflow (view_	irflow)	
DOMAIN			
DESCRIPTION	view_irflow		
Permission list irflow_read contain	nment_read process_analysis	_read live_response_read	artifact_handler_read
response_scenario_read	deploy_tool_handler_read	event_read	

Detail in	formation	User list
ole detail information		Cancel
Name	view_live_response	•
Domain		
Description	view_live_response	
ermission list		2
ermission list live_response_read × read		2
ermission list live_response_read × read containment_read		2
ermission list live_response_read × read containment_read containment_manage		2
ermission list	ad	2
ermission list	ad	2



- + User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;





+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

_=▶	viett aJii	ant	Set	tting / Account Ma	anagement / Role Management									8 0
ē.	Role M	anagem	ent						Guidelines	view_live_response				×
▲ "≞	Type ro	Add	Jser Int	to Role								Cancel Save		edate user
۲													s	ACTION
5			ser avaita	able to add into role	t (3 selected)			User in role					ive	×
		2) NO.	USERNAME	FULLNAME	EMAIL		NO.	USERNAME	FULLNAME	EMAIL		ive	×
			1	admin	Supper Admin	admin@ajiant.com		1	bichpt3	Bich PT	bichpt@gmail.com			
成		C	2	alert_viewer	alert_viewer	alert_viewer@ajiant.com		2	viewer	quyền view	aaaa@gmail.com			
		0	3	anhvn	anhvn	anhvn@gmail.com								
ē		8	4	autotest107	fullname	jackie.anderson@yahoo.com								
			5	autotest11	fullname	sondra.trantow@yahoo.com								
			6	autotest136	fullname	howard.mcclure@hotmail.com								
		0	7	autotest156	fullname	timothy.jerde@yahoo.com	3_							
			8	autotest161	fullname	jaunita.gislason@gmail.com	»							
			9	autotest167	fullname	jeannette.hirthe@yahoo.com								
		0	10	autotest27	fullname	joe.kuvalis@yahoo.com								
			11	autotest271	fullname	hank.moen@gmail.com								
		0	12	autotest285	fullname	karlyn.bayer@gmail.com								
		C	13	autotest300	fullname	douglass.sauer@yahoo.com								
		C	14	autotest34	fullname	enriqueta.beahan@yahoo.com								
		C	15	autotest416	fullname	natosha.ziemann@hotmail.com								
			16	autotest419	fullname	dillon.purdy@hotmail.com								
		C	17	autotest436	fullname	londa.rempel@hotmail.com								
			18	autotest44	fullname	tanner.okeefe@yahoo.com								
			19	autotest459	fullname	benton.walker@hotmail.com								
				11 1000										
					view_response_scenario									
					view_role_management									

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login;

 4 – Xóa role: click vào role cần xóa, chọn "Delete" > click OK trên màn hình confirm



≡	aJiant	Setting / Account M	lanagement / Role Management					# 0
ē	Role Management				Guidelines	New_Role1		×
A	Type role name to search.				Q Delete Create role	Detail info	ormation	User list
-	🗅 default		🗅 hbc_t	🗅 Haites	• • • • • • • • • • • • • • • • • • •			
	🗅 root	>	□ liennt_tes >	liennt_permission		Role detail information		0
<u> </u>			manage_agent_management	Liennt_t1234566		DOMAIN	New_Role1 (new_role1)	
			manage_alert	🗅 Na_test		DESCRIPTION	New_Role1	
0			manage_appctrl_handler	C New_Role1		Permission list		
Eλ			manage_containment					
ē			manage_deploy_tool					
			manage_detection	Delete		×		
			manage_endpointfw_handler		Are you sure you want to delete role : New Role1 ?			
			manage_event_search					
			manage_group_management		Cancel Delete			
			manage_investigation_result			-		
			manage_investigation_tool					
			manage_irflow					
			manage_live_response					
			manage_permission_management					
			manage_policy_management					
			manage process analysis					
			C1 manage role management					

Lưu ý: Sau khi xóa 1 role, tất cả các user sử dụng role này được thay đổi: Nếu user X nằm trong role bị xóa và user X chỉ có 1 role thì chuyển user X về role mặc định, ngược lại, nếu user X có nhiều role thì chỉ loại bỏ role bị xóa ra khỏi danh sách role của user X.

3.7.4.3 User management

Quản lý các tài khoản đăng nhập vào hệ thống Portal VCS-aJiant. Các chức năng chính trên màn hình này gồm có:

- + Tìm kiếm tài khoản;
- + Thêm mới tài khoản;
- + Chỉnh sửa tài khoản;
- + Xóa tài khoản;
- 1 Tìm kiếm tài khoản: click vào textbox Search > hiện danh sách các tài khoản trong hệ thống > Lựa chọn tài khoản cần tìm kiếm trong danh sách hoặc nhập ký tự <text> vào textbox để lọc bớt các tài khoản> Click "Search" hoặc chọn tài khoản cần tìm trong danh sách các tài khoản đã được lọc

Page | 205



Ę,	User	rmanagement					Guidelines
A	Тур	e username to search					Q
H ¹	44 -	result(s)					+ Create
۲	NO	USERNAME	FULLNAME	EMAIL	LAST LOGON	STATUS	ACTION
5	1	admin		t	N/A	Active	0 û
	2	alert_viewer	alert_viewer	alert_viewer@ajiant.com	N/A	C Active	0
Ø	3	anhbd25		11	N/A	C Active	0 🗊
Ē.	4	anhnn		anhnn@gmail.com	N/A	Active	0 11
	5	anhnn19		tba	N/A	Active	0 11
<u>s</u>	6	anhvn		anhvn@gmail.com	N/A	C Active	0 Ū
	7	autotest151	fullname	clint.kris@yahoo.com	N/A	C Active	0
	8	autotest281	fullname	marjory.ritchie@hotmail.com	N/A	C Active	0 û
	9	autotest289	fullname	alec.stamm@gmail.com	N/A	Active	0 🗊
	10	autotest35	fullname	alica.lueilwitz@gmail.com	N/A	C Active	0 Ū
	11	autotest362	fullname	mao.huel@hotmail.com	N/A	Active	0 11

Thêm mới tài khoản: click "Create" > Nhập thông tin vào form hiện lên > click "Next"

	Guidelines
	Q
	+ Custo
STATUS	ACTION
Active	0 🗊
Active	0 🗊
Active	0 🗊
Active	0 🗉
Active	0 0
Active	0 11
Active	0 🗊
C Active	0 🗊
Active	0 🗊
Active	0 11
Active	0 11
Active	0 î
Active	0 1
Active	0 11
Active	0 11
Active	0
Active	0 0
Active	0
Active	0
Active	
Active	
Active	
	SUUS Adve A

+ Lựa chọn role (nhóm quyền) sẽ gán cho tài khoản, sau đó click "next";

+ Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó:

- User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống;
- User đăng nhập thuộc Role default: Hiển thị Role default;

 User đăng nhập thuộc Role cha: Hiển thị tất cả Role thuộc của user đang login và group con tương ứng;

Page | 206



• User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login;

Ξ÷.	66 n	esult(s)							+ Create
۲	NO.	USERNAME	FULLNAME		EMAIL	LAST LOGON		STATUS	ACTION
	1	admin	Supper Admin		admin@ajiant.com	N/A		Active	0 11
	2	alert_viewer	alert_viewer		alert_viewer@ajiant.com	N/A		C Active	0 🗊
	3	anhvn	E dia li suo				v	C Active	a la constante da la constante
Ē.	4	autotest107	Edit User				^	C Active	- a 🗈
R	5	autotest11	User information Role Group					C Active	0 🗊
ι.Ψ.	6	autotest136						C Active	0 E
	7	autotest156	Username	admin				C Active	0 î
	8	autotest161	Fullname	Supper Admin				C Active	0 🗊
	9	autotest167	Email	admin@ejiant.com				Active	0 🗊
	10	autotest27	Shite	Antina O Develo				C Active	0 0
	11	autotest271	Status	Change password	e			Active	0
	12	autotest285						C Active	0 E
	13	autotest300			Cancel Next			C Active	0
	14	autotest34			2			C Active	0 🗊
	15	autotest416	fullname		natosha.ziemann@hotmail.com	N/A		C Active	0 🗄
	16	autotest419	fullname		dillon.purdy@hotmail.com	N/A		Active	0 î

Trên màn hình add role cho User, có thể tìm kiếm các role tương tự phần tìm kiếm tài khoản, sau khi nhập các ký tự tìm kiếm vào textbox "Search" > click icon Search hoặc Enter hiện màn hình các role thỏa mãn điều kiện tìm kiếm;

Edit User								×
User information Role Gr	NP		Type role neme to search	۹	4 role selecte	ted		
🗅 default 🖾	hbc_test				default			
⊃ reet 💶 🦕	E liennt_test	••			Permission	ons: read dashboard_read		
	manage_agent_management				Permission	ons: agent_management_manage		Ŷ
	manage_alert				manage_al	alert		×
	🗅 manage_appctrl_handler				Permission	ons: alerts_manage irflow_manage		
	manage_containment				Permission	_sppctrl_handler ons: _sppctrl_handler_manage _update_group_manage		×
	manage_deploy_tool						l	
	manage_detection							
	manage_endpointfw_handler							
	manage_event_search							
	manage_group_management							
	manage_investigation_result							
	manage_investigation_tool							
	manage_inflow							
	manage_live_response							
	manage_permission_managem	nt 🗌		2				
			Back	Next				

+ Click chọn checkbox tương ứng với role cần thêm, sau đó click "Go to role" để về màn hình danh sách role ban đầu, sau đó click "Create" để tạo tài khoản;

+ Lưu ý: Tài khoản đang đăng nhập tạo 1 tài khoản mới chỉ tạo được các tài khoản chứa các role con thuộc danh sách role mà tài khoản đang đăng nhập được cấp;

+ Lựa chọn group sẽ gán cho tài khoản, sau đó click "Create";

+ Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó;



- User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
- User đăng nhập thuộc group default: Hiển thị group default;

 User đăng nhập thuộc group cha: Hiển thị Group thuộc group của user đang login và group con tương ứng;

User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc group của user đang login;

Edit User			×
			-
User Information Role Group	Type group name to search Q	4 group selected	0
admin 🛛 🖸		test_group3 admin / chayen_test / test_group2	×
default		n- chuyen test	×
		admin -	e 2
J pros		C admin	×
1		C root	×
1 BODIELI			
			2
2 accesso			2 I.
			 2
1. Company of the second sec			2
14 microsoft.co			- 1
 parents 			 2
2 (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (1999) (199			- 2
Statement (2 I I
			- E
2 access**			
			- I
			< C
	Back Cancel Sove		

+ Click chọn checkbox tương ứng với group cần thêm, sau đó click "Go to role" để về màn hình danh sách group ban đầu, sau đó click "Create" để tạo tài khoản.
 Xóa tài khoản: click vào icon Xóa sau đó click OK trên màn hình confirm
 Kiểm tra hiển thi icon xóa:

+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login;



NO. USERNAME	PULLNAME	DIAL		LAST LODON	STATUS	ACTION
1 admin	Supper Admin	admin@ajiant.com		N/A	Active	0 0
2 alert_viewer	alert_viewer	alert_viewer@ajiant.com		NA	Active	0 0
3 anhvn	anhvn	anhvn@gmail.com		29/04/2022 10:44:40	Active	/ 0
4 autotest107	fullname	jackie.anderson@yahoo.com		NA	Active	/ 0
5 autotestii	fullname	sondra.trantow@yahoo.com		n(A	Active	10
6 autotest136	fullname	howard.mcclure@hotmail.com		NA	Active	/ 0
7 autotest156	fuliname	timothy.jerde@yahoo.com		NA	Active	· •
8 autotesti61	fullname	jaunita.gislason@gmail.com		N(A	Active	/ 0
9 autotest167	fullname	Delete	×	NA	Active	0
10 autotest27	fullname	- Citra		N/A	Active	0 0
11 sutotest271	fullname	Are you sure you want to delete user : anhwn ?		N/A	Active	/ 0
12 autotest285	fullname			NA	Active	0
13 autotest300	fullname	Cancel Diete 2		N(A	Active	10
14 autotest34	fullname			NA	Active	/ 0
15 sutotest416	fullname	natosha.ziemann@hotmail.com		NA	Active	0 0
16 autotest419	fullname	dillon.purdy@hstmail.com		N/A	Active	0

3.7.5 Update management

3.7.5.1 *Update groups*

Mục đích: là tính năng cho phép quản lý, tạo mới và cập nhật các Update Group (Chia các Agent thành các nhóm cập nhật, giúp dễ dàng phân chia, quản lý)

- 1 Tìm kiếm:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

Upda	ate groups Packages						
٩	Search						٩
8	group(s)					•	New update group
	Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
L.	Jpdate_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
	Jpdate_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
e	alpha	Group alpha test team agent core	release	0	Update manually	N/A	
t	peta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
0	congne	Update group congnc	N/A	0	Update manually	N/A	
F	phula_test	Update group phula_test	release	0	Update manually	N/A	
r	elease	Update group release	release	4	Update manually	N/A	
t	lest	Update group test	test	0	Update manually	N/A	

- **Bước 4:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- Bước 5: Nhập từ khóa tìm kiếm vào ô textbox và chọn nút "Search"



Upc	date groups Packages				0		
	Q update						© C
	8 group(s) Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
	Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
	Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
	alpha	Group alpha test team agent core	release	0	Update manually	N/A	
	beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
	congne	Update group congnc	N/A	0	Update manually	N/A	
	phula_test	Update group phula_test	release	0	Update manually	N/A	
	release	Update group release	release	5	Update manually	N/A	
	test	Update group test	test	0	Update manually	N/A	

- 2 Thêm mới Update groups:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

Update groups Packages						
Q Search						٩
8 group(s)						New update group
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

Bước 4: Chọn nút "New update group", hệ thống hiển thị màn hình thêm mới Update Group;



Update groups Packages		2	
Q Search		Create new group ×	
Name of update group	Description	Description (optional)	Upcoming package Action
Update_1hour Update_specific	update sau 1 hour Update vao chu nhat hang tuan	About your update group	se N/A 3.3.4 (03/07/2022 08:00:00)
alpha beta	Group alpha test team agent core Group Beta update ngay		N/A N/A
congno	Update group congno	0/2000 Package version	N/A N/A
release	Update group release	Choose the package version for this group. Only deployed and not removed package versions related to agents can be shown here.	num N/A
text	Update group test	2.3.7 (lates) ✓ Update schedule When a new package version is deployed: ○ Update manually (change in the section "Package version" above) ○ Update automatically Time to update Update automatically Digital With the section "Package version" above) ○ Update automatically ☐ Update automatically ○ Update at a specific time ① Cancer	NA

- **Bước 5:** Nhập thông tin thêm mới Update Group và chọn nút "Create". Hệ thống ghi nhận và quay về màn hình danh sách Update Group.
 - 3 Cập nhật Update groups:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

Update groups Packages						
Q Search						Q
8 group(s)						New update group
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congne	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

Bước 4: Tại bản ghi cần cập nhật/ chỉnh sửa thông tin, chọn icon "Cập nhật" thông tin Update Group:



A	Update groups Packages						
e الار	Q update						© Q
	8 group(s)						New update group
	Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Č	Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
*	Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	Ð
¢.	alpha	Group alpha test team agent core	release	0	Update manually	N/A	
CA.	beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
Q	congne	Update group congnc	N/A	0	Update manually	N/A	
	phula_test	Update group phula_test	release	0	Update manually	N/A	
	release	Update group release	release	5	Update manually	N/A	
	test	Update group test	test	0	Update manually	N/A	

Bước 5: Hệ thống hiển thị màn hình thông tin chi tiết Update Group, cho phép cập nhật/ chỉnh sửa thông tin và lưu lại bằng cách chọn nút "Apply":

pdate		Edit group detail	×		٢
oup(s) me of update group	Description	Update_thour Name contains only letters, numbers, and special characters " Description (optional)	- 11	Upcoming package	New update gro Action
Name of update group Update, specific sights beta congino privila, test release test	update sau 1 hour Update vao chu nhat hung tuan Group alpha test team agent core Group Beta update ngay Update group congno Update group phula_test Update group phula_test	update gay 1 hour (update] Package version Oncose the package version for this group. Only deployed and not ren versions related to agents can be shown here.	ase 1 26/2000 noved package	N/A 3.3.4 (03/07/2022 08:00:00) N/A N/A N/A N/A N/A	
	upoare group rest	3.3.7 (utket) Update schedel Wen annv package version is deployed: Update automatically Time to update Update immediately Update art 1		RA.	

