



Viettel Endpoint Detection & Response (VCS-aJiant)

Phiên bản 3.3.0 – Năm 2021

Ngày cập nhật: 29/11/2021

Tài liệu Hướng dẫn sử dụng



Mục lục

Thuật ngữ	5
1. GIỚI THIỆU	6
1.1 Thực trạng hiện nay.....	6
1.2 Sự phát triển của công nghệ	6
1.3 VCS-aJiant	6
1.4 Các thông tin nâng cấp	6
2. TỔNG QUAN	7
2.1 Công nghệ.....	7
2.2 Kiến trúc hạ tầng	8
2.3 Làm việc với giao diện quản trị	8
3. HƯỚNG DẪN SỬ DỤNG	9
GIAO DIỆN WEB-PORTAL	9
3.1 Đăng nhập.....	9
3.2 Dashboard VCS-aJiant (default)	10
3.2.1 Thao tác với dữ liệu	11
3.2.2 Thống kê Overview.....	12
3.2.3 Theo dõi Security Operation	16
3.2.4 Theo dõi Agent Monitoring	18
3.2.5 Theo dõi Risk Detection.....	20
3.3 Dashboard Kaspersky (optional)	22
3.3.1 Thao tác với dữ liệu	24
3.3.2 Thống kê Overview.....	25
3.3.3 Theo dõi Risk Detection.....	26
3.3 Dashboard Anti-malware (optional)	28
3.3.1 Thao tác với dữ liệu	30
3.3.2 Thống kê Overview.....	31

3.3.3 Theo dõi Risk Detection.....	33
3.4 Quản lý alert	35
3.4.1 Tìm kiếm alert.....	37
3.4.2 Danh sách alert	40
3.4.3 Gom nhóm alert	41
3.4.4 Xem tóm tắt alert.....	43
3.4.5 Xem chi tiết alert	44
3.4.6 Biểu đồ điều tra (Investigation Graph).....	45
3.4.7 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert.....	53
3.4.8 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert	53
3.4.9 Thêm 01/nhiều alert hoặc nhóm alert vào IR fLow đã có.....	54
3.5 Màn hình IRFlow.....	55
3.5.1 Danh sách hiển thị.....	55
3.5.2 Tìm kiếm IRFlow.....	55
3.5.3 Cách tạo IRFlow.....	56
3.5.4 Các bước thực hiện trong IRFlow	57
3.5.5 IRFlow – Detection	58
3.5.6 IRFlow – Containment.....	59
3.5.7 IRFlow – Investigation	61
3.5.8. IRFlow – Response	79
3.5.9 Close IRFlow	91
3.6 Màn hình Investigation.....	94
3.6.1 Investigation_Process Analysis	94
3.6.2 Investigation_Event Search.....	102
3.6.3 Investigation_Deploy Tools	107
3.7 Màn hình Response	111
3.7.1 Response_Live Response	111
3.8 Màn hình Setting.....	116
3.8.1 Agent Management	116

3.8.2 Policy Setting	129
3.8.3 Group Management.....	134
3.8.4 Account Management	143
3.9 Màn hình BLS.....	154
3.9.1 Thống kê vi phạm (Violation statistic)	154
3.9.2 Thống kê phần mềm (Software statistic).....	160
3.10 Rules Correlation	163
3.10.1 Danh sách hiển thị.....	163
3.10.2 Thêm mới Rules Correlation	169
3.10.3 Sửa Rules Correlation	175
3.10.4 Xóa Rules Correlation.....	177
3.11 Protect & Prevention	179
3.11.1 Application Control	179
3.11.2 Endpoint Firewall	182
GIAO DIỆN PHÍA AGENT.....	184
3.12 Main	184
3.13 About.....	186
3.14 Reports	186
3.15 Scan	187

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 hỗ 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 - LiveResponse	
Timeline	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	

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.

1.4 Các thông tin nâng cấp

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

Bổ sung tính năng Dashboard: Ngoài Dashboard mặc định của VCS-aJiant, tại một số đơn vị triển khai đồng thời với Kaspersky hoặc có tính năng Anti-malware, sản phẩm hỗ trợ Dashboard riêng cho dữ liệu được phân tích từ Kaspersky và AV engine.

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.

Bổ sung giao diện phía Agent cho phép theo dõi tình hình an toàn thông tin tại máy và thao tác chủ động quét mã độc để xử lý.

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

2. TỔNG QUAN

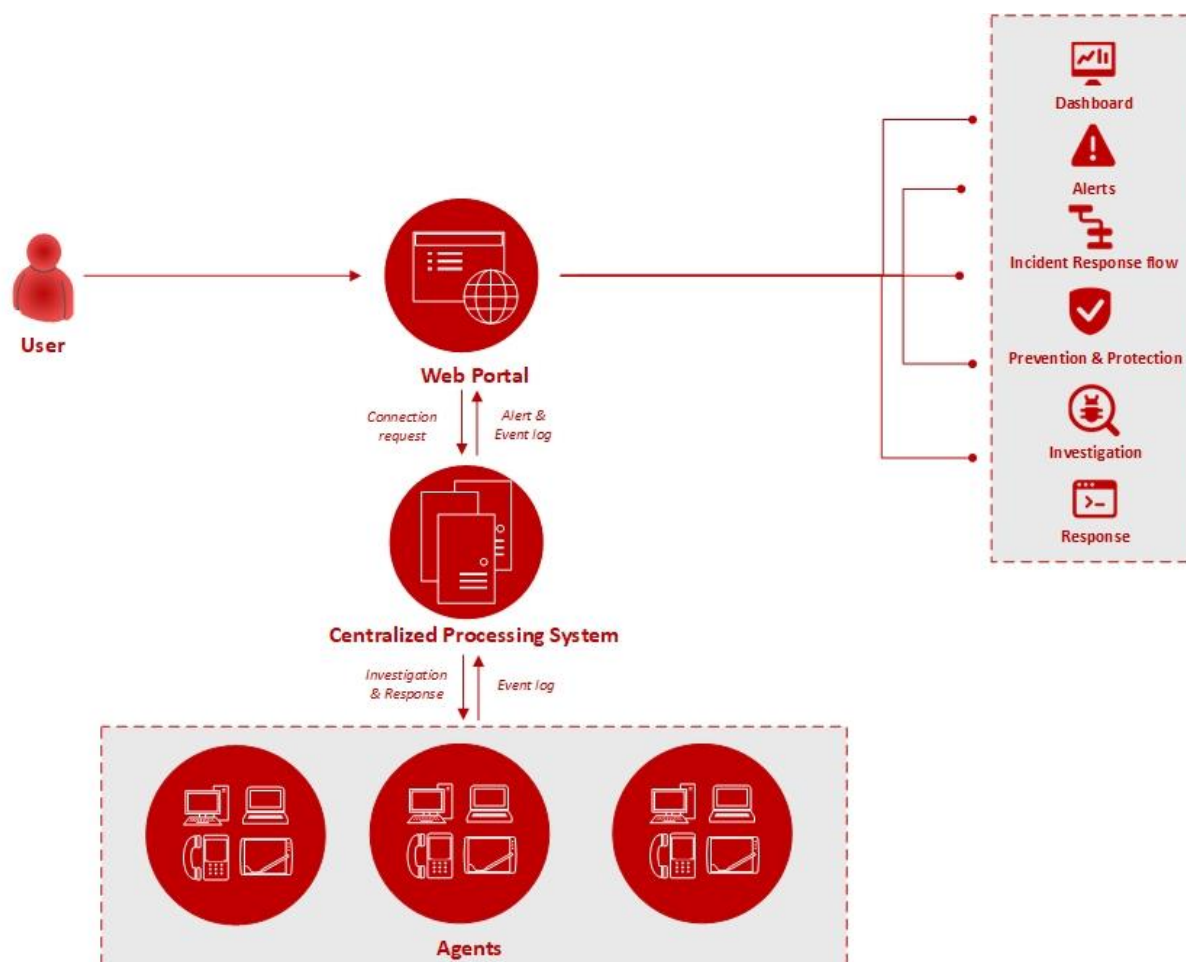
2.1 Công nghệ

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 hiệu 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:

- **Agents:** 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.
- **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.

2.3 Làm việc với giao diện quản trị

Hiện tại VCS-aJiant cung cấp 02 giao diện

1. 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)
2. Giao diện phía Agent bao gồm các giao diện chức năng và các luồng xử lý sau
- Main: Trang chủ cho phép xem nhanh tình trạng an toàn thông tin máy cài agent
 - Reports: Báo cáo tình hình xử lý mã độc phát hiện tại máy
 - Scan: Cho phép người dùng chủ động quét mã độc với các file, folder trong máy gồm 03 cơ chế Quick Scan, Full Scan và Custom Scan
 - About: Cung cấp thông tin phiên bản và hỗ trợ sản phẩm

3. HƯỚNG DẪN SỬ DỤNG

GIAO DIỆN WEB-PORTAL

3.1 Đăng nhập

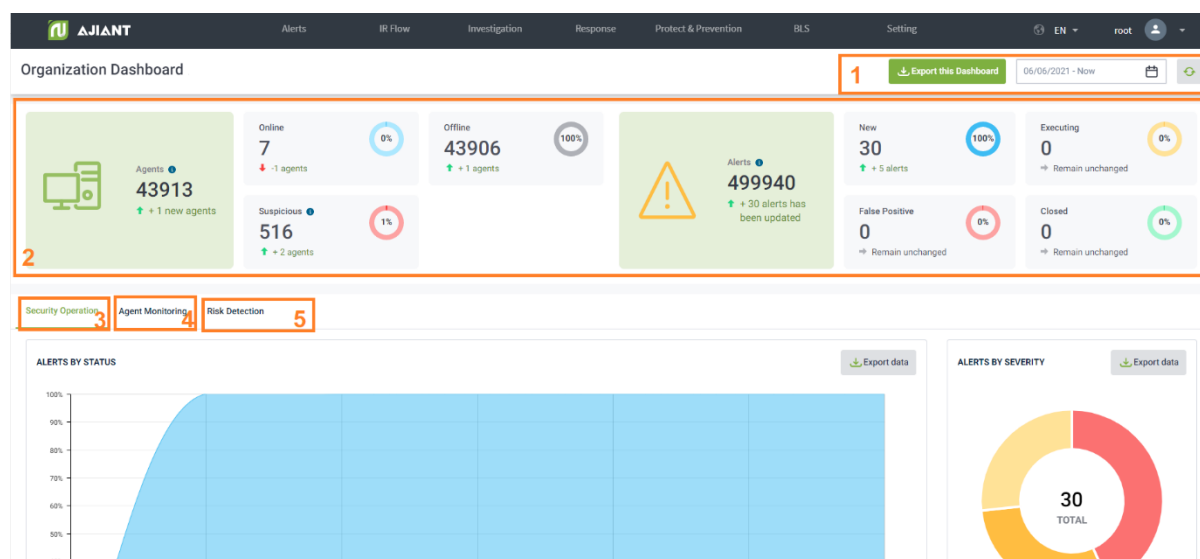
- Truy cập vào hệ thống tại địa chỉ được cung cấp



- Đăng nhập với user/pass được cấp

3.2 Dashboard VCS-aJiant (default)

- Các tính năng chính gồm có:



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

- Cho phép trích xuất dữ liệu hiện có trên giao diện dashboard bằng cách chọn  , 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:

Absolute time range	Relative time range
From 06/06/2021 	☐ Last 90 days
Apply time range	☐ Last 60 days
	☐ Last 30 days
	☐ Last 24 hours

- 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.

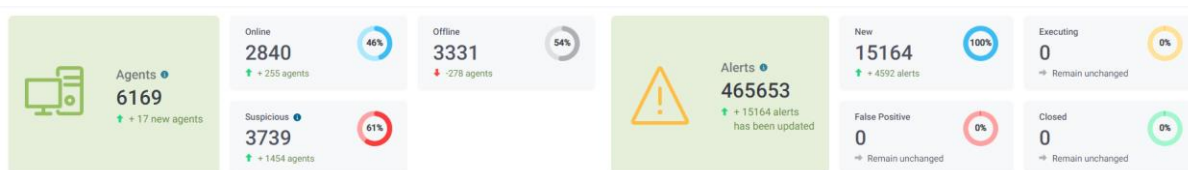
+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn  để tải lại dữ liệu tương ứng.

3.3.1.3 Làm mới dữ liệu

- Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

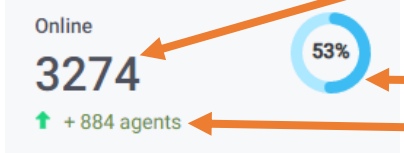
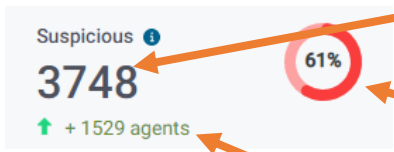
3.2.2 Thống kê Overview

- 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



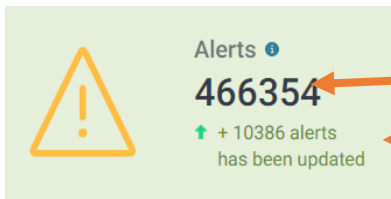
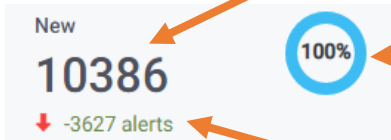
+ Thống kê liên quan đến agents

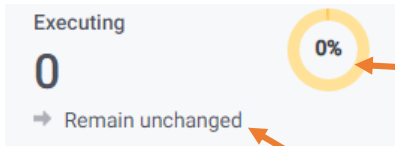
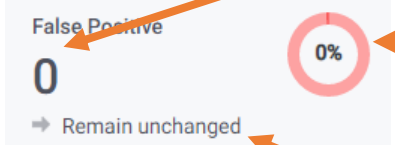
Số thống kê	Ý nghĩa
 Agents 6171 + 19 new agents	Bao gồm 02 chỉ số Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm (+: Máy mới cài đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)

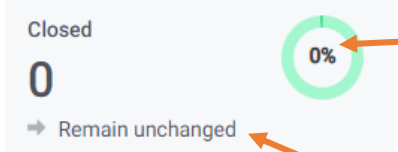
	Bao gồm 03 chỉ số Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00) Tỷ lệ máy Online trung bình so với toàn hệ thống Số lượng máy Online trung bình chênh lệch so với chu kỳ trước. (+: Số lượng máy Online trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
	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) Tỷ lệ máy Offline trung bình so với toàn hệ thống Số lượng máy Offline trung bình chênh lệch so với chu kỳ trước. (+: Số lượng máy Offline trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
	Bao gồm 03 chỉ số 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 Tỷ lệ máy có phát sinh alert so với số lượng máy trên toàn hệ thống (không phụ thuộc thời gian tìm kiếm) 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

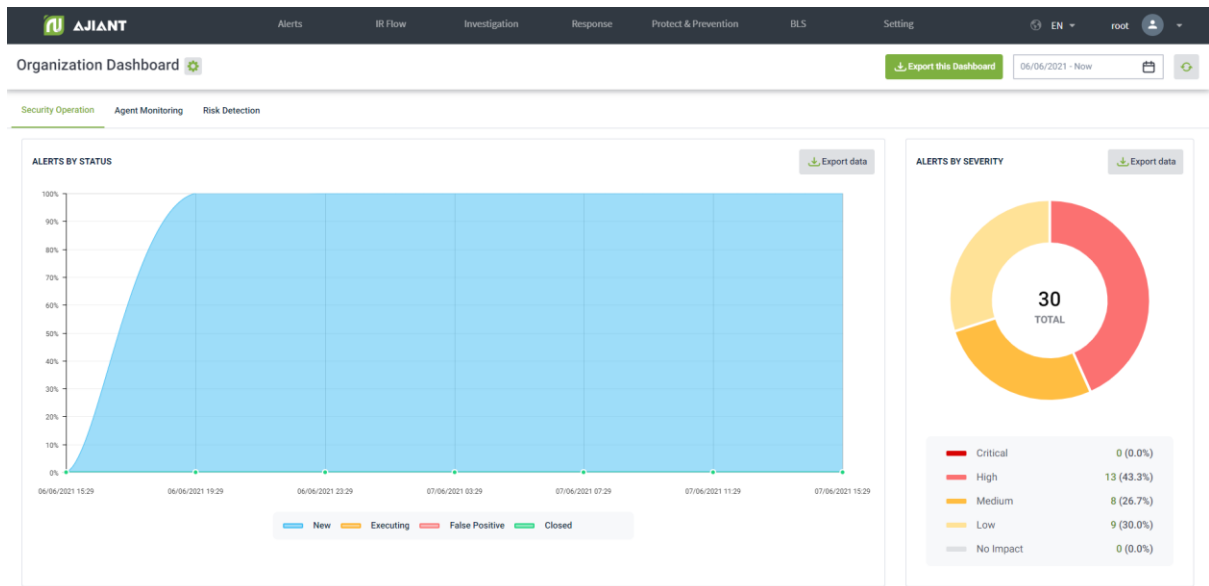
Số thống kê	Ý nghĩa
	Bao gồm 02 chỉ số Tổng số alert trên toàn bộ hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm (+: Alert mới phát sinh, Remain unchanged: Không có alert mới phát sinh trong khoảng thời gian tìm kiếm)
	Bao gồm 03 chỉ số Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW 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 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)
	Bao gồm 03 chỉ số

	Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <> (NEW, FALSE POSITIVE, CLOSED) Tỷ lệ alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <> (NEW, FALSE POSITIVE, CLOSED) so với toàn bộ alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <> (NEW, FALSE POSITIVE, CLOSED) chênh lệch so với chu kỳ trước. (+: Tổng số alert tăng so với giai đoạn trước, Remain unchanged: Tổng số alert không thay đổi so với giai đoạn trước)
	Bao gồm 03 chỉ số Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED Tỷ lệ alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED so với toàn bộ alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm 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. (+: Tổng số alert tăng so với giai đoạn trước, Remain unchanged: Tổng số alert không thay đổi so với giai đoạn trước)
	Bao gồm 03 chỉ số

	Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE 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 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. (+: Tổng số alert tăng so với giai đoạn trước, Remain unchanged: Tổng số alert không thay đổi so với giai đoạn trước)
---	--

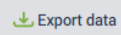
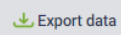
3.2.3 Theo dõi Security Operation

- 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



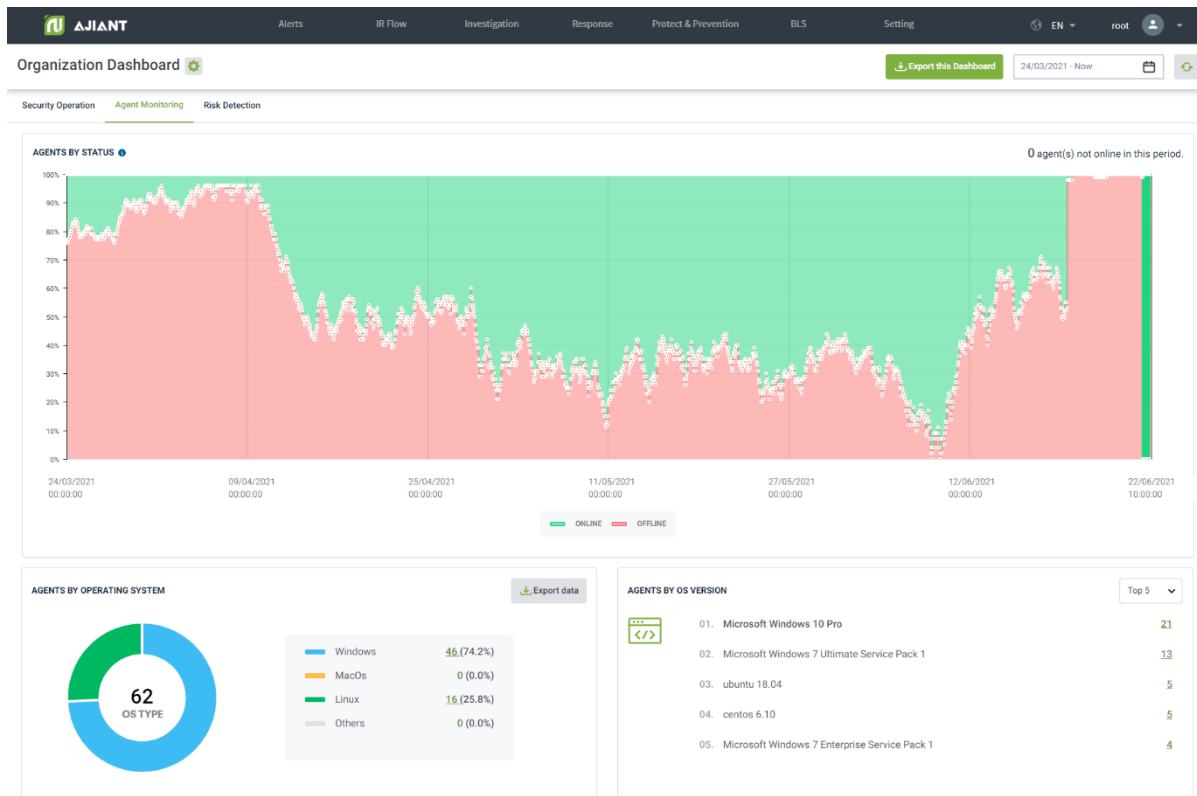
Viettel Cyber Security

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

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  để tải về danh sách alert sắp xếp theo trạng thái
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  để tải về danh sách alert sắp xếp theo mức độ nguy hiểm

3.2.4 Theo dõi Agent Monitoring

- 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 tuyến)
 - + Thống kê agent theo hệ điều hành, phiên bản hệ điều hành
 - + Trích xuất dữ liệu thông tin agent

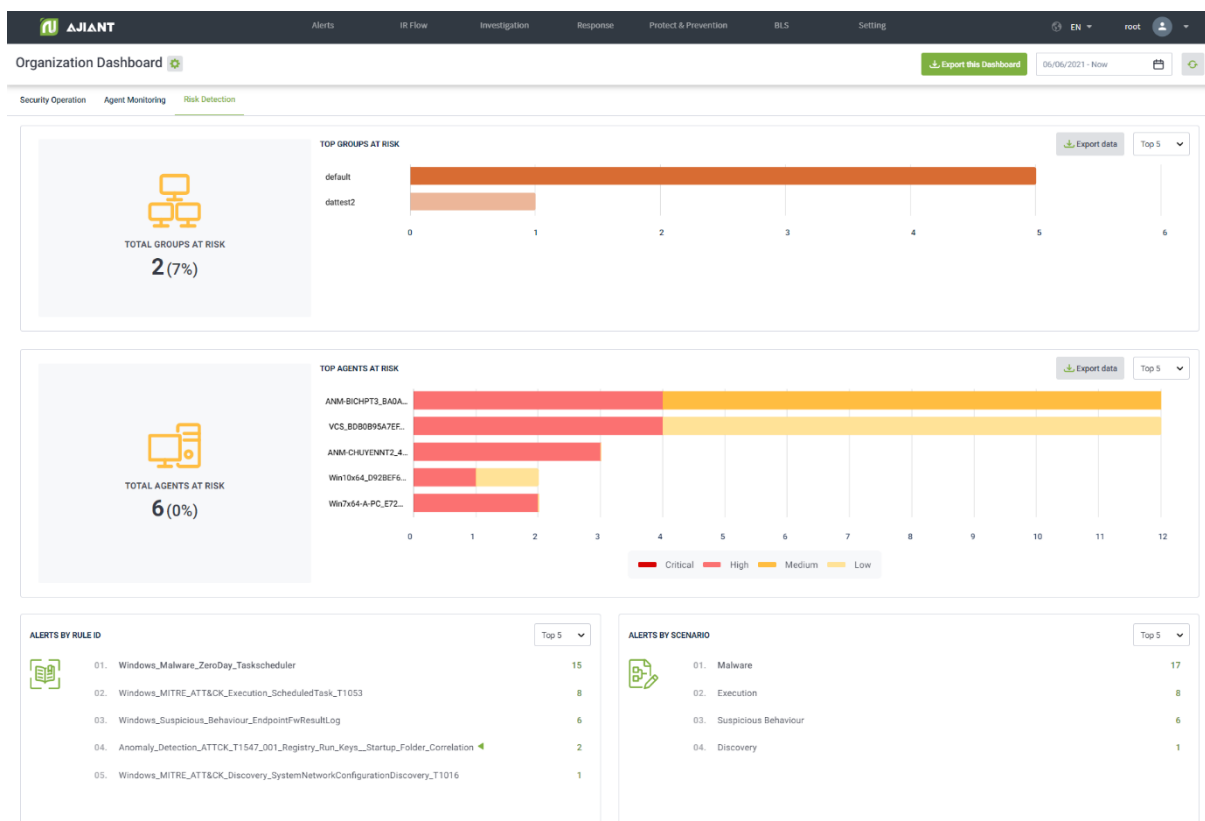


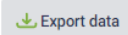
Biểu đồ/thống kê	Ý nghĩa
Agent by status	Biểu đồ miền- Theo dõi tình hình ghi nhận máy theo trạng thái (Online/Offline) trong chu kỳ báo cáo tính đến thời điểm hiện tại, bao gồm: - Trục y: Tỷ lệ máy phân chia theo 02 nhóm status (Online, Offline) - Trục x: thời gian thống kê - Hiển thị số lượng máy không 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.

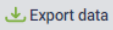
	- Cho phép chọn Export data để tải về danh sách máy sắp xếp theo thông tin hệ điều hành
Agent by OS version	Thống kê top phiên bản hệ điều hành cài đặt trên máy nhiều nhất. - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5

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 báo nhất
 - + Trích xuất dữ liệu thông tin theo đối tượng nguy hại

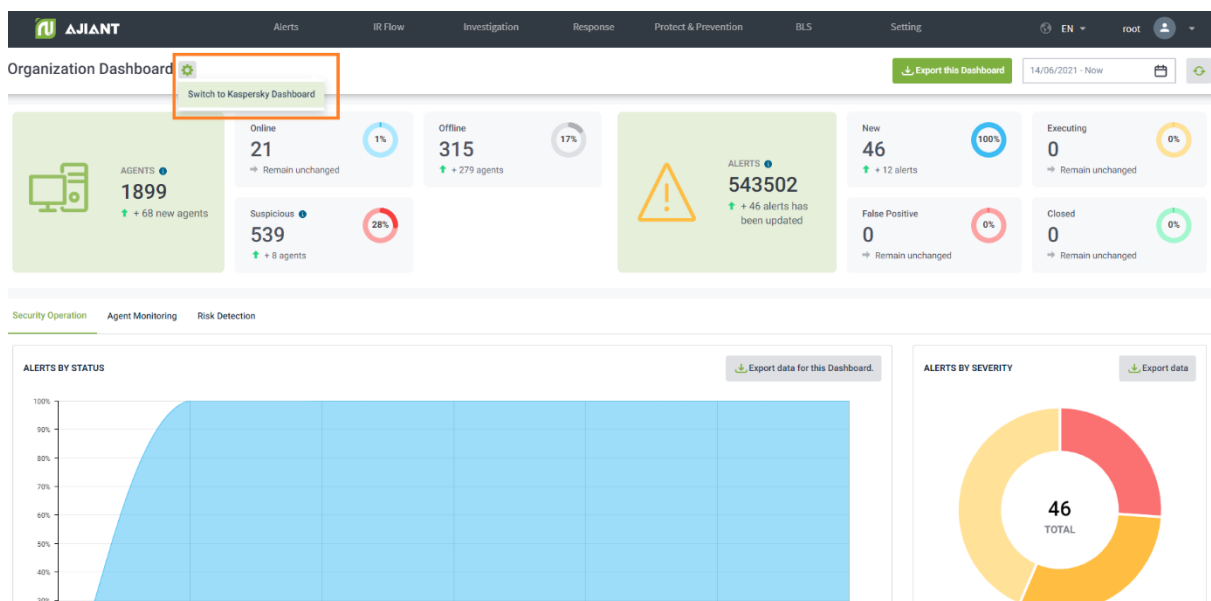


Biểu đồ/thống kê	Ý nghĩa
Total groups at risk	Tổng số nhóm có chứa máy tính phát sinh alert mới ghi nhận hoặc có cập nhật (không kể alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm. Tỷ lệ nhóm khả nghi so với toàn bộ nhóm trên hệ thống (không kể nhóm đã bị xóa)
Top groups 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  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 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  để tải về danh sách máy tính phát sinh alert
Alerts by RuleID	Thống kê top rule Id 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 chọn 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 Dashboard Kaspersky (optional)

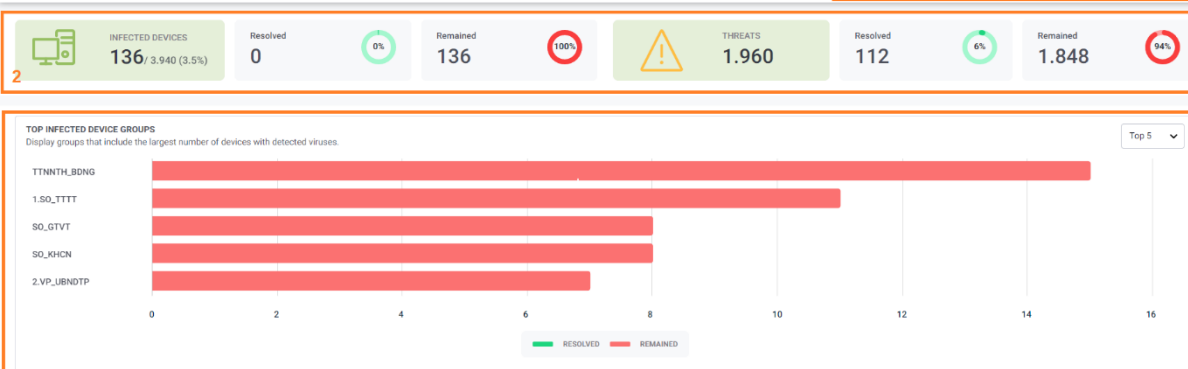
- Tại một số tổ chức có triển khai đồng thời VCS-aJiant và Kaspersky, hệ thống bổ sung Dashboard cho riêng dữ liệu thu thập được từ Kaspersky.
- Ban đầu khi truy cập hệ thống, mặc định hiển thị Dashboard VCS-aJiant



- Chọn biểu tượng  và chọn  để truy cập Dashboard của Kaspersky



- Các tính năng chính gồm có:



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 devices và threats)

3 - Risk Detection: Theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều mã độc nhất hệ thống)

Phân quyền dữ liệu tại tính năng như sau:

+ Cho phép hiển thị toàn bộ dữ liệu, không phân theo đơn vị.

3.3.1 Thao tác với dữ liệu

3.3.1.1 Xuất dữ liệu

- Cho phép trích xuất dữ liệu hiện có trên giao diện dashboard bằng cách chọn

 , 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

3.3.1.2 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:

Absolute time range	Relative time range
From 06/06/2021 	☐ Last 90 days
Apply time range	☐ Last 60 days
	☐ Last 30 days
	☐ Last 24 hours

- 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.

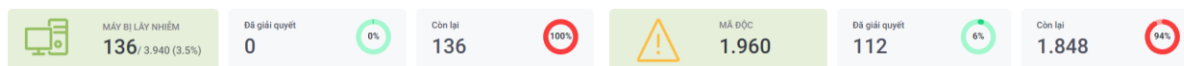
+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn  để tải lại dữ liệu tương ứng.

3.3.1.3 Làm mới dữ liệu

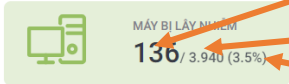
- Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.3.2 Thống kê Overview

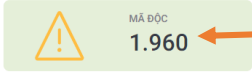
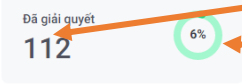
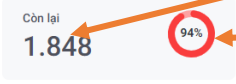
- Cho phép thống kê nhanh về tình hình an toàn thông tin trên tổ chức theo khoảng thời gian đã chọn trong phần tìm kiếm



+ Thống kê liên quan đến agents

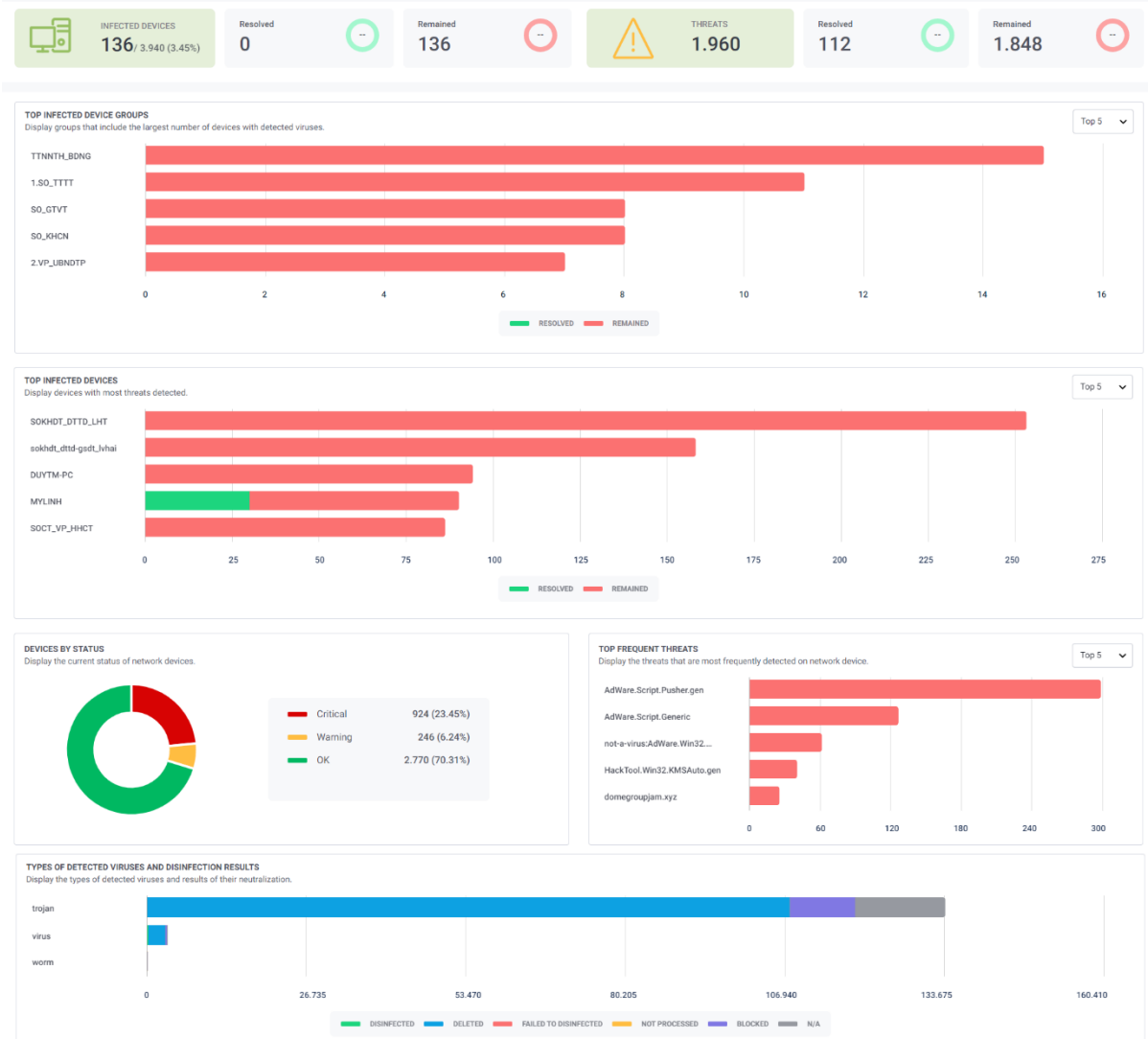
Số thống kê	Ý nghĩa
	Bao gồm 03 chỉ số - Tổng số máy bị lây nhiễm trên hệ thống trong khoảng thời gian tìm kiếm - Tổng số máy cài đặt agent trong hệ thống (không kể thời gian tìm kiếm) - Tỷ lệ máy bị lây nhiễm so với toàn bộ máy cài đặt agent trong hệ thống
	Bao gồm 02 chỉ số - Tổng số máy bị lây nhiễm trên hệ thống đã được xử lý thành công - Tỷ lệ máy bị lây nhiễm được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống
	Bao gồm 02 chỉ số - Tổng số máy bị lây nhiễm trên hệ thống chưa được xử lý thành công - Tỷ lệ máy bị lây nhiễm chưa được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống

+ Thống kê liên quan đến alerts

Số thống kê	Ý nghĩa
	Bao gồm 01 chỉ số Tổng số mã độc ghi nhận trên toàn bộ hệ thống
	Bao gồm 02 chỉ số Tổng số mã độc trên hệ thống đã được xử lý thành công Tỷ lệ mã độc đã được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống
	Bao gồm 02 chỉ số Tổng số mã độc trên hệ thống chưa được xử lý thành công Tỷ lệ mã độc trên hệ thống chưa được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống

3.3.3 Theo dõi Risk Detection

- Cho phép theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng nhiễm mã độc nhiều nhất hệ thống)
 - + Thống kê top các nhóm bị lây nhiễm
 - + Thống kê top các máy bị lây nhiễm
 - + Thống kê máy theo trạng thái
 - + Thống kê các mã độc thường gặp
 - + Thống kê tình trạng xử lý virus

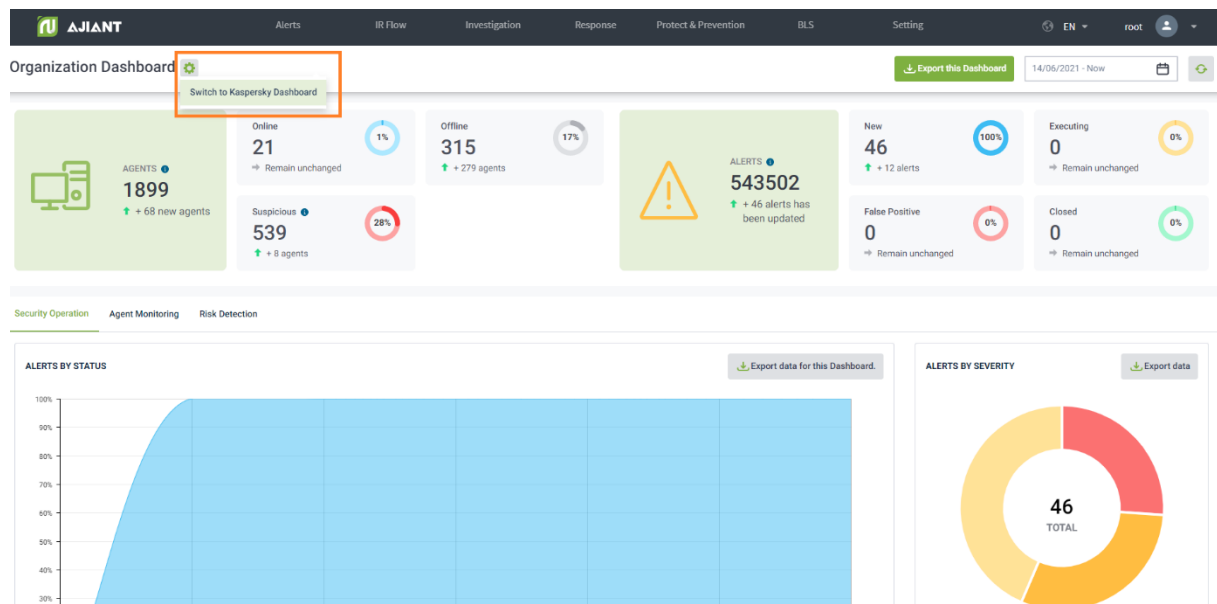


Biểu đồ/thống kê	Ý nghĩa
Top infected device groups	Biểu đồ cột liệt kê nhóm máy có nhiều máy lây nhiễm mã độc nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng máy lây nhiễm mã độc tại từng nhóm theo trạng thái xử lý (Resolved - máy có toàn bộ mã độc đã xử lý và Remain - máy có ít nhất 01 mã độc chưa xử lý xong)

	- Trục y: Tên nhóm máy tương ứng - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5
Top infected devices	Biểu đồ cột liệt kê máy bị lây nhiễm mã độc nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc lây nhiễm theo trạng thái xử lý (Resolved và Remain) - 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
Devices by status	Biểu đồ tròn - Theo dõi tình hình máy trong hệ thống theo trạng thái tại thời điểm hiện tại, bao gồm: - Tỷ lệ: Tỷ lệ máy tại từng trạng thái so với tổng số toàn bộ máy
Top frequent threats	Biểu đồ cột liệt kê mã độc lây nhiễm nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc phát sinh - Trục y: Tên loại mã độc - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5
Types of detected viruses and disinfected results	Biểu đồ cột liệt kê virus xuất hiện trong thời gian tìm kiếm tính đến thời điểm hiện tại (sắp xếp theo số lượng virus giảm dần) - Trục x: số lượng virus phát sinh theo trạng thái xử lý - Trục y: Tên virus

3.3 Dashboard Anti-malware (optional)

- Tại một số tổ chức có triển khai đồng thời VCS-aJiant và nhóm tính năng Anti-malware (thông qua việc tích hợp AV engine), hệ thống bổ sung Dashboard cho riêng dữ liệu thu thập được từ AV.
- Ban đầu khi truy cập hệ thống, mặc định hiển thị Dashboard VCS-aJiant



- Chọn biểu tượng  và chọn **Switch to Anti-malware Dashboard** để truy cập Dashboard Anti-malware



- Các tính năng chính gồm có:



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 devices và threats)

3 - Risk Detection: Theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều mã độc nhất hệ thống)

Phân quyền dữ liệu tại tính năng như sau:

- + Cho phép hiển thị toàn bộ dữ liệu, không phân theo đơn vị.

3.3.1 Thao tác với dữ liệu

3.3.1.1 Xuất dữ liệu

- 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

3.3.1.2 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:

Absolute time range

From

06/06/2021

Apply time range

Relative time range

Last 90 days

Last 60 days

Last 30 days

Last 24 hours

- 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.

3.3.1.3 Làm mới dữ liệu

- Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.3.2 Thống kê Overview

- 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



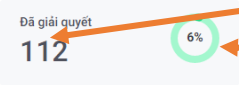
+ Thống kê liên quan đến agents

Số thống kê	Ý nghĩa

	Bao gồm 03 chỉ số - Tổng số máy bị lây nhiễm trên hệ thống trong khoảng thời gian tìm kiếm - Tổng số máy cài đặt agent trong hệ thống (không kể thời gian tìm kiếm) - Tỷ lệ máy bị lây nhiễm so với toàn bộ máy cài đặt agent trong hệ thống
	Bao gồm 02 chỉ số - Tổng số máy bị lây nhiễm trên hệ thống đã được xử lý thành công - Tỷ lệ máy bị lây nhiễm được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống
	Bao gồm 02 chỉ số - Tổng số máy bị lây nhiễm trên hệ thống chưa được xử lý thành công - Tỷ lệ máy bị lây nhiễm chưa được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống

+ Thống kê liên quan đến alerts

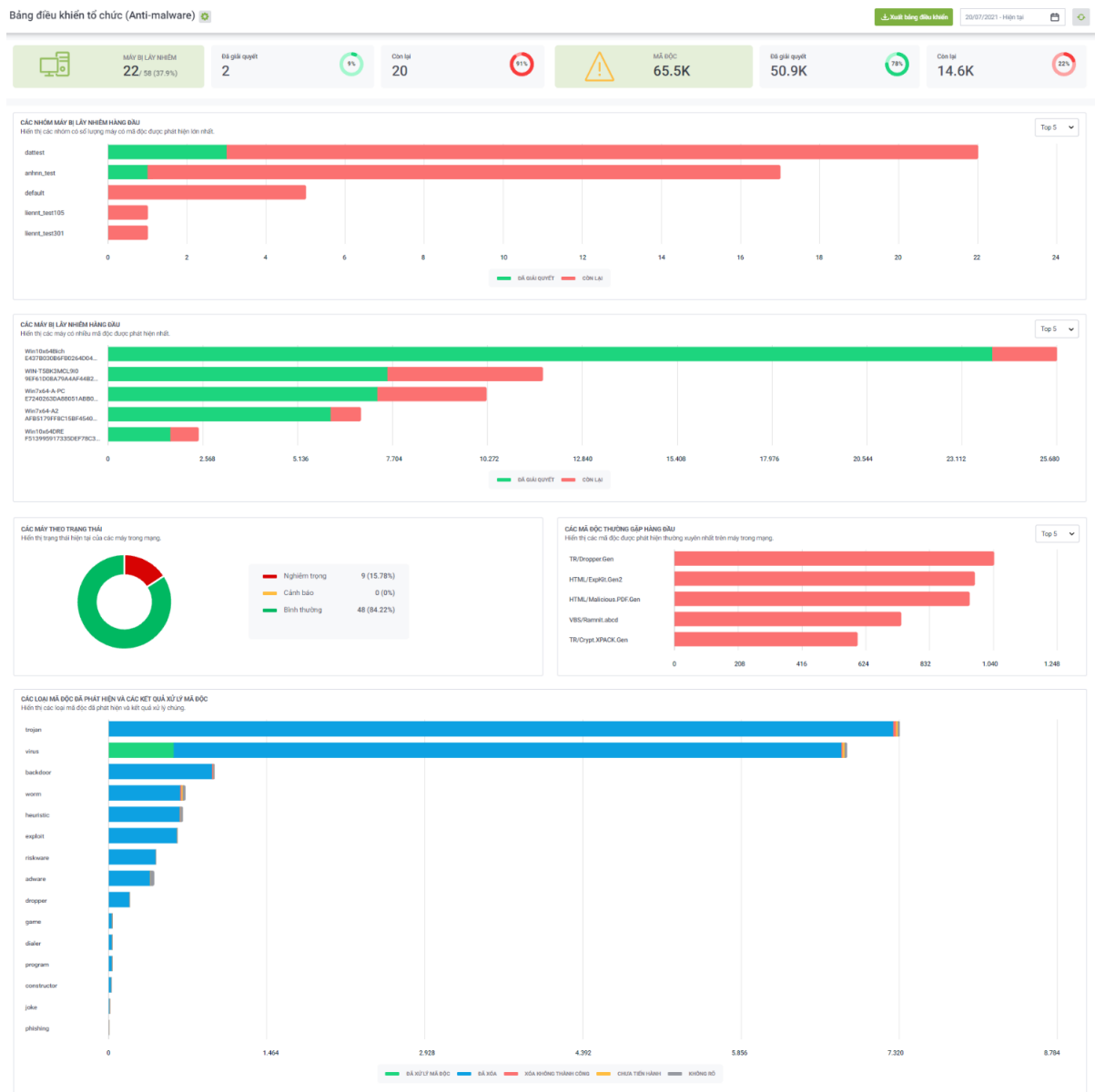
Số thống kê	Ý nghĩa
	Bao gồm 01 chỉ số Tổng số mã độc ghi nhận trên toàn bộ hệ thống

	Bao gồm 02 chỉ số Tổng số mã độc trên hệ thống đã được xử lý thành công Tỷ lệ mã độc đã được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống
	Bao gồm 02 chỉ số Tổng số mã độc trên hệ thống chưa được xử lý thành công Tỷ lệ mã độc trên hệ thống chưa được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống

3.3.3 Theo dõi Risk Detection

- Cho phép theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng nhiễm mã độc nhiều nhất hệ thống)
 - + Thống kê top các nhóm bị lây nhiễm
 - + Thống kê top các máy bị lây nhiễm
 - + Thống kê máy theo trạng thái
 - + Thống kê các mã độc thường gặp
 - + Thống kê tình trạng xử lý virus

Bảng điều khiển tổ chức (Anti-malware)



Biểu đồ/thống kê

Top infected device groups

Ý nghĩa

Biểu đồ cột liệt kê nhóm máy có nhiều máy lây nhiễm mã độc nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại:

- Trục x: số lượng máy lây nhiễm mã độc tại từng nhóm theo trạng thái xử lý (Resolved - máy có toàn bộ mã độc đã xử lý và Remain - máy có ít nhất 01 mã độc chưa xử lý xong)

	- Trục y: Tên nhóm máy tương ứng - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5
Top infected devices	Biểu đồ cột liệt kê máy bị lây nhiễm mã độc nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc lây nhiễm theo trạng thái xử lý (Resolved và Remain) - 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
Devices by status	Biểu đồ tròn - Theo dõi tình hình máy trong hệ thống theo trạng thái tại thời điểm hiện tại, bao gồm: - Tỷ lệ: Tỷ lệ máy tại từng trạng thái so với tổng số toàn bộ máy
Top frequent threats	Biểu đồ cột liệt kê mã độc lây nhiễm nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc phát sinh - Trục y: Tên loại mã độc - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5
Types of detected viruses and disinfected results	Biểu đồ cột liệt kê virus xuất hiện trong thời gian tìm kiếm tính đến thời điểm hiện tại (sắp xếp theo số lượng virus giảm dần) - Trục x: số lượng virus phát sinh theo trạng thái xử lý - Trục y: Tên virus

3.4 Quản lý alert

- Các tính năng chính gồm có:

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:

- + User đăng nhập thuộc group root: Hiện thị tất cả alert trong hệ thống
- + User đăng nhập thuộc group default: Hiện thị tất cả alert thuộc group default
- + User đăng nhập thuộc group cha: Hiện 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

3.4.1 Tìm kiếm alert

- 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.

3.4.1.1 Tìm kiếm theo thời gian

- Mặc định khi vừa truy cập vào hệ thống, tìm kiếm alert theo 7 ngày gần đây

The screenshot shows a search interface with two main sections: 'Absolute time range' and 'Relative time range'. The 'Absolute time range' section has 'From' and 'To' date pickers, both set to '03/06/2021 10:53:05', and a green 'Apply time range' button. The 'Relative time range' section is a dropdown menu with options: 'Last 15 minutes', 'Last 1 hour', 'Last 6 hours', 'Last 12 hours', 'Last 24 hours', 'Last 7 days' (highlighted in green), and 'Last 30 days'. A search icon and a 'Last 7 days' filter are visible at the top right of the interface.

- 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.

3.4.1.2 Tìm kiếm nhanh

- 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
 - + Scenario: kịch bản sinh ra alert

+ Assigned to: người được phân công xử lý alert

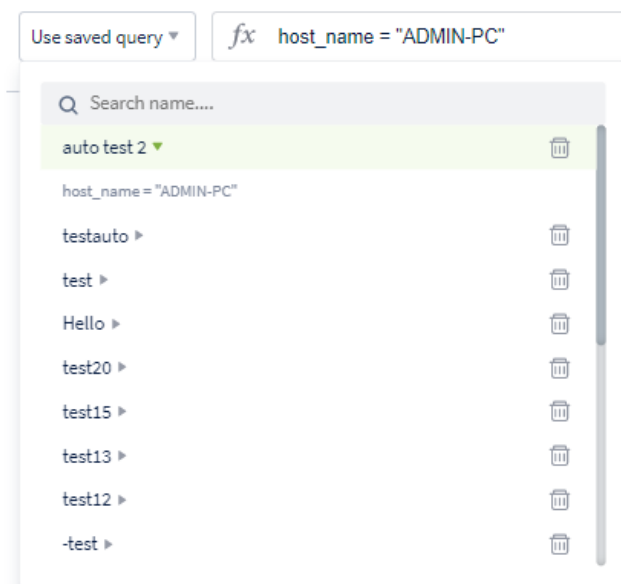
3.4.1.3 Tìm kiếm theo câu query



- 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
- Bước 2: Xem lại nội dung câu query trước khi chọn bằng cách chọn
- Trường hợp muốn xóa câu query cũ, di chuột qua bản ghi muốn xóa và chọn
- Bước 3: Click vào bản ghi muốn sử dụng để truy vấn, nội dung query cũ được hiển thị tại ô nhập query



Trường hợp muốn thêm mới/chỉnh sửa nội dung câu query, có thể cập nhật ngay tại ô nhập query và chọn để lưu lại.

Lưu ý: nút 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:
<tên_trường> <toán tử> "<value>" AND/OR <tên_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: kịch 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 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. Để xem nhiều bản ghi hơn thực hiện scroll dữ liệu xuống cuối trang, hệ thống sẽ load 50 bản ghi tiếp theo
- Bước 3: 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:

NAME FOR THIS QUERY

query 1

Cancel Save

Lưu ý: nút

Save query

chỉ hiển thị khi câu lệnh query đúng cấu trúc.

3.4.2 Danh sách alert

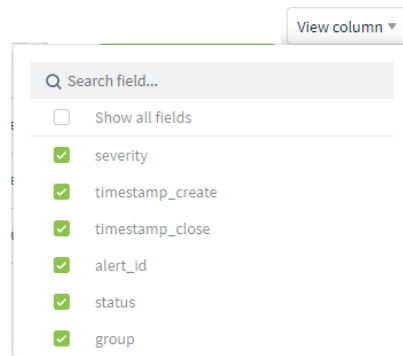
- Cho phép xem danh sách các alert đáp ứng điều kiện tìm kiếm

3 result(s)

SEVERITY	TIMESTAMP_CREATE	TIMESTAMP_CLOSE	ALERT_ID	STATUS	GROUP	HOST_NAME	SCENARIO	IR_FLOW_NAME	DESCRIPTION	ACTION
HIGH	16:23:19 10/06/2021	N/A	20210610_92321_102926463_784417	New	default	WIN10X64	Malware	N/A	[IOC] Detect process [nul	
HIGH	16:17:32 10/06/2021	N/A	20210610_91734_461280860_412414	New	default	ANM-BICHPT3	Malware	N/A	[IOC] Detect process [nul	
LOW	15:56:16 10/06/2021	N/A	20210610_91111_314657586_582156	New	default	WIN10X64	Privilege Escalation	N/A	Detect process [null] (PI	

Showing 3/3 result(s)

- Bước 1: Chọn View column để lựa chọn các trường muốn hiển thị trên danh sách alert



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

STATUS	GROUP	HOST_NAME	DESCRIPTION	TIMESTAMP_CREATE	SEVERITY	SCENARIO
New	default	WIN10X64	[IOC] Detect process [nul	16:23:19 10/06/2021	HIGH	Malware
New	default	ANM-BICHPT3	[IOC] Detect process [nul	16:17:32 10/06/2021	HIGH	Malware
New	default	WIN10X64	Detect process [null] (PI	15:56:16 10/06/2021	LOW	Privilege Escalation

1. Chọn trường muốn thay đổi vị trí

2. Kéo đến vị trí mới

+ Click 01 lần để xem thông tin tóm tắt, chi tiết xem trong [3.3.4 Xem tóm tắt alert](#)

+ Click 02 lần hoặc chọn ⓘ để xem thông tin chi tiết, chi tiết xem trong [3.3.4 Xem chi tiết alert](#)

- + Chọn  để đánh dấu không nguy hiểm cho alert, xem trường hợp đánh dấu 01 alert trong [3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert](#)
- + Chọn  để đưa alert vào IR flow, xem trường hợp đưa 01 alert vào IR flow đã tồn tại trong [3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR flow đã có](#) hoặc vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert](#)
- + Chọn  để xem lý do đánh dấu không nguy hiểm tại các alert đang ở trạng thái “FALSE POSITIVE”
- Bước 3: 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

Selected 3 alert(s)											
Add to IRFlow Set false positive Export selected alert(s) Clear selection											
☐	SEVERITY	TIMESTAMP_CREATE	TIMESTAMP_CLOSE	ALERT_ID	STATUS	GROUP	HOST_NAME	SCENARIO	IR_FLOW_NAME	DESCRIPTION	ACTION
☒	MEDIUM	09:17:38 11/06/2021	N/A	20210611_21841_450884396_801941	New	default		N/A	N/A	Test KIAN Alert	
☒	MEDIUM	09:17:38 11/06/2021	N/A	20210611_21843_451494270_398683	New	default		N/A	N/A	Test KIAN Alert	
☐	MEDIUM	09:17:38 11/06/2021	N/A	20210611_21848_455351315_775451	New	default		N/A	N/A	Test KIAN Alert	
☐	MEDIUM	09:17:38 11/06/2021	N/A	20210611_21852_462470354_542493	New	default		N/A	N/A	Test KIAN Alert	

+ Chọn  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”, thao tác sẽ bị ẩn đi 

. Chi tiết xem trong trường hợp đưa 01 alert vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert](#) hoặc thêm vào IR flow đã tồn tại trong [3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR flow đã có](#)

+ Chọn  để đánh dấu không nguy hiểm cho 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 [3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert](#)

+ Chọn  để trích xuất các alert đang được chọn.

3.4.3 Gom nhóm alert

- 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  để lựa chọn các tiêu chí muốn sử dụng làm tiêu chí gom nhóm alert.

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

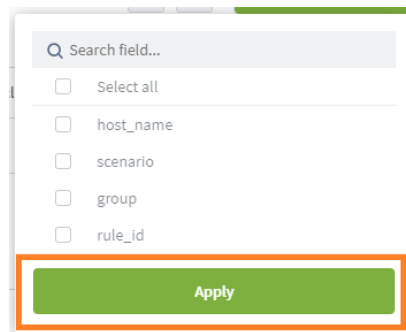
- Bước 2: Chọn **Apply** để áp dụng.

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.