- 4 Xóa Update groups:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



Q Search						
8 group(s)						New update group
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

Bước 4: Tại bản ghi cần xóa, chọn icon "Xóa" Update Group:

Update groups Packages						
Q update						© 0
8 group(s)						New update group
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	14
alpha	Group alpha test team agent core	release	0	Update manually	N/A	G
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congne	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

Bước 5: Hệ thống hiển thị Popup Xác nhận xóa Update Group, Người dùng chọn nút "Delete" để xác nhận yêu cầu Xóa Update Group và chọn nút "Cancel" để hủy yêu cầu Xóa Update Group.

A	Update groups Packages						
ī± @	Q update						© Q
	8 group(s)						New update group
	Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
ĭ.	Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after releas	ie N/A	
*	Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
r.	alpha	Group alpha test team agent core		-	nually	N/A	
	beta	Group Beta update ngay		Π	х у	N/A	
œ	congne	Update group congnc	Dolo	te this group?	nually	N/A	
	phula_test	Update group phula_test	Dele	te tills group:	nually	N/A	
	release	Update group release			nually	N/A	
	test	Update group test	Do you really war	t to delete this update group?	nually	N/A	
			Cane	rel Koep delete			

- 3.7.5.2 Update packages
- 1 Tìm kiếm packages:

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;



- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;

date groups	Packages								
λ Search									
10 package(s)	Backend version: 3.3 Tố	ng số package trên	hệ thống				Automatic deployment	Show unused packages	1. Upload new pac
Storage: 6.91 G	B used of 55.59 GB	Số dung lượng đ dung lượng h	là sử dụng trên tổng ệ thống cung cấp						
Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp.	 Not deployed 	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	 Not deployed 	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ	 Not deployed 	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	 Not deployed 	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install successed	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install successed	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
	N/A	N/A	Ves	Verified	Old repository release	Install successed	N/A	N/A	

Bước 5: Nhập từ khóa tìm kiếm vào ô textbox và chọn nút "Search"

Search									
0 package(s	Backend version: 3.3						Automatic deployment	Show unused packages	1, Upload new packa
torage: 6.91	GB used of 55.58 GB								
Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	Not deployed	root	N/A	
1.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp	 Not deployed 	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	 Not deployed 	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ	 Not deployed 	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install successed	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install successed	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	 Install failed 	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install successed	N/A	N/A	

2 - Auto Update

Mục đích: là tính năng cho phép tự động triển khai các bản update tới khách hàng một cách nhanh chóng và hiệu quả. Auto Update cho phép upload các gói qua giao diện portal hoặc tự động lấy các bản update qua trang hub.viettelcybersecurity.com;

Page | 214



Lưu ý: Đội triển khai gửi lại các thông tin trên cho đội dự án Ajiant để cập nhật vào hệ thống để cho phép triển khai gói tự động tại khách hàng. Về sau, khi cần triển khai gói update mới, đội triển khai hoặc phía khách hàng chỉ cần lấy gói update được cung cấp và upload lên portal ajiant và chọn triển khai gói.

- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;

A	ipdate groups	Packages								
H,	Q Search									Q
Ŭ E	10 package(s)	Backend version: 3.3 Tổng	g số package trên hệ	thống				Automatic deployment	Show unused packages	1. Upload new package
•	Storage: 6.91 GB	used of 55.59 GB	Số dụng lượng đã s dụng lượng hệ t	iử dụng trên tổng iống cung cấp						
÷.	Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
	3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	Not deployed	root	N/A	
Ē	3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp	 Not deployed 	dat	N/A	
	3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	 Not deployed 	root	N/A	
	3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	 Not deployed 	dat	N/A	
	3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ	 Not deployed 	dat	N/A	
	3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	 Not deployed 	dat	N/A	
	3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	 Install successed 	dat	10/05/2022 17:37:46	
	3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install successed	dat	10/05/2022 17:36:29	
	3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	 Install failed 	dat	10/05/2022 17:33:42	
	release	N/A	N/A	Yes	Verified	Old repository release	Install successed	N/A	N/A	

Bước 5: Chọn nút "Update new package", hệ thống hiển thị Popup "Upload package";

Search									
10 package(s Storage: 6.91	i) Backend version: 3.3 GB used of 55.59 GB					C	Automatic deployment	Show unused packages	1. Upload new pa
Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Actio
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp	 Not deployed 	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	 Not deployed 	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	 Not deployed 	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	 Not deployed 	dat	N/A	
	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install successed	dat	10/05/2022 17:37:46	
3.3.7						a lostal averaged	dat	10/05/2022 17:26:20	
3.3.7 3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	 Install successed 	Gai	10/03/2022 17:30:29	

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Bước 6: Chọn tải lên package;

λ Search										
10 package(:	s) Backend version: 3.3							Automatic deployment	Show unused packages	1. Upload new pac
Storage: 6.91	GB used of 55.58 GB									
Version	Release date	File size	Related to agents?	Signature	Description	Deployment	status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	Not deploy	ed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp	• Not deploy	ed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deploy	ed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Upload par	ckage >	< lot deploy	ed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No		the standing in the Control of the same in Table	lot deploy	ed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Choose f	me Max the size is counter, supported file type is .ZIP.	lot deploy	ed	dat	N/A	
227	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	• Install sug	cessed	dat	10/05/2022 17:37:46	
0.0.7		142.46 MB	Yes	Verified	3.3.4 description	Install sug	cessed	dat	10/05/2022 17:36:29	
3.3.4	28/03/2022 09:59:12									
3.3.4	28/03/2022 09:59:12 09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install faile	d	dat	10/05/2022 17:33:42	

Bước 7: Bật/ Tắt Action "Automatic Development" để tự động triển khai các bản cập nhật package tới khách hàng.

Search									
10 package(s	i) Backend version: 3.3					0	2 Automatic deployment	Show unused packages	1 Upload new
Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Act
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe.	 Not deployed 	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp.	 Not deployed 	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	 Not deployed 	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	 Not deployed 	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ	 Not deployed 	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	 Not deployed 	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install successed	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	 Install successed 	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	 Install failed 	dat	10/05/2022 17:33:42	
rologga	N/A	N/A	Vac	Vorified	Old repository release	Install successed	N/A	N/A	

3 – Deploy package

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;


Upd	sate groups	Packages								
٩	Search									٩
E	10 package(s) B	lackend version: 3.3 Tổng	j số package trên hệ) thống			0	Automatic deployment	Show unused packages	1 Upload new package
1	Storage: 6.91 GB u	ised of 55.59 GB	Số dung lượng đã s dung lượng hệ t	lử dụng trên tổng hồng cung cấp						
	Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
	3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	 Not deployed 	root	N/A	
	3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp	 Not deployed 	dat	N/A	
	3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
	3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	Not deployed	dat	N/A	
	3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nổi ra ngoài internet, chí	 Not deployed 	dat	N/A	
	3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	 Not deployed 	dat	N/A	
	3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install successed	dat	10/05/2022 17:37:46	
	3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	 Install successed 	dat	10/05/2022 17:36:29	
	3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	 Install failed 	dat	10/05/2022 17:33:42	
	rologga	N/A	N/A	Yes	Verified	Old repository release	Install successed	N/A	N/A	

Bước 5: Chọn icon "Deploy this package" tại bản ghi package đó, hệ thống hiển thị Popup Xác nhận Deploy package

) Search									
10 package(s)	Backend version: 3.3						Automatic deployment	Show unused packages	Upload new packag
Storage: 6.91	GB used of 55.58 GB								
Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	 Not deployed 	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp.	Not deployed	dat	N/A	-
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	 Not deployed 	root	N/A	ف
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	 Not deployed 	dat	N/A	Deploy this pa
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nổi ra ngoài internet, chỉ	 Not deployed 	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	 Not deployed 	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	 Install successed 	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	 Install successed 	dat	10/05/2022 17:36:29	
222	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	 Install failed 	dat	10/05/2022 17:33:42	
0.0.2									

Bước 6: Chọn nút "Deploy" để xác nhận Deploy package trên thiết bị hoặc chọn nút "Cancel" để hủy thao tác Deploy package.

date groups	Packages										
L Search											
10 package(s) Backend version: 3.3								Automatic deployment	Show unused packages	1 Upload new package
Storage: 6.91	GB used of 55.58 GB										
Version	Release date	File size	Related to agents?	Signature	Description			Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified		~ *	ESRe	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	<u>ب</u>	^ n	hợp	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Deploy this people and			Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Deploy this package?	- 1		Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified		et	, chí	 Not deployed 	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Do you want to deploy the package?	iv.	e Re	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Rebuild agent installer	- 1		Install successed	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	Cancel Deploy	- 1		Install successed	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified				 Install failed 	dat	10/05/2022 17:33:42	
and a new second	NI/A	NI/A	Vac	Verified	Old repository release			heseonus listen	N/A	N/A	

4 – Chi tiết Package

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;



- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;

pdate groups	Packages								
Q Search									
10 package(s)	Backend version: 3.3	ng số package trên	hệ thống			C	Automatic deployment	Show unused packages	1. Upload new package
Storage: 6.91 (GB used of 55.59 GB	Số dung lượng đi dung lượng hệ	ã sử dụng trên tổng ệ thống cung cấp						
Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp.	. Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	 Not deployed 	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ	 Not deployed 	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install successed	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	 Install successed 	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	 Install failed 	dat	10/05/2022 17:33:42	
					Old	a local strategy and			

Bước 5: Chọn icon "View Detail" tại bản ghi package đó, hệ thống hiển thị Popup thông tin chi tiết của Package vừa chọn:

Package detail		×
Deployment		
Status	 Not deployed 	
Information		
Backend version	N/A	
Package version	3.3.8	
File size	13.92 MB	
SHA256	46bac489a084ed4115de3ef71f30e89ceed60fa15b4d23f93edb929bc39c3d83	
Signature	Not verified	
Release date	28/03/2022 09:59:12	
Upload date	10/05/2022 17:33:05	
Uploader	dat	
Description	Gói update 3.3.8: Cập nhật tính năng hồ trơ NCSC Alert Agent Offline Live Reponse v2 Fix lồi Dashboard, checkmarx	1

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



3.8 Màn hình BLS

3.8.1 Thống kê vi phạm (Violation statistic)

Mục đích: Chức năng Thống kê vi phạm hỗ trợ người quản trị thống kê các vi phạm của agent đã cài đặt bao gồm:

- + Top các vi phạm base line, top đơn vị vi phạm baseline;
- + Xem danh sách các vi phạm và danh sách agent vi phạm trong từng đơn

vį;

+ Xem danh sách các đơn vị vi phạm và danh sách vi phạm trong từng đơn

vį;

- + Xem chi tiết của Agent;
- + Export vi phạm;
- + Report vi phạm;

Click vào tab "BLS" >> Thống kê vi phạm;

3.8.1.1 Màn hình Thống kê vi phạm

≡	v a	ettel Jiant BLS / Statistics / Violation Statistic						8 0
Ę	Vio	lation Statistic		•		Ouidelines		
A	٩	Search for group	Q Violation type				Last 30 days	٩
)¥ ©	2	top baseline violated rule			Top baseline violated group			
	T	Quy định cấu hình chính sách mặt khẩu	1		¹ na_test			4
	L	2 Quy định tự động khóa màn hình sau S phứt	1					
<u>e</u>		³ Quy định máy tính phải join domain, và sử dụng tài khoản domain để dàng nhập máy tính	1					
	L	Quy định nghiêm căm lưu trữ mặt khẩu trên trinh duyệt	1					

Hệ thống hỗ trợ thực hiện các tính năng:

+ Thống kê Top 10 vi phạm base line nhiều nhất sắp xếp theo thứ tự giảm dần

 Mỗi bản ghi được hiển thị các thông tin gồm: Nội dung vi phạm, số lượng máy vi phạm;

• Chọn bản ghi bất kì trong Top vi phạm baseline, hệ thống sẽ di chuyển đến màn hình chi tiết tương ứng với vi phạm đã được chọn;

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 219



+ Thống kê Top 10 đơn vị vi phạm base line nhiều nhất sắp xếp theo thứ tự giảm dần:

 Mỗi bản ghi được hiển thị các thông tin gồm: Tên đơn vị vi phạm, số lượng máy vi phạm;

• Chọn bản ghi bất kì trong Top đơn vị vi phạm baseline, hệ thống sẽ di chuyển đến màn hình chi tiết tương ứng với đơn vị đã được chọn;

- + Tìm kiếm
 - Tìm kiếm riêng lẻ:
 - Tìm kiếm theo Đơn vị
 - Top đơn vị vi phạm hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng (nếu có);
 - Top vi phạm: Hiển thị các vi phạm của đơn vị và đon vị con (nếu có) tương ứng;
 - Loại vi phạm
 - Top đơn vị vi phạm: hiển thị danh sách đơn vị vi phạm Loại vi phạm đã chọn;
 - Top vi phạm: Hiển thị vi phạm đã chọn;
 - Thời gian bị vi phạm;

• Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND;

3.8.1.2 Tab Loại vi phạm

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@vietteLcom.vn | W: www.viettelcybersecurity.com



aliant BLS / Statistics / Violation Statistics	istic							# 0
Violation Statistic							•	Guidelines
A Search for group			Q Quy định cấu hình chính sách mặt khẩu			×	Last 30 days	٩
Invot TENANT_sean.com TENANT_sean.com TENANT_sean.com TENANT_sean.com TENANT_sean.com default default	Volation type Croop VOLATION TYPE Our draw hand hand soch migt tabla Our draw hand hand soch migt tabla 3	850040 0 (70)	(MRESOUR) 1 (1995)	904/0 1 (29)	CN AGENT	VOL/ 1	Report.	الله Export
BLS / Statistics / Violation Stati	istic							# 0
Violation Statistic								Guidelines
Q Search for group			Q Quy định cấu hình chính sách mặt khẩu			×	Last 30 days	٩
Image: Second	Valution type Group COCUP Fina_list	CREINE IN DAY D (D%)	OHAME IN 10 DWS RECENTLY 0	RESOLVED O (ON.)	UNRESOLVED 1 (100%)	VIOLATION AGENT 1 (0%)	VICLATION REAE	🚖 Export

Hệ thống hỗ trợ thực hiện các tính năng:

+ Chọn link Top vi phạm: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm

- + Cây dữ liệu đơn vị của hệ thống
 - Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con;
 - Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc vi phạm;
- + Tab Loại vi phạm:

• Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Violation type, Resolved, Unresolved, Violation Computer, Violation unit;

• Chọn bản ghi Loại vi phạm trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm;

• Chọn máy tính: Hiển thị thông tin chi tiết máy tính và danh sách vi phạm tương ứng của máy tính;



≡	aJiant BLS / Statistics / Violation Stati	istic				# 0
ų.	Violation Statistic				Agent and group list baseline violation	Collapse all 🖌 🗙
▲	Q Search for group			Q Quy định cấu hình chính sách mặt khẩu	na_test	^
ž	a root				WIN7X64-A-PC E7240263DA88051AB80CD78E201FD8966269E3C2 • 1 violation	Hide >
©.	TENANT_nsm.com TENANT_viettel.com.vn	Violation type Group			Quy định cấu hình chính sách mật khẩu 09:53:11 22/06/2022	Not resolved yet
0	global	Quy định cấu hình chính sách mật khẩu	RESOLVED 0 (0%)	UNRESOLVED 1 (100%)		
0	admin					
ē.	default					

Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (tất cả loại vi phạm của máy)