21 result(s)

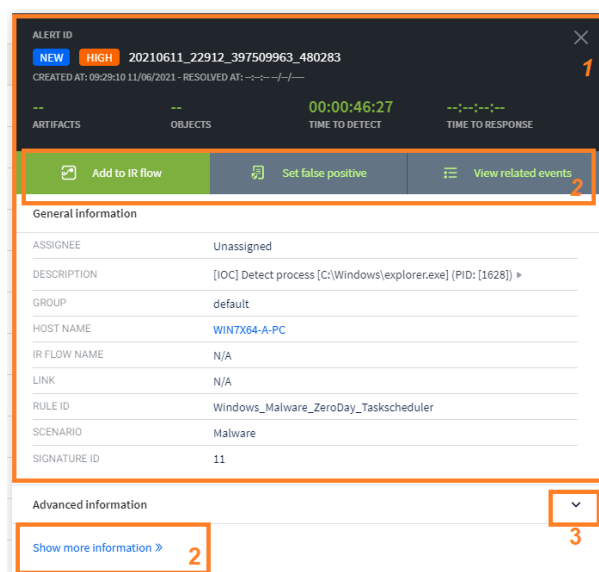
SCENARIO	HOST_NAME	GROUP	SEVERITY	TIMESTAMP_CREATE	TIMESTAMP_CLOSE	ALERT_ID	STATUS	IR_FLOW_NAME	DESCRIPTION	ACTION
☐ Malware	WIN10X64	default	MEDIUM	17:53:53 10/06/2021	N/A	20210610_105355_63452087_644270	In Progress	bennt_dashboard_close	[T1543.003] Windows Servi >	
☐ Malware	WIN7X86-A-PC	default	HIGH	10:42:33 10/06/2021	N/A	20210610_34234_317154921_141482	New	N/A	[IOC] Detect process [nul] >	
☒ alert(s) in group Malware	ANM-BICHPT3	default	HIGH	09:40:59 04/06/2021	N/A	20210611_12543_444783129_799979, 20210611_12144_236343336_627307 and 31 others	New	N/A	[T1547.001] Registry Run >	
☐ Malware	KHAUTB	default	HIGH	14:02:51 03/06/2021	N/A	20210603_7252_652579214_467528	New	N/A	[IOC] Detect process [nul] >	
☐ Malware	ANM-CHUYENNT2	default	HIGH	06:53:42 02/06/2021	N/A	20210601_235343_653743842_344462	In Progress	HoanhN test	[IOC] Detect process [C:] >	
☒ alert(s) in group Malware	WIN7X64-A-PC	default	HIGH	16:29:41 01/06/2021	N/A	20210611_22912_397509963_480283, 20210610_212644_79442733_693462 and 64 others	New	N/A	[IOC] Detect process [C:] >	
☒ alert(s) in group Malware	VUONGVIMTEST	default	HIGH	15:31:40 01/06/2021	N/A	20210602_2635_224577402_753210, 20210601_161543_266010266_987263 and 3 others	New	N/A	[IOC] Detect process [nul] >	
☒ alert(s) in group Malware	TEST_SEABANK_KH	datetest2	HIGH	13:11:40 28/05/2021	N/A	20210528_6472_820898330_774157, 20210528_6438_322265580_874336 and 5 others	New	N/A	[T1543.003] Windows Servi >	

- Trong đó:
 - + Các trường được sử dụng làm tiêu chí gom nhóm sẽ được bôi đậm
 - + Hiện 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



3.4.4 Xem tóm tắt alert

- Cho phép xem nhanh thông tin tóm tắt của alert
- Bước 1: Click 01 lần tại alert muốn xem tóm tắt, hiển thị các thông tin như sau:



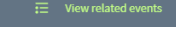
1 – Nhóm thông tin chung của alert, trong đó:

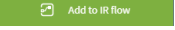
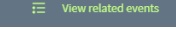
- + Artifacts: Danh sách các đối tượng khả nghi được đánh dấu tự động/thủ công trong alert
- + Objects: Danh sách các đối tượng trong alert
- + Time to detect: Tổng thời gian phát hiện và điều tra alert, tính từ khi alert sinh ra đến khi được đưa vào IR flow hoặc đánh dấu “FALSE POSITIVE”
- + Time to response: Tổng thời gian xử lý alert, tính từ khi alert được đưa vào IR flow đến khi đóng IR flow

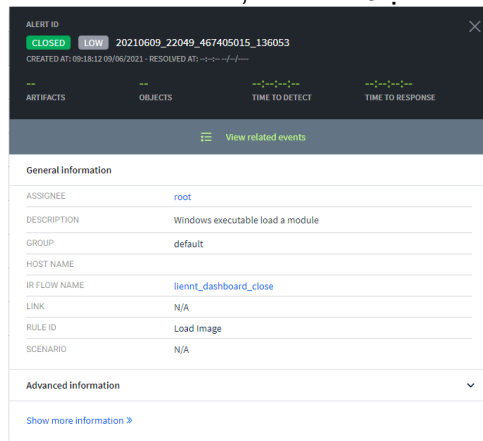
2 – Nhóm các thao tác với alert

+ Chọn  để đưa alert vào IR flow, xem trường hợp đưa 01 alert vào IR flow đã tồn tại trong [3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR flow đã có](#) hoặc vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert](#)

+ Chọn  để đánh dấu không nguy hiểm cho alert, xem trường hợp đánh dấu 01 alert trong [3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert](#)

+ Chọn  để chuyển đến tính năng Event Search với thời gian mặc định là 04 tiếng trước và sau thời gian phát sinh alert

Lưu ý: Chỉ hiển thị thao tác  và  đối với alert đang ở trạng thái “NEW”, trường hợp alert khác “NEW”, chỉ hiển thị  như sau:



ALERT ID: 20210609_22049_467405015_136053
CLOSED LOW
CREATED AT: 09:18:12 09/06/2021 - RESOLVED AT: ...

ATTRIBUTES: OBJECTS: TIME TO DETECT: TIME TO RESPONSE:



General information

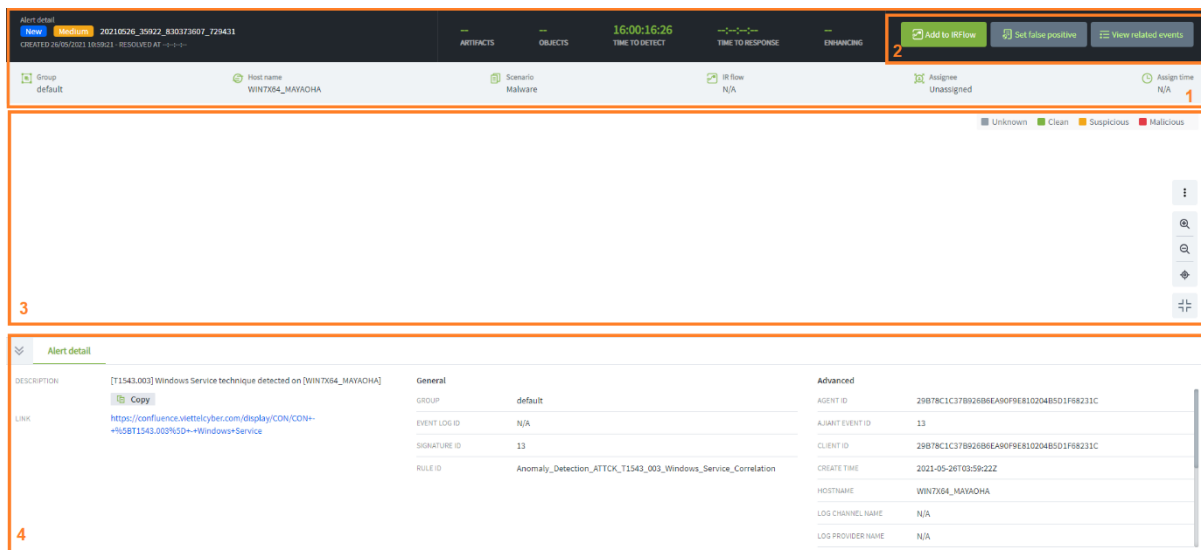
ASSIGNEE	root
DESCRIPTION	Windows executable load a module
GROUP	default
HOST NAME	
IR FLOW NAME	liennt_dashboard_close
LINK	N/A
RULE ID	Load image
SCENARIO	N/A

Advanced information

[Show more information >](#)

3.4.5 Xem chi tiết alert

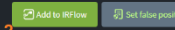
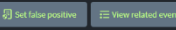
- Cho phép xem thông tin chi tiết alert, hỗ trợ tự động làm giàu thông tin bằng cách tự động thu thập thông tin các sự kiện liên quan đến alert vừa phát sinh, cung cấp biểu đồ trực quan để xem nhanh mối quan hệ giữa các đối tượng có trong alert



Alert detail
New Medium 20210526_35922_830373807_729431
CREATED AT: 09:00:11 26/05/21 - RESOLVED AT: ...

Group: default Host name: WIN7X64_MAYAOHA Scenario: Malware IR flow: N/A Assign: Unassigned Assign time: N/A

16:00:16:26
TIME TO DETECT: TIME TO RESPONSE:

Unknown Clean Suspicious Malicious

Alert detail

DESCRIPTION: [T1543.003] Windows Service technique detected on [WIN7X64_MAYAOHA]

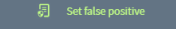
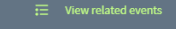
LINK: <https://confluence.viettelcyber.com/display/CON/CDN-+95B11543.002%5D+-+Windows+Service>

General

GROUP	default
EVENT LOG ID	N/A
SIGNATURE ID	13
RULE ID	Anomaly_Detection_ATTCK_T1543_003_Windows_Service_Correlation

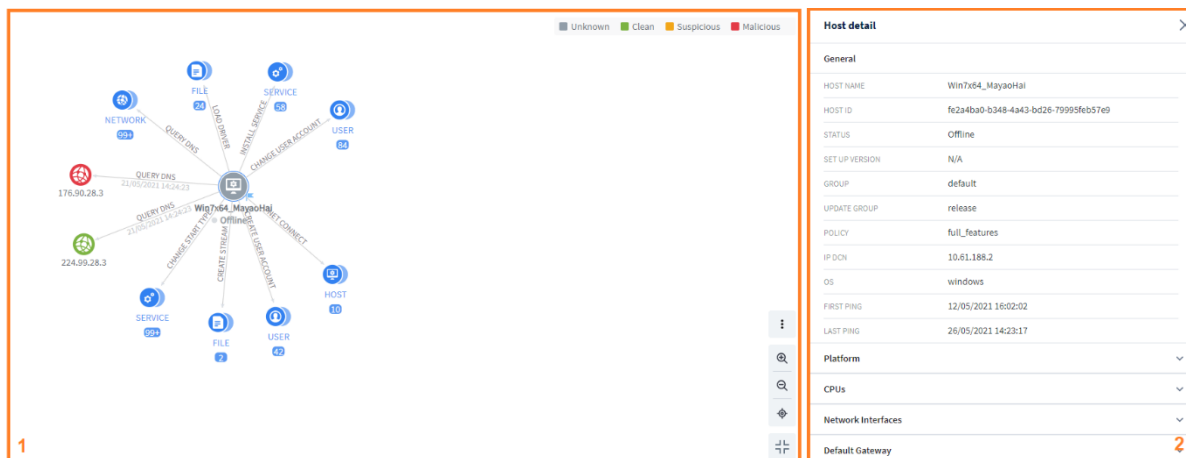
Advanced

AGENT ID	29878C1C37B92686EA90F9E81020485D1F8231C
ALERT EVENT ID	13
CLIENT ID	29878C1C37B92686EA90F9E81020485D1F8231C
CREATE TIME	2021-05-26T03:59:22Z
HOSTNAME	WIN7X64_MAYAOHA
LOG CHANNEL NAME	N/A
LOG PROVIDER NAME	N/A

- 1 – Nhóm thông tin chung của alert, trong đó:
 - + Artifacts: Danh sách các đối tượng khả nghi được đánh dấu tự động/thủ công trong alert
 - + Objects: Danh sách các đối tượng trong alert
 - + Time to detect: Tổng thời gian phát hiện và điều tra alert, tính từ khi alert sinh ra đến khi được đưa vào IR flow hoặc đánh dấu “FALSE POSITIVE”
 - + Time to response: Tổng thời gian xử lý alert, tính từ khi alert được đưa vào IR flow đến khi đóng IR flow
 - + Enhancing: Tỷ lệ hoàn thành quá trình tự động làm giàu thông tin của hệ thống
- 2 – Nhóm các thao tác với alert
 - + Chọn  để đưa alert vào IR flow, xem trường hợp đưa 01 alert vào IR flow đã tồn tại trong [3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR flow đã có](#) hoặc vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert](#)
 - + Chọn  để đánh dấu không nguy hiểm cho alert, xem trường hợp đánh dấu 01 alert trong [3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert](#)
 - + Chọn  để chuyển đến tính năng Event Search với thời gian mặc định là 04 tiếng trước và sau thời gian phát sinh alert
- 3 – Biểu đồ điều tra (Investigation Graph): Chi tiết xem trong [3.3.5 Biểu đồ điều tra \(Investigation Graph\)](#)
- 4 – Tab các thông tin liên quan đến alert: Hiện tại chỉ hỗ trợ Alert Detail

3.4.6 Biểu đồ điều tra (Investigation Graph)

- 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.



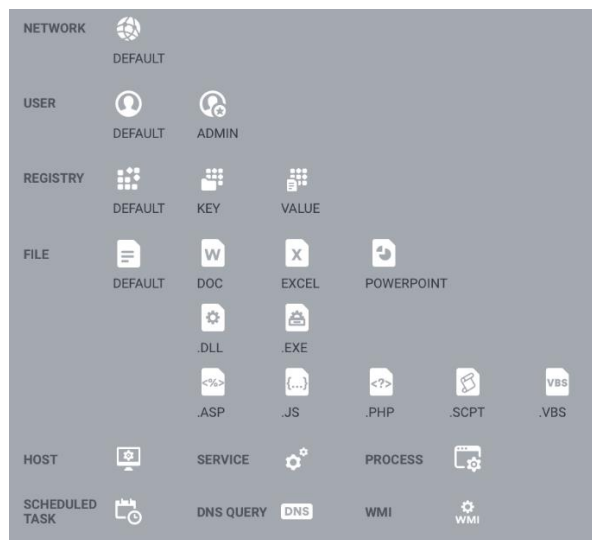
- 1 – Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ
- 2 – Khu vực hiển thị thông tin chi tiết các đối tượng trên biểu đồ

3.4.6.1 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:



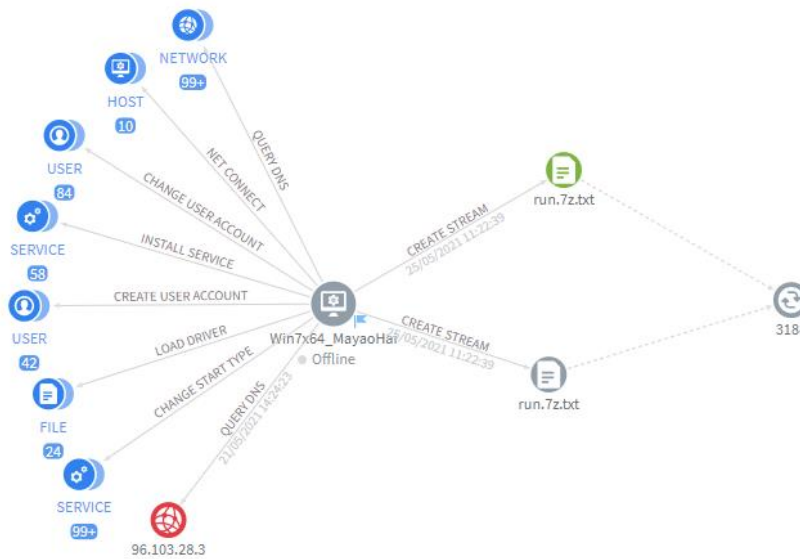
- Mỗi đối tượng bao gồm các trạng thái như sau: Unknown Clean Suspicious Malicious
- Giữa các đối tượng, hiển thị mối quan hệ bao gồm:
 - + Relationship: Mối quan hệ định nghĩa theo các sự kiện phát sinh trong vòng 01 ngày từ thời điểm phát sinh alert (trong đó tên mối quan hệ nằm phía trên mũi tên nối liền 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)



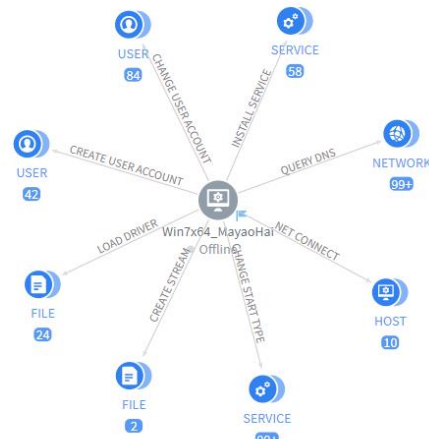
+ Ví dụ:



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

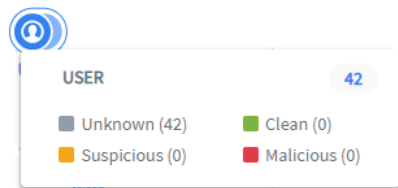
Thao tác hỗ trợ hiển thị	Ý nghĩa
Hide reference Hide relationship name	Cho phép ẩn/hiện các thông tin trên biểu đồ: + Reference: Khi chọn, cho phép ẩn/hiện thông tin tham chiếu bao gồm mũi tên nét đứt và đối tượng tham chiếu tại tất cả các đối tượng hiện có trên biểu đồ + Relationship name: Khi chọn,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

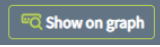
Hover để xem thống kê nhanh tại từng nhóm đối tượng như sau:



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:

Objects in this group network						
Search object...						
☒ Unknown (48) ☒ Clean (125) ☒ Malicious (87)						
Selected 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	
☐	Clean	crf4.digicert.com	80.105.28.3	N/A	SYSTEM	
☐	Clean	crf4.microsoft.com	16.87.28.3	N/A	SYSTEM	
☐	Malicious	www.microsoft.com	96.103.28.3	N/A	SYSTEM	
☐	Clean	ocsp.digicert.com	240.94.28.3	N/A	SYSTEM	
☐	Clean	crf4.verisign.com	224.91.28.3	N/A	SYSTEM	
☐	Malicious	www.msfnets.com	0.96.28.3	N/A	SYSTEM	
☐	Clean	csc3-2010-crf4.verisign.com	112.89.28.3	N/A	SYSTEM	
☐	Clean	ocsp.globalign.com	48.88.28.3	N/A	SYSTEM	
☐	Clean	crf4.digicert.com	80.105.28.3	N/A	SYSTEM	

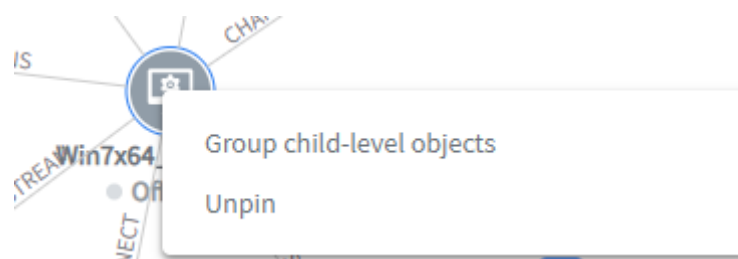
- + Cho phép lọc các đối tượng trong nhóm theo trạng thái ■ Unknown ■ Clean ■ Suspicious ■ Malicious hoặc tìm kiếm nhanh bằng cách nhập dữ liệu muốn tìm kiếm trong tất cả các trường
- + Khi đã chọn được đối tượng phù hợp, chọn  để hiển thị 01 đối tượng lên biểu đồ hoặc chọn  để chọn tối đa 20 đối tượng lên biểu đồ

Lưu ý: 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

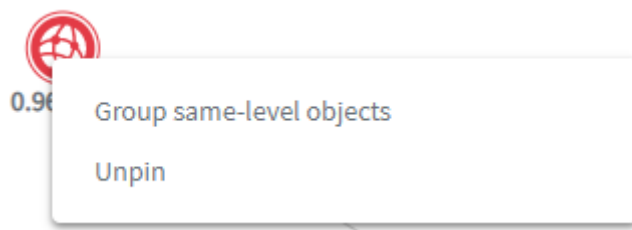


Bước 2: Sau khi đã hiển thị các đối tượng cần điều tra trên biểu đồ, các thao tác hỗ trợ mở rộng/thu gọn bao gồm:

- + 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”

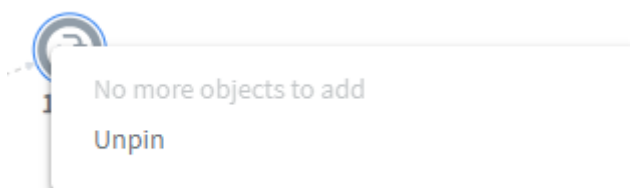


- + Tại các đối tượng khác: Hỗ trợ thu gọn bằng cách nhóm lại theo loại đối tượng và loại quan hệ với các đối tượng cùng cấp bằng cách chọn chuột phải tại đối tượng, sau đó chọn “Group same-level objects”

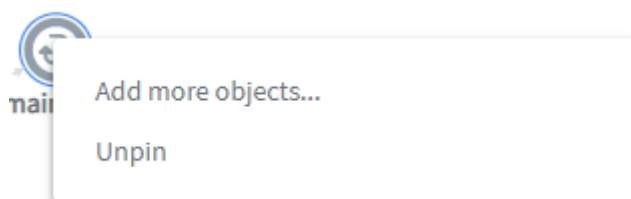


+ Tại đối tượng là tiến trình (process) cho phép mở rộng để điều tra loang bằng cách chọn chuột phải tại đối tượng,

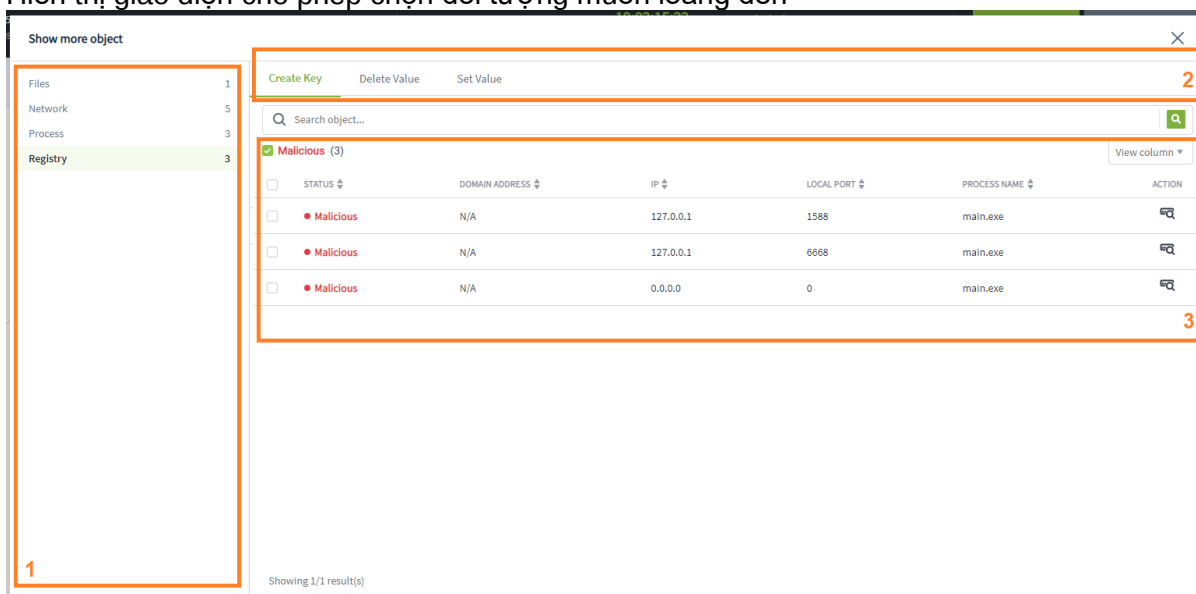
Trường hợp không thể tiếp tục loang, hiển thị:



Trường hợp có thể tiếp tục loang, chọn “Add more objects...”



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

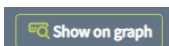


1 – Chọn loại đối tượng

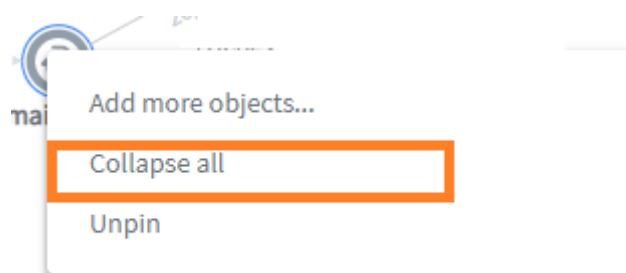
2 – Chọn loại quan hệ từ tiến trình tới đối tượng

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

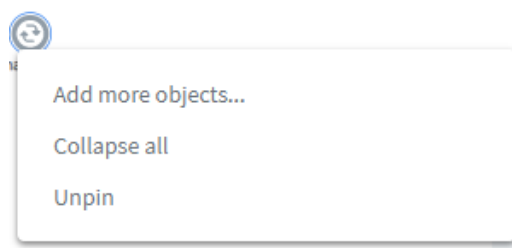
Khi đã chọn được đối tượng phù hợp, chọn  để hiển thị 01 đối tượng lên biểu đồ hoặc chọn  để chọn tối đa 20 đối tượng lên biểu đồ

+ 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,



+ 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



3.4.6.2 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 Copy
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 ▼

1 - 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 ▼ để mở rộng và hiển thị nhóm thông tin.

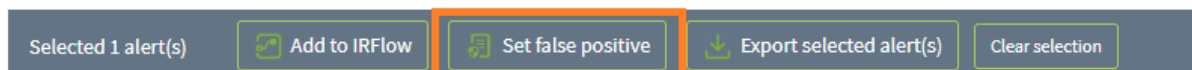
Thao tác **Copy** hỗ trợ sao chép nội dung trường thông tin

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	1941d3f261033344b22c5e9cf246e5683c17d450ac87d0af6f3ed7a52f431bb6	
PROCESS PATH	C:\users\admin\desktop\taodataoang\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	

3.4.7 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert

- Cho phép đánh dấu alert là không nguy hiểm và không tiếp tục xử lý
- Bước 1: Chọn 01/nhiều alert muốn đánh dấu không nguy hiểm
- Bước 2: Click nút “Set False Positive” (Nút Set False Positive chỉ hiển thị trong bản ghi có trạng thái là NEW hoặc tất cả các bản ghi được chọn đều ở trạng thái NEW)



- Bước 3: Nhập lý do đánh dấu không nguy hiểm và chọn

COMMENT

Write your reason here...

Cancel

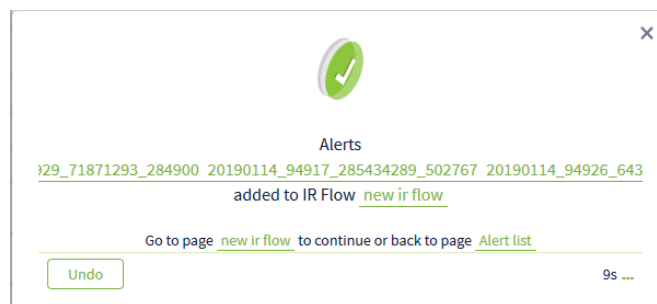
Set false positive

3.4.8 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert

- Bước 1: Lựa chọn 01/nhiều alert để tạo IRFlow
- Bước 2: Nhập các thông tin và tạo IRFlow

Dữ liệu hiển thị trong Combobox Assigned to bao gồm:

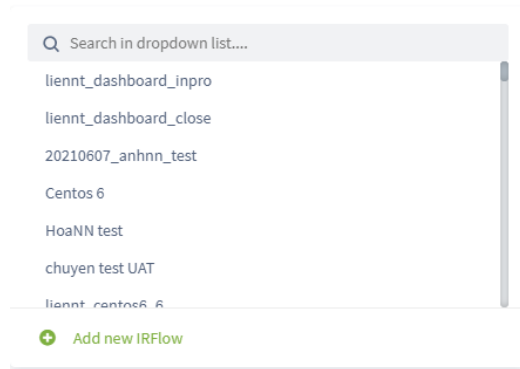
- + User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống
- + User đăng nhập thuộc group default: Hiển thị tên User đang login
- + User đăng nhập thuộc group cha: Hiển thị tất cả tên User thuộc group con của user đang login và user đang login
- + User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tên User đang login
- Bước 3: Sau khi tạo xong hiện cửa sổ sau để có thể hoàn tác trong 10s



- + Để hoàn tác: chọn “Undo” trong 10 s
- + Để tạo ngay IR flow và chuyển sang màn hình IR flow chọn tên IR flow vừa tạo: chọn “new ir flow”
- + Để quay về màn hình alert chọn “Alert list”

3.4.9 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



3.5 Màn hình IRFlow

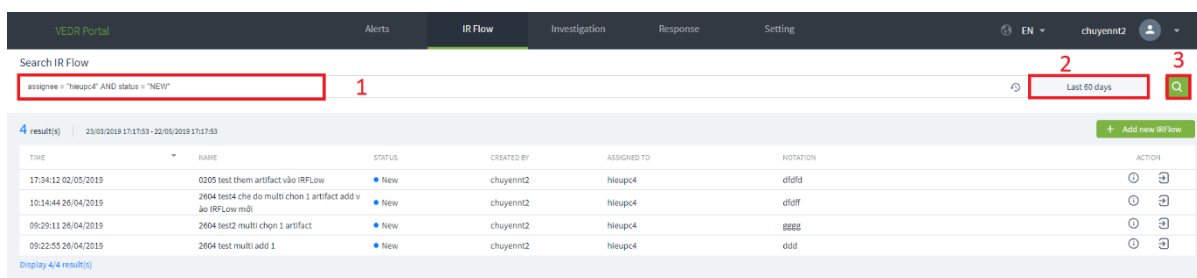
3.5.1 Danh sách hiển thị

- 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

3.5.2 Tìm kiếm IRFlow

Chỉ tìm kiếm được những bản ghi tương ứng với user đang đăng nhập

- Tương tự chức năng tìm kiếm ở màn hình alert, màn hình iRFlow hỗ trợ tìm kiếm theo query như sau



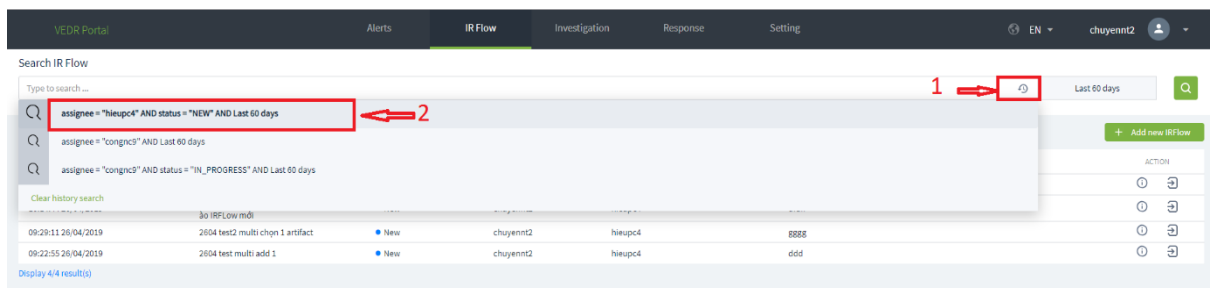
- Bước 1: Nhập vào textbox Search câu query với format như sau:
<tên_trường> <toán tử> "<value>" AND/OR <tên_trường> <toán tử> "<value>".....

Trong đó:

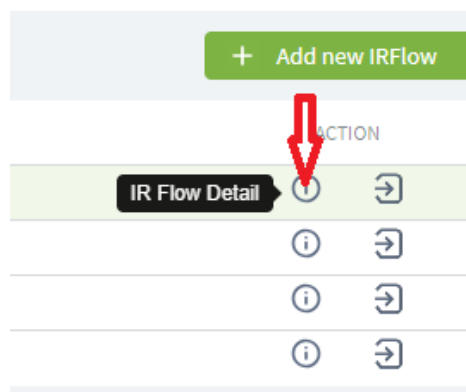
Viettel Cyber Security

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

- <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 button 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



ĐỂ vào xem thông tin chi tiết 1 IRFlow và thực hiện các hành động điều tra, xử lý người dùng chọn “IRFlow Detail”



3.5.3 Cách tạo IRFlow

- Bước 1: Click vào Add new IRFlow



Last 7 days



+
Add new IRFlow

	ACTION
	
	

- Bước 2: 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 IRFlow

×

IR Flow Name

IR Flow Name...

Assigned to

Choose assignees...

First Note

First Note ...

Cancel

Create

- Bước 4: Click button Create => IRFlow vừa tạo hiển thị trên Màn hình IRFlow

3.5.4 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

3.5.5 IRFlow – Detection

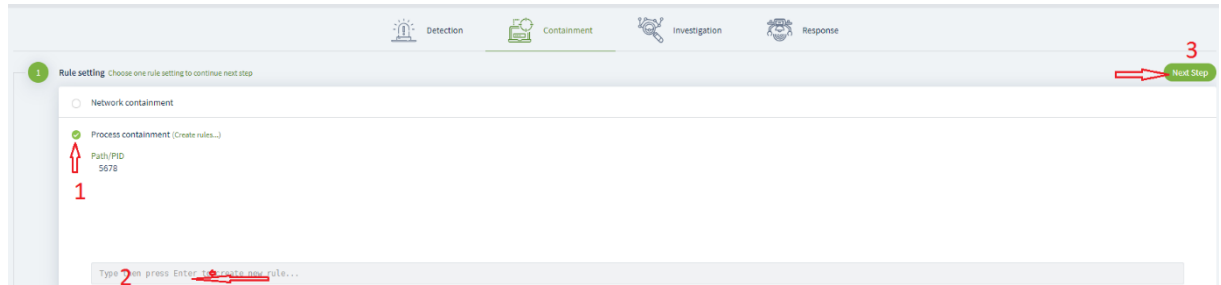
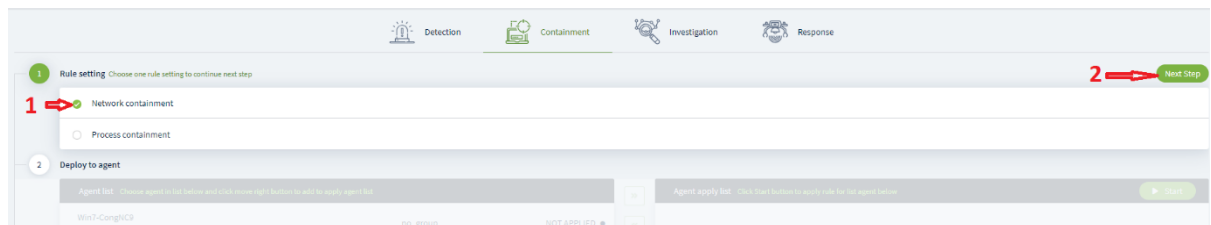
- Tab Detection hiển thị các đối tượng liên quan đến alert như:
 - + Danh sách máy tính có alert
 - + Danh sách alert
 - + Danh sách artifacts được phát hiện trong quá trình điều tra (investigation)

 Detection  Containment  Investigation  Response																								
Original detection																								
Agent DESKTOP-HHN2B1Q																								
Alert <table> <thead> <tr> <th>TIME</th><th>GROUP</th><th>HOSTNAME</th><th>SCENARIO</th><th>SEVERITY</th></tr> </thead> <tbody> <tr> <td>07:00:00 14/01/2019</td><td>no_group</td><td>DESKTOP-HHN2B1Q</td><td>Execution</td><td>High</td></tr> <tr> <td>07:00:00 14/01/2019</td><td>no_group</td><td>DESKTOP-HHN2B1Q</td><td>Execution</td><td>High</td></tr> <tr> <td>07:00:00 14/01/2019</td><td>no_group</td><td>DESKTOP-HHN2B1Q</td><td>Initial Access</td><td>High</td></tr> </tbody> </table>					TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY	07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Execution	High	07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Execution	High	07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Initial Access	High
TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY																				
07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Execution	High																				
07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Execution	High																				
07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Initial Access	High																				
Additional detection																								
Artifacts <table> <thead> <tr> <th>TIME</th><th>AGENT ID</th><th>OBJECT</th><th>FROM</th><th>REFERENCE</th></tr> </thead> <tbody> <tr> <td>07:25:05 14/01/2019</td><td>9D76E75C81645C8B88E18B46961C5D75C8154752</td><td>c:\Users\Test\Desktop\demo.exe</td><td>WIN_EVENT_LOG</td><td>plq35Wg8Ty9dpUVUJ-d</td></tr> <tr> <td>07:25:05 14/01/2019</td><td>9D76E75C81645C8B88E18B46961C5D75C8154752</td><td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\demo</td><td>WIN_EVENT_LOG</td><td>plq35Wg8Ty9dpUVUJ-d</td></tr> </tbody> </table>					TIME	AGENT ID	OBJECT	FROM	REFERENCE	07:25:05 14/01/2019	9D76E75C81645C8B88E18B46961C5D75C8154752	c:\Users\Test\Desktop\demo.exe	WIN_EVENT_LOG	plq35Wg8Ty9dpUVUJ-d	07:25:05 14/01/2019	9D76E75C81645C8B88E18B46961C5D75C8154752	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\demo	WIN_EVENT_LOG	plq35Wg8Ty9dpUVUJ-d					
TIME	AGENT ID	OBJECT	FROM	REFERENCE																				
07:25:05 14/01/2019	9D76E75C81645C8B88E18B46961C5D75C8154752	c:\Users\Test\Desktop\demo.exe	WIN_EVENT_LOG	plq35Wg8Ty9dpUVUJ-d																				
07:25:05 14/01/2019	9D76E75C81645C8B88E18B46961C5D75C8154752	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\demo	WIN_EVENT_LOG	plq35Wg8Ty9dpUVUJ-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

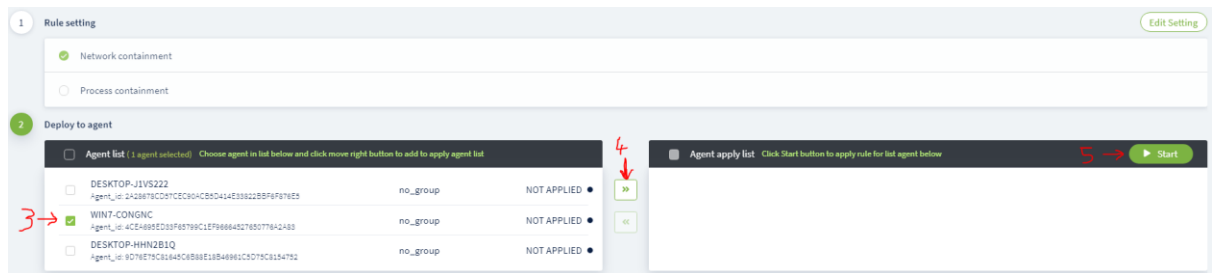
3.5.6 IRFlow – Containment

- 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”

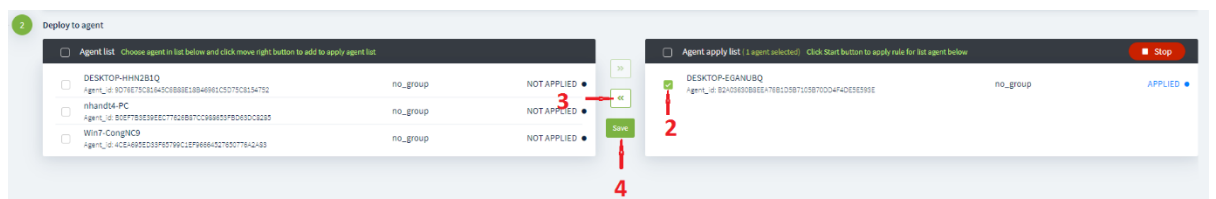
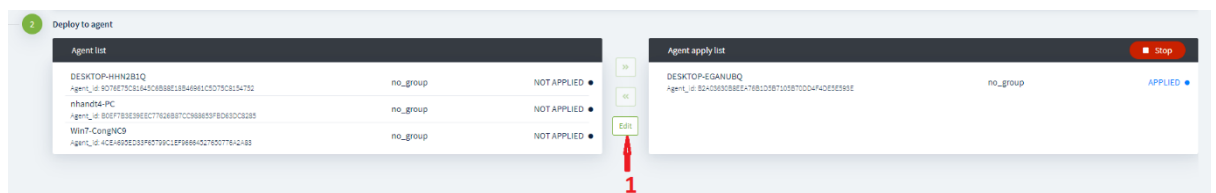
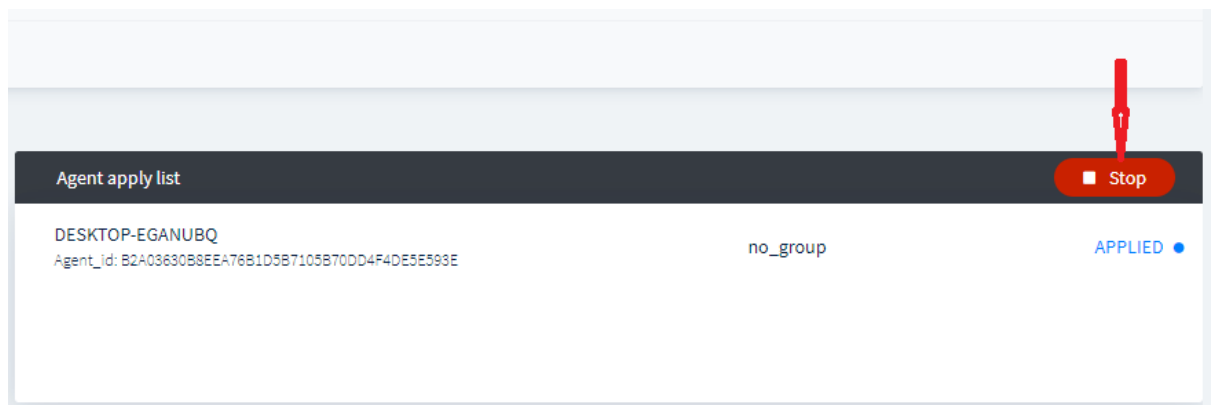


Lưu ý: sau khi nhập Path/PID thì phải ấn Enter để lưu lại cấu hình. Có thể suspend cùng lúc nhiều tiến trình

- Bước 2: chọn danh sách Agent cần cô lập và chọn “Start” để bắt đầu cô lập



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



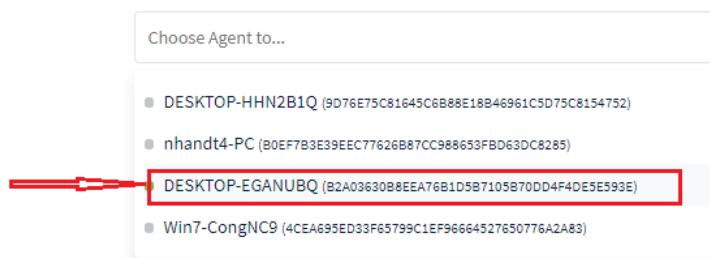
- Trong trường hợp người quản trị không chủ động dừng việc cô lập trên Portal thì sau thời gian mặc định (24h) thì Agent cũng tự động gỡ cô lập dưới Agent.

3.5.7 IRFlow – Investigation

3.5.7.1 Process Analysis

3.5.7.1.1 Xem thông tin process

- Đây 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



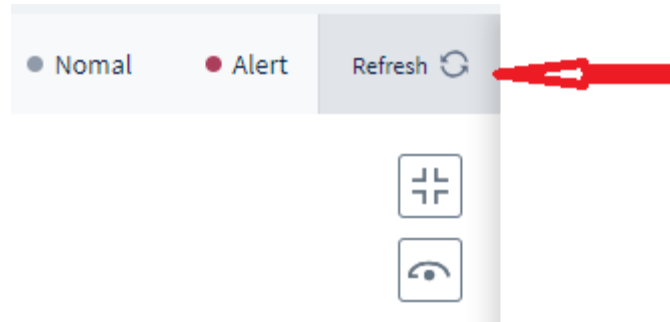
- Lưu ý:
 - + Thời gian timeout tạo kết nối là 60s. Hết 60s không kết nối được Agent thì cần kết nối lại.
 - + Tại 1 thời điểm trong 1 IRFlow chỉ có thể tạo 1 kết nối tới Agent. Trong trường hợp có tài khoản khác đang kết nối với Agent trong cùng IRFlow thì sẽ thông báo lỗi

DESKTOP-EGANUBQ

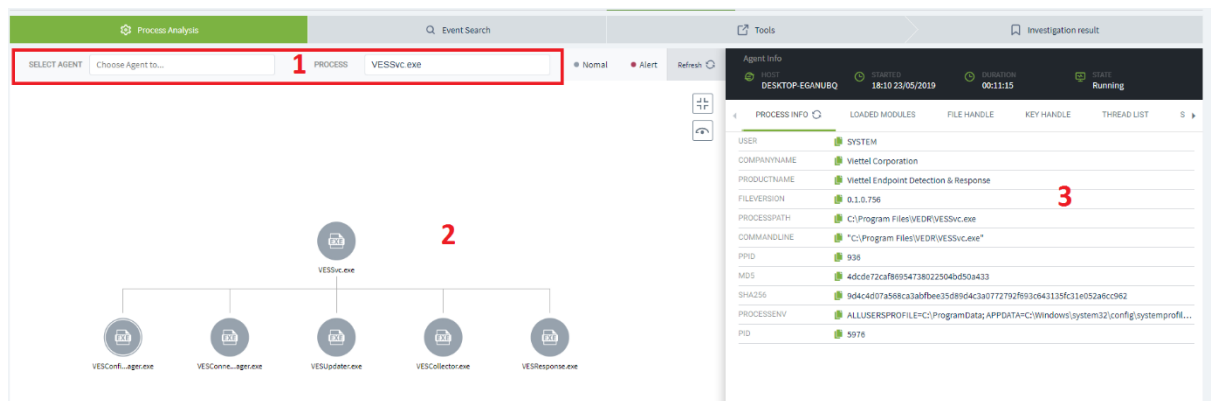
CreateSession failed: another websocket connected

Try Again

- 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



- Vùng 1: chọn agent và chọn process
- Vùng 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
- Vùng 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 Info	
HOST DESKTOP-EGANUBQ	STARTED 18:10 23/05/2019
DURATION 00:26:31	STATE Running
PROCESS INFO	LOADED MODULES
FILE HANDLE	KEY HANDLE
THREAD LIST	S
USER	SYSTEM
COMPANYNAME	Viettel Corporation
PRODUCTNAME	Viettel Endpoint Detection & Response
FILEVERSION	0.1.0.756
PROCESSPATH	C:\Program Files\VEDR\VESSvc.exe
COMMANDLINE	"C:\Program Files\VEDR\VESSvc.exe"
PPID	936
MD5	4dcde72caf86954738022504bd50a433
SHA256	9d4c4d07a568ca3abfbee35d89d4c3a0772792f693c643135fc31e052a6cc962
PROCESSENV	ALLUSERSPROFILE=C:\ProgramData; APPDATA=C:\Windows\system32\config\systemprofil...
PID	5976

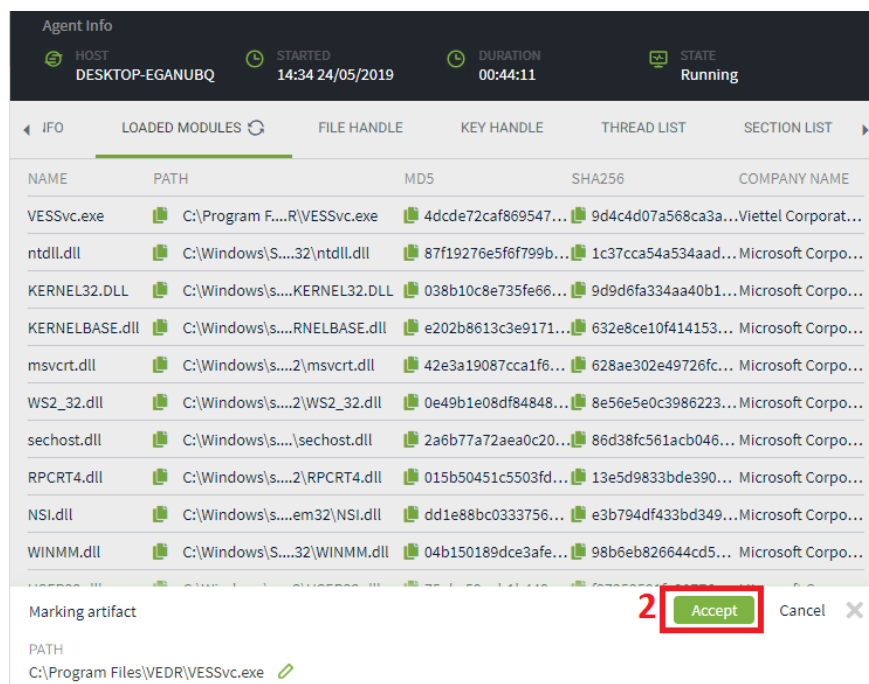
- Lưu ý:
 - + Khi chuyển tab con trong Investigation như Event Search, Tools, Investigation Result thì phiên kết nối với Agent được giữ và không cần kết nối lại
 - + Khi chuyển tab khác như Detection, Containment, Response hay Alert, Setting.... Hoặc F5, Logout... thì cần phải tạo lại kết nối với Agent
 - + 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

3.5.7.1.2 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
- Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào button "Marking artifact"

Agent Info				
HOST DESKTOP-EGANUBQ	STARTED 14:34 24/05/2019	DURATION 00:41:42	STATE Running	
IFO	LOADED MODULES	FILE HANDLE	KEY HANDLE	THREAD LIST
SECTION LIST				
NAME	PATH	MD5	SHA256	COMPANY NAME
VESSvc.exe	C:\Program F....R\VESSvc.exe	4dcde72caf869547...	9d4c4...	Marking artifact
ntdll.dll	C:\Windows\S....32\ntdll.dll	87f19276e5f6f799b...	1c37cca54a534aad...	Microsoft Corpo...
KERNEL32.DLL	C:\Windows\s....KERNEL32.DLL	038b10c8e735fe66...	9d9d6fa334aa40b1...	Microsoft Corpo...
KERNELBASE.dll	C:\Windows\s....RNELBASE.dll	e202b8613c3e9171...	632e8ce10f414153...	Microsoft Corpo...
msvcrt.dll	C:\Windows\s....2\msvcrt.dll	42e3a19087cca1f6...	628ae302e49726fc...	Microsoft Corpo...
WS2_32.dll	C:\Windows\s....2\WS2_32.dll	0e49b1e08df84848...	8e56e5e0c3986223...	Microsoft Corpo...
sechost.dll	C:\Windows\s....\sechost.dll	2a6b77a72aea0c20...	86d38fc561acb046...	Microsoft Corpo...

- Bước 2: Click vào button “Accept”, có thể chỉnh sửa đường dẫn file khi click vào icon Edit

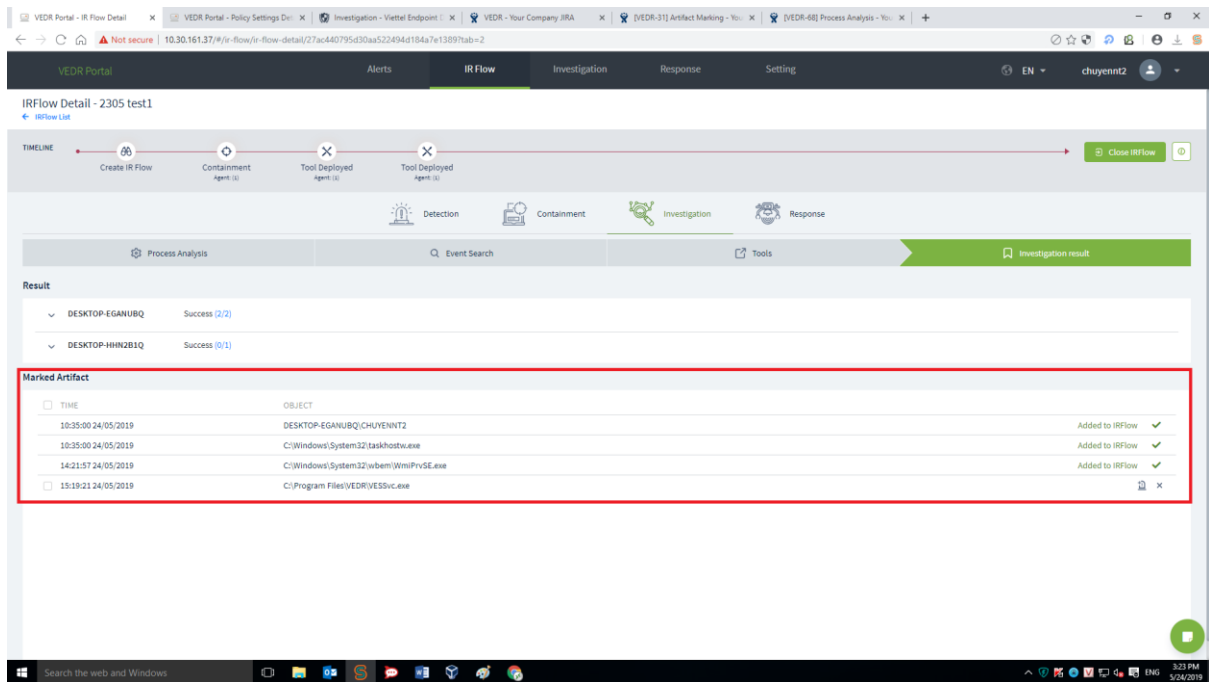


Trường hợp chọn bản ghi có Agent chưa tồn tại trong Detection sẽ có thêm check box Add Agent to IRFlow. Khi thực hiện Accept thì Agent tương ứng sẽ được add vào Detection

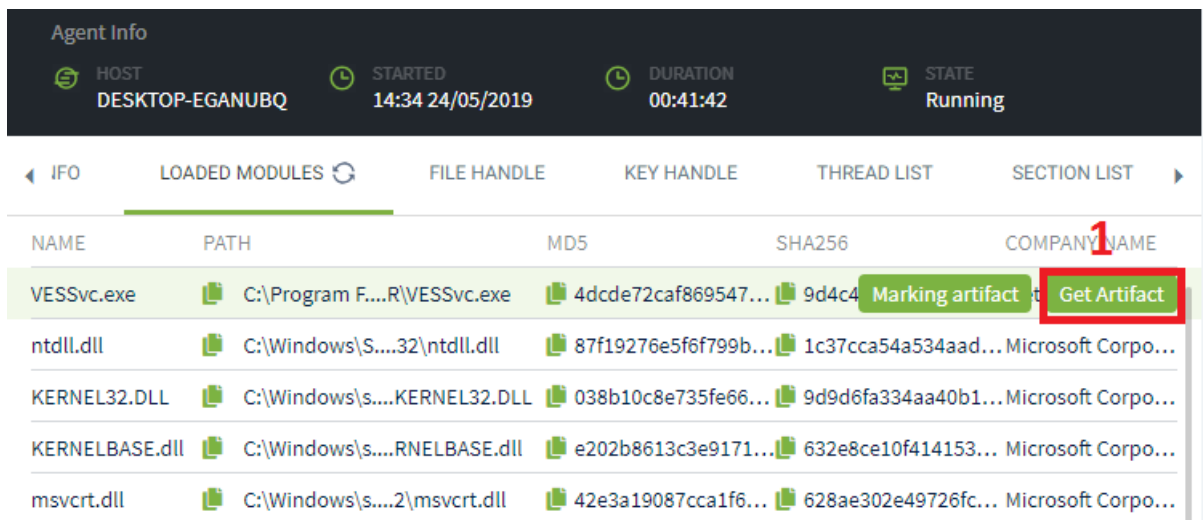
The screenshot shows the AjiAnt IRFlow Detail interface for agent 'lienntesst5.5'. It displays a table of events with columns: AGENTID, EVENTID, COMPUTER, LOGTYPE, SYSTEMTIMESTAMP, and TIMESTAMP. A 'Marking artifact(s)' dialog box is open, listing several artifacts with checkboxes. The artifacts include 'YCHUYENNT2', 'C:\Windows\system32', 'C:\Windows\Microsoft.NET\Framework\4.0.30319\regasm.exe', and 'C:\Windows\Microsoft.NET\Framework\4.0.30319\RegAsm.exe'. The 'Add Agent To IR Flow' button is highlighted with a red circle.

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

The screenshot shows the 'Agent Info' section with details for agent 'DESKTOP-EGANUBQ', including 'HOST', 'STARTED' time (14:34 24/05/2019), 'DURATION' (00:45:22), and 'STATE' (Running). Below this is the 'FILE HANDLE' section, which is a table with columns: NAME, PATH, MD5, SHA256, and COMPANY NAME. The first row is highlighted in red and contains the text 'Marked artifact...' and 'View all Artifacts in Investigation Result'. A red box highlights the 'View all Artifacts in Investigation Result' link. A red number '3' is also present next to the link.



- 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 button “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



2

3

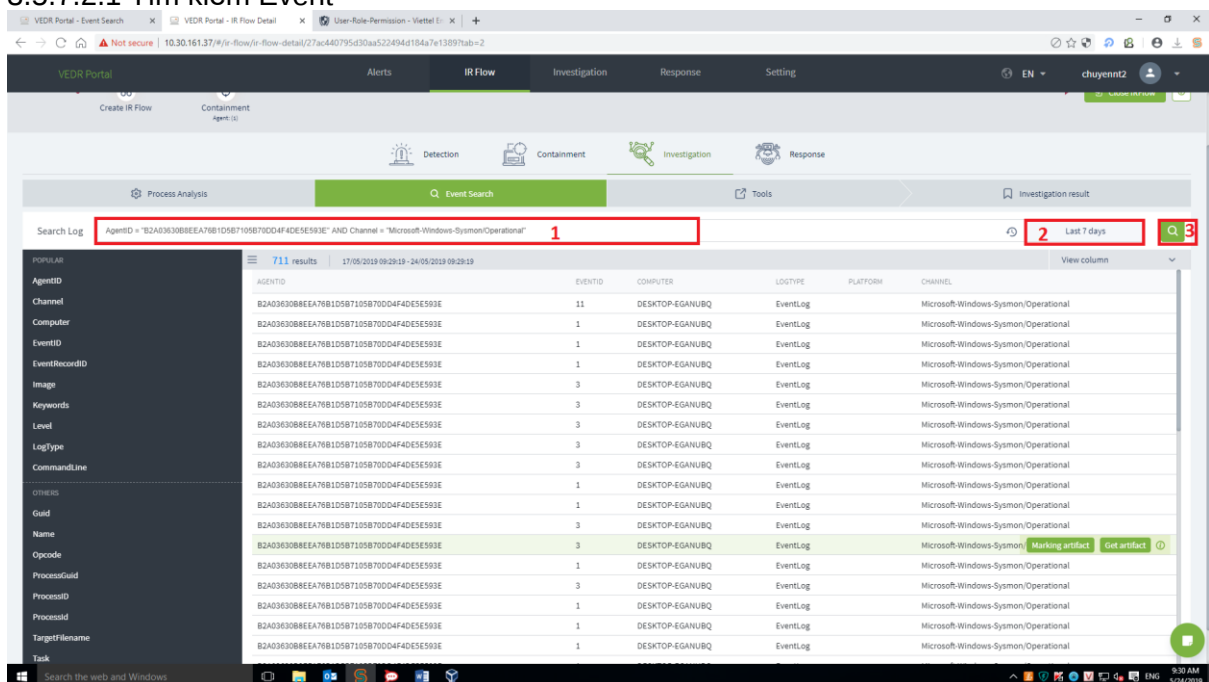
Accept

Cancel

3.5.7.2 Event Search

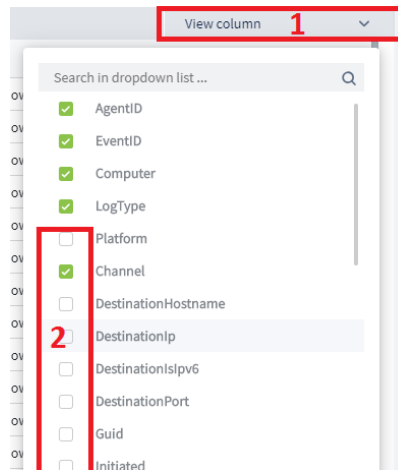
- Đây là quá trình tìm kiếm các đối tượng dựa vào event logs. Khác với các tab khác trong IRFLow chỉ hiển thị thông tin các Agent được add vào IRFLow thì ở tab này hiển thị toàn bộ event của tất cả Agent trong hệ thống

3.5.7.2.1 Tìm kiếm Event

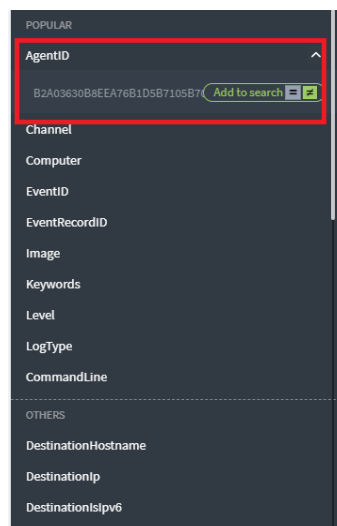


- Bước 1: Nhập vào textbox Search câu query với format như sau:
`<tên_trường> <toán tử> "<value>" AND/OR <tên_trường> <toán tử> "<value>".....`
- Trong đó:

- <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 2: Chọn khoảng thời gian tìm kiếm bằng cách click vào button Date & Time và chọn thời gian tùy ý. Nếu không chọn thời gian thì hệ thống chọn mặc định là Last 7 days.
- Bước 3: 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
 - + Để thêm cột hiển thị click vào “View Column” và tích chọn các trường cần thiết



- Ngoài ra, người dùng có thể tìm kiếm các trường trong phần Popular và Others bằng cách show các value của các trường và hover vào value trong Popular/Others, bản ghi đó sẽ hiển thị 2 icon là: “=” và “!=”.
- + Nếu người dùng chọn “=” thì trên phần textbox Search sẽ hiện câu query tương ứng với toán tử “=”.
- + Nếu người dùng chọn “!=” thì trên phần textbox Search sẽ hiện câu query tương ứng với toán tử “!=”.
- + Nếu trong textbox Search đã có dữ liệu và người dùng chọn thêm các value trong phần Popular/Others thì 2 vế của câu query được kết nối với nhau bởi toán tử AND.

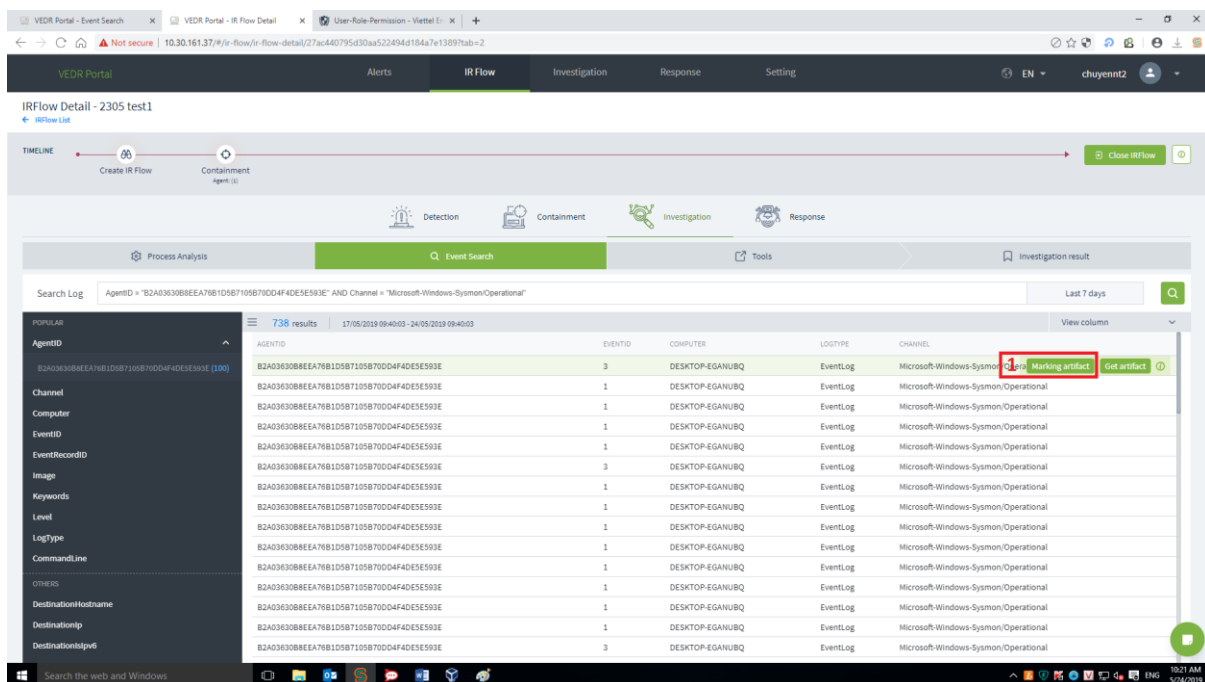


- Ở phần Others hiển thị toàn bộ các trường của log.
- Khi show/hide 1 trường sẽ hiển thị 5 trường có số lượng bản ghi nhiều nhất, sắp xếp từ cao xuống thấp.

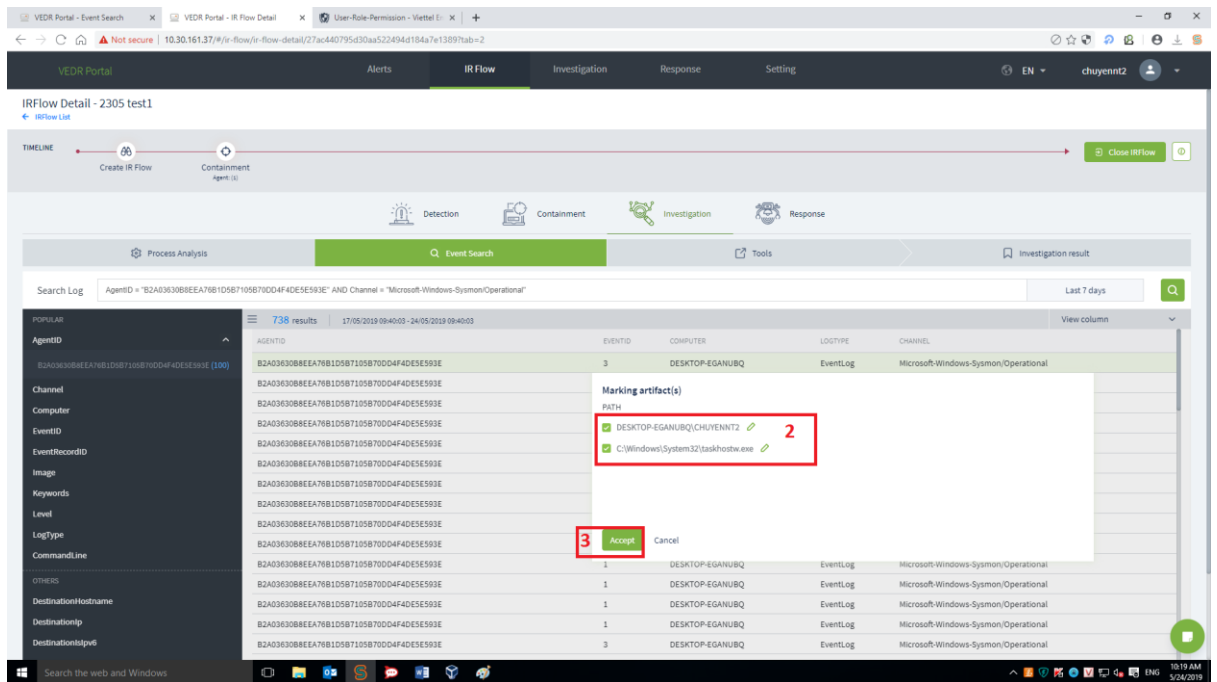
- Khi người dùng load more thì cập nhật bản ghi từng trường theo số lượng bản ghi hiển thị trên màn hình.
- + Ở phần Popular hiển thị 10 trường phổ biến của log được tìm kiếm nhiều nhất
- + Nếu có ≥ 10 trường thì hiển thị 10 trường có số lượng tìm kiếm nhiều nhất, nếu có ít hơn 10 trường thì hiển thị toàn bộ các trường đó ra.
- Khi show/hide trường sẽ hiển thị 5 trường có số lượng bản ghi nhiều nhất, sắp xếp từ cao xuống thấp.
- Khi người dùng load more thì cập nhật bản ghi từng trường theo số lượng bản ghi hiển thị trên màn hình.
- Khi kích đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó
- + Tab thông tin chi tiết hiển thị là dạng Table, dữ liệu hiển thị dưới dạng bảng
- + Khi chọn tab JSON thì dữ liệu hiển thị dưới dạng JSON

3.5.7.2.2 Xử lý Event

- Marking artifact: Đánh dấu artifact



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



- Trường hợp chọn event của Agent không thuộc IRFlow thì sẽ có lựa chọn để người dùng add Agent vào IRFlow. Agent sẽ được thêm vào màn hình Detection của IRFlow đang thao tác

Marking artifact(s)

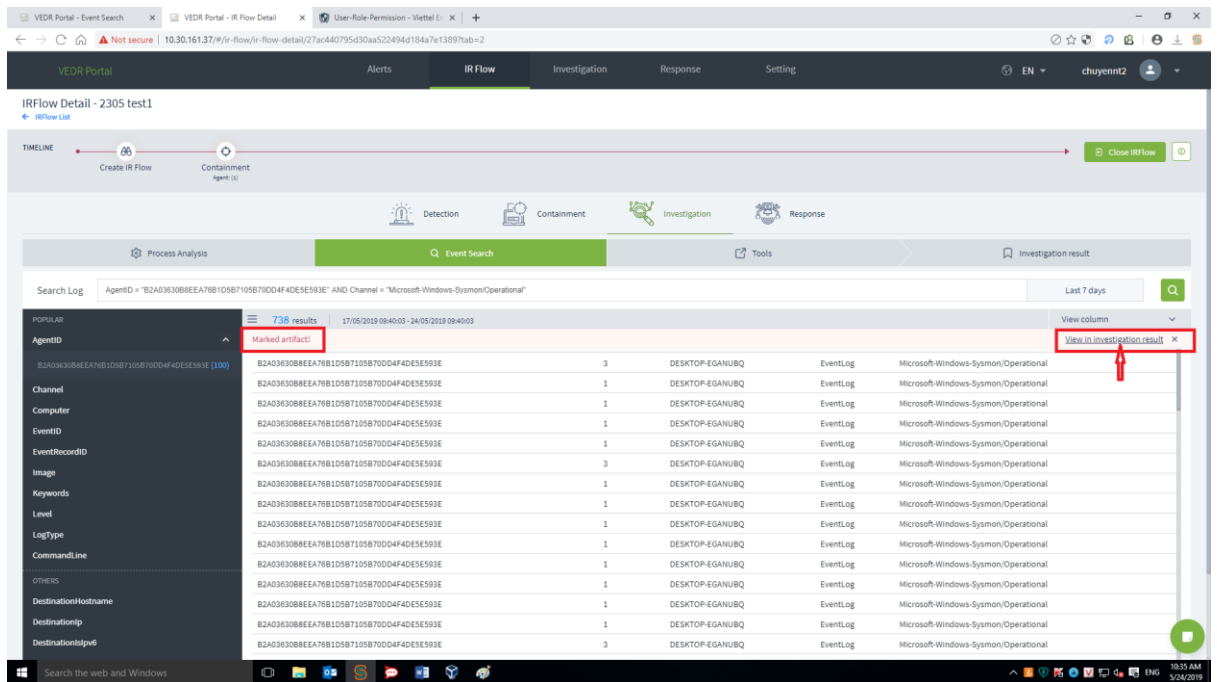
PATH

- ☐ TCP/IP Route Command
- ☐ NT AUTHORITY\SYSTEM
- ☒ C:\Program Files\VEDR\AgentInfo.exe
- ☐ C:\Windows\system32
- ☐ C:\Windows\System32\ROUTE.EXE

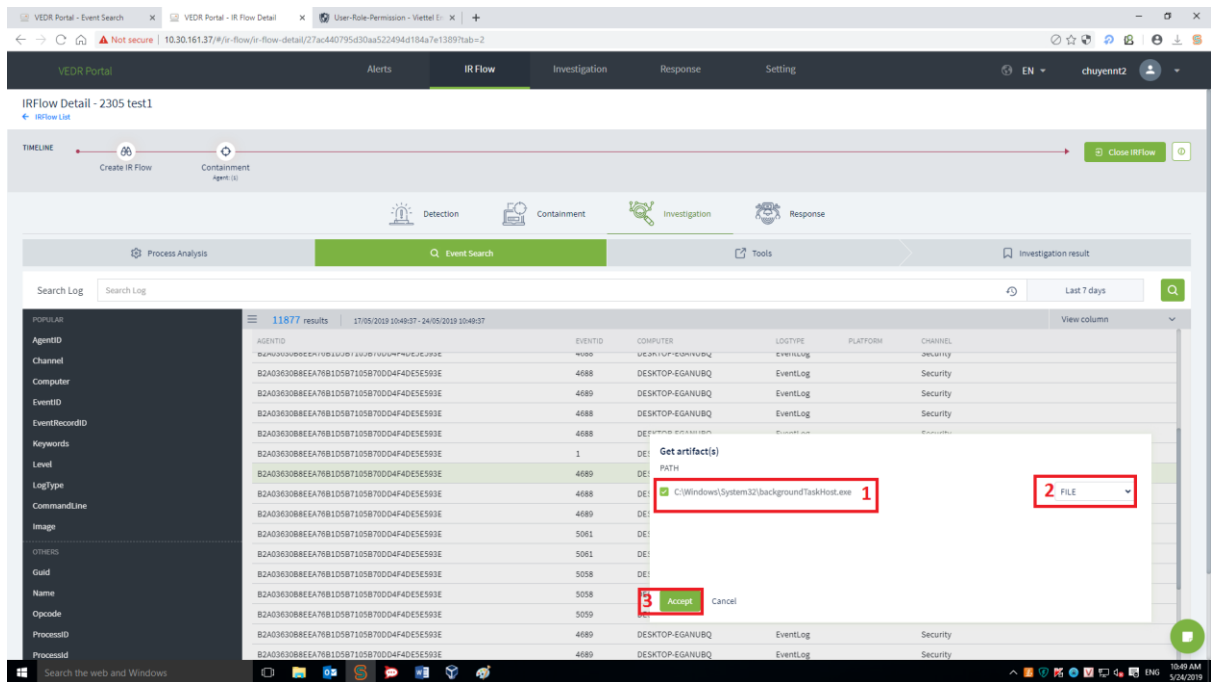
Accept Cancel

☒ Add Agent To IR Flow

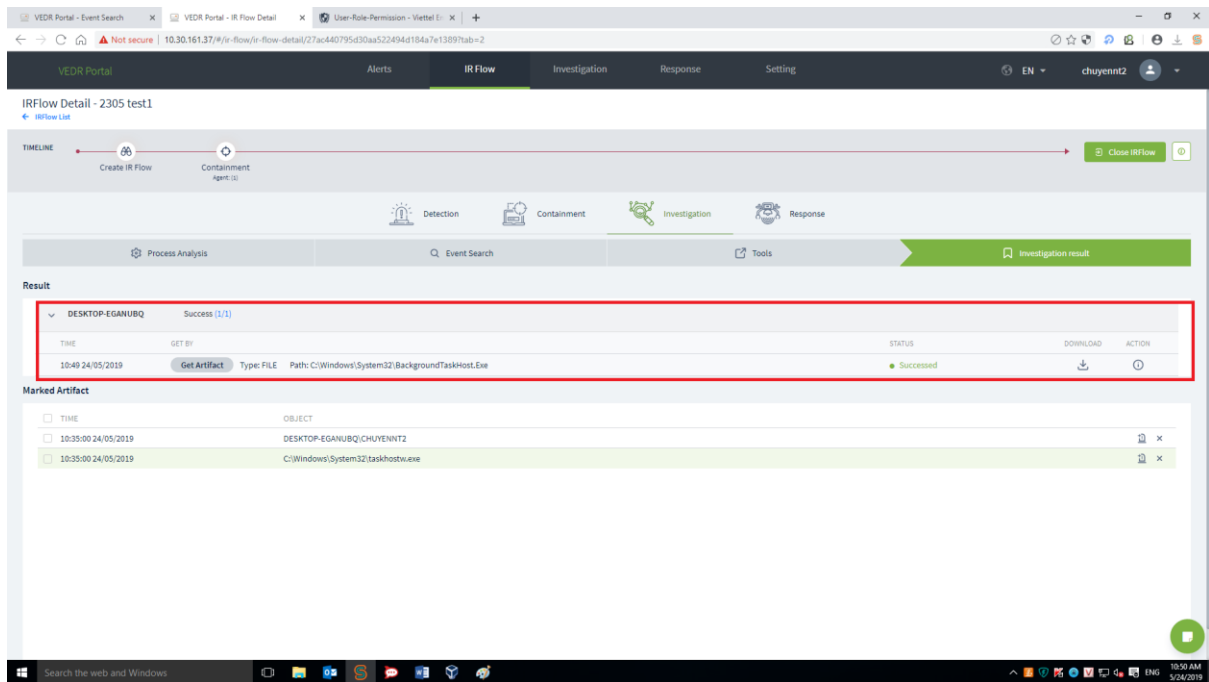
- Bước 2: Chọn path phù hợp để marking artifact. Sau đó nhấn vào Accept để thực hiện marking. Nếu chọn Cancel thì việc marking artifact sẽ bị trì hoãn.
- Khi marking artifact thành công màn hình sẽ hiển thị thông báo. Click vào "View in investigation result" để chuyển đến màn hình Investigation Result và event được marking sẽ được chuyển đến tab này



- 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 button “Get artifact” Trên màn hình sẽ hiển thị popup như sau:



- 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



- Xem thông tin chi tiết event: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó, click vào icon Xem chi tiết



3.5.7.2.3 Deploy Tools

- Đây 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:

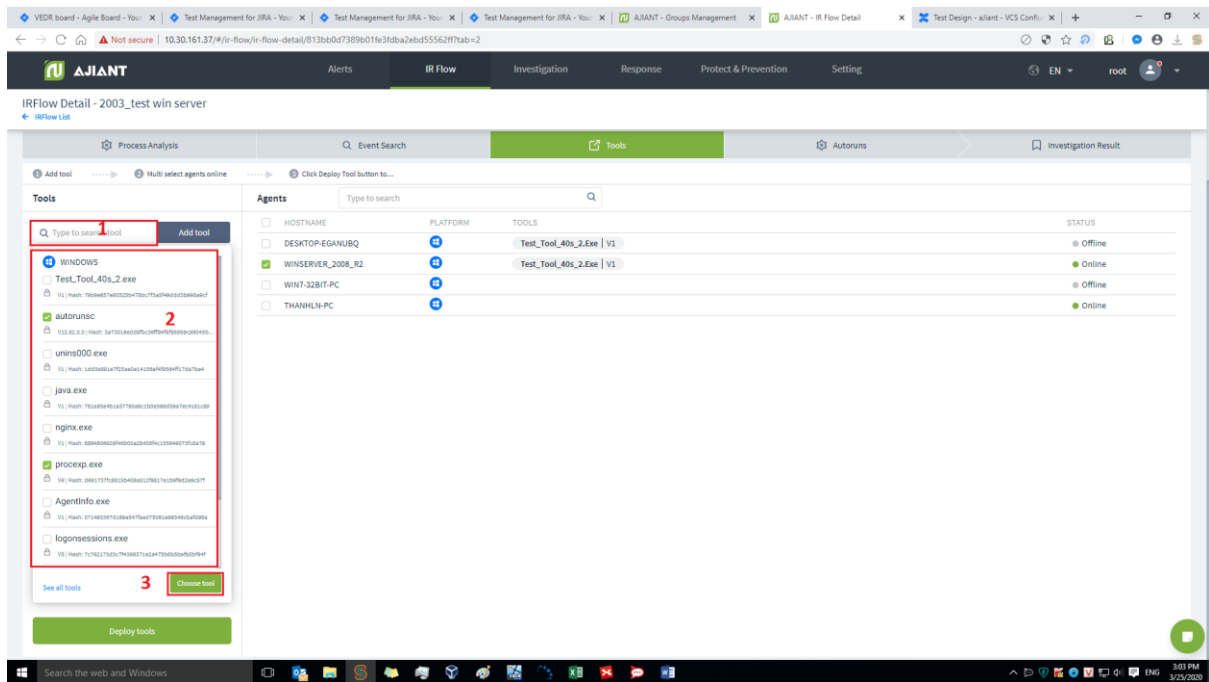
- + ListService: lấy danh sách service dưới máy agent

Luồng thực hiện chức năng này như sau:

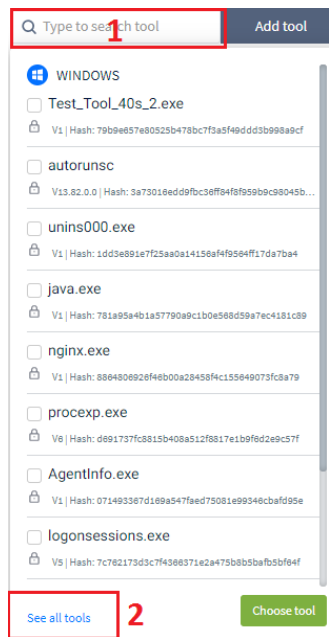
Thực hiện lựa chọn tool > Chọn agent > click “Deploy tools”

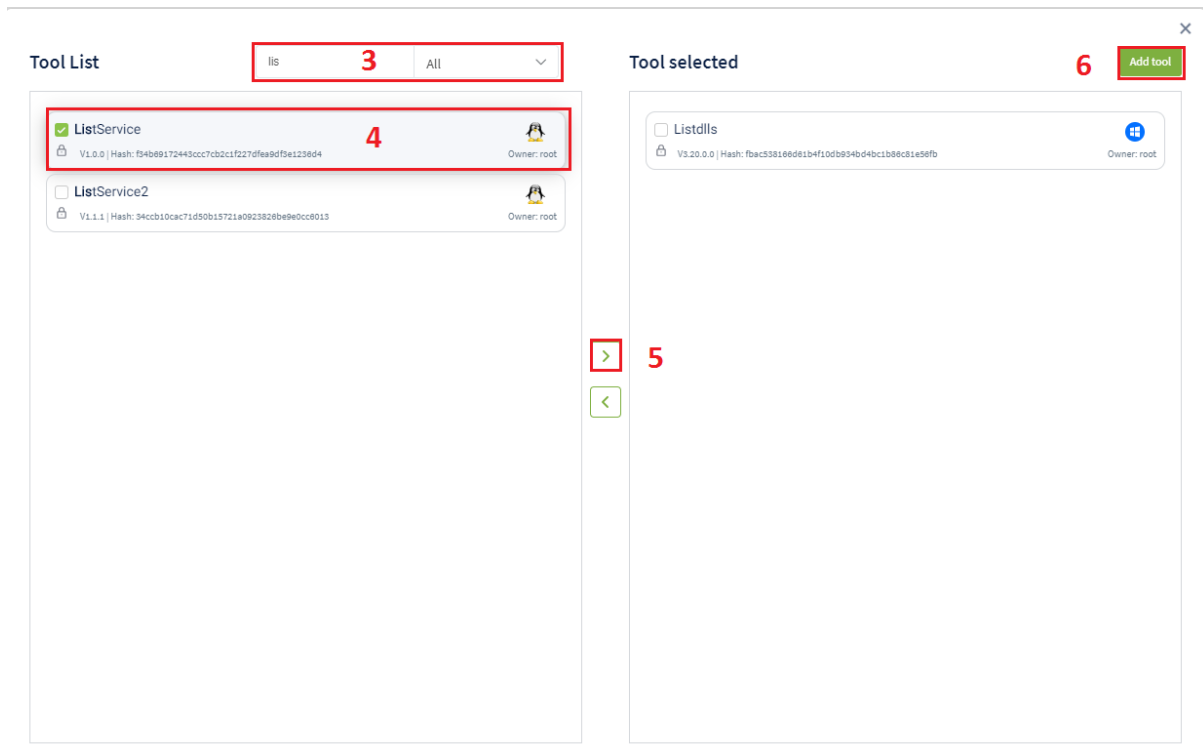
Để lựa chọn tool thích hợp có 2 cách sau:

- Cách 1: click vào textbox search tool > click tool cần deploy > click “Choose tool”

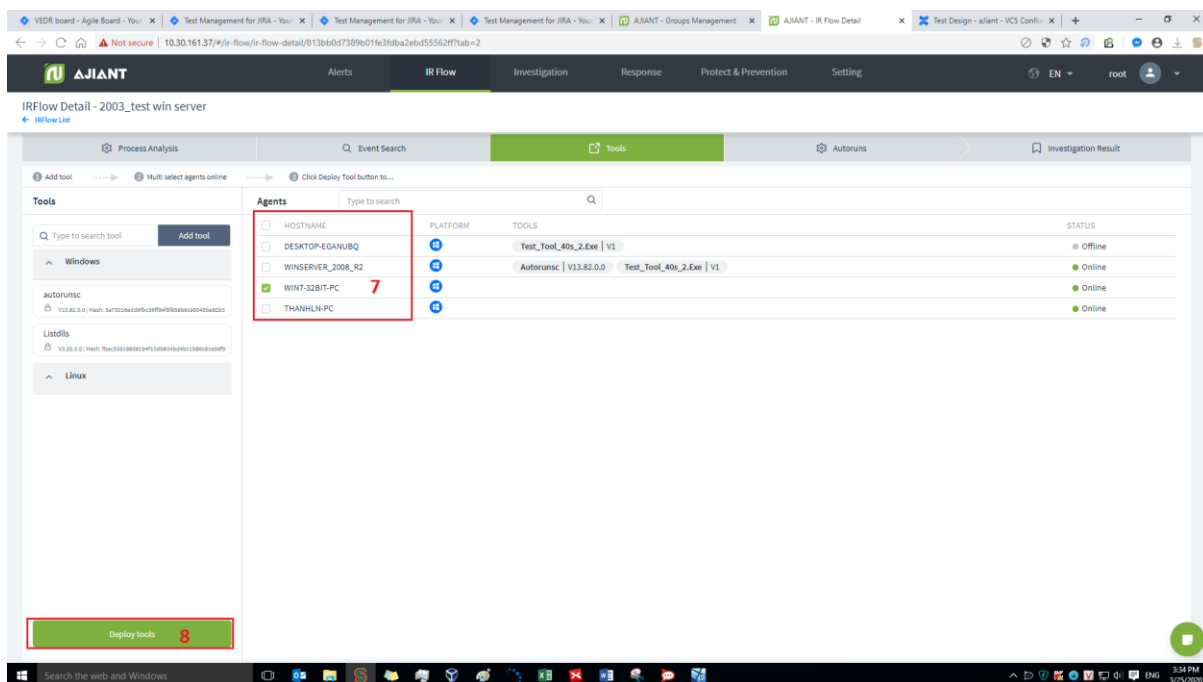


- Cách 2: Click vào textbox search tool > click “See all tools” => hiện ra màn hình danh sách tool đầy đủ > Tìm kiếm và lựa chọn tool cần deploy > click “Add tool”





- Sau bước tìm kiếm tool thực hiện chọn agent và click “Deploy tools”



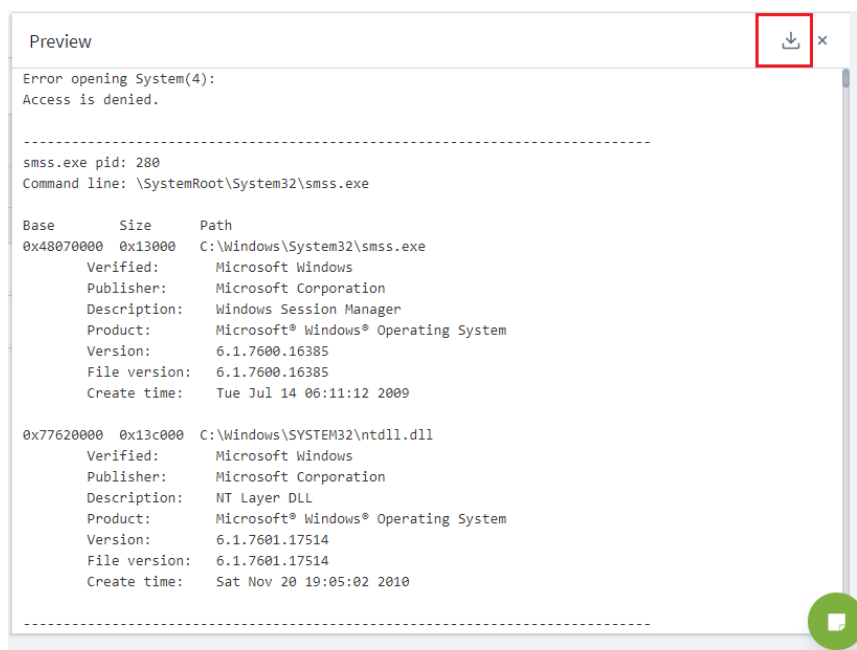
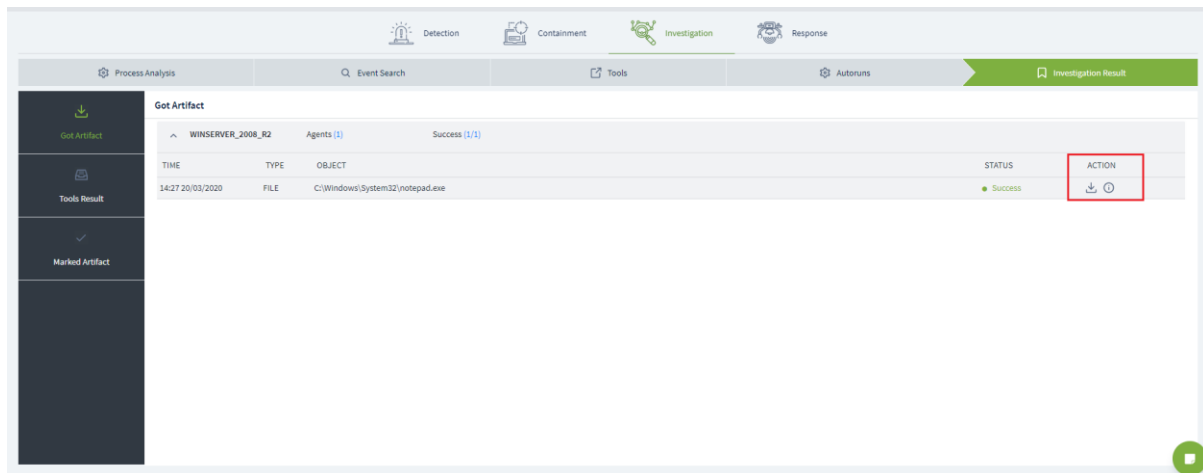
- Sau khi deploy tool thì xem kết quả ở tab Investigation Result, tab Tools Result

The screenshot displays the AJANT IR Flow Detail interface for a specific incident. The top navigation bar includes tabs for Alerts, IR Flow (selected), Investigation, Response, Protect & Prevention, and Setting. The main content area shows a timeline of events with icons for Detection, Containment, Investigation, and Response. Below the timeline, there are tabs for Process Analysis, Event Search, Tools, and Autotools. The 'Tools' tab is active, showing a table of tool results.

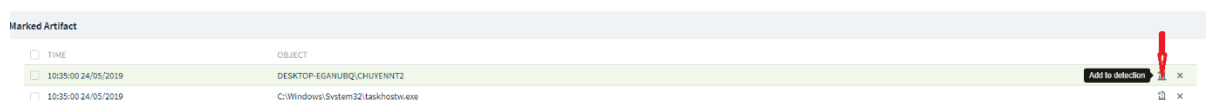
TIME	PLATFORM	AGENT ID	HOSTNAME	STATUS	ACTION
15:36 25/03/2020	Win7-32bit-PC	6B8C0237D1B81664B13E549126E02443BF0707F	Win7-32bit-PC	Success	Download

3.5.7.2.4 Xử lý Event

- 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
 - + 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 Xem chi tiết > click icon Download trên màn hình này



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



Chọn nhiều artifact và click “Add to detection”

Marked Artifact

Selected (2)

2

Add to detection

1

✓

✓

✓

TIME

10:35:00 24/05/2019

10:35:00 24/05/2019

OBJECT

DESKTOP-EGANUBQ\CHUYENNT2

C:\Windows\System32\taskhostw.exe

Marked Artifact		view all artifacts	Detection phase
Added artifacts to detection			
10:35:00 24/05/2019	DESKTOP-EGANUBQ\CHUYENNT2	Added to IRFlow	✓
10:35:00 24/05/2019	C:\Windows\System32\taskhostw.exe	Added to IRFlow	✓

- 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

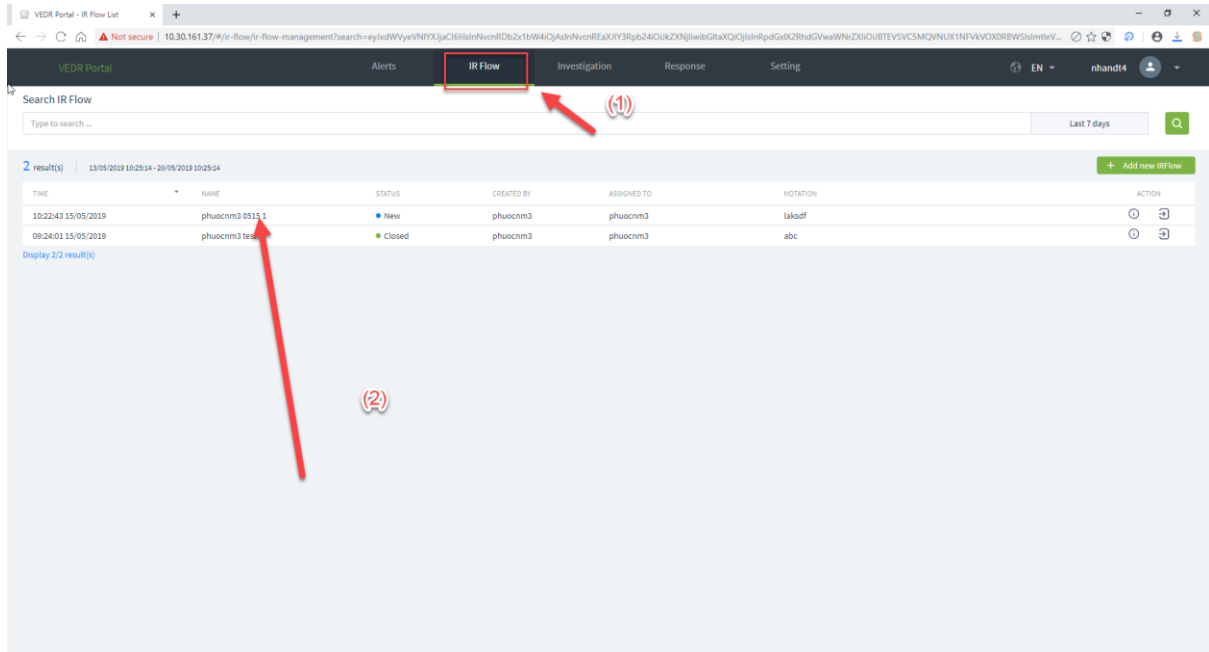
TIME	AGENT ID	OBJECT	FROM	REFERENCE
10:35:00 24/05/2019	B2A0360B8EEA76B1D5B71058700D4F4DE5E593E	DESKTOP-EGANUBQ\CHUYENNT2	WIN_EVENT_LOG	fpC1520B88fgfaypNjx0
10:35:00 24/05/2019	B2A0360B8EEA76B1D5B71058700D4F4DE5E593E	C:\Windows\System32\taskhostw.exe	WIN_EVENT_LOG	fpC1520B88fgfaypNjx0
14:21:57 24/05/2019	B2A0360B8EEA76B1D5B71058700D4F4DE5E593E	C:\Windows\System32\wbem\WmiPrivSE.exe	WIN_EVENT_LOG	hPC1600B88fgfayp-rm5

3.5.8. IRFlow – Response

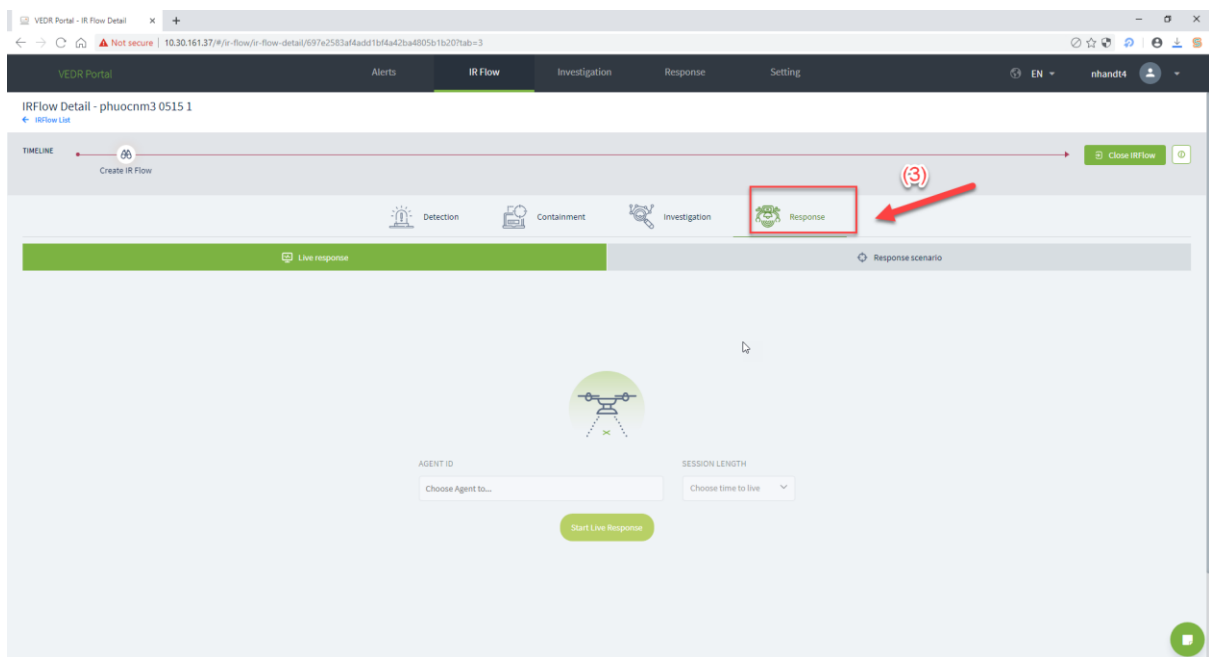
3.5.8.1 Live Response

- 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.

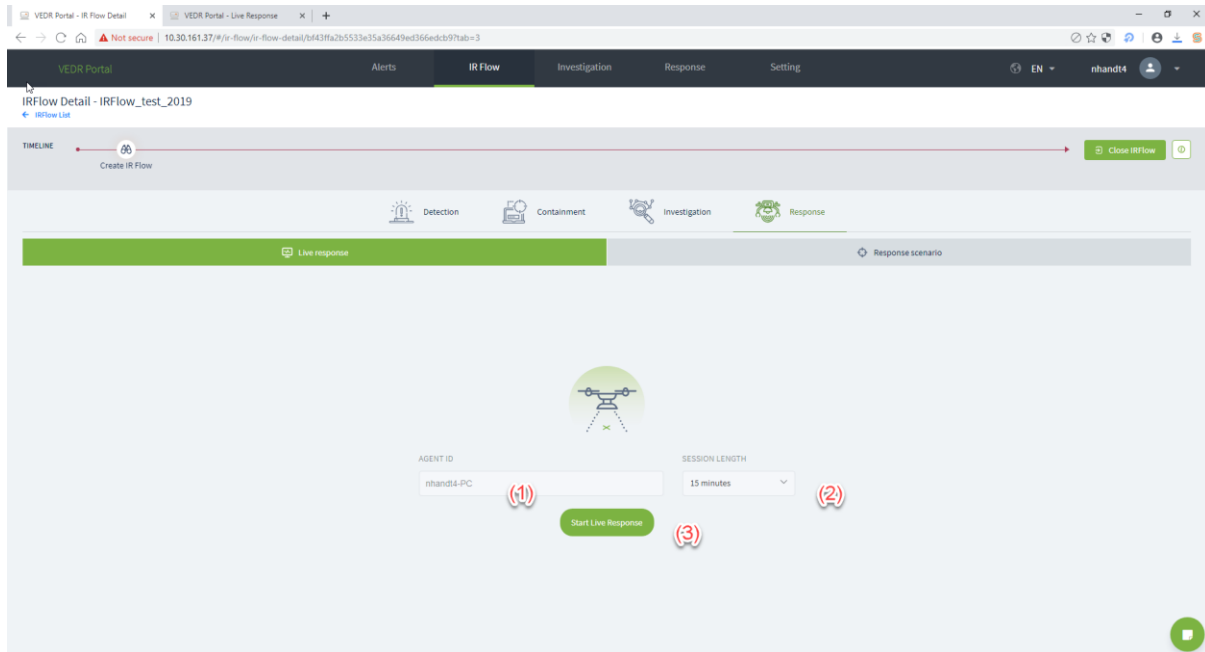
- Các bước thực hiện chức năng Live Response trong IRFlow:
- Bước 1: Click tab IRFlow
- Bước 2: Click duplicate vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Live Response)



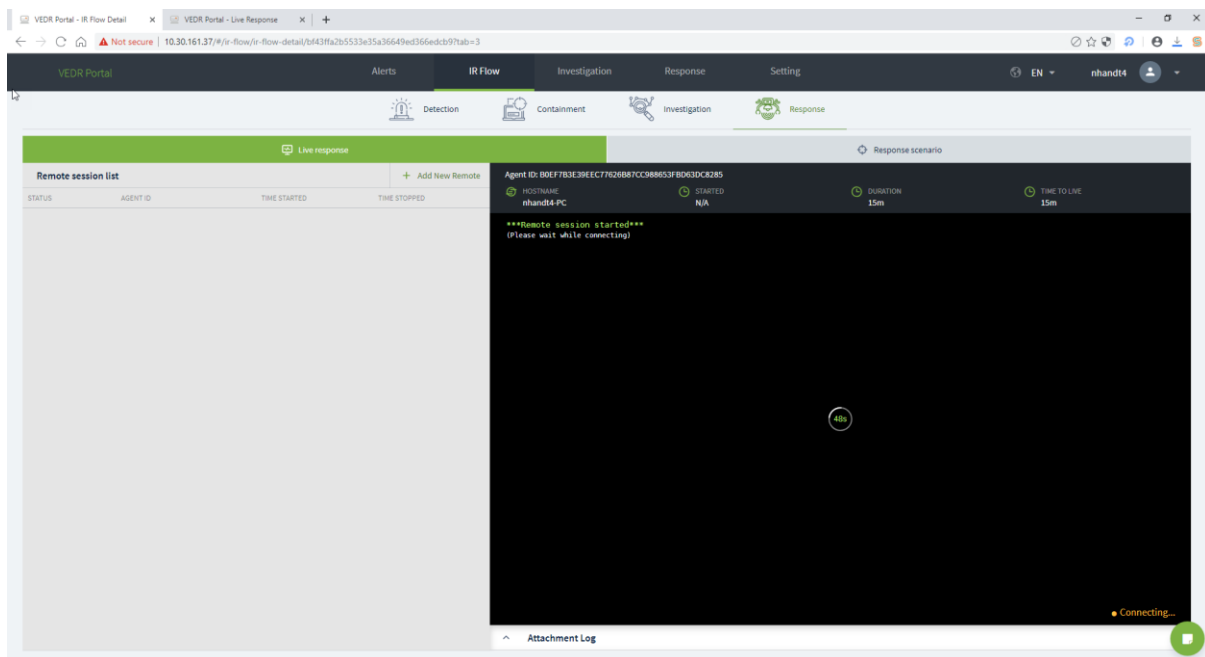
- Bước 3: Click tab con Response



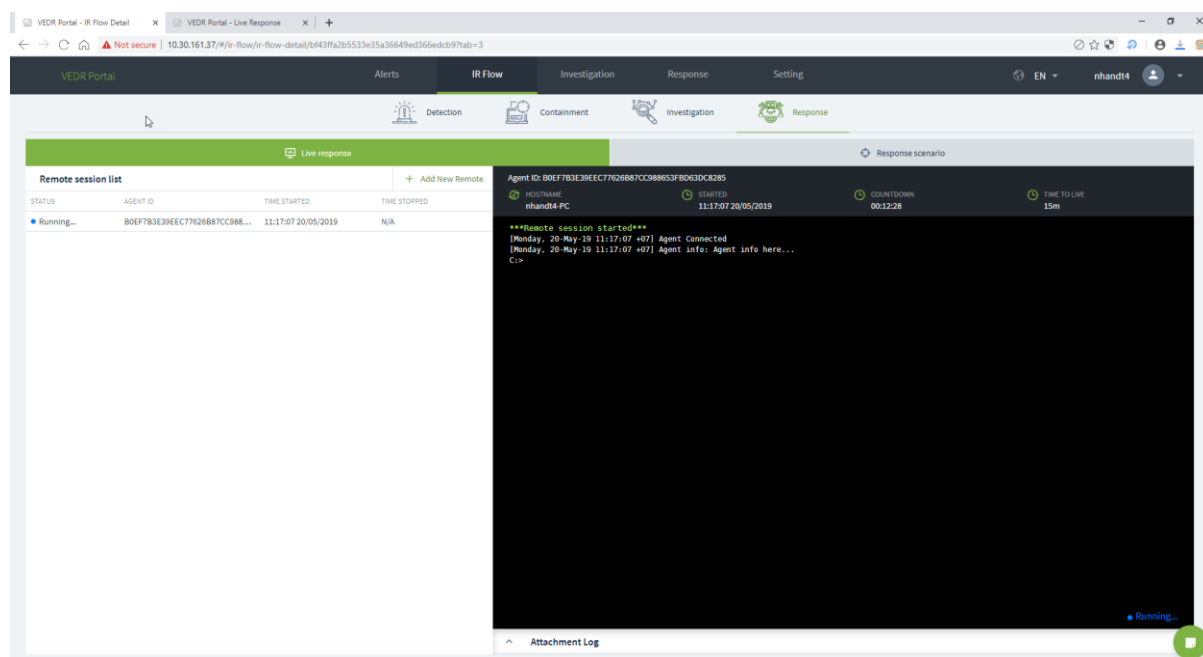
- Bước 4: Chọn Agent và khoảng thời gian cần thực hiện (5 phút/ 15 phút/ 1 giờ/ 3 giờ) Live Response và bấm nút “Start Live Response”.
- Danh sách Agent hiển thị trong combobox là tất cả các Agent hiển thị trong tab Detection



- 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”.
(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.



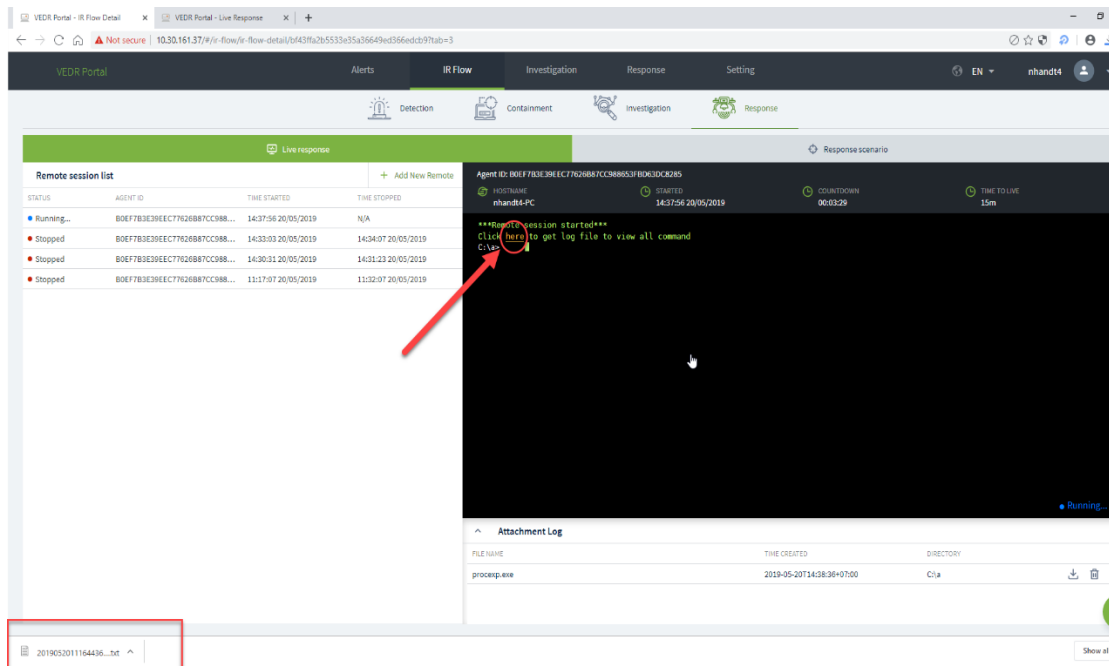
- Người dùng có thể thực hiện các lệnh tại màn hình console như sau:

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

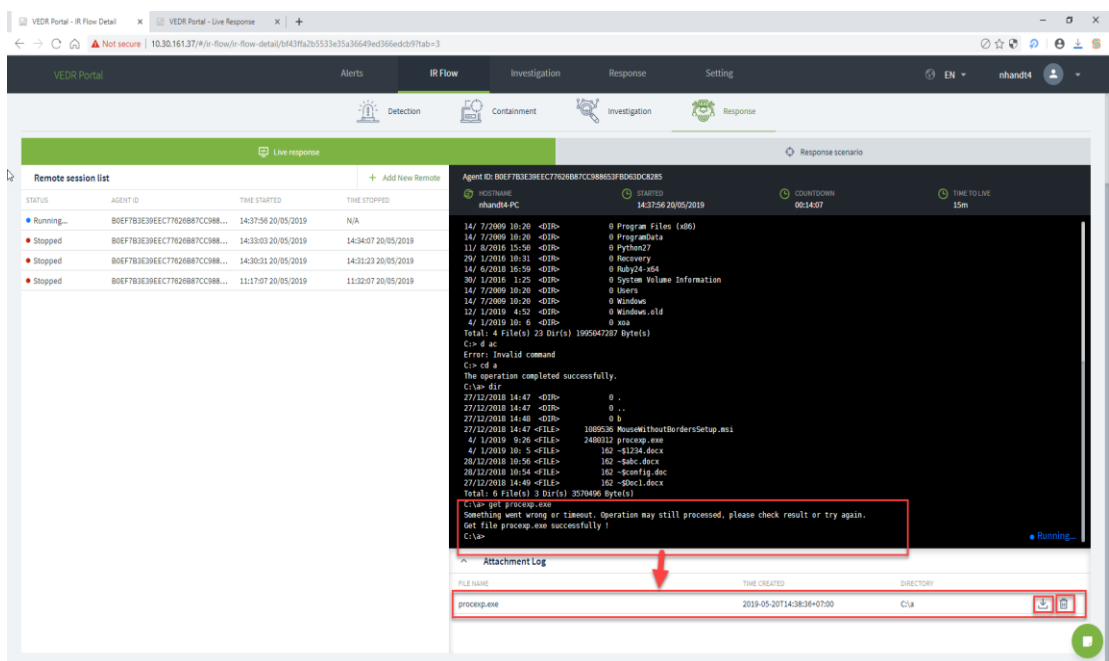
		delete -folder temp\axvers	
		delete -all <folderpath> ví dụ: delete -all c:\temp	Xóa tất cả các file/ thư mục con trong thư mục (nhưng không xóa thư mục)
6	viewfile	<filepath><sizeinbytes>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	get	<filepath>	Upload 1 file từ host lên server
8	put	<url><folderpath>	Download 1 file tới máy host
9	mkdir	<dir name>	Tạo 1 thư mục
10	reg		Các lệnh liên quan đến Registry
		query <keyname> -v <valuenam> ví dụ: reg -query "HKLM\Software\abc xyz" -v "run path"	Truy vấn dữ liệu value của 1 key
		query <keyname> -s ví dụ: reg -query "HKLM\Software\abc xyz" -s	Truy vấn tất cả các subkey và value và data
		add <keyname> ví dụ: reg -add "HKLM\software\abc xyz"	Thêm 1 key
		add <keyname> -v <valuenam> -t <type> -d <data> ví dụ: reg -add "HKLM\software\abc xyz" -v "run path" -t REG_SZ -d "c:\temp\bin.exe"	Thêm 1 value
		delete <keyname> ví dụ: reg -delete HKU\S-1-5-21-3791698801-2327923109-	Xóa 1 key và tất cả các subkey và value

		636705026-2080\Software\Test	
		delete <keyname> -v <valuenam>	Xóa 1 giá trị của key
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg
11	process		Các lệnh liên quan đến process
		-t <processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid>	Tạm dừng 1 tiến trình
		-r <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>	Liệt kê các process của 1 user
12	service		Các lệnh liên quan đến service
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename>	Start 1 service
		-stop <servicename>	Stop 1 service
13	user	-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
14	cls		Xóa màn hình console
15	help		Lệnh help

- 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 đây, bằng thao tác click vào link “here”

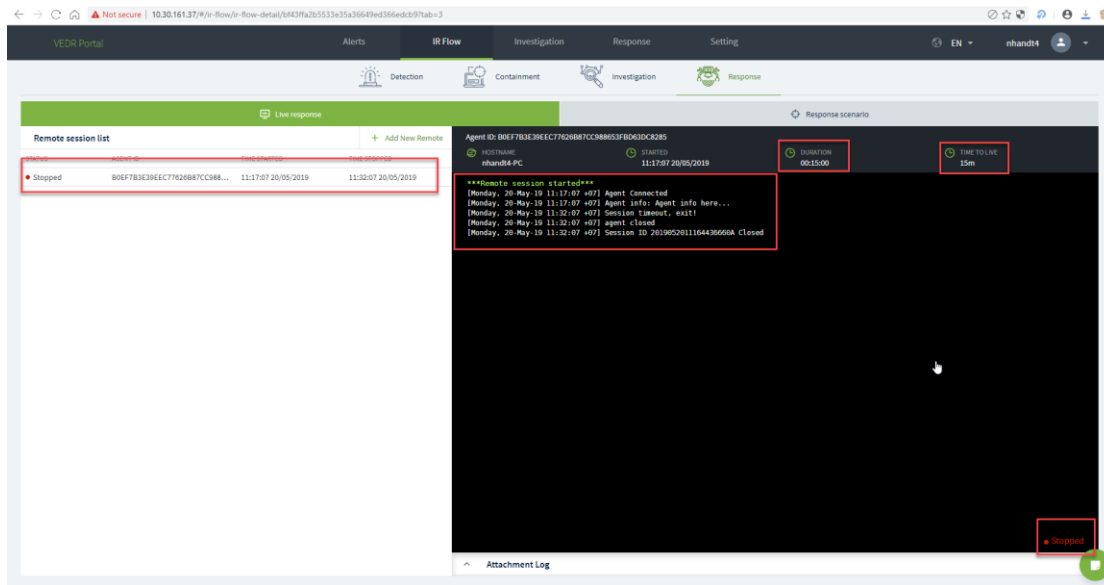


- Lệnh get <filepath>: ví dụ: get proccp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình Attachment Log ở phía dưới góc bên phải của màn hình. Người dùng được phép tải file về trình duyệt hoặc xóa file đã lấy về server.