≡	aJiant BLS / Statistics / Violation Statis	atic						B
Ę	Violation Statistic ← Top violation			Agent and group list baseline violation	Collapse all A	Detail informatio	n	×
▲	Q Search for group			na_test ^		AGENT	WIN7X64-A-PC	
Ť	📮 root			WIN7X64-A-PC E7240263DA88051A880CD78E201FDB966269E3C2 • 1 violation	Hide »	AGENT ID IP ADDRESS	E7240263DA88051A880CD78E201FD8966269E3C2	
Q	TENANT_nsm.com	Violation type Group		Quy định cấu hình chính sách mật khẩu 09:53:11 22/06/2022	Not resolved yet	DOMAIN		
	- 🖸 global	VIOLATION TYPE Quy định cấu hình chính sách mật khẩu	RESOLVED 0 (0%)			RESOLVED	na_test Not yet	
9	E Tabari, accom					DETAIL	Quy diphi dia khin khin sidin mik khila DEGORETON NA 104 055311 22/06/2022 0581101 OMININI 0, feading_password_complex*0, "password_bittop" (0)	d_len':)

Tìm kiếm

- + Tìm kiếm riêng lẻ:
 - Tìm kiếm theo Đơn vị: Hiển thị đơn vị đã nhập và danh sách đơn vị con

tương ứng

- Loại vi phạm: Hiển thị vi phạm đã chọn
- Thời gian bị vi phạm

+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND



3.8.1.3 Tab Đơn vị

≡	aJiant BLS / Statistics / Violation Sta	tistic							8 0
Ę.	Violation Statistic		Guidelines						
▲ -	Q Search for group			Q Quy định cấu hình chính sách mặt khẩu			×	Last 30 days	۵
•	TENANT_nsm.com	Violation type Group						Report	🛓 Export
Ð	- global - TENANT_edr.com	GROUP 3 na_test	0 (0%)	ONLINE IN 30 DAVIS RECENTLY 0	RESOLVED 0 (0%)	UNRESOLVED 1 (100%)	VIOLATION ADENT 1 (0%)	VIOLATION RULE	
e.	admin default 2								

Hệ thống hỗ trợ thực hiện các tính năng:

+ Chọn link Top đơn vị: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm;

- + Cây dữ liệu đơn vị của hệ thống;
 - Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con;
 - Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc đơn vị cha

– con;

+ Tab Đơn vị;

• Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Unit, Online in day, Online in 30 days recent, Resolved, Unresolved, Violation computer, Violation rule;

 Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm bao gồm Tên đơn vị, Tên máy tính|Agent ID, danh sách vi phạm của từng máy, thời gian vi phạm, trạng thái vi phạm (đã fix hay chưa fix vi phạm);

a Jiant BLS / Statistics / Viol	ation Statistic					8	0
Violation Statistic			Violation information			ation	×
Q TENANT_edi.com			na_test		AGENT	WIN7X64-A-PC	
-			Violation rule Violation agent		ADENTID	E7240263DA88051ABB0CD78E201FDB966269E3C2	
toon 🖸			WIN7X64-A-PC1E724026304880514880CD78E201ED8966269E3C2		# AZDRESS		
TENANT_nam.com	Violation type Group	CREINE IN DAY	I violation	Hide >	DOMMIN		
TENANI_viettei.com.vn	anour		Quy định cấu hình chính sách mặt khẩu		GROUP	na_test	
TENANT educore	na_test	0(0%)	09:53:11 22/06/2022	Not resolved yet	RESOLVED	Not yet	
default					DETAIL	Quy pho da biho habiho da hu ga tuda Description NGA 1940 1940 1940 1940 1940 1940 1940 1940	en":



Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (tất cả loại vi phạm của máy);

Chọn icon detail của cột violation rule trên danh sách: Hiển thị danh sách vi phạm của đơn vị;

Ш	aliant BLS / Statistics / Violation Stati	latic					8 0	
5	Violation Statistic ← Top violation					Violation Information	×	
▲	Q TENANT_edr.com		× Q Quy din	h cấu hình chính sách mặt khẩu		na_test		
7 <u>4</u>	-					Violation rule Violation agent		
	toot 🗐							
۹	-E TENANT_nsm.com	Violation type Group				Quy định cấu hình chính sách mật khẩu		
-	- TENANT_viettel.com.vn							
Ŀ	global	GROUP	ONLINE IN DAY	ONLINE IN 30 DAY'S RECENTLY	RESOLVED			
0	TENANT_edr.com	na_test	0 (0%)	0	0 (0%)			
	admin							
	default							
ą.								

Tìm kiếm

+ Tìm kiếm riêng lẻ:

• Tìm kiếm theo Đơn vị: Hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng;

- Loại vi phạm: Hiển thị vi phạm đã chọn;
- Thời gian bị vi phạm;

+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND;

3.8.2 Thống kê phần mềm (Software statistic)

Mục đích: Chức năng Thống kê phần mềm hỗ trợ người quản trị thống kê các phần mềm đã cài đặt trong một đơn vị bao gồm:

- + Xem danh sách các phần mềm đã cài trong 1 đơn vị được chọn;
- + Xem chi tiết của Agent;
- + Export phần mềm;



=	aJiant BLS / Statistics / Soft	ftware Statistic						# 0
Ę.	Software statistic							• Guidelines
▲	Q Search	h for group		Q Search for software	Installed	~	Last 30 days	٩
н,	root							
۵	TENANT_nsm.com						MUMPER OF COOLING	Export to excer
	- 🖾 global	2 60	oogle Chrome			1	1	
	admin		Version 102.0.5005.115			1	1	
	default							
ιų.								

Hệ thống hỗ trợ thực hiện các tính năng:

- + Cây dữ liệu đơn vị của hệ thống
- + Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con
- + Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc phần mềm
- + Danh sách phần mềm

• Mỗi phần mềm được hiển thị các thông tin chung gồm: Software name, munber of computer, munber of unit;

≡	aliant BLS / Statistics / Software Statis	stic					# 0
Ę.	Software statistic						Guidelines
▲ -	Q. Search for group		Q Search for software	Installed	~	Last 30 days	٩
*	TENANT_nsm.com	SOFTWARE NAME		NUI	IBER OF AGENTS	NUMBER OF GROUPS	ٹ Export to excel
	global TENANT_edr.com	Google Chrome Version 102.0.5005.115		1		1	
.	default						ð

 Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị bao gồm Tên đơn vị, Tên máy tính|Agent ID, Version;

≡	aJiant BLS/Sta	atistica / Software Stati	istic				0 🕷
Ę.	Software statistic					Software statistic (installed) - Google Chrome	×
۵ ک	ints	Q Search for group		Q. Search for software	Installed	group_bichpt3 (display 1/1 agent)	^
,** © © ©	root TEHANT_rusm.com TEHANT_viettel.com.vn global TEHANT_viettel.com. admin default		GOTTWARE NAME Geogle Chome Version 102.8 8005.115		NU 1 1	WIRC764.4.PC (E724033094889514885C974E201F0696329453C2 - Version 182.0.5055.115	

• Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Software information (software name, version);

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



=	aJiant BLS / Sta	itistica / Software Stati	istic				B 0
Ę	Software statistic				Software statistic (installed) - Google Chrome	Detail informati	on ×
₽		Q. Search for group		Q Search for software	group_bichpt3 (display 1/1 agent)	Agent information	
Ē	E mot				WIN7X64-A-PC E7240263DA88051AB80CD78E201FD8966269E3C2	AGENTID	E7240263DA88051ABB0CD78E201FDB966269E3C2
۲	TENANT_nsm.com				- version 102.0.3003.113	GROUP	group_bichpt3
5	TENANT_viettel.com.vn		SOFTWARE NAME			DOMAIN	
	global		Google Chrome			IP ADDRESS	127.0.0.1
0	TENANT_edr.com		Version 102.0.5005.115			AGENT NAME	Win7x64-A-PC
₿ <u>⊾</u>	default					Software informati	on
۹.						SOFTWARE	Google Chrome
					VERSION	- Version 102.0.5005.115	
						Software list in co	mputer >

• Chọn link [List softwares in computer]: Hệ thống đi chuyển đến màn hình Agent management và popup chi tiết máy tính tương ứng đã chọn hiển thị;

≡	aJi	ant	BLS / Statistics	/ Software Statist	tic											1	8 0
¢,	Softw	are statis	stic					Software statistic (in	stalled) - Goo	ogle Chrome				Detail informati	on		×
▲			Q s	Search for group		Q S	arch for software	group_bichpt3 (display	1/1 agent)				^	Agent information			
•# ⊕		t TENANT_ns	sm.com					WIN7X64-A-PC E7240 - Version 102.0.5005.1	63DA88051A 5	880CD78E201FD	B966269E3C2			AGENIT ID GROUP	E7240263DA88051 group_bichpt3	ABB0CD78E201FDB9	66269E3C2
	-0	ENANT_viett global	tel.com.vn		Google Chrome									IP ADDRESS	10.0.2.15 127.0.0.1		
	0	admin	2.00m		Version 102.0.5	005.115								AGENTINAME	Win7x64-A-PC		
•••	- de	fault												Software informat	ion		
*														VERSION	- Version 102.0.500	5.115	
													10	Software list in co	mputer »		
=	viett aJi	ant	Setting / Ag	Management					• Of Agent	ffline Agent Wi	in7x64-A-PC 51A880C078E201FD8966	1696302				T Uninstal	• ×
孕	Agent	managem	ient						First p	oing: N/A Last pin	g: 24/05/2022 17:51:07						
A	Agenti) = "E72402630	DA88051A880C078E2	201FDB956269E3C2*					Agent	t properties							
T _2	1	result(s)							Set P	folicy		Set update group		Move to group			
_		NAME				GROUP	UPDATE GROUP	LAST PING	full	l_features_v2	~	release	~	group_bichpt3	~	Save changes	1
<u>ح</u>		Win7x64-A	-PC	© Offline		Group_bichpt3	Release	24/06/2022 17:51:07	About	t this agent							
♥ ®	Display	1/1 result							C Gener Host N	General info	Installation Files Versi Win7x64-A-PC	on Installed Certificates Sch	duled Tas Netw IP v4	ks Disks & parti ork Interfaces	tions Environment	variables Installed	d softv >
-									Host D	D	acc37e95-b394-4c2	5-a44a-c72023363016	IP v6		fe80::4129:c4d9:998	e:73b5	
									Setup	Version	N/A windows		Name		08:00:27:d8:0a:49 Local Area Connecti	20	
									Platfor	m	Microsoft Windows	7 Ultimate Service Pack 1	IP 14		127.0.0.1		
									Platfor	rm Version	6.1.7601 Build 7601		IP v6		:1		
									Platfor	rm Family	Standalone Workst	tion	MAC		N/A		
									Physic	ecture cal Memory	an1064 N/A		Name		Loopback Pseudo-In	terface 1	
									CPUs	1			Pv4		fe80::5efe:a00:20f		
									Cores		2		MAC		00:00:00:00:00:00:00	i:e0	
									mhz		1992.000000		Name		isatap.(EF9B5CC8-C	F7D-485C-ACB7-	
									Model	v ID	Intel(R) Core(TM) i GenuineIntel	r-107001 CPU @ 2.00GHz			3A685F9F1F79}		
									10.00				IP v4		N/A 2001:0:7deb:43b:24	12-2987-15#F fdfD	
													IP v6		fe80:2402:2987:15ff	fdf0	
													MAC		00:00:00:00:00:00	te0	
													Name		Local Area Connecti	on* 9	
													Defa	ult Gateway			
													10.0	2.2			
													DNS	Server			
													10.2	55.244.122			
													10.2	5.244.133			

Tìm kiếm

- + Tìm kiếm riêng lẻ:
 - Tìm kiếm theo Đơn vị: Hiển thị các phần mềm đã cài trong đơn vị





- Tên phần mềm: hiển thị danh sách phần mềm đã nhập
- Tìm kiếm theo trạng thái: Installed, uninstalled
- Thời gian cài

+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

Export: Chọn Export: Hệ thống sẽ download file Export có dữ liệu giống với dữ liệu đang hiển thị trên màn hình

3.9 Rules Correlation

3.9.1 Danh sách hiển thị

Mục đích: Chức năng cho phép người dùng xem danh sách rules correlation trong hệ thống. Nhập hoặc chọn điều kiện tìm kiếm để thực hiện tìm kiếm rule đang có trên hệ thống, thao tác deploy/undeploy/xóa nhanh với các rule.

- + Bộ lọc FITTER;
- + Bộ lọc FITTER bao gồm:
 - 6 Engine: Whitelist, Agg Trigger, Agg Action, Filter, Indicator, False-

Positive;

- Text box search theo các trường: Name, content, description;
- Thời gian cập nhật;
- Tạo bởi tôi;
- Lọc theo Engine;

≡	aJi	ant Setting / Rules Corre	elation / Rules Mar	sagement								8 0
Ę.	Search	h rules										Ouidelines
▲	ENGINE :	White List	Ass Trisser	Agg Action >> CREATOR:	Only me Type to search by name, content,	description					Last 7 days	٩
₹ <u>÷</u>	View	column ~ 3 result(s)	21/06/2022 10:1	7:17 - 28/06/2022 10:17:17							速 Export 🖄 Import 🗸	+ Create
۲		UPDATED TIME	PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	
		22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Deployed	9 / î
Ø		22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Deployed	9 0 îi
Ē,		22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Undeployed	9 / û
8	Showing	3/3 result(s)										

Bước 1: Chọn 1 hoặc nhiều Engine mặc định;

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com





Bước 2: Chọn Mở rộng để thêm các Engine cần lọc;

=	aJiant Setting / Rules Corr	elation / Rules Ma	nagement								# 0
₽ ₽	Search rules	 Agg Trigger 	Agg Action	CREATOR: Orly me Type to search by name, conte	nt, description					Last 7 days	0 Guidelines
₽ #	View column v 1 result(s)	21/06/2022 10.5 PROBITY	20.05 - 28/06/2022 10.20.05	740	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	BLETVE O	OPTIONAL TYPE Q	🛃 Export 🗠 Import 🗸	+ Create
	22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detection	MITRE ATT&CK	root	builder	custom	Undeployed	8 0 û
2 12 12	Showing 1/1 result(s)										

Khi chọn 2 hoặc nhiều Engine, màn hình trả về kết quả được lọc theo phép toán AND;

Bước 3: Tích chọn người tạo Rules là user đang login vào hệ thống;

=	aJia	ant Setting / Rules Cor	relation / Rules Ma	anagement	\							ŧ	0
E.	Search	n rules										0	juidelines
₽	ENGINE :	 White List 	 Agg Trigger 	Agg Action	35 CREATOR: Only me Type to search by name, control	ent, description					Last 7 days		۹
r ₄	View	column ~ 1 result(s)	21/06/2022 10:	20.05 - 28/06/2022 10:20:05							👌 Export 👌 Import 🕚	+	Create
۲		UPDATED TIME	PRORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULETYPE Q	OPTIONAL TYPE Q	STATUS		1
		22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Undeployed	8 0	
₽	Showing	g 1/1 result(s)											

Bước 4: Nhập Name, content, description muốn search vào text box;

=	viettel aJiant Setting / Rules Co	rrelation / Rules Ma	anagement		\						# 0
Ę.	Search rules			_	<u>\</u>						Guidelines
▲	ENGINE: Vibite List	 Ass Trigger 	Agg Action	30 CREATOR: Only me	Type to search by name, content, description					Last 7 days	Q
τ ₂	View column v 1 result(s)	21/06/2022 10:	20.05 - 28/06/2022 10.20.05							速 Export 🙏 Import	✓ + Create
۲	UPDATED TIME	PRORITY	NAME Q	TAG	CATEGORY C	SUB CATEGORY Q	CREATOR Q	RULETYPE Q	OPTIONAL TYPE Q	STATUS	
	22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Det on	NOTE MITRE ATTECK	root	builder	custom	Undeployed	9 0 ū
•	Showing 1/1 result(s)										
ē,											
<u>e</u>											

Bước 5: Nhập thông tin cần tìm kiếm;

Bước 6: Nhấn Search để hiển thị kết quả tìm kiếm.

Page | 228



Chọn cột

Cho phép người dùng lựa chọn các cột hiển thị trên màn hình correlation.

Các bước thực hiện:

Bước 1: Click vào combo box View column. Màn hình hiển thị danh sách lựa chọn các cột ở dạng check box;

≡	viettet aJiant	Setting / Rules Corre	elation / Rules Mar	nagement									×	0
Ę	Search rules												😗 Guid	delines
▲	ENGINE:	White List	Ass Trisser	Agg Action	>> CREATOR: Only me	Type to search by name, content, o	description					Last 7 days	C	A .
₹±	View column	~ 1 result(s)	21/06/2022 10:2	20:05 - 28/06/2022 10:20:05								🛃 Export 🔄 İmport 🗸	+ •	reate
۲	UPDATED	DITIME	PRORITY	NAME Q	TAG		CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULETYPE Q	OPTIONAL TYPE Q	STATUS		
Ē	22/06/2	2022 18:04:48	1	T1059_005_VisualBasic			Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Undeployed	9 0 i	ū
•	Showing 1/1 resi	ult(s)												
Ē.														
0														

Bước 2: Chọn vào những tên cột muốn hiển thị;

=	viettel a Jiant Setting / Rules Correlation / Rules Managemen	ni						B 0
Ę.	Search rules							Ø Guidelines
▲	ENCINE: Utilat Agg Trigger	AggAction Filter Indicator	False Positive GREATOR:	Only me Type to search by name, content, o	description		Last 7 days	Q
τ±.	View column - 3 result(s) 21.06/2022 10.22:30-28/	06/2022 10:22:30					🛓 Export 🖄 Import 🗸	+ Create
۹	Search in dropdown list	a TAG	CATEGORY Q SUB CATEGORY Q	CREATOR Q	RULETYPE Q	OPTIONAL TYPE Q	STATUS	1 A
	 Updated time Priority 	ModifyRegistry	Anomaly Detecti MITRE ATT&CK	root	builder	custom	Deployed	
0	Name	SystemInformationDiscovery	Anomaly Detecti MITRE ATT&CK	root	builder	custom	Deployed	900
e <u>r</u>	 Tag Category 	005_VisualBasic	Anomaly Detecti MITRE ATTECK on	root	builder	custom	Undeployed	9 / ū
	Sub category							
	Rule type							
	Optional type Status							
		1						

- 1 Hỗ trợ tìm kiếm nhanh
- Tìm kiếm theo tên rule

Bước 1: Click icon <a> dể hiển thị thanh tìm kiếm;

t,	Searc	ch rules										Guidelines
A	ENGINE	White List	Agg Trigger	Agg Action S CREATOR: Only	me Type to search by name, content,	description					Last 7 days	٩
₹±	Viev	v column ~ 3 result(s)	21/06/2022	11-28/06/2022 10:44:11							🛓 Export 🖄 Import 🗸	+ Create
۹		UPDATED TIME	PRORTY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULETYPE Q	OPTIONAL TYPE Q	STATUS	1.0
1		22/06/2022 18:2	×	Apply odifyRegistry		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Deployed	
0		22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Deployed	90
Ē <u>.</u>		22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Undeployed	9 0 û
P	Showin	ng 3/3 result(s)										

- Bước 2: Nhập tên rules muốn tìm kiếm;
- Bước 3: Nhấn Enter để hiển thị kết quả tìm kiếm.





4	Searc	ch rules											😗 Guide	elines
▲	ENGINE	U White List	 Ass Trisser 	Agg Action	>> CREATOR: Only me	Type to search by name, content,	description					Last 7 days	٩	
P.A	View	v column v 3 result(s)	21/06/2022 10-	47:53 - 28/06/2022 10:47:53								🛃 Export 🔔 Import	~ + Cre	eate
۲		UPDATED TIME	PRIORITY	NAME Q	TAG		CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULETYPE Q	OPTIONAL TYPE Q	STATUS		
		22/06/2022 18:12:19	1	T1112_ModifyRegistry			Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Deployed	80	
0		22/06/2022 18:10:57	1	T1082_SystemInformationDi	scovery		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Deployed		
Ē.		22/06/2022 18:04:48	1	T1059_005_VisualBasic			Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Undeployed	801	ĩ
	Showin	ng 3/3 result(s)												

Tìm kiếm theo Category: Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Windows, Linux, MacOS.

Bước 4: Click icon <a> dể hiển thị danh sách loại Category;

<u>ال</u>	Geodelees													
▲	ENGINE	: White List		Last 7 days	Q									
τ _ά	Ver column 🗸 3 resultja 2/66/2022/66/35 -266/2022/66/35 - 266/2022/66/2022/66/202 - 266/2022/66/202 - 266/2022/66/202 - 266/202-2022/66/2022/66/202-2020-2020-20													
Ð		UPDATED TIME	PRORTY	TI Q.	TAG		CATEGORY Q SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS			
E		22/06/2022 18:12:19	1	T1112_ModifyRegistry	Windows	Linux	MacOS	Anomaly Detection	builder	custom	C Deployed	901		
•		22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery	Policy	🗌 Exploit	U Malware	Clear Apply	builder	custom	Deployed	901		
Ē <u>à</u>		22/06/2022 18:04:48	1	T1059_005_VisualBasic			on MITRE ATT&CK	root	builder	custom	Undeployed	9 0 û		
Đ	Showi	ng 3/3 result(s)												

Bước 5: Chọn category muốn tìn kiếm;

Bước 6: Click "Apply";

Tìm kiếm Sub Category: Hỗ trợ tìm kiếm nhanh theo loại triển khai, gồm 3 loại mặc định là: Metre ATT&CK, Malware, Suspicious Behaviour:

- **Bước 1:** Click icon dể hiển thị thanh tìm kiếm;
- Bước 2: Chọn sub category muốn tìn kiếm;
- Bước 3: Click "Apply";

Tìm kiếm Creator

- **Bước 1:** Click icon dể hiển thị thanh tìm kiếm;
- Bước 2: Nhập tên người tạo muốn tìn kiếm;
- Bước 3: Click "Apply";

Tìm kiếm Rule type: Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Advanced, Builder, All.

Page | 230





- Bước 1: Click icon Q để hiển thị danh sách Rule type;
- Bước 2: Click vào "Rule type" muốn tìm kiếm;
- Bước 3: Click "Apply";

Tìm kiếm Optional type: Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Built-in, Custom, All.



Bước 1: Click icon dễ hiển thị danh sách Optional type;

- Bước 2: Click "Optional" type muốn tìn kiếm;
- Bước 3: Click "Apply";

Hỗ trợ Deploy/Undeploy cho nhiều Rules

S	earch	n rules	Ass Trisser	Agg Action	🗌 Filter	Indicator	False Positive	CHEATOR: 0	nly me Type to search by name, contr	ent, description			Last 7 days	0 Guidelines Q
	View	column ~ 3 result(s)	21/06/2022 10.4	17:53 - 28/06/2022 10:47:53								2	🗄 Export 🔔 Import	
	1 Sel	ected:									Deploy	Undeploy	🚊 Deport 📄 Delete	Cancel
		UPDATED TIME	PRIORITY	TT Q	TA	ug.	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	4 OPTIONAL TYPE Q	STATUS		
		22/06/2022 18:12:19	1	T1112_ModifyRegistry			Anomaly Detecti on	MITRE ATT&CK	root	builder	custom		Deployed	
	•	22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery			Anomaly Detecti on	MITRE ATT&CK	root	builder	custom		Deployed	
		22/06/2022 18:04:48	1	T1059_005_VisualBasic			Anomaly Detecti on	MITRE ATT&CK	root	builder	custom		Undeployed	
SI	howing	3/3 result(s)												

Bước 1: Click vào nhiều check box có cùng trạng thái là Deploy hoặc Undeploy;

Bước 2: Click vào nút "Deploy/Undeploy";





Bước 3: Chọn "Deploy/Undeploy" trên popup hiển thị để thực hiện Deploy/Undeploy;

3	Searc	ch rules									9 Guidelines
	ENGINE :	White List	Ass Trisser	Agg Action	Filter Indicator	False Positive	CREATOR:	Only me Type to search b	y name, content, description		Last7 days
	View	v column v 3 result(s)	21/06/2022 10	47:53 - 28/06/2022 10:47:53							速 Export 🖞 Import 🗸 + Creste
	1 Se	elected:									Undeploy L Deport Definite Cancel
		UPDATED TIME	PRIORITY	TI Q	TAG	CATEDORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	+ OPTIONAL TYPE Q	STATUS
		22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	C Deployed
		22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	C Deployed
		22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detecti on	MITRE ATT&CK	root	builder	custom	Undeployed
	Showin	ng 3/3 result(s)									
					[×			
							0				
						U	ndeploy rule				
						Are you gure you wa	at to undaplos: : All miles	relected 2			
						Are you sure you wa	ne to undeproy All rules	selected r			
						Car	Undeploy				

3.9.2 Thêm mới Rules Correlation

Mục đích: Chức năng cho phép người dùng cấu hình một rule correlation mới hoàn chỉnh.

Tổng quan

+ Engine: Gồm tất cả 6 engine với thông tin chi tiết lần lượt là:

 Whitelist là một Stateless Engine thực hiện loại bỏ nhanh các event mà hệ thống không cần xử lý. Các event khớp với rule whitelist sẽ bị drop khỏi luồng xử lý;

• Agg_trigger và Agg_action là một Stateful Engine thực hiện gom nhóm các event tương tự nhau. Mỗi rule aggregate chứa các thông tin về điều kiện gom nhóm (định nghĩa event tương tự nhau), khoảng thời gian gom nhóm (ví dụ 30s, 1 phút, 2 phút, ...). Các event khớp điều kiện gom nhóm được lưu lại và chỉ trả về một event có kèm theo số lượng sau một khoảng thời gian. Các event không khớp điều kiện gom nhóm được trả ra ngay lập tức với số lượng là 1;

Filter là một Stateless Engine thực hiện lọc các điều kiện để đẩy vào indicator;

• Indicator là một Stateful Engine thực hiện kiểm tra, thống kê trên các event thỏa mãn Filter. Đầu vào của Indicator là các event thỏa mãn Filter, đầu ra là



các Indicator Event hoặc Alert Event. Indicator hỗ trợ các phép thống kê số lượng (count) trong một đơn vị thời gian (time-windows) của cùng một đối tượng, không Alert lặp lại đối với cùng một đối tượng trong khoảng thời gian quy định trước. Mỗi rule indicator chỉ thực hiện xét các điều kiện cùng loại, trên cùng một hệ thống;

• FalsePositive engine là một Stateless Engine thực hiện loại bỏ các trường hợp Alert bị Alert sai. Mỗi Alert khi khớp với rule Falsepositive sẽ bị drop;

+ Debug/ Not Debug là hai trạng thái của engine. Khi thực hiện thao tác debug, log được đẩy về thoả mãn điều kiện của engine sẽ hiển thị trên màn hình Gỡ rối Correlation;

+ Điều kiện: Mỗi engine sẽ hỗ trợ các điều kiện về Event, not Event, Alert Event, not Alert Event, Accumulate, Function, not Function khác nhau. Chi tiết về các điều kiện và cách sử dụng:

- Event: Được sử dụng cho các trường event;
- Not Event: Chỉ được tạo ra khi có event;
- Alert: Được sử dụng cho các trường Alert;
- Not Alert: Xét xem không có Alert event trong bao lâu;

Accumulate: Thực hiện gom nhóm điều kiện event thoả mãn số lượng từ đó sinh ra Alert;

• Function: Là các hàm. Lưu ý: Vớicác hàm boolean, giá trị trả về là true hoặc false;

• Not Function: Với not function, các hàm được sử dụng giống với function. Tuy nhiên giá trị trả về sẽ có kết quả true/false ngược lại.

+ Toán tử :

- Các toán tử cơ bản gồm: =, !=, >, <, >=, <= .
- In: Kiểm tra giá trị của một trường có nằm trong danh sách không.
 - Bên trái toán tử: Tên trường cần kiểm tra.



- Bên phải toán tử: Danh sách giá trị để kiểm tra được phân cách bởi dấu ",".
- Contains: kiểm tra giá trị của một trường có chứa giá trị mà cần kiểm

tra.

- Bên trái toán tử: Tên trường cần kiểm tra (trường này cần có giá trị là mảng hoặc string);
- Bên phải toán tử: Giá trị để kiểm tra.
- Assign: để gán giá trị của một trường vào một biến.
 - Bên trái toán tử: Tên trường cần gán;
 - Bên phải toán tử: Tên biến cần gán.
- Matches: kiểm tra giá trị của một trường có thoả mãn một chuỗi regex.
 - Bên trái toán tử: Tên trường cần kiểm tra;
 - Bên phải toán tử: Chuỗi regex.

• Cấu hình thời gian: Kiểm tra điều kiện trong một khoảng thời gian, chỉ có ở các engine Agg_trigger, Agg_action và Indicator.

• Count: Kiểm tra số event đếm được trong một khoảng thời gian có thoả mãn điều kiện không.

+ Nhóm/ Bỏ nhóm : Cho phép người dùng gộp hoặc tách nhanh các điều kiện trong một toán tử AND hoặc OR. Các bước thực hiện gộp nhóm/ tách nhóm:

- Gộp nhóm
- Bước 1: Click vào vào trường cần gộp nhóm;
- Bước 2: Chọn NHÓM Màn hình chi tiết các bước thực hiện gộp nhóm;
 - Tách nhóm:
- Bước 1: Click vào các item cần tách nhóm;
- Bước 2: Chọn BỞ NHÓM Màn hình chi tiết các bước thực hiện tách nhóm
 - + Restore: Tự động reset lại đến ngay sau khi nhấn "Save" gần nhất;



- + Reset: Thực hiện reset condition (về trạng thái ban đầu);
- + **Delete:** Xóa Condition đang được focus;

Các bước thêm mới rule correlation:

Bước 1: Tại màn hình Correlation, Chọn nút "Create" > Hệ thống hiển thị màn hình tạo mới rule;

≡	aJiant Setting		۵
Ę	Create ← Back to list	Protex Som & Diplay	Save
▲ ¹ H ④	Category* Windows Rule name* Type rule name	Subscription* Pauloption* Pauloption* Pauloption* V MITE ATTEX Ten deception Tege V Ten deception* Tege Tege Choose toge Choose toge Choose toge	1
e R	ENGINE GROUP	Condition	Debug
	LE, Agg Trigger UNGROUP		
	tál Indicator SAVE False positive RESTORE		
	RESET		

Bước 2: Nhập thông tin của rule;

Category* Sub category*	Description*	Priority*
Windows V MITRE ATT&CK V	Type description	1
Rule name*		Tags
Type rule name		Choose tags
RUIED Windows_MITRE_ATT&CK_		

Lưu ý: Các trường có dấu (*) là các trường bắt buộc nhập.

Bước 3: Chọn Engine, nhập điều kiện cho các Event, not Event, Alert, not Alert, Accumulate, Function tương ứng;



≡	aJiant Setting			# 0
Ę	Create ← Back to list		Preview Save & Deploy	Save
4 , ^µ * ⊕ ∐ ►	Category" Windows Rule name" Type rule name RuleID Windows_MITRE_	Sub category* Description* Proving* V MITRE ATTRCK Type description Type description ATTRCK Attrack Colore topp		1
¢.	ENGINE vhite Lat f, Agg Action v Fiter file dedicator file fate positive	Condition Condit	5	Chon tang thái debug
		Action (7. Chipa Action Netco)		

Bước 4: Nhấn "Save" để lưu lại điều kiện hoặc nhấn "Restore" để trở lại ngay sau bước mới lưu;

Bước 5: Tại Hành động , chọn hành động cần thực hiện đối với engine đó.

Các bước thực hiện thêm hành động tương ứng với từng engine: Khi người dùng thực hiện xong các bước tạo điều kiện và nhấn lưu, màn hình sẽ hiển thị các hành động cho từng engine. Mỗi engine sẽ bao gồm các hành động tương ứng. Engine Agg_trigger sẽ không có hành động.