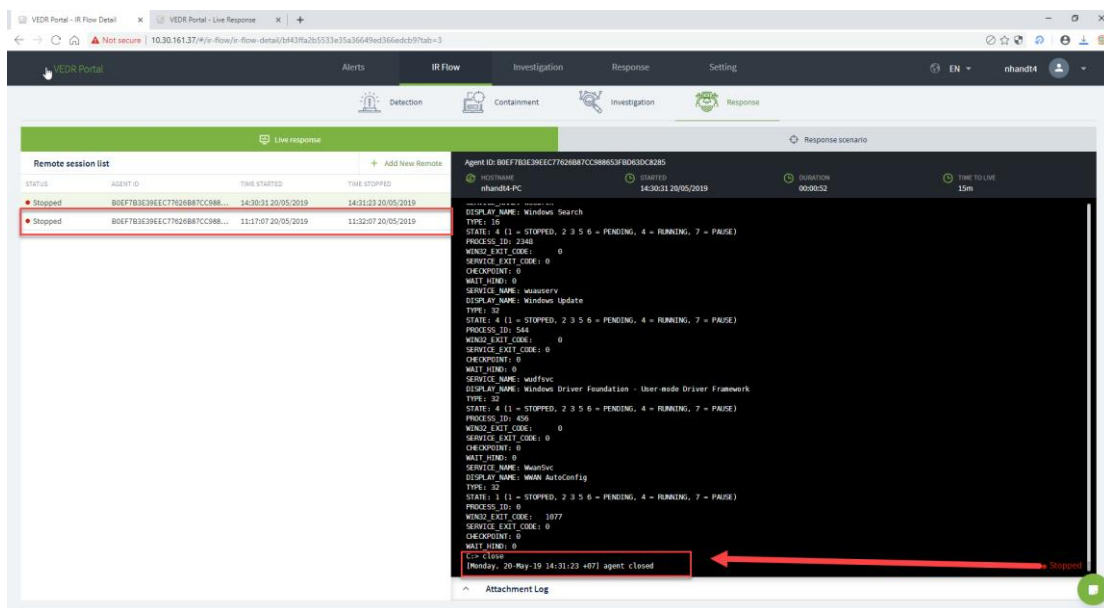


- Bước 6: Phiên làm việc của Live Response kết thúc khi:

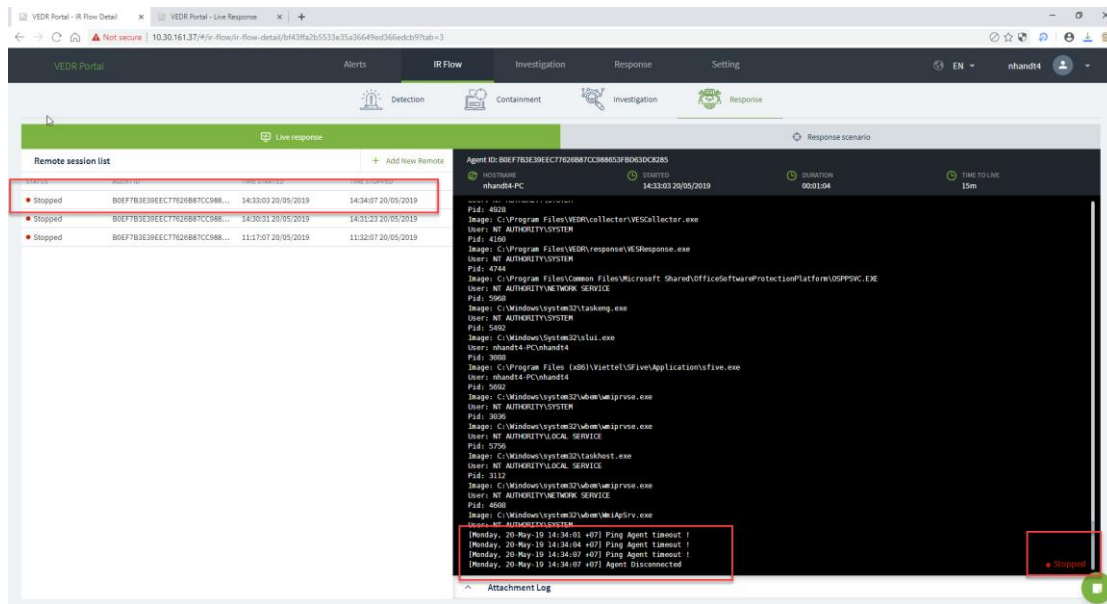
- Thời gian của phiên hết hiệu lực: Khi trường “Duration” bằng thời gian với trường “Time To Live”.



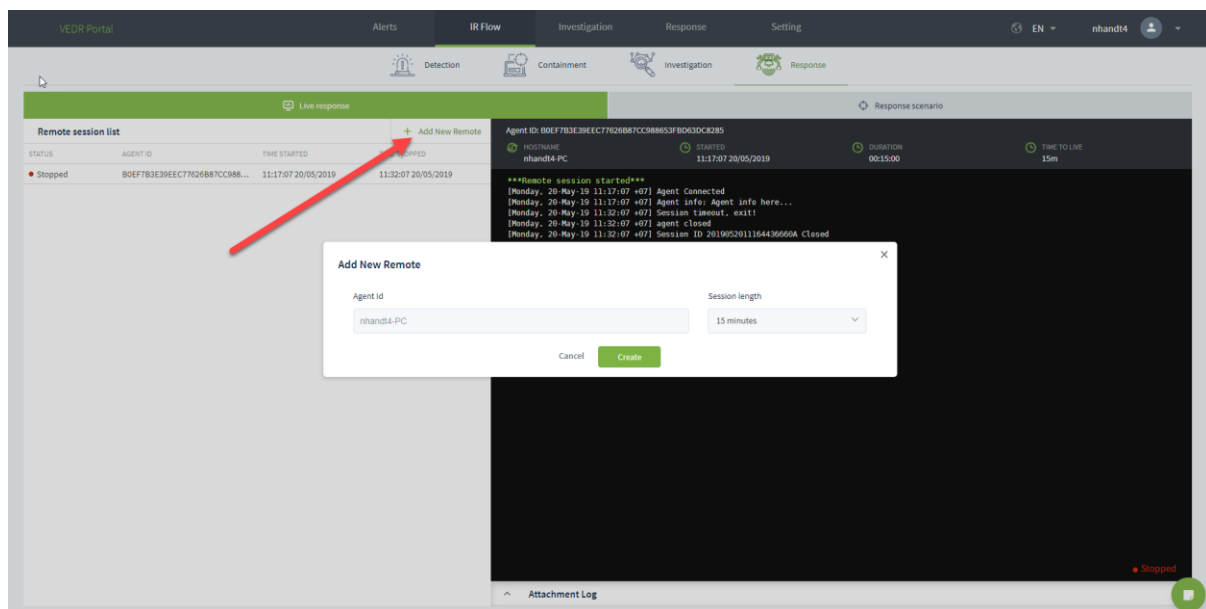
- Người dùng chủ động yêu cầu đóng kết nối bằng lệnh “close”.



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

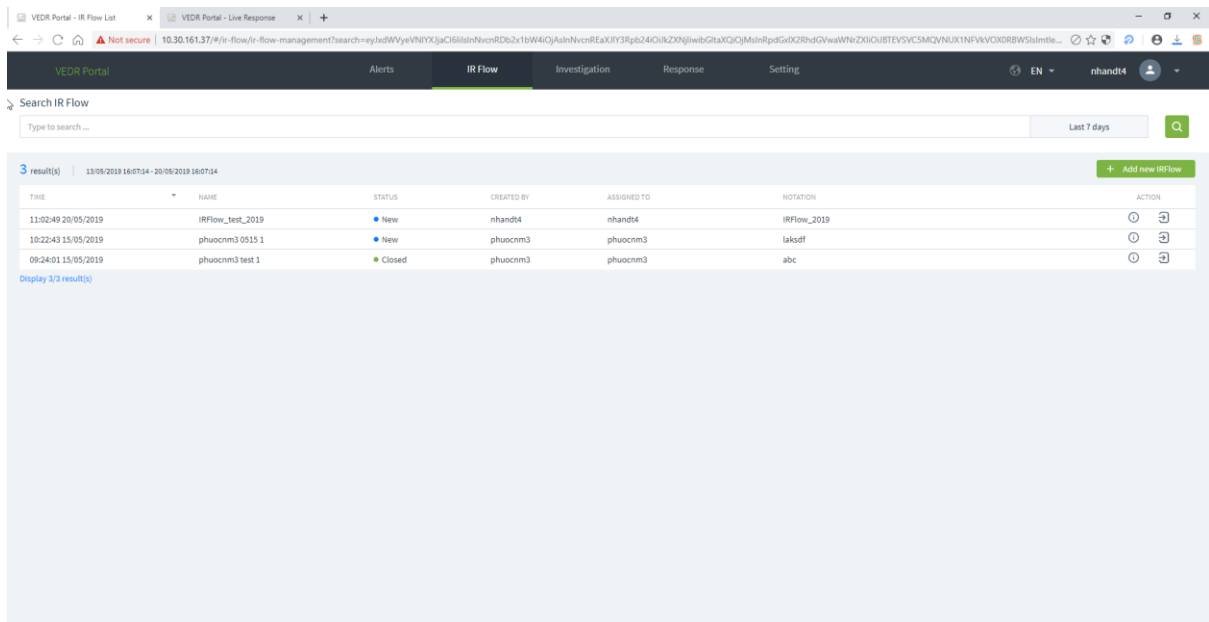


- Ngoài ra, người dùng có thể click nút “+ Add New Remote” để tạo 1 phiên live response mới:

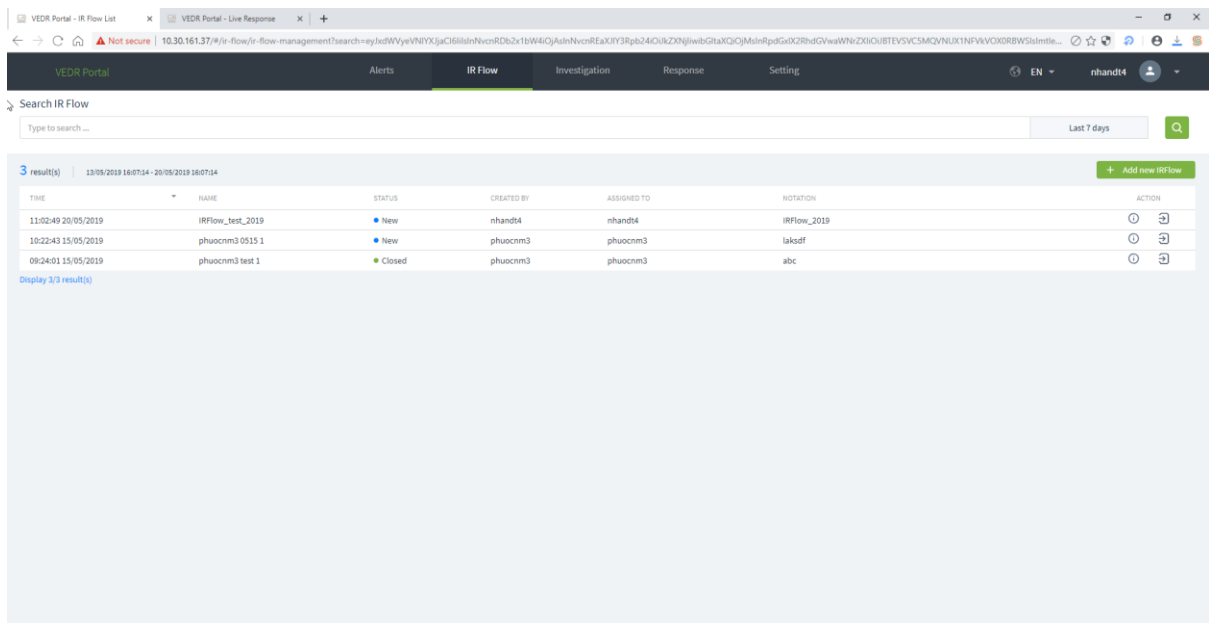


3.5.8.2 Response Scenario

- = 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



- 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:

Original detection

TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY
14:39:29 17/05/2019	unknown	nhand4-PC	Execution	High

Additional detection

TIME	AGENT ID	OBJECT	FROM	REFERENCE
14:38:53 24/05/2019	B0E7B3E39EEC77626887CC388653F8063DC8285	C:\Windows\regedit.exe	WIN_EVENT_LOG	UvC06G0889gfygzLk4
14:39:05 24/05/2019	B0E7B3E39EEC77626887CC388653F8063DC8285	C:\Windows\system32\SnippingTool.exe	WIN_EVENT_LOG	DPC56G0889gfygzLk4
14:42:40 24/05/2019	B0E7B3E39EEC77626887CC388653F8063DC8285	C:\Users\nhand4\AppData\Local\Temp\procepxp64.exe	WIN_EVENT_LOG	D_C56G0889gfygzLk4
17:24:51 24/05/2019	B0E7B3E39EEC77626887CC388653F8063DC8285	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{40344037-3505-4974-804E-75B040A56C0A}\DateLastConnected	WIN_EVENT_LOG	V_BC6W0889gfygzLk4

- **Bước 3: Click Response Tab >> Response Scenario**

Response scenario

1 Add action to artifact (Choose artifacts have same type to add action! Drag and Drop artifact in table to change position)

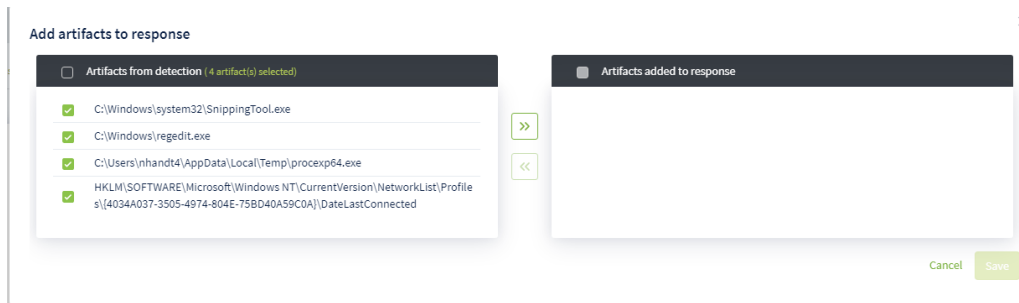
2 Deploy to agent

Agent list	Agent apply list
Choose ONLINE agent in list below and click => button to add to apply agent list	Click Deploy button to apply rule for agent list below

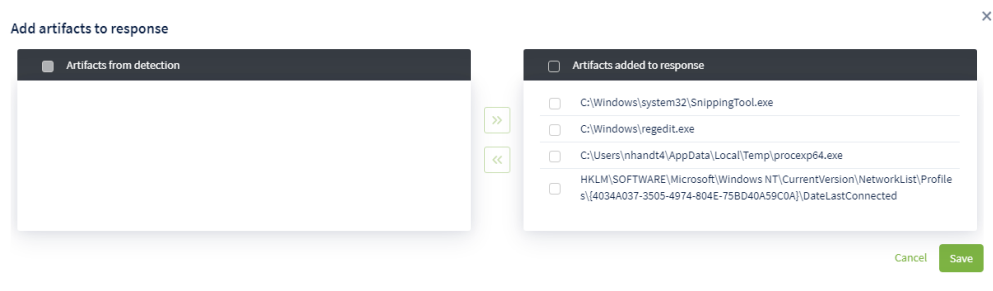
- **Bước 4: Thực hiện các cấu hình chi tiết:**

Add action to Artifact

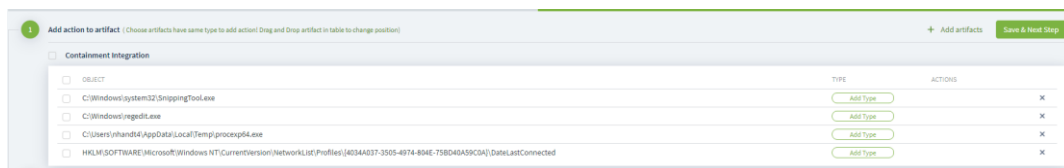
- Click button **Add artifacts from detection phase** để bắt đầu thêm artifacts vào kịch bản phản ứng.
- Danh sách Artifact hiển thị từ tab Detection



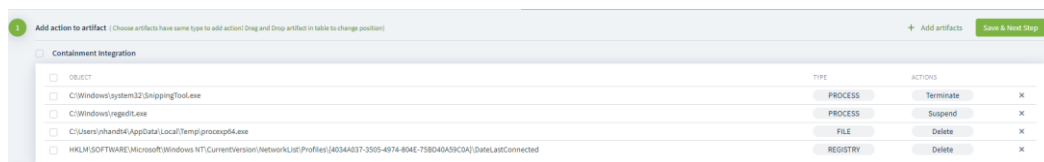
- Click button  để chuyển sang phần các artifact trong kịch bản phản ứng

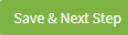
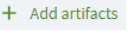


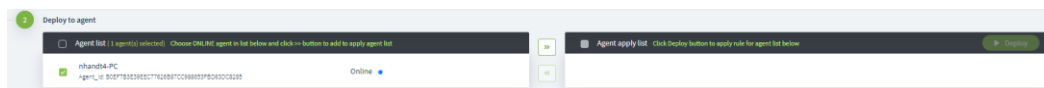
- Click Save để lưu lại danh sách Artifact đã chọn hoặc Cancel để hủy bỏ thao tác chọn trên.



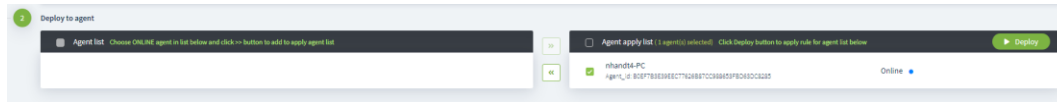
- Lựa chọn Type cho các Artifact. Hệ thống hỗ trợ gán từng type và action cho từng Artifact hoặc 1 type/action cho nhiều Artifact. Có 3 type: File, Process, Registry. Mỗi Type lại có 1 action riêng.



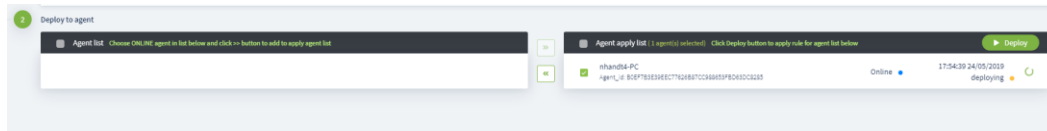
- Sau khi hoàn tất phần gán Type và Action, Click  để lưu và chuyển sang bước tiếp hoặc Click  để tiếp tục thêm Artifact.
- Deploy to Agent: Danh sách Agent được lấy từ tab Detection
- Tích chọn Agent đang online trong List Agent của IRFlow để thực hiện chuyển sang List các agent thực hiện kịch bản phản ứng



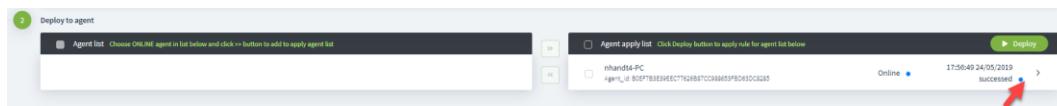
- Click  để chuyển sang List các agent có thể deploy
- Tích chọn Agent để Deploy



- Bấm nút Deploy
- Sau khi bấm nút Deploy, có các trạng thái:
- Deploying



- Succeeded



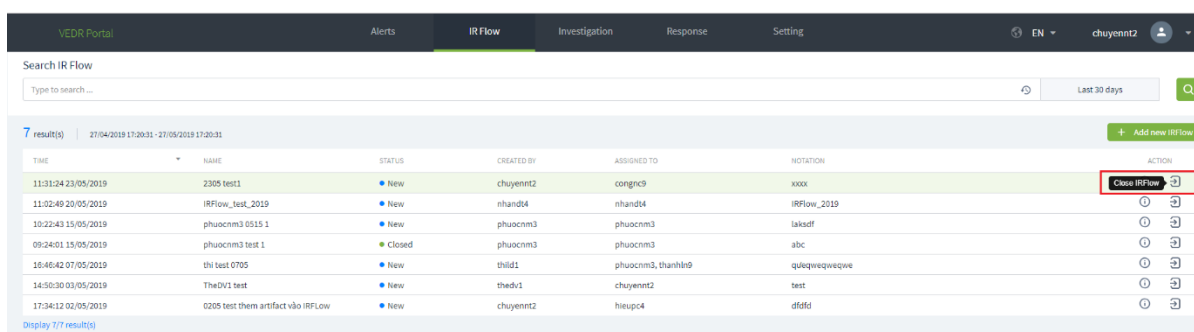
- Click vào chi tiết để xem kết quả triển khai kịch bản

Deploy result

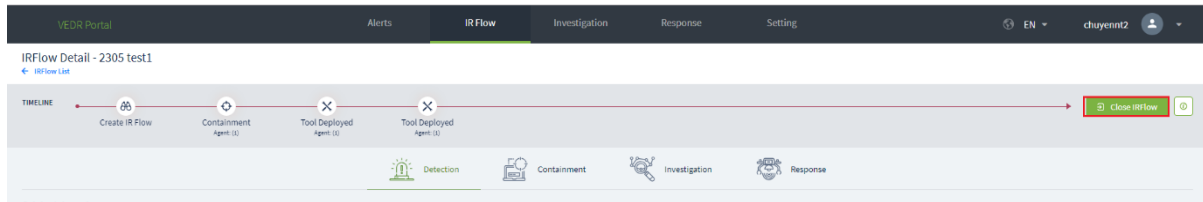
Object	Type	Action	Result
C:\Windows\system32\SnippingTool.exe	PROCESS	Terminate	successed
C:\Windows\regedit.exe	PROCESS	Suspend	Error: Incorrect function.
C:\Users\nhandt4\AppData\Local\Temp\procxp64.exe	FILE	Delete	Error: The request is not supported.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{4034A037-350...	REGISTRY	Delete	successed

3.5.9 Close IRFlow

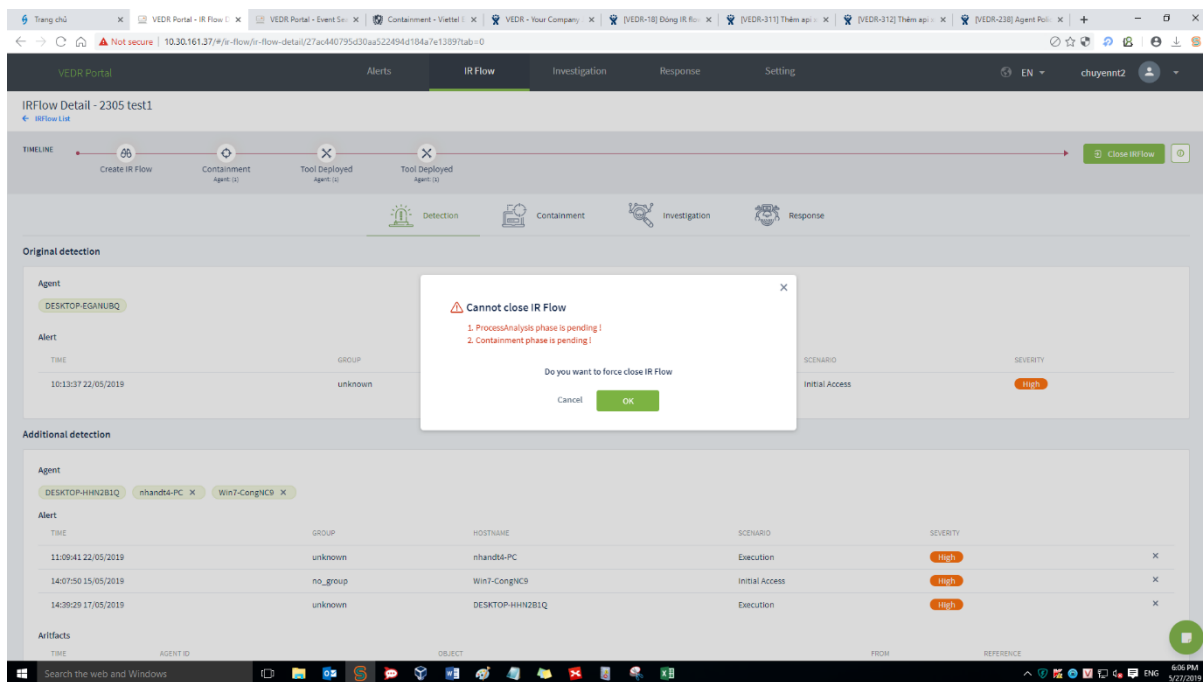
- Đóng IRFlow sau khi đã điều tra và xử lý xong
- Để thực hiện close IRFlow click “Close IRFlow” trên màn hình danh sách IRFlow



- Hoặc click “Close IRFlow” trên timeline ở bất cứ pha nào trong IRFlow: Detection, Containment, Investigation, 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



- 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.

The screenshot shows the 'IRFlow Detail - 2305 test1' page in the VEDR Portal. The interface includes a timeline at the top with steps: Create IR Flow, Containment Agent (x), Tool Deployed Agent (x), Tool Deployed Agent (x), and Close IR Flow. Below the timeline are tabs for Detection, Containment, Investigation, and Response. The 'Rule setting' section has two options: 'Network containment' (selected) and 'Process containment'. The 'Deploy to agent' section shows a table of agents and their status.

Agent list	Choose agent in list below and click mouse right button to add to apply agent list	Agent apply list	Click Start button to apply rule for list agent below
DESKTOP-HHNG8Q	no_group	NOT APPLIED	[Start]
agent_id: 80787626344038887384861207602634792			
chandu84_PC	no_group	NOT APPLIED	
agent_id: 80787626344038887384861207602634792			
DESKTOP-EGANUBQ	no_group	STOPPED	
agent_id: 80787626344038887384861207602634792			
Win7-CongVCS	no_group	NOT APPLIED	
agent_id: 80787626344038887384861207602634792			

The screenshot shows the 'IRFlow Detail - 2305 test1' page in the VEDR Portal. The timeline at the top shows the flow has reached the 'Close IR Flow' step. The 'Investigation' tab is active, displaying a message: 'IRFlow is closed'. Below the message, it says 'Go to Investigation Result to view data!'. The interface also includes tabs for Process Analysis, Event Search, Tools, and Investigation result.

IRFlow Detail - 2305 test1

Timeline: Create IR Flow → Containment Agent (1) → Tool Deployed Agent (1) → Tool Deployed Agent (1) → Close IR Flow

Investigation Result:

TIME	GET BY	STATUS	DOWNLOAD	ACTION
13:48 24/05/2019	Get Artifact Type: FILE Path: C:\Program Files\VEDR\VEDRService.exe	Expired		
11:52 24/05/2019	Tools Autotunc 13.82.0.0	Successful	Download	Info
10:49 24/05/2019	Get Artifact Type: FILE Path: C:\Windows\System32\BackgroundTaskHost.exe	Successful	Download	Info

Marked Artifact:

TIME	OBJECT	ACTION
10:35:00 24/05/2019	DESKTOP-EGANUBQ\CHUYENNT2	Added to IRFlow ✓
10:35:00 24/05/2019	C:\Windows\System32\taskhost.exe	Added to IRFlow ✓
14:21:57 24/05/2019	C:\Windows\System32\wbem\WmiPrvSE.exe	Added to IRFlow ✓
15:19:21 24/05/2019	C:\Program Files\VEDR\VEDRService.exe	Added to IRFlow ✓
17:12:26 24/05/2019	C:\Program Files\VEDR\VEDRConnectionManager.exe	Added to IRFlow ✓
17:12:26 24/05/2019	C:\Windows\system32\KERNEL32.DLL	Added to IRFlow ✓

3.6 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

3.6.1 Investigation Process Analysis

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

Process Analysis

Choose agent... [How to use this function?](#)

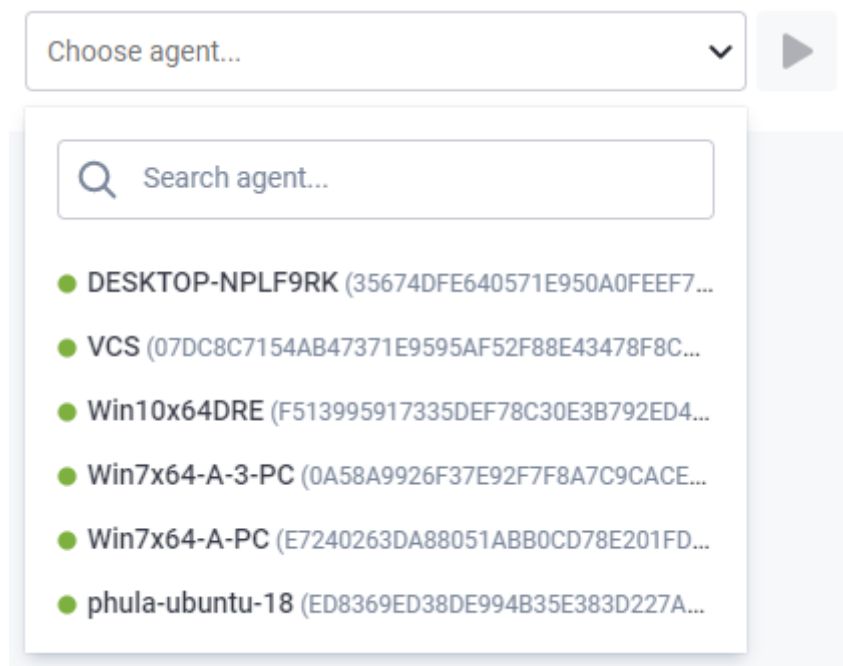
Search agent...

- DESKTOP-NPLF9RK (35674DF640571E950ADFEE7...
- VCS (70C8C7154A847371E955AF52F8BE43478FBC...
- Win10x64DRE (F513995917335DEF78C38E38702ED4...
- Win7x64-A-3-PC (0A58A926F37E92F7F8A7C9CADE...
- Win7x64-A-PC (E7240263DA88051ABB0C078E201FD...
- phala-ubuntu-18 (EDB369ED38DE94835E383D227A...

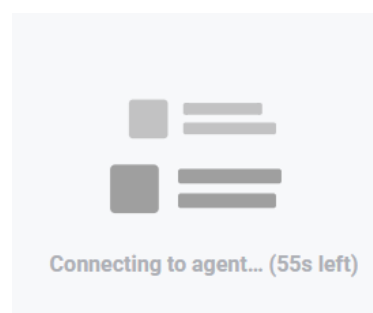
Choose an online agent for analyzing running processes, then click the beside green button to start.

- 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 bảo có thể kết nối, danh sách chỉ hiển thị các máy đang Online)



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



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

Process Analysis

Win7x64-A-3-PC How to use this function?

HOST NAME: Win7x64-A-3-PC (0A58A992F37E92F7F8A7C9CACE8FC3040C548FE) CONNECTED TIME: 27/10/2021 10:29:57 DURATION: 00:00:56 STATUS: Running

44 results | Last updated: 27/10/2021 10:30:02

Type to search... Refresh Verify signature Filter by signature Show columns

Name	PID	Path	User name	Command line	Signature	Action
smss.exe	300	C:\Windows\System32\smss.exe	SYSTEM	\SystemRoot\System32\smss.exe	N/A	
csrss.exe	376	C:\Windows\System32\csrss.exe	SYSTEM	%SystemRoot%\system32\csrss.exe Obj...	N/A	
wininit.exe	416	C:\Windows\System32\wininit.exe	SYSTEM	wininit.exe	N/A	
services.exe	516	C:\Windows\System32\services.exe	SYSTEM	C:\Windows\system32\services.exe	N/A	
svchost.exe	644	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\system32\svchost.exe -k Dco...	N/A	
unsecapp.exe	1620	C:\Windows\System32\wbem\unsecapp.e...	SYSTEM	C:\Windows\system32\wbem\unsecapp.e...	N/A	
prevhost.exe	3384	C:\Windows\System32\prevhost.exe	AnhNN	C:\Windows\system32\prevhost.exe [914...	N/A	
slui.exe	5952	C:\Windows\System32\slui.exe	AnhNN	C:\Windows\System32\slui.exe -Embedding	N/A	
WmiPrvSE.exe	12636	C:\Windows\System32\wbem\WmiPrvSE...	NETWORK SERVICE	C:\Windows\system32\wbem\wmiaprse.e...	N/A	
VBoxService.exe	704	C:\Windows\System32\VBoxService.exe	SYSTEM	C:\Windows\System32\VBoxService.exe	Oracle Corporation	
svchost.exe	772	C:\Windows\System32\svchost.exe	NETWORK SERVICE	C:\Windows\system32\svchost.exe -k RP...	N/A	
svchost.exe	832	C:\Windows\System32\svchost.exe	LOCAL SERVICE	C:\Windows\System32\svchost.exe -k Loc...	N/A	
svchost.exe	920	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\System32\svchost.exe -k Loc...	N/A	

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 thái 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

Refresh : 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)

Verify 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

Filter by signature

- ☒ Select all
- ☒ Verified
- ☒ Not verified
- ☒ Not available

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

CRYPTSP.dll	C:\Windows\system32\d0c2fbb6d97416b01... 7eab6c37f0a845e64...	Microsoft Corporation	Microsoft Windows
GDI32.dll	C:\Windows\system32\1084aa52ccc324ea5... 6e972cf624f7c0de81...	Microsoft Corporation	Microsoft Windows
IMM32.DLL	C:\Windows\system32\aa2c08ce85653b1a0... 83dfd0c119b20aadb...	Microsoft Corporation	Microsoft Windows
KERNELBASE.dll	C:\Windows\system32\da68c291b4ef2dec9c...21aa4779fc21e7621...	Microsoft Corporation	Microsoft Windows
LPK.dll	C:\Windows\system32\d202223587518b13d... 9db971b866d058adb...	Microsoft Corporation	Microsoft Windows
MSCTF.dll	C:\Windows\system32\c431eaf5caa1c82cac... addf850128dc675e6...	Microsoft Corporation	Microsoft Windows
NSI.dll	C:\Windows\system32\044fe45ff6ad40e3b... a1688a5e6e0f7037c...	Microsoft Corporation	Microsoft Windows
PerfCtrl.dll	C:\Program Files\Aija... a8a221af714077ec8... e11aec935d0a34766...	Viettel Corporation	Viettel Group
RPCRT4.dll	C:\Windows\system32\0611473c1ad9e2d99... 90afcc2a60350ece27...	Microsoft Corporation	Microsoft Windows
USER32.dll	C:\Windows\system32\fe70103391a64039a... f7d219d75037bc98f6...	Microsoft Corporation	Microsoft Windows
USP10.dll	C:\Windows\system32\2f8b1e3ee3545d3b5... 2a3ec01f3bafed7d6...	Microsoft Corporation	Microsoft Windows
VESSvc.exe	C:\Program Files\Aija... e381c58f04dae8f2a2... c6510091a2433f918f...	N/A	N/A
advapi32.dll	C:\Windows\system32\6df46d2bd74e3da1b... 2dc945f6f2c4a82189...	Microsoft Corporation	Microsoft Windows

- 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 ▼

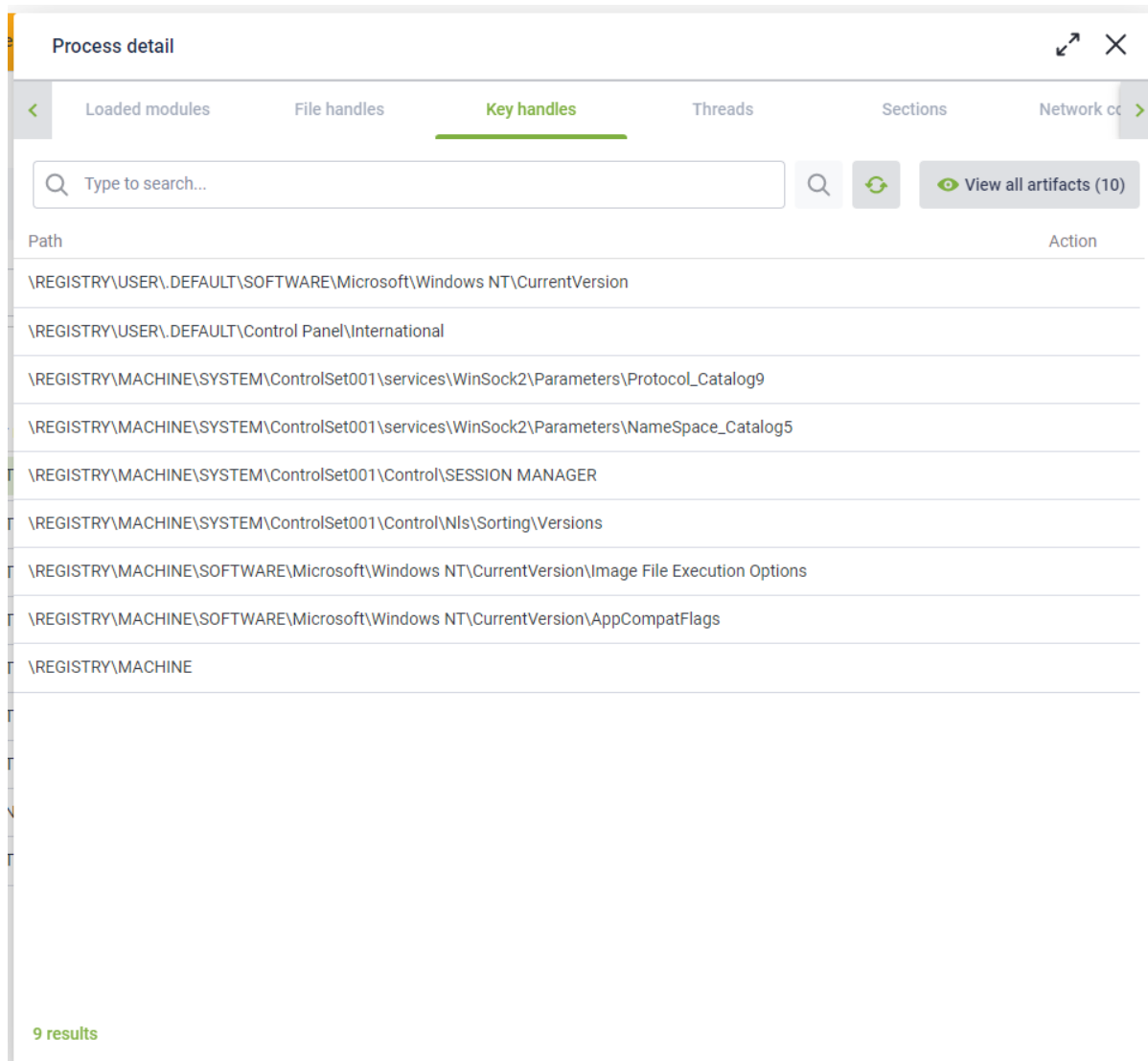
: Cho phép điều chỉnh trường hiển thị trên danh sách tiến trình. Trên danh sách ngoài trường “Name” luôn hiển thị cố định, các trường còn lại đều có thể tùy chọn hiển thị hoặc không hiển thị.

Show columns ▼

Select all

☒ Name
 ☒ PID
 ☒ Path
 ☒ User name
 ☒ Command line
 ☒ Signature
 ☐ Company name
 ☐ Product name
 ☐ File version
 ☐ Parent process path

- (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



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

Name	PID	Path	User name	Command line	Signature	Action
smss.exe	300	C:\Windows\System32\smss.exe	SYSTEM	\SystemRoot\System32\smss.exe	N/A	
csrss.exe	376	C:\Windows\System32\csrss.exe	SYSTEM	%SystemRoot%\system32\csrss.exe Obje...	N/A	
wininit.exe	416	C:\Windows\System32\wininit.exe	SYSTEM	wininit.exe	N/A	
services.exe	516	C:\Windows\System32\services.exe	SYSTEM	C:\Windows\system32\services.exe	N/A	
svchost.exe	644	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\system32\svchost.exe -k Dco...	N/A	
unsecapp.exe	1620	C:\Windows\System32\wbem\unsecapp.e...	SYSTEM	C:\Windows\system32\wbem\unsecapp.e...	N/A	
prehost.exe	3384	C:\Windows\System32\prehost.exe	AnhNN	C:\Windows\system32\prehost.exe (914...	N/A	
slui.exe	5952	C:\Windows\System32\slui.exe	AnhNN	C:\Windows\System32\slui.exe -Embedding	N/A	

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

Path	Action
\REGISTRY\USER\S-1-5-21-3949336984-4152371306-1276221334-1000_CLASSES	 Mark artifact
\REGISTRY\USER\S-1-5-21-3949336984-4152371306-1276221334-1000	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions	
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	
\REGISTRY\MACHINE	

Với mỗi đối tượng được chọn, lựa chọn “Mark with edit” – đánh dấu trực tiếp nội dung hiện tại

C:\Windows\system32\Dwm.exe	Mark without edit 
C:\Windows\System32\dwm.exe	
C:\Windows\System32\svchost.exe	

Hoặc người dùng có thể chỉnh sửa nội dung đối tượng trước khi đánh dấu

C:\Windows\system32\Dwm.exe	
C:\Windows\System32\dwm.exe	Edit and mark artifact  
C:\Windows\System32\svchost.exe	

- Sau khi đánh dấu, có thể xem lại danh sách bằng cách click

 View all artifacts (10)

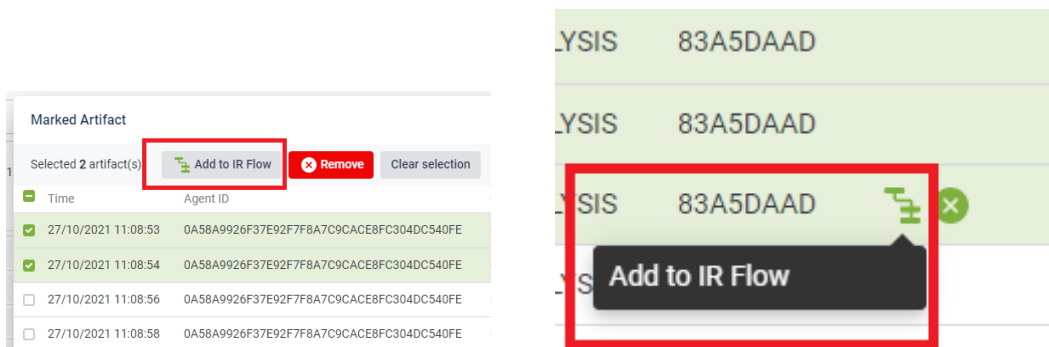
Lưu ý button này chỉ hiển thị khi có ít nhất 01 artifact được đánh dấu.

Marked Artifact						
☐	Time	Agent ID	Object	From	Reference	Action
☐	27/10/2021 11:08:53	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Windows\System32\services.exe	PROCESS_ANALYSIS	83A5DAAD	
☐	27/10/2021 11:08:54	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajjant\VESSvc.exe	PROCESS_ANALYSIS	83A5DAAD	
☐	27/10/2021 11:08:56	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajjant\autoscan\VESAuto...	PROCESS_ANALYSIS	83A5DAAD	
☐	27/10/2021 11:08:58	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajjant\VESUpdater.exe	PROCESS_ANALYSIS	83A5DAAD	
☐	27/10/2021 11:09:01	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajjant\propre\VESProPre...	PROCESS_ANALYSIS	83A5DAAD	
☐	27/10/2021 11:09:05	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajjant\propre\RI S\Securi...	PROCESS_ANALYSIS	83A5DAAD	

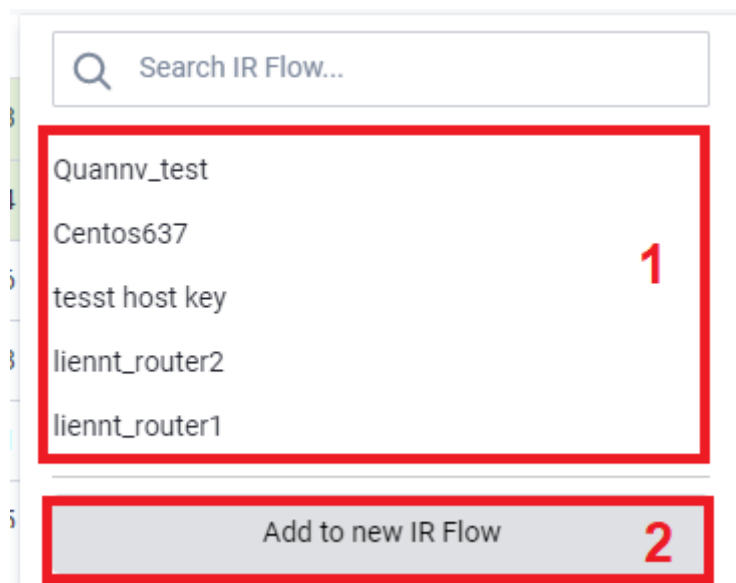
10 results

- **Bước 4: Thêm artifact vào IRFlow**

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”



- **Lựa chọn IRFlow đã tạo sẵn hoặc tạo mới IRFlow**



(1) 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 Flow

IR Flow name: Centos637

Assignee(s): root

Note (optional): - may that

List of artifacts

C:\Windows\System32\services.exe

C:\Program Files\Ajjant\VESSvc.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

Original detection

TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY
10:13:37 22/05/2019	unknown	DESKTOP-EGANUBQ	Initial Access	High

Additional detection

TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY
11:09:41 22/05/2019	unknown	nhand4-PC	Execution	High
14:07:50 15/05/2019	no_group	Win7-Conglic9	Initial Access	High
14:39:29 17/05/2019	unknown	DESKTOP-HHN2B1Q	Execution	High

Artifacts

TIME	AGENT ID	OBJECT	FROM	REFERENCE
10:35:00 24/05/2019	B2A0383088EEA76B1D5B7105B700D4F4DE5E593E	DESKTOP-EGANUBQ\CHUYENIT2	WIN_EVENT_LOG	IPC1520889fgyprk3d
10:35:00 24/05/2019	B2A0383088EEA76B1D5B7105B700D4F4DE5E593E	C:\Windows\System32\Taskhost.exe	WIN_EVENT_LOG	IPC1520889fgyprk3d
14:21:57 24/05/2019	B2A0383088EEA76B1D5B7105B700D4F4DE5E593E	C:\Windows\System32\wbem\WinPrtSE.exe	WIN_EVENT_LOG	HPC160889fgyprk3d
17:12:26 24/05/2019	B2A0383088EEA76B1D5B7105B700D4F4DE5E593E	C:\Program Files\VEDR\VESConnectionManager.exe	PROCESS_ANALYSIS	96202461
17:12:26 24/05/2019	B2A0383088EEA76B1D5B7105B700D4F4DE5E593E	C:\Windows\system32\KERNEL32.DLL	PROCESS_ANALYSIS	96202461

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?

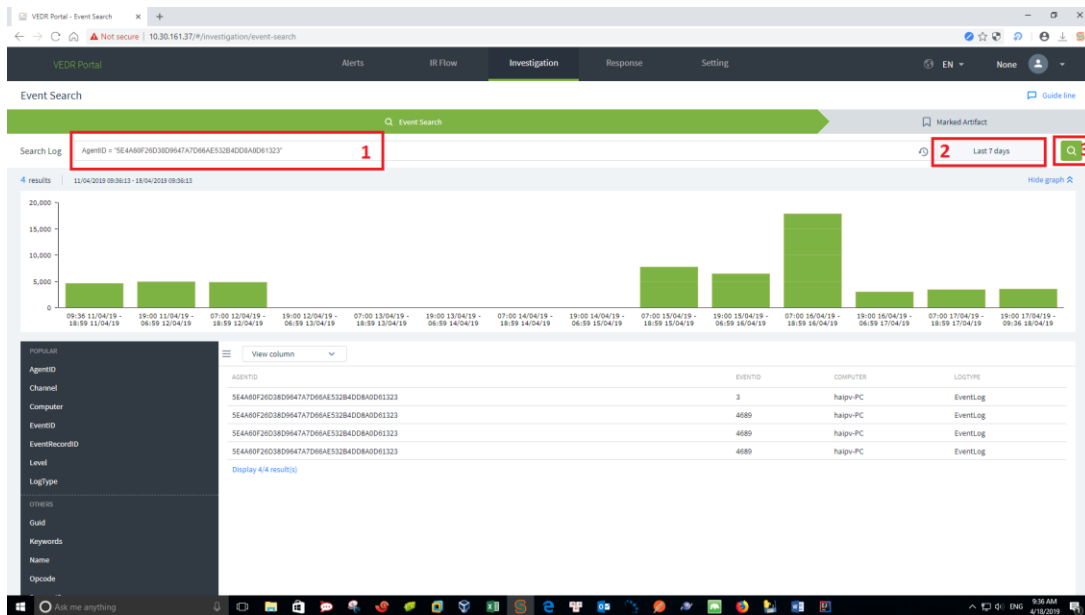
Changes you made may not be saved.



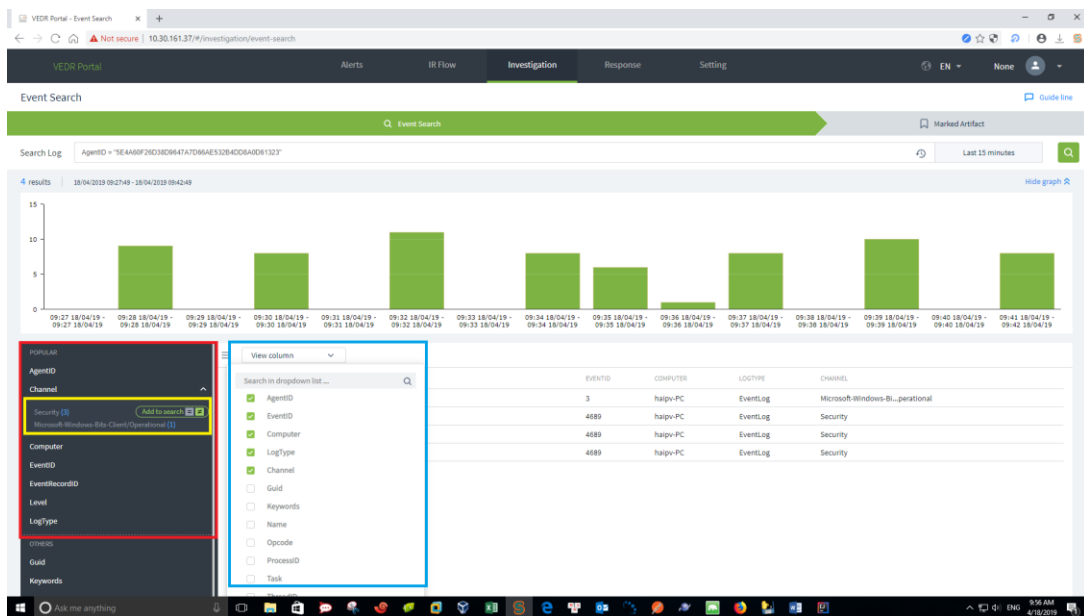
3.6.2 Investigation_Event Search

3.6.2.1 Tìm kiếm Event

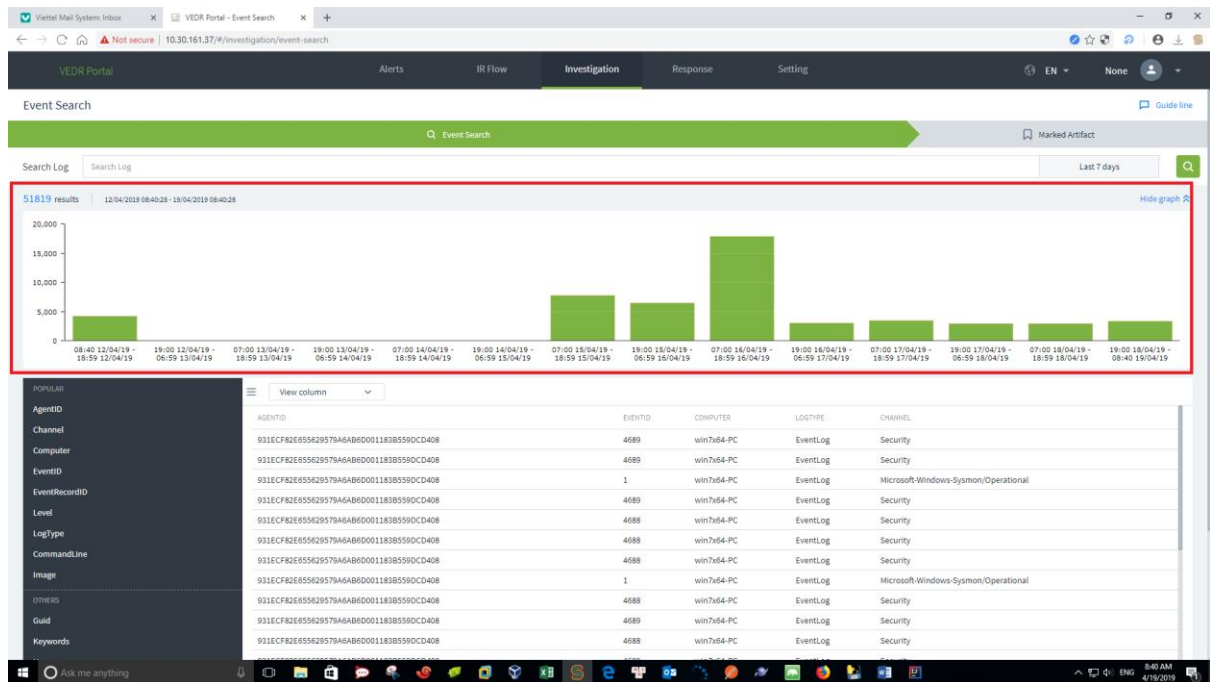
- Chức năng này tương tự trong Event Search của IRFlow:
- Bước 1: Nhập câu query > Chọn khoảng thời gian > Click Search



- Bước 2: Thêm các trường tìm kiếm vào câu query với trường Popular và Others



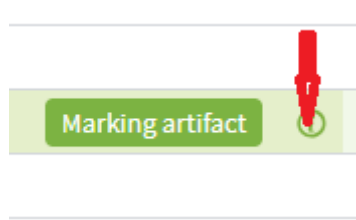
3.6.2.2 Biểu đồ



- Bước 1: Thực hiện tìm kiếm như phần Tìm kiếm event
- Bước 2: Biểu đồ hiển thị thống kê theo khoảng thời gian tìm kiếm. Cách phân chia các khoảng thời gian tương ứng với các cột trên biểu đồ như sau:
 - + Thống kê ≥ 90 ngày, chia 30 khoảng thống kê
 - + Thống kê events trong 60 ngày gần đây, thì chia thành 20 khoảng, mỗi khoảng thống kê số event trong 3 ngày
 - + Thống kê 30 ngày, chia 15 khoảng, mỗi khoảng 2 ngày
 - + Thống kê 7 ngày, chia 14 khoảng, mỗi khoảng 12 giờ
 - + Thống kê 1 ngày, chia thành 24 khoảng, mỗi khoảng 1 giờ
 - + Thống kê 12 giờ, chia 12 khoảng, mỗi khoảng 1 giờ
 - + Thống kê 6 giờ, chia 12 khoảng, mỗi khoảng 30 phút
 - + Thống kê 1 giờ, chia thành 12 khoảng, mỗi khoảng 5 phút
 - + Thống kê 30 phút, chia 15 khoảng, mỗi khoảng 2 phút
 - + Dưới 30 phút, chia thành các khoảng thời gian 1 phút
- Khi hover vào mỗi cột sẽ hiển thị Khoảng thời gian và số lượng bản ghi tìm kiếm được trong khoảng thời gian đó.
- Lưu ý: Các mốc thời gian trên chart là các thời điểm tính tròn theo ngày/giờ/phút cho phù hợp khoảng thời gian thống kê dài hay ngắn.

3.6.2.3 Xử lý Event

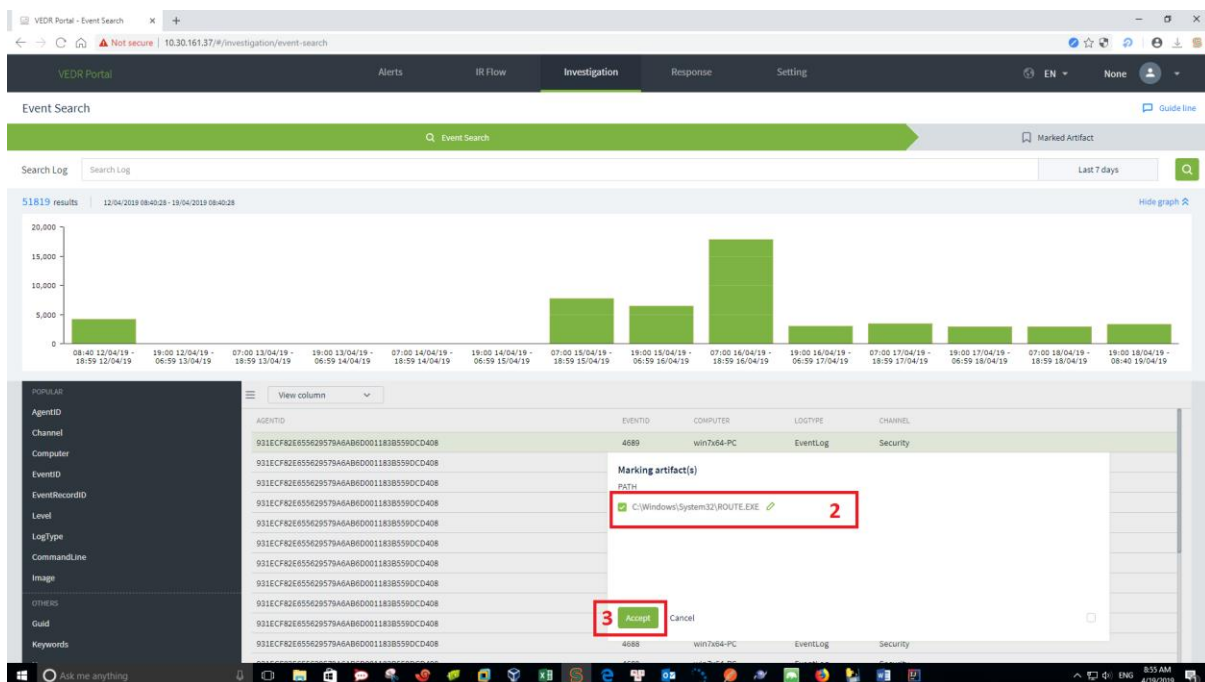
- Xem thông tin chi tiết event: click đúp vào 1 bản ghi hoặc hover vào 1 bản ghi và click icon Xem chi tiết



- Marking artifact: Hover vào 1 bản ghi và chọn “Marking artifact”

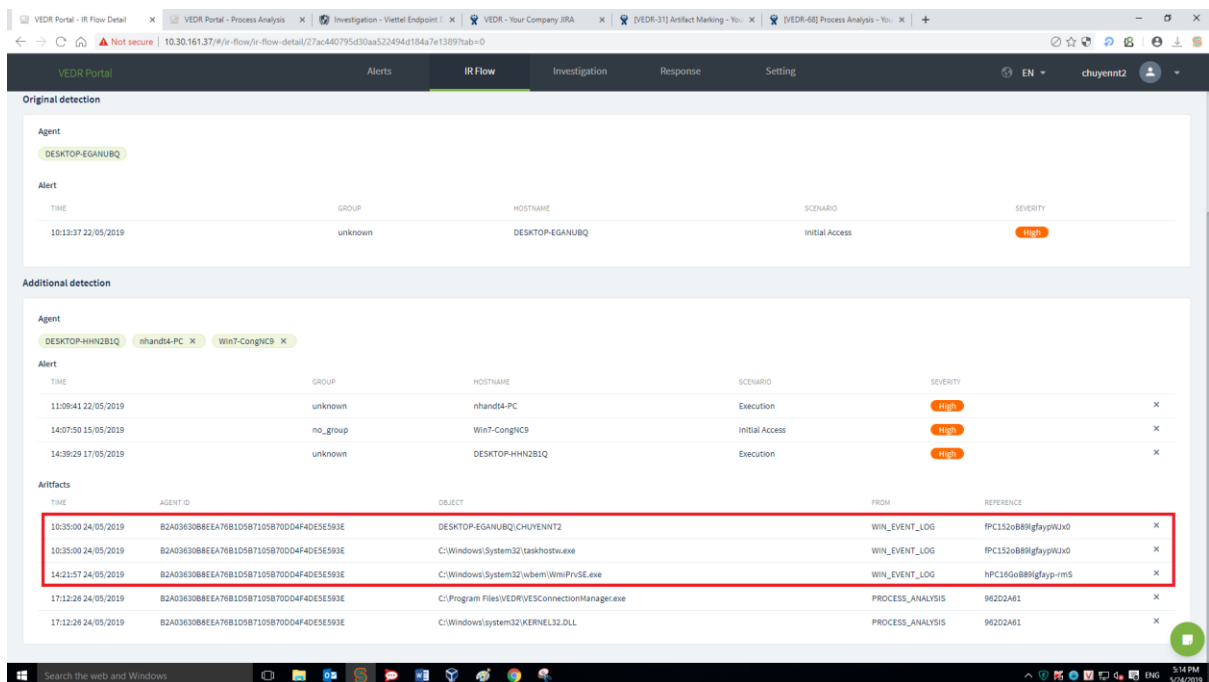
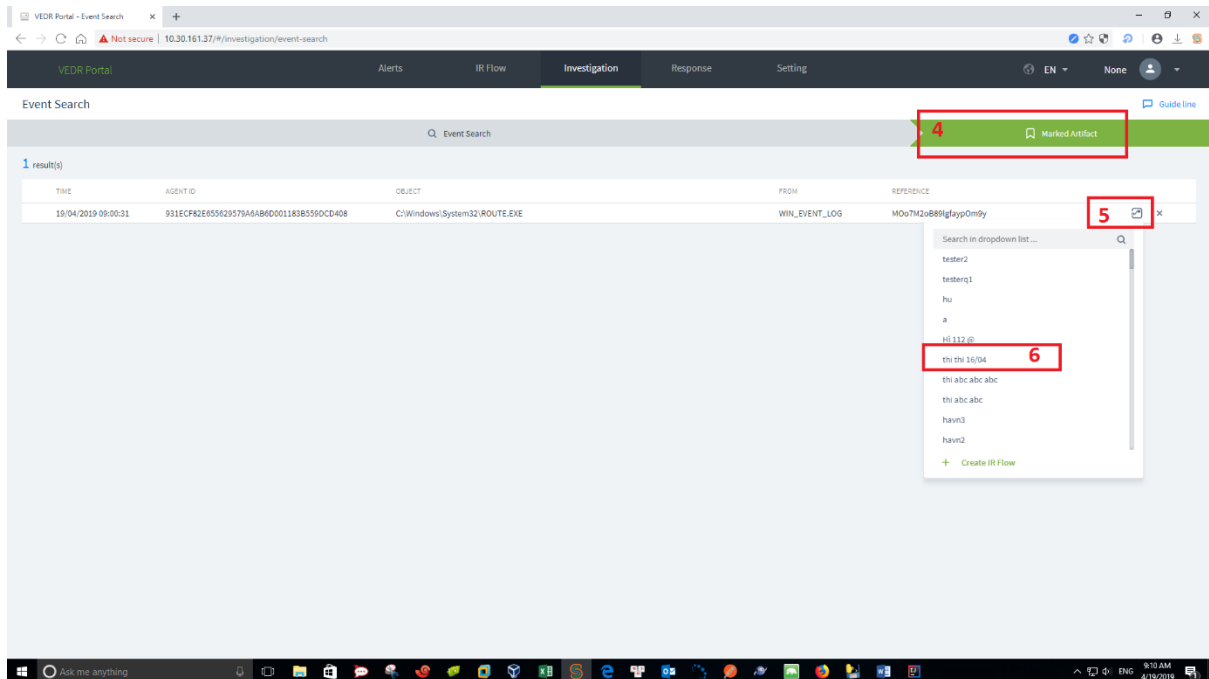


- Lựa chọn path và click “Accept”



Hình 2: Investigation/Event Search_Marking artifact

- Chọn IRFlow và add artifact đó vào Irfow



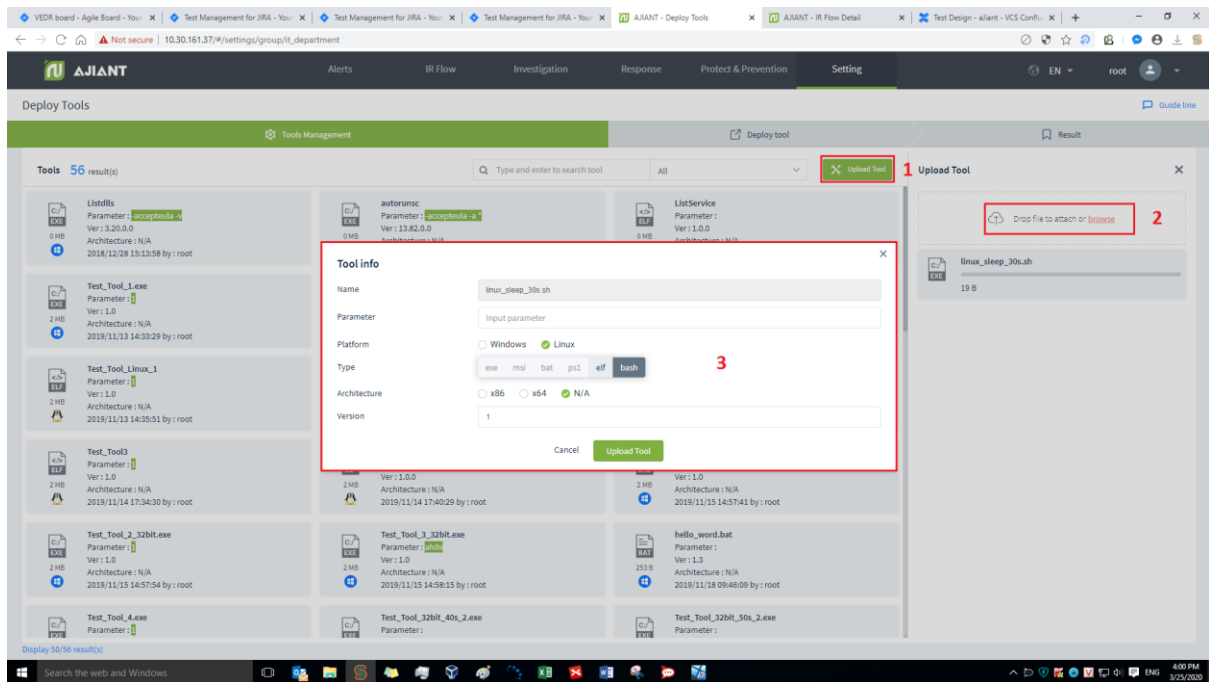
- Tương tự chức năng Process Analysis cũng có 1 số lưu ý:

- + Nếu thực hiện chuyển tab giữa Event Search và Marked artifact thì dữ liệu màn Marked artifact sẽ không bị mất đi
- + Nếu thực hiện chuyển sang tab lớn: Alert, IRFlow, Response, Setting thì dữ liệu màn Marked artifact sẽ bị mất đi

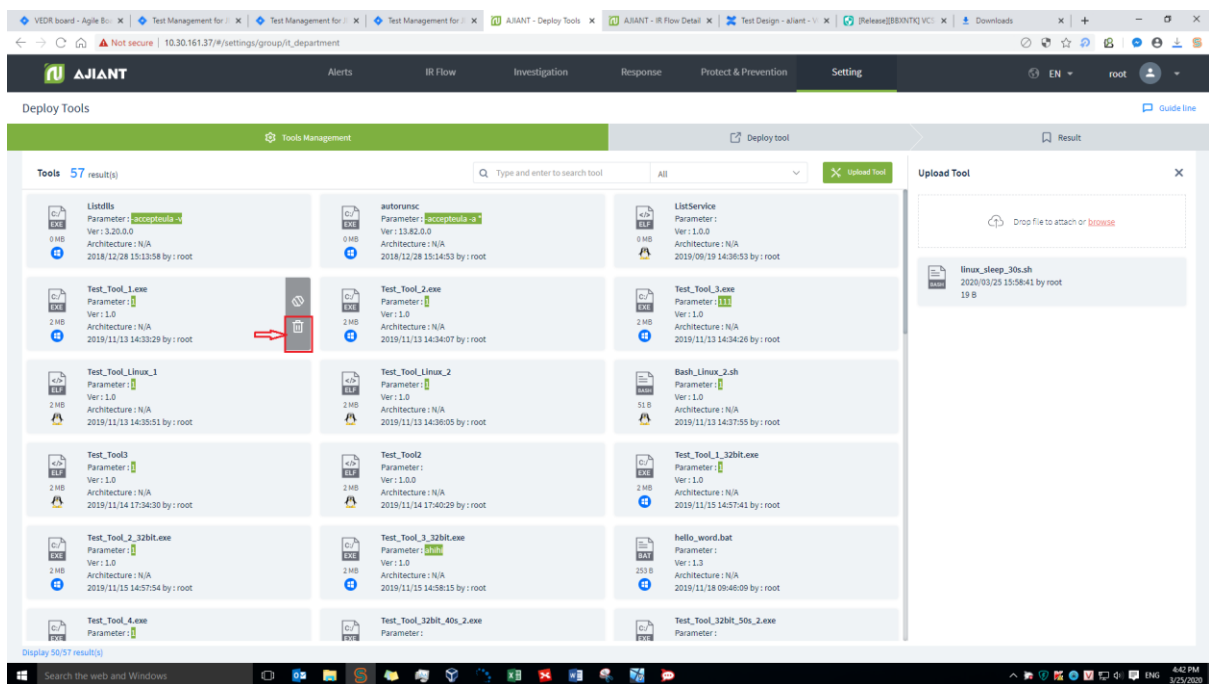
3.6.3 Investigation_Deploy Tools

3.6.3.1 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, mã Hash.
 - + Tìm kiếm tool: Tìm kiếm theo nhiều tiêu chí như All (toàn bộ các trường dữ liệu), theo Name (tên tool), Tool ID, Version, SHA1, Upload User, Platform.
 - + Upload tool: upload tool chạy trên agent Windows và Linux có dung lượng tối đa 10MB
- Xóa tool
- 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"



- Với tính năng xóa tool, hover chuột vào tool cần xóa > chọn Delete

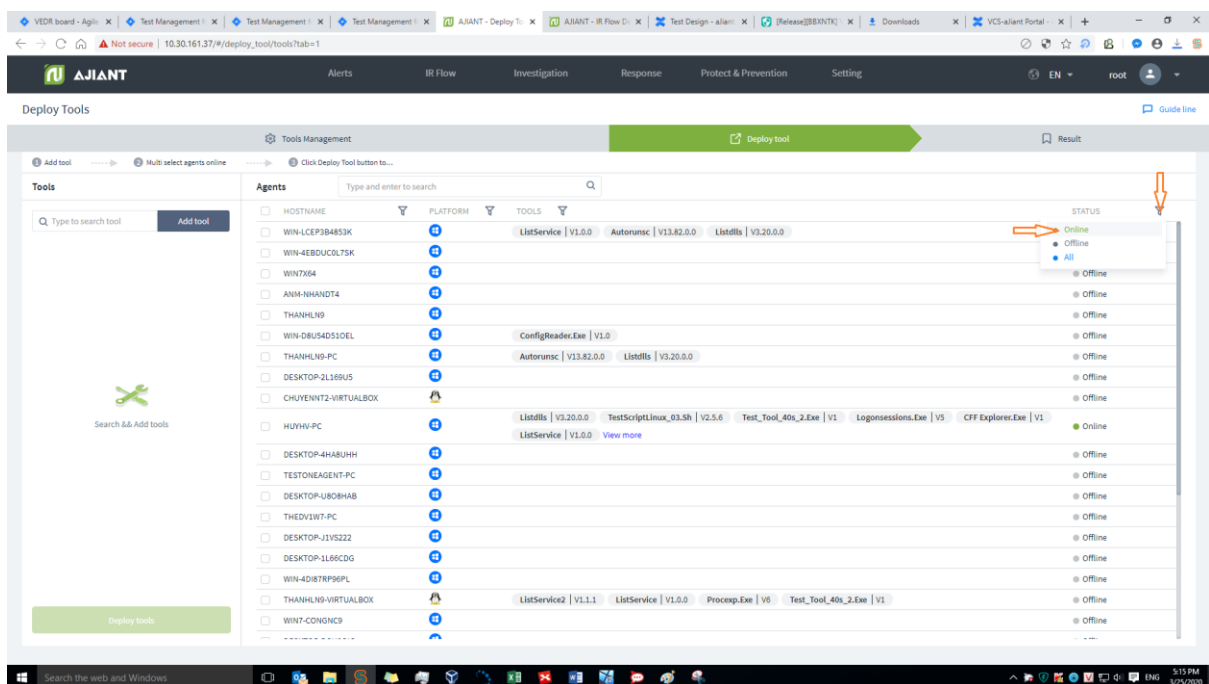


3.6.3.2 Deploy tool

- Các thao tác tương tự chức năng Deploy tool trong IRFlow ở mục 3.4.4.3

Tuy nhiên có 1 số điểm khác như sau:

- + 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
- Có thể lọc các agent đang online sau đó tìm kiếm agent



- Sau khi lựa chọn tool và agent để deploy kiểm tra kết quả trên tab Result. Ở màn hình này cũng có thể xem kết quả chạy tool dưới agent hoặc download được kết quả về máy local tương tự giống trong IRFlow

The screenshot displays the AJIANT web interface for managing and deploying tools. The top navigation bar includes tabs for VEDR, Test Management, and ASANT. The main content area is titled "Deploy Tools" and features a "Tools Management" section on the left and an "Agents" table on the right.

Tools Management: This section includes a search bar and a list of tools categorized by Windows and Linux. The "Tools" list shows the following tools:

- Windows:**
 - autornunc (V1.0.0.0) (Path: %SystemRoot%\System32\cmd.exe)
- Linux:**
 - Test_Tool_Linux_03.Sh (V2.5.6)
 - Test_Tool_40s_2.Exe (V1)
 - Logonsessions.Exe (V5)
 - CFF Explorer.Exe (V1)

Agents: This table lists various agents with their status and associated tools. The agents are:

- HOSTNAME:** Listfile (V3.20.0.0), TestScriptLinux_03.Sh (V2.5.6), Test_Tool_40s_2.Exe (V1), Logonsessions.Exe (V5), CFF Explorer.Exe (V1). Status: Online.
- HUWV-PC:** ListService (V1.0.0), View more. Status: Online.
- WIN7-32BIT-PC:** Autornunc (V13.82.0.0), Test_Tool_40s_2.Exe (V1), ListService (V1.0.0), Proccexp.Exe (V6), Test_Tool_Linux_1 (V1.0), View more. Status: Online.
- THANHLN-PC:** Autornunc (V13.82.0.0), Proccexp.Exe (V6), Test_Tool_40s_2.Exe (V1), ListService (V1.0.0), ConfigReader.Exe (V1.0), View more. Status: Online.
- THLD1-PC:** Listfile (V3.20.0.0), View more, Test_Tool_40s_2.Exe (V1), Listfile (V3.20.0.0), ListService (V1.0.0). Status: Online.

A green button at the bottom right indicates "Deploy tool successfully!".

AJIAN.T

Tools Management | Deploy tool | Result

Deploy Tools

Tools Result **279** result(s)

TIME	Platform	Agent ID	Hostname	Status	ACTION
17:15 25/03/2020		8BBCD23F7D18B816E4B13E549126E02443BF070F	Win7-32bit-PC	● Success	
▼	Autorunsc	Agents (1) Success (1/1)			
▼	Autorunsc	Agents (1) Success (1/1)			
▼	ListService	Agents (1) Success (0/1)			
▼	Autorunsc	Agents (1) Success (1/1)			
▼	Autorunsc	Agents (1) Success (1/1)			
▼	ListService	Agents (1) Success (0/1)			
▼	Autorunsc	Agents (1) Success (1/1)			
▼	Autorunsc	Agents (1) Success (1/1)			
▼	Autorunsc	Agents (1) Success (1/1)			
▼	Test_Tool_40s_3.Exe	Agents (1) Success (1/1)			
▼	Sleep_10s_linux.Sh	Agents (1) Success (0/1)			

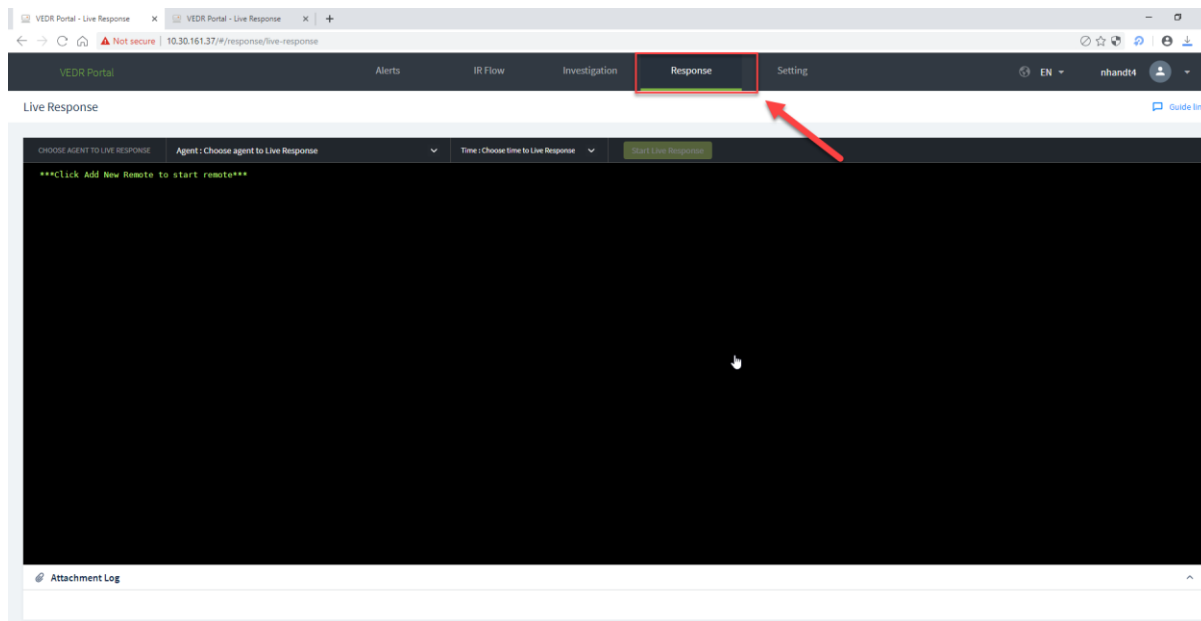
Display 15/279 result(s)

« < 1 2 3 4 5 6 7 8 ... 19 > »

3.7 Màn hình Response

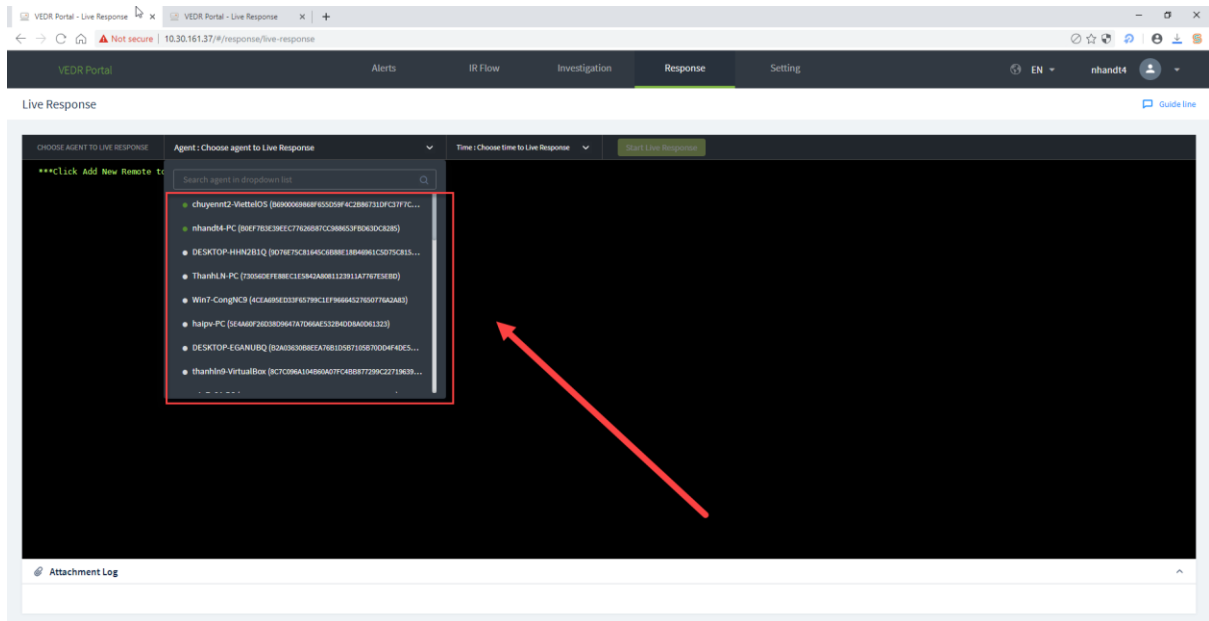
3.7.1 Response_Live Response

- 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

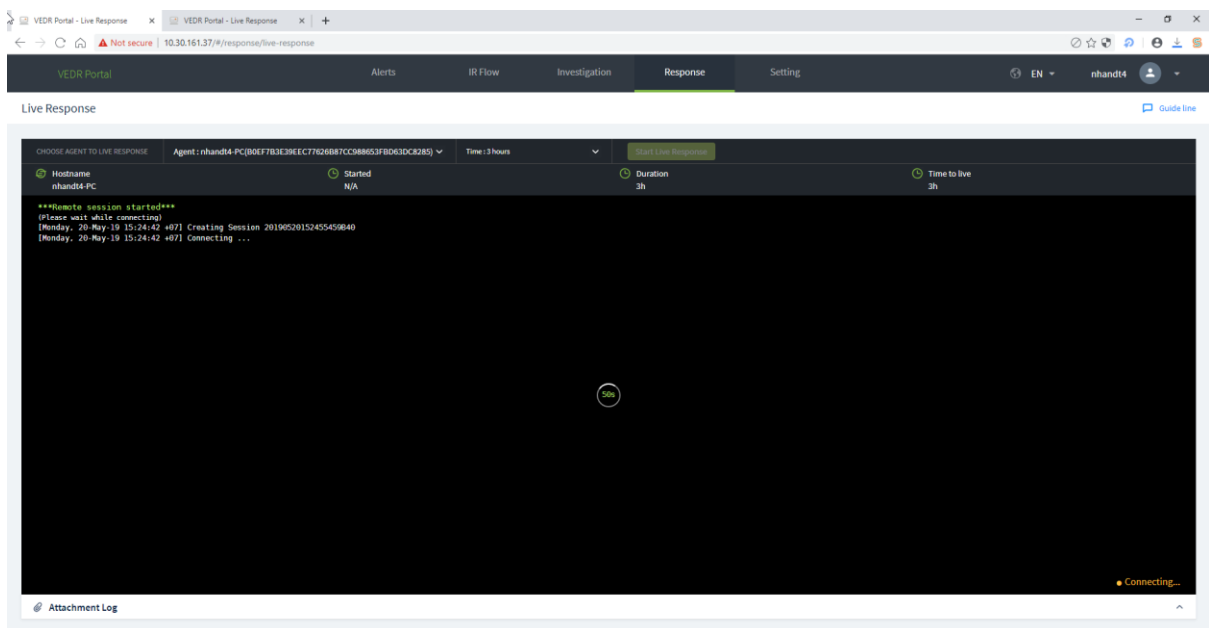


- Bước 2: Thực hiện tạo mới 1 phiên live response
- Chọn Agent: Hiển thị danh sách các agent:
 - + User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày
 - + User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default
 - + User đăng nhập thuộc group 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 (●).
- + Chọn Time: có các khoảng thời gian 5 phút, 15 phút, 1 giờ, 3 giờ.

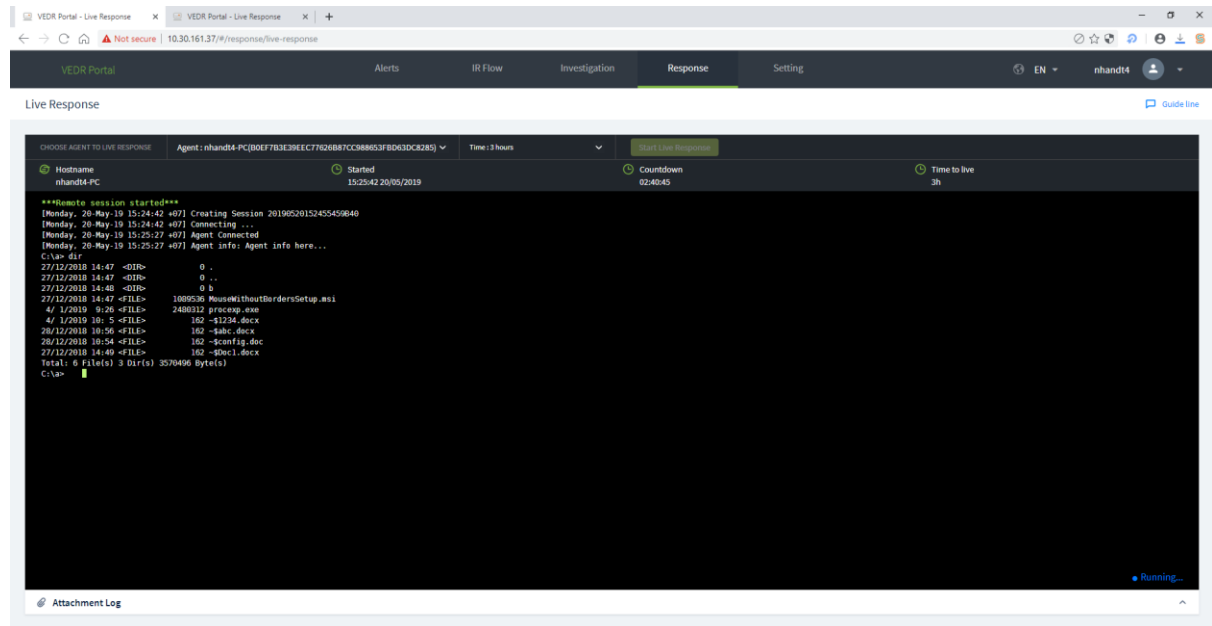
+ Click nút “Start Live Response”



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



-
- 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.

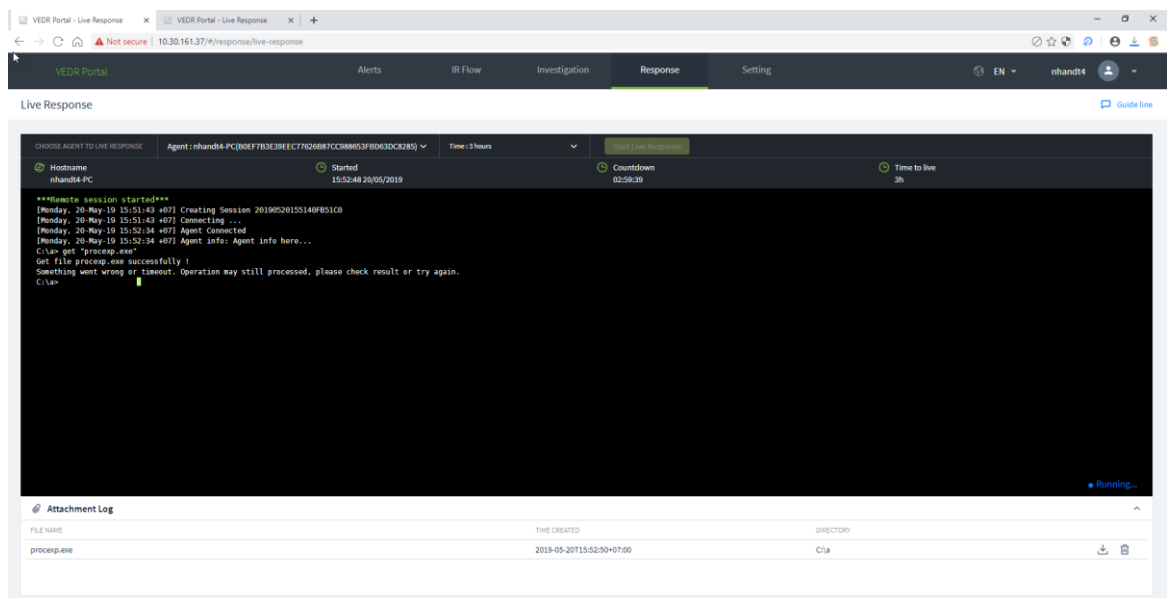


- Người dùng có thể thực hiện các lệnh tại màn hình console như sau:

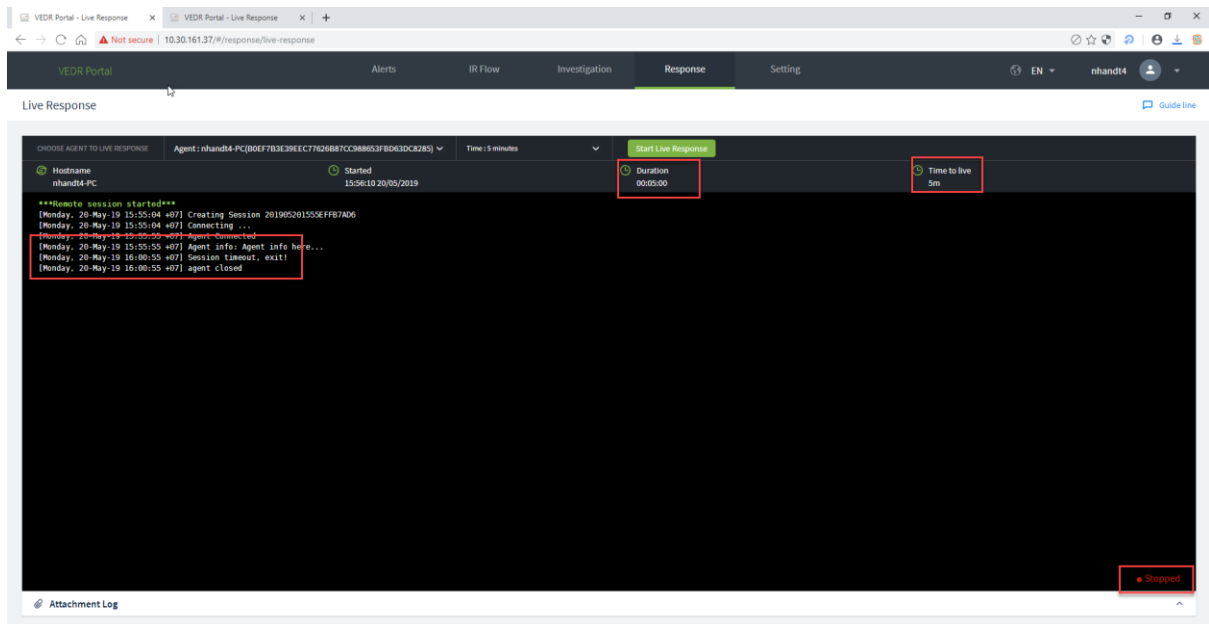
STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath>	Thay đổi thư mục làm việc hiện tại
2		cd.. hoặc cd ..	Chuyển về thư mục cha
3	pwd		In thư mục hiện thời đang làm việc
4	dir		Liệt kê các file/ các thư mục con trong thư mục hiện thời
5	delete	delete -file <path> ví dụ: delete -file "c:\temp\run path.exe"	Xóa 1 file
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers	Xóa 1 thư mục
		delete -all <folderpath> ví dụ: delete -all c:\temp	Xóa tất cả các file/ thư mục con trong thư mục (nhưng không xóa thư mục)
6	viewfile	<filepath><sizeinbytes>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	get	<filepath>	Upload 1 file từ host lên server
8	put	<url><folderpath>	Download 1 file tới máy host
9	mkdir	<dir name>	Tạo 1 thư mục
10	reg		Các lệnh liên quan đến Registry
		query <keyname> -v <valuenam> ví dụ:	Truy vấn dữ liệu value của 1 key

		reg -query "HKLM\Software\abc xyz" -v "run path"	
		query <keyname> -s ví dụ: reg -query "HKLM\Software\abc xyz" -s	Truy vấn tất cả các subkey và value và data
		add <keyname> ví dụ: reg -add "HKLM\software\abc xyz"	Thêm 1 key
		add <keyname> -v <valuenam> -t <type> -d <data> ví dụ: reg -add "HKLM\software\abc xyz" -v "run path" -t REG_SZ -d "c:\temp\bin.exe"	Thêm 1 value
		delete <keyname> ví dụ: reg -delete HKU\S-1-5-21-3791698801-2327923109-636705026-2080\Software\Test	Xóa 1 key và tất cả các subkey và value
		delete <keyname> -v <valuenam>	Xóa 1 giá trị của key
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg
11	process		Các lệnh liên quan đến process
		-t <processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid>	Tạm dừng 1 tiến trình
		-r <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>	Liệt kê các process của 1 user
12	service		Các lệnh liên quan đến service
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename>	Start 1 service
		-stop <servicename>	Stop 1 service
13	user		
		-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
14	cls		Xóa màn hình console
15	help		Lệnh help

- 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 đây, 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.

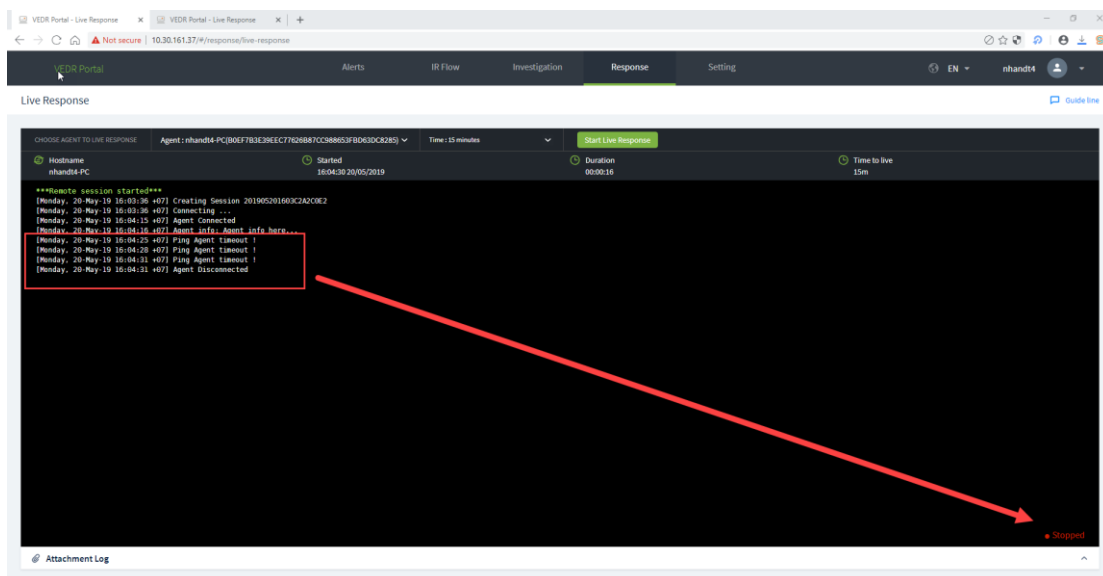


- Bước 6: Phiên làm việc của Live Response kết thúc khi:
 - + Thời gian của phiên hết hiệu lực: Khi trường “Duration” bằng thời gian với trường “Time To Live”.



+ 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.



3.8 Màn hình Setting

3.8.1 Agent Management

- 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)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
DESKTOP-EGANUBQ	Online	No_group	Release	20/05/2019 16:47:07	17/04/2019 10:16:46	192.168.4.222,192.168.4.111	test_sample
ThanhN-PC	Online	No_group	Release	20/05/2019 16:47:01	13/03/2019 13:30:45	192.168.4.222,192.168.4.111	test_sample
NhandB-PC	Online	No_group	Release	20/05/2019 16:46:45	13/03/2019 13:09:22	192.168.4.111	test_sample
Chuyent2-ViettelOS	Offline	No_group	Release	20/05/2019 16:35:19	22/04/2019 16:56:49	192.168.4.222,192.168.4.111	test_sample
DESKTOP-HHQB1Q	Offline	No_group	Release	20/05/2019 13:43:08	05/11/2018 14:21:48	192.168.4.111,192.168.4.222	test_sample
W-PC	Offline	No_group	Release	16/05/2019 18:41:25	25/03/2019 17:38:14	192.168.129.2	test_sample
Hanoi-PC	Offline	No_group	Release	14/05/2019 15:27:58	01/04/2019 17:11:43	192.168.253.2	test_sample
ThanhN-VirtualBox	Offline	No_group	Test	03/05/2019 15:48:57	11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A
Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10	29/01/2019 04:57:35	192.168.4.222	test_sample
Chuyent12-ViettelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52	22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A
ThanhN-VirtualBox	Offline	No_group	Test	20/04/2019 10:36:54	13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A
DESKTOP-SC8PVC	Offline	No_group	Release	01/04/2019 18:51:50	05/11/2018 14:42:16	192.168.11.2	test_sample
Hanoi-PC	Offline	No_group	Release	01/04/2019 16:00:13	13/03/2019 11:50:06	192.168.253.2	test_sample
DESKTOP-U8QBHAR	Offline	No_group	Release	29/03/2019 15:48:06	12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample
ThanhN-PC	Offline	No_group	Release	26/03/2019 17:48:49	21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A
DESKTOP-JV5222	Offline	No_group	Release	02/03/2019 22:54:03	19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample
DESKTOP-TN54D0	Offline	No_group	Release	28/02/2019 16:30:14	22/02/2019 10:53:15	192.168.4.111	test_sample
ANM-THANHHLNB	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample
WIN10-CONGVCS	Offline	No_group	Release	25/01/2019 09:35:41	08/11/2018 10:55:46	192.168.129.2	test_sample
ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:43:19	192.168.4.111,192.168.4.222	test_sample

- 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: Hiện thị tất cả Agent trong hệ thống active < 30 ngày

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

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

+ User đăng nhập thuộc group một hoặc nhiều con: Hiện 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 "=", "!=", "~".

VEDR Portal - IR Flow Detail | VEDR Portal - Agent Management | VEDR Portal - Agent Management

Alerts | IR Flow | Investigation | Response | **Setting**

Agent Management

Type to search agent ...

AgentID Agent ID
ComputerName Agent Computer Name
OS Agent Operating System
Architecture Agent Architecture
Platform Agent Platform

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
Nhand4-PC	Offline	No_group	Release	20/05/2019 17:02:46	13/03/2019 13:05:22	192.168.4.111	test_sample
Chuyent2-VietelOS	Offline	No_group	Release	20/05/2019 16:35:19	22/04/2019 16:56:49	192.168.4.222,192.168.4.111	N/A
DESKTOP-HNHB10	Offline	No_group	Release	20/05/2019 13:43:08	05/11/2018 14:21:48	192.168.4.111,192.168.4.222	test_sample
Hanoi-PC	Offline	No_group	Release	14/05/2019 15:27:58	01/04/2019 17:11:43	192.168.253.2	test_sample
Thanhho-VirtualBox	Offline	No_group	Test	03/05/2019 15:48:57	11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A
Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10	29/01/2019 04:57:35	192.168.4.222	test_sample
Chuyent2-VietelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52	22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A
Thanhho-VirtualBox	Offline	No_group	Test	20/04/2019 10:36:54	13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A
DESKTOP-SCRPVCE	Offline	No_group	Release	01/04/2019 18:51:50	05/11/2018 14:42:16	192.168.11.2	test_sample
Hanoi-PC	Offline	No_group	Release	01/04/2019 16:00:13	13/03/2019 11:50:06	192.168.253.2	test_sample
DESKTOP-U8QBHAB	Offline	No_group	Release	29/03/2019 15:48:06	12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample
Thanhho-PC	Offline	No_group	Release	26/03/2019 17:48:49	21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A
DESKTOP-JV5222	Offline	No_group	Release	02/03/2019 22:54:03	19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample
DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14	22/02/2019 10:53:15	192.168.4.111	test_sample
ANM-THANHLO	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample
WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41	08/11/2018 10:55:46	192.168.129.2	test_sample
ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample

Display 35/35 result

- Ví dụ về các câu tìm kiếm:
Tìm kiếm với điều kiện “=”

VEDR Portal - Alerts | IR Flow | Investigation | Response | **Setting**

Agent Management

AgentID = "0A913568B48ED24E20E9606FF9C3D2F7E4912B"

1 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
ANM-NHAND4	Offline	No_group	Test	18/12/2018 10:37:10	12/12/2018 09:06:04	192.168.4.222	test_sample

Display 1/1 result

Tìm kiếm với điều kiện “!=”

VEDR Portal - Alerts | IR Flow | Investigation | Response | **Setting**

Agent Management

AgentID != "0A913568B48ED24E20E9606FF9C3D2F7E4912B"

34 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
DESKTOP-EGANUBO	Online	No_group	Release	24/05/2019 10:42:43	17/04/2019 10:16:46	192.168.4.222,192.168.4.111	test_sample
Thanhho-VirtualBox	Offline	No_group	Test	24/05/2019 09:17:22	11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A
Nhand4-PC	Offline	No_group	Release	23/05/2019 16:44:37	13/03/2019 13:05:22	192.168.4.111	test_sample
Thanhho-VirtualBox	Offline	No_group	Test	22/05/2019 14:32:06	13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A
Thanhho-PC	Offline	No_group	Release	22/05/2019 09:26:27	13/03/2019 13:30:43	192.168.4.222,192.168.4.111	test_sample
Win7-CONGNC9	Offline	No_group	Release	21/05/2019 18:19:26	25/03/2019 17:38:14	192.168.129.2	test_sample
Chuyent2-VietelOS	Offline	No_group	Release	21/05/2019 16:04:51	22/04/2019 16:56:49	192.168.4.222,192.168.4.111	N/A
DESKTOP-HNHB10	Offline	No_group	Release	21/05/2019 15:18:40	05/11/2018 14:21:48	192.168.4.111,192.168.4.222	test_sample
Hanoi-PC	Offline	No_group	Release	14/05/2019 15:27:58	01/04/2019 17:11:43	192.168.253.2	test_sample
Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10	29/01/2019 04:57:35	192.168.4.222	test_sample
Chuyent2-VietelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52	22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A
DESKTOP-SCRPVCE	Offline	No_group	Release	01/04/2019 18:51:50	05/11/2018 14:42:16	192.168.11.2	test_sample
Hanoi-PC	Offline	No_group	Release	01/04/2019 16:00:13	13/03/2019 11:50:06	192.168.253.2	test_sample
DESKTOP-U8QBHAB	Offline	No_group	Release	29/03/2019 15:48:06	12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample
Thanhho-PC	Offline	No_group	Release	26/03/2019 17:48:49	21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A
DESKTOP-JV5222	Offline	No_group	Release	02/03/2019 22:54:03	19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample
DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14	22/02/2019 10:53:15	192.168.4.111	test_sample
ANM-THANHLO	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample
WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41	08/11/2018 10:55:46	192.168.129.2	test_sample
ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample

Tìm kiếm với điều kiện “~”

VEDR Portal Alerts IR Flow Investigation Response **Setting** EN nhand4

Agent Management

ComputerName - "ANM"

6 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
ANM-THANHUN	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample
ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample
ANM-SHANDT4	Offline	No_group	Test	18/12/2018 10:37:10	12/12/2018 09:06:04	192.168.4.222	test_sample
ANM-CONGNC3	Offline	No_group	Alpha	03/12/2018 15:01:10	30/11/2018 16:13:13	192.168.4.222,192.168.4.111	test_sample
ANM-PHUOCNM2	Offline	No_group	Alpha	03/12/2018 14:31:13	30/11/2018 16:12:38	192.168.4.222,192.168.4.111	test_sample
ANM-CONGNC9	Offline	N/A	N/A	N/A	N/A	192.168.129.2	N/A

Display 6/6 result

Tìm kiếm theo tiêu chí kết hợp AND

VEDR Portal Alerts IR Flow Investigation Response **Setting** EN nhand4

Agent Management

ComputerName - "ANM" AND Platform - "Microsoft Windows 10 Pro"

2 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY	PLATFORM
ANM-CONGNC9	Offline	No_group	Alpha	03/12/2018 15:01:10	30/11/2018 16:13:13	192.168.4.222,192.168.4.111	test_sample	Microsoft Windows 10 Pro
ANM-CONGNC9	Offline	N/A	N/A	N/A	N/A	192.168.129.2	N/A	Microsoft Windows 10 Pro

Display 2/2 result

Tìm kiếm theo tiêu chí kết hợp OR

VEDR Portal Alerts IR Flow Investigation Response **Setting** EN nhand4

Agent Management

ComputerName - "ANM" OR Platform - "Microsoft Windows 10 Pro"

14 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY	PLATFORM
DESKTOP-EGANUBQ	Online	No_group	Release	24/05/2019 10:50:45	17/04/2019 10:16:46	192.168.4.222,192.168.4.111	test_sample	Microsoft Windows 10 Pro
DESKTOP-HHQB1Q	Offline	No_group	Release	21/05/2019 15:18:40	05/11/2018 14:21:48	192.168.4.111,192.168.4.222	test_sample	Microsoft Windows 10 Pro
DESKTOP-ACBPVCE	Offline	No_group	Release	01/04/2019 18:51:50	05/11/2018 14:42:16	192.168.11.2	test_sample	Microsoft Windows 10 Pro
DESKTOP-UBQBHAB	Offline	No_group	Release	29/03/2019 15:48:06	12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample	Microsoft Windows 10 Pro
DESKTOP-JUV222	Offline	No_group	Release	02/03/2019 22:54:03	19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample	Microsoft Windows 10 Pro
ANM-THANHUN	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample	Microsoft Windows 10 Enterprise
WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41	08/11/2018 10:55:46	192.168.129.2	test_sample	Microsoft Windows 10 Pro
ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample	Microsoft Windows 7 Enterprise Service Pack
ANM-SHANDT4	Offline	No_group	Test	18/12/2018 10:37:10	12/12/2018 09:06:04	192.168.4.222	test_sample	Microsoft Windows 10 Enterprise
ANM-CONGNC2	Offline	No_group	Alpha	03/12/2018 15:01:10	30/11/2018 16:13:13	192.168.4.222,192.168.4.111	test_sample	Microsoft Windows 10 Pro
ANM-PHUOCNM2	Offline	No_group	Alpha	03/12/2018 14:31:13	30/11/2018 16:12:38	192.168.4.222,192.168.4.111	test_sample	Microsoft Windows 10 Enterprise
DESKTOP-OMETB1E	Offline	No_group	Release	30/11/2018 14:30:30	30/11/2018 14:04:16	192.168.4.111,192.168.4.222	test_sample	Microsoft Windows 10 Pro
DESKTOP-30TIL7P	Offline	No_group	Release	26/11/2018 15:31:19	17/11/2018 17:11:19	8.8.8.8,8.8.4.4	test_sample	Microsoft Windows 10 Pro
ANM-CONGNC2	Offline	N/A	N/A	N/A	N/A	192.168.129.2	N/A	Microsoft Windows 10 Pro

Display 14/14 result

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

AJIA

NT

Alerts

IR Flow

Investigation

Response

Protect & Prevention

Setting

EN

Agent Management

Type to search agent ...

First Ping

Last Ping

33 result(s)

View column

Selected (3)

Set Policy

Move to group

Set update group

Cancel

☐	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY
☒	DESKTOP-4C8V54I	Offline	Test_scan_ip	Test	22/05/2020 15:46:14	15/05/2020 17:38:55	10.61.188.2	Agent Performance
☒	ThanhLN9-PC	Offline	Liennt_group1	Alpha	25/05/2020 15:05:57	21/03/2019 13:31:53	10.61.188.2	bbs_test
☒	Huythv-PC	Offline	Test_scan_ip	Test	25/05/2020 14:40:55	31/01/2020 17:23:19	10.61.188.2	Agent Performance
☐	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10.61.188.2	huythv-2211
☐	WIN-MM956/NPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10.61.188.2	N/A
☐	Chuyent2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10.61.188.2	default
☐	DESKTOP-BGH80IG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10.61.188.2	full_features
☐	DESKTOP-LBT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10.61.188.2	huythv_15.01.ProPre
☐	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10.61.188.2	N/A
☐	Ubuntu18x64chuyent	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10.61.188.2	Agent Performance
☐	WIN-QH33SL48BRJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10.61.188.2	hieupc4
☐	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10.61.188.2	Agent Performance
☐	Ubuntu18x64chuyent-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10.61.188.2	test
☐	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10.61.188.2	Agent Performance
☐	localhostLocaldomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10.61.188.2	centos
☐	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10.61.188.2	full_features
☐	DESKTOP-31SSAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10.61.188.2	huythv_15.01.ProPre

+ Tích chọn 1 agent/ nhiều agent để vào phiên Multiselect

+ Thực hiện Set Policy

Selected (1) Set Policy Cancel

☐	NAME	Policy	UP
☒	Nhand	test_sample	group
☐	Win7-C		group
☐	Thanh		group

Set Policy

+ Kết quả sau khi set policy

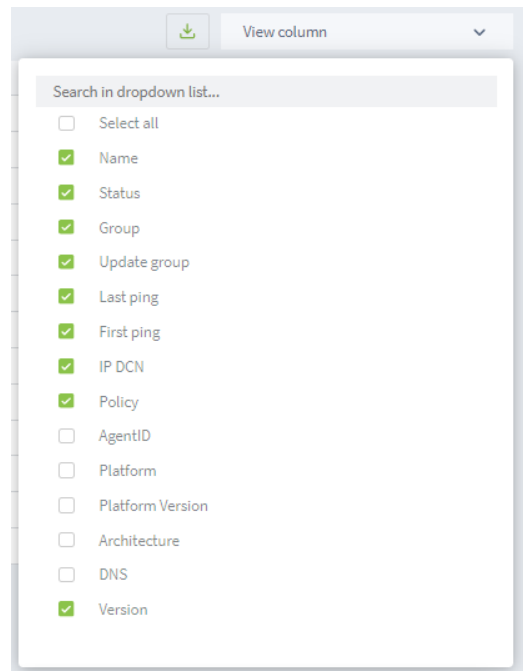
test_sample

11,13

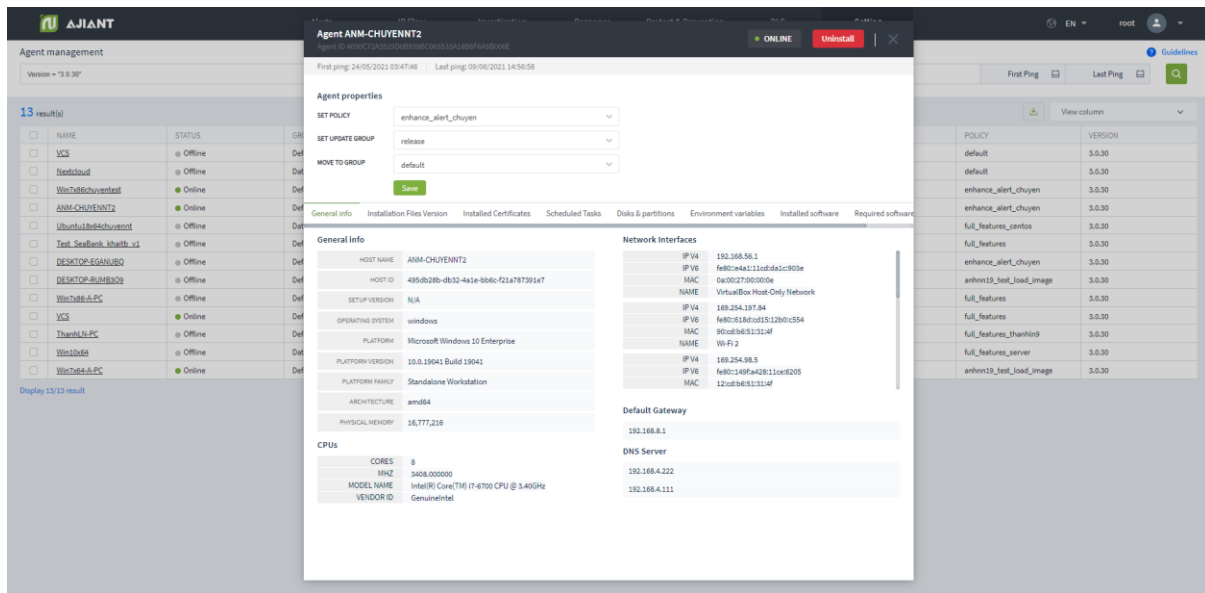
Set Policy successfully!

+ Hủy thao tác ở màn hình Multiselect

- 4 - View Column: Cấu hình hiển thị các cột theo mong muốn.



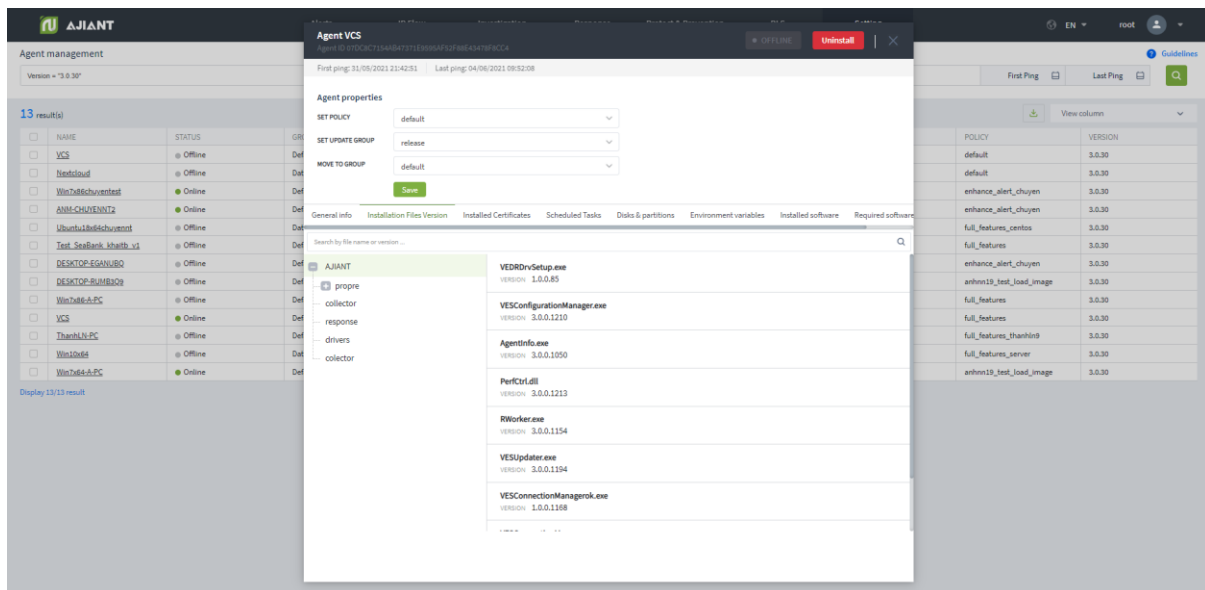
- 5 - Xem chi tiết 1 agent bằng việc click duplicate chuột vào 1 row bất kỳ
Hệ thống hỗ trợ người dùng thiết lập Policy, Update Group và Move to group cho Agent 1 cách nhanh chóng.
 - + User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống
 - + User đăng nhập thuộc group default: Hiển 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.