Whitelist: Gồm 4 hành động dưới dạng check box : Drop, Chuyển sang aggregate, Alert và Danh sách Active, người dùng bắt buộc phải chọn 1 trong 4 hành động này. Khi các log đẩy vào thoả mãn điều kiện sẽ thực hiện 1 trong 4 hành động mà người dùng đã tích chọn. Chi tiết chức năng của 4 hành động:

 Drop: Các log được đẩy vào thoả mãn điều kiện sẽ được loại bỏ khỏi luồng xử lý;

• Chuyển sang aggregate: Log đẩy vào thoả mãn điều kiện sẽ được chuyển sang engine aggregate để tiếp tục xử lý;

• Alert: Khi thêm các trường key và value cho Alert, các log đẩy vào thoả mãn điều kiện sẽ hiển thị Alert tại màn hình quản lý Alert;

• Danh sách Active: Các value của active list sẽ được thêm vào danh sách hiển thị trên màn hình Active List;



Các bước thêm trường cho hành động Alert/ Danh sách active:

- Bước 5.1: Click chọn hành động muốn them;
- Bước 5.2: Click nút "edit" để nhập giá trị cho trường;
- Bước 5.3: Nhập giá trị cho trường;
- Bước 5.4: Click nút "Save";
- Bước 5.5: Click nút "Add" để thêm mới một trường vào Alert.

ENGINE	Condition Condition	Debug
🗊 White List		
🖭 Agg Trigger	kalone	
Ed. Ann Action		
Agg Account		
Tilter	Eesaanulay X ++ v loportype X	
i≦íÍ Indicator		
False positive		
	0	
	Action	
	0 Dmp	
	0 More to appropria	
	Airr 1 Chen acton	Delete
	кту учине (Станана)	TION
	seventy 1 1 1 Mag gat the seventy to the sevent the sev	×
	alet - 2 Chon size cbp	0
	alpentage - negative	0
	egenesion_group "	0
	Active alert	

- + Để xoá hành động vừa tạo, click icon "Delete";
- + Để chỉnh sửa hành động, Click icon "edit";

Lưu ý: Có thể tạo nhiều hành động với các trường khác nhau tuỳ theo mục đích người sử dụng.

Agg_action: Tại engine này, người dùng có thể thực hiện hành động thêm code.

Các bước thêm trường cho hành động thêm code

- Bước 5.1: Nhập đầy đủ điều kiện và toán tử. Click vào "Save";
- Bước 5.2: Tại mục Action, click vào icon "Enable action";
- Bước 5.3: Nhập nội dung của code;



• Bước 5.4: Chọn nút "clear" => Nội dung nhập của code sẽ bị xóa toàn

bộ;

Category* The integory* Decompose Decompose Nonety* Accompto factoria V Martine factoria activity on machine Factoria	
Anomaly Detection V MITRE ATTBOX V for deleted suppose administration	
	1
Rue non" Tapa	
Tite2_systemidomator/sizeway Disoss tags	
Anomaly Detection_MITRE ATTRACK_T1082_System/information/Discovery	
ENGINE Condition	Debug
Is, Aga Tropper	
Age Action DEFE	8
Y Fiber	
sgi indextor	
Fale positive (NO -)	
teget commontive x matches = 100 "valuant." x	
(2) v (c topp, commative x matches - 10) "toppmer * x	
E Regulacommendia a mathe - 'D' (grana." *	
C	
RTHE	
Action	
	Disable action Clear

Filter : Gồm 3 hành động: Alert, Enrichment và Danh sách Active. Người dùng có thể 1 hoặc nhiều hành động trong cùng engine. Chi tiết chức năng của 3 hành động:

- Enrichment: Thêm trường vào Alert;
- Alert và Danh sách Active (như engine Whitelist).

Các thao tác thêm mới, sửa, xoá cho các hành động của engine filter tương tự với khi thêm mới các trường cho engine whitelist.

Indicator : Hành động Alert. Các thao tác thêm mới, sửa, xoá cho các hành động của engine Indicator tương tự với khi thêm mới các trường cho engine whitelist .

FalsePositive: Hành động Enrichment. Các thao tác thêm mới, sửa xoá cho các hành động của engine FalsePositive tương tự với khi thêm mới các trường cho engine whitelist .

Bước 6: Nhấn "Save" để lưu rule vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống, đồng thời deploy xuống correl engince thì nhấn "Save & Deploy".



Lưu ý: Khi có lỗi, người dùng có thể nhấn nút "Preview" để xem lỗi.

3.9.2.1 Sửa Rules Correlation

Cho phép người dùng chỉnh sửa các rule đã tạo.

Các bước thực hiện:

Bước 1: Tại màn hình quản lý rule, click icon Chỉnh sửa của rule muốn chỉnh sửa;

≡	ali	iant Setting / Rules Correl	ation / Rules Manag	ement											
₽	Search	h rules												0	Guidelines
▲	(NOME)	📋 White List	AggTrigger	C Agg Action >> cettalton	🗌 Only me	Type to search by name, content, descri	union						Last 7 days		۹
τ _ά	View	column ~ 3 result(s)	21/06/2022 11:52:57	- 26/06/2022 11 52:57									🛃 Export 🔝 Import	-	+ Creine
Q		+ UPDATED OME	PROBILY	11 Q		alg	CATEGORY Q	SUN CATEGORY Q	CINATOR Q	MALETIME Q	OFTIONALTYPE Q	STATUS			
		22/06/2022 18:12:19	1	T1112_ModifyRegistry			Anomaly Detection	MITRE ATTBCK	root	builder	custom		Deployed	8	0.0
•		22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery			Anomaly Detection	MITRE ATT&CK	root	builder	custom		Deployed	0	0.0
Ēλ		22/06/2022 18:04:48	1	T1059_005_VisualBasic			Anomaly Detection	MITRE ATTECK	root	builder	custom		Undeployed		0
	Showing	g 3/3 result(s)													5

Bước 2: Tại màn hình chỉnh sửa , nhập thông tin cần chỉnh sửa;

=	aJiant Setting	0						B 0
5	Edit - T1082_SystemIn ← Beckto Est	nformationDiscovery					Preview Save & Deploy	Save
x ™ © © 0 0 0 0 0 0 0 0 0 0 0 0 0	Calegoy" Anomaly Calegory Telliz Systemicionau Calegor Real Of Anomaly Development Calegory C	Sid origon/ Inter-ATEA wy cocourt Condition Condition Condition Condition Condition Condition Condition	ox when a too be over a set of the set of t	Denotypine" Use data supposes antivities an mactive	···· (m) ·····	Nonfy" Tag) Debug
		Action						

Lưu ý: Các trường tên rule, category, subcategory là những trường không chỉnh sửa được.

Bước 3: Nhấn nút "Save" để lưu rule lại vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống, đồng thời deploy xuống correlation engine thì nhấn "Save & Deploy".

Với những rule chỉnh sửa nhưng chỉ Lưu, người dùng phải click Redeploy tại màn hình quản lý rule thì rule mới có tác dụng đối với hệ thống.

Page | 239



Lưu ý: Khi có lỗi, người dùng có thể nhấn Preview để xem lỗi.

3.9.3 Xóa Rules Correlation

_														
=	aJiant	Setting / Rules Correl	ation / Rules Manag	ement									œ	0
ş	Search rules	15											0 😡	idelines
▲	ENGINE :	 White List 	Agg Trigger	 Agg Action 	>> CREATOR: Only me	Type to search by name, content, descri	iption					Last 7 days	4	a I
Ť±	View column	n v <mark>3</mark> result(s)	21/06/2022 11:55:29	- 28/06/2022 11:55:29								🚖 Export 👶 Import	~ + c	Create
۲	☐ ↓ UPD	DATED TIME	PRIORITY	TI Q	n	1G	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS		
	22/06	5/2022 18:12:19	1	T1112_ModifyRegistry			Anomaly Detection	MITRE ATT&CK	root	builder	custom	C Deployed	0	
0	22/06	6/2022 18:10:57	1	T1082_SystemInformationDis	covery		Anomaly Detection	MITRE ATT&CK	root	builder	custom	C Deployed	0 0	0
Ē.	22/06/	5/2022 18:04:48	1	T1059_005_VisualBasic			Anomaly Detection	MITRE ATT&CK	root	builder	custom	Undeployed	Delete	
ē	Showing 3/3 re	eouit(s)												J

Các bước thực hiện xóa 01 rule:

Bước 1: Click icon "Xoá" tại rule muốn xoá;

Bước 2: Màn hình hiển thị thông báo xác nhận xoá , chọn "Cancel" hoặc "Delete";

	aJiant Setting / Rules Cor	rrelation / Rules Manager	ment							
	Search rules ENGINE: White List	Agg Trigger	Agg.Action 🔅 CREATOR: Only n	ne Type to search by name, content, d	lescription					Last 7 days
	The View column v 3 result(s)	21/06/2022 11:55:29 -	28/96/2022 11:55:29		CATEGORY O	SUB CATEGORY O	CERAICE O	RAFINE O		Export 🖞 Import 🗸
	22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detection	MITRE ATT&CK	root	builder	custom	epioyed
	22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detection	MITRE ATT&CK	root	builder	custom	eployed
	22/06/2022 18:04-46 Showing 3/3 result(s)	1	T1059_005_WeueBlasc		n	MITHE ATTROX	root	builder	custom	laepioyea
				-	Āre you sure you want t	Delete rule	×			
Bước 3:				_	c	ancel Delete				

+ Nếu chọn "Delete", rule được chọn xoá sẽ biến mất khỏi màn hình hiển

thị;

≡	aJ	Jant Strog / Max Garantino / Max Management											
ş	Searc	ch rules									🙆 Guide	dines	
▲	ENGINE	White List	App Trigger	Agg Action CREATOR: Only me	e Type to search by name, content, descr	ption					Last 7 days	1	
÷	Vie	w column 👻 3 result(s)	21/06/2022 11:55:29	- 28/06/2022 11:55:29							🛓 Export 🔹 Import 👻 🕂 Cre	-	
۹	1 S	elected								💿 Depisy	Undeploy 🛃 Export 📋 Delete Cance		
	1	4 UPDATED TIME	PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	status 2		
0		22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detectio n	MITRE ATT&CK	root	builder	custom	C Deployed		
θλ	0	22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detectio n	MITRE ATT&CK	root	builder	custom	C Deployed		
۹	8	22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detectio n	MITRE ATT&CK	root	builder	custom	Undeployed		
	Showie	ng 3/3 result(s)											

Các bước thực hiện xóa nhiều rule:

Bước 1: Click chọn những rule muốn xoá (Có thể xoá tất cả bằng cách Click Chọn tất cả rule);





Bước 2: Màn hình hiển thị thông báo xác nhận xoá, chọn "Cancel" hoặc "Delete";

	aJiant Setting / Rules	s Correlation / Rules Man	agement						8 0
5	Search rules								Ouidelines
▲	ENGINE : Diffite List	Agg Trigger	Agg Action Secure:	Only me Type to search by name, co	ntent, description				Last 7 days
73	View column ~ 3 result	t(s) 21/06/2022 11:55	29 - 28/06/2022 11:55:29						. 출 Export _ ☆ Import _ ← Create
۹	1 Selected.							💿 Deploy	🛞 Undephy 🛃 Export 👔 Delete Cancel
	UPDATED TIME	PRIORITY	NAME Q		CATEGORY Q SUB CATEGO	RY Q CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS
Ø	22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detectio MITRE ATT	&CK root	builder	custom	C Deployed
e <u>r</u>	22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detectio MITRE ATT	&CK root	builder	custom	C Deployed
Đ	22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detectio MITRE ATT	SCK root	builder	custom	Undeployed
	Showing 3/3 result(s)								
						×			
					Deleteru	le			
					Are you sure you want to delete Mult	ti-rule : All rules selected ?			
					Cancel	dete			

Bước 3: Chọn "Delete", tất cả rule sẽ được xoá khỏi màn hình hiển thị. Chọn "Cancel", thao tác vừa chọn sẽ được huỷ bỏ.

3.10 Protect & Prevention

3.10.1 Application Control

Mục đích: Chức năng Application Control cho phép cấu hình các ứng dụng/tiến trình (process) sẽ chặn dưới máy người dùng không cho phép chạy (execute). Ứng dụng/tiến trình được nhận dạng dựa vào mã băm (MD5, SHA1, SHA256) hoặc đường dẫn.

3.10.1.1 Hiển thị danh sách các ứng dụng/tiến trình bị chặn

Click vào tab Protect & Prevention > chọn Application control sẽ hiển thị toàn bộ các ứng dụng/tiến trình dưới máy người dùng không cho sử dụng.

Type object path/hash to search			
0 agent(s) updated Time updated: 2022/06/17 15:52:36			Import Application List 🗸 🕂 Add New Appl
Object	Туре	Description	Created Time A
Citempransomware.exe	Path	import from file	2022/06/15 15:06:46
D:\Doc\tmp.dll	Path	import from file	2022/06/15 15:06:46
B5A45CF9385E4E3F43D6DF8FDCE52D26E14B4D93	Hash	import from file	2022/06/15 15:06:46
"temp\virus.dll	Path	import from file	2022/06/15 15:06:46
	Path	import from file	2022/06/15 15:06:46
"malware."			
"matware." D002c5611B30295008FEF124870F9863CEDADF12	Hash	import from file	2022/06/15 15:06:46



3.10.1.2 Tìm kiếm ứng dụng/tiến trình bị chặn

Người dùng có thể tìm kiếm theo mã băm hoặc đường dẫn của ứng dụng bị chặn

Protect & Prevent / Application Control			
Q. 04			×
0 agent(s) updated Time updated: 2022/06/17 15:52:36			Import Application List 🗸 🔰 + Add New Applic
Object	Туре	Description	Created Time Ad
C/tempransomware.exe	Path	import from file	2022/06/15 15:06:46
D/Doc/imp.dll	Path	import from file	2022/06/15 15:06:46
B5A45CF9385E4E3F43D6DF8FDCE52D26E14B4D93	Hash	import from file	2022/06/15 15:06:46
*\temp\virus.dll	Path	import from file	2022/06/15 15:06:46
http://ware.*	Path	import from file	2022/06/15 15:06:46
D8D2C6E11B3D295C08FEF124870F9863CEDADF12	Hash	import from file	2022/06/15 15:06:46
C:\Windows\System32\asdawb.exe	Path	AnhNN Test	2022/02/08 14:38:11

3.10.1.3 Thêm mới ứng dụng/tiến trình bị chặn

Click vào "Add new" để thêm mới ứng dụng/tiến trình bị chặn, người dùng có thể chọn chặn theo Path hoặc mã Hash (MD5, SHA1, SHA256)

≡	Jiant Protect & Prevent / Application Control			**	0
ē	Q D8			×	٩
ла Т, т	0 agent(s) updated Time updated: 2022/06/17 15:52:36			Import Application List ~ + Add New Application	
۲	Object	Туре	Description	Created Time Action	
	C:\tempransomware.exe	Path	import from file	2022/06/15 15:06:46	
	D:\Doc\tmp.dll	Path	import from file	2022/06/15 15:06:46	
×	B5A45CF9385E4E3F43D6DF8FDCE52D26E14B4D93		rom file	2022/06/15 15:06:46	
Ē	*\temp\virus.dll	Add new application	from file	2022/06/15 15:06:46	
ത	*malware.*	Application name	from file	2022/06/15 15:06:46	
÷	D8D2C6E11B3D295C08FEF124870F9863CEDADF12	Chrome	from file	2022/06/15 15:06:46	
	C:\Windows\System32\asdawb.exe	Hash/path O Path O Hash	Test	2022/02/08 14:38:11	
		C	Cancel Apply 3		

3.10.1.4 Thêm mới ứng dụng/tiến trình từ tập tin có sẵn

Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại;

Click "Import", chọn đường dẫn đến file cần tải lên và click "Open", hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống.