✓ Installation Files Version

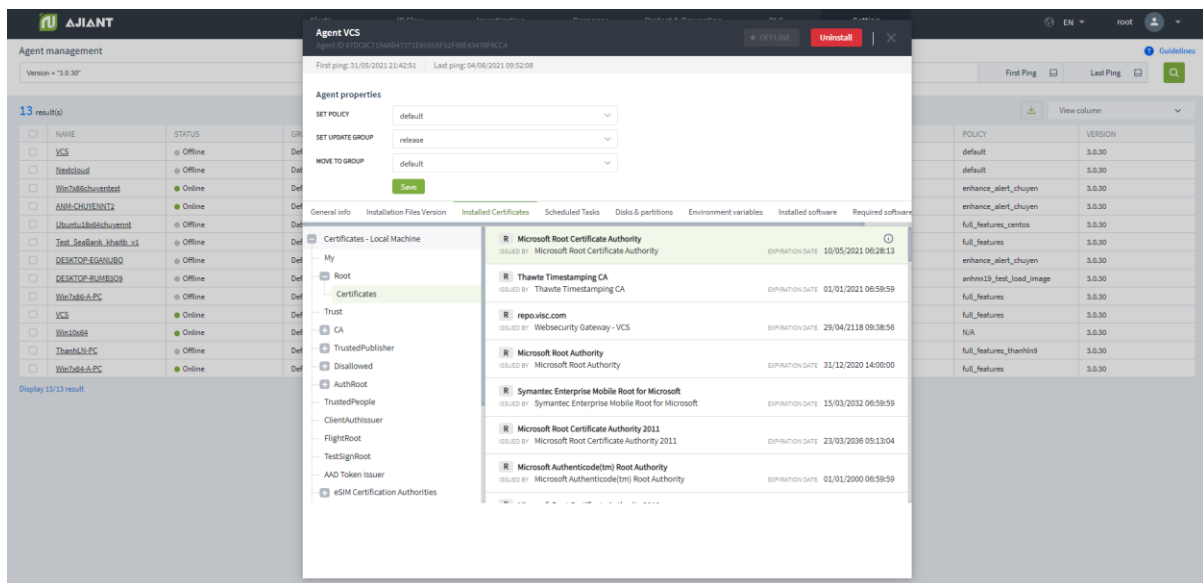
- Thống kê tất cả các file cài agent, bao gồm các thông tin: Tên folder chứa file cài, File name, Version

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



✓ Installed Certificates

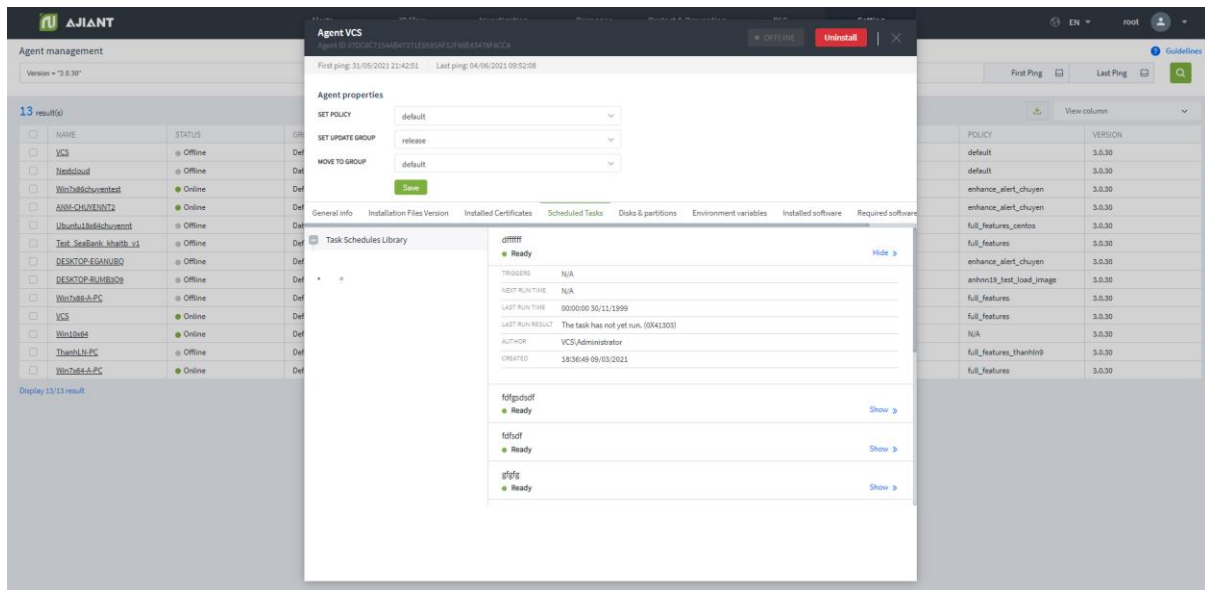
- Thống kê tất cả các certificate trên máy cài agent, bao gồm các thông tin: Danh sách certificates trên máy, Issued by, Issued to, Expiration date, Status



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

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

XML Detail



```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2021-03-09T18:36:49.6502882</Date>
    <Author>VCS\Administrator</Author>
    <URI>\dftgdsd</URI>
  </RegistrationInfo>
  <Triggers />
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-21-3942219608-2782901308-3935319899-500</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
  </Settings>
</Task>
```

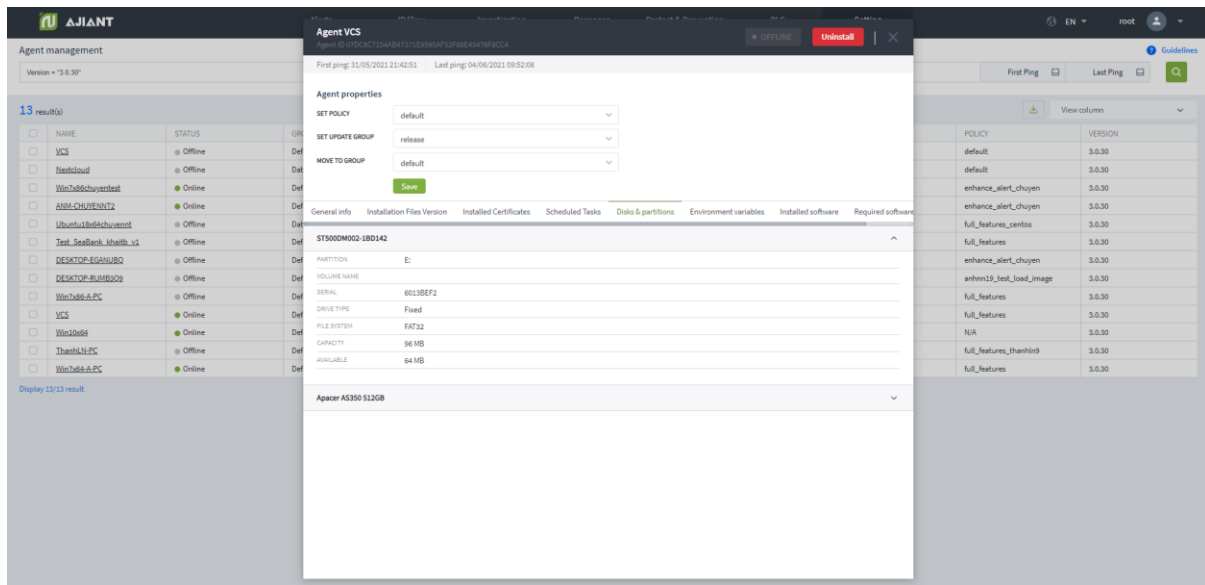
 **Export to XML**

+ Chọn  để tải về thông tin scheduled task, hỗ trợ định dạng .xml

✓ 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.

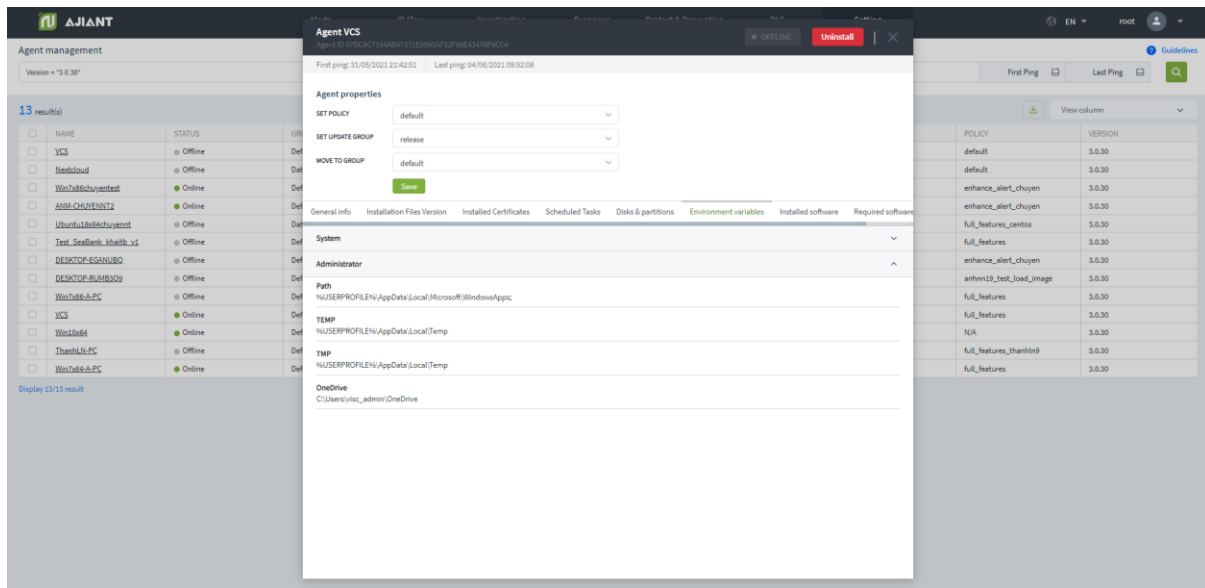
+ Chọn  hoặc  để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



✓ Environment variables

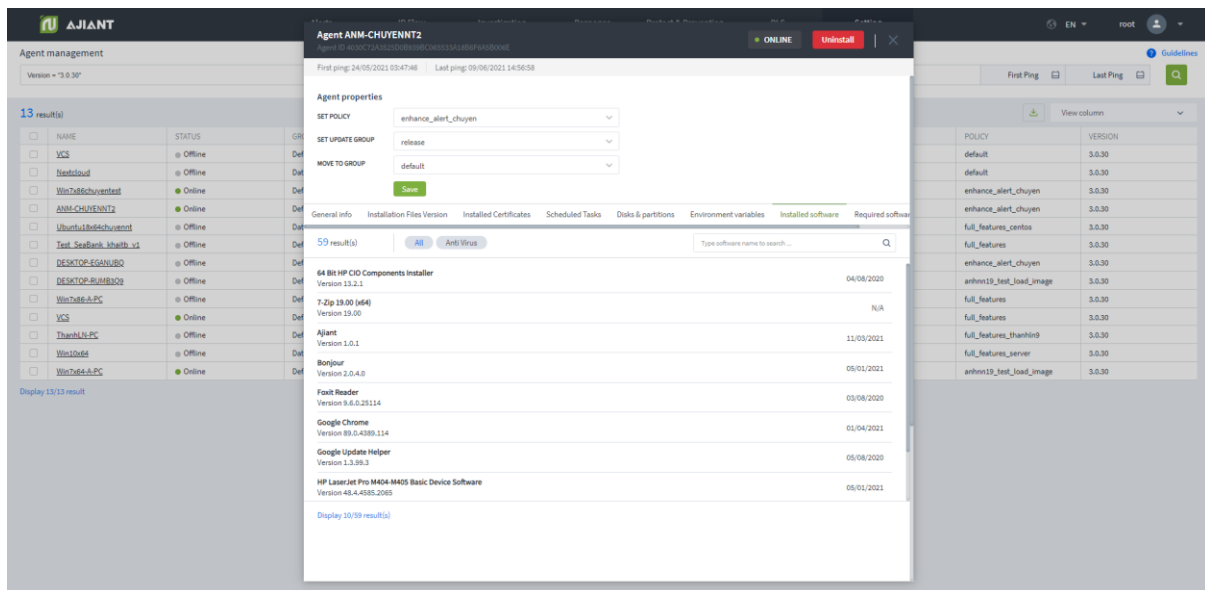
- Thống kê tất cả environment variables trên máy cài agent, bao gồm các thông tin: Danh sách system và users, tên biến, giá trị trực thuộc system hoặc user.

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



✓ Tab Installed Software

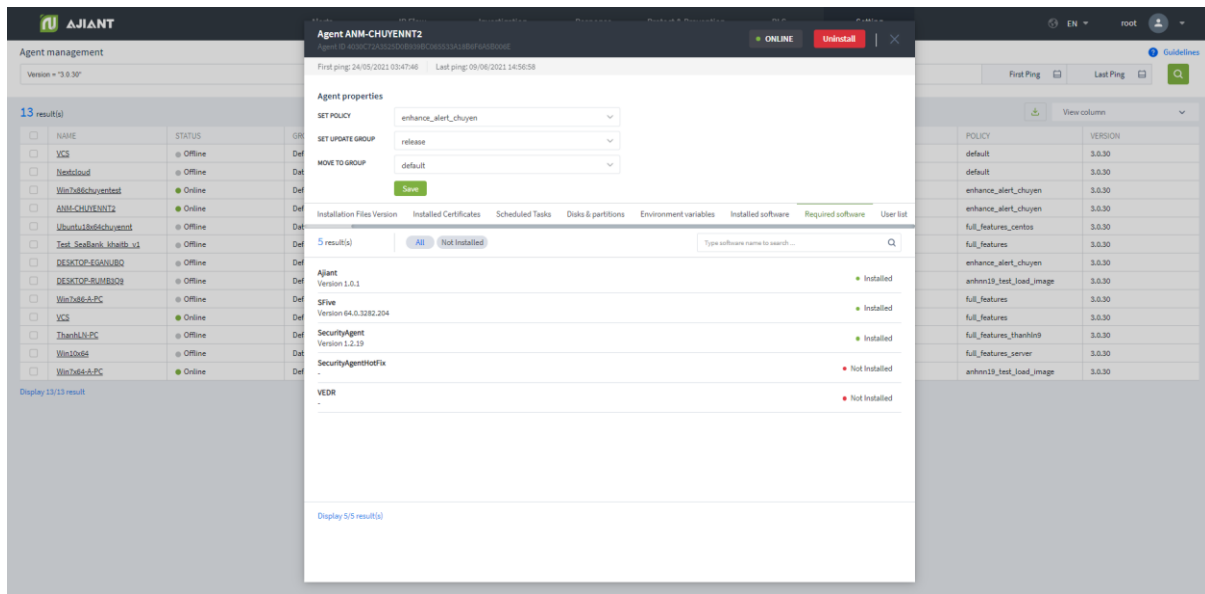
- Thống kê tất cả phần mềm đã cài trong agent bao gồm thông tin: Tên phần mềm, version cài, ngày cài
- + Hỗ trợ search nhanh phần mềm Antivirus đã cài hoặc nhập tên phần mềm vào text box search



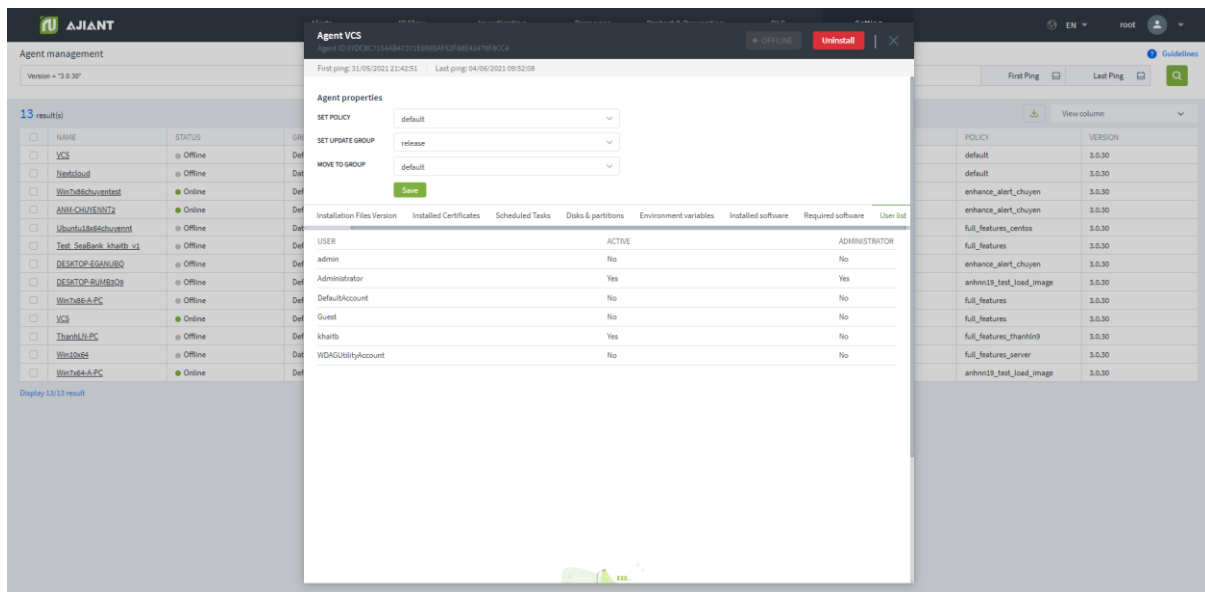
✓ Tab Required Software

- 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 Multiselect

AJANT Alerts IR Flow Investigation Response Protect & Prevention **Setting** EN root

Agent Management

Type to search agent ... First Ping Last Ping

33 result(s)

Selected (3) **Set Policy** **Move to group** **Set update group** Cancel

NAME Groups UPDATE GROUP LAST PING FIRST PING IP DCM POLICY

☒ DESKTOP-4C6V54I	Select an Option	Test	22/05/2020 15:46:14	15/05/2020 17:38:55	10.61.188.2	Agent Performance	
☒ ThanhN9-PC		Alpha	25/05/2020 15:05:57	21/03/2019 13:31:53	10.61.188.2	bbs_test	
☒ HuyHV-PC		Test	25/05/2020 14:40:55	31/01/2020 17:23:19	10.61.188.2	Agent Performance	
☐ Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10.61.188.2	huyhv-2211
☐ WIN-MM956VNF020	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10.61.188.2	N/A
☐ Chuyent23viettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10.61.188.2	default
☐ DESKTOP-8IGH80IG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10.61.188.2	full_features
☐ DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10.61.188.2	huyhv_15.01.ProPre
☐ LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10.61.188.2	N/A
☐ Ubuntu18x64chuyent	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10.61.188.2	Agent Performance
☐ WIN-QH33SL4BBRJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10.61.188.2	hieupc4
☐ Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10.61.188.2	Agent Performance
☐ Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10.61.188.2	test
☐ ThanhN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10.61.188.2	Agent Performance
☐ LocalhostLocaldomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10.61.188.2	centos
☐ DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10.61.188.2	full_features
☐ DESKTOP-31SSAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10.61.188.2	huyhv_15.01.ProPre

+ Thực hiện Move to group

Danh sách Group trong combobox Move to group

- User đăng nhập thuộc group root: Hiện thị tất cả Group trong hệ thống
- User đăng nhập thuộc group default: Hiện thị Group default
- User đăng nhập thuộc group cha: Hiện 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: Hiện 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 Multiselect

AJIANT									
Agent Management									
Type to search agent ...									
33 result(s)									
Selected (3) Set Policy Move to group Set update group Cancel									
☐	NAME	STAT	Update Groups	IOUP	LAST PING	FIRST PING	IP DCN	POLICY	
☒	DESKTOP-4C6V54I	Off	Select an Option		22/05/2020 15:46:14	15/05/2020 17:38:55	10.61.188.2	Agent Performance	
☒	ThanhN3-PC	Off			25/05/2020 15:05:57	21/03/2019 13:31:53	10.61.188.2	bbs_test	
☒	HuyHV-PC	Off	Set Update Group		25/05/2020 14:40:55	31/01/2020 17:23:19	10.61.188.2	Agent Performance	
☐	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10.61.188.2	huyhv-2211	
☐	WIN-MM956VNPDS0	Offline	Lient_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10.61.188.2	N/A	
☐	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10.61.188.2	default	
☐	DESKTOP-BIGH8QIG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10.61.188.2	full_features	
☐	DESKTOP-LBT704L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10.61.188.2	huyhv_15.01.ProPre	
☐	LienNT-TestPC	Offline	Lient_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10.61.188.2	N/A	
☐	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10.61.188.2	Agent Performance	
☐	WIN-QH33SL488RJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10.61.188.2	hieupc4	
☐	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10.61.188.2	Agent Performance	
☐	Ubuntuhyerv-Virtual_Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10.61.188.2	test	
☐	ThanhN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10.61.188.2	Agent Performance	
☐	localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10.61.188.2	centos	
☐	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10.61.188.2	full_features	
☐	DESKTOP-31SSAGT	Offline	Lient_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10.61.188.2	huyhv_15.01.ProPre	

- 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

3.8.2 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:

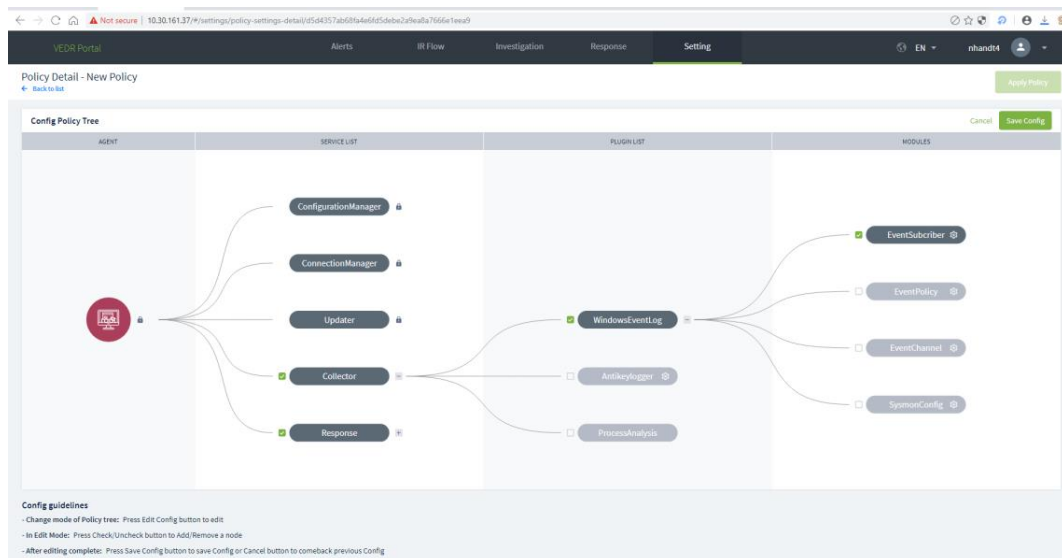
VEDR Portal									
Alerts IR Flow Investigation Response Setting									
Policy List									
NAME NUMBER OF AGENT CREATE TIME UPDATE TIME APPLIED TIME APPLY STATUS									
default	1	28/01/2019 14:11:52	19/04/2019 17:06:17	26/03/2019 17:33:51	Not applied				
test	0	02/03/2019 14:13:28	25/04/2019 17:13:57	25/04/2019 17:19:07	Applied				
test_sample	25	04/03/2019 11:07:09	21/05/2019 13:43:57	21/05/2019 13:44:03	Applied				
test_sample 1	0	04/03/2019 13:53:51	04/03/2019 13:53:51	N/A	Not applied				
test2	0	04/03/2019 17:53:51	04/03/2019 17:54:23	05/03/2019 09:23:02	Applied				
hieupc4	0	05/03/2019 15:44:15	05/03/2019 15:44:15	05/03/2019 15:44:20	Applied				
0503_test1	0	05/03/2019 17:19:27	06/03/2019 14:10:13	06/03/2019 15:03:18	Applied				
0703_policy	0	07/03/2019 09:04:29	07/03/2019 09:04:29	07/03/2019 09:04:33	Applied				
2003_test_core service	0	20/03/2019 10:14:49	20/03/2019 15:34:56	20/03/2019 15:35:28	Applied				
2003_test_plugin Response	0	20/03/2019 10:37:48	20/03/2019 15:36:07	20/03/2019 15:38:33	Applied				
2003_test_du plugin	0	20/03/2019 10:53:16	20/03/2019 10:53:39	20/03/2019 10:57:55	Applied				
2003_test_collector chưa module	0	20/03/2019 17:35:34	20/03/2019 17:35:43	20/03/2019 17:35:46	Applied				

- 1 - Hiện 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).

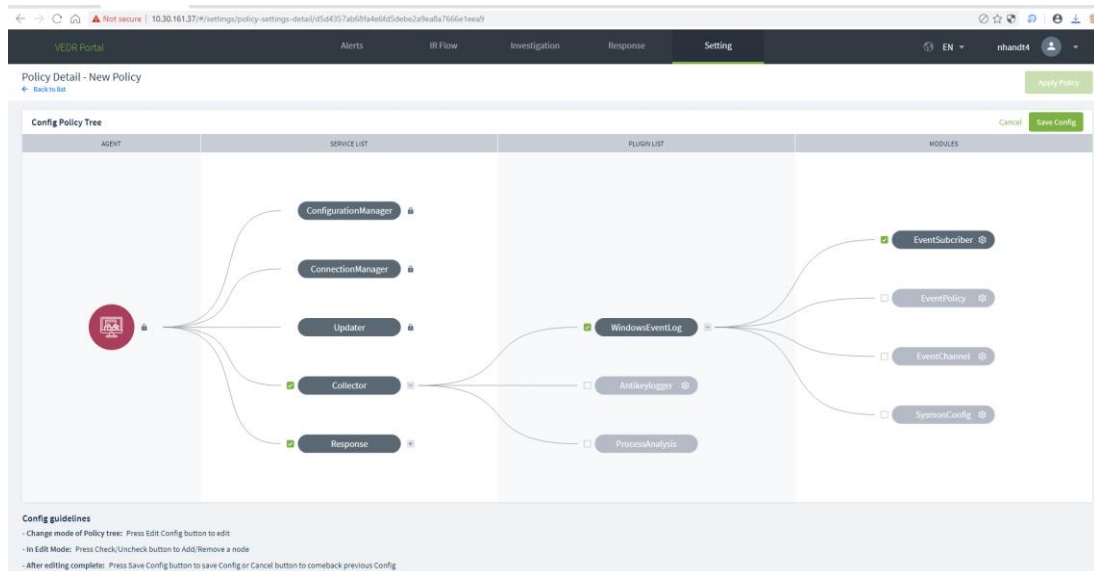
- 2 - Tạo mới một chính sách: Click vào button **+ Create New Policy** hệ thống hiển thị Popup tạo mới chính sách như sau:

- 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:

- 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 button **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: Người dùng nhấn nút “Save config” để lưu các thay đổi hoặc nhấn nút “Cancel” để quay lại cấu hình trước đây.



- Bước 4: Click icon  để thực hiện cấu hình chi tiết cho từng module/Plugin của các Service.

+ WindowsEventLog: cấu hình các nguồn log lấy dưới Agent

EventSubscriber: chỉ định các kênh lấy log

Yêu cầu dữ liệu:

- o trường **event_filter** (lọc theo Event ID): các string con cách nhau dấu phẩy (,)

VD: “4”: lọc các event có eventID = 4

“-689”: lọc 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

+ 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

+ EventChannel: cấu hình chi tiết 1 số nguồn log:

Retention: có lưu log xoay vòng hay không (Nếu chọn Retention 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

+ SysmonConfig: enable/disable sysmon tool trên Agent để lấy log sysmon: Microsoft-Windows-Sysmon/Operational

- 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			Clear
WILTYPE	SCAN TYPE	DATA	
Select	Select	Type to...	<button>Add new</button>
WhitelistCer	RawInput	Microsoft Corporation	
WhitelistPath	HookMessage	C:\users\win 10 64\desktop\unikey40rc2-1101-win64\unikeynt.exe	

- Bước 5: Click button **Apply Policy** để thiết lập Policy vừa được cấu hình cho Agent.

+ Clone chính sách mới: Click vào button  hệ thống sao chép toàn bộ chi tiết của policy được clone ngoại trừ tên policy.

Clone from policy:

test_sample

NAME OF POLICY

Enter name of policy...

Cannot edit name of policy after create policy

Create

+ Xóa chính sách: Click vào button  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: **hieupc4**

This policy has been assigned to agent(s). If this policy is deleted, agent(s) will be reset to default policy!

Cancel

Accept

+ Khi click duplicate 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.

3.8.3 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:
 - 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: Hiện thị tất cả Group trong hệ thống
- + User đăng nhập thuộc group default: Hiện thị group default
- + User đăng nhập thuộc group cha: Hiện thị Group thuộc group của user đang login và group con tương ứng
- + User đăng nhập thuộc group một hoặc nhiều con: Hiện 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.

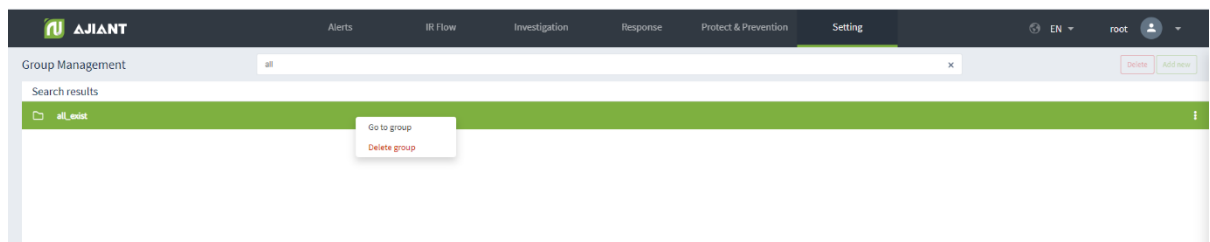
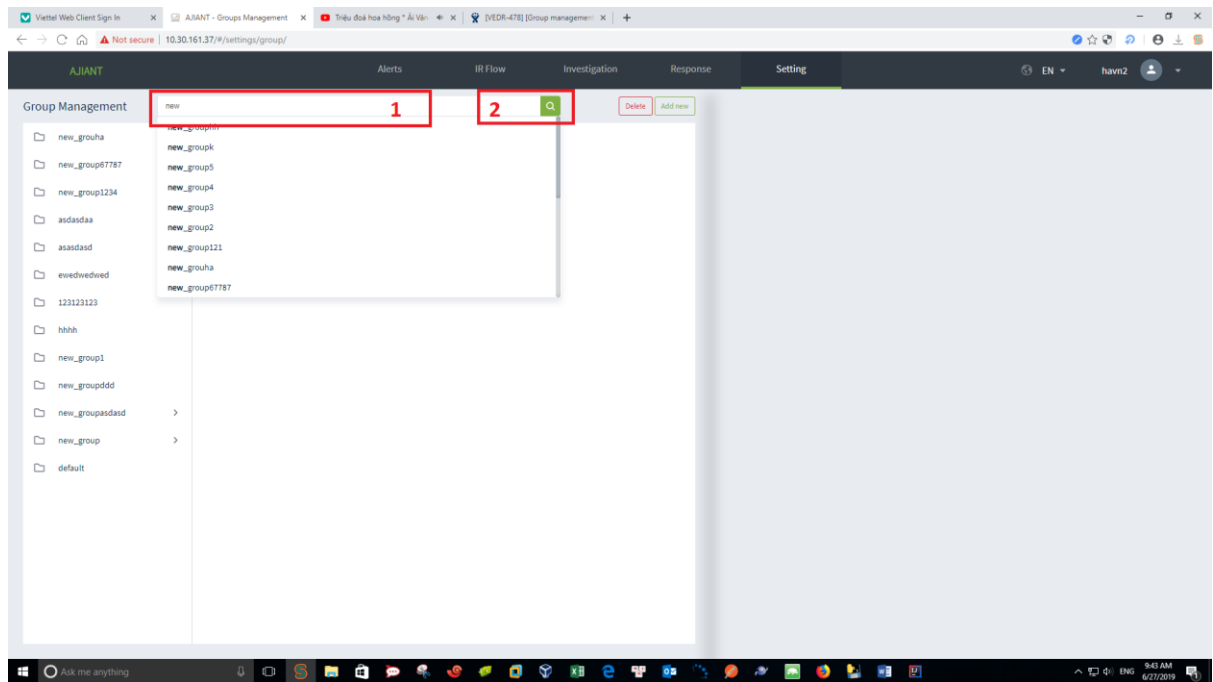
Các rule của nhóm là độc lập giữa các nhóm (không có kế thừa cha con). Việc quản lý nhóm theo cây để quản lý dễ dàng hơn khi số lượng agent lớn và có sự phân cấp về quản lý agent theo công ty, phòng, ban...

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



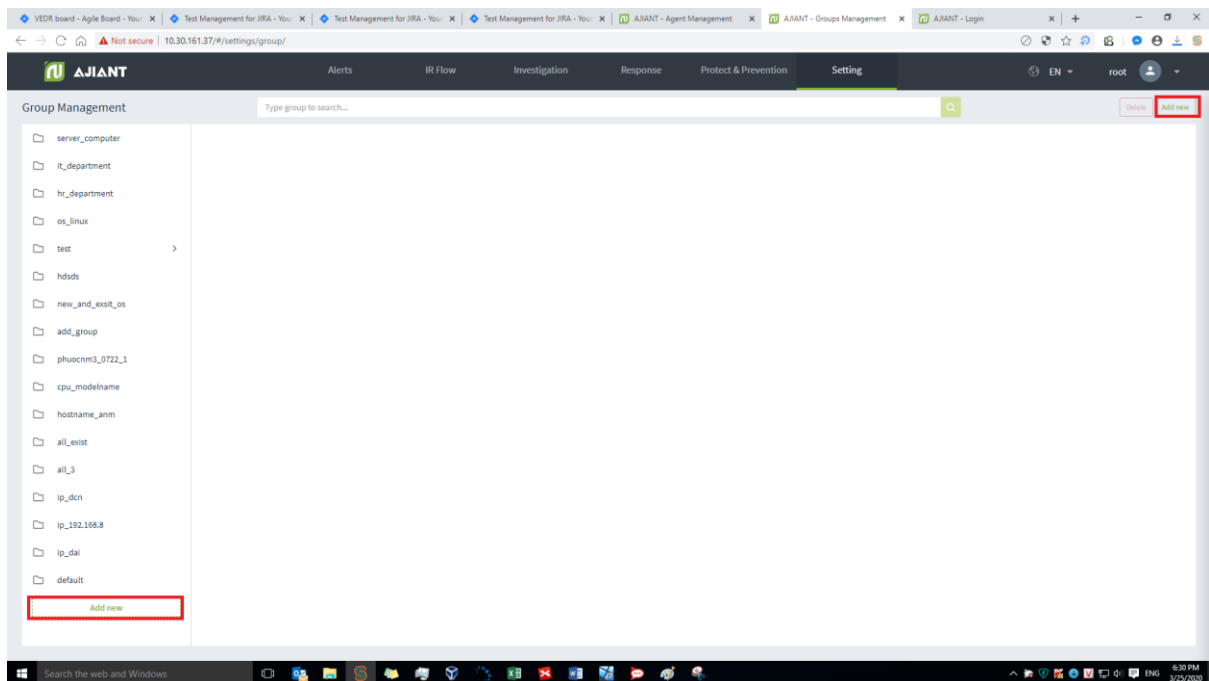
- Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.
 - o Tab thông tin chi tiết hiển thị là Detail, dữ liệu của group đó là Rule, Policy, Apply to.
 - o Khi chọn tab Agent list thì dữ liệu thông tin các agent match với group đó.
- Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 2 option: Go to group và Delete group.
 - o Nếu chọn Go to group thì đưa user đến vị trí của group đó trên cây
 - o Nếu chọn Delete group thì hiển thị popup confirm xóa group.
- Khi click vào menu góc phải mỗi bản ghi cũng hiển thị 2 option: Go to group và Delete group.

(3) Thêm mới nhóm:

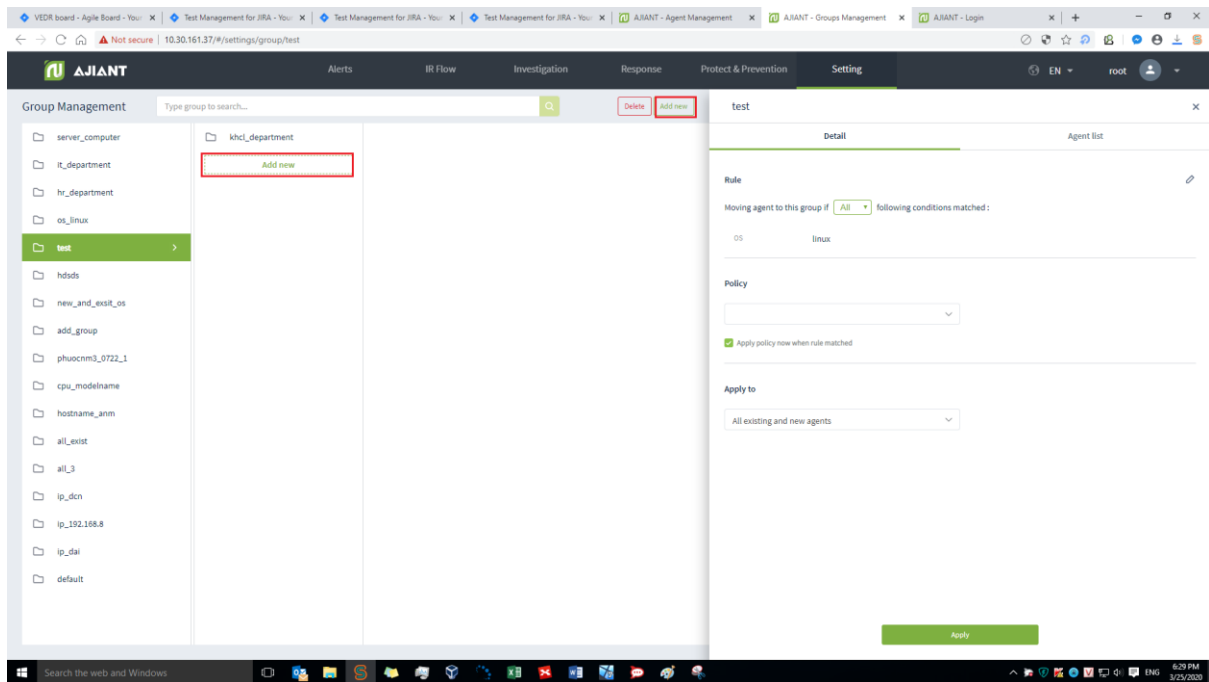
- + User đăng nhập thuộc group root: Có thể thêm mới tất cả Group trong
- + User đăng nhập thuộc group default: Không thể thêm mới
- + User đăng nhập thuộc group cha: có thể thêm mới group con tương ứng của group thuộc user đang login
- + User đăng nhập thuộc group một hoặc nhiều con: có thể thêm mới group con tương ứng của group thuộc user đang login

B1: Lựa chọn vị trí nhóm sẽ tạo

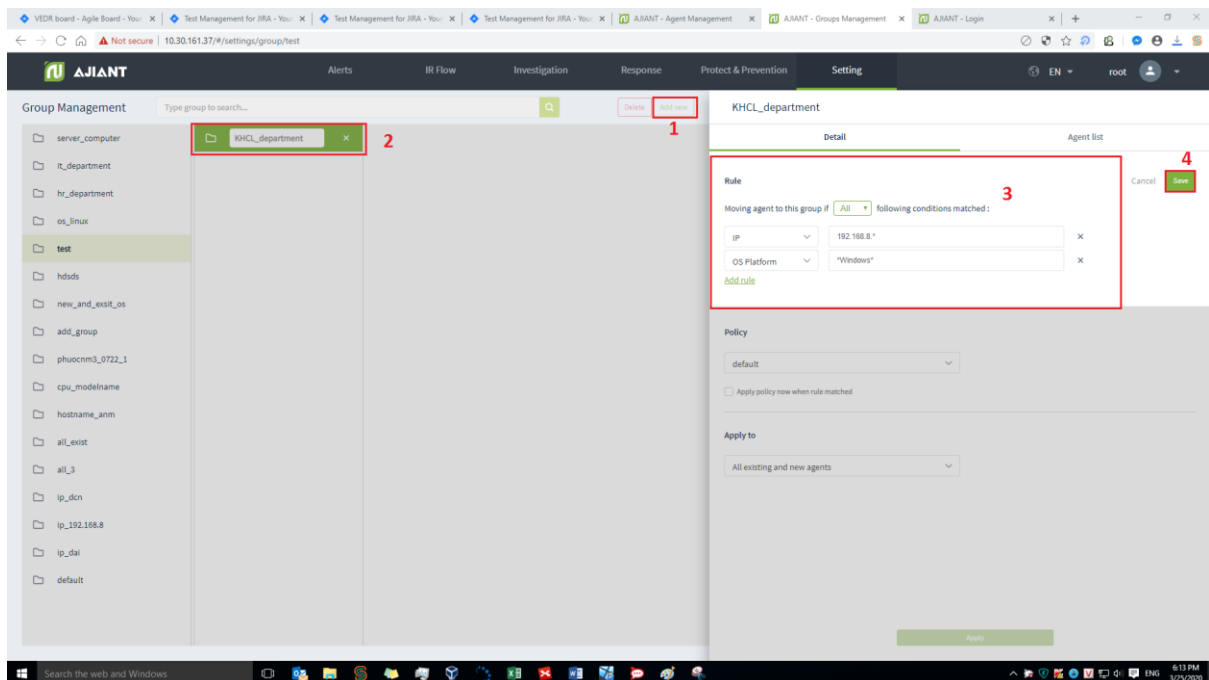
Nếu tạo mới nhóm ở danh sách nhóm gốc, click button “Add new” góc phải màn hình hoặc hover vào cuối danh sách nhóm gốc trên màn hình, click Add new



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 “Add new” trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click “Add new”



- 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



- Bước 3: lựa chọn policy và loại agent sẽ apply policy nếu thỏa mãn rule

khcl_department

Detail

Agent list

Rule

Moving agent to this group if

All

following conditions matched :

IP

192.168.8.*

OS

Windows

Policy

test

5

☐ Apply policy now when rule matched

Apply to

All existing agents

6

Apply

7

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

khcl_department ×

Detail

Agent list

Rule  1

Moving agent to this group if All following conditions matched :

IP	192.168.8.*
OS	*Windows*

Chỉnh sửa luật của nhóm sau đó click Save

khcl_department ×

Detail

Agent list

Rule

Moving agent to this group if All following conditions matched :

IP ▼ 192.168.8.* ×

OS Platform ▼ *Windows* ×

[Add rule](#)

2

Cancel

Save

3

Sau đó có thể chỉnh sửa ở mục “Policy” và “Apply to” rồi click Apply



Lưu ý:

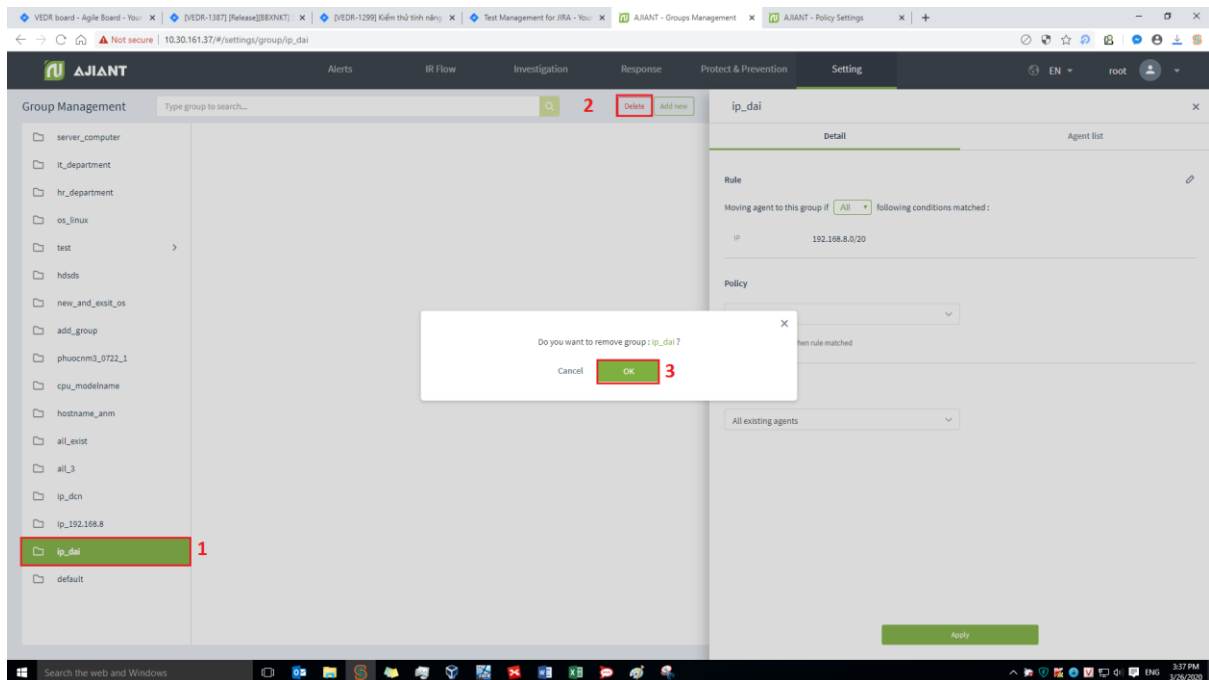
- Trường hợp sửa các thành phần của nhóm (Rule, Policy hoặc Apply to) sau đó ko click Apply thì nội dung chỉnh sửa đã được lưu lại, nhưng không cập nhật Agent list. Với các Agent cài mới thì xử lý như sau:
 - + Chuyển nhóm: phụ thuộc Agent mới có được chọn ở mục “Apply to” hay không, nếu được chọn sẽ 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 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



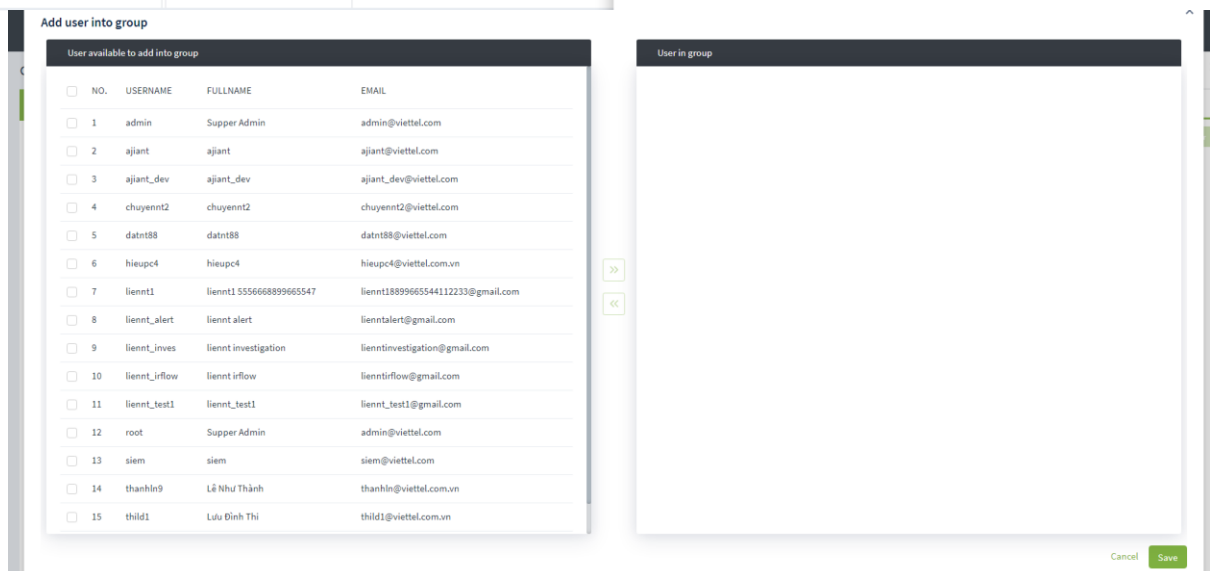
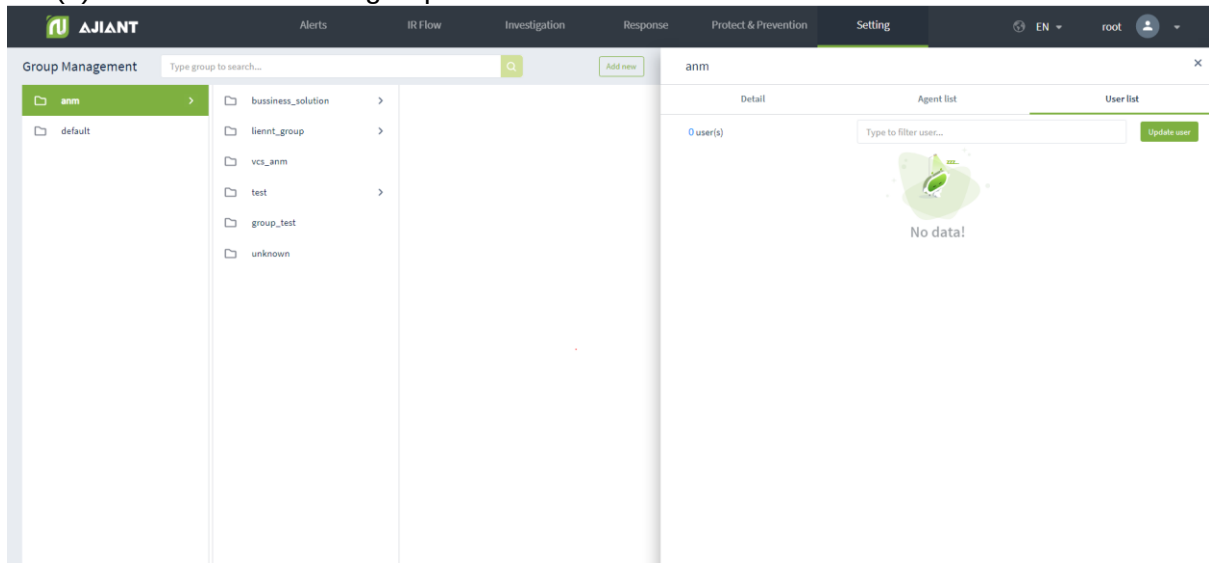
Để xóa Agent khỏi nhóm thì click vào tab Agent list, click icon “x” để xóa agent khỏi nhóm. Sau khi xóa agent khỏi nhóm thì agent được chuyển về nhóm mặc định: “default”, policy giữ nguyên

os_linux						
Detail			Agent list			
7 agent(s)		Type to filter agent...		View column		
NO.	AGENT ID	HOSTNAME	STATUS	POLICY		
1	CFF901BC683AE08EA4077690...	thedv1-VirtualBox	Offline	default		X
2	68555CF02D2580563A8F12B4...	ubuntu18x64chuyennt	Offline	thanhln0910		X
3	B6900069868F655D59F4C2B8...	chuyennt2-ViettelOS	Offline	thanhln_demo		X
4	EA3892E4CBB2887FB04DF59E...	chuyennt2-ViettelOS-test	Offline	default		X
5	8C7C096A104B60A07FC4BB87...	thanhln9-VirtualBox	Offline	thanhln_demo		X
6	C9FFB3E6991525CE5EA6D360...	test-windows7	Offline	thanhln0910		X
7	C8B5960DEF7C9E832536930F...	chuyennt2-VirtualBox	Offline	default		X

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

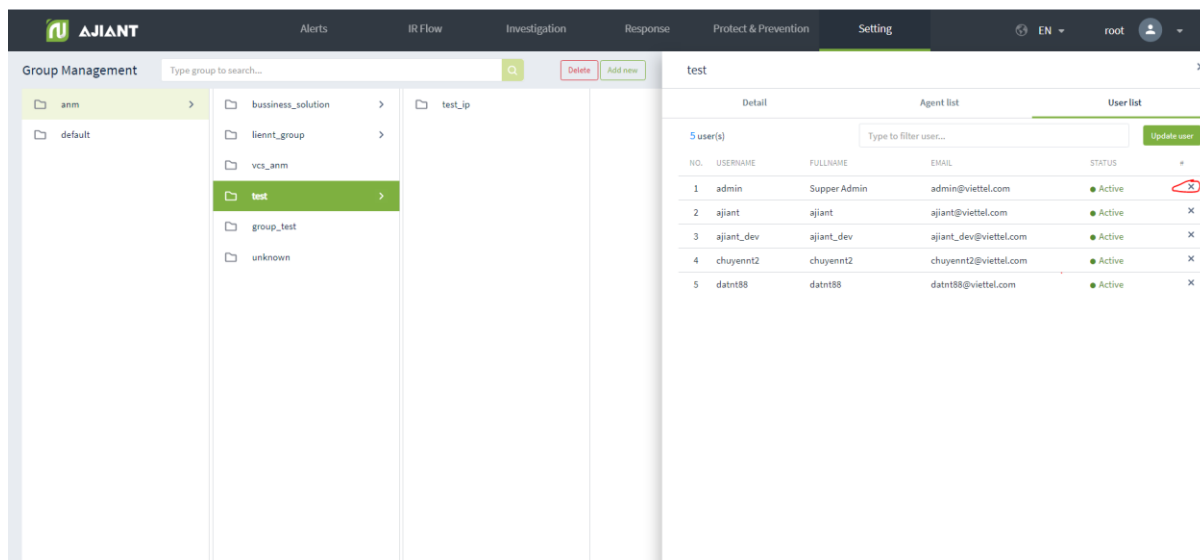
(6) Thêm mới user vào group



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

(7) Xóa user



3.8.4 Account Management

- Quản lý các tài khoản, quyền, nhóm quyền của hệ thống Portal

3.8.4.1 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:

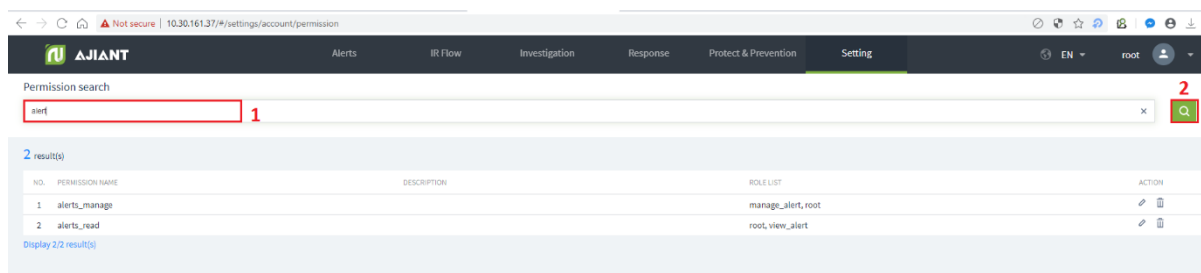
+ Quản lý các permission

+ Tìm kiếm permission

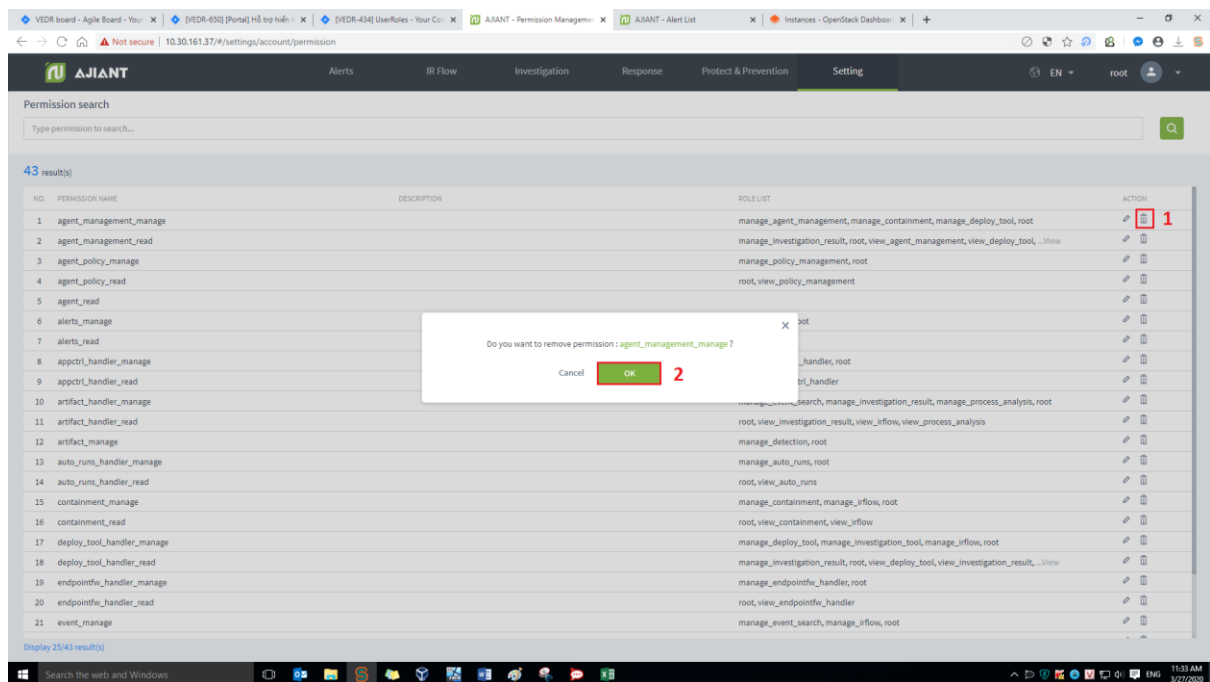
+ Xóa permission

(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 textbox Search > click Enter hoặc Search => hiển thị danh sách permission thỏa mãn



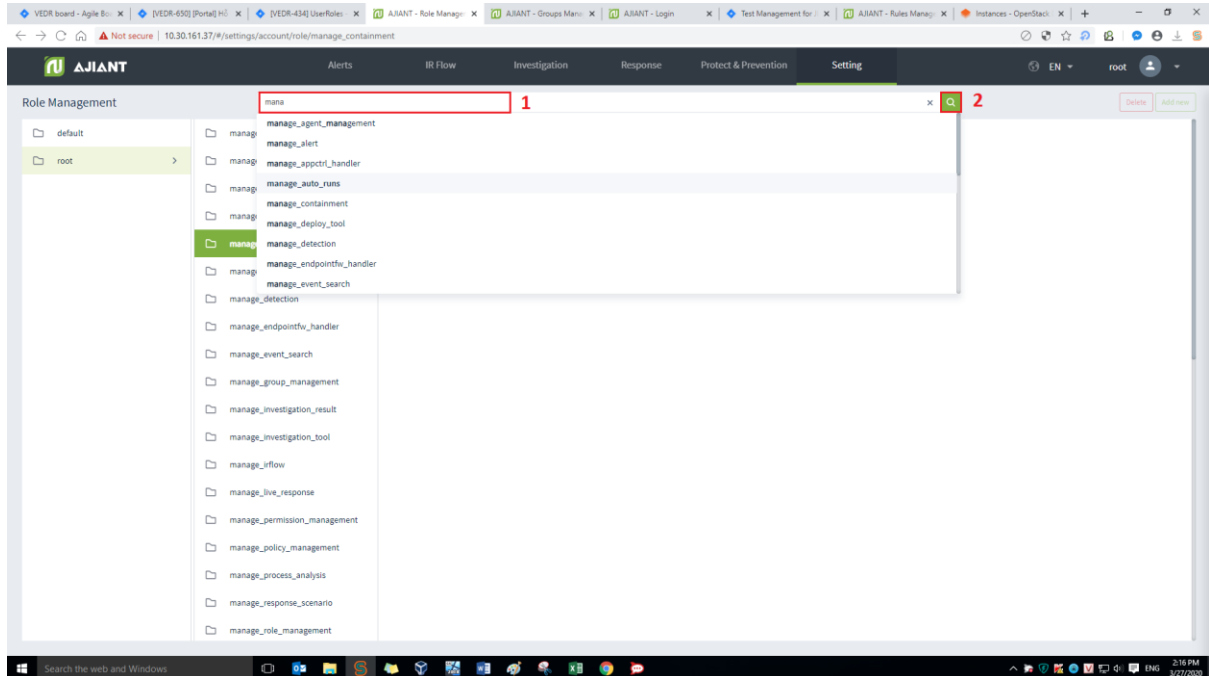
(3) Xóa permission: click icon Xóa > click OK trên màn hình confirm là xóa thành công



3.8.4.2 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”
 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 button Search

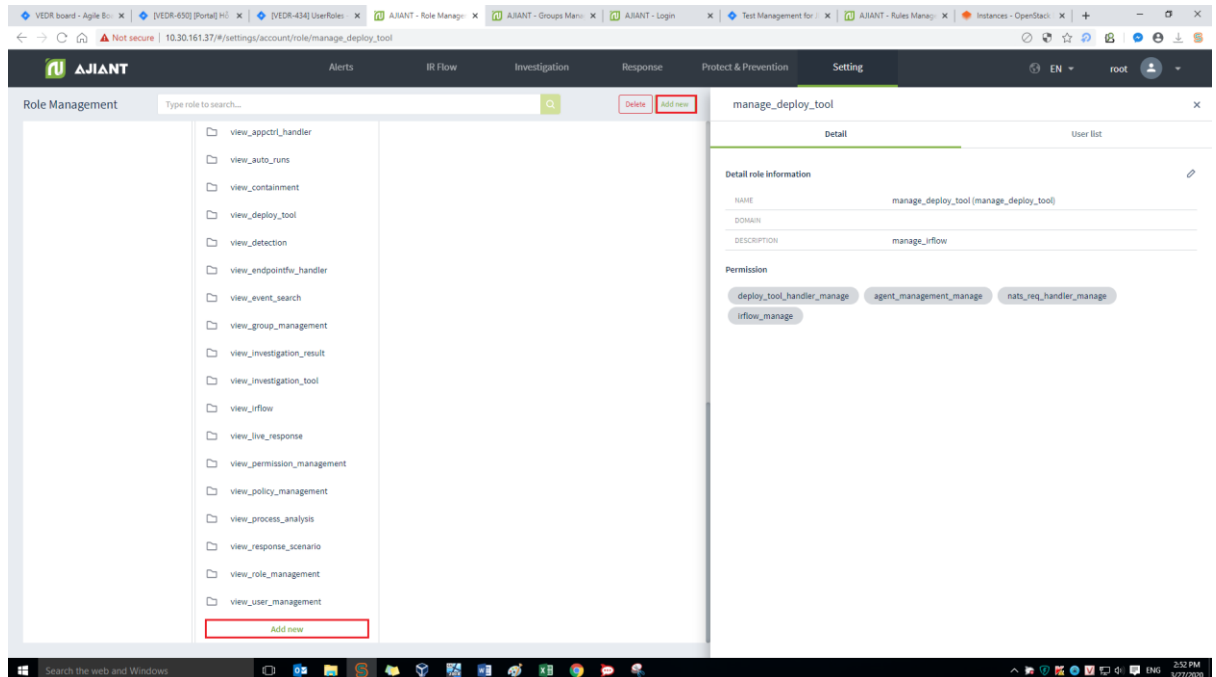


- + Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.
 - o Tab thông tin chi tiết hiển thị là Detail, dữ liệu của role bao gồm thông tin role và các permission của role đó
 - o Khi chọn tab User list là danh sách User chứa role
- + Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 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 thêm 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 thêm mới role cùng cấp
- + User đăng nhập thuộc group một hoặc nhiều con: có thể thêm 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.