	Viettet a Jiant Protect & Prevent / Application Control			** 0							
₽ •	Q, Type object path/hash to search										
н ₄	0 agent(s) spdated Time updated 2022/06/17 155236 Import Applica										
۹	Object	Туре	Description	Download sample file							
	C\tempransomware.exe D\Doc\tmp.dll	Path	import from file	2022/06/15 15:06:46							
Ē	B5N45CF9385E4E3F4306DF8FDCE52D26E14B4D93 *\temp\virus.dll	Hash Path	import from file import from file	2022/06/15 15:06:46							
ē	*maiware.* popological popological popological popological popological	Path	import from file	2022/06/15 15:06:46							
	Deb2/de1163/2/50/08/EF124670/9603/EE/NUF12 C:\Windows\System32\addawb.exe	Path	AnhNN Test	2022/02/08 14:38:11							

3.10.1.5 Xóa ứng dụng/tiến trình bị chặn trong danh sách

Hệ thống hỗ trợ xóa 1 hoặc nhiều ứng dụng bị chặn;

Click vào từng ứng dụng cần xóa và click icon "Delete", hoặc click vào checbox đầu mỗi ứng dụng và click nút "Delete"

a	ettel Jia	Protect & Prevent / Application Control				# O
Q	Туре	e object path/hash to search				۹
	0 agen	nt(s) updated Time updated: 2022/06/17 15:52:36			Import Application List \checkmark	+ Add New Application
	Sele	ected 2 aplication(s) Cancel				
	•	Object	Туре	Description	Created Time	Action
1 1		C:\tempransomware.exe	Path	import from file	2022/06/15 15:06:46	
		D:\Doc\tmp.dll	Path	import from file	2022/06/15 15:06:46	
		B5A45CF9385E4E3F43D6DF8FDCE52D26E14B4D93	Hash	import from file	2022/06/15 15:06:46	
		*\temp\virus.dll		import from file	2022/06/15 15:06:46	
		malware.	<u> </u>	import from file	2022/06/15 15:06:46	
		D8D2C6E11B3D295C08FEF124870F9863CEDADF12		import from file	2022/06/15 15:06:46	
		C:\Windows\System32\asdawb.exe	Delete	AnhNN Test	2022/02/08 14:38:11	
			Are you sure you want to delete application ? Cancel			

3.10.1.6 Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công

Sau khi người dùng thêm/sửa/xóa danh sách các tiến trình trên giao diện, hệ thống sẽ cập nhật danh sách này xuống dưới các agent theo luồng update file agent (chu kỳ 3 phút/lần). Agent nhận được cấu hình mới, phát sinh log với eventID =101 và đẩy lên server, hiển thị trên màn hình Event search. Sau đó hệ thống sẽ tự động cập nhật số lượng agent đã cập nhật danh sách cấu hình mới trên màn Application control.

Q Type object path/hash to search		٩
0 agent(s) updated Time updated: 2022/06/17 15:52:36	Import Application List \checkmark	+ Add New Application



3.10.2 Endpoint Firewall

Mục đích: Chức năng Endpoint Firewall cho phép cấu hình các kết nối sẽ chặn dưới máy người dùng, bao gồm chặn theo ip, port, hoặc cả ip và port, hỗ trợ các protocol TCP, UDP, ICMP, hỗ trợ Ipv4 và Ipv6, hỗ trợ inbound và outbound connection.

3.10.2.1 Hiển thị danh sách các kết nối bị chặn

Click vào tab Protect & Prevention > chọn Endpoint Firewall sẽ hiển thị toàn bộ danh sách các kết nối bị chặn.

≡	vie aJ	ttel iant Protect & Prevent / Endpoint Fin	rewall						# 0
S.	End	point Firewall							Guidelines
▲	8 resu	ilt(s) Agent updated: 0 Time updated:	: 2022/06/07 09:49:20				Q Type IP or port to search	1 import v	+ Create
P _±		P	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION		4.00
0		192.168.4.5/24	80	INBOUND	UDP	2022/03/28 14:02:09	import from file		Û
Q		123.168.5.6	2345	OUTBOUND	ICMPV6	2022/03/28 14:02:09	import from file		û
>		123.168.5.5	2345	OUTBOUND	ICMP	2022/03/28 14:02:09	import from file		Û
		192.168.2.5	44	ALL	ALL	2022/03/28 14:02:09	import from file		Û
×		192.168.2.5	22	INBOUND	TCP	2022/03/28 14:02:09	import from file		û
Ē		122.13.4.5	2343	ALL	ALL	2022/03/28 14:02:09	import from file		û
ര		3.2.2.43/8	4	ALL	ALL	2022/03/28 14:02:09	import from file		Û
-		1.2.3.4	8888	ALL	ALL	2022/02/08 14:43:58	AnhNN Test		ŵ
	Showi	ng 8/8 result(s)							

3.10.2.2 Tìm kiếm các kết nối bị chặn

Người dùng có thể tìm kiếm theo địa chỉ IP và port đã thiết lập;

≡	Viettet a Jiant Protect & Prevent / Endpoint Firewall										
Ş	Endpoint Firewall										
▲	1 result(s) Agent updated: 0 Time updated	: 2022/06/07 09:49:20				Q 122 x	+ Create				
P _±	□ P	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION	+				
a	122.13.4.5	2343	ALL	ALL	2022/03/28 14:02:09	import from file	Û				
ď	Showing 1/1 result(s)										
Þ											
\bigcirc											
Ē.											
ē											

3.10.2.3 Thêm mới các kết nối bị chặn

Click nút "Add new", nhập thông tin trên popup thêm mới kết nối bị chặn

- + IP: địa chỉ IP cần chặn;
- + Port: port cần chặn, nếu chặn tất cả port thì nhập 0;
- + Direction: inbound, outbound, All (chặn cả 2 chiều);
- + Protocol: ICMP, TCP, UDP, ICMPV6, ALL;



_	vie	ttel	Destant & Descart / Factoria Fi						× 0
	a	iant	Protect & Prevent / Endpoint Fil	rewall					2 U
Ę	Endp	oint Firew	all						D Guidelines
▲	8 resu	lt(s)	Agent updated: 0 Time updated	1: 2022/06/07 09:49	20			Q Type IP or port to sea	rch Import + Create
₹ _±		P		PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION	s 🤨
		192.168.4.5	/24	80	INBOUND	UDP	2022/03/28 14:02:09	import from file	ū
ď		123.168.5.6		2345	OUTBOUND	ICMPV6	2022/03/28 14:02:09	import from file	ů
5		123.168.5.5		2345	OUTBOUND	ICMP	2022/03/28 14:02:09	import from file	ū
		192.168.2.5		44	ALL	2 411	2022/02/29 14:02:00	import from filo	D D D D D D D D D D D D D D D D D D D
–		192.168.2.5		22	Create			×	ū
Ē,		122.13.4.5		2343	IP	123.168.5.6			Û
۲		3.2.2.43/8		-1	Port	80			ů
Ť		1.2.3.4		8888					Ū.
	Showi	ng 8/8 result(s)		Direction	INBOUND		<u> </u>	
					Protocol	UDP		~	
					Description	import from file			
Cancel Create							Cancel Create		
									1

3.10.2.4 Thêm mới kết nối bị chặn từ tập tin có sẵn

Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại;

Click nút "Import", chọn đường dẫn đến file cần tải lên và click nút "Open", hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống;

	vie a_	ttel Protect & Prevent / Endpoint Fire	ewall					* 0
Ş	End	point Firewall						📮 Guidelines
▲	8 resi	ult(s) Agent updated: 0 Time updated:	2022/06/07 09:49:20				Q Type IP or port to search	1 Import - Create
Η		p	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION	2
@		192.168.4.5/24	80	INBOUND	UDP	2022/03/28 14:02:09	import from file	û
Q		123.168.5.6	2345	OUTBOUND	ICMPV6	2022/03/28 14:02:09	import from file	Û
> -		123.168.5.5	2345	OUTBOUND	ICMP	2022/03/28 14:02:09	import from file	û
		192.168.2.5	44	ALL	ALL	2022/03/28 14:02:09	import from file	û
×		192.168.2.5	22	INBOUND	TCP	2022/03/28 14:02:09	import from file	û
Ē		122.13.4.5	2343	ALL	ALL	2022/03/28 14:02:09	import from file	û
ര		3.2.2.43/8	-1	ALL	ALL	2022/03/28 14:02:09	import from file	Û
-		1.2.3.4	8888	ALL	ALL	2022/02/08 14:43:58	AnhNN Test	û
	Showi	ing 8/8 result(s)						

3.10.2.5 Xóa kết nối bị chặn trong danh sách

Hệ thống hỗ trợ xóa 1 hoặc nhiều kết nối bị chặn;

Click vào từng kết nối cần xóa và click icon "Delete", hoặc click vào checbox đầu mỗi kết nối và click nút "Delete";



≡	aJi	Protect & Prevent / Endpoint Fit	ewall						* 0
Ę,	Endp	oint Firewall							📁 Guidelines
▲	8 resul	t(s) Agent updated: 0 Time updated	: 2022/06/07 09:49:20				Q. Type IP or port to search	1 Import 🗸	+ Create
r _±	Selec	ted (2) Delete Cancel							
۲		P	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION		2
\sim		192.168.4.5/24	80	INBOUND	UDP	2022/03/28 14:02:09	import from file		
		123.168.5.6	2345	OUTBOUND	ICMPV6	2022/03/28 14:02:09	import from file		
		123.168.5.5	2345	OUTBOUND	ICMP	2022/03/28 14:02:09	import from file		
		192.168.2.5	44	ALL	ALL	2022/03/28 14:02:09	import from file		
Ēλ		192.168.2.5	22	INBOUND	TCP	2022/03/28 14:02:09	import from file		
٥		122.13.4.5	2343	ALL			import from file		
Ť		3.2.2.43/8	-1	ALL		×	import from file		
		1.2.3.4	8888	ALL		U I	AnhNN Test		
	Showin	g 8/8 result(s)			Del	ete object			
					Are you sure yo	u want to delete objects ?			
					Can	cel Delete			

3.10.2.6 Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công

Sau khi người dùng thêm/sửa/xóa danh sách các kết nối trên giao diện, hệ thống sẽ cập nhật danh sách này xuống dưới các agent theo luồng update file agent (chu kỳ 3 phút/lần). Agent nhận được cấu hình mới, phát sinh log với eventID =201 và đẩy lên server, hiển thị trên màn hình Event search. Sau đó hệ thống sẽ tự động cập nhật số lượng agent đã cập nhật danh sách cấu hình mới trên màn Endpoint Firewall;

3.11 Anti – Malware

3.11.1 Scan Schedule

Mục đích: Chức năng Scan Schedule cho phép người dùng lập lịch quét virus dưới các máy trạm từ xa.

3.11.1.1 Tìm kiếm Scan Schedule task

Mục đích: Chức năng tìm kiếm Scan Schedule task cho phép người dùng tìm kiếm các lập lịch quét dưới các máy trạm theo Task name.

Các bước thực hiện:



Task name Author Created time Scan type Number of agent(s) Trigger Start time Next run time Expired time Scan type uburtu 2 root 06/10/2022 · 161556 Quick scan 1 Immediately 06/10/2022 · 161556 N/A N/A N/A Quick Win 11 root 06/10/2022 · 161734 Quick scan 1 Immediately 06/10/2022 · 161734 N/A N/A N/A Quick Win 11 root 06/10/2022 · 160734 Quick scan 1 Immediately 06/10/2022 · 160734 N/A N/A N/A Quick Win 11 root 06/10/2022 · 160734 Quick scan 1 Immediately 06/10/2022 · 160734 N/A N/A Quick scan 1 Immediately 06/10/2022 · 160734 N/A N/A Quick scan 1 Immediately 06/10/2022 · 160734 N/A N/A Quick scan 1 Immediately 06/10/2022 · 160734 N/A N/A Quick scan 1 Immediately 06/10/2022 · 160734 N/A N/A Quick scan 1 Immediately	edule 🔶 Status • Finished • Finished • Finished	New ta Actio	
Created time Soan type Number of agent(s) Trigger Start time Not nu time Expired time Scan type Number of agent(s) Trigger Start time Not nu time Expired time Scan type Number of agent(s) Trigger Start time Not a N/A N/A <th col<="" th=""><th>edule 🛨 Status • Finished • Finished</th><th>New ta Actio</th></th>	<th>edule 🛨 Status • Finished • Finished</th> <th>New ta Actio</th>	edule 🛨 Status • Finished • Finished	New ta Actio
Task name Author Created time Scan type Number of agent(s) Trigger Start time Next run time Expired time Scan type ubuntu 2 root 06/10/2022 - 16:15:56 Quick scan 1 Immediately 06/10/2022 - 16:15:56 N/A N/A VIA Ubuntu root 06/10/2022 - 16:15:40 Quick scan 1 Immediately 06/10/2022 - 16:11:44 N/A N/A VIA Quick Win 11 root 06/10/2022 - 16:07:34 Quick scan 1 Immediately 06/10/2022 - 16:07:34 N/A N/A VIA VI	Status Finished Finished Finished	Actio	
ubuntu 2 root 06/10/2022 - 16:15:56 Quick scan 1 Immediately 06/10/2022 - 16:15:56 N/A N/A N/A Ubuntu root 06/10/2022 - 16:11:44 Quick scan 1 Immediately 06/10/2022 - 16:11:44 N/A N/A N/A Quick Win 11 root 06/10/2022 - 16:07:34 Quick scan 1 Immediately 06/10/2022 - 16:07:34 N/A N/A N/A Quick Win 11 root 06/10/2022 - 16:07:34 Quick scan 1 Immediately 06/10/2022 - 16:07:34 N/A N/A Quick Win 11 root 06/10/2022 - 16:03:41 Custom scan 1 Immediately 06/10/2022 - 16:03:41 N/A N/A Quick Scan 1 At 06/10/2022 - 16:03:41 N/A N/A N/A Quick Scan 1 At 06/10/2022 - 16:03:41 N/A N/A N/A Quick Scan 1 At 06/10/2022 - 16:03:41 N/A N/A N/A Quick Scan 1 At 06/10/2022 - 16:03:41 N/A N/A Quick Scan 1 At 06/10/2022 - 16:03:41 N/A N/A	 Finished Finished Finished 		
Ubuntu root 06/10/2022-16.11:44 Quick scan 1 Immediately 06/10/2022-16.11:44 N/A N/A N/A Quick Win 11 root 06/10/2022-16.07.34 Quick scan 1 Immediately 06/10/2022-16.07.34 N/A	Finished		
Quick Win 11 root 06/10/2022-16:07:34 Quick scan 1 Immediately 06/10/2022-16:07:34 N/A N/A N/A Task win 11 root 06/10/2022-16:07:34 Custom scan 1 Immediately 06/10/2022-16:07:34 N/A N/A N/A N/A Task 456 mot 06/10/2022-11:37:08 Quick scan 1 At 06/10/2022-12:39:30 06/10/2022-12:39:30 N/A N/A N/A	Finished		
Task win 11 root 06/10/2022-16/0341 Custom scan 1 Immediately 06/10/2022-16/0341 N/A N/A 4 Task 456 root 06/10/2022-11/37/08 Ouick scan 1 A106/10/2022-12/39/30 06/10/2022-12/39/30 N/A N/A 4			
Task 456 root 06/10/2022 - 11:37:08 Oulck scan 1 At 06/10/2022 - 12:39:30 06/10/2022 - 12:39:30 N/A N/A	Finished		
	Finished		
Task 123 root 06/10/2022 11:34:26 Quick scan 1 Immediately 06/10/2022 11:34:26 N/A N/A	Finished		
éwewe root 06/10/2022 - 11:17:59 Quick scan 2 Immediately 06/10/2022 - 11:17:59 N/A N/A N/A	Finished		
Task 1 root 06/10/2022 - 11:14:04 Quick scan 2 Immediately 06/10/2022 - 11:14:04 N/A N/A	Finished		
Task mai root 06/10/2022 - 11:10:10 Quick scan 1 Immediately 06/10/2022 - 11:10:10 N/A N/A	Finished		
maltest root 06/10/2022 - 10:5437 Quick scan 1 Immediately 06/10/2022 - 10:5437 N/A N/A	Finished		
Task 2 root 06/10/2022 - 09:09:09 Custom scan 1 Immediately 06/10/2022 - 09:09:09 N/A N/A	Finished		

Bước 4: Người dùng nhập vào từ khóa tìm kiếm;

- **Bước 5:** Chọn nút A hoặc nhấn **Enter** để xác nhận thao tác tìm kiếm với từ khóa vừa nhập.
- Bước 6: Hệ thống sẽ hiển thị danh sách lập lịch quét theo từ khóa tìm kiếm.

3.11.1.2 Thêm mới Scan Schedule task

Mục đích: Cho phép người dùng thêm mới một lập lịch quét, cấu hình thời gian và thông tin máy trạm.

Các bước thực hiện:

Bước 7: Tại màn hình danh sách lập lịch quét, người dùng chọn nút New task



=	aJiant Anti-Malware	/ Scan Scheduler									# 0
Ţ.	Q Search										Q
▲ [∓] ≟	Showing 11 of 11 result(s)								Show only my s	schedule 🕒	1 New task
0	Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
1	ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	 Finished 	
<u>D-</u>	Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	Finished	
◙	Quick WIn 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	Finished	
-	Task win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	Finished	
	Task 456	root	06/10/2022 - 11:37:08	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	Finished	
Ē <u>.</u>	Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	 Finished 	
-	éwewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	Finished	
ц <u>я</u>	Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	 Finished 	
	Task mai	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	Finished	
	maitest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	Finished	
	Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	 Finished 	
										Ø Ba	ack to top
											4

Bước 8: Hệ thống hiển thị màn hình thêm mới một lập lịch quét, người dùng nhập vào các thông tin:

≡	aJiant Anti-Malware / S	Scan Scheduler										* 0
1 A	Q Search											Q
▲ ™	Showing 11 of 11 result(s)			F	Create new task	>	<			Show only	my schedule	New task
0	Task name	Author	Created time	Scar	Task name		time		Next run time	Expired time	Status	Action
	ubuntu 2	root	06/10/2022 - 16:15:56	Quic			10/2022 - 1	6:15:56	N/A	N/A	Finished	
<u>.</u>	Ubuntu	root	06/10/2022 - 16:11:44	Quic	new task i		10/2022 - 1	6:11:44	N/A	N/A	 Finished 	
	Quick Win 11	root	06/10/2022 - 16:07:34	Quic	Scan type 🚯	Priority 🚯	10/2022 - 1	6:07:34	N/A	N/A	Finished	
	Task win 11	root	06/10/2022 - 16:03:41	Cust	Quick scan	Low	10/2022 - 1	6:03:41	N/A	N/A	 Finished 	
*	Task 456	root	06/10/2022 - 11:37:08	Quic	Tringer		10/2022 - 1	2:39:30	N/A	N/A	 Finished 	
Ē	Task 123	root	06/10/2022 - 11:34:26	Quic	When this task is created		2 0/2022 - 1	1:34:26	N/A	N/A	 Finished 	
_	éwewe	root	06/10/2022 - 11:17:59	Quic	Run immediately		10/2022 - 1	1:17:59	N/A	N/A	 Finished 	
의	Task 1	root	06/10/2022 - 11:14:04	Quic	 Run on a schedule 		10/2022 - 1	1:14:04	N/A	N/A	 Finished 	
	Task mai	root	06/10/2022 - 11:10:10	Quic	Assignee(s)		10/2022 - 1	1:10:10	N/A	N/A	 Finished 	
	maitest	root	06/10/2022 - 10:54:37	Quic	 All agents (total 38 agents) 		0/2022 - 1	0:54:37	N/A	N/A	 Finished 	
	Task 2	root	06/10/2022 - 09:09:09	Cust	 Choose group(s) and agent(s) 		10/2022 - 0	9:09:09	N/A	N/A	 Finished 	
					0 assignee(s)	Add agent/group Import from list •						
					Information of selected	agent(s) will be showing here.	-					
						Cancel Create	1					
												tack to top
												14

2 - Thông tin lập lịch quét bao gồm: Task name, Scan type, Priority

Task name: Người dùng nhập vào tên lập lịch quét;

Scan type: Người dùng lựa chọn một trong 3 loại scan. Cho phép:

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 248



+ Quét nhanh: Kiểm tra nhanh các tệp và thư mục đáng ngờ tiềm ẩn;

+ Quét toàn bộ: Kiểm tra toàn bộ các tệp và thư mục trong máy tính. Quá trình này có thể mất vài giờ để hoàn thành;

+ Quét tùy chỉnh: Cho phép người dùng một tệp / thư mục cụ thể trong máy tính của bạn để quét.

Priority: Cho phép người dùng lựa chọn tốc độ quét và thay đổi mức độ chiếm dụng tài nguyên của máy. Khi đặt mức ưu tiên cao, hệ thống sẽ quét nhanh chóng, tuy nhiên sẽ tiêu tốn nhiều tài nguyên của CPU. Tương tự, nếu chọn mức độ ưu tiên thấp, hệ thống sẽ quét chậm hơn và tiết kiệm tài nguyên CPU.

3 – Thông tin Trigger cho phép người dùng lựa chọn loại lập lịch quét:

Run immediately: Cho phép người dùng lập lịch quét ngay lập tức dưới các máy trạm khi task vừa được tạo thành công;

Run on Schedule: Cho phép người dùng lập lịch quét theo cấu hình của người dùng:

Run on a schedule	
One time	~
Start time	
31/10/2022 - 10:45:27	団
Run task as soon as possible after a schedule is misse	ed 🚯

- + Schedule:
 - One time: Lập lịch quét một lần;
 - Daily: Lập lịch quét hàng ngày;
 - Weekly: Lập lịch quét hàng tuần;
 - Monthly: Lập lịch quét hàng tháng;
- + Start time: Cho phép người dùng nhập vào thời gian bắt đầu lập lịch quét



+ Ví dụ: Schedule: Daily, Start time: 15/08/2022 – 03:00:00. Được hiểu là cấu hình lập lịch quét hàng ngày lúc 03:00:00;

+ Run task as soon as possible after schedule is missed: Cho phép người dùng cấu hình lập lịch quét lại ngay khi lập lịch trước bị bỏ lỡ.

4 – Thông tin Assignee: Cho phép người dùng cấu hình thông tin các máy trạm nhận lập lịch

All Agent(s): Lập lịch với tất cả các máy trạm thuộc quyền quản lý của người dùng đang đăng nhập;

Choose Agent(s) or Group(s):

+ Mục đích: Cho phép cấu hình, lựa chọn các máy trạm hoặc các nhóm máy

trạm:

As	signee(s)		
0	All agents (total 38 agents)		
0	Choose group(s) and agent(s)		2
	0 assignee(s)		Import from list▼
	Information of se	lected agent(s) will be sho	wing here.

+ Các bước thực hiện: Add Agents or Group

• Add Agents or Group - Người dùng chọn **Add Agent**. Hệ thống hiển thị popup lựa chọn máy trạm:



Q Search				Create	new	task		×						
Showing 11 of 11 result(s)				Task name	•							Show only	my schedule	New tas
Task name	Author	Created tin	Add	agent(s)						×	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/202	fx	Search by queries					_	Q	N/A	N/A	· Finished	
Ubuntu	root	06/10/202	-						_		N/A	N/A	· Finished	
Quick Win 11	root	06/10/202	38 res	sult(s)				121000			N/A	N/A	· Finished	
Task win 11	root	06/10/202	0	Agent ID		Computer name	IP Address	Group		status	N/A	N/A	· Finished	
Task 456	root	06/10/202		06A6927157E4EEE09A00	C76	ajiant-agent-centos6	127.0.0.1, 10.255.250	auto_test			N/A	N/A	· Finished	***
Task 123	root	06/10/202		0715289C3AB47DF72E6	E6C	phula-viettelos1018	127.0.0.1, 192.168.12	default		• Offline	N/A	N/A	· Finished	
éwewe	root	06/10/202		0A691ACC638F0D4E54C	A75_	Win7x64-A-PC	10.0.2.15, 127.0.0.1	maitest1		Offline	N/A	N/A	· Finished	
Task 1	root	06/10/202		0AC36E41E40C67DE5A1	EF8_	phula-redhat7.7	127.0.0.1, 192.168.12	chuyen_test		offline	N/A	N/A	· Finished	
Task mai	root	06/10/202		0B726365F86EBFF5000E	E6B2_	localhost.localdomain	127.0.0.1, 192.168.19	no_group		• Offline	N/A	N/A	 Finished 	
maitest	root	06/10/202		0E1CBE9249C35DCDF76	i3F2	ubuntu	127.0.0.1, 192.168.12	maitest1_1		• Offline	N/A	N/A	 Finished 	
Task 2	root	06/10/202		155E59FAED2450B57500	CEF	phula.redhat8.4	127.0.0.1, 192.168.12	global		• Offline	N/A	N/A	 Finished 	
				15706171377B8D10F47E	BE8	agent-core-mac	127.0.0.1, 192.168.6.2.	. no_group		• Offline				
								(1 2	3 4	5 >				
										- <i>6</i>				
								Car	ncel					
							Cancel	Consta						
							Curren	(Section 1)						
				Contraction of the local division of the loc										

• Tìm kiếm máy trạm:

 Tại popup Add agent(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: AgentID, Computer name, IP Adress, Group, Status, …

Người dùng chọn icon a hoặc nhấn nút Enter để xác nhận tìm

kiếm;

- Hệ thống sẽ hiển thị danh sách máy trạm theo truy vấn.
- Tích chọn một hoặc nhiều các máy trạm để thực thi lập lịch quét:



Q Search				Create new	v task		×					
Showing 11 of 11 result(s)			Add	d agent(s)				×		Show only	my schedule	New tas
Task name	Author	Created tin	fx	Search by queries				Q	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/202	Selec	cted (1)					N/A	N/A	Finished	
Ubuntu	root	06/10/202	pl	hula-redhat7.7 \times				0 ~	N/A	N/A	 Finished 	
Quick Win 11	root	06/10/202							N/A	N/A	 Finished 	
Task win 11	root	06/10/202	38 re	sult(s)					N/A	N/A	 Finished 	
Task 456	root	06/10/		Agent ID	Computer name	IP Address	Group	Status	N/A	N/A	 Finished 	
Task 123	root	06/10/202	0	06A6927157E4EEE09A0C76.	ajiant-agent-centos6	127.0.0.1, 10.255.250.	_ maitest1_2_3	e Offline	N/A	N/A	 Finished 	
éwewe	root	06/10/202	0	0715289C3AB47DF72E6E6C.	phula-viettelos1018	127.0.0.1, 192.168.12.	default	e Offline	N/A	N/A	 Finished 	
Task 1	root	06/10/202	0	0A691ACC638F0D4E54CA75	Win7x64-A-PC	10.0.2.15, 127.0.0.1	maitest1	e Offline	N/A	N/A	 Finished 	
Task mai	root	06/10/202		0AC36E41E40C67DE5A1EF8.	phula-redhat7.7	127.0.0.1, 192.168.12.	. chuyen_test	e Offline	N/A	N/A	 Finished 	
maitest	root	06/10/202	0	0B726365F86EBFF5000E6B2	_ localhost.localdomain	127.0.0.1, 192.168.19.	. no_group	• Offline	N/A	N/A	 Finished 	
Task 2	root	06/10/202	0	0E1CBE9249C35DCDF763F2	ubuntu	127.0.0.1, 192.168.12.	maitest1_1	• Offline	N/A	N/A	 Finished 	
				155E59FAED2450B5750CEF.	phula.redhat8.4	127.0.0.1, 192.168.12.	global	e Offline				
				15706171377B8D10F47BE8	agent-core-mac	127.0.0.1, 192.168.6.2	_ no_group	e offline				
			-									
								4 3 7				
							Cancel	Add	2			
			-	_		Cancel	Create and		1			
						Guiner						

- Chọn nút Add để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút Cancel để thực hiện hủy thao tác thêm thông tin Agent/ Group;

➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin máy trạm đã được chọn.

• Add Agents or Group - Người dùng chọn **Add Group**. Hệ thống hiển thị popup lựa chọn group:

• Tìm kiếm group:

 Tại popup Add group(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: Group name

Người dùng chọn icon a hoặc nhấn nút Enter để xác nhận tìm

kiếm;

- → Hệ thống sẽ hiển thị danh sách group
 - Tích chọn một hoặc nhiều group để thực thi lập lịch quét:

Page | 252


≡	aJiant Anti-Malware / Sc	an Scheduler									# 0
	Q Search			Add group(s)				×			٩
A				Q Search by group name				Q			
Ρđ	Showing 50 of 759.426 result(s)			• NOTE: In this interface, users b	elonging to	the parent group have full control over all the child	d groups of their parent gr Se	e more >>		Show only	my schedule 🕒 New task
0	Task name	Author	Created time	TENANT nsm con	n)	Sthanhnm18 test	S & liennt		Next run time	Expired time	Status Action
	Duplicate this task	root_test	22/09/2022 - 1		. ,		0 00		5 N/A	N/A	 Finished
6	Test immediately	root_test	22/09/2022 - 1	🗖 💑 global	>	🖉 💑 no_group 💦 🔉			7 N/A	N/A	 Finished
	Task name immediately main	root_test	22/09/2022 - 1	🗖 🐣 admin	>	D S phula test	1		7 N/A	N/A	Finished
	Task name immediately mai	root_test	22/09/2022 - 1			0.00			7 N/A	N/A	 Finished
*	Task name immediately	root_test	22/09/2022 - 1	TENANT_edr.com	>	new_group			7 N/A	N/A	 Finished
Ê	Task test immediately	root_test	22/09/2022 - 1	TENANT_viettel.c	>	n 🖧 anhnn_test 🔹			5 N/A	N/A	 Finished
	Task mai test immediately	root_test	22/09/2022 - 0			- •••	1	_	5 N/A	N/A	 Finished
ي ا	data 1	root_test	20/09/2022 - 1	Selected					> N/A	N/A	Finished
	test create	root_test	16/09/2022 - 1	3 group(s)					N/A	N/A	 Finished
	create test agent edr test 2	root_test	14/09/2022 - 1	Group	Loca	tion		Action	2 N/A	N/A	 Finished
	data-test-1-20-5-9-999	root_test	09/09/2022 - 1	TENANT_nsm.com					5 N/A	N/A	 Finished
	data-test-1-20-5-9-998	root_test	09/09/2022 - 1	vcs_server	globr	al		×	5 N/A	N/A	 Finished
	data-test-1-20-5-9-997	root_test	09/09/2022 - 1						5 N/A	N/A	Finished
	data-test-1-20-5-9-996	root_test	09/09/2022 - 1	💑 no_group	admi	in			5 N/A	N/A	 Finished
	data-test-1-20-5-9-995	root_test	09/09/2022 - 1						5 N/A	N/A	Finished
	data-test-1-20-5-9-994	root_test	09/09/2022 - 1						5 N/A	N/A	 Finished
	data-test-1-20-5-9-993	root_test	09/09/2022 - 1						5 N/A	N/A	Finished
	data-test-1-20-5-9-992	root_test	09/09/2022 - 1						5 N/A	N/A	Finished
	data-test-1-20-5-9-991	root_test	09/09/2022 - 1						5 N/A	N/A	Finished
							Cancel	Save			
								·			G Back to top

- Chọn nút Add để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút Cancel để thực hiện hủy thao tác thêm thông tin Agent/ Group;
- ➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin group đã được chọn.

+ Import from .CSV: Cho phép người dùng tải lên danh sách máy trạm bằng cách:

• Lựa chọn vào nút Import from list;

• Lựa chọn **Download sample file**, cho phép tải xuống file mẫu danh sách máy trạm;

• Người dùng nhập thông tin máy trạm và tải lên file danh sách máy trạm bằng cách chọn nút **Import from .CSV**

Bước 9: Người dùng chọn nút **Create** để hoàn thiện thao tác thêm mới lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác thêm mới lập lịch quét

Page | 253



3.11.1.3 Nhân bản Schedule task

Mục đích: Cho phép người dùng nhân bản lập lịch quét.