- 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.

test
×

Detail
User list

1


Detail role information

NAMEtest (test)

DOMAIN

DESCRIPTIONtest

Permission

test
×

Detail
User list

Detail role information
CancelSave
3

Name
test

Domain

Description
test

Permission

agent_management_read × deploy_tool_handler_manage ×

2

auto_runs_handler_manage

auto_runs_handler_read

containment_manage

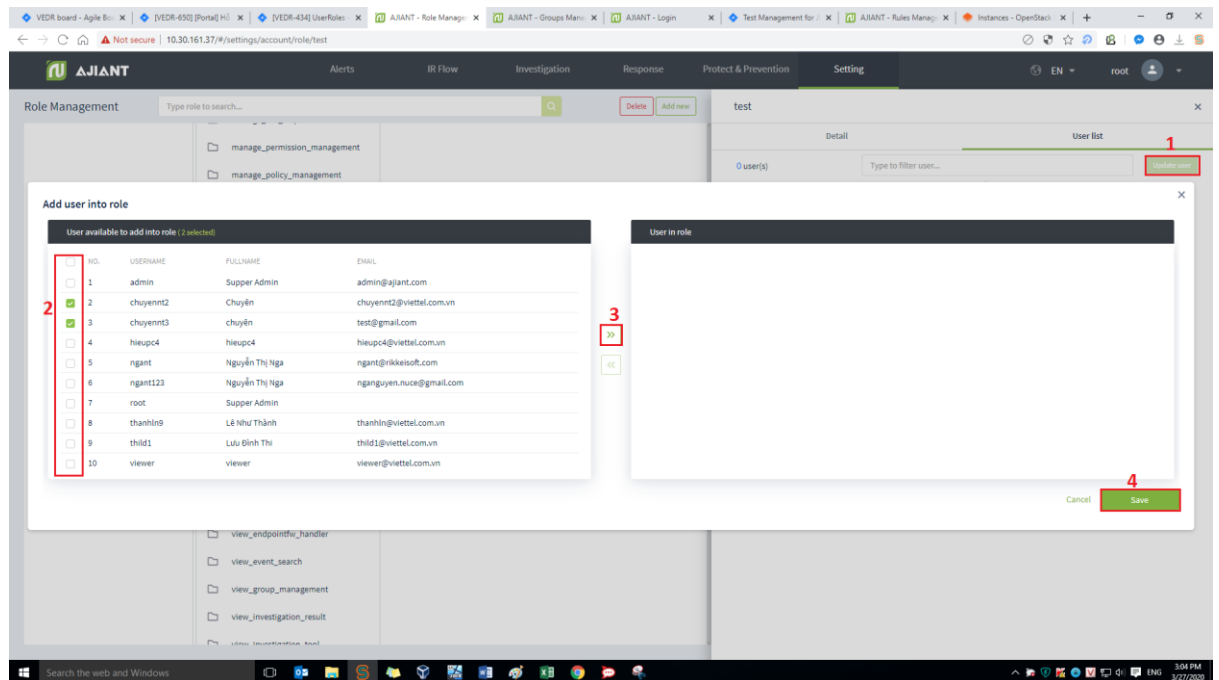
containment_read

deploy_tool_handler_read

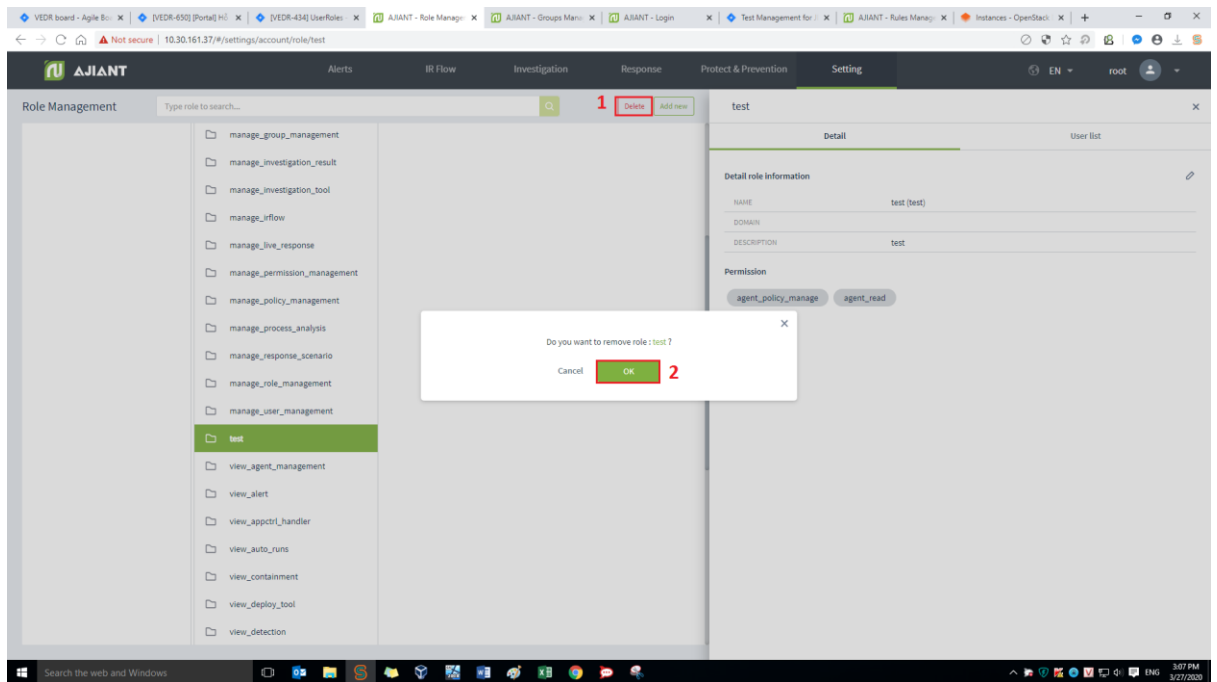
endpointfw_handler_manage

- Bước 3: Chuyển sang tab User list để thêm role vào danh sách role của User
- + User đăng nhập thuộc group root: Hiện 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



(4) Xóa role: click vào role cần xóa, chọn “Delete” > click OK trên màn hình confirm



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.

3.8.4.3 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

Tìm kiếm tài khoản

ng
ngant
ngant123

Nhập tài khoản

STT	TÊN ĐĂNG NHẬP	HỌ VÀ TÊN	EMAIL	TRẠNG THÁI	THAO TÁC
1	admin	Supper Admin	admin@ajiant.com	☒ Hoạt động	
2	chuyent2	Chuyên	chuyent2@viettel.com.vn	☒ Hoạt động	
3	hieupc4	hieupc4	hieupc4@viettel.com.vn	☒ Hoạt động	
4	ngant	Nguyễn Thị Nga	ngant@rikasoft.com	☒ Hoạt động	
5	ngant123	Nguyễn Thị Nga	ngantuyen.nuce@gmail.com	☒ Hoạt động	
6	root	Supper Admin		☒ Hoạt động	
7	thanhin9	Lê Như Thành	thanhin@viettel.com.vn	☒ Hoạt động	
8	thid1	Lưu Đình Thi	thid1@viettel.com.vn	☒ Hoạt động	
9	viewer	viewer	viewer@viettel.com.vn	☒ Hoạt động	

Hiện thị 9/9 kết quả

(2) Thêm mới tài khoản: click “Add user” > Nhập thông tin vào form hiện lên > click “Next”

AJANT

Alerts IR Flow Investigation Response Setting

EN liennt_inflow

User search

Type to search ...

16 result(s)

Add user

Information Role Group

Username

Fullname

Email

Password

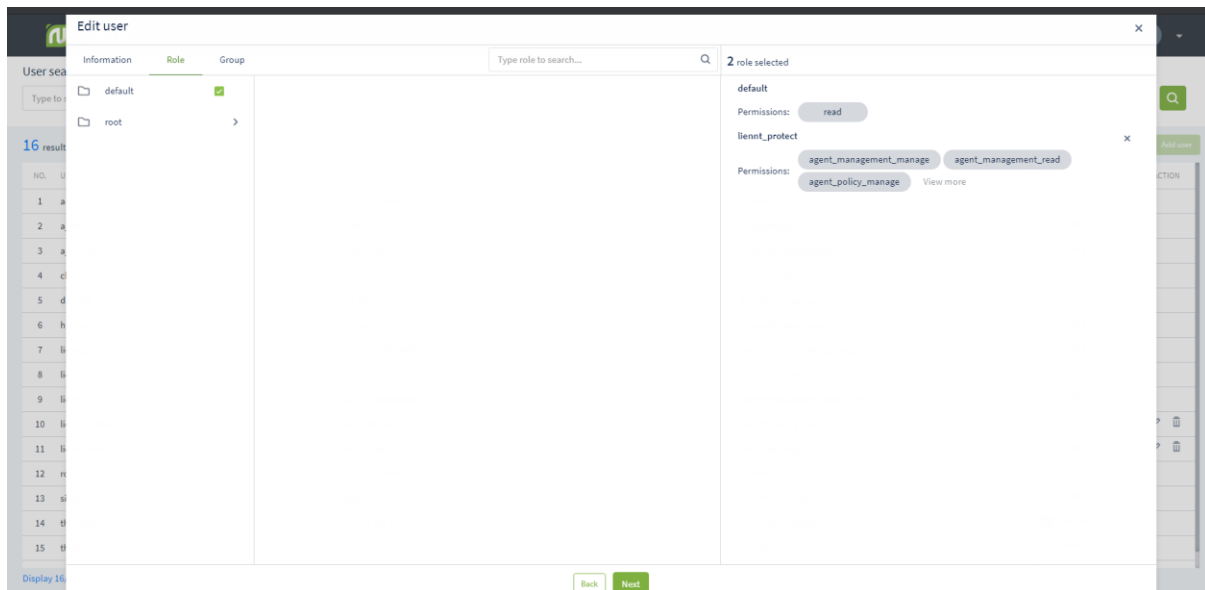
Status ☒ Active ☐ Inactive

Cancel Next

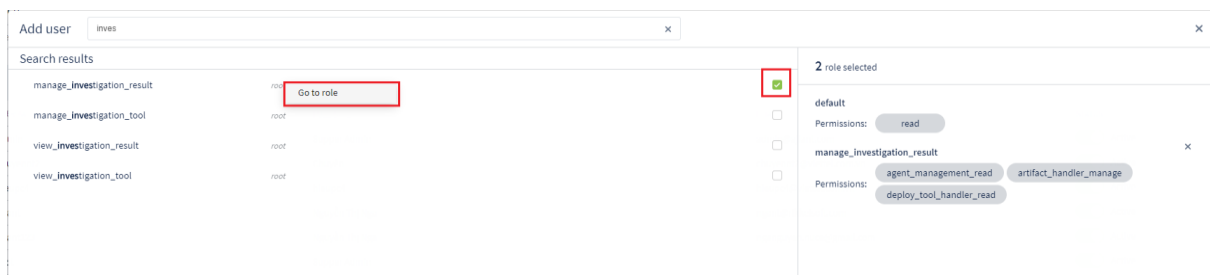
NO.	USERNAME	STATUS	ACTION
1	admin	☒ Active	
2	ajiant	☒ Active	
3	ajiant_dev	☒ Active	
4	chuyent2	☒ Active	
5	datnt88	☒ Active	
6	hieupc4	☒ Active	
7	liennt1	☒ Active	
8	liennt_alert	☒ Active	
9	liennt_inves	☒ Active	
10	liennt_inflow	☒ Active	
11	liennt_test1	☒ Active	
12	root	☒ Active	
13	siem	☒ Active	
14	thanhin9	☒ Active	
15	thid1	☒ Active	

Display 16/36 result(s)

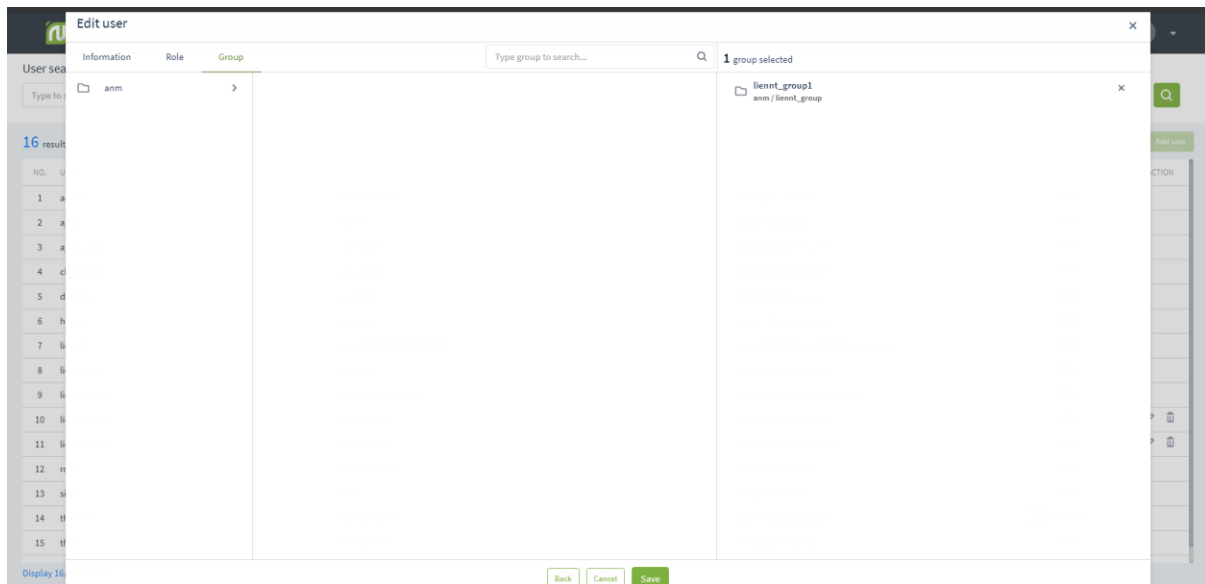
- Lựa chọn role (nhóm quyền) sẽ gán cho tài khoản, sau đó click “next”
- Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó
 - + User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống
 - + User đăng nhập thuộc Role default: Hiển thị Role default
 - + User đăng nhập thuộc Role cha: Hiển thị tất cả Role thuộc của user đang login và group con tương ứng
 - + User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login



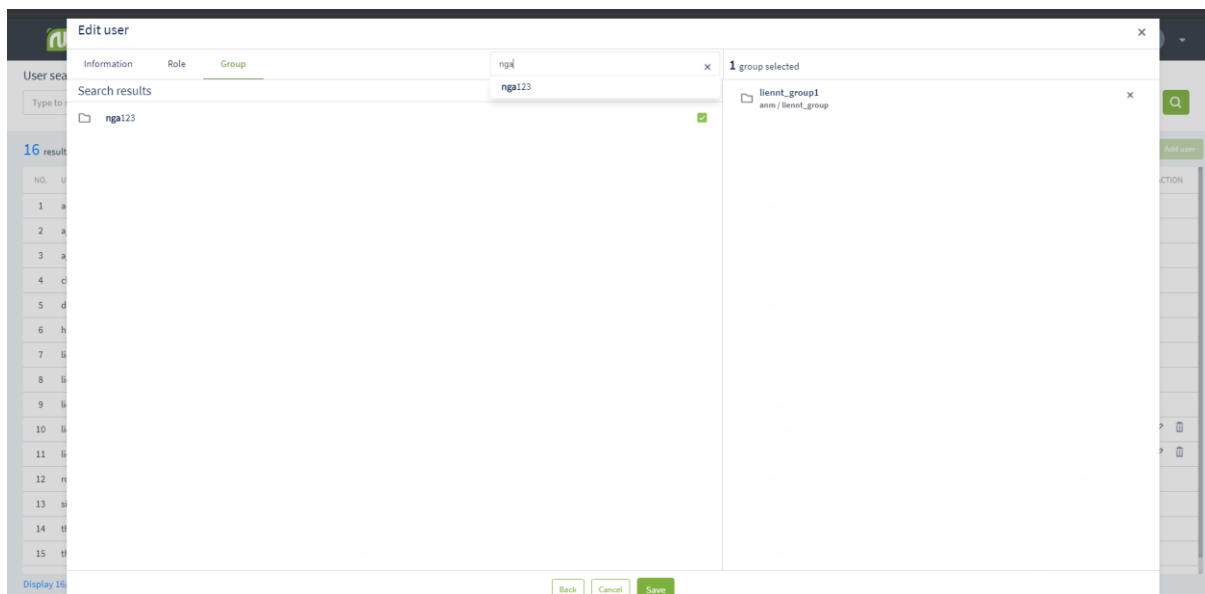
- Trên màn hình add role cho User, có thể tìm kiếm các role tương tự phần tìm kiếm tài khoản, sau khi nhập các ký tự tìm kiếm vào textbox “Search” > click icon Search hoặc Enter hiện màn hình các role thỏa mãn điều kiện tìm kiếm.



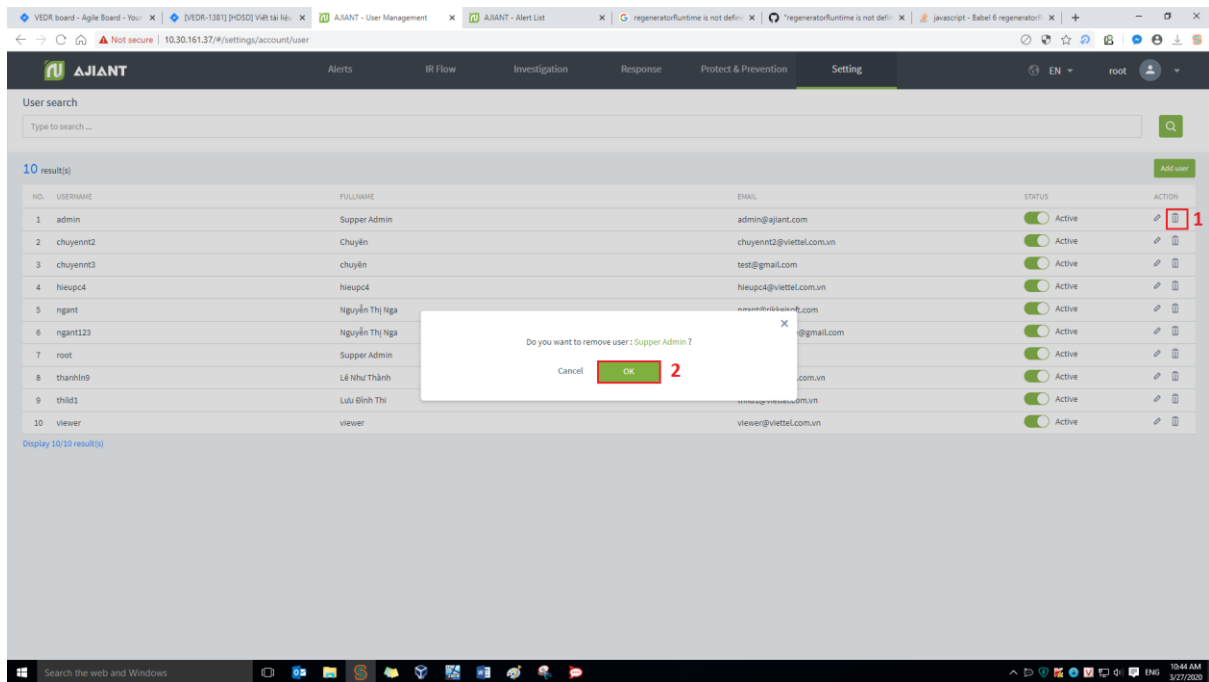
- Click chọn checkbox tương ứng với role cần thêm, sau đó click “Go to role” để về màn hình danh sách role ban đầu, sau đó click “Create” để tạo tài khoản.
- Lưu ý: Tài khoản đang đăng nhập tạo 1 tài khoản mới chỉ tạo được các tài khoản chứa các role con thuộc danh sách role mà tài khoản đang đăng nhập 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: Hiện thị tất cả Group trong hệ thống
 - + User đăng nhập thuộc group default: Hiện thị group default
 - + User đăng nhập thuộc group cha: Hiện thị Group thuộc group của user đang login và group con tương ứng
 - + User đăng nhập thuộc group một hoặc nhiều con: Hiện thị tất cả Group thuộc group của user đang login



- 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.



- (3) Xóa tài khoản: click vào icon Xóa sau đó click OK trên màn hình confirm
- Kiểm tra hiển thị 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

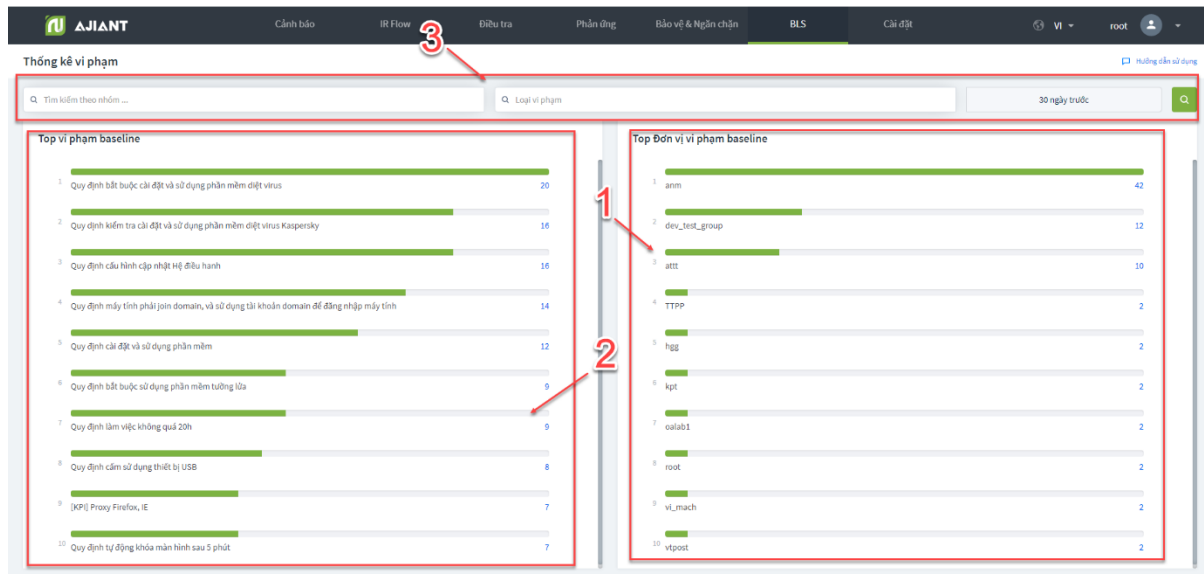


3.9 Màn hình BLS

3.9.1 Thống kê vi phạm (Violation statistic)

- 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 vị
 - + Xem danh sách các đơn vị vi phạm và danh sách vi phạm trong từng đơn vị
 - + Xem chi tiết của Agent
 - + Export vi phạm
 - + Report vi phạm
- Click vào tab BLS >> Thống kê vi phạm

3.9.1.1 Màn hình Thống kê vi phạm



- Hệ thống hỗ trợ thực hiện các tính năng:

(1) 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

(2) 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

(3) 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 đơn 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

3.9.1.2 Tab Loại vi phạm

Thống kê vi phạm

Loại vi phạm: Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus

Loại vi phạm	Đã xử lý	Chưa xử lý	Mất vi phạm	Đơn vị vi phạm
Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus	3 (22%)	11 (79%)	14 (84%)	17

Hiện thị 2/1 kết quả

Thống kê vi phạm baseline

Đơn vị	Online trong ngày	Online trong 30 ngày gần nhất	Đã xử lý	Chưa xử lý	Mất vi phạm	Lỗi vi phạm
root	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2
default	1 (9%)	11	2 (17%)	10 (83%)	12 (100%)	0
anm	2 (50%)	4	0 (0%)	4 (100%)	4 (100%)	12
unknown	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
lannt_group2.1	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
ajiant_dev	0 (0%)	2	0 (0%)	2 (100%)	2 (100%)	0
dev_test_group	1 (50%)	2	0 (0%)	3 (100%)	3 (150%)	10
kpt	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2
vt	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vt_khoi_khcn_hgd_tt_kh_vsa_marketing	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
OS31	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vt_cskh-dng	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
oku2	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vt_vdi_normal	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vt_khoi_cntt	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
ybi	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
Tổng	4 (100%)	17	2 (12%)	15 (88%)	14 (82%)	44

Hiện thị 50/58 kết quả

- Hệ thống hỗ trợ thực hiện các tính năng:

(1) Chọn link Top vi phạm: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm

(2) Cây dữ liệu đơn vị của hệ thống

Hiện 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

(3) 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

The screenshot shows the AJIANT security dashboard. On the left, there's a 'Violation statistic' panel with a tree view of units (root, test, server, no_group, kdi, kpt, thi_truong, anm, default). The main panel displays a 'Violation statistic baseline' table with columns for Violation type, Unit, Resolved, and Unresolved. Below this, there's a 'List computers and units baseline violation' panel showing a list of computers and their associated violations. The table includes columns for Computer, Agent ID, IP Address, Domain, Group, Resolved, and Detail.

Violation type	Unit	Resolved	Unresolved
Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus	anm	3 (25%)	9 (75%)
Quy định kiểm tra cài đặt và sử dụng phần mềm diệt virus Kaspersky	anm	4 (31%)	9 (89%)
Quy định cấu hình cập nhật Hệ điều hành	anm	1 (11%)	8 (89%)
Quy định máy tính phải join domain, và sử dụng tài khoản domain để đăng nhập máy tính	anm	1 (11%)	8 (89%)
Quy định cài đặt và sử dụng phần mềm diệt virus	anm	1 (13%)	7 (88%)
Quy định làm việc không quá 20h	anm	0 (0%)	3 (100%)
Quy định bắt buộc sử dụng phần mềm tường lửa	anm	0 (0%)	5 (100%)
Quy định cấm sử dụng thiết bị USB	anm	2 (40%)	3 (60%)
[XP] Proxy Firefox, IE	anm	1 (33%)	2 (67%)
Quy định tự động khóa màn hình sau 5 phút	anm	3 (50%)	3 (50%)
Quy định nghiêm cấm kết nối trực tiếp mạng Internet.	anm	2 (100%)	0 (0%)
Quy định nghiêm cấm lưu trữ mật khẩu trên trình duyệt	anm	0 (0%)	3 (100%)
Quy định bắt buộc cập nhật phần mềm diệt virus	anm	1 (50%)	1 (50%)

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)

The screenshot shows the AJIANT security dashboard with the 'Detail information' panel expanded. It displays detailed information for a specific computer, including its name, agent ID, IP address, domain, group, and a list of violations. The 'Resolved' column shows the status of each violation.

Computer	Agent ID	IP Address	Domain	Group	Resolved	Detail
WIN7-32BIT-PC	5EF765BF9CE6221DA50F787ACB52C48AE32FB00C			anm	Not yet	Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus
HUYHY-PC	1D15A98115CDFE8BB1DAD98B1D0575221BF958D3				Not resolved yet	Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus
thanhlinh-VirtualBox	8C7C096A104B6A07FC4BB87299C2219639FA				Not resolved yet	Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus
DESKTOP-HHN2B1Q	59221A0A9179C465DCD95A4E6F38D2E78E2126DF				Not resolved yet	Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus

(4) 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

3.9.1.3 Tab Đơn vị

The screenshot shows the 'Đơn vị' (Unit) tab in the Viettel Security interface. The interface includes a sidebar with a tree view of units, a search bar, and a table of violation statistics. Red annotations 1, 2, 3, and 4 highlight specific features: 1 points to the 'Loại vi phạm' dropdown, 2 points to the unit selection tree, 3 points to the 'Đơn vị' tab, and 4 points to the search bar.

Đơn vị	ONLINE TRONG NGÀY	ONLINE TRONG 30 NGÀY GẦN NHẤT	ĐÃ XỬ LÝ	CHƯA XỬ LÝ	MÃ VI PHẠM	LƯỢT VI PHẠM
root	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2
default	1 (0%)	11	2 (17%)	10 (83%)	12 (100%)	0
anm	2 (50%)	4	0 (0%)	4 (100%)	4 (100%)	12
unknown	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
lennt_group2.1	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
ajiant_dev	0 (0%)	2	0 (0%)	2 (100%)	2 (100%)	0
dev_test_group	1 (50%)	2	0 (0%)	3 (100%)	3 (100%)	10
kpt	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2
vtt	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vacan@hcn_hgd_tt_kh_vsa_marketing	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
OS11	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vtt_cskh-dng	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
oku2	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vtt_vdi_normal	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
vtt_khoi_cott	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1
ybi	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1

- Hệ thống hỗ trợ thực hiện các tính năng:
 - (1) Chọn link Top đơn vị: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm
 - (2) 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
 - (3) 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 vi phạm)

The screenshot displays the AJANT security dashboard. The top navigation bar includes tabs for Alerts, IR Flow, Investigation, Response, Protect & Prevention, BLS, and Setting. The main content area is divided into three sections: Violation statistic, Violation information, and Detail information.

Violation statistic: Shows a tree view of groups (root, test, server, no_group, kdl, kpt, thi_truong, ann, default) and a list of violation types (UNIT, root, default, ann, unknown, lennt_group2.1, ajant_dev, dev_test_group, kpt, vtt, vtt_khoi_khcn_hgd_tt_kh, vtt_cakh-dng, vtt_vdi_normal, vtt_khoi_cntt, ybi, bss, tsh, and a link to Display 50/62 result(s)).

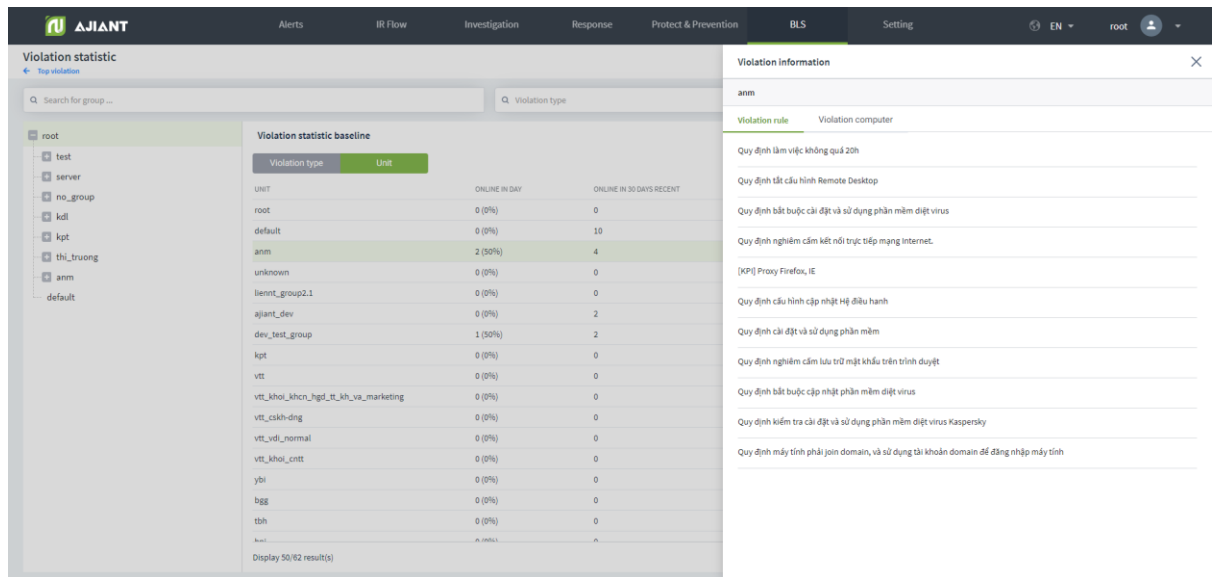
Violation information: A table listing violations with columns for Violation rule, Violation computer, and status. The table shows 14 violations, with the first one being 'Not resolved yet' and the others being 'Resolved'.

Detail information: A detailed view of a specific violation, showing fields for COMPUTER (ANM-CHUYENNT), AGENT ID (E65744E6BCF118CTD9AF21C7A0893D74489A8F05), IP ADDRESS, DOMAIN, GROUP (ann), and RESOLVED (Not yet). The detail section also includes a description of the violation and a list of related events.

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)

This screenshot is identical to the one above, showing the AJANT security dashboard with the same navigation tabs and content sections: Violation statistic, Violation information, and Detail information.

Chọn icon detail của cột violation rule trên danh sách: Hiển thị danh sách vi phạm của đơn vị



(4) 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

3.9.2 Thống kê phần mềm (Software statistic)

- 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

Software statistic

Search for group ... Search for software ... Installed Date & Time

root

- test
- server
- no_group
- kdl
- kpt
- thi_truong
- anm
- default

SOFTWARE NAME	NUMBER OF COMPUTERS	NUMBER OF UNITS
☐ 7-Zip 16.04	1	1
☐ Version 16.04	1	1
☐ 7-Zip 19.00	17	5
☐ Version 19.00.00.0	17	5
☐ 7-Zip 19.00 (x64)	1	1
☐ Version 19.00	1	1
☐ Adobe Acrobat Reader DC	12	5
☐ Version 20.006.20042	12	5
☐ Adobe Acrobat Reader DC (19.012.20036)	15	5
☐ Version 20.006.20042	15	5
☐ Adobe Acrobat Reader DC (19.012.20040)	15	4
☐ Version 20.006.20042	15	4
☐ Adobe Acrobat Reader DC (19.021.20048)	11	2
☐ Version 20.006.20042	11	2
☐ Adobe Acrobat Reader DC (19.021.20049)	15	5
☐ Version 20.006.20042	15	5
☐ Adobe Acrobat Reader DC (19.021.20056)	16	5

Display 50/388 result(s)

Export

- Hệ thống hỗ trợ thực hiện các tính năng:

(1) 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

(2) Danh sách phần mềm

Mỗi phần mềm được hiển thị các thông tin chung gồm: Software name, number of computer, number of unit

Software statistic

Search for group ... Search for software ... Installed Date & Time

root

- test
- server
- no_group
- kdl
- kpt
- thi_truong
- anm
- default

SOFTWARE NAME	NUMBER OF COMPUTERS	NUMBER OF UNITS
☐ 7-Zip 16.04	1	1
☐ Version 16.04	1	1
☒ 7-Zip 19.00	17	5
☐ Version 19.00.00.0	17	5
☐ 7-Zip 19.00 (x64)	1	1
☐ Version 19.00	1	1
☐ Adobe Acrobat Reader DC	12	5
☐ Version 20.006.20042	12	5
☐ Adobe Acrobat Reader DC (19.012.20036)	15	5
☐ Version 20.006.20042	15	5
☐ Adobe Acrobat Reader DC (19.012.20040)	15	4
☐ Version 20.006.20042	15	4
☐ Adobe Acrobat Reader DC (19.021.20048)	11	2
☐ Version 20.006.20042	11	2
☐ Adobe Acrobat Reader DC (19.021.20049)	15	5
☐ Version 20.006.20042	15	5
☐ Adobe Acrobat Reader DC (19.021.20056)	16	5

Display 50/388 result(s)

Export

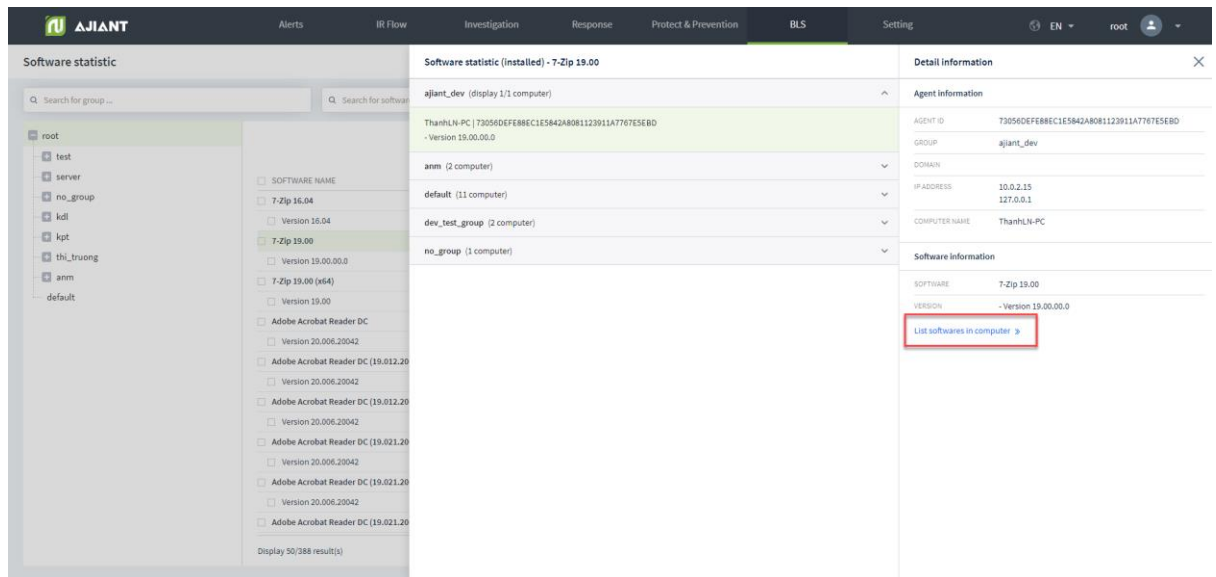
Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị bao gồm Tên đơn vị, Tên máy tính|Agent ID, Version

The screenshot shows the 'Software statistic' page in the AJIANT interface. On the left, there's a tree view of groups: root, test, server, no_group, kdl, kpt, thi_truong, anm, and default. The 'anm' group is selected. In the center, a list of software is displayed with checkboxes. The '7-Zip 19.00' software is highlighted. On the right, a popup titled 'Software statistic (installed) - 7-Zip 19.00' shows a list of computers where this software is installed. The first entry is 'ajiant_dev (display 1/1 computer)'.

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)

This screenshot shows the same 'Software statistic' page, but with the 'Detail information' popup open for the selected computer. The popup is divided into three sections: 'Agent information', 'Software information', and 'List softwares in computer'. The 'Agent information' section shows details like Agent ID, Group, Domain, IP Address, and Computer Name. The 'Software information' section shows the software name '7-Zip 19.00' and its version. The 'List softwares in computer' section has a link to view all installed software on that computer.

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



(3) 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

(4) Export

Chọn Export: Hệ thống sẽ download file Export có dữ liệu giống với dữ liệu đang hiển thị trên màn hình

3.10 Rules Correlation

3.10.1 Danh sách hiển thị

- Chức năng cho phép người dùng 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

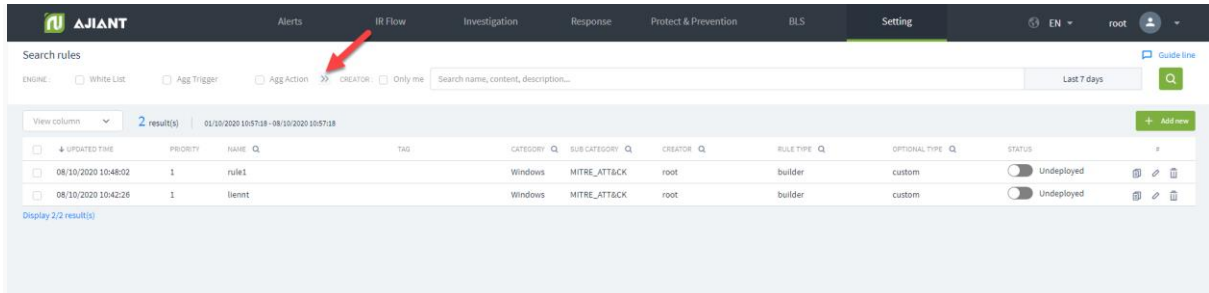
+ Bộ lọc FITTER bao gồm:

- 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

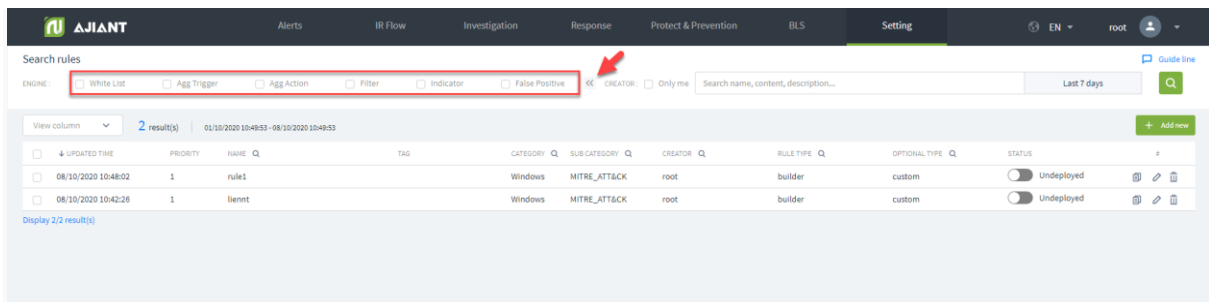
Lọc theo Engine

- Bước 1: Chọn 1 hoặc nhiều Engine mặc định



Màn hình tìm kiếm rule

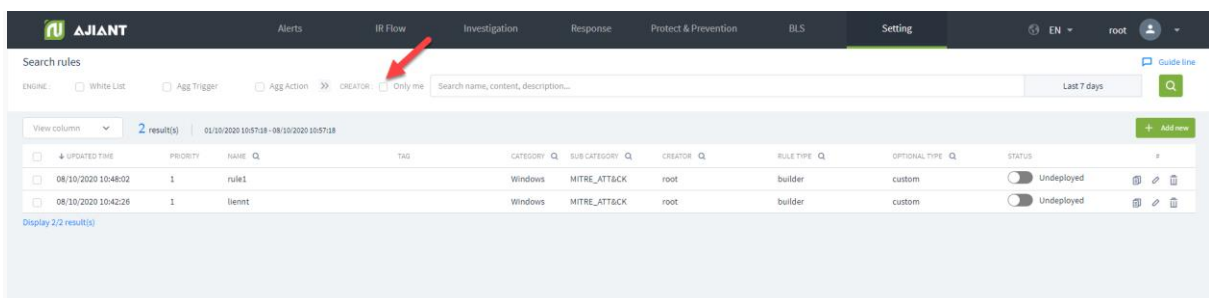
- Bước 2: Chọn Mở rộng để thêm các Engine cần lọc.



Màn hình mở rộng các điều kiện tìm kiếm rule

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

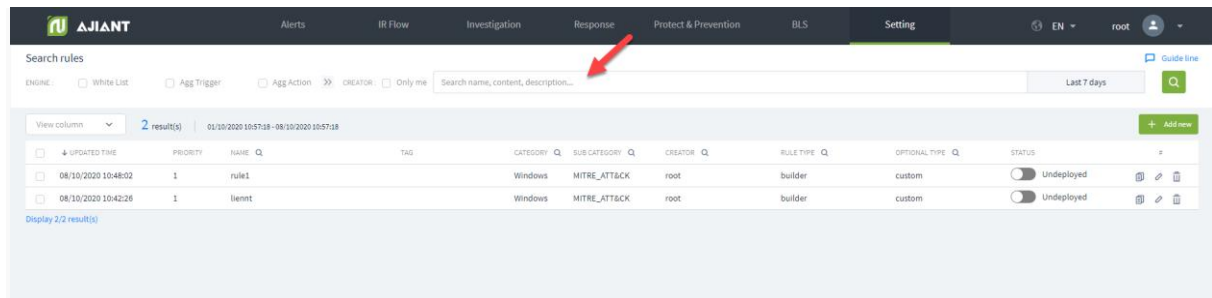


Màn hình lọc theo Creator

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 4: Nhập Name, content, description muốn search vào text box



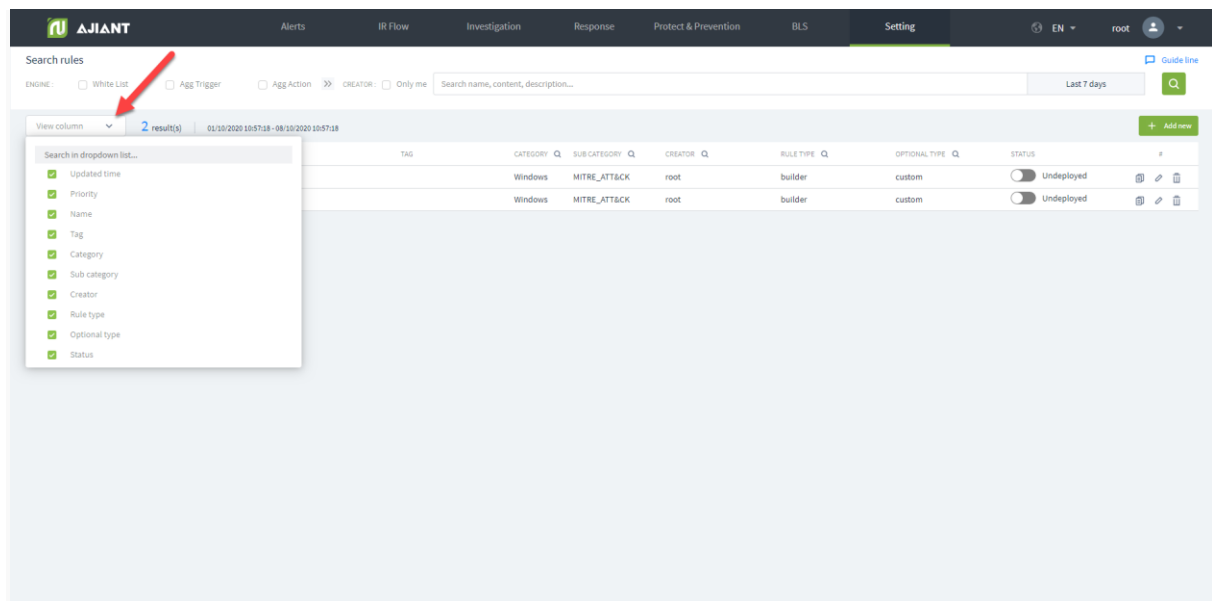
- Bước 5: Nhập thông tin cần tìm kiếm.
- Bước 6: Nhấn Search để hiển thị kết quả tìm kiếm.

Chọn cột

Cho phép người dùng lựa chọn các cột hiển thị trên màn hình correlation.

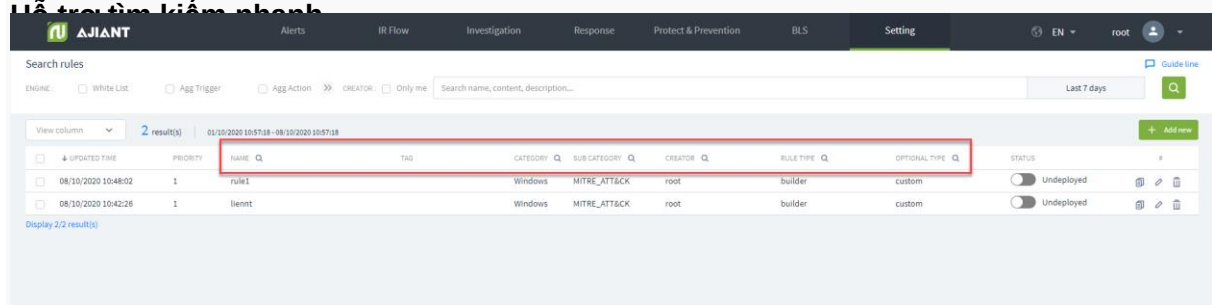
Các bước thực hiện:

- Bước 1: Click vào combo box View column. Màn hình hiển thị danh sách lựa chọn các cột ở dạng check box.
- Bước 2: Click Chọn vào những tên cột muốn hiển thị.



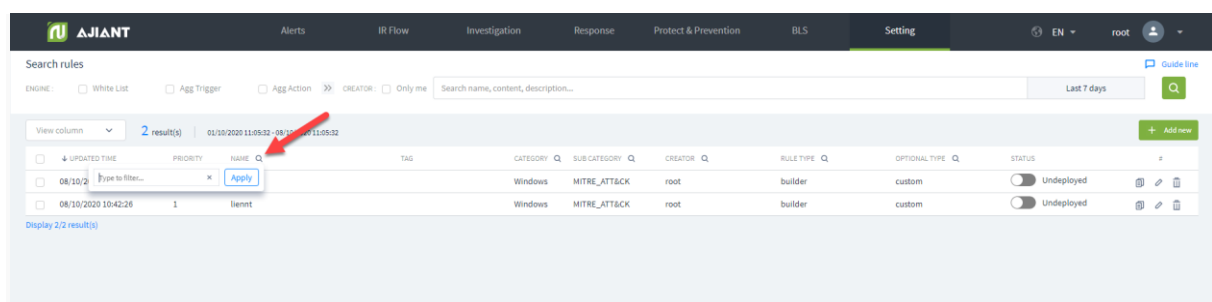
Màn hình Tùy chọn hiển thị thêm cột

Hỗ trợ tìm kiếm nhanh



Tìm kiếm theo tên rule

- Bước 1: Click icon  để hiển thị thanh tìm kiếm



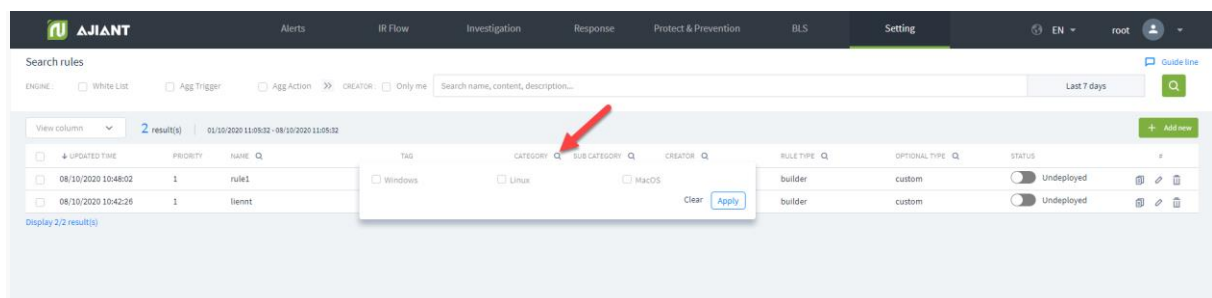
Màn hình tìm kiếm nhanh theo tên rule

- Bước 2: Nhập tên rules muốn tìm kiếm
- Bước 3: Nhấn Enter để hiển thị kết quả tìm kiếm.

Tìm kiếm theo Category

Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Windows, Linux, MacOS.

- Bước 1: Click icon  để hiển thị danh sách loại Category.



Màn hình tìm kiếm nhanh theo lo theo **Category**

- Bước 2: Chọn category muốn tìm kiếm
- Bước 3: Click Apply

Tìm kiếm Sub Category

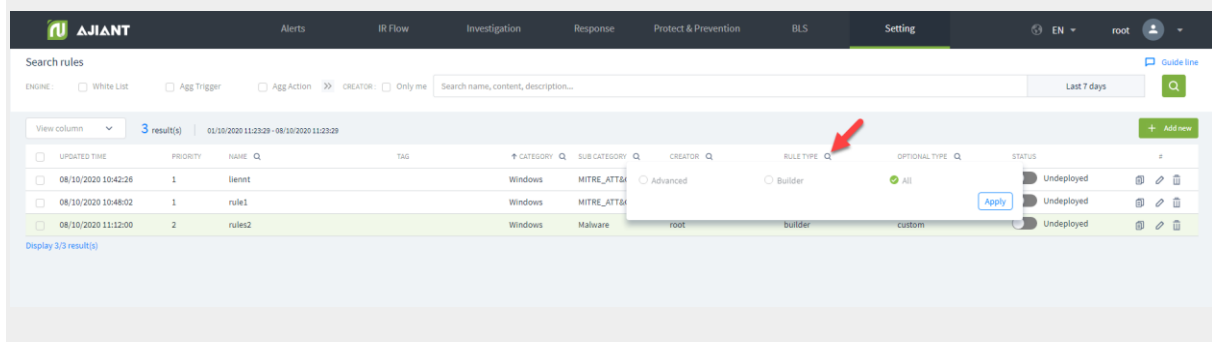
Hỗ trợ tìm kiếm nhanh theo loại triển khai, gồm 3 loại mặc định là: Metre ATT&CK, Malware, Suspicious Behaviour

- Bước 1: Click icon  để hiển thị thanh tìm kiếm
- Bước 2: Chọn sub category muốn tìm kiếm
- Bước 3: Click Apply

Tìm kiếm Creator

- Bước 1: Click icon  để hiển thị thanh tìm kiếm
- Bước 2: Nhập tên người tạo muốn tìm kiếm
- Bước 3: Click Apply

Tìm kiếm Rule type

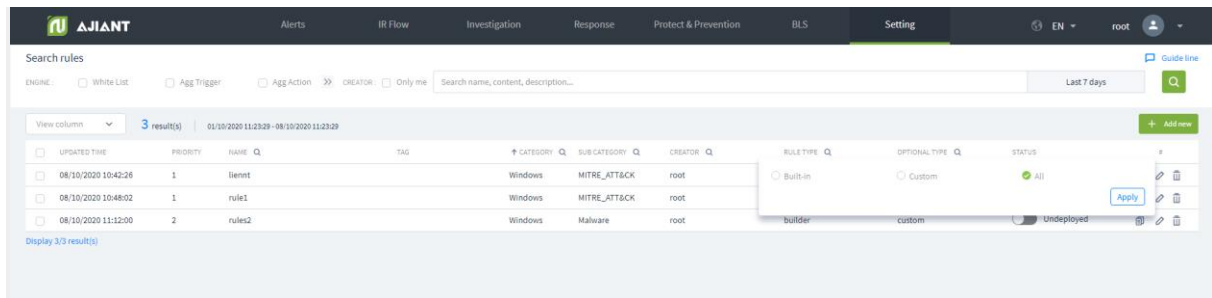


Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Advanced, Builder, All.