Các bước thực hiện:

Bước 10: Tại màn hình danh sách task, người dùng chọn **Duplicate** bản ghi task cần nhân bản:

Ż	Anti-Malware / Sci Jiant	in Scheduler									* (
	Q Search										
	Showing 11 of 11 result(s)								Show only m	ny schedule	New task
	Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
	ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	Finished	
	Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	View report	
	Quick Win 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	View detail	
	Task win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	Duplicate this task	¢
	Task 456	root	06/10/2022 - 11:37:08	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	Delete this task	_
	Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	• Fillionou	
	éwewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	Finished	
	Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	Finished	
	Task mai	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	Finished	
	maitest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	Finished	
	Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	Finished	
										🕜 Ba	

Bước 11: Hệ thống hiển thị màn hình Duplicate task, người dùng nhập lại task name và kiểm tra lại toàn bộ thông tin trước khi nhân bản



O const											
Q Search			-	Duplicate task			×				
				Task name							
Showing 50 of 759.426 res	sult(s)									Show only	my schedule 🕀 New t
Tack name	Author	Created time	Foot					rt time	Next nun time	Expired time	Status Activ
Duplicate this task	Aution	01/00/2022 17:25/26	Oraia	 You can't leave this field blank Scan type 	Priority ()			00/2022 17/25/26	Next full title	Expired time	a Cinished
Dupricate this task	TOOCtest	22/09/2022 - 17.23.30	Quic	Quick coop	Ne Low			09/2022 - 17.23.30	NA	N/A	• rensed
Test ininediately	root_test	22/09/2022 - 10.50.27	Cust	Quick scall	LOW		•	09/2022-10.50.2/	N/A	N/A	• Finished
Task name immediately n	nain root_test	22/09/2022 - 10:27:27	Cust	Trigger				09/2022 - 10:30:47	N/A	N/A	• Finished
Task name immediately n	nar root_test	22/09/2022 - 10:19:37	Cust	When this task is created				09/2022 - 10:19:37	N/A	N/A	Finished
Task name immediately	root_test	22/09/2022 - 10:17:37	Cust	Run immediately Sup on a schedule				09/2022 - 10:17:37	N/A	N/A	 Finished
Task test immediately	root_test	22/09/2022 - 10:05:35	Cust	() Run on a schedule				09/2022 - 10:05:35	N/A	N/A	 Finished
Task mai test immediatel	y root_test	22/09/2022 - 09:53:55	Cust	Assignee(s)				09/2022 - 09:53:55	N/A	N/A	 Finished
data 1	root_test	20/09/2022 - 17:42:46	Quic	 All agents (total 830 agents) Choose group(s) and agent(s) 				09/2022 - 17:42:46	N/A	N/A	 Finished
test create	root_test	16/09/2022 - 15:04:59	Quic	 Choose group(s) and agent(s) 				09/2022 - 15:04:59	N/A	N/A	 Finished
create test agent edr test	2 root_test	14/09/2022 - 10:08:36	Cust	4 assignee(s)	Add agent/gro	import fro	m list▼	09/2022 - 10:10:42	N/A	N/A	 Finished
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quic	Assignee Type	Computer name	IP Address	Action	09/2022 - 18:54:45	N/A	N/A	Finished
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quic	1FBAFFB82BBC6 agent	virtual_agent_phul	172.17.0.22		09/2022 - 18:54:45	N/A	N/A	 Finished
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quic	09D9E77F49E63 agent	virtual_agent_phul	172.17.0.2		09/2022 - 18:54:45	N/A	N/A	 Finished
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quic	504615DE542C6 agent	Win10x64MAINTN	192.168.74.12	В	09/2022 - 18:54:45	N/A	N/A	Finished
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quic	EC8EB5F0DAB21 agent	Win10x64_MaiNT	N 192.168.74.12	в	09/2022 - 18:54:45	N/A	N/A	 Finished
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quic				-	09/2022 - 18:54:45	N/A	N/A	 Finished
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quic					09/2022 - 18:54:45	N/A	N/A	 Finished
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quic					09/2022 - 18:54:45	N/A	N/A	• Finished
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quic			Cancel		09/2022 - 18:54:45	N/A	N/A	Finished
		40.00.0000 AD 54.15	-10		2.1.2	_					State and

Bước 12: Người dùng chọn nút **Create** để hoàn thiện thao tác nhân bản lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác nhân bản lập lịch quét.

Q Search			1	AL 10 (487/68 0)									
				Duplicate task				×					
Showing 50 of 759 426 result(s)				Task name							Show only	my schedule	New
sources and a second se				Task 1							a show only		TUT
Task name	Author	Created time	Scar	L					rt time	Next run time	Expired time	Status	Acti
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quic	Scan type 0	PI	riority 😗			09/2022 - 17:25:36	N/A	N/A	 Finished 	
Test immediately	root_test	22/09/2022 - 10:56:27	Cust	Quick scan	~	Low		~	09/2022 - 10:56:27	N/A	N/A	 Finished 	
Task name immediately main	root_test	22/09/2022 - 10:27:27	Cust	Trigger					09/2022 - 10:30:47	N/A	N/A	 Finished 	
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Cust	When this task is created					09/2022 - 10:19:37	N/A	N/A	 Finished 	
Task name immediately	root_test	22/09/2022 - 10:17:37	Cust	 Run immediately 					09/2022 - 10:17:37	N/A	N/A	· Finished	
Task test immediately	root_test	22/09/2022 - 10:05:35	Cust	 Run on a schedule 					09/2022 - 10:05:35	N/A	N/A	 Finished 	
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Cust	Assignee(s)					09/2022 - 09:53:55	N/A	N/A	 Finished 	
data 1	root_test	20/09/2022 - 17:42:46	Quic	 All agents (total 836 agents) 					09/2022 - 17:42:46	N/A	N/A	 Finished 	
test create	root_test	16/09/2022 - 15:04:59	Quic	 Choose group(s) and agent(s) 					09/2022 - 15:04:59	N/A	N/A	 Finished 	
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Cust	4 assignee(s)	🕀 Add	agent/group	Import from	n list v	09/2022 - 10:10:42	N/A	N/A	· Finished	
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quic	Assignee Type	Compute	er name II	P Address	Action	09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quic	1FBAFFB82BBC6 agent	virtual_a	igent_phul 1	172.17.0.22		09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quic	09D9E77F49E63 agent	virtual_a	gent_phul 1	172.17.0.2		09/2022 - 18:54:45	N/A	N/A	· Finished	
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quic	504615DE542C6 agent	Win10x6	MAINTN 1	192.168.74.128		09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quic	EC8EB5F0DAB21 agent	Win10x6	4_MaiNTN 1	192.168.74.128		09/2022 - 18:54:45	N/A	N/A	· Finished	
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quic					-	09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quic				<	•••	2/2022 - 18:54:45	N/A	N/A	• Finished	
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quic						/2022 - 18:54:45	N/A	N/A	• Finished	
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quic				Cancel	Create	09/2022 - 18:54:45	N/A	N/A	• Finished	
			-	10 1	P. 1.1	-						and the second	

3.11.1.4 **Xem** chi ti**ết**

Mục đích: Cho phép người dùng xem thông tin chi tiết lập lịch quét Các bước thực hiện:



Page | 255



Bước 13: Tại màn hình danh sách task, người dùng chọn **View Detail** bản ghi task cần xem chi tiết;

α.	Jiant	Toeneduler													-
C	Q Search														
					View task detail					×					
	Showing 50 of 759.426 result(s)				Task name								Show only	my schedule	New ta:
	Tack name	Author	Created time	Scor	Task test immediately						rt time	Next run time	Evoired time	Statue	Action
	Task fidille	Aution	created time	Scal							t une	Next full time	Expired unie	Status	Action
	Test immediately	root test	22/09/2022 - 17:25:36	Quic	Scan type 🕕		_	Phonty ()			09/2022 - 17:25:36	N/A	N/A	Finished	
	Task name immediately	root test	22/09/2022 - 10:30:27	Cust	Custom scan		~	Low		~	09/2022 10:36:27	N/A	N/A	Finished	
	Task name immediately main	root_test	22/09/2022 - 10:27:27	Cust	Target(s)						09/2022-10:30:47	N/A	N/A	Finished	
	Task name immediately mai	root test	22/09/2022 - 10:19:37	Cust	Application Data X					~	09/2022-10:19:37	N/A	N/A	Finished	
	Task name immediately	root_test	22/09/2022 - 10:17:37	Cust	Trimera						09/2022 - 10:17:37	N/A	N/A	Finished	
	Task test immediately	root toot	22/09/2022 - 10:05:35	Cust	When this task is create	d					09/2022 - 10:05:35	N/A	N/A	 Finished 	
	data 1	root test	22/09/2022 - 09:53:55	Ouio	 Run immediately 	u					09/2022-09:53:55	N/A	N/A	Finished	
	test create	root_test	20/09/2022 - 17:42:40	Quic	Run on a schedule						09/2022-17:42.40	N/A	N/A	Finished	
	create test agent edit test 2	root test	10/09/2022 - 15:04:59	Quic	Assignee(s)						09/2022-15:04:59	N/A	N/A	Finished	
	data tast 1 00 5 0 000	root_test	14/09/2022 - 10:08:30	Cust	All agents (total 836	6 agents)					09/2022-10:10:42	N/A	N/A	Finished	
	data-test-1-20-5-9-999	root test	09/09/2022 - 18:54:45	Quic	Choose group(s) an	id agent(s))				09/2022-18:54:45	N/A	N/A	 Finished 	
	data test 1 20 5 0 007	root test	09/09/2022 - 18:54:45	Quic	1 assignee(s)		O Ad			m list	09/2022-18:54:45	N/A	N/A	Finished	
	data test 1 20 5 0 004	root_test	09/09/2022 - 10.34.45	Quie	Assignee	Туре	Compu	ter name	IP Address	Action	00/2022-10:34.43	N/A	N/A	Finished	
	data test 1.20.5.0.005	root test	00/00/2022 - 10:54:45	Quic	AE6C56DE45E9A	agent	Maintn	Ninx64	192 168 74 128		00/2022 - 10:54:45	N/A	N/A	 Finished 	
	data-test-1-20-5-9-995	root test	09/09/2022 - 18:54:45	Quic		-gent				_	09/2022-18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-994	root test	09/09/2022 - 18:54:45	Quic					•	1 >	09/2022-18:54:45	N/A	N/A	 Finished 	
	data test 1.20.5.0.002	root test	00/00/2022 - 10:34:45	Quic							00/2022 - 10:54:45	N/A	N/A	 Finished 	
	data-test-1-20-5-0-001	root test	09/09/2022 - 18:54:45	Quic						Cancel	09/2022 - 18:54:45	N/A	N/A	Finished	
		Tool_tost	09/09/2022 * 10.34.43	Quic			10				09/2022-10.04.40		10/6	• Philshed	

→ Hệ thống hiển thị màn hình chi tiết lập lịch quét

Bước 14: Người dùng chọn nút **Cancel** hoặc icon **Close** để hủy thao tác xem chi tiết lập lịch quét

3.11.1.5 Xóa Schedule task

Mục đích: Cho phép xóa lập lịch quét trong danh sách task; Các bước thực hiện:

Bước 15: Tại màn hình danh sách task, người dùng chọn **Delete this task** bản ghi task cần xóa;



aJiant Anti-Malware / Sc	an Scheduler									+
Q Search										
Showing 50 of 759.426 result(s)								Show or	ly my schedule) New tas
Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	Finished	
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	 Finished 	
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	Finished	
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	Finished	
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	View report	
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	View detail	
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	Duplicate this task	k
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	Delete this task	
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A	• Financo	_
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A	Finished	
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
			A 11	**	and the second sec					

Bước 16: Hệ thống hiển thị màn hình popup Xác nhận xóa. Người dùng chọn No để hủy thao tác xóa lập lịch quét hoặc chọn Yes, keep delete để tiếp tục thao tác xóa

₩	aJiant Anti-Malware / Sci	an Scheduler										# 0
<u>_</u>	Q Search											Q
A												
P.H	Showing 50 of 759.426 result(s)									Show only	my schedule 🕒	New task
0	Task name	Author	Created time	Scan type	Number of agent(s)	Trigger		Start time	Next run time	Expired time	Status	Action
_	Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately		22/09/2022 - 17:25:36	N/A	N/A	• Finished	
<u>}-</u>	Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately		22/09/2022 - 10:56:27	N/A	N/A	Finished	
	Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47		22/09/2022 - 10:30:47	N/A	N/A	Finished	
	Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom sca			×	22/09/2022 - 10:19:37	N/A	N/A	Finished	
	Task name immediately	root_test	22/09/2022 - 10:17:37	Custom sca		•		22/09/2022 - 10:17:37	N/A	N/A	Finished	
Ēλ	Task test immediately	root_test	22/09/2022 - 10:05:35	Custom sca		Delete this task?		22/09/2022 - 10:05:35	N/A	N/A	Finished	
	Task mai test immediately	est immediately root_test 22/09/2022 - 09:53:55 Custom sca					22/09/2022 - 09:53:55	N/A	N/A	Finished		
ě	data 1	root_test	20/09/2022 - 17:42:46	Quick scan				20/09/2022 - 17:42:46	N/A	N/A	Finished	
_	test create	root_test	16/09/2022 - 15:04:59	Quick scan	Are you sure yo	ou want to delete the task "Task name immediately mai"?		16/09/2022 - 15:04:59	N/A	N/A	Finished	
	create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom sca				29/09/2022 - 10:10:42	N/A	N/A	Finished	
	data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan		No Yes, keep delete		09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan				09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	 Finished 	
	data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	Finished	
	data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately		09/09/2022 - 18:54:45	N/A	N/A	Finished	
_				~ ' '	**		_				ant - 1 - 1	
												ack to top

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



3.11.1.6 Xem báo cáo

Mục đích: Cho phép người dùng xem báo cáo lập lịch quét;

Các bước thực hiện:

Bước 17: Tại màn hình danh sách task, người dùng chọn **View report** bản ghi task cần xem báo cáo;

Q Search										
Showing 50 of 759.426 result(s)								Show or	ly my schedule	New t
Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Actio
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	Finished	
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	Finished	
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	Finished	
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	Finished	
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	Finished	
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	Finished	
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	Finished	
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	View report	
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A	View detail	
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A	Duplicate this tas	ik
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Delete this task	
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	• Fillioneu	
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	 Finished 	
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
			a 11	**						

Bước 18: Hệ thống hiển thị màn hình View report:

5 – Tìm kiếm:

Mục đích: Cho phép tìm kiếm truy vấn các thông tin trong báo cáo như: AgentID, Computer name, IP Address, Platform, Group, Status, Result Các bước thực hiện:



View task repo	ort						×
Task name	Task per			Created time	14/09/202	22 14:32:24	
Author	root_test			Scan type	Custom se	can 🙎	
fx						Q 🕁 Export	to Excel
5 result(s)							
Agent ID		Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F	681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.1 36	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	 Scan skip 	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59	292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	• Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E	505BF7D25CA6A7DC68D1FC37D	Blchpt3_Win10Tes t	192.168.255.1 38	Microsoft Windows 10 Pro	group_windows	• Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0
							Back to top

+ Người dùng nhập vào thông tin truy vấn và chọn icon <a> hoặc nhấn nút Enter để xác nhận truy vấn;

→ Hệ thống hiển thị danh sách kết quả báo cáo lập lịch quét sau khi truy vấn.

6 - Export to Excel

Mục đích: Cho phép người dùng tải xuống báo cáo kết quả lập lịch quét theo định dạng file Excel;

View task repo	ort						×
Task name	Task per			Created time	14/09/202	22 14:32:24	
Author	root_test			Scan type	Custom s	can	
fx						Q ± B	xport to Excel
5 result(s)							
Agent ID		Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F	681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.1 36	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	• Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59	292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	 Scan completed 	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E	505BF7D25CA6A7DC68D1FC37D	Blchpt3_Win10Tes t	192.168.255.1 38	Microsoft Windows 10 Pro	group_windows	• Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0
							Back to top



Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút **Export to Excel**

→ Hệ thống cho phép tải xuống file kết quả báo cáo lập lịch quét.

7 - View on dashboard

Mục đích: Cho phép xem báo cáo thống kê Anti-malware của hệ thống

Vie	w task repor	t						:	×
Task	name	Task per			Created time	14/09/202	22 14:32:24		
Auth	ior	root_test			Scan type	Custom s	can		
fx	6						Q Export	to Excel	d
5 res	sult(s)								
Age	ent ID		Computer name	IP Address	Platform	Group	Status	Result	
FCS	97D9289BFA70F68	81BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.1 36	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	• Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule	
524	B30C4C568F5929	92D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	 Scan completed 	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0	
F2A	A317BE87690E50	05BF7D25CA6A7DC68D1FC37D	Blchpt3_Win10Tes t	192.168.255.1 38	Microsoft Windows 10 Pro	group_windows	 Scan completed 	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0	
								Back to top	

Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút **View on** dashboard

→ Hệ thống điều hướng sang trang báo cáo thống kê Anti-malware của hệ thống;