- Bước 1: Click icon  để hiển thị danh sách Rule type.
- Bước 2: Click vào Rule type muốn tìm kiếm
- Bước 3: Click Apply

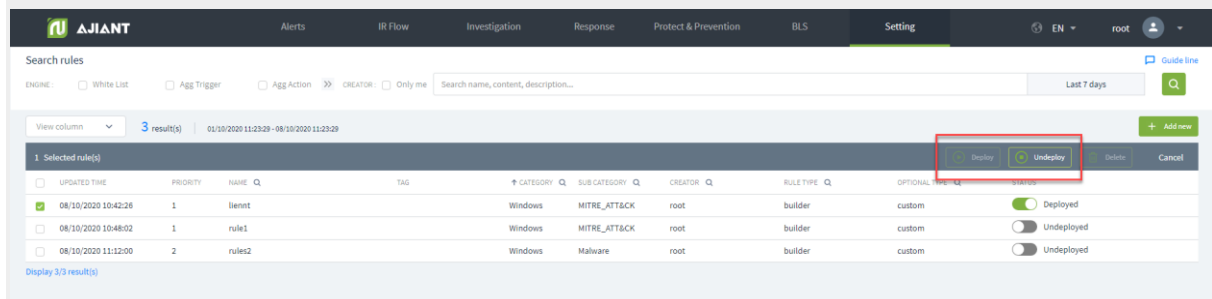
Tìm kiếm Optional type

Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Built-in, Custom, All.

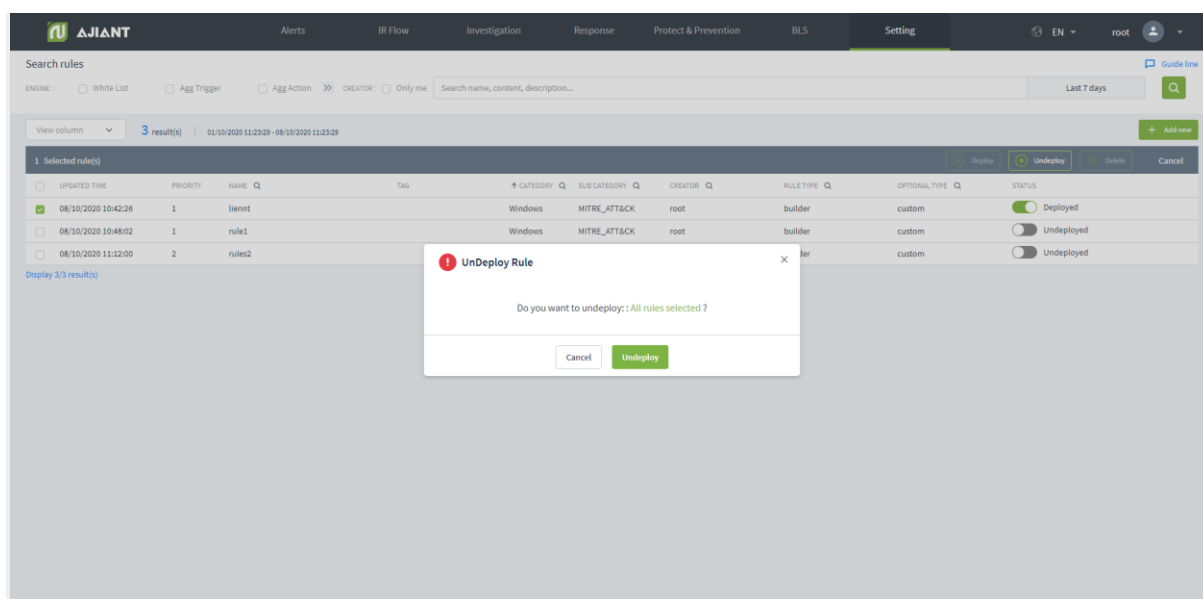


- Bước 1: Click icon  để hiển thị danh sách Optional type
- Bước 2: Click Optional type muốn tìm kiếm
- Bước 3: Click Apply

Hỗ trợ Deploy/Undeploy cho nhiều Rules



- Bước 1: Click vào nhiều check box có cùng trạng thái là Deploy hoặc Undeploy
- Bước 2: Click vào button Deploy/Undeploy
- Bước 3: Chọn Deploy/Undeploy trên popup hiển thị để thực hiện Deploy/Undeploy



3.10.2 Thêm mới Rules Correlation

- 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 thỏa 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 thỏa mãn số lượng từ đó sinh ra alert.
 - Function: Là các hàm. Lưu ý: Với các 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 thỏa mãn một chuỗi regex.
 - Bên trái toán tử: Tên trường cần kiểm tra.
 - Bên phải toán tử: Chuỗi regex.

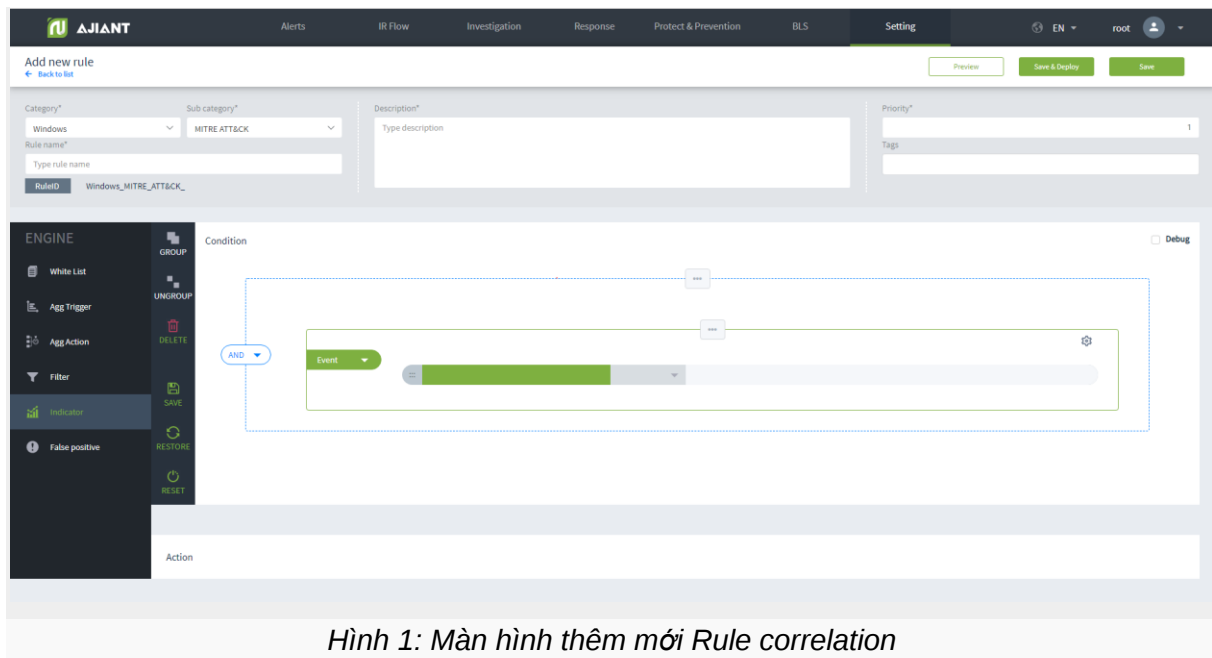
- Cấu hình thời gian: Kiểm tra điều kiện trong một khoảng thời gian , chỉ có ở các engine Agg_trigger ,Agg_action và Indicator.
- Count: Kiểm tra số event đếm được trong một khoảng thời gian có thỏa mãn điều kiện không.
- Nhóm/ Bỏ nhóm : Cho phép người dùng gộp hoặc tách nhanh các điều kiện trong một 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 BỎ 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

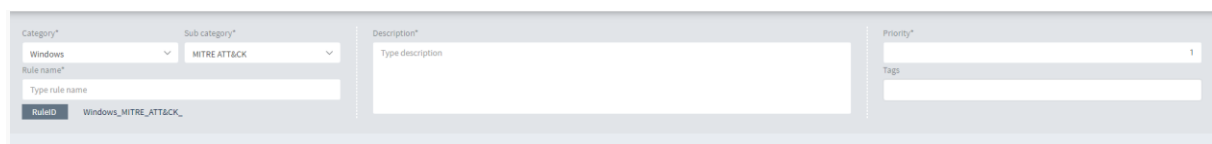
Các bước thêm mới rule correlation:

- Bước 1: Tại màn hình Correlation, Chọn button Thêm mới > Hệ thống hiển thị màn hình tạo mới rule



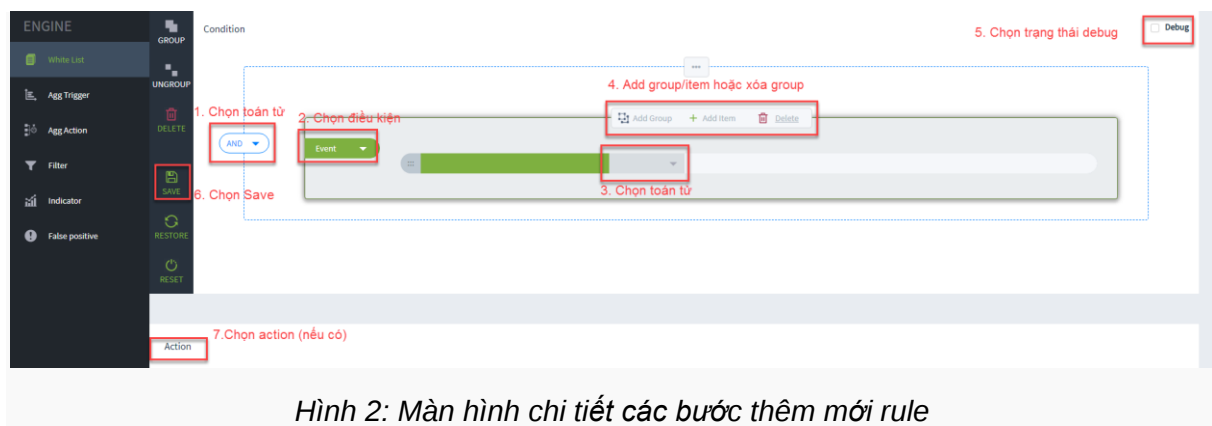
Hình 1: Màn hình thêm mới Rule correlation

- Bước 2: Nhập thông tin của rule.



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.



Hình 2: Màn hình chi tiết các bước thêm mới rule

- Bước 4: Nhấn Lưu để lưu lại điều kiện hoặc nhấn Huỷ 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:

- o Drop: Các log được đẩy vào thoả mãn điều kiện sẽ được loại bỏ khỏi luồng xử lý.
- o Chuyển sang aggregate: Log đẩy vào thoả mãn điều kiện sẽ được chuyển sang engine aggregate để tiếp tục xử lý.
- o 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.
- o 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 thêm.
- Bước 5.2: Click button Sửa để nhập giá trị cho trường
- Bước 5.3: Nhập giá trị cho trường
- Bước 5.4: Click Save
- Bước 5.5: Click button Add để thêm mới một trường vào alert.

Hình 3: Màn hình thêm mới hành động cho rule correlation

Để xoá hành động vừa tạo, click icon Xoá .

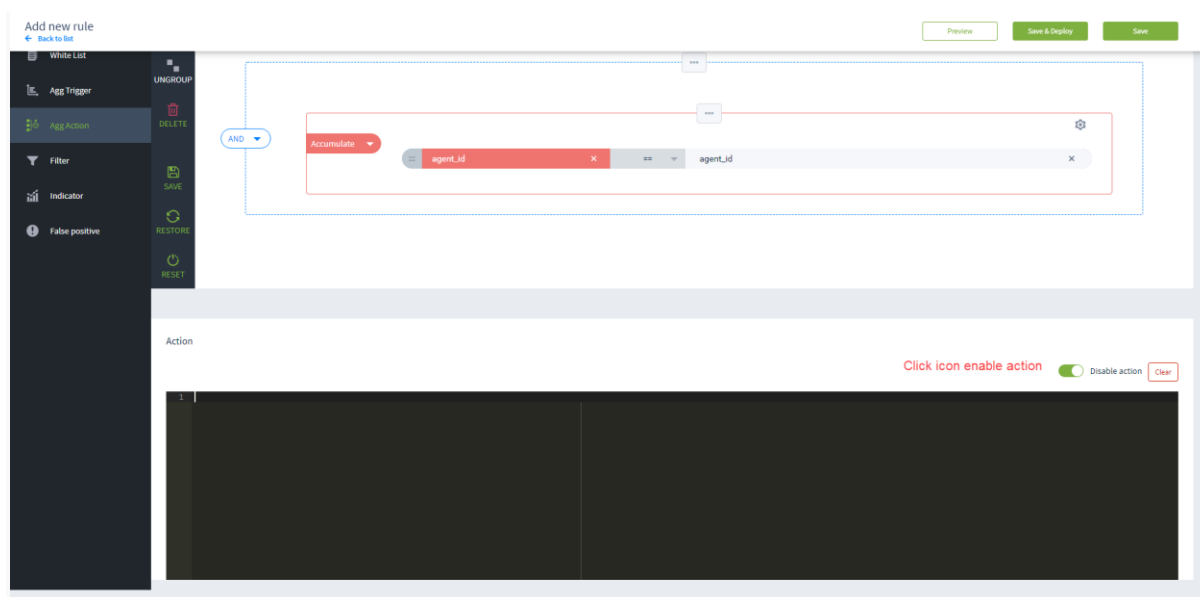
Để chỉnh sửa hành động, Click icon Chỉnh sửa .

Lưu ý: Có thể tạo nhiều hành động với các trường khác nhau tùy 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 button clear => Nội dung nhập của code sẽ bị xóa toàn bộ



Hình 4: Màn hình thêm mới nội dung Code của engine Agg_action

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, xóa 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, xóa 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 xóa cho các hành động của engine FalsePositive tương tự với khi thêm mới các trường cho engine whitelist .

- Bước 6: Nhấn Lưu để lưu rule vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống , đồng thời deploy xuống correl engine thì nhấn Lưu & Deploy.

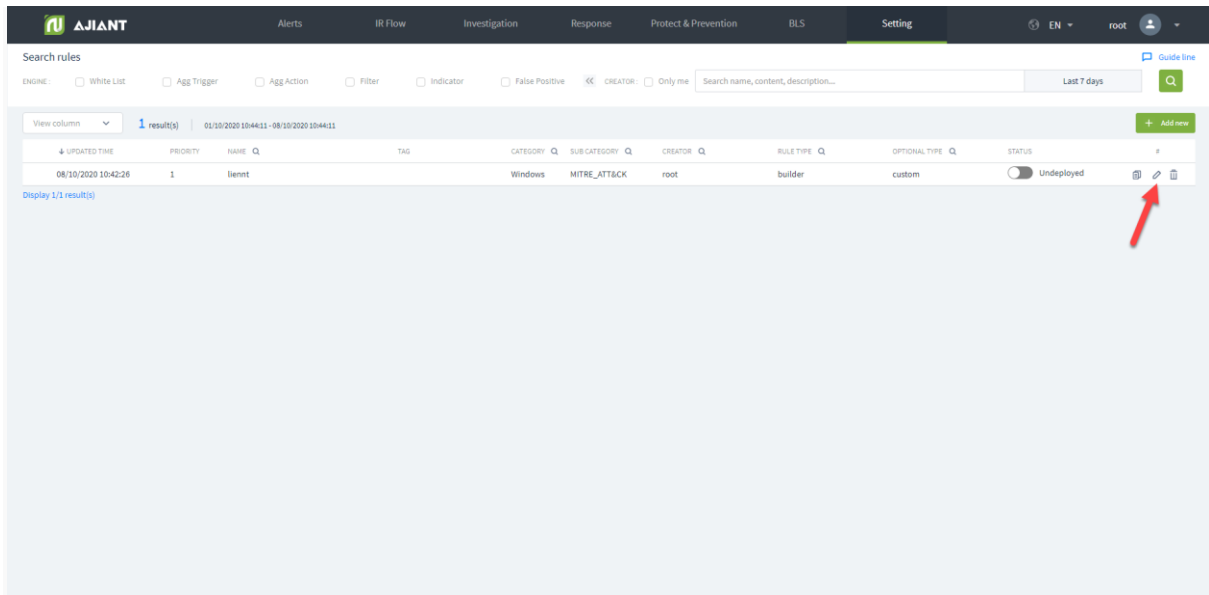
Lưu ý: Khi có lỗi, người dùng có thể nhấn button Preview để xem lỗi.

3.10.3 Sửa Rules Correlation

- Cho phép người dùng chỉnh sửa các rule đã tạo.

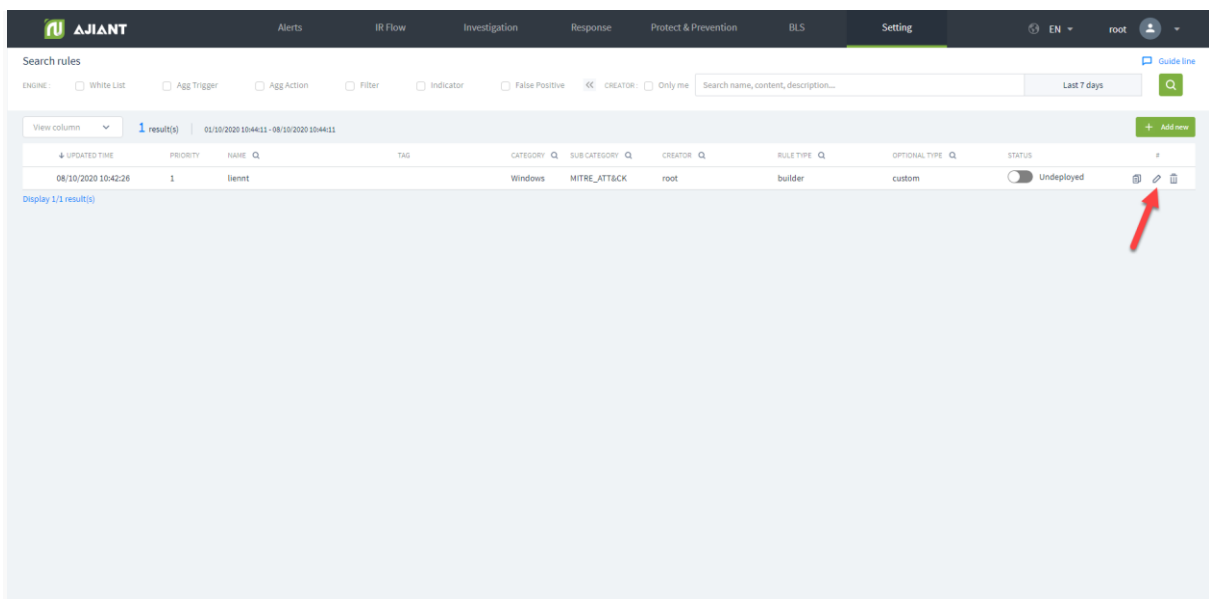
Các bước thực hiện:

- Bước 1 : Tại màn hình quản lý rule, click icon Chỉnh sửa của rule muốn chỉnh sửa.



Hình 5: Màn hình quản lý rule

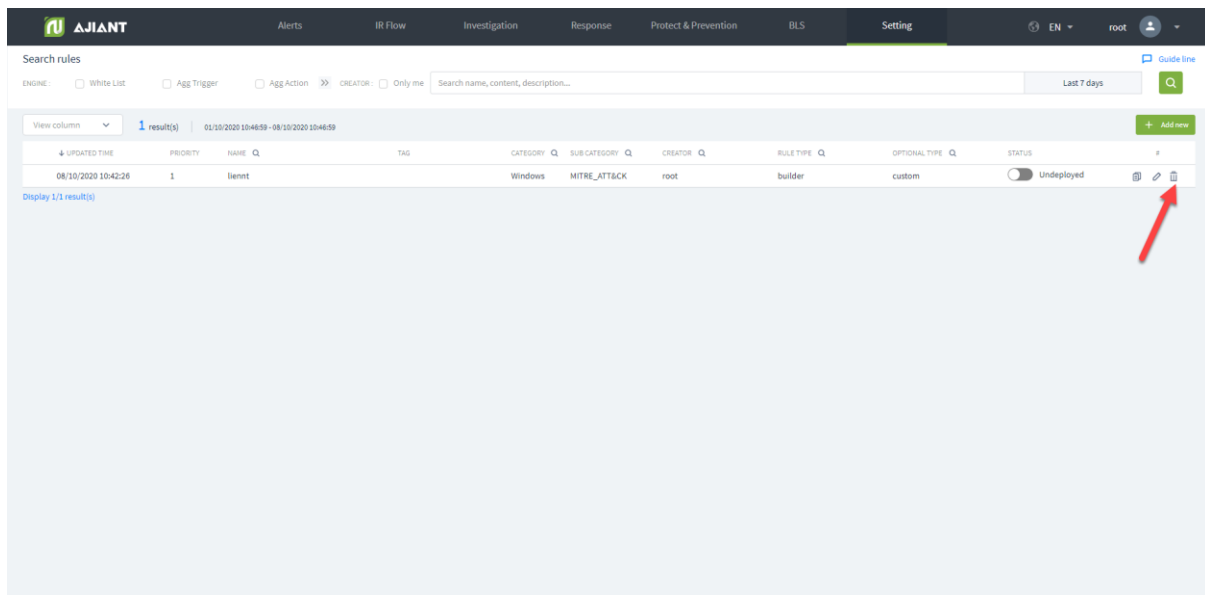
- Bước 2: Tại màn hình chỉnh sửa , nhập thông tin cần chỉnh sửa.



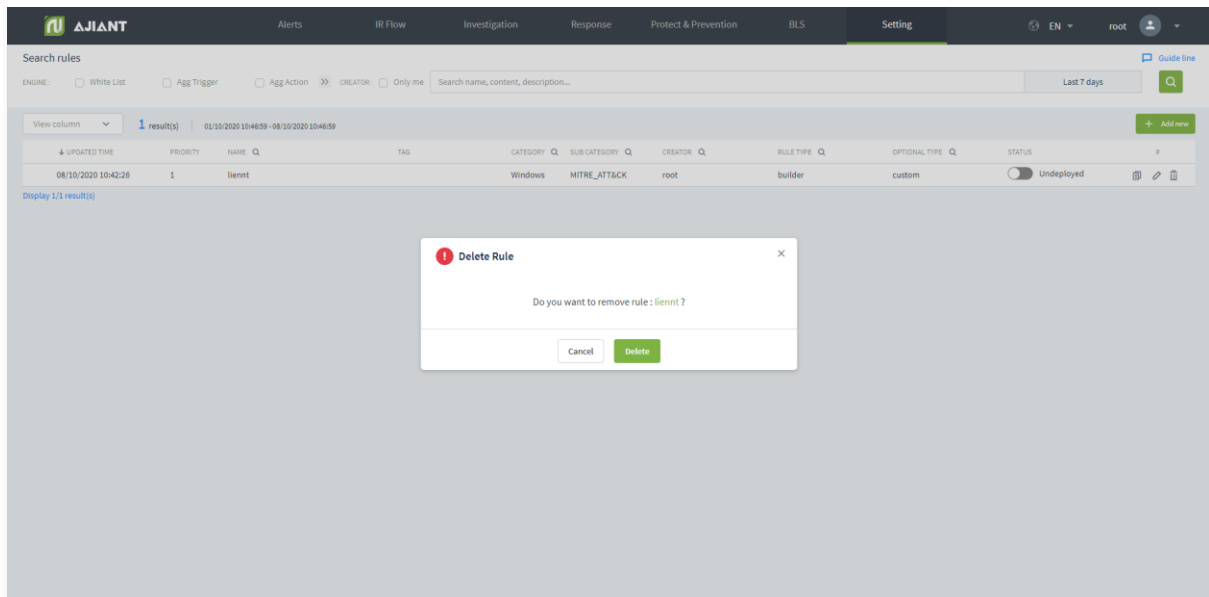
Hình 6: Màn hình thông tin chi tiết của rule

- Lưu ý: Các trường tên rule, category, subcategory là những trường không chỉnh sửa được.
- Bước 3: Nhấn Lưu để lưu rule lại vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống, đồng thời deploy xuống correlation engine thì nhấn Lưu & 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.
- Lưu ý: Khi có lỗi, người dùng có thể nhấn Preview để xem lỗi.

3.10.4 Xóa Rules Correlation

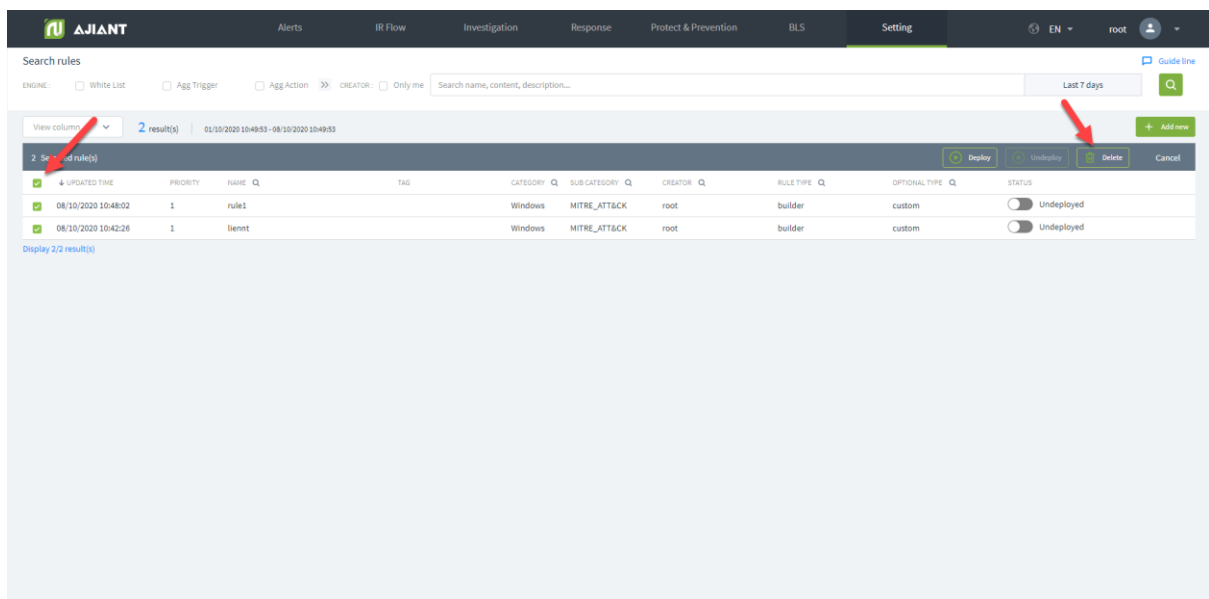


- Các bước thực hiện xóa 01 rule:
- Bước 1: Click icon Xóa tại rule muốn xóa.
- Bước 2: Màn hình hiển thị thông báo xác nhận xóa, chọn HỦY/ ĐỒNG Ý.



Hình 7: Popup xác nhận xóa rule

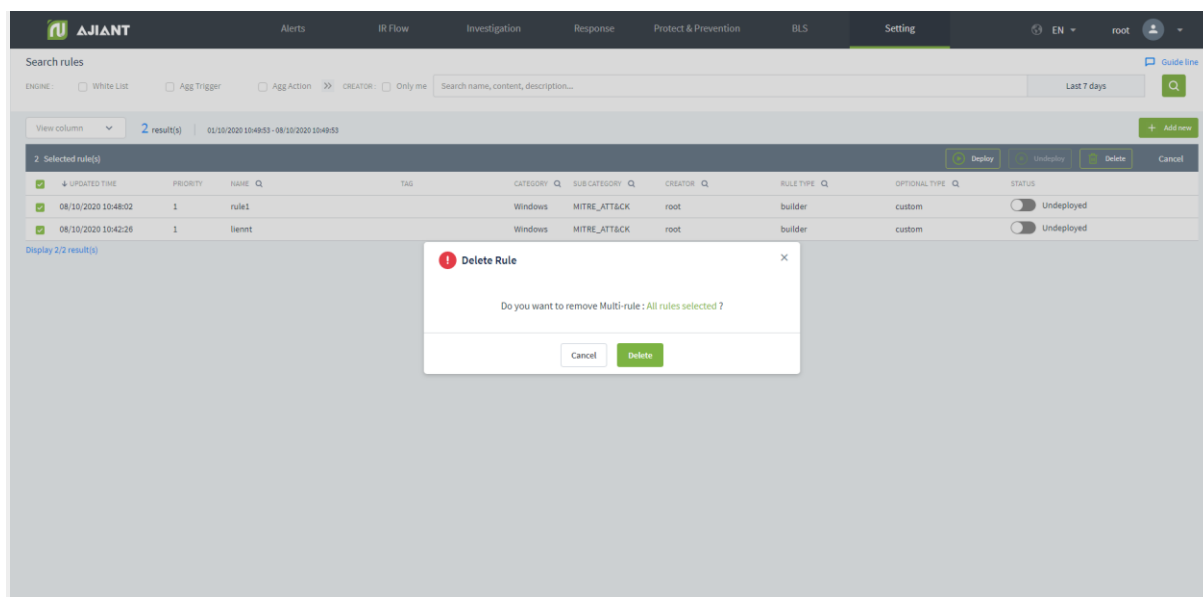
- Nếu chọn **ĐỒNG Ý**, rule được chọn xóa sẽ biến mất khỏi màn hình hiển thị.



Hình 8: Màn hình chức năng xóa đồng thời nhiều rule

Các bước thực hiện xóa nhiều rule:

- Bước 1: Click chọn những rule muốn xóa (Có thể xóa tất cả bằng cách Click Chọn tất cả rule).
- Bước 2: Màn hình hiển thị thông báo xác nhận xóa, chọn **HỦY/ ĐỒNG Ý**.



Hình 9: Màn hình xác nhận xóa

- Chọn ĐỒNG Ý, tất cả rule sẽ được xóa khỏi màn hình hiển thị. Chọn HỦY, thao tác vừa chọn sẽ được huỷ bỏ.

3.11 Protect & Prevention

3.11.1 Application Control

- 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.

Application Control				
Agent updated: 0 Time updated: 2020/10/12 10:04:45				
Q Type and enter to filter				
☐	OBJECT	TYPE	DESCRIPTION	CREATED TIME
☐	Hailest	PATH	Nguyễn Thị Duyên hải thêm ngày 25/09	2020/09/25 18:42:22
☐	*notepad.exe	PATH	tttt	2020/09/23 10:21:34
☐	*procmon.exe	PATH	test	2020/09/23 10:21:20
☐	procmon.exe	PATH	test	2020/09/23 10:20:52
☐	B5486691F78A935A222C18B8A8B800AF	HASH	chrome	2020/09/22 17:48:28
☐	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	PATH	chrome	2020/09/22 17:42:27
☐	C:\Program Files\Google\Chrome\Application\chrome.exe	PATH	chrome	2020/09/18 18:52:13
☐	6B6B7FC1360B8E70525459B8BA91E9	HASH	chrome	2020/09/18 18:51:45
☐	*chrome.exe	PATH	ttt	2020/09/18 18:44:33
☐	nga	PATH	123123123123	2020/09/09 15:20:28
☐	test22	PATH	1	2020/08/20 11:01:11
☐	test21	PATH	1	2020/08/20 11:00:53
☐	test20	PATH	1	2020/08/20 11:00:47
☐	test19	PATH	1	2020/08/20 11:00:41
☐	test18	PATH	1	2020/08/20 11:00:34
☐	test17	PATH	17	2020/08/20 10:57:25
☐	test16	PATH	16	2020/08/20 10:57:17
☐	test15	PATH	15	2020/08/20 10:56:53
☐	test14	PATH	14	2020/08/20 10:56:46
☐	test13	PATH	13	2020/08/20 10:56:38
☐	test12	PATH	12	2020/08/20 10:56:27
☐	test11	PATH	11	2020/08/20 10:55:43

Màn hình danh sách ứng dụng/tiến trình bị chặn

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

Application Control				
Agent updated: 0 Time updated: 2020/10/12 10:04:45				
Q notepad				
☐	OBJECT	TYPE	DESCRIPTION	CREATED TIME
☐	*notepad.exe	PATH	tttt	2020/09/23 10:21:34

Màn hình tìm kiếm ứng dụng/tiến trình bị chặn

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)

Application Control				
Agent updated: 0 Time updated: 2020/10/12 10:04:45				
Q Type and enter to filter				
☐	OBJECT	TYPE	DESCRIPTION	CREATED TIME
☐	Hailest	PATH	Nguyễn Thị Duyên hải thêm ngày 25/09	2020/09/25 18:42:22
☐	*notepad.exe	PATH	tttt	2020/09/23 10:21:34
☐	*procmon.exe	PATH	test	2020/09/23 10:21:20
☐	procmon.exe	PATH	test	2020/09/23 10:20:52
☐	B5486691F78A935A222C18B8A8B800AF	HASH	chrome	2020/09/22 17:48:28
☐	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	PATH	chrome	2020/09/22 17:42:27
☐	C:\Program Files\Google\Chrome\Application\chrome.exe	PATH	chrome	2020/09/18 18:52:13
☐	6B6B7FC1360B8E70525459B8BA91E9	HASH	chrome	2020/09/18 18:51:45
☐	*chrome.exe	PATH	ttt	2020/09/18 18:44:33
☐	nga	PATH	123123123123	2020/09/09 15:20:28
☐	test22	PATH	1	2020/08/20 11:01:11
☐	test21	PATH	1	2020/08/20 11:00:53
☐	test20	PATH	1	2020/08/20 11:00:47
☐	test19	PATH	1	2020/08/20 11:00:41
☐	test18	PATH	1	2020/08/20 11:00:34

Add New

Object
Type
Description

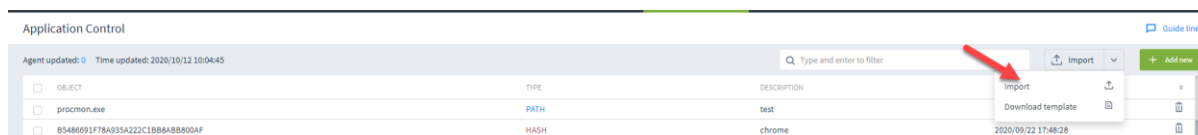
Type value object
PATH HASH
Type description

Cancel Add new

Màn hình thêm mới ứng dụng/tiến trình bị chặn

3.10.1.4 Thêm mới ứng dụng/tiến trình từ tập tin có sẵn

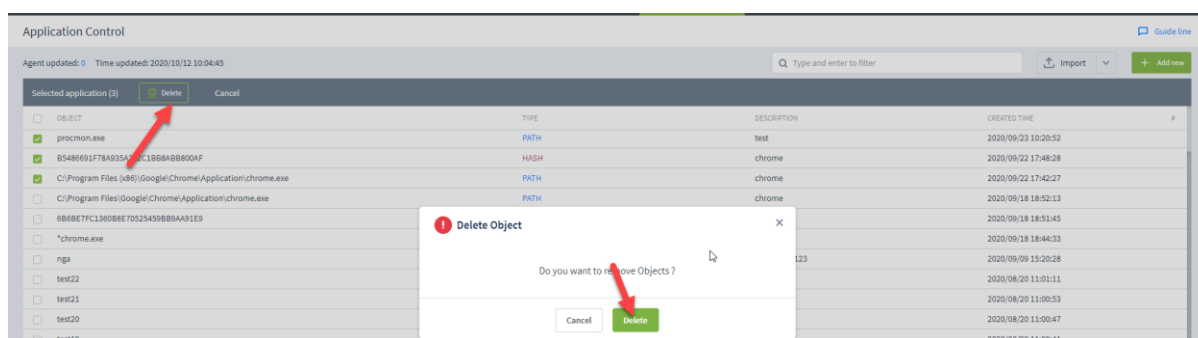
- Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại.
- Click <Import>, chọn đường dẫn đến file cần tải lên và click Open, hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống.



Màn hình thêm mới ứng dụng/tiến trình từ tập tin có sẵn

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 checkbox đầu mỗi ứng dụng và click button <Delete>



Màn hình xóa ứng dụng/tiến trình bị chặn

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.

Application Control

Agent updated: 0 Time updated: 2020/10/12 10:04:45

3.11.2 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.

3.11.2.1 Hiện 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.

Endpoint Firewall

94 result(s) Agent updated: 0 Time updated: 2020/10/01 14:01:06

Q Type and enter to filter Import Add new

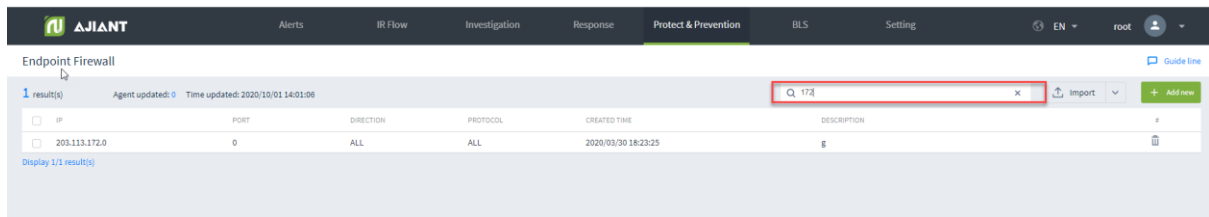
IP	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION	#
☐ 1.1.1.82	33	INBOUND	TCP	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.92	33	ALL	ICMPV6	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.84	33	INBOUND	TCP	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.95	33	INBOUND	UDP	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.99	33	OUTBOUND	ALL	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.3	33	INBOUND	UDP	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.23	33	ALL	ICMPV6	2020/04/16 09:21:35	Import from file	
☐ 1.1.1.37	33	INBOUND	TCP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.69	33	OUTBOUND	ALL	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.74	33	ALL	ICMPV6	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.80	33	ALL	ICMPV6	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.18	33	OUTBOUND	ALL	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.21	33	INBOUND	UDP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.33	33	INBOUND	UDP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.70	33	INBOUND	TCP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.7	33	INBOUND	TCP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.63	33	OUTBOUND	ALL	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.93	33	OUTBOUND	ALL	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.68	33	ALL	ICMPV6	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.72	33	INBOUND	UDP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.77	33	INBOUND	UDP	2020/04/15 13:23:37	Import from file	
☐ 1.1.1.78	33	INBOUND	UDP	2020/04/15 13:23:37	Import from file	

Display 10/94 items (100) Back to top

Màn hình danh sách các kết nối bị chặn

3.11.2.2 Tìm kiếm các kết nối bị chặn

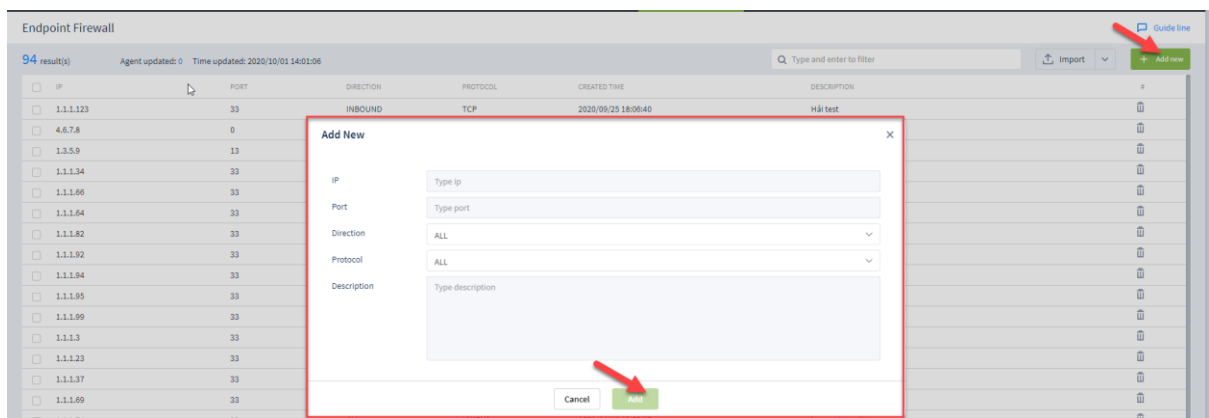
- Người dùng có thể tìm kiếm theo địa chỉ IP và port đã thiết lập



Màn hình tìm kiếm các kết nối bị chặn

3.11.2.3 Thêm mới các kết nối bị chặn

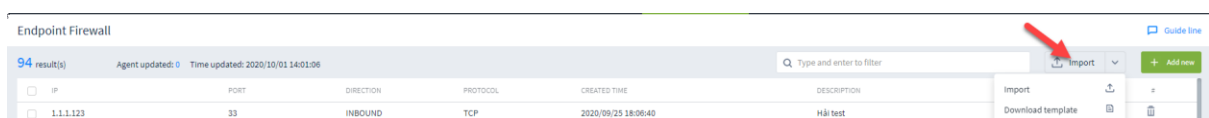
- Click button <Add new>, nhập thông tin trên popup thêm mới kết nối bị chặn
 - + IP: địa chỉ IP cần chặn
 - + Port: port cần chặn, nếu chặn tất cả port thì nhập 0
 - + Direction: inbound, outbound, All (chặn cả 2 chiều)
 - + Protocol: ICMP, TCP, UDP, ICMPV6, ALL



Màn hình thêm mới địa chỉ kết nối bị chặn

3.11.2.4 Thêm mới kết nối bị chặn từ tập tin có sẵn

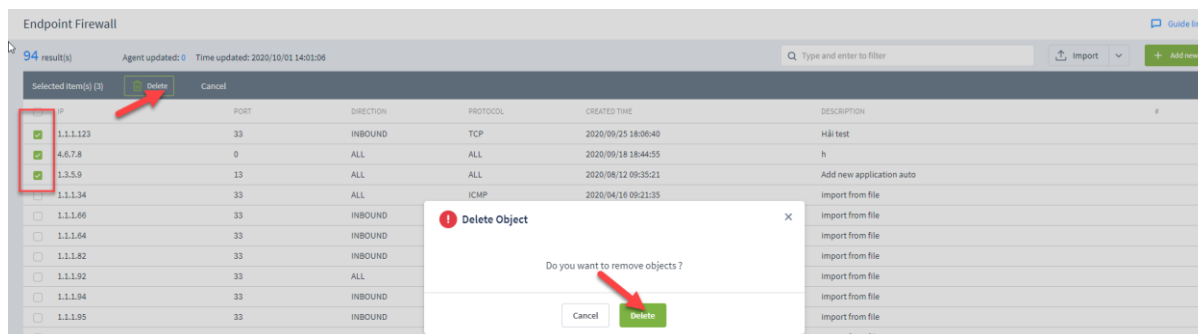
- Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại.
- Click <Import>, chọn đường dẫn đến file cần tải lên và click Open, hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống.



Màn hình thêm mới ứng dụng/tiến trình từ tập tin có sẵn

3.11.2.5 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 checkbox đầu mỗi kết nối và click button <Delete>



Màn hình xóa kết nối bị chặn

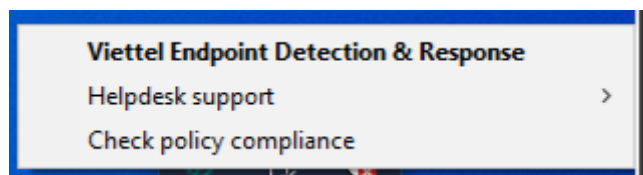
3.11.2.6 Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công

- 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.

GIAO DIỆN PHÍA AGENT

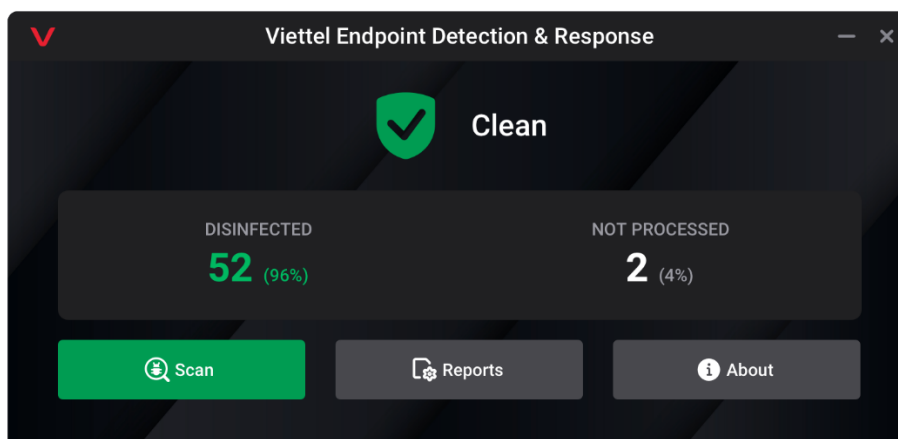
3.12 Main

- Chức năng cho phép người dùng xem nhanh trạng thái an toàn thông tin tại máy đang cài agent
- Trên thanh taskbar tìm icon  click chuột phải và chọn “Viettel Endpoint Detection & Response”

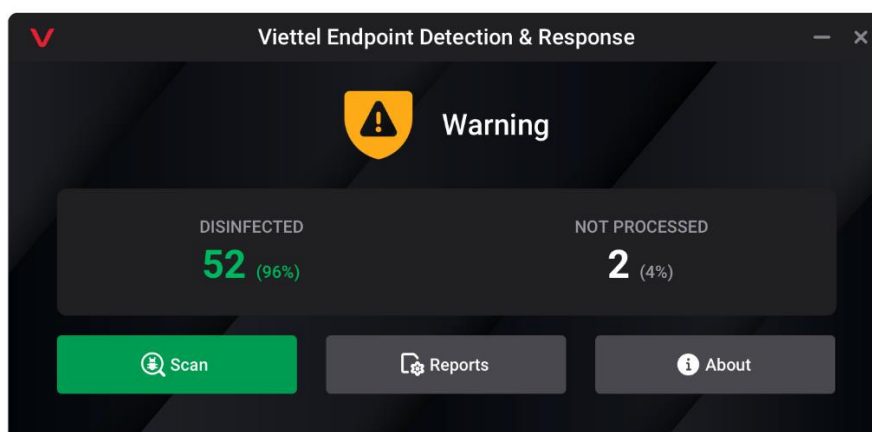


- Hệ thống hiển thị các thông tin

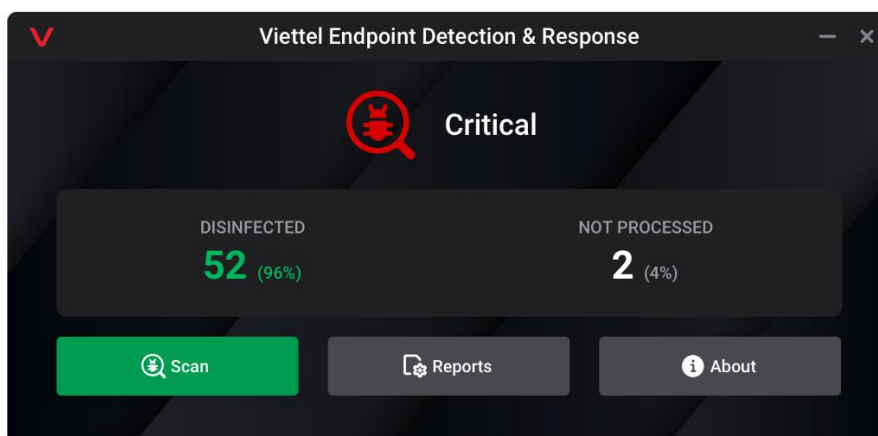
+ Trường hợp máy không có mã độc nào hoặc toàn bộ mã độc đã được xử lý



+ Trường hợp máy có ít nhất 01 mã độc và không có mã độc nào có độ nguy hiểm cao



+ Trường hợp máy có ít nhất 01 mã độc có độ nguy hiểm cao

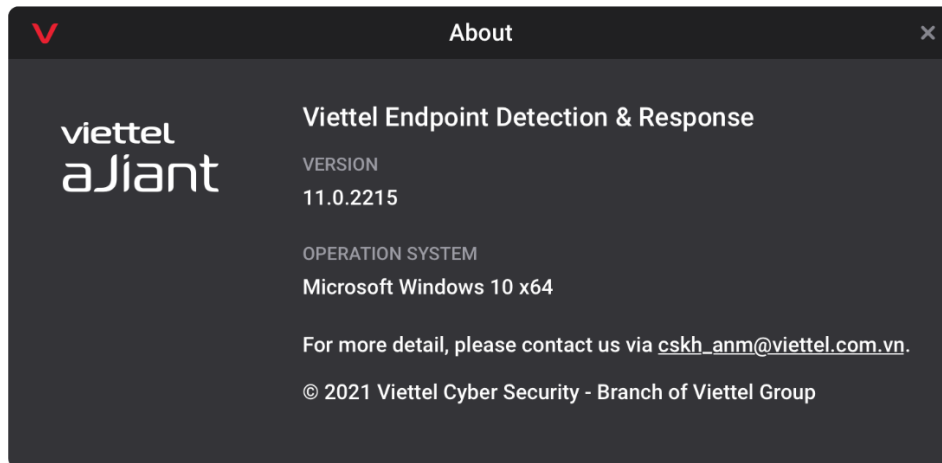


+ Ngoài ra hệ thống hiển thị con số thống kê liên quan đến tổng số mã độc đã được phát hiện

- Disinfected: Tổng số và tỷ lệ mã độc đã phát hiện và được xử lý
- Not processed: Tổng số và tỷ lệ mã độc đã phát hiện nhưng chưa được xử lý

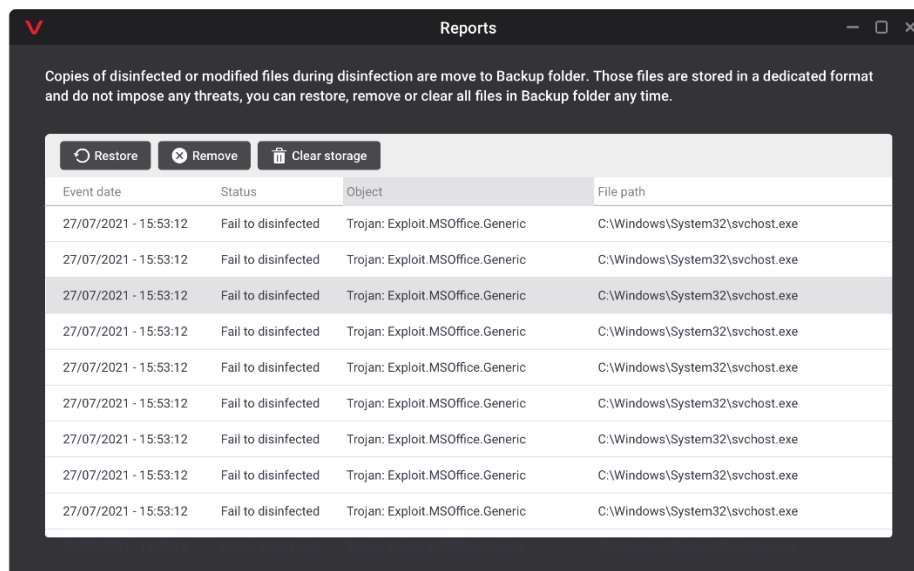
3.13 About

- Chức năng cung cấp thông tin về phiên bản Agent cài trên máy người dùng và thông tin hỗ trợ sản phẩm



3.14 Reports

- Chức năng tổng hợp danh sách các mã độc đã được phát hiện trên hệ thống và tình trạng xử lý tính đến thời điểm hiện tại



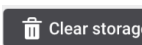
- Các file chứa mã độc trước khi được xử lý đều được lưu trữ bản gốc trong thư mục Backup, để dọn thư mục Backup hoặc phục hồi file, sản phẩm cung cấp các tính năng sau:



: Cho phép lựa chọn 01 file để phục hồi



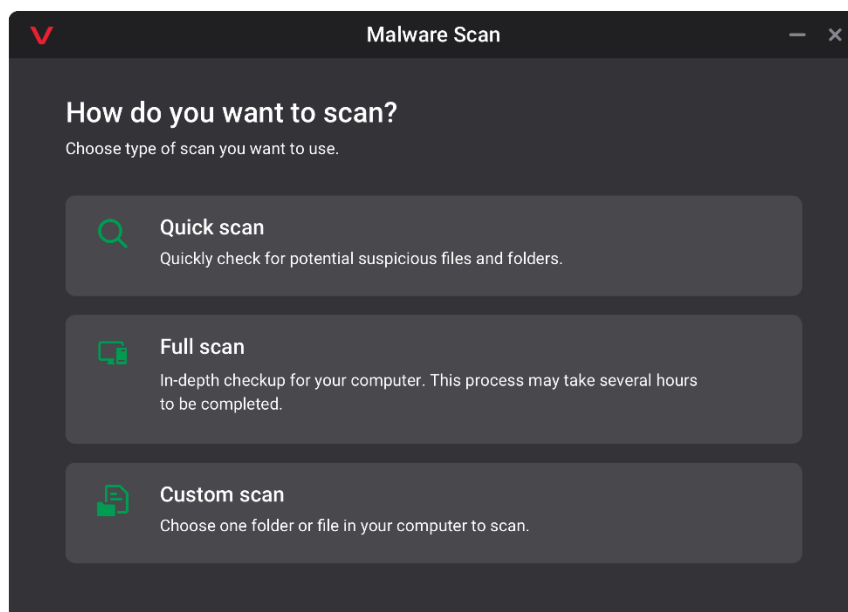
: Cho phép lựa chọn 01 file để xóa khỏi thư mục Backup



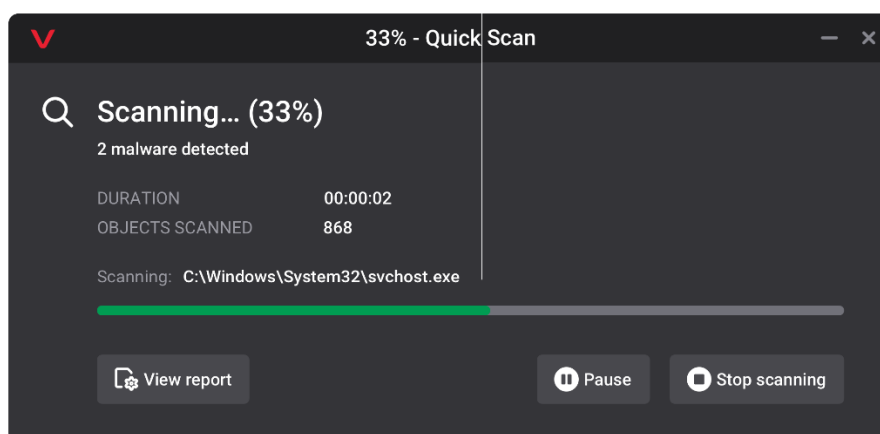
: Cho phép dọn nhanh toàn bộ file hiện có trong thư mục Backup

3.15 Scan

- Chức năng cho phép người dùng chủ động sử dụng hệ thống để quét và xử lý mã độc trên máy.
- Các phương thức quét được hỗ trợ bao gồm
 - + Lựa chọn trực tiếp từ file explorer, cho phép chọn nhiều tệp tin và thư mục, chuột phải chọn quét (Context scan)
 - + Lựa chọn các hình thức quét từ giao diện phía agent
 - Quick scan: Quét trên một tập các thư mục được định nghĩa trước, đây là các thư mục thường xuyên phát sinh mã độc, khi chọn quét toàn bộ các tệp tin và thư mục trực thuộc các thư mục đã chọn.
 - Full scan: Quét toàn bộ các tệp tin và thư mục có trong máy người dùng.
 - Custom scan: Tương tự context scan, khi chọn hình thức này agent hiển thị file explorer cho phép người dùng lựa chọn 01 tệp tin hoặc thư mục để quét



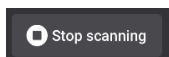
- Sau khi chọn phương thức phù hợp, hệ thống thực hiện quét và xử lý mã độc:



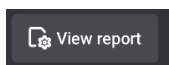
- Hỗ trợ các thao tác trong lúc quét như sau:



: Cho phép tạm dừng quá trình quét

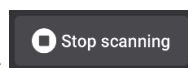
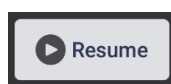
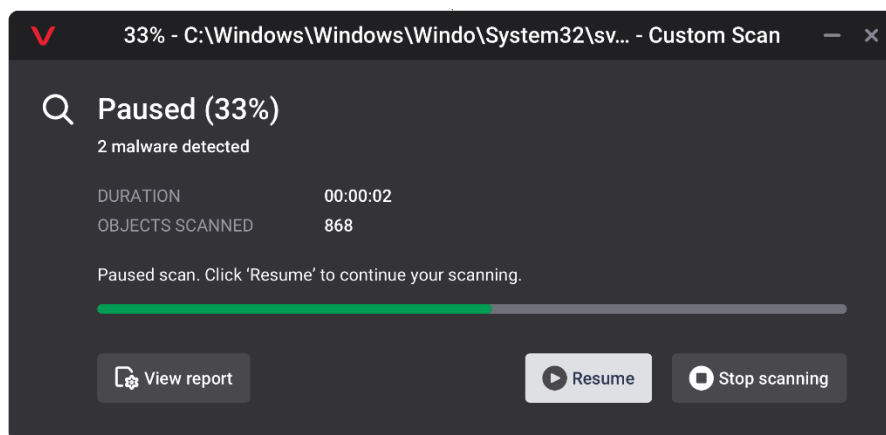


: Cho phép kết thúc quá trình quét



: Trường hợp phát hiện được ít nhất một mã độc, cho phép xem nhanh trạng thái xử lý tại [3.14 Reports](#)

- Màn hình khi người dùng chọn tạm dừng quá trình quét



: Cho phép chọn để tiếp tục quét hoặc để hoàn thành quá trình quét

- Khi hoàn thành quét, hiển thị kết quả như sau:

