

Viettel Endpoint Detection & Response

(VCS-aJiant)

Phiên bản 3.3.31 – Ngày cập nhật: 10/10/2022

Tài liệu Hướng dẫn sử dụng





Lịch sử cập nhật

| STT | Ngày cập nhật | Phiên bản | Lý do thay đổi | Ghi chú |
|-----|---------------|-----------|---|---------|
| 1 | • • • | 3.3.0 | | |
| 2 | 30/06/2022 | 3.3.20 | Bổ sung/ cập nhật hướng dẫn: 3.7.5 Update management - 174 | |
| 3 | 10/10/2022 | 3.3.31 | Bổ sung/ cập nhật hướng dẫn: 3.5 Anti – Malware – 79 | |

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



Mục lục

| 1. | G | IỚI THIỆU | .6 |
|----|-----|---------------------------------|------------|
| | 1.1 | Thực trạng hiện nay | .6 |
| | 1.2 | Sự phát triển của công nghệ | .6 |
| | 1.3 | VCS-aJiant | .7 |
| | 1.4 | Các thông tin nâng cấp | .7 |
| 2. | Т | ĎNG QUAN | .7 |
| | 2.1 | Công nghệ | .7 |
| | 2.2 | Kiến trúc hạ tầng | .8 |
| | 2.3 | Làm việc với giao diện quản trị | .9 |
| 3. | н | ƯỚNG DẪN SỬ DỤNG | 10 |
| | A. | Giao diện web Portal | 10 |
| | 3.1 | Đăng nhập | 10 |
| | 3.2 | Dashboard VCS-aJiant | 10 |
| | 3. | 2.1 Thao tác với dữ liệu | 12 |
| | | 3.2.1.1 Xuất dữ liệu | 12 |
| | | 3.2.1.2 Tìm kiếm theo ngày | 12 |
| | | 3.2.1.3 Làm mới dữ liệuŕ | 13 |
| | 3. | 2.2 Thống kê Overview | 13 |
| | 3. | 2.3 Theo dõi Security Operation | 19 |
| | 3. | 2.4 Theo dõi Agent Monitoring | 20 |
| | 3. | 2.5 Theo dõi Risk Detection | 22 |
| | 3.3 | Dashboard Anti-malware | <u>2</u> 4 |
| | | | |

viettel

security

| 3.3.1 | Tha | ao tác với dữ liệu | 26 |
|--------|---------|-----------------------------|-----------|
| 3.3 | .1.1 | Xuất dữ liệu | 26 |
| 3.3 | .1.2 | Tìm kiếm theo ngày | 26 |
| 3.3 | .1.3 | Làm mới dữ liệu | 27 |
| 3.3.2 | Thá | ống kê Overviewź | 27 |
| 3.3.3 | The | eo dõi Risk Detection | <u>29</u> |
| 3.4 Ma | àn hì | nh Setting | 32 |
| 3.4.1 | Age | ent Management | 32 |
| 3.4.2 | Pol | licy Setting | 12 |
| 3.4.3 | Gro | oup Management | 48 |
| 3.4.4 | Aco | count Management | 57 |
| 3.4 | .4.1 | Permission management | 58 |
| 3.4 | .4.2 | Role Management | 59 |
| 3.4 | .4.3 | User management | 35 |
| 3.4.5 | Up | date management | 39 |
| 3.4 | .5.1 | Update groups | 39 |
| 3.4 | .5.2 | Update packages | 73 |
| 3.5 Ar | nti — ľ | Malware | 79 |
| 3.5.1 | Sca | an Schedule | 79 |
| 3.5 | .1.1 | Tìm kiếm Scan Schedule task | 79 |
| 3.5 | .1.2 | Thêm mới Scan Schedule task | 79 |
| 3.5 | .1.3 | Nhân bản Schedule task | 36 |
| 3.5 | .1.4 | Xem chi tiết | 37 |
| 3.5 | .1.5 | Xóa Schedule task | 38 |

 \square



| 3.5.1.6 | Xem báo cáo | 90 |
|---------|---|---|
| Giao | diện Agent | 92 |
| Main | | 92 |
| About . | | 94 |
| Reports | 5 | 95 |
| Scan | | 95 |
| | 3.5.1.6 Giao Main About . Reports Scan | 3.5.1.6 Xem báo cáo Giao diện Agent Main About Reports Scan. |

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 | |



| Thuật ngữ | Diễn giải | Ghi chú |
|-----------|--|---------|
| 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 ScenarioLiveResponse | |
| 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:

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

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

2. TỔNG QUAN

2.1 Công nghệ

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



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

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



2.2 Kiến trúc hạ tầng

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



Có 3 thành phần chính:

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

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

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

2.3 Làm việc với giao diện quản trị

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

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

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

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

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

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

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

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



3. HƯỚNG DẪN SỬ DỤNG

A. Giao diện web Portal

3.1 Đăng nhập

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

| | Version 3.3.0 (backs: 12.7,6) o 2.021 Verbei Sparthr - Branch of Verbei Group | |
|--|--|--|

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

3.2 Dashboard VCS-aJiant

Các tính năng chính gồm có:

Ĺ



| ≡ | aJiant Dashboard | | | | 0 | 🗮 😃 🕅 |
|---------------------|--------------------------|-----------------------------------|-------------------------------------|---------------------------------|---|--------------------------------------|
| | Organization Dashboard 🔹 | | | | | 08/06/2022 - Now 💾 📀 |
| ▲ 1 ⁺ | 2 AGENTS 0 | Online 5 * Remain unchanged | Offline 12 ⇒ Remain unchanged | ALERTS • 5.1M | New 17 * +8 alerts | Executing 0 → Remain unchanged |
| | + 1 new agents | Suspicious 16 t + 7 agents | | + 17 alerts has been updated | False Positive 0 ⇒ Remain unchanged | Closed 0 ⇔ Remain unchanged |
| <u>ب</u> | Agent Monitoring | lection | | | | |
| | ALERTS BY STATUS | | | ط Exp | ALERTS BY SEVERITY | ع Export data |
| | 100% | | | | | |
| | 805 | | | | | |
| | 70% | | | | | 17 |
| | 50% - | | | | | IUIAL |
| | 40% - | | | | | |
| | 20%- | | | | | |

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

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



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

3.2.1 Thao tác với dữ liệu

3.2.1.1 Xuất dữ liệu

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

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

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

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

3.2.1.2 Tìm kiếm theo ngày

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

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

| Absolute time range | Relative time range |
|---------------------|---------------------|
| From | Last 90 days |
| 08/06/2022 | Last 60 days |
| Apply time range | Last 30 days |
| | Last day |
| | |
| | |

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



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

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

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

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

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

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

3.2.1.3 Làm mới dữ liệu

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

3.2.2 Thống kê Overview

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

| -13 | AGENTS 0 | Online 5 ⇒ Remain unchanged | ninity | Offline 12 ⇒ Remain unchange | Infinity's | ^ | ALERTS • 5.1M | New 17 † + 8 alerts | 100% | Executing 0 ⇒ Remain unchanged | 0% |
|------|------------------|-----------------------------------|--------|------------------------------------|------------|-----|--|---------------------------|------------|--------------------------------------|----|
| L-10 | t + 1 new agents | Suspicious 16 +7 agents | 94% | | | ΣiΖ | + 17 alerts has been updated | False Positive 0 | 0 % | Closed O * Remain unchanged | 0% |

+ Thống kê liên quan đến agents:

| Số thống kê | Ý nghĩa |
|--|---|
| | Bao gồm 02 chỉ số: |
| AGENTS • 17 1 t + 1 new agents 2 | 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) |
| Online 2 53% | Bao gồm 03 chỉ số: |
| 32/4 + 884 agents 3 | Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00); |
| | 2 – Tỷ lệ máy Online trung bình so với toàn hệ thống; |
| | 3 – Số lượng máy Online trung bình chênh lệch so với chu kỳ trước. |
| | (+: Số lượng máy Online trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch) |
| Offline 1 247% | Bao gồm 03 chỉ số |
| ↓ -898 agents | Trung bình số máy Offline trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00); |
| | 2 – Tỷ lệ máy Offline trung bình so với toàn hệ thống; |
| | 3 – Số lượng máy Offline trung bình chênh lệch so với chu kỳ trước. |



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

+ Thống kê liên quan đến Alerts:

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

 \square



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



| | (NEW, FALSE POSITIVE, CLOSED); |
|--|---|
| | 2 – 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; |
| | 3 – 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) |
| False Positive 0 1 20% → Remain unchanged 3 | Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED; |
| | 2 – 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; |
|------------------------|---|
| | 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED chênh lệch so với chu kỳ trước. |
| | (+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước) |
| Closed 2 | Bao gồm 03 chỉ số: |
| O → Remain unchanged 3 | 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE; |
| | 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; |
| | 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE chênh lệch so với chu kỳ trước. |

 \square



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

3.2.3 Theo dõi Security Operation

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

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



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 trạng thái 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 trong khoảng thời gian; |

3.2.4 Theo dõi Agent Monitoring

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

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





| aJiant Dashboard | | | | | | | | | ₩ ±°0 |
|--|-----------------------------------|---|-------------|-----------------------------------|---|---------------------------|-----------------------------------|--------------------------------------|------------------------|
| Organization Dashboard 🔹 | | | | | | | txport this Dashb | 08/06/2022 - Now | ÷ |
| AGENTS 0 | Online 5 → Remain unchanged | Offline Infantry 12 * Remain unchanged | (effective) | \wedge | ALERTS • 5.1M | New 17 * + 8 alerts | 1005 | Executing 0 ⇒ Remain unchanged | 0% |
| t + 1 new agents | Suspicious 16 1 + 7 agents | • | | t + 17 alerts has been updated | False Positive 0 * Remain unchanged | (r) | Closed 0 ⇒ Remain unchanged | 0% | |
| Security Operation Agent Monitoring Risk Detection | | | | | | | | | |
| AGENTS BY STATUS | | | | | | | | 7 agent(s) not onli | ine in this period. |
| 16 | | | | | | | | | |
| 12 - | | | | | | | | | |
| 8- 6- | | | | | | | | | |
| 4 | | | | | | | | | |
| | | | | | | | | | |
| 08/06/2022 00:00:00 | 08/06/2022 12:00:00 | | 09/06/20 | 022 | | 09/06/2022 12:00:00 | | | 09/06/2022 18:00:00 |
| | | | ONLINE | OFFLINE | | | | | |
| | | | | | | | | | |

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

 \square



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

3.2.5 Theo dõi Risk Detection

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

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

| = ä, | liant | Buddoord | | | | | | | | | | | | | | ⊞ é` ⊖ |
|--------------|--------------|--|------------------------------------|--|------|------------------------------------|---------|-----------|----------|---|------------|---|-------|-------------------------------------|------------------|---------------|
| 🔤 Org | anization | Dashboard o | | | | | | | | | | | | Laport this Dashbo | 08/06/2022 - New | 8 0 |
| ▲ ** @ | | | Online 5 * Remain exchanged | | Θ | offine 12 + Remain unchanged | \odot | | \wedge | 5.1M | | New 17 • + Elainta | (101) | Decoding 0 * Remain unchanged | | n |
| в d | | المعالي المعالي المعالي المعالي | Sespicious • 16 • + 7 agents | | (*** | | | | <u> </u> | TWI + 17 alerts has been updated | 1 | Palan Positive O + Remain unchanged | 6 | Closed 0 + Remain unchanged | | Ô |
| (i) beat | ly Operation | Agent Monitoring Toxi Detection | | | | | | | | | | | | | | |
| | | | | TOP GROUPS AT RISK default TENANT, solicions News nati, usener | | | | | | | | | | | different data | Tep 5 w |
| | | - (| | TOP AGENTS AT NEW | • | | 1 | | | 2 | | 3 | | • | ي. Report data | 1 Tes v |
| | | 1004A.402NT8.47 HEKK 7 (41%) | | We/Yolk_BIOPPE3_mmm. UAAMUR_DEPACABITEA. We/Yolk4086_151200. DESKTOP 4206347_180. Iocoboxt | | | | | | | | | | | | |
| | | | | | • | | 2 | | | - CRITCH HOI - 1 | A LDUR LDR | , | | 7 | | |
| A12 | | | | | | | Top 5 v | ALERTS 81 | BORNARIO | | | | | | [| Tep 5 v |
| 5 | a . | 1. Anomaly Detection, Monitor, Agent, Disconnect | | | | | 9 | 6. | 01. | Command, Control | | | | | | 3 |
| C | ۳ | 2. Anomaly Detection_MITRE ATTECK_ATTCK_T1071_001_02_Web_ | Protocols | | | | 3 | 20 | 02. | Defense Evasion | | | | | | 3 |
| | 0 | 0. Anomaly_Detection_ATTDK_T1099_Timestomp_Correlation | | | | | 3 | | 60. | Suspicious Dehaviour | | | | | | 2 |
| | 1 | Malware_IOC_Realtime_Protection | | | | | 2 | | 04. | Malware | | | | | | 1 |
| | 0 | Windows, Swepicious, Behaviour, AgentMonitor, RoleCorrelation, 55 | 0005 | | | | | | | | | | | | | |

+ 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 |
| Total agents at risk | Tổng số máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể máy tính đã không hoạt động quá 30 ngày gần đây) trong thời gian tìm kiếm; Tỷ lệ máy khả nghi so với toàn bộ máy trên hệ thống (không kể máy tính đã không hoạt động quá 30 ngày gần đây). |
| Top agents at risk | Biểu đồ cột – thống kê top máy tính phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất (không kể |

 \square



| | Alert false positive và closed) trong thời gian tìm |
|---------------------|--|
| | kiếm; |
| | - Trục x: số lượng Alert tại từng host, phân |
| | chia rõ tỷ lệ theo severity = (Critical, High, Medium, |
| | Low) |
| | Trục y: tên máy tương ứng; |
| | Cho phép thay đổi khoảng thống kê: Top 5, |
| | Top 10, Top 20, Top 50. Mặc định chọn Top 5; |
| | - Cho phép chọn 🖾 Export data để tải về danh |
| | sách máy tính phát sinh Alert. |
| Alerts by RuleID | Thống kê top rule ld phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất trong thời gian tìm kiếm; |
| | - Cho phép thay đổi khoảng thống kê: Top 5, |
| | 10p 10, 10p 13, 10p 20. Mặc dịnh chộn 10p 3. |
| 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 Anti-malware

- Chức năng cung cấp các biểu đồ trực quan phục vụ theo dõi tình hình an toàn thông tin của tổ chức thông qua số liệu liên quan đến việc tiêu diệt mã độc;



| Organization I | Drganization Dashboard (Anti-malware) 🕸 🕹 Expert this Dashboard (| | | | | | | | | 0/07/2021 - Now | ₿ 🕹 |
|---|---|-------------------------|------------|-------------|----------------|----------------|---------|----------------|-----|-------------------|---------|
| Ţ | INFECTED DEVICES 22/ 58 (37.9%) | Resolved 2 | 9% | Remained 20 | 91% | \land | MALWARE | Resolved 50.9K | 78% | Remained 14.6K | 22% |
| TOP INFECTED MAL Display groups that | WARE GROUPS | f devices with detected | i malware. | | | | | | | | Top 5 🗸 |
| anhnn_test default | | | | | | | | | | | |
| liennt_test105 | | | | | | | | | | | |
| | 0 | 2 | 4 6 | 8 | 10 RESOLVED | 12 REMAINED | 14 | 16 18 | 20 | 22 | 24 |
| | | | | | | | | | | | |

Các tính năng chính gồm có:

| Organization Dashboard (Anti-malware) 🔯 | | | | | | | | ± Export 1 | Lexport this Dashboard 20/07/2021 - Nov | | |
|---|---|-------------------------|----------|----------|----------|----------|---------|------------|---|-------------------|---------|
| 2 | INFECTED DEVICES 22/ 58 (37.9%) | Resolved 2 | 95 | Remained | 91% | Ŵ | MALWARE | Resolved | 78% | Remained 14.6K | 223 |
| TOP INFECTED MAI Display groups that | WARE GROUPS nclude the largest number of | f devices with detected | malware. | | | | | | | | Top 5 🗸 |
| dattest anhnn_test | | | | | | | | | | | |
| default liennt_test105 | | | | | | | | | | | |
| liennt_test301 | 0 | 2 | 4 6 | 8 | 10 | 12 | 14 | 16 18 | 20 | 22 | 24 |
| 3 | | | | | RESOLVED | REMAINED | | | | | |

- 4 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;

- 5 Overview: Thống kê tổng quan tình hình an toàn thông tin tổ chức (thông qua trạng thái devices và threats);
- 6 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:

| 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 ^e 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 |
|---|--|
| Már Bị Lâr NHIÊM 136/3.940 (3.5%) - 3 1 2 | Bao gồm 03 chỉ số 1 – Tổng số máy bị lây nhiễm trên hệ thống trong khoảng thời gian tìm kiếm 2 – Tổng số máy cài đặt agent trong hệ thống (<i>không kể thời gian tìm kiếm</i>) 3 – Tỷ lệ máy bị lây nhiễm so với toàn bộ máy cài đặt agent trong hệ thống |



| Resolved 0% 2 | Bao gồm 02 chỉ số: 1 – Tổng số máy bị lây nhiễm trên hệ thống đã được xử lý thành công |
|---------------|--|
| | 2 – Tỷ lệ máy bị lây nhiễm được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống. |
| Remained 0% 2 | Bao gồm 02 chỉ số: 1 – Tổng số máy bị lây nhiễm trên hệ thống chưa được xử lý thành công 2 – 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 |
|--------------------------------|---|
| МА ВОС 1.960 | Bao gồm 01 chỉ số: 1 – Tổng số mã độc ghi nhận trên toàn bộ hệ thống |
| Dă giải quyết 112 1 2 | Bao gồm 02 chỉ số: 1 – Tổng số mã độc trên hệ thống đã được xử lý thành công; 2 – Tỷ lệ mã độc đã được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống. |

Ĺ



| 1.848 995 1 2 | Bao gồm 02 chỉ số: 1 – Tổng số mã độc trên hệ thống chưa được xử lý thành công; 2 – 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, |
| | 10p 10, 10p 20, 10p 50. Mặc dịnh chộn 10p 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; |

 \square



3.4 Màn hình Setting

3.4.1 Agent Management

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

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

| = | viettet a Jiant Setting / Agent Management | | | | | | | | | | | |
|----------------|--|-----------------------|---------|---------|--------------|---------------------|---------------------|-------------|---------------------|----------|--|--|
| - Li | Agent management | | | | | | | | | | | |
| A | Type to search by queries First Ping 📋 Last Ping 📋 Q | | | | | | | | | | | |
| P _± | 3 result(s) | | | | | | | | | v column | | |
| ۲ | 0 | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | FIRST PING | IP DCN | POLICY | VERSION | | |
| _ | | Localhost.Localdomain | Offline | Default | Phula_test | 09/06/2022 10:43:58 | 05/04/2022 14:49:51 | 10.61.188.2 | phula_test | | | |
| >- | 1 | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | 10.61.188.2 | anhnn_full_features | 3.3.8 5 | | |
| | | N/A | Offline | N/A | N/A | N/A | N/A | N/A | N/A | - | | |
| Ē. | Display 3 | /3 result | | | | 1 | | | | | | |
| ē | | | | | | | | | | | | |
| | | | | | | | | | | | | |

- Hệ thống hỗ trợ thực hiện các tính năng:

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

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

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

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

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



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

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

| ≡ | viet aJ | tel iant Setting / Agent Management | | | 💥 🖞 🤃 |
|------------|------------|--|------------------------|---------------|---------------|
| ē. | Agen | t management | | Guideline | |
| A | Agen | tID = "03D31B3FE60E83372C6EA3F8D5737FA19DBA598B" AND | First Ping | Last Ping 📋 🛛 | |
| | ۵ | AgentID | Agent ID | | |
| Ŧ | ۵ | ComputerName | Agent Computer Name | 📩 Vi | ew column 🗸 🗸 |
| ۹ | 00 | OS | Agent Operating System | POLICY | VERSION |
| 5- | Ø | Architecture | Agent Architecture | phula_test | 220 |
| | O | Platform | Agent Platform | N/A | 0.0.0 |
| × | O | Policy | Applied Policy | | |
| Ē <u>.</u> | ۲ | IPDCN | IP DCN | | |
| ē. | | | | | |
| | | | | | |

- Ví dụ về các câu tìm kiếm:
 - + Tìm kiếm với điều kiện "=":

| = | aJia | el Setting / Agent | Management | | | | | | | | | | * | ¢, | 0 |
|--------|-----------|-----------------------|------------|---------|--------------|---------------------|--|---------------------|--|-------------|--------------|--------|-----------|----|---|
| Ξ. | Agent | Agent management | | | | | | | | | 3 Guidelines | | | | |
| A | Policy = | "phula_test" | | | | | | | | | First Ping | 8 | Last Ping | • | Q |
| ۔ + | 1 result | t(s) | | | | | | | | | | 🛃 View | v column | | v |
| ۲ | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | | FIRST PING | | IP DCN | POLICY | | VERSION | | |
| _ | | Localhost.Localdomain | Offline | Default | Phula_test | 09/06/2022 10:43:58 | | 05/04/2022 14:49:51 | | 10.61.188.2 | phula_test | | | | _ |
| ⊾ | Display 1 | 1/1 result | | | | | | | | | | | | | |
| Ē | | | | | | | | | | | | | | | |
| ē. | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

+ Tìm kiếm với điều kiện "!=":



| ≡ | viette aJia | Setting / Agent | t Management | | | | | | | * | b ° () |
|-----------|----------------|-----------------|--------------|---------|--------------|---------------------|---------------------|-------------|---------------------|-------------|---------------|
| 1 T | Agent r | management | | | | | | | | 0 | Guidelines |
| A | Policy != | = "phula_test" | | | | | | | First Ping | Last Ping 📋 | Q |
| P.H | 2 result | (\$) | | | | | | | 🛃 Viev | v column | ~ |
| ۲ | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | FIRST PING | IP DCN | POLICY | VERSION | |
| _ | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | 10.61.188.2 | anhnn_full_features | 3.3.8 | |
| <u>}-</u> | | N/A | Offline | N/A | N/A | N/A | N/A | N/A | N/A | | |
| ◙ | Display 2 | 2/2 result | | | | | | | | | |
| ¢۵. | | | | | | | | | | | |
| | | | | | | | | | | | |
| ē | | | | | | | | | | | |

+ Tìm kiếm với điều kiện "~":

| | vietti aJia | el ant Setting / Agent | t Management | | | | | | | | | | * | ы [®] | 0 |
|-----------|-----------------------|---------------------------|-----------------------------|---------|--------------|---------------------|--|---------------------|--|-------------|------------------|-----|-------------|----------------|--------|
| Ę | Agent management | | | | | | | | | | | | | 🗿 Guide | elines |
| A | ComputerName - 'ubun' | | | | | | | | | | First Ping (| 3 | Last Ping 🗧 | | ۹ |
| ۶đ | 1 result | t(s) | | | | | | | | | ٤ | Vie | w column | , | , |
| ۲ | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | | FIRST PING | | IP DCN | POLICY | | VERSION | | |
| | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | | 07/06/2022 10:50:23 | | 10.61.188.2 | anhnn_full_featu | res | 3.3.8 | | |
| <u>}-</u> | Display | 1/1 result | | | | | | | | | | | | | |
| 0 | | | | | | | | | | | | | | | |
| Ē | | | | | | | | | | | | | | | |
| ē | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

+ Tìm kiếm theo tiêu chí kết hợp AND:

| ≡ | viette aJia | el Bint Setting / Agen | nt Management | | | | | | | | | * | 6 6 |
|--|------------------|----------------------------------|----------------------|---------|--------------|---------------------|--|---------------------|--|-------------|---------------------|-------------------|------------|
| a la | Agent management | | | | | | | | | | | Guidelines | |
| A | Compute | terName ~ "ubun" AND Policy = "a | anhnn_fuil_features" | | | | | | | | First Ping | Last Ping 📋 | Q |
| ₽ ₄ | 1 result(| (s) | | | | | | | | | 土 | View column | ~ |
| ۲ | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | | FIRST PING | | IP DCN | POLICY | VERSION | |
| _ | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | | 07/06/2022 10:50:23 | | 10.61.188.2 | anhnn_full_features | 3.3.8 | |
| 5 | Display 1 | I/T result | | | | | | | | | | | |
| • | | | | | | | | | | | | | |
| ¢, | | | | | | | | | | | | | |
| ٩ | | | | | | | | | | | | | |
| _ | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

+ Tìm kiếm theo tiêu chí kết hợp OR:

| ≡ | viette aJia | el ant Setting / Agent | t Management | | | | | | | æ ⊎ | 0 |
|----------|----------------|-----------------------------------|-----------------------------|---------|--------------|---------------------|---------------------|-------------|---------------------|-------------|----------|
| Ę | Agent | management | | | | | | | | 😗 Gui | idelines |
| A | Policy = | "anhnn_full_features" OR Policy = | "phula_test" | | | | | | First Ping | Last Ping 📋 | Q |
| Η | 2 result | :(s) | | | | | | | 👌 View | v column | ~ |
| ۲ | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | FIRST PING | IP DCN | POLICY | VERSION | |
| _ | | Localhost.Localdomain | Offline | Default | Phula_test | 09/06/2022 10:43:58 | 05/04/2022 14:49:51 | 10.61.188.2 | phula_test | | |
| <u>-</u> | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | 10.61.188.2 | anhnn_full_features | 3.3.8 | |
| Ø | Display 2 | 2/2 result | | | | | | | | | |
| Ê | | | | | | | | | | | |
| () () | | | | | | | | | | | |

Viettel Cyber Security

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



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

| ≡ | viettel a Jiant Setting / Agent Management 🗟 🎍 🕘 | | | | | | | | | | | ⊎ 0 | |
|----------|---|---------|-----------------------|-------------------------------|---------|--------------|---------------------|---------------------|--|-------------|---------------------|-------------|---|
| Ę | Agent management | | | | | | | | | | | Guidelines | |
| A | Type to search by quartes | | | | | | | | | | First Ping | Last Ping 📋 | Q |
| H, | 3 result(s) | | | | | | | | | | | × | |
| ۲ | s | Selecte | rd (2) Set Policy Mov | e to group 🦉 Set update group | Cancel | | | | | | | | |
| _ | | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | FIRST PING | | IP DCN | POLICY | VERSION | |
| <u>-</u> | T. | | Localhost.Localdomain | Offline | Default | Phula_test | 09/06/2022 10:43:58 | 05/04/2022 14:49:51 | | 10.61.188.2 | phula_test | | |
| ◙ | | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | | 10.61.188.2 | anhnn_full_features | 3.3.8 | |
| - | | | N/A | Offline | N/A | N/A | N/A | N/A | | N/A | N/A | | |
| ΕÅ | Dis | splay 3 | I/3 result | | | | | | | | | | |
| ē | | | | | | | | | | | | | |

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

| ≡ | viette aJia | int | Setting / Agent Management | | | | | | * | ы [.] О |
|--------------|----------------|--------------|--|--------------|---------------------|---------------------|-------------|---------------------|-----------|------------------|
| Ň | Agent m | nanager | ment | | | | | | • | Guidelines |
| A | Type to s | search by qu | ieries | | | | | First Ping | Last Ping | Q |
| ₹± | 3 result(s | s) | | | | | | خ Vie | w column | ~ |
| ۲ | Selected | d (2) | Set Policy Move to group Set update group Cancel | | | | | | | |
| | | NAME | Policies | UPDATE GROUP | LAST PING | FIRST PING | DCN | POLICY | VERSION | |
| <u>>-</u> | | Localhe | Select an Option | Phula_test | 09/06/2022 10:43:58 | 05/04/2022 14:49:51 | 10.61.188.2 | phula_test | | |
| ◙ | | Ubuntu | | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | 10.61.188.2 | anhnn_full_features | 3.3.8 | |
| | | N/A | | N/A | N/A | N/A | N/A | N/A | | |
| Ē, | Display 3/ | /3 result | default | | | | | | | |
| (B) | | | full_features | | | | | | | |
| Ψ. | | | full_features_khaitb | | | | | | | |
| | | | phula_test | | | | | | | |
| | | | full_features_v2 | | | | | | | |
| | | | anhnn_full_features | | | | | | | |
| | | | Full_AV | | | | | | | |
| | | | full fostures masse | | | | | | | |

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





5 – Xem chi tiết 1 agent bằng việc click duplicate chuột vào 1 row bất kỳ Hệ thống hỗ trợ người dùng thiết lập Policy, Update Group và Move to group cho Agent 1 cách nhanh chóng.

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

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

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

- Tab General info

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


| = | aJiant Setting / Agen | t Management | | | Offline Agent I Agent ID 31F6FA372944 | ocalhost.localdomain 1072C2DC854E155A63170CE9 | 586AD | | | Ô | (Uninstall | × |
|------------|---------------------------|--------------|---------|--------------|---|--|------------------------|-----------------|--------------------|----------------------------|-----------------|---|
| E. | Agent management | | | | First ping: 05/04/2022 1 | 14:49:51 Last ping: 09/06/20 | 22 10:43:58 | | | | | |
| A | Type to search by queries | | | | Agent properties | | | | | | | |
| τ. | 2 | | | | Set Policy | 5 | Set update group | Ma | ve to group | | | |
| | O result(s) | | | | phula_test | ~ | phula_test | ~ 0 | lefault | ✓ Save | changes | |
| 3 | NAME | STATUS | GROUP | UPDATE GROUP | | | | | | | | |
| _ | Localhost Localdomain | Offline | Default | Phula_test | About this agent | | | | | | | |
| 9 | Ubuntu18 | offline | Default | Test | < General info | Installation Files Version | Installed Certificates | Scheduled Tasks | Disks & nartitions | Environment variables | Installed softw | > |
| | <u>N/A</u> | Offline | N/A | N/A | | | instance continuates | Schoules Tasks | onado a partitiono | control intent randoles | | |
| | Display 3/3 result | | | | General info | | | Network | Interfaces | | | |
| Ξ <u>λ</u> | | | | | Host Name | localhost.localdomair | 1 | 1P v4 | 127. | 0.0.1 | | 1 |
| ē. | | | | | Host ID | 015a4d56-e545-241a | -e66b-14410ce8c348 | IP v6 | :1 | | | |
| | | | | | Setup Version | N/A | | MAC | N/A | | | |
| | | | | | Operating System | linux | | Name | lo | | | |
| | | | | | Platform | redhat | | IP v4 | 192 | 168.121.132 | | |
| | | | | | Platform Version | 8.2 | | IP v6 | fe80 | :437e:dc7a:2765:34ad | | |
| | | | | | Platform Family | rhel | | MAC | 00:0 | lc:29:e8:c3:48 | | |
| | | | | | Architecture | amd64 | | Name | ensi | 160 | | |
| | | | | | Physical Memory | 1,843,832 | | | | | | 1 |
| | | | | | CPUs | | | Default | Sateway | | | |
| | | | | | Come | 1 | | 102 168 | 121.2 | | | |
| | | | | | when | 1992 001000 | | 172.100. | 1.1.1. | | | |
| | | | | | Hadal Name | Intel/P) Core/TM) i7- | 10700T CRU @ 2 00GH+ | DNS Ser | ver | | | |
| | | | | | Vandor ID | GenuineIntel | 197991 919 (0 2.00012 | 192.168 | 121.2 | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

- 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

| ≡ | viette aJia | Setting / Agent | t Management | | | Offline Agent I Agent ID 31F6FA37294 | localhost.localdomain 4D72C2DC854E155A63170CE | :9686AD | | | | 🗂 Uninstall | × |
|----------|----------------|----------------------------------|---|---------|------------|--|--|--------------------------------------|----------------|----------------------|--------------------|---------------------|---|
| <u> </u> | Agent | management | | | | First ping: 05/04/2022 | 14:49:51 Last ping: 09/06/ | 2022 10:43:58 | | | | | |
| A | Type to | search by queries | | | | Agent properties | | | | | | | |
| ۶± | 3 result | (\$) | | | | Set Policy | ~] | Set update group | | Move to group | | Save changes | |
| ۲ | | NAME | E STATUS GROUP UPDATE GROU host Localdomáin e Offline Default Phula, test utilia e Offline Default Test | | | | | phula_test | | Gerauit | | Save changes | |
| | | Localhost.Localdomain | Offline | Default | Phula_test | About this agent | About this agent | | | | | | |
| D | | Ubuntu18 | allocat.cocatoonaan of Offline Default Productest ntul of Offline Default Test of Offline N/A N/A | | | | Installation Files Versi | n Installed Certificates | Scheduled Task | s Disks & partitions | Environment variab | les Installed softw | > |
| ◙ | | <u>N/A</u> | A Offline N/A N/A | | | | | _ | | | | | |
| ¢۵. | Display 3 | NA © Ottime N/A N/A /3 result | | | | Search by file name or ve | ersion | | | | | | Q |
| CA. | | 3 result | | | | AJIANT | | VESUpdater | | | | | |
| ۹ | | | | | | response | | VERSION 3.3.0 | | | | | |
| | | | | | | collector | | VERSION 3.3.0 | | | | | |
| | | | | | | drivers | | PERSON DISIO | | | | | |
| | | | | | | | | RWorker VERSION 3.3.0 | | | | | |
| | | | | | | | | VESConfigurationMar VERSION 3.3.0 | nager | | | | |
| | | | | | | | | Agentinfo VERSION 3.3.0 | | | | | |
| | | | | | | | | VESConnectionMana VERSION 3.3.0 | ger | | | | |
| | | | | | | | | | | | | | |

- Installed Certificates

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

Page | 37



+ Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn 0, hiển thị màn hình như sau:

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

- Scheduled Tasks

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

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

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



| XML Detail | × |
|--|------------|
| rml 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>\dfffff</uri> </registrationinfo> <triggers></triggers> <principals> <principal id="Author"> <userld>S-1-5-21-3942219608-2782901308-3935319899-500</userld> <logontype>InteractiveToken</logontype> <runlevel>LeastPrivilege</runlevel> </principal></principals> <settings> <multipleinstancespolicy>IgnoreNew</multipleinstancespolicy> <disallowstartifonbatteries>true</disallowstartifonbatteries> <stopifgoingonbatteries>true</stopifgoingonbatteries> <allowhardterminate>Irue</allowhardterminate> <startwhenavailable>false</startwhenavailable> <idlesettings> <stoponidleend>true</stoponidleend> <restartonidle>false</restartonidle></idlesettings></settings></task> | |
| | Let to XML |

Export to XML dể tải về thông tin scheduled task, hỗ trợ định dạng

.xml

- Disks & partitions

+ Chọn

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

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

Page | 39



| ≡ | aJia | Setting / Agent Mana | ogement | | | | Online Agent DESKTOP-R2GBJEF Agent ID 180A66FD56EDD4C2C6D557DDFDE794 | SF5040FCCC | | 🛍 Uninstall 🛛 🗙 |
|----------|-----------|----------------------|-----------|---------------|--------------|---------------------|--|--|-------------------------------|------------------------------------|
| <u>_</u> | Agent r | nanagement | | | | | First ping: 09/06/2022 11:28:00 Last ping: 29/ | 16/2022 18:23:58 | | |
| A | Type to | search by queries | | | | | Agent properties | | | |
| Ť | 9 | result(s) | | | | | Set Policy full_features_baolt | Set update group | Move to group | Save changes |
| ۰. | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | |) [| | |
| | | Bichpt3-Centos7 | © Offline | Default | Release | 28/06/2022 16:35:13 | About this agent | | | |
| | | DESKTOP-R2GBJEE | Online | Default | Release | 29/06/2022 18:23:58 | (| | Dista 6 contribution and | |
| 9 | | Win10x64bichpt3 | © Offline | Default | Release | 29/06/2022 17:36:14 | General info Installation Files ver | sion Installed Certificates schedured II | Joko Disks & partitions Envir | onment variables Installed softy r |
| Ŭ. | | Bichpt3-Ubuntu18 | © Offline | Default | Release | 29/06/2022 17:35:26 | VMware Virtual NVMe Disk | | | ^ |
| Ê | | WIN-T5BK3MCL9I0 | Offline | Default | Release | 28/06/2022 11:38:23 | Partition | C: | | |
| | | Anhnn19-Centos7 | Offline | Default | Release | 29/06/2022 14:11:30 | Volume Name | | | |
| * | | Centos6 | Offline | Default | Release | 29/06/2022 17:38:15 | Serial | 629825D5 | | |
| | | Win7x64-A-PC | Offline | Group_bichpt3 | Release | 28/06/2022 15:38:25 | Drive Type | Fixed | | |
| | | <u>N/A</u> | Offline | N/A | N/A | N/A | File System | NTFS | | |
| | Display 9 | /9 result | | | | | Capacity | 50553 MB | | |
| | | | | | | | Available | 25128 MB | | |
| | | | | | | | CD-ROM Disc | | | ^ |
| | | | | | | | Partition | D: | | |
| | | | | | | | Volume Name | ESD-ISO | | |
| | | | | | | | Serial | DD15656F | | |
| | | | | | | | Drive Type | CDRom | | |
| | | | | | | | File System | UDF | | |
| | | | | | | | Capacity | 4071 MB | | |
| | | | | | | | Available | 0 MB | | |
| | | | | | | 1 | | | | |

- Environment variables

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

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

| = | aJi | Setting / Agent Mana | gement | | | | Online Agent DESKTOP-R2GBJEF Agent ID 180A66FD56EDD4C2C6D557D0FD879A6F3 | 5040FCCC | | $	ilde{ m II}$ Uninstall $	imes$ |
|---|---------|----------------------|-----------|---------------|--|---------------------|---|---|--|----------------------------------|
| 4 | Agent | management | | | | | First ping: 09/06/2022 11:28:00 Last ping: 29/06/ | /2022 18:23:58 | | |
| A | Type to | search by queries | | | | | Agent properties | | | |
| | | | | | | | Set Policy | Set update group | Move to group | |
| È | 9 | result(s) | | | | | full_features_baolt ~ | release ~ | default ~ | Save changes |
| ۲ | | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | | | | |
| _ | | Bichpt3-Centos7 | Offline | Default | Release | 28/06/2022 16:35:13 | About this agent | | | |
| | | DESKTOP-R2GBJEF | Online | Default | Release | 29/06/2022 18:23:58 | General info Installation Files Versio | ion Installed Certificates Scheduled Te | eks Disks & partitions Environment v | ariables Installed softy > |
| • | | Win10x64bichpt3 | Offline | Default | Release | 29/06/2022 17:36:14 | - General Into Instanation Price Versio | on instance certificates acheored to | sks bisks a parabolis controllingit in | Instance Solly - |
| | | Bichpt3-Ubuntu18 | © Offline | Default | Release | 29/06/2022 17:35:26 | System | | | ^ |
| Ē | | WIN-T5BK3MCL9I0 | © Offline | Default | Release | 28/06/2022 11:38:23 | ComSpec | | | |
| | | Anhnn19-Centos7 | Offline | Default | Release | 29/06/2022 14:11:30 | %SystemRoot%\system32\cmd.exe | | | |
| - | | Centos6 | © Offline | Default | Release | 29/06/2022 17:38:15 | DriverData | | | |
| | | Win7x64-A-PC | Offline | Group_bichpt3 | Release | 28/06/2022 15:38:25 | C:\Windows\System32\Drivers\DriverData | | | |
| | | <u>N/A</u> | Offline | N/A | N/A | N/A | os | | | |
| | | | | | NTHERT COM, DELEAT, CMO, VIBL, VIBL, JO, JSE, WS PACCESSO, ARCHITECTURE ANDOL PROCEEDING, ARCHITECTURE ANDOL PROCEEDING ANDOL TURE VisitemBooth/TELIP VisitemBooth/TELIP USERNAM USERNAM | F, WSH, MSC | Shelivi OModules | | | |
| | | | | | | | NUMBER_OF_PROCESSORS 8 PROCESSOR_LEVEL 6 | | | |

- Tab Installed Software

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



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

- Tab Required Software

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

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

- Tab User list

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

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

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

| ≡ | vietti aJia | el ant Setting / Agent | t Management | | | | | | | 🗮 🖞 🕅 |
|-----------|----------------|---------------------------|-----------------------------|---------|--------------|---------------------|---------------------|-------------|---------------------|---------------|
| Ę | Agent | management | | | | | | | | 😗 Guidelines |
| A | Type to | search by queries | | | | | | | First Ping | Last Ping 📋 🔍 |
| Р | 3 result | t(s) | | | | | | | 🛃 Vie | w column 🗸 |
| ۲ | Select | ed (2) Set Policy Mov | e to group Set update group | Cancel | | | | | | |
| _ (| | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | FIRST PING | IP DCN | POLICY | VERSION |
| <u>}-</u> | | Localhost.Localdomain | Offline | Default | Phula_test | 09/06/2022 10:43:58 | 05/04/2022 14:49:51 | 10.61.188.2 | phula_test | |
| ◙ | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | 10.61.188.2 | anhnn_full_features | 3.3.8 |
| | 0 | N/A | Offline | N/A | N/A | N/A | N/A | N/A | N/A | |
| ΓA | Display : | 3/3 result | | | | | | | | |
| ē | | | | | | | | | | |
| | | | | | | | | | | |

+ Thực hiện Move to group:

Danh sách Group trong combobox Move to group:

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

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

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



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

| ≡ | viette aJia | el ant Setting / Agen | it Management | | | | | | | 光 山 | • 0 |
|-----|----------------|--------------------------|------------------------------|------------|--------------|---------------------|---------------------|-------------|---------------------|------------|-----------|
| | Agent | management | | | | | | | | 🕜 GL | uidelines |
| A | Type to | search by queries | | First Ping | Last Ping | Q | | | | | |
| ₽,± | 3 result | t(s) | 2 | | | | | | 🛃 Vie | w column | ~ |
| ۲ | Selecte | ed (2) Set Policy Mov | ve to group Set update group | Cancel | | | | | | | |
| _ | 1- | NAME | STATUS | GROUP | UPDATE GROUP | LAST PING | FIRST PING | IP DON | POLICY | VERSION | |
| ▶- | | Localhost.Localdomain | Offline | Default | Phula_test | 09/06/2022 10:43:58 | 05/04/2022 14:49:51 | 10.61.188.2 | phula_test | | |
| ◙ | | Ubuntu18 | Offline | Default | Test | 09/06/2022 17:24:22 | 07/06/2022 10:50:23 | 10.61.188.2 | anhnn_full_features | 3.3.8 | |
| | 0 | N/A | Offline | N/A | N/A | N/A | N/A | N/A | N/A | | |
| Ē | Display 3 | 3/3 result | | | | | | | | | |
| ē | | | | | | | | | | | |

• Thực hiện Set update group;

Lưu ý:

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

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

3.4.2 Policy Setting

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

| ≡ | aJiant Setting / Policy Set | tting | | | | | | 0 'ه 🕱 |
|---|-----------------------------|------------------|---|---------------------|---------------------|---------------------|-----------------------------|------------|
| 2 | Policy management | | | | | | Guidelines | + Create |
| ٩ | POLICY NAME T | NUMBER OF AGENTS | ٣ | CREATED TIME | UPDATED TIME | APPLIED TIME | STATUS | ¥ 💁 🖪 |
| | default | 0 | | 28/01/2019 14:11:52 | 03/12/2020 11:42:43 | 03/12/2020 11:42:50 | Applied | 1 |
| | cull_features | 0 | | 09/12/2021 10:20:00 | 26/05/2022 14:14:25 | 08/06/2022 13:54:08 | Applied | 0 0 |
| 1 | rull_features_khaitb | 0 | | 13/01/2022 13:49:13 | 13/01/2022 14:15:50 | 13/01/2022 14:15:53 | Applied | @ û |
| 1 | phula_test | 1 | | 14/01/2022 13:17:12 | 31/03/2022 13:07:30 | 31/03/2022 13:07:35 | Applied | ø ū |
| | full_features_v2 | 0 | | 17/01/2022 14:29:12 | 08/06/2022 16:02:34 | 08/06/2022 16:02:37 | Applied | 0 ū |
| | anhnn_full_features | 1 | | 08/02/2022 15:51:36 | 08/06/2022 16:19:12 | 08/06/2022 16:19:14 | Applied | @ ū |
| | FulLAV | 0 | | 01/03/2022 14:36:25 | 20/05/2022 15:02:30 | 20/05/2022 15:02:34 | Applied | a û |
| | full_features_macos | 0 | | 11/03/2022 18:22:01 | 18/03/2022 11:29:29 | 18/03/2022 11:29:32 | Applied | a û |
| | full_features_anhnn | 0 | | 15/03/2022 15:14:32 | 25/05/2022 17:50:28 | 25/05/2022 17:50:31 | Applied | Ø Ü |
| | full_features_baolt | 0 | | 17/03/2022 15:12:01 | 09/06/2022 15:32:37 | 09/06/2022 15:32:40 | Applied | a ū |
| | Showing 10/10 result(s) | | | | | | | |

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

1 – Hiển thị danh sách các Policy đã được tạo trên hệ thống. Mỗi 1 policy gồm các thông tin: Tên, số lượng Agent được áp chính sách, Thời gian tạo,



thời gian cập nhật, Thời gian áp chính sách, trạng thái (có 2 trạng thái: Applied và Not Applied);

 2 – Tạo mới một chính sách: Click vào nút "Create" hệ thống hiển thị Popup tạo mới chính sách như sau:



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

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

| Policy configuration tree | | | Cancel Save configuration |
|---|---|---|---|
| AGENT | SERVICE LIST | PLUGIN LIST | MODULE LIST |
| | ConfigurationManager ConnectionManager Updater Urviers Collector | WindowsEventLog Antikeylogger (3) PracessAnalysis PeriodicScan AdvanceCollector | EventSubcriber EventPolicy EventChannel (3) SysmonConfig |
| · ~ | E Response | Containment Containment ResponseScenario | |
| | Protection&Prevention | ApplicationControl EndpointFirewall BisPlugin © NacAuPlugin | |
| | De AutoScan - | AviraEngine PerformanceControl | |
| Configuration guidelines - Change mode of policy tree configuration: Press | s edit configuration button to edit | | |
| - In edit mode: Press check/uncheck button to a | udd/remove a node | | |
| - After completed editting: Press save configurat | tion button to save configuration or cancel button to comeback previous configura | tion | |

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

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



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

| Policy configuration tree | | | Cancel Save configuration |
|---|--|---|---|
| AGENT | SERVICE LIST | PLUGIN LIST | MODULE LIST |
| | ConfigurationManager ConnectionManager Updater Drivers 10 Collector | (WindowsEventLog Antikeylogger (8) ProcessAnalysis PeriodicScan (8) (AdvanceCollector (8) | I EventSubcriber 8 I EventSolicy 9 I EventSolicy 9 I EventSolicy 9 I SysmonConfig 9 |
| • | t Response | d LiveReponse E Containment d ResponseScenario | |
| | C Protection&Prevention | fi ApplicationControl fi EndpointFirewall E BloPlugin (2) NacAuPlugin | |
| | D AutoScan CoreService | C AviraEngine | |
| Configuration guidelines - Change mode of policy tree configuration: Press - In edit mode: Press check/uncheck button to ac - After completed editting: Press save configurati | edit configuration button to edit dd/remove a node o button to save configuration or cancel button to comeback previous configur | ation | |

Bước 3: Sau khi hoàn thành chế độ edit:

• Người dùng nhấn nút "Save config" để lưu các thay đổi;

• Người dùng nhấn nút "Cancel" để hủy thao tác cập nhật Policy và hệ thống quay lại cấu hình trước đấy.

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

- WindowsEventLog: cấu hình các nguồn log lấy dưới Agent:
- EventSubcriber: chỉ định các kênh lấy log
- Yêu cầu dữ liệu:

+ Trường **event_filter** (lọc theo Event ID): các string con cách nhau dấu phẩy (,);

VD: "4": loc các event có eventID = 4

"-689": loc các event có eventID # 689

- + Trường **providers** các string con cách nhau dấu chấm phẩy (;);
- + Các trường bắt buộc phải điền: subs_type, channel;



- + Channel: nguồn log;
- + sub_type:
 - PUSH: khi có event mới → gọi hàm của VCS-aJiant để xử lý;
 - POLLING: VCS-aJiant sau 1 khoảng thời gian chủ động lấy log;
 - PULL: VCS-aJiant chủ động lấy log sau 1 khoảng thời gian;
- Sau khi cấu hình xong cần Save lại:

| Event subscriber configuration | | | | | Clear Save |
|--------------------------------|--------------------------------|--|-------------|----------------------------|------------|
| SUBSCRIBER TYPE | CHANNEL | EVENT FILTER | LEVEL | PROVIDERS | |
| Click to select | ✓ Type to | Multi value separated by , | Select 🗸 | Multi value separated by ; | Create |
| PULL | System | 7040 | information | | û |
| PULL | System | 7040,7045 | | | ū |
| PULL | Security | 4624,4625,4698,4699,4700,4701,4702,4697,4738, 4720,4785,4787,5136,5137,5138,5139,5141 | | | ŵ |
| PULL | AdvanceCollector/Operational | | | | ŵ |
| PULL | ApplicationControl/Operational | | | | Û |
| PULL | EndpointFirewall/Operational | | | | ŵ |
| PULL | VEDR | 300 | | | Û |

+ EventPolicy: Thiết lập policy để enable/disable 1 số loại log mà hệ thống mặc định chưa có;

• Yêu cầu: có ít nhất 1 trường được chọn

| AUDIT POLICIES CROUP | E | vent policy configuration | |
|---|---|---------------------------|-----------------------------|
| Account Logon Powershell Account Management Detail Tracking Detail Tracking | A | JDIT POLICIES | GROUP POLICIES |
| Account Management Process Create Command Line Detail Tracking | | Account Logon | Powershell |
| Detail Tracking | | Account Management | Process Create Command Line |
| | | Detail Tracking | |

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

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

khi file log đầy có log mới sẽ ghi đè lên log cũ nhất);

- Log file path: đường dẫn file log;
- Log file size: kích thước file log;
- Yêu cầu: tất cả dữ liệu đều phải điền;



| Event channel configuration | | | | Cites Save |
|-----------------------------|-----------|---------------|---|------------|
| CHANNEL | LOGROTATE | LOG FILE PATH | LOG FILE SIZE (BYTES) | |
| Type to | | Type to | Note: max 52428800[50MB] min 10485760(10MB) | Create |
| Chanel | 8 | %hffha% | 10485760 | <u> </u> |
| | | | | |
| | | | | |
| | | | | |

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

| s | ysmon | config | guration | | | Create |
|---|----------|--------|-------------|----------------|----------------|--------|
| 4 | urrent o | onfig | | Description | disable common | • |
| | Params | s | -accepteura | Description | disable sysmon | |
| | # | NO. | PARAMS | DESCRIPTION | | # |
| | 0 | 1 | -accepteula | disable sysmon | | 0 🖬 |
| | | | | | | |
| - | | | | | | |

• Antikeylogger: là một SelfRun Plugin của VCS-aJiant, có nhiệm vụ định kỳ quét toàn bộ máy để tìm ra KeyLogger đang chạy trên máy nếu có;

- Scan setting: cấu hình các loại KeyLogger cần quét;
- Yêu cầu:
 - Scan cycle: min là 1 phút, max là 180 phút;
 - Chọn ít nhất 1 loại Keylogger;

+ Whitelist setting: cấu hình whitelist 1 số phần mềm theo đường dẫn của file trên ổ đĩa hoặc theo chữ ký số (cert) của file chạy key logger

- Yêu cầu: điền đầy đủ các trường;
- Sau khi nhập xong cần "Save" lại cấu hình:

| White list setting | | | Clear |
|--------------------|-------------|--|---------|
| WLTYPE | SCAN TYPE | DATA | |
| Select 🗸 | Select 🗸 | Type to | Add new |
| WhiteListCer | Rawinput | Microsoft Corporation | Û |
| WhiteListPath | HookMessage | C:\users\win 10 64\desktop\unikey40rc2-1101-win64\unikeynt.exe | ŵ |

+ Self defend: Bổ sung cơ chế chống unintall cho Self Defense;

• Yêu cầu: Lựa chọn Chọn Drivers > Tích chọn Self Defense để bật tính năng Self Defense hoặc bỏ chọn để tắt > chọn Save > chọn Apply Policy;

• Sau khi cập nhật thay đổi xong cần "Save" lại cấu hình:



| Vertet aliant Policy detail - anhnn_full_features + basked Updave Ordecor Collector Response ProtectionsDrevest AttoScan Cordservice | Mindows/wmit.og ProcessAnalyss Profedicican AdvanceCollector Ukrehterponor Contamment ResponseScenario BisFrugan AdviseControl EndoponteForevolal BisFrugan AdviseControl | عند الله الله الله الله الله الله الله الل |
|--|--|--|
| Driver configuration Diable all File Monitoring Process Monitoring Network Monitoring | Registry Monitoring Soft Defense Pipe Monitoring Update configuration accompany | Sare |

Bước 5: Click nút dễ thiết lập Policy vừa được cấu hình cho Agent:

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

| Clone from policy: test_sample |
|-----------------------------------|
| NAME OF POLICY |
| Enter name of policy |
| Create |

+ Xóa chính sách: Click vào nút ¹ 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;

Page | 47



| Delete Policy | × |
|--|---|
| Do you want to delete policy: <i>hieupc4</i> This policy has been assigned to agent(s). If this policy is deleted, agent(s) will be reset to default policy! | |
| Cancel Accept | |

+ Khi click đúp vào từng bản ghi hệ thống sẽ chuyển tiếp tới trang chi tiết của 1 policy để người dùng xem/ thay đổi cấu hình cho Policy.

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

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



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

- Danh sách nhóm hiển thị theo dạng cây bao gồm các nhóm gốc và mỗi nhóm gốc gồm các nhóm con cấp 1, cấp 2...

- Mỗi nhóm gồm tên nhóm, thông tin cấu hình của nhóm (rule, policy, apply to), và danh sách agent thuộc nhóm.

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

- Khi user thuộc group con, chọn group cha sẽ không nhìn thấy popup group detail

2 – Tìm kiếm nhóm

+ Cách 1: Click vào textbox Search > hiện danh sách các nhóm của tương ứng với user đang login có thể scroll được > Chọn nhóm trong danh sách hiện ra;

+ Cách 2: Click vào textbox Search > nhập ký tự tìm kiếm vào textbox > hệ thống tự động tìm kiếm các bản ghi chứa ký tự nhập vào > Chọn 1 bản ghi phù hợp trong danh sách gợi ý hoặc click Search hoặc Enter sẽ hiện danh sách các bản ghi thỏa mãn;

| ≡ | viettel aJiant | Setting / Group Man | agement | | | | | | | | × 0 |
|------------|-----------------------|---------------------|----------------|-----|---------|---|------------|---|-------------------|--------------|-----------|
| ē. | Group managem | ent | | | | | Guidelines | vcs_anm | | | × |
| ▲ | Type group name to se | arch | | | | ٩ | Create | Detail information | Ag | gent list | User list |
| ÷ | 🗅 viettel | > | khoi_phu_thuoc | → D | vcs_anm | | | | | | |
| ۲ | | | | | | | | Rule | | | 0 |
| 57 | | | | | | | | Moving agent to this group if All Y follo | owing conditions | matched : | |
| | | | | | | | | IP_DCN 10.61.188.2/32 | | | |
| ž | | | | | | | | Policy | | Update group | |
| U <u>A</u> | | | | | | | | beta vrs | ~ | beta | ~ |
| ē | | | | | | | | Apply policy immediately when rule matched | | | |
| | | | | | | | | | | | |
| | | | | | | | | Apply to | | | |
| | | | | | | | | Applying to existing agents may take a while, | you can check lat | ter. | |
| | | | | | | | | New agents only | ~ | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | _ | | | Apply | |

viettel

Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.

+ Tab thông tin chi tiết hiển thị là Detail, dữ liệu của group đó là Rule, Policy, Apply to;

+ Khi chọn tab Agent list thì dữ liệu thông tin các agent match với group đó.

+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 2 option: Go to group và Delete group.

+ Nếu chọn Go to group thì đưa user đến vị trí của group đó trên cây;

+ Nếu chọn Delete group thì hiển thị popup confirm xóa group.

- Khi click vào menu góc phải mỗi ản ghi cũng hiển thị 2 option: Go to group và Delete group.

3 – Thêm mới nhóm:

+ User đăng nhập thuộc group root: Có thể them mới tất cả Group trong;

+ User đăng nhập thuộc group default: Không thể thêm mới;

+ User đăng nhập thuộc group cha: có thể thêm mới group con tương ứng của group thuộc user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: có thể them mới group con tương ứng của group thuộc user đang login;

Bước 1: Lựa chọn vị trí nhóm sẽ tạo

+ Nếu tạo mới nhóm ở danh sách nhóm gốc, click nút "Add new" góc phải màn hình hoặc hover vào cuối danh sách nhóm gốc trên màn hình, click Add new ;



| ≡ | viettel aJiant | Setting / Group Man | agement | | | | | | | # 0 |
|------------|------------------------|---------------------|----------------|---|-----------|---|------------|---|----------------------|------------|
| ē. | Group managem | ent | | | | 6 | Guidelines | vcs_anm | | × |
| ▲ | Type group name to see | irch | | | | Q | Create | Detail information | Agent list | User list |
| 7 <u>4</u> | 🗅 viettel | > | khoi_phu_thuoc | > | C vcs_anm | | | | | |
| ۲ | | | | | | | | Rule | | 0 |
| 57 57 | | | | | | | | Moving agent to this group if All Y following | conditions matched : | |
| | | | | | | | | IP_DCN 10.61.188.2/32 | | |
| ÷ | | | | | | | | Policy | Update group | |
| E7 | | | | | | | | hata use | V has | |
| ē | | | | | | | | Anniv nolicy immediately when nile matched | Deta | |
| | | | | | | | | Adda have a second and a second | | |
| | | | | | | | | Apply to | | |
| | | | | | | | | Applying to existing agents may take a while, you ca | n check later. | |
| | | | | | | | | New agents only | \sim | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | Apply | |

+ Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2... thì click vào nhóm cha sau đó click "Create" trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click "Create";

Bước 2: Nhập tên nhóm và cấu hình luật;

Lưu ý: tên và luật cấu hình không được trùng với tên và luật đã có.

+ Nếu chọn toán tử "All": luật thỏa mãn khi cả 2 trường được thỏa mãn;

+ Nếu chọn toán tử "Any": luật thỏa mãn khi 1 trong 2 hoặc cả 2 trường thỏa

mãn;



| ≡ | viettel aJiant | Setting / | Group Management | | | | | | × 0 |
|----|-----------------------|-----------|------------------|-------------|-----------|--------------|---|----------------------|------------------|
| ē | Group managem | ent | | | | 3 Guidelines | EDR_group | | |
| ▲ | Type group name to se | arch | | | 2 | Create | Detail information | Agent list | User list |
| Έŧ | ettel | > | L khol_phu_thuoc | > 🗅 vcs_anm | EDR_group | × | Rule | | 3 Cancel Save |
| 8 | | | | | | | Moving agent to this group if All v following | conditions matched : | |
| | | | | | | | IP Type rule value | | |
| ¢λ | | | | | | | | | |
| ē | | | | | | | | | |
| | | | | | | | Add rule | | |
| | | | | | | | Policy | Update group | |
| | | | | | | | default | × | ~ |
| | | | | | | | Apply policy immediately when rule matched | | |
| | | | | | | | Apply to | | |
| | | | | | | | All existing and new agents | ~ | |
| | | | | | | | | | |
| | | | | | | | | | |

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

- Sau khi click Apply kiểm tra agent được chuyển nhóm trong tab Agent list: danh sách agent thỏa mãn luật và được chuyển nhóm sang nhóm vừa thêm. Tùy thuộc vào lựa chọn ở phần "Apply to" để chuyển nhóm cho các agent trong hệ thống:

+ All existing agents: chuyển nhóm cho tất cả agent đang tồn tại trong hệ thống, các agent cài mới sau khi apply nếu có khớp luật cũng KHÔNG chuyển nhóm;

+ New agents only: chỉ chuyển nhóm cho các agent cài mới sau khi Apply, các agent đang tồn tại trên hệ thống nếu khớp luật cũng KHÔNG chuyển nhóm;

+ All existing and new agents: chuyển nhóm cho tất cả agent đang tồn tại trong hệ thống và agent cài mới sau khi apply nếu khớp luật;

Lưu ý:

+ Nếu chọn checkbox "Apply policy now when rule matched", sau đó click "Apply" thì với các agent được lựa chọn Apply sẽ kiểm tra các giá trị nếu khớp với luật đã cấu hình sẽ chuyển policy cho agent sang policy đã chọn ở mục "Policy", đồng thời chuyển nhóm;

Trong trường hợp ko chọn checkbox trên thì sau khi Apply, các agent được chọn Apply chuyển nhóm nhưng không chuyển policy, tức là agent giữ nguyên policy trong



khi chuyển sang nhóm có policy khác; với các agent cài mới nếu khớp luật thì chuyển nhóm và được áp policy "**default**" do không chọn checkbox > áp policy mặc định;

+ Nếu agent mới khớp luật của nhiều nhóm sẽ ưu tiên chuyển vào nhóm được tạo mới nhất, không tính thời gian sửa nhóm.

- 4 Sửa nhóm: có thể lựa chọn sửa 1 hoặc 2 hoặc cả 3 thành phần trong một nhóm: Rule, Policy, Apply to
 - + User đăng nhập thuộc group root: Có thể sửa tất cả group trong hệ thống;
 - + User đăng nhập thuộc group default: Không được sửa group default;

+ User đăng nhập thuộc group cha: Có thể sửa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả group thuộc user đang login;

+ Để sửa Rule (luật) của nhóm, click vào icon Edit > Chỉnh sửa luật của nhóm sau đó click Save > Sau đó có thể chỉnh sửa ở mục "Policy" và "Apply to" rồi click Apply;

| vcs_anm | | × |
|--|---------------------------|-----------|
| Detail information | Agent list | User list |
| Rule Moving agent to this group if All v follo IP_DCN 10.61.188.2/32 | wing conditions matched : | Edit |
| Policy | Update group | |
| beta_vcs | ∨ beta | ~ |
| Apply to Applying to existing agents may take a while, y | rou can check later. | |
| New agents only | \sim | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |



| vcs_anm | | | × |
|--|--------------------|--------------|-------------|
| Detail information | Ag | ent list | User list |
| Rule | | | Cancel Save |
| Moving agent to this group if All v fol | llowing conditions | matched : | |
| IP DCN • 10.61.188.2/3 | 2 | | |
| | | | |
| | | | |
| | | | |
| Add rule | | | |
| Policy | | Update group | |
| beta_vcs | ~ | beta | ~ |
| Apply policy immediately when rule matched | | | |
| Apply to | | | |
| New agents only | ~ | | |
| | | | |
| | | | |
| | | Apply | |

Lưu ý:

+ Trường hợp sửa các thành phần của nhóm (Rule, Policy hoặc Apply to) sau đó ko click Apply thì nội dung chỉnh sửa đã được lưu lại, nhưng không cập nhật Agent list. Với các Agent cài mới thì xử lý như sau:

 Chuyển nhóm: phụ thuộc Agent mới có được chọn ở mục "Apply to" hay không, nếu được chọn sẽ kiểm tra phía Agent, khớp luật của nhóm sẽ được chuyển vào nhóm;

 Apply policy: policy của agent phụ thuộc việc chọn checkbox "Apply policy now when rule matched", nếu checkbox được chọn thì sẽ apply policy của nhóm, nếu không được chọn sẽ áp policy "default" do không chọn checkbox sẽ áp policy mặc định.

+ Trường hợp sửa xong các thành phần của nhóm rồi click Apply thì nội dung chỉnh sửa được lưu lại, đồng thời nếu có lựa chọn "All existing agents" trong

 Viettel Cyber Security

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

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



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;

| ≡ | aJiant | Setting / Group Man | agement | | | | | | | | | 8 0 |
|--------------|-------------------------|---------------------|-------------|-------|---|----------------------|---------------------------------|-------------------|-------------------------------------|-------------------|-----------|------------|
| en T | Group managemen | nt | | | | | 2 Suidelines | huyenpk_gr | oup | | | × |
| • | Type group name to sear | :h | | | | | Q Delete Create | Detail in | formation | Agent list | User list | |
| - <u>-</u> - | 🗅 admin | > | 🗅 new_gro | up | > | huyenpk_group | | | | | | |
| ۹ | 🗅 default | | 🗅 test_wile | lcard | | | | Rule | | | | 0 |
| | 🗅 global | | hbc_ser | er | | | | Moving agent to t | his group if All Y following cond | ditions matched : | | |
| | | | 🗅 auto_ter | t | > | | | IP_DCN | 123.123.12.31/241 | | | |
| • | | | 🗅 no_grou | p | > | | | Balley | | Undate group | | |
| <u>α</u> λ | | | C chuyen | test | > | Delete | | × | | opuace group | | |
| ē | | | | | | - | | | ~ | | | |
| | | | | | | Are you sure you wan | t to delete group : huyenpk_gro | oup ? | slately when rule matched | | | |
| | | | | | | | | | | | | |
| | | | | | | Ca | Delete | | agents may take a while, you can ch | eck later. | | |
| | | | | | | | | All existing and | new agents 🗸 🗸 | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | Apply | | |



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

| vcs_anm | | | | | |
|------------------------------|--------------|--------------|-----------|---|---|
| Detail information | | Agent list | | User list | |
| 50/279 agent(s) | | Search agent | | | |
| AGENT ID | HOSTNAM | IE GROUP | STATUS | POLICY | # |
| 4AE8D11BFB5037899FD20F5CEDF | ANM-HOANGNE | D31 vcs_anm | • Offline | full_features_with_autoscan_selfdefense | × |
| \1B37DBD39D0F632D9F7BEFBE421 | ANM-SANGLV11 | 1 vcs_anm | • Offline | full_features_with_autoscan_selfdefense | × |
| 75E895D48390F5C642FC57AD62C | ANM-THONGNE | 07 vcs_anm | • Offline | full_features_with_autoscan_selfdefense | × |
| (F8AF3B15A9A343F992D3596EBA3 | ANM-HOABT21 | vcs_anm | • Offline | full_features_with_autoscan_selfdefense | × |
| 2FA6F1E3E016C748600CAF0C1A7 | ubunbu-18 | vcs_anm | • Offline | full_features_3.3.0 | × |
| :5CA1E94EC4C99ACE5EDB202FD7E | ANM-ANHNN19 |) vcs_anm | • Offline | full_features_with_autoscan_selfdefense | × |
| 9ACE6C4888F8E1F04428BC8BDD1 | IS-LANNT | vcs_anm | • Offline | beta_vcs | × |
| 343E35A30D5CC8EFC65AC7A83EB1 | ANM-THANGNM | /14 vcs_anm | • Offline | full_features_with_autoscan | × |
| A04CF97FF6250F800308CE68352 | ANM-DUCDH8 | vcs_anm | • Offline | full_features_with_autoscan_selfdefense | × |
| | | | | | |

Lưu ý: trường hợp xóa một nhóm cha:

+ Xóa tất cả nhóm con;

+ Chuyển tất cả agent của nhóm cha và các nhóm con về nhóm mặc định: "default":

- + Giữ nguyên policy của các agent trong nhóm cha và con;
- 6 Thêm mới user vào group

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

Viettel Cyber Security



| aJiant | t | Settin | g / Group Management | | | | | | | | # 0 |
|--|-------------------------|---------|-------------------------|-------------------|-----------------------------|---------------|---------------------|----------------------|-------------------------|---------|-------------------|
| Froup man | nageme | ent | | | | | O Guidelines | admin | | | |
| Type D Ar | dd us | er to | group | | | | | | Cancel | er list | 1 Nysteen same |
| ~ | u | lser av | ailable to add to group | , | | User in group | | | | | * |
| 0 | | NC | USERNAME | FULLNAME | EMAIL | | USERNAME | FULLNAME | EMAIL | tive | × |
| No. Description Image: Second secon | 2 | 1 | admin | | t | 0.1 | iml_edr | iml_edr | iml_edr@ajiant.com | tive | × |
| | alert_viewer@ajiant.com | □ 2 | is_toanbd | is_toanbd@adf.com | is_toanbd@adf.com | tive | × | | | | |
| | ć | 3 | anhbd25 | | t1 | 3 | khaitb | Trần Bá Khai khaitb@ | khaitb@viettel.com.vn | | |
| | C | 4 | anhnn | | anhnn@gmail.com | □ 4 | thanhln9 | thanhin9 | thanhIn9@viettel.com.vn | | |
| | C | 5 | anhnn19 | | tba | | | | | | |
| | C | 6 | anhvn | | anhvn@gmail.com | | | | | | |
| | C | 7 | autotest151 | fullname | clint.kris@yahoo.com | | | | | | |
| | C | 8 | autotest281 | fullname | marjory.ritchie@hotmail.com | | | | | | |
| | C | 9 | autotest289 | fullname | alec.stamm@gmail.com | | | | | | |
| | E | 10 | autotest35 | fullname | alica.lueilwitz@gmail.com | | | | | | |
| | C | 11 | autotest362 | fullname | mao.huel@hotmail.com | | | | | | |
| | | 12 | autotest419 | fullname | rachael.pouros@hotmail.com | | | | | | |
| | | 13 | autotest457 | fullname | clyde.grady@gmail.com | | | | | | |
| | | 14 | autotest5 | fullname | mckinley.ratke@gmail.com | | | | | | |

- Danh sách user:
 - + User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;
 - + User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

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

7 – Xóa user

| ≡ | aJiant Setting / Group | Managerr | ent | | | | | | | | # 0 |
|----|---------------------------|----------|---------------|---|-----------------|------|--------------------|----------|---------------------------|----------------------------|-------------------------------|
| Ę | Group management | | | | Ø Guidelines | test | _wildcard | | | | × |
| A | Type group name to search | | | | Q Delete Create | | Detail information | | Agent list | User li: | st |
| - | 🗅 admin | > C |] new_group | | | 3 us | er(s) | | Type to filter user | | Update user |
| | 🗅 default | C | test_wildcard | | | NO. | USERNAME | FULLNAME | EMAIL | STATUS | $\overline{\mathbf{X}^{(i)}}$ |
| অ | 🗅 global | C |] hbc_server | | | 1 | anhvn | anhvn | anhvn@gmail.com | Active | × |
| | | C |] auto_test | > | | 2 | autotest107 | fullname | jackie.anderson@yahoo.com | Active | × |
| | | C | no_group | > | | 3 | autotest11 | fullname | sondra.trantow@yahoo.com | Active | × |
| Ē. | | C | chuyen_test | > | | | | | | | |
| ē | | | | | | | | | | | |

3.4.4 Account Management

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



3.4.4.1 *Permission management*

- Quản lý các quyền truy cập vào tài nguyên (API) của hệ thống. 1 permission là quyền truy cập vào 1 tài nguyên xác định (API) của hệ thống;

- Các chức năng chính trên màn hình này:
 - + Quản lý các permission;
 - + Tìm kiếm permission;
 - + Xóa permission;
- 1 Quản lý các permission: hiển thị toàn bộ các permission của hệ thống. Trong trường hợp xóa permission trên màn hình này, khi thực hiện các chức năng trên portal mà bị thiếu permission thì sẽ tự động thêm permission đã xóa trên màn hình quản lý Permission
- 2 Tìm kiếm permission: nhập ký tự tìm kiếm vào texbox Search > click
 Enter hoặc nút "Search" => hiển thị danh sách permission thỏa mãn

| aJiant | Setting / Account Management / Permission Management | | | |
|---------------------|--|-------------|---|--------|
| Permission mar | nagement | | | 0 |
| Type permission nar | ne to search | | • | 2 |
| | | | | |
| 56 result(s) | | | | |
| NO. PERMISSION | NAME | DESCRIPTION | ROLE LIST | ACTION |
| 1 agent_ma | nagement_manage | | manage_agent_management, manage_containment, manage_deploy_tool, root | 0 11 |
| 2 agent_mai | nagement_read | | liennt_test, manage_investigation_result, root, view_agent_management,View | 0 11 |
| 3 agent_pol | cy_manage | | manage_policy_management, root | 0 11 |
| 4 agent_pol | cy_read | | liennt_test, root, view_policy_management | 0 1 |
| 5 agent_rear | 3 | | | 0 11 |
| 6 alert_read | | | | 0 11 |
| 7 alert_man | ager | | manage_alert, root | 0 1 |
| 8 alerts_rear | 1 | | root, view_alert | 0 11 |
| 9 appctrl_ha | ndler_manage | | manage_appctri_handler, root | 0 11 |
| 10 appctrl_ha | ndler_read | | root, view_appctrl_handler | 0 11 |
| 11 artifact_ha | ndler_manage | | manage_event_search, manage_investigation_result, manage_process_analysis, root | 0 11 |
| 12 artifact_ha | ndler_read | | root, view_investigation_result, view_irflow, view_process_analysis | 0 11 |
| 13 artifact_m | anage | | manage_detection, root | 0 11 |
| 14 containme | nt_manage | | manage_containment, manage_irflow, root | 0 11 |
| 15 containme | nt_read | | root, view_containment, view_irflow | 0 11 |
| 16 correlation | _manage | | | 0 11 |
| 17 correlation | Lread | | | 0 11 |
| 18 dashboard | _read | | default, root | 0 11 |
| 19 deploy_to | ol_handler_manage | | manage_deploy_tool, manage_investigation_tool, manage_irflow, root | 0 11 |
| 20 deploy_to | ol_handler_read | | manage_investigation_result, root, view_deploy_tool, view_investigation_result,View | 0 11 |
| 21 endpointfi | v_handler_manage | | liennt_test, manage_endpointfw_handler, root | 0 ū |

3 – Xóa permission: click icon "Delete" > click "OK" trên màn hình confirm là xóa thành công:



| = | viettel aJiant Setting / Account Management / Permission Management | | | | # 0 | |
|----------------|---|--|--------------|--|--------------|--|
| en en | Permission management | | | | @ Guidelines | |
| | Type permission name to search | | | | Q | |
| 45 | | | | | | |
| H ⁴ | 56 result(s) | | | | | |
| ۹ | NO. PERMISSION NAME | DESCRIPTION | ROLE LIST | | ACTION | |
| _ | 1 agent_management_manage | | manage_a | ent_management, manage_containment, manage_deploy_tool, root | 0 | |
| - | 2 agent_management_read | | liennt_test, | manage_investigation_result, root, view_agent_management,View | 0 1 | |
| • | 3 agent_policy_manage | | manage_p | olicy_management, root | 0 🗊 | |
| _ | 4 agent_policy_read | | liennt_test, | root, view_policy_management | 0 11 | |
| ЦÂ | 5 agent_read | Delote | × | | 0 11 | |
| Ø | 6 alert_read | Delete | | | 0 11 | |
| | 7 alert_manager | | | irt, root | 0 11 | |
| | 8 alerts_read | Are you sure you want to delete permission : agent_read ? | | ilert | 0 1 | |
| | 9 appctrl_handler_manage | | | pctrl_handler, root | 0 Ū | |
| | 10 appctrl_handler_read | Cancel Delete 2 | | ippctrl_handler | 0 11 | |
| | 11 artifact_handler_manage | | | ent_search, manage_investigation_result, manage_process_analysis, root | 0 11 | |
| | 12 artifact_handler_read | | root, view_ | investigation_result, view_irflow, view_process_analysis | 0 D | |
| | 13 artifact_manage | | manage_de | stection, root | 0 11 | |
| | 14 containment_manage | | manage_co | ntainment, manage_irflow, root | 0 | |
| | 15 containment_read | | root, view_ | containment, view_irflow | 0 | |
| | 16 correlation_manage | | | | 0 11 | |
| | 17 correlation_read | | | | 0 10 | |
| | 18 dashboard_read | | default, roo | ¢ | 0 11 | |
| | 19 deploy_tool_handler_manage | | manage_de | ploy_tool, manage_investigation_tool, manage_inflow, root | 0 11 | |
| | 20 deploy_tool_handler_read | manage_investigation_result, root, view_deploy_tool, view_investigation_result | | | | |
| | 21 endpointfw_handler_manage | | liennt_test, | manage_endpointfw_handler, root | 0 1 | |
| | Showing 25/56 result(s) | | | | | |

3.4.4.2 Role Management

- Quản lý các role (nhóm quyền hay nhóm permission) của hệ thống;
- Các chức năng trên màn hình này bao gồm:
 - + Quản lý danh sách role:
 - User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống;
 - User đăng nhập thuộc Role default: Hiển thị Role default;

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

• User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login;

- + Tìm kiếm role;
- + Thêm mới role;
- + Xóa role.
- 1 Quản lý danh sách role: quản lý danh sách role theo dạng cây. Có 2 role
 ở gốc mặc định đã tạo sẵn: role "default" và "root"

Page | 59



+ Role "default": User có quyền "default" chỉ có quyền truy cập vào Portal, không có quyền xem dữ liệu hoặc thao tác chức năng;

+ Role "root": bao gồm toàn bộ các role của hệ thống, User có role "root" có toàn bộ quyền sử dụng tất cả chức năng trên Portal;

+ Click vào 1 role sẽ hiển thị thông tin chi tiết của role. Một role sẽ bao gồm các thông tin: tên role, danh sách các permission, danh sách User (tài khoản) chứa role, role cha hoặc danh sách role con (nếu có)

2 – Tìm kiếm role

+ Cách 1: Click vào textbox Search > hiển thị danh sách các role trong hệ thống và có thể scroll được danh sách role > Lựa chọn role trong danh sách hiện ra

+ Cách 2: Click vào textbox Search > Nhập ký tự tìm kiếm vào textbox > Hệ thống lọc ra các role chứa ký tự tìm kiếm > chọn role trong danh sách đã lọc hoặc click Enter hoặc click nút "Search"

| ≡ | viettel aJiant | Setting / Account Management / Role Management | | × 0 |
|---|------------------------|--|------------------|--|
| ē. | Role Managemer | it | @ Guidelines | root × |
| A | Type role name to sear | ch | Create role | Detail information User list |
| ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- ,- , | For enangement | nagement andler Imanage_deploy_tool manage_deploy_tool manage_detection manage_event_search manage_group_management manage_group_management manage_lowestigation_result | Costerois | root x Detail information User list Detail information User list Rede detail information Rute root (root) Dorson Detection Detail information Permission list read containment_read containment_manage agent_management_manage agent_management_read agent_management_manage agent_policy_read agent_management_manage agent_manage agent_mana |
| | | manage_investigation_tool manage_inflow manage_inflow | | update_group_manage appcrti_handier_read appcrti_handier_manage endpointhv_handier_read endpointhv_handier_manage violation_statistic_handier_read software_statistic_handier_read software_read patch_statistic_handier_read patch_read proxy_read proxy_manage alter_read enhance_alter_mad databload_read correlation_manage correlation_read |
| | | manage_priv(epponte manage_permission_management manage_process_analysis | | |

- Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.
 - Tab thông tin chi tiết hiển thị là Detail, dữ liệu của role bao gồm thông tin role và các permission của role đó;



• Khi chọn tab User list là danh sách User chứa role;

+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị Go to role. Click vào "Go to role" đưa về danh sách role dạng cây ban đầu;

+ Khi click vào menu góc phải mỗi bản ghi cũng hiển thị option: Go to role;

3 – Thêm mới role:

+ User đăng nhập thuộc group root: Có thể them mới tất cả role trong các cây dữ liệu;

+ User đăng nhập thuộc group default: Không thể thêm mới;

+ User đăng nhập thuộc group cha: Có thể thêm mới role con tương ứng của group thuộc user đang login, không thể them mới role cùng cấp;

+ User đăng nhập thuộc group một hoặc nhiều con: có thể them mới group con tương ứng của group thuộc user đang login.

Bước 1: Có các cách tạo mới role như sau:

- Click vào 1 role sau đó hover vào cuối danh sách role chọn "Add new" để tạo role cùng cấp với role đã chọn

- Click "Add new" trên màn hình để tạo role con của role đã chọn
- Chuột phải vào 1 cột trong cây chọn "Add new role"
- Sau đó nhập tên role không trùng với tên role đã tồn tại trong hệ thống.



| = | aJiant Setting / | / Account Management / Role Management | | ※ 0 |
|---|------------------|--|----------------------------|---|
| * | Role Management | ٩ | Guidelines Create role | root x Detail information User list |
| | | view_containment view_deploy_tool view_detection view_endpointiw_handler view_group_management view_investigation_result view_investigation_tool view_inforw view_lore_response view_policy_management view_policy_management view_policy_management view_policy_management view_policy_management view_policy_management view_policy_management view_policy_management view_policy_management view_ucpdate_goop view_user_management | | Back estall information NME not(foot) COLUMN 000 foot) ColumN 0000 foot) Colum |

Bước 2: Click icon Edit để thêm thông tin permission cho role > Lựa chọn permission để thêm vào role > click Save:

- + User đăng nhập thuộc group root: Có thể sửa tất cả role trong hệ thống;
- + User đăng nhập thuộc group default: Không được sửa role default;

+ User đăng nhập thuộc group cha: Có thể sửa tất cả role thuộc đang login và role con role ;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả role thuộc user đang login;

Lưu ý: danh sách permission của role con là tập con của role cha. Tức là khi muốn lựa chọn permission gán cho role con thì role đó phải thuộc danh sách permission của role cha.



| view_irflow | | | × |
|-------------------------------------|-----------------------------|--------------------------|-----------------------|
| Detail ir | nformation | User | list |
| Role detail information | | | 0 |
| NAME | view_irflow (view_ | irflow) | |
| DOMAIN | | | |
| DESCRIPTION | view_irflow | | |
| Permission list irflow_read contain | nment_read process_analysis | _read live_response_read | artifact_handler_read |
| response_scenario_read | deploy_tool_handler_read | event_read | |
| | | | |
| | | | |
| | | | |
| | | | |

| Detail in | formation | User list |
|--|--------------------|-----------|
| Role detail information | | Cancel |
| Name | view_live_response | |
| Domain | | |
| Description | view_live_response | |
| | | |
| Permission list | | |
| Permission list | | 2 |
| Permission list | | 2 |
| Permission list (live_response_read ×) read containment_read | | 2 |
| Permission list live_response_read read containment_read containment_manage | | 2 |
| Permission list live_response_read read containment_read containment_manage agent_management_read | ad | 2 |
| Permission list live_response_read × read containment_read containment_manage agent_management_read agent_management_manage agent_managem | ad | 2 |



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





+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

| =⊧ | aJi | tel ant | Set | tting / Account Ma | anagement / Role Management | | | | | | | | | . 0 |
|---------------|---------|------------|------------|-----------------------|--|-----------------------------|---|--------------|------------|--------------------|------------------|-------------|-----|------------|
| ē. | Role M | lanagem | ent | | | | | | Guidelines | view_live_response | | | | × |
| ▲ ™ | Type ro | Add | lser Int | to Role | | | | | | | | Cancel Save | | pdate user |
| ۲ | | | or mails | able to add into role | a (2 subsetsed) | | | User in mie | | | | | 5 | ACTION |
| | | | ser avaita | ible to and into role | (3 selected) | | | User in role | | | | | ive | × |
| | | 2 | NO. | USERNAME | FULLNAME | EMAL | | □ NO. | USERNAME | FULLNAME | EMAIL | | | |
| • | | | 1 | admin | Supper Admin | admin@ajiant.com | | 1 | bichpt3 | Bich PT | bichpt@gmail.com | | | |
| Eλ | | | 2 | alert_viewer | alert_viewer | alert_viewer@ajiant.com | | 2 | viewer | quyên view | aaaa@gmail.com | | | |
| | | | 3 | anhvn | anhvn | anhvn@gmail.com | | | | | | | | |
| Ŷ | | | 4 | autotest107 | fullname | Jackie anderson@yahoo.com | | | | | | | | |
| | | | 5 | autotest11 | fullname | bound meduca@botmail.com | | | | | | | | |
| | | | 0 | autotest150 | fulname | timothy larde@urbos.com | | | | | | | | |
| | | | | autotast161 | fullnama | isunita sistaron@smail.com | 4 | 1 | | | | | | |
| | | | | autotest167 | fulloame | Jasmatta hithe®vahoo rom | » | | | | | | | |
| | | | 10 | autotest27 | fullname | jee.kuvalis@vahoo.com | ~ | | | | | | | |
| | | | 11 | autotest271 | fullname | hank.moen@gmail.com | | | | | | | | |
| | | | 12 | autotest285 | fullname | karlyn.baver@gmail.com | | | | | | | | |
| | | | 13 | autotest300 | fullname | douglass.sauer@vahoo.com | | | | | | | | |
| | | | 14 | autotest34 | fullname | enriqueta.beahan@yahoo.com | | | | | | | | |
| | | i i | 15 | autotest416 | fullname | natosha.ziemann@hotmail.com | | | | | | | | |
| | | | 16 | autotest419 | fullname | dillon.purdy@hotmail.com | | | | | | | | |
| | | C | 17 | autotest436 | fullname | londa.rempel@hotmail.com | | | | | | | | |
| | | | 18 | autotest44 | fullname | tanner.okeefe@yahoo.com | | | | | | | | |
| | | | 19 | autotest459 | fullname | benton.walker@hotmaiLcom | | | | | | | | |
| | | | | 1.1.1.000 | 1.0 | | | | | | | | | |
| | | | | | view_response_scenario view_role_management | | | | | | | | | |

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

4 – Xóa role: click vào role cần xóa, chọn "Delete" > click OK trên màn hình confirm



| ≡ | aJiant s | Setting / Account M | anagement / Role Management | | | | | # 0 |
|------------|--------------------------|---------------------|------------------------------|-------------------|---|-------------------------|-------------------------|------------|
| Ā | Role Management | | | | g Guidelines | New_Role1 | | × |
| ▲ | Type role name to search | | | | Q Delete Create role | Detail inf | ormation | Userlist |
| ₹ <u>+</u> | 🗅 default | | 🗅 hbc_t | 🗅 Haites | | | | |
| ۲ | 🗅 root | > | □ liennt_tes > | liennt_permission | | Role detail information | New Polet (serve colet) | 0 |
| Ē | | | manage_agent_management | Liennt_t1234566 | | DOMAIN | new_notes (new_notes) | |
| - | | | 🗅 manage_alert | Na_test | _ | DESCRIPTION | New_Role1 | |
| ě | | | manage_appctrl_handler | New_Role1 | | Permission list | | |
| ¢λ | | | manage_containment | | _ | | | |
| ē | | | manage_deploy_tool | | | | | |
| | | | manage_detection | U Delete | | | | |
| | | | manage_endpointfw_handler | | Are you sure you want to delete role : New_Role1? | | | |
| | | | manage_event_search | | | | | |
| | | | manage_group_management | | Cancel Defete | | | |
| | | | manage_investigation_result | | | E. | | |
| | | | manage_investigation_tool | | | | | |
| | | | manage_irflow | | | | | |
| | | | manage_live_response | | | | | |
| | | | manage_permission_management | | | | | |
| | | | manage_policy_management | | | | | |
| | | | manage_process_analysis | | | | | |
| | | | manage_proxy | | | | | |
| | | | manage_response_scenario | | | | | |
| | | | □ manage mie management | | | | | |

Lưu ý: Sau khi xóa 1 role, tất cả các user sử dụng role này được thay đổi: Nếu user X nằm trong role bị xóa và user X chỉ có 1 role thì chuyển user X về role mặc định, ngược lại, nếu user X có nhiều role thì chỉ loại bỏ role bị xóa ra khỏi danh sách role của user X.

3.4.4.3 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



| Ę, | User r | management | | | | | Guidelines |
|------------|--------|--------------------|--------------|-----------------------------|------------|--------|------------|
| A | Туре | username to search | | | | | Q |
| ₹₹ | 44 re | sult(s) | | | | | + Create |
| ۲ | NO. | USERNAME | FULLNAME | EMAIL | LAST LOGON | STATUS | ACTION |
| 5-1 | 1 | admin | | t | N/A | Active | 0 |
| _ | 2 | alert_vlewer | alert_viewer | alert_viewer@ajiant.com | N/A | Active | 0 |
| ₽ | 3 | anhbd25 | | tl | N/A | Active | 0 |
| Ē. | 4 | anhnn | | anhnn@gmail.com | N/A | Active | 0 û |
| (A) | 5 | anhnn19 | | tba | N/A | Active | 0 11 |
| ц <u>т</u> | 6 | anhvn | | anhvn@gmail.com | N/A | Active | 0 û |
| | 7 | autotest151 | fullname | clint.kris@yahoo.com | N/A | Active | 0 Û |
| | 8 | autotest281 | fullname | marjory.ritchie@hotmail.com | N/A | Active | 0 |
| | 9 | autotest289 | fullname | alec.stamm@gmaiLcom | N/A | Active | 0 |
| | 10 | autotest35 | fullname | alica.lueilwitz@gmail.com | N/A | Active | 0 11 |
| | 11 | autotest362 | fullname | mao.huel@hotmail.com | N/A | Active | 0 11 |

- Thêm mới tài khoản: click "Create" > Nhập thông tin vào form hiện lên > click

"Next"

| = | viettet aJiant Setting / Account Management / User M | anagement | | | B O |
|------------|---|----------------------------|-----------------------------|-----------|---------------|
| ē | User management | | | | Ouidelines |
| A | Type username to search | | | | Q |
| - <u>1</u> | 66 result(s) | | | | -+ Cust |
| (ii) | NO. USERNAME | PULUNAME | EMAIL | LASTLOGON | STATUS ACTION |
| | 1 admin | Supper Admin | admin⊜ailant.com | N/A | Active 0 |
| | 2 alert viewer | alert_viewer | alert_viewer@aiiant.com | N/A | Active / 🗊 |
| | 3 anhvn | | | | Active 0 |
| ÷ | 4 autotest107 | Create | | * | Active Ø |
| EV | 5 autotest11 | User information Role Grou | ip. | | Active Ø |
| ē | 6 autotest136 | | | | Active Ø |
| | 7 autotest156 | Username | Type username | | Active 0 |
| | 8 autotest161 | Fullname | Type fullname | | 💽 Active 🖉 📋 |
| | 9 autotest167 | Email | Type email | | Active 0 |
| | 10 autotest27 | Busuard | | | Active 0 |
| | 11 autotest271 | Passiloro | lype password | | Active 0 🔒 |
| | 12 autotest285 | Status | Active Desctive | | Active 0 |
| | 13 autotest300 | | 2 | | Active 0 |
| | 14 autotest34 | | Cancel Next | | Active / 🗊 |
| | 15 autotest416 | fullname | natosha.ziemann@hotmail.com | N/A | C Active |
| | 16 autotest419 | fullname | dillon.purdy@hotmail.com | N/A | C Active |
| | 17 autotest436 | fullname | londa.rempel@hotmail.com | N/A | C Active 0 |
| | 18 autotest44 | fullname | tanner.okeefe@yahoo.com | N/A | C Active 0 |
| | 19 autotest459 | fullname | benton.walker@hotmail.com | N/A | C Active 0 |
| | 20 autotest483 | fullname | pete.hickle@yahoo.com | N/A | 💽 Active 🖉 🗊 |
| | 21 autotest49 | fullname | geraldo.ledner@gmail.com | N/A | C Active 0 |
| | 22 autotest493 | fullname | stefany.hill@yahoo.com | N/A | 💽 Active 🖉 🗊 |
| | Showing 25/66 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;

| _₽ | 66 | result(s) | | | | | | | | + Create |
|----|----|---------------|-----------------------|-------|--|-----------------------------|--------|-------|----------|----------|
| ۲ | NC | . USERNAME | PULLNAME | | | EMAIL | LAST U | .000N | STATUS | ACTION |
| 5 | 1 | admin | Supper Admin | | | admin@ajiant.com | N/A | | C Active | 0 0 |
| | 2 | alert_viewer | alert_viewer | | | alert_viewer@ajiant.com | N/A | | Active | 0 0 |
| | 3 | anhvn | | | | | | | Active | |
| Eλ | 4 | autotest107 | Edit User | | | | | ^ | C Active | |
| | 5 | autotest11 | User information Role | Group | | | | | Active | e 🗉 |
| Ψ | 6 | autotest136 | | | | | | | Active | e 🗉 |
| | 7 | autotest156 | Username | | admin | | | | Active | 0 |
| | 8 | autotest161 | Fullname | | Supper Admin | | | | Active | 0 D |
| | 9 | autotest167 | Email | | admin@aiiant.com | | | | Active | e 🗈 |
| | 10 | autotest27 | 6.1.c | | | | | | Active | e 🗉 |
| | 11 | autotest271 | status | | Active Usective Change password | | | | Active | P 🗊 |
| | 12 | autotest285 | | | | | | | C Active | 0 E |
| | 13 | autotest300 | | | | Cancel Next | | | C Active | 0 D |
| | 14 | autotest34 | | | | 2 | | | C Active | 0 🗊 |
| | 15 | 5 autotest416 | fullname | | | natosha.ziemann@hotmail.com | N/A | | C Active | 0 0 |
| | 10 | 3 autotest419 | fullname | | | dillon.purdy@hotmail.com | N/A | | C Active | 0 🗄 |

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

| Edit User | | | | | | | | × |
|------------------|----------|-----------------------------|------|--------------------------|------|-------------|--|---|
| User information | Role Gro | a. | | Type role name to search | ۹ | 4 role: | eselected | |
| 🗅 default | | hbc_test | | | | defa | leult | |
| ⊃ root | | D liennt_test | •• | | | Perm | missions: read dashboard_read | |
| | | manage_agent_management | | | | man Perm | mage_agent_management | × |
| | | manage_alert | | | | man | mage_alert | × |
| | | manage_appctrl_handler | | | | Perm | missions: alerts_manage irflow_manage | |
| | | manage containment | | | | man | nage_appctrl_handler | × |
| | | | | | | Perm | missions: appctrl_handler_manage update_group_manage | |
| | | manage_ueproy_cool | | | | - | | |
| | | manage_detection | | | | | | |
| | | manage_endpointfw_handler | | | | | | |
| | | manage_event_search | | | | | | |
| | | manage_group_management | 0 | | | | | |
| | | manage_investigation_result | | | | | | |
| | | manage_investigation_tool | | | | | | |
| | | iffow manage_iffow | | | | | | |
| | | manage_live_response | | | | | | |
| | | manage_permission_manageme | nt 🗌 | | | | | |
| | | | | Back | Next | | | |

+ Click chọn checkbox tương ứng với role cần thêm, sau đó click "Go to role" để về màn hình danh sách role ban đầu, sau đó click "Create" để tạo tài khoản;

+ Lưu ý: Tài khoản đang đăng nhập tạo 1 tài khoản mới chỉ tạo được các tài khoản chứa các role con thuộc danh sách role mà tài khoản đang đăng nhập được cấp;

+ Lựa chọn group sẽ gán cho tài khoản, sau đó click "Create";

+ Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó;



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

• User đăng nhập thuộc group cha: Hiển thị Group thuộc group của user đang login và group con tương ứng;

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

| Edit User | | | × |
|-----------------------------|-----------------------------|--|---|
| User Information Role Group | Type group name to search Q | 4 group selected | |
| j admin 💆 | | test_group3 admis/chuyen_isst/test_group2 | × |
| D default 🗌 | | chuyen_test | × |
| D globel 🗌 | | 🗅 admin | × |
| | | toon 🖸 | × |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Back Cancel Sove | | |

+ Click chọn checkbox tương ứng với group cần thêm, sau đó click "Go to role" để về màn hình danh sách group ban đầu, sau đó click "Create" để tạo tài khoản.

- Xóa tài khoản: click vào icon Xóa sau đó click OK trên màn hình confirm Kiểm tra hiển 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;



| NO. USERNAME | PULLNAME | DWL | | LAST LOODN | STATUS | ACTION |
|----------------|--------------|--|---|---------------------|----------|--------|
| 1 admin | Supper Admin | admingajiant.com | | NA | C Active | 0 |
| 2 alert_viewer | alert_viewer | alert_viewer@ajiant.com | | NA | Active | 00 |
| 3 anhvn | anhvn | anhvn@gmail.com | | 29/04/2022 10:44:40 | Active | 0 |
| 4 autotest107 | fullname | jackie.anderson@yahoo.com | | NA | Active | 0 |
| 5 autotestii | fullname | sondra.trantow@yahoo.com | | NA | Active | 00 |
| 6 autotest136 | fullname | howard.mcclure@hotmail.com | | NA | Active | 10 |
| 7 autotest156 | fullname | timothy.jerde@yshoo.com | | NA | Active | o 👤 |
| 8 autotest161 | fullname | jaunita.gislason@gmail.com | | N/A | Active | 00 |
| 9 autotest167 | fullname | Delete | × | NA | C Active | 0 |
| 10 autotest27 | fullname | U | | NA | Active | 0.0 |
| 11 sutotest271 | fullname | Are you sure you want to delete user : anhwn ? | | NA | Active | 0 |
| 12 autotest285 | fullname | | | NA | Active | 0 |
| 13 autotest300 | fullname | Cascel Delete 2 | | NA | Active | 00 |
| 14 autotest34 | fullname | | | NA | Active | 0 |
| 15 autotest416 | fullname | natosha.ziemann@hotmail.com | | NA | Active | 00 |
| 16 autotest419 | fullname | dillon.purdy@hotmail.com | | NA | Active | 00 |
| | | | | | | |

3.4.5 Update management

3.4.5.1 *Update groups*

- Mục đích: là tính năng cho phép quản lý, tạo mới và cập nhật các Update Group (Chia các Agent thành các nhóm cập nhật, giúp dễ dàng phân chia, quản lý)

- 1 Tìm kiếm:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

| Update groups Packages | | | | | | |
|------------------------|----------------------------------|-----------------|------------------|-------------------------|-----------------------------|------------------|
| Q Search | | | | | | Q |
| 8 group(s) | | | | | | New update group |
| Name of update group | Description | Current package | Number of agents | Update schedule | Upcoming package | Action |
| Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) after release | N/A | |
| Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | |
| alpha | Group alpha test team agent core | release | 0 | Update manually | N/A | |
| beta | Group Beta update ngay | 3.3.7 | 0 | Immediately | N/A | |
| congnc | Update group congnc | N/A | 0 | Update manually | N/A | |
| phula_test | Update group phula_test | release | 0 | Update manually | N/A | |
| release | Update group release | release | 4 | Update manually | N/A | |
| test | Update group test | test | 0 | Update manually | N/A | |
| | | | | | | |
| | | | | | | |

- **Bước 4:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- Bước 5: Nhập từ khóa tìm kiếm vào ô textbox và chọn nút "Search"



| Upr | date groups Packages | | | | | | |
|-----|----------------------|----------------------------------|-----------------|------------------|-------------------------|-----------------------------|------------------|
| | λ update | | | | | | © 0 |
| | 8 group(s) | | | | | Q | New update group |
| | Name of update group | Description | Current package | Number of agents | Update schedule | Upcoming package | Action |
| | Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) after release | N/A | |
| | Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | |
| | alpha | Group alpha test team agent core | release | 0 | Update manually | N/A | |
| | beta | Group Beta update ngay | 3.3.7 | 0 | Immediately | N/A | |
| | congne | Update group congnc | N/A | 0 | Update manually | N/A | |
| | phula_test | Update group phula_test | release | 0 | Update manually | N/A | |
| | release | Update group release | release | 5 | Update manually | N/A | |
| | test | Update group test | test | 0 | Update manually | N/A | |
| | | | | | | | |
| | | | | | | | |

- 2 Thêm mới Update groups:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

| Q Search E group(s) Name of update group Update, thour update asu 1 hour | Curren | nt package Nu | umber of agents | Ibela sebala | 0 | lew update group |
|---|--------------------|----------------|--------------------|-------------------------|-----------------------------|------------------|
| 8 group(s) Name of update group Description Update_Thour update sau 1 hour | Curren | int package Nu | umber of agents I | Liofata eshadula | • | lew update group |
| Name of update group Description Update_1hour update sau 1 hour | Curren | ent package Nu | umber of agents | Lindate schedule | | |
| Update_1hour update sau 1 hour | | | anner er agented e | opuate acredute | Upcoming package | Action |
| | 3.3.7 | 0 | 1 | 1 hour(s) after release | N/A | |
| Update_specific Update vao chu nhat | ang tuan 3.3.7 | 0 | c | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | |
| alpha Group alpha test tear | agent core release | se 0 | U | Update manually | N/A | |
| beta Group Beta update n | ay 3.3.7 | 0 | In | Immediately | N/A | |
| congnc Update group congni | N/A | 0 | U | Update manually | N/A | |
| phula_test Update group phula_ | ist release | se 0 | U | Update manually | N/A | |
| release Update group release | release | se 4 | U | Update manually | N/A | |
| test Update group test | test | 0 | U | Update manually | N/A | |

Bước 4: Chọn nút "New update group", hệ thống hiển thị màn hình thêm mới Update Group;



| Update groups Packages | | 2 | | |
|------------------------|----------------------------------|---|-------------------------------|---|
| Q Search | | Create new group Name of update group U0_01 | × | Q |
| Name of update group | Description | Description (optional) | Upcoming package Action | |
| Update_1hour | update sau 1 hour | About your update group | 35e N/A | |
| Update_specific | Update vao chu nhat hang tuan | |) 3.3.4 (03/07/2022 08:00:00) | |
| alpha | Group alpha test team agent core | | N/A | |
| beta | Group Beta update ngay | | , N/A | |
| congnc | Update group congnc | 0/2000 | 00 N/A | |
| phula_test | Update group phula_test | Package version | N/A | |
| release | Update group release | versions related to agents can be shown here. | N/A | |
| test | Update group test | 3.3.7 (latest) 🗸 | N/A | |
| | | Update schedule When a new package version is deployed: Update manually (change in the section "Package version" above) Update automatically Update automatically Update after | 3 | |

- **Bước 5:** Nhập thông tin thêm mới Update Group và chọn nút "Create". Hệ thống ghi nhận và quay về màn hình danh sách Update Group.
 - 3 Cập nhật Update groups:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

| Update groups Packages | | | | | | |
|------------------------|----------------------------------|-----------------|------------------|-------------------------|-----------------------------|------------------|
| Q Search | | | | | | ٩ |
| 8 group(s) | | | | | I | New update group |
| Name of update group | Description | Current package | Number of agents | Update schedule | Upcoming package | Action |
| Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) after release | N/A | |
| Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | |
| alpha | Group alpha test team agent core | release | 0 | Update manually | N/A | |
| beta | Group Beta update ngay | 3.3.7 | 0 | Immediately | N/A | |
| congne | Update group congnc | N/A | 0 | Update manually | N/A | |
| phula_test | Update group phula_test | release | 0 | Update manually | N/A | |
| release | Update group release | release | 4 | Update manually | N/A | |
| test | Update group test | test | 0 | Update manually | N/A | |
| | | | | | | |

Bước 4: Tại bản ghi cần cập nhật/ chỉnh sửa thông tin, chọn icon "Cập nhật" thông tin Update Group:



| A | Update groups Packages | | | | | | | | |
|------------------|------------------------|----------------------------------|-----------------|------------------|-------------------------|-----------------------------|--------------------|--|--|
| ь ^н (| Q update | • | | | | | | | |
| S E | 8 group(s) | | | | | | • New update group | | |
| | Name of update group | Description | Current package | Number of agents | Update schedule | Upcoming package | Action | | |
| Ť | Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) after release | N/A | | | |
| Ж | Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | Ð | | |
| ÷ | alpha | Group alpha test team agent core | release | 0 | Update manually | N/A | | | |
| ĽД | beta | Group Beta update ngay | 3.3.7 | 0 | Immediately | N/A | | | |
| P | congnc | Update group congnc | N/A | 0 | Update manually | N/A | | | |
| | phula_test | Update group phula_test | release | 0 | Update manually | N/A | | | |
| | release | Update group release | release | 5 | Update manually | N/A | | | |
| | test | Update group test | test | 0 | Update manually | N/A | | | |

Bước 5: Hệ thống hiển thị màn hình thông tin chi tiết Update Group, cho phép cập nhật/ chỉnh sửa thông tin và lưu lại bằng cách chọn nút "Apply":

| Update groups Packages | | | | | |
|---|--|---|---------------------|--|-----------------------------|
| Q update | | Edit group detail | × | | ۵ ۵ |
| 8 group(s) Name of update group | Description | Update_Thour Name contains only letters, numbers, and special characters 1,0 10,11 Description (optional) | | Upcoming package | New update group Action |
| Update_thour Update_specific alpha beta congnc phula_test release test | Update sau 1 hour Update vao chu chat hang tuan Oroup alpha test tean agent core Oroup Betau update ngay Update group congroc Update group phula_test Update group phula_test Update group test | update ggg 1 hour (update] Package version Occose the package version for this group. Only deployed and not re- version related to agents can be shown here. 3.7.7 (elsert) | ASE 3 | N/A 3.3.4 (05/07/2022 08:00:00) N/A N/A N/A N/A N/A N/A | |
| | | Update schedule Wen a new package version is deployed: () Update manually (change in the section "Package version" above 2) Update automatically Ime to update () Update immediately () Update af a specific time 2) Update af a specific time | a <mark>Proy</mark> | | |

- 4 Xóa Update groups:
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;


| Q Search | | | | | | |
|----------------------|----------------------------------|-----------------|------------------|-------------------------|-----------------------------|------------------|
| 8 group(s) | | | | | | New update group |
| Name of update group | Description | Current package | Number of agents | Update schedule | Upcoming package | Action |
| Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) after release | N/A | |
| Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | |
| alpha | Group alpha test team agent core | release | 0 | Update manually | N/A | |
| beta | Group Beta update ngay | 3.3.7 | 0 | Immediately | N/A | |
| congnc | Update group congnc | N/A | 0 | Update manually | N/A | |
| phula_test | Update group phula_test | release | 0 | Update manually | N/A | |
| release | Update group release | release | 4 | Update manually | N/A | |
| test | Update group test | test | 0 | Update manually | N/A | |

Bước 4: Tại bản ghi cần xóa, chọn icon "Xóa" Update Group:

| Update groups Packages | | | | | | |
|------------------------|----------------------------------|-----------------|------------------|-------------------------|-----------------------------|------------------|
| Q update | | | | | | 8 |
| 8 group(s) | | | | | | New update group |
| Name of update group | Description | Current package | Number of agents | Update schedule | Upcoming package | Action |
| Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) after release | N/A | |
| Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at 08:00 | 3.3.4 (03/07/2022 08:00:00) | 16 |
| alpha | Group alpha test team agent core | release | 0 | Update manually | N/A | L. |
| beta | Group Beta update ngay | 3.3.7 | 0 | Immediately | N/A | - |
| congne | Update group congnc | N/A | 0 | Update manually | N/A | |
| phula_test | Update group phula_test | release | 0 | Update manually | N/A | |
| release | Update group release | release | 5 | Update manually | N/A | |
| test | Update group test | test | 0 | Update manually | N/A | |

Bước 5: Hệ thống hiển thị Popup Xác nhận xóa Update Group, Người dùng chọn nút "Delete" để xác nhận yêu cầu Xóa Update Group và chọn nút "Cancel" để hủy yêu cầu Xóa Update Group.

| A | Update groups Packages | | | | | | | |
|-------------|------------------------|----------------------------------|------------------|---------------------------------|----------------|------------|-----------------------------|------------------|
| ÷ | Q update | | | | | | | <u></u> |
| ۲ | | | | | | | | |
| D -0 | 8 group(s) | | | | | | | New update group |
| | Name of update group | Description | Current package | Number of agents | Update sched | dule | Upcoming package | Action |
| × I | Update_1hour | update sau 1 hour | 3.3.7 | 0 | 1 hour(s) afte | er release | N/A | |
| * | Update_specific | Update vao chu nhat hang tuan | 3.3.7 | 0 | On Sunday at | 108:00 | 3.3.4 (03/07/2022 08:00:00) | |
| n. | alpha | Group alpha test team agent core | | - | nu | sally | N/A | |
| UA. | beta | Group Beta update ngay | | Π | × y | | N/A | |
| <u>e</u> | congne | Update group congno | Dala | to this group? | nu | sally | N/A | |
| | phula_test | Update group phula_test | Dele | te this group? | nu | ually | N/A | |
| | release | Update group release | | | nu | sally | N/A | |
| | test | Update group test | Do you really wa | nt to delete this update group? | nu | ually | N/A | |
| | | | Can | cel Keep delete | _ | | | |

- 3.4.5.2 Update packages
- 1 Tìm kiếm packages:

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;



- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;

| date groups | Packages | | | | | | | | |
|-----------------|----------------------|---------------------------------|---|--------------|--|----------------------------------|----------------------|----------------------|--------------------|
|) Search | | | | | | | | | |
| 10 package(s) | Backend version: 3.3 | ng số package trên | hệ thống | | | | Automatic deployment | Show unused packages | 1. Upload new pack |
| Storage: 6.91 0 | BB used of 55.59 GB | Số dung lượng đ dung lượng h | ã sử dụng trên tổng ê thống cung cấp | | | | | | |
| Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deployed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp. | Not deployed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ | Not deployed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | Install successed | dat | 10/05/2022 17:37:46 | |
| 3.3.4 | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| 3.3.2 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| | N/A | N/A | Vec | Verified | Old repository release | Install successed | N/A | N/A | |

Bước 5: Nhập từ khóa tìm kiếm vào ô textbox và chọn nút "Search"

| date groups | Packages | | | | | | | | |
|-------------------------------|---|-----------|--------------------|--------------|--|---------------------------------------|----------------------|----------------------|----------------------|
| Search | | | | | | | | | |
| 10 package(s Storage: 6.91 |) Backend version: 3.3 GB used of 55.58 GB | | | | | | Automatic deployment | Show unused packages | 1. Upload new packag |
| Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deployed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp | . • Not deployed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ | Not deployed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cái đặt 3.3.7, cập nhật file agents | Install successed | i dat | 10/05/2022 17:37:46 | |
| 3.3.4 | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | i dat | 10/05/2022 17:36:29 | |
| | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| 3.3.Z | | | | Marified | Old repository release | A Install successed | N/A | N/A | |

2 - Auto Update

- Mục đích: là tính năng cho phép tự động triển khai các bản update tới khách hàng một cách nhanh chóng và hiệu quả. Auto Update cho phép upload các gói qua giao diện portal hoặc tự động lấy các bản update qua trang hub.viettelcybersecurity.com;



Lưu ý: Đội triển khai gửi lại các thông tin trên cho đội dự án Ajiant để cập nhật vào hệ thống để cho phép triển khai gói tự động tại khách hàng. Về sau, khi cần triển khai gói update mới, đội triển khai hoặc phía khách hàng chỉ cần lấy gói update được cung cấp và upload lên portal ajiant và chọn triển khai gói.

- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;

| A | ipdate groups | Packages | | | | | | | | |
|----------------|------------------|---------------------------|--|-------------------------------------|--------------|--|---------------------------------------|----------------------|----------------------|-----------------------|
| H ⁴ | Q Search | | | | | | | | | Q |
| Ŭ E | 10 package(s) | Backend version: 3.3 Tổng | g số package trên hệ | thống | | | | Automatic deployment | Show unused packages | 1. Upload new package |
| • | storage: 6.91 GB | used of 55.59 GB | Số dụng lượng đã s dụng lượng hệ th | iếr dụng trên tổng tổng cung cấp | | | | | | |
| ¥. | Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| | 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deployed | root | N/A | |
| Ēλ | 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp | Not deployed | dat | N/A | |
| ٥ | 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| | 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| | 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ | Not deployed | dat | N/A | |
| | 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| | 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | Install successed | dat | 10/05/2022 17:37:46 | |
| | 3.3.4 | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| | 3.3.2 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| | release | N/A | N/A | Yes | Verified | Old repository release | Install successed | N/A | N/A | |
| | | | | | | | | | | |

Bước 5: Chọn nút "Update new package", hệ thống hiển thị Popup "Upload package";

| late groups | Packages | | | | | | | | |
|--------------------------------|----------------------|-----------|--------------------|--------------|--|------------------------------------|----------------------|----------------------|--------------------|
| Search | | | | | | | | | |
| 10 package(s) Storage: 6-91 | Backend version: 3.3 | | | | | ¢ | Automatic deployment | Show unused packages | 1. Upload new pack |
| Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | . Not deployed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp | . Not deployed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ | Not deployed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | Install successed | dat | 10/05/2022 17:37:46 | |
| | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| 3.3.4 | | | | Marified | Gói undate 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| 3.3.4 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Vermed | ou spoure ou a receber re | | | | |

Viettel Cyber Security

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



Bước 6: Chọn tải lên package;

| λ Search | | | | | | | | | | |
|-----------------|--|-----------|--------------------|------------|--|--------------|----------|----------------------|----------------------|------------------|
| | | | | | | | | | | |
| | | | | | | | | | | |
| 10 package(|) Backend version: 3.3 | | | | | | | Automatic deployment | Show unused packages | 1 Upload new pac |
| Storage: 6.91 | GB used of 55.58 GB | | | | | | | | | |
| | | | | | | | | | | |
| Version | Release date | File size | Related to agents? | Signature | Description | Deployment | t status | Uploader | Deploy date | Action |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deplo | yed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp | • Not deplo | yed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not depla | yed | root | N/A | |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Upload par | ckage > | < lot deplo | yed | dat | N/A | |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | | | lot deple | yed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Choose f | me Max tile size is buumb, supported file type is .ZIP. | lot deple | yed | dat | N/A | |
| 337 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | • Install su | ocessed | dat | 10/05/2022 17:37:46 | |
| | | 142.46 MB | Yes | Verified | 3.3.4 description | • Install su | ccessed | dat | 10/05/2022 17:36:29 | |
| 3.3.4 | 28/03/2022 09:59:12 | | | | | | | | | |
| 3.3.4 | 28/03/2022 09:59:12 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install fai | led | dat | 10/05/2022 17:33:42 | |

Bước 7: Bật/ Tắt Action "Automatic Development" để tự động triển khai các bản cập nhật package tới khách hàng.

| Search | | | | | | | | | |
|---------------|----------------------|-----------|--------------------|--------------|--|---------------------------------------|----------------------|----------------------|--------------|
| , | | | | | | | | | |
| 10 package(s | Backend version: 3.3 | | | | | a | Automatic deployment | Show unused packages | 1 Upload new |
| Storage: 6.91 | GB used of 55.59 GB | | | | | | | | |
| Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Ad |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe. | Not deployed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp. | Not deployed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ | Not deployed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | Install successed | dat | 10/05/2022 17:37:46 | |
| 3.3.4 | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| 3.3.2 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| | N/A | NI/A | Vec | Morified | Old repository release | a Install successed | N/A | N/A | |

- 3 Deploy package
- Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;
- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;



| Upd | sate groups | Packages | | | | | | | | |
|-----|--------------------|---------------------------|---------------------------------------|------------------------------------|--------------|--|---------------------------------------|----------------------|----------------------|----------------------|
| ٩ | Search | | | | | | | | | ٩ |
| E | 10 package(s) B | lackend version: 3.3 Tổng | j số package trên hệ |) thống | | | 0 | Automatic deployment | Show unused packages | 1 Upload new package |
| 1 | Storage: 6.91 GB u | ised of 55.59 GB | Số dung lượng đã s dung lượng hệ t | lử dụng trên tổng hồng cung cấp | | | | | | |
| | Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| | 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deployed | root | N/A | |
| | 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp | Not deployed | dat | N/A | |
| | 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| | 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| | 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nổi ra ngoài internet, chí | Not deployed | dat | N/A | |
| | 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| | 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | Install successed | dat | 10/05/2022 17:37:46 | |
| | 3.3.4 | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| | 3.3.2 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| | rologga | N/A | N/A | Yes | Verified | Old repository release | Install successed | N/A | N/A | |

Bước 5: Chọn icon "Deploy this package" tại bản ghi package đó, hệ thống hiển thị Popup Xác nhận Deploy package

| odate groups | Packages | | | | | | | | |
|-----------------|----------------------|-----------|--------------------|--------------|--|---------------------------------------|----------------------|----------------------|----------------------|
|) Search | | | | | | | | | |
| 10 package(s) | Backend version: 3.3 | | | | | | Automatic deployment | Show unused packages | 1. Upload new packag |
| Storage: 6.91 G | B used of 55.58 GB | | | | | | | | |
| Version | Release date | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deployed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp. | Not deployed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | ± 0 |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | Deploy this pac |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ | Not deployed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Gói cái đặt 3.3.7, cập nhật file agents | Install successed | i dat | 10/05/2022 17:37:46 | |
| | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| 3.3.4 | | | | | | | | | |
| 3.3.4 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |

Bước 6: Chọn nút "Deploy" để xác nhận Deploy package trên thiết bị hoặc chọn nút "Cancel" để hủy thao tác Deploy package.

| date groups | Packages | | | | | | | | | | |
|---------------|----------------------|-----------|--------------------|--------------|------------------------------------|---|---------|----------------------|----------------------|----------------------|-----------------------|
| | | | | | | | | | | | |
| Search Search | | | | | | | | | | | |
| | | | | | | | | | | | |
| 10 package(s | Backend version: 3.3 | | | | | | | | Automatic deployment | Show unused packages | 1. Upload new package |
| Storage: 6.91 | GB used of 55.58 GB | | | | | | | | | | |
| | | | | | | | | | | | |
| Version | Release date | File size | Related to agents? | Signature | Description | | | Deployment status | Uploader | Deploy date | Action |
| 3.3.19 | 13/06/2022 17:18:34 | 1.64 MB | Yes | Verified | | × | VESRe | Not deployed | root | N/A | |
| 3.3.18 | 10/05/2022 17:45:07 | 230.98 MB | Yes | Verified | <u>ب</u> | ^ | ng hợp | Not deployed | dat | N/A | |
| 3.3.11 | 09/04/2022 17:45:30 | 132.6 KB | Yes | Verified | Deplementaria analysis 2 | | | Not deployed | root | N/A | |
| 3.3.10 | 09/04/2022 17:42:13 | 1.37 MB | Yes | Verified | Deploy this package? | | | Not deployed | dat | N/A | |
| 3.3.9 | 09/04/2022 17:45:30 | 1.59 MB | No | Verified | | | et, chí | Not deployed | dat | N/A | |
| 3.3.8 | 28/03/2022 09:59:12 | 13.92 MB | No | Not verified | Do you want to deploy the package? | | ive Re | Not deployed | dat | N/A | |
| 3.3.7 | 28/03/2022 09:59:12 | 13.92 MB | Yes | Verified | Rebuild agent installer | | | Install successed | dat | 10/05/2022 17:37:46 | |
| 3.3.4 | 28/03/2022 09:59:12 | 142.46 MB | Yes | Verified | Cancel Deploy | | | Install successed | dat | 10/05/2022 17:36:29 | |
| 3.3.2 | 09/04/2022 17:45:30 | 44.52 MB | Yes | Verified | | | | Install failed | dat | 10/05/2022 17:33:42 | |
| | | | | | Old see all an enlance | | | · Install successful | N/A | | |

4 – Chi tiết Package

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;



- **Bước 2:** Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- **Bước 3:** Chọn Update Management, hệ thống hiển thị Danh sách Update Group;
- **Bước 4:** Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;

| iend version: 3.3 Tổng s | số package trên hệ | thống | | | a | Automatic deployment | Show unused packages | 1. Upload new package |
|--------------------------|---|--|--|---|--|--|--|---|
| d of 55.59 GB | ố dung lượng đã s dung lượng hệ th | ử dụng trên tổng ống cung cấp | | | | | | |
| lease date F | File size | Related to agents? | Signature | Description | Deployment status | Uploader | Deploy date | Action |
| /06/2022 17:18:34 1 | 1.64 MB | Yes | Verified | Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe | Not deployed | root | N/A | |
| /05/2022 17:45:07 | 230.98 MB | Yes | Verified | Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp | Not deployed | dat | N/A | |
| /04/2022 17:45:30 1 | 132.6 KB | Yes | Verified | Update pack 3.3.10 | Not deployed | root | N/A | |
| /04/2022 17:42:13 1 | 1.37 MB | Yes | Verified | Gói update 3.3.10 Bổ sung hash md5 event 7 | Not deployed | dat | N/A | |
| /04/2022 17:45:30 | 1.59 MB | No | Verified | Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chí | Not deployed | dat | N/A | |
| /03/2022 09:59:12 1 | 13.92 MB | No | Not verified | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re | Not deployed | dat | N/A | |
| /03/2022 09:59:12 1 | 13.92 MB | Yes | Verified | Gói cài đặt 3.3.7, cập nhật file agents | Install successed | dat | 10/05/2022 17:37:46 | |
| /03/2022 09:59:12 | 142.46 MB | Yes | Verified | 3.3.4 description | Install successed | dat | 10/05/2022 17:36:29 | |
| /04/2022 17:45:30 | 44.52 MB | Yes | Verified | Gói update 3.3.2 Release AV | Install failed | dat | 10/05/2022 17:33:42 | |
| A 1 | N/A | Yes | Verified | Old repository release | Install successed | N/A | N/A | |
| | nd version 3.3 Táng 1 of 55.59 08 6x2022 17.18.34 04/2022 17.45.07 04/2022 17.45.07 04/2022 17.45.00 00/2022 09.512 03/2022 09.512 03/2022 09.512 04/2022 17.45.30 | ord version: 3.3 Tiding add package trials not during large tr | ed version: 1 3 Tong of package tein he thong of 55.9 of BI esse date File size heided to agoung th is duop tein heid of 2000221 171845 1.64 AMB Ves 04/2022 174520 1.57 AMB Ves 04/2022 174530 1.57 AMB Ves 04/2022 174530 1.57 AMB Ves 04/2022 174530 1.59 AMB No 00.2022 2095912 1.59 ZMB Ves 04/2022 174530 1.59 AMB Ves 04/2022 174530 1.50 AMB Ves 04/2021 AMB Ves 04/2021 1.50 AMB Ves 04/2021 AMB Ves 04/ | es element 13 of 55.9 08 of 55.9 08 ese date File size 04/2022 17.145.07 02.222 17.45.07 03.2022 07.15.04 04.2022 17.145.07 05.7022 17.116.47 04.2022 17.145.07 12.2 k/B Ves Verified 04.2022 17.145.07 13.97 MB Ves Verified 00.2022 07.05.91 13.92 MB No Verified 00.2022 07.05.91 13.92 MB Ves Verified 00.2022 07.05.91 Ves Verified | Order Tong of package trief hit Information of 55.90 GB • Order of package trief hit Information of 55.90 GB • File side • Related to agents? • Signature Description ord 55.90 GB • File side • Related to agents? • Signature Description 06/2022 17:164.57 20.98 MB Yes Verified Doptime pack 33.19 B6 sung source process path via Self Defemse cho VESRe. 06/2022 17:164.50 120 KB Yes Verified Doptime pack 33.19 B6 sung source process path via Self Defemse cho VESRe. 06/2022 17:164.50 Yes Verified Doptime pack 33.10 Doptim pack 33.10 | Order Tring of package trikin htt ming Tring of package trikin htt ming of 55.90 Ell • Obang ummy QB aic stage trikin bit ming ord social constraints Description Description Description Deployment status 0/55.90 Ell Of thing package trikin httming ord social Pale size Pale size Pale size Pale size Pale size Pale size Pale size Pale size <td>Streams 1.1 Tông số puscage têin hệ Mộc Automatic deployment of 55.9 001 Để dạng tựng thi bộng cang chến Signature Description Deployment status Uploader 07 55.9 001 Hie size Nie date Nie si Viented Uploader Description Deployment status Uploader 06 2022 17184 164 M8 Yes Vented Update pack 3.19 B6 sung source process path và Bell Defense chv UBBe. • Not deploymed root 04 2022 17457 23.0 94 M8 Yes Vented Odi update 3.3.18 D6 sung source process path và Bell Defense chv UBBe. • Not deploymed root 04 2022 17458 122 k/H Yes Vented Odi update 3.3.18 D6 sung thah más vent 7 Not deploymed root 02/2022 17453 1.95 M8 No Vented Odi update 3.3.0 Edp night inthin high bông to kill fill angels internet, chi. • Not deployed dat 02/2022 075912 1.92 M8 No Not everted Odi update 3.3.2 Gip night fill angels intrail not deployed dat 00/2022 075912 1.92 M8 No Not everted Odi update 3.3.2 Gip night fill angels intrail not deployed dat 00/2022 075912 1</td> <td>Image of participants Thing of parcarge with Holing Description <thdescription< th=""> Description</thdescription<></td> | Streams 1.1 Tông số puscage têin hệ Mộc Automatic deployment of 55.9 001 Để dạng tựng thi bộng cang chến Signature Description Deployment status Uploader 07 55.9 001 Hie size Nie date Nie si Viented Uploader Description Deployment status Uploader 06 2022 17184 164 M8 Yes Vented Update pack 3.19 B6 sung source process path và Bell Defense chv UBBe. • Not deploymed root 04 2022 17457 23.0 94 M8 Yes Vented Odi update 3.3.18 D6 sung source process path và Bell Defense chv UBBe. • Not deploymed root 04 2022 17458 122 k/H Yes Vented Odi update 3.3.18 D6 sung thah más vent 7 Not deploymed root 02/2022 17453 1.95 M8 No Vented Odi update 3.3.0 Edp night inthin high bông to kill fill angels internet, chi. • Not deployed dat 02/2022 075912 1.92 M8 No Not everted Odi update 3.3.2 Gip night fill angels intrail not deployed dat 00/2022 075912 1.92 M8 No Not everted Odi update 3.3.2 Gip night fill angels intrail not deployed dat 00/2022 075912 1 | Image of participants Thing of parcarge with Holing Description Description <thdescription< th=""> Description</thdescription<> |

Bước 5: Chọn icon "View Detail" tại bản ghi package đó, hệ thống hiển thị Popup thông tin chi tiết của Package vừa chọn:

| Package detail | | × |
|-----------------|---|----|
| Deployment | | |
| Status | Not deployed | |
| Information | | |
| Backend version | N/A | |
| Package version | 3.3.8 | |
| File size | 13.92 MB | |
| SHA256 | 46bac489a084ed4115de3ef71f30e89ceed60fa15b4d23f93edb929bc39c3d83 | |
| Signature | Not verified | |
| Release date | 28/03/2022 09:59:12 | |
| Upload date | 10/05/2022 17:33:05 | |
| Uploader | dat | |
| Description | Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Reponse v2 Fix lỗi Dashboard, checkmarx | // |

 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



security

3.5 Anti – Malware

3.5.1 Scan Schedule

- Mục đích: Chức năng Scan Schedule cho phép người dùng lập lịch quét virus dưới các máy trạm từ xa.

3.5.1.1 Tìm kiếm Scan Schedule task

- Mục đích: Chức năng tìm kiếm Scan Schedule task cho phép người dùng tìm kiếm các lập lịch quét dưới các máy trạm theo Task name.

- Các bước thực hiện:

| howing 11 Task name | of 11 result(s) | | | | | | | | | | |
|------------------------|-----------------|--------|-----------------------|-------------|--------------------|--------------------------|-----------------------|---------------|--------------|------------------------------|-----|
| ask name | | | | | | | | | Show only | my schedule | New |
| | | Author | Created time | Scan type | Number of agent(s) | Trigger | Start time | Next run time | Expired time | Status | Ac |
| Jountu 2 | | root | 06/10/2022 - 16:15:56 | Quick scan | 1 | Immediately | 06/10/2022 - 16:15:56 | N/A | N/A | Finished | |
| Ibuntu | | root | 06/10/2022 - 16:11:44 | Quick scan | 1 | Immediately | 06/10/2022 - 16:11:44 | N/A | N/A | Finished | |
| uick WIn 1 | 11 | root | 06/10/2022 - 16:07:34 | Quick scan | 1 | Immediately | 06/10/2022 - 16:07:34 | N/A | N/A | Finished | |
| ask win 11 | 1 | root | 06/10/2022 - 16:03:41 | Custom scan | 1 | Immediately | 06/10/2022 - 16:03:41 | N/A | N/A | Finished | |
| ask 456 | | root | 06/10/2022 - 11:37:08 | Quick scan | 1 | At 06/10/2022 - 12:39:30 | 06/10/2022 - 12:39:30 | N/A | N/A | Finished | |
| ask 123 | | root | 06/10/2022 - 11:34:26 | Quick scan | 1 | Immediately | 06/10/2022 - 11:34:26 | N/A | N/A | Finished | |
| wewe | | root | 06/10/2022 - 11:17:59 | Quick scan | 2 | Immediately | 06/10/2022 - 11:17:59 | N/A | N/A | Finished | |
| ask 1 | | root | 06/10/2022 - 11:14:04 | Quick scan | 2 | Immediately | 06/10/2022 - 11:14:04 | N/A | N/A | Finished | |
| 'ask mai | | root | 06/10/2022 - 11:10:10 | Quick scan | 1 | Immediately | 06/10/2022 - 11:10:10 | N/A | N/A | Finished | |
| naitest | | root | 06/10/2022 - 10:54:37 | Quick scan | 1 | Immediately | 06/10/2022 - 10:54:37 | N/A | N/A | Finished | |
| ask 2 | | root | 06/10/2022 - 09:09:09 | Custom scan | 1 | Immediately | 06/10/2022 - 09:09:09 | N/A | N/A | Finished | |

Bước 1: Người dùng nhập vào từ khóa tìm kiếm;

Bước 2: Chọn nút ^Q hoặc nhấn **Enter** để xác nhận thao tác tìm kiếm với từ khóa vừa nhập.

Bước 3: Hệ thống sẽ hiển thị danh sách lập lịch quét theo từ khóa tìm kiếm.

3.5.1.2 Thêm mới Scan Schedule task

- Mục đích: Cho phép người dùng thêm mới một lập lịch quét, cấu hình thời gian và thông tin máy trạm.

- Các bước thực hiện:

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

Page | 79



| Bước 4: | Tai màn hình da | nh sách lập lịch quét. | naười dùna c | hon nút New task |
|----------------------|------------------|------------------------|----------------|------------------|
| Du 00 4 . | r ar mar minn da | ni saon iqp ijon quot, | ingu or dung o | non nuc new lask |

| = | Anti-Malware / Sci | an Scheduler | | | | | | | | | # 0 |
|----------------|----------------------------|--------------|-----------------------|-------------|--------------------|--------------------------|-----------------------|---------------|----------------|------------------------------|---------------|
| <u>_</u> | Q Search | | | | | | | | | | ٩ |
| ¹ t | Showing 11 of 11 result(s) | | | | | | | | Show only my s | schedule 🕀 | 1 New task |
| 0 | Task name | Author | Created time | Scan type | Number of agent(s) | Trigger | Start time | Next run time | Expired time | Status | Action |
| | ubuntu 2 | root | 06/10/2022 - 16:15:56 | Quick scan | 1 | Immediately | 06/10/2022 - 16:15:56 | N/A | N/A | Finished | |
| , | Ubuntu | root | 06/10/2022 - 16:11:44 | Quick scan | 1 | Immediately | 06/10/2022 - 16:11:44 | N/A | N/A | Finished | |
| , | Quick Win 11 | root | 06/10/2022 - 16:07:34 | Quick scan | 1 | Immediately | 06/10/2022 - 16:07:34 | N/A | N/A | Finished | |
| | Task win 11 | root | 06/10/2022 - 16:03:41 | Custom scan | 1 | Immediately | 06/10/2022 - 16:03:41 | N/A | N/A | Finished | |
| 2 | Task 456 | root | 06/10/2022 - 11:37:08 | Quick scan | 1 | At 06/10/2022 - 12:39:30 | 06/10/2022 - 12:39:30 | N/A | N/A | • Finished | |
| | Task 123 | root | 06/10/2022 - 11:34:26 | Quick scan | 1 | Immediately | 06/10/2022 - 11:34:26 | N/A | N/A | Finished | |
| | éwewe | root | 06/10/2022 - 11:17:59 | Quick scan | 2 | Immediately | 06/10/2022 - 11:17:59 | N/A | N/A | • Finished | |
| | Task 1 | root | 06/10/2022 - 11:14:04 | Quick scan | 2 | Immediately | 06/10/2022 - 11:14:04 | N/A | N/A | Finished | |
| | Task mai | root | 06/10/2022 - 11:10:10 | Quick scan | 1 | Immediately | 06/10/2022 - 11:10:10 | N/A | N/A | Finished | |
| | maitest | root | 06/10/2022 - 10:54:37 | Quick scan | 1 | Immediately | 06/10/2022 - 10:54:37 | N/A | N/A | Finished | |
| | Task 2 | root | 06/10/2022 - 09:09:09 | Custom scan | 1 | Immediately | 06/10/2022 - 09:09:09 | N/A | N/A | Finished | |
| | | | | | | | | | | | |
| | | | | | | | | | | | 4 |

Bước 5: Hệ thống hiển thị màn hình thêm mới một lập lịch quét, người dùng nhập vào các thông tin:

| | aJiant Anti-Malware / S | Scan Scheduler | | | | | | | | | * 0 |
|----------------------|----------------------------|----------------|-----------------------|------|--|--------|--------------------|---------------|--------------|------------------------------|----------|
| -11 | Q Search | | | | | | | | | | ۹ |
| A⊾ ¹ ± | Showing 11 of 11 result(s) | | | 1 | Create new task | × | | | Show only | my schedule | New task |
| 9 | Task name | Author | Created time | Scar | Task name | | time | Next run time | Expired time | Status | Action |
| | ubuntu 2 | root | 06/10/2022 - 16:15:56 | Quic | new task 1 | | 10/2022 - 16:15:56 | N/A | N/A | • Finished | |
| | Ubuntu | root | 06/10/2022 - 16:11:44 | Quic | | | 10/2022 - 16:11:44 | N/A | N/A | Finished | |
| | Quick Win 11 | root | 06/10/2022 - 16:07:34 | Quic | Scan type Priority | | 10/2022 - 16:07:34 | N/A | N/A | Finished | |
| | Task win 11 | root | 06/10/2022 - 16:03:41 | Cust | Quick scan 🗸 Low | ~ | 10/2022 - 16:03:41 | N/A | N/A | Finished | |
| | Task 456 | root | 06/10/2022 - 11:37:08 | Quic | Tringer | | 10/2022 - 12:39:30 | N/A | N/A | Finished | |
| | Task 123 | root | 06/10/2022 - 11:34:26 | Quic | When this task is created | | 2)/2022 - 11:34:26 | N/A | N/A | Finished | |
| | éwewe | root | 06/10/2022 - 11:17:59 | Quic | Run immediately | | 10/2022 - 11:17:59 | N/A | N/A | Finished | |
| | Task 1 | root | 06/10/2022 - 11:14:04 | Quic | Run on a schedule | | 10/2022 - 11:14:04 | N/A | N/A | Finished | |
| | Task mai | root | 06/10/2022 - 11:10:10 | Quic | Assignee(s) | | 10/2022 - 11:10:10 | N/A | N/A | Finished | |
| | maitest | root | 06/10/2022 - 10:54:37 | Quic | All agents (total 38 agents) | | J/2022 - 10:54:37 | N/A | N/A | Finished | |
| | Task 2 | root | 06/10/2022 - 09:09:09 | Cust | Choose group(s) and agent(s) | | 10/2022 - 09:09:09 | N/A | N/A | Finished | |
| | | | | | Add agent/group Import from II | ist 🔻 | | | | | |
| | | | | | Information of selected agent(s) will be showing here. | | | | | | |
| | | | | | Cancel | Create | 4 | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | - |

5 – Thông tin lập lịch quét bao gồm: Task name, Scan type, Priority



- Task name: Người dùng nhập vào tên lập lịch quét;

- Scan type: Người dùng lựa chọn một trong 3 loại scan. Cho phép:

+ Quét nhanh: Kiểm tra nhanh các tệp và thư mục đáng ngờ tiềm ẩn;

+ Quét toàn bộ: Kiểm tra toàn bộ các tệp và thư mục trong máy tính. Quá trình này có thể mất vài giờ để hoàn thành;

+ Quét tùy chỉnh: Cho phép người dùng một tệp / thư mục cụ thể trong máy tính của bạn để quét.

- Priority: Cho phép người dùng lựa chọn tốc độ quét và thay đổi mức độ chiếm dụng tài nguyên của máy. Khi đặt mức ưu tiên cao, hệ thống sẽ quét nhanh chóng, tuy nhiên sẽ tiêu tốn nhiều tài nguyên của CPU. Tương tự, nếu chọn mức độ ưu tiên thấp, hệ thống sẽ quét chậm hơn và tiết kiệm tài nguyên CPU.

6 – Thông tin Trigger cho phép người dùng lựa chọn loại lập lịch quét:

- Run immediately: Cho phép người dùng lập lịch quét ngay lập tức dưới các máy trạm khi task vừa được tạo thành công;

- Run on Schedule: Cho phép người dùng lập lịch quét theo cấu hình của người dùng:

| Run on a schedule | |
|---|---|
| One time | ~ |
| Start time | |
| 31/10/2022 - 10:45:27 | ŧ |
| Run task as soon as possible after a schedule is missed | |

+ Schedule:

- One time: Lập lịch quét một lần;
- Daily: Lập lịch quét hàng ngày;
- Weekly: Lập lịch quét hàng tuần;



• Monthly: Lập lịch quét hàng tháng;

+ Start time: Cho phép người dùng nhập vào thời gian bắt đầu lập lịch quét

+ Ví dụ: Schedule: Daily, Start time: 15/08/2022 – 03:00:00. Được hiểu là cấu hình lập lịch quét hàng ngày lúc 03:00:00;

+ Run task as soon as possible after schedule is missed: Cho phép người dùng cấu hình lập lịch quét lại ngay khi lập lịch trước bị bỏ lỡ.

 7 – Thông tin Assignee: Cho phép người dùng cấu hình thông tin các máy trạm nhận lập lịch

- All Agent(s): Lập lịch với tất cả các máy trạm thuộc quyền quản lý của người dùng đang đăng nhập;

- Choose Agent(s) or Group(s):

+ Mục đích: Cho phép cấu hình, lựa chọn các máy trạm hoặc các nhóm máy trạm:



+ Các bước thực hiện: Add Agents or Group

• Add Agents or Group - Người dùng chọn **Add Agent**. Hệ thống hiển thị popup lựa chọn máy trạm:



| Q Search | | | | Create n | new t | ask | | × | | | | | |
|----------------------------|--------|-------------|--------|-----------------------|--------|----------------------|-------------------------|-------------|----------|-----------------|--------------|------------------------------|---------|
| Showing 11 of 11 result(s) | | | | Task name | | | | | | | Show only | my schedule | New tas |
| Task name | Author | Created tin | Add | agent(s) | | | | | > | < Next run time | Expired time | Status | Action |
| ubuntu 2 | root | 06/10/202 | fx | Search by queries | | | | | a | N/A | N/A | · Finished | |
| Ubuntu | root | 06/10/202 | - | | | | | | | N/A | N/A | · Finished | |
| Quick Win 11 | root | 06/10/202 | 38 res | sult(s) | 32 | - | | | 2.02 | N/A | N/A | · Finished | |
| Task win 11 | root | 06/10/202 | 0 | Agent ID | c | computer name | IP Address | Group | Status | N/A | N/A | · Finished | |
| Task 456 | root | 06/10/202 | | 06A6927157E4EEE09A0C | 76 a | ajiant-agent-centos6 | 127.0.0.1, 10.255.250 | auto_test | e Offiin | N/A | N/A | Finished | *** |
| Task 123 | foot | 06/10/202 | | 0715289C3AB47DF72E6E | 6C p | ohula-viettelos1018 | 127.0.0.1, 192.168.12 | default | e Offlin | N/A | N/A | Finished | |
| éwewe | root | 06/10/202 | | 0A691ACC638F0D4E54CA | 475_ V | Win7x64-A-PC | 10.0.2.15, 127.0.0.1 | maitest1 | e Offlin | N/A | N/A | · Finished. | |
| Task 1 | root | 06/10/202 | | 0AC36E41E40C67DE5A1E | F8_ p | phula-redhat7.7 | 127.0.0.1, 192.168.12 | chuyen_test | e Offlin | N/A | N/A | · Finished | |
| Task mai | root | 06/10/202 | | 0B726365F86EBFF5000E6 | 6B2 l | ocalhost.localdomain | 127.0.0.1, 192.168.19 | no_group | e Offlin | N/A | N/A | Finished | |
| maitest | root | 06/10/202 | | 0E1CBE9249C35DCDF763 | 8F2 u | ubuntu | 127.0.0.1, 192.168.12 | maitest1_1 | e Offlin | N/A | N/A | Finished | |
| Task 2 | root | 06/10/202 | | 155E59FAED2450B5750C8 | EF. p | ohula.redhat8.4 | 127.0.0.1, 192.168.12 | global | e Offlin | N/A | N/A | Finished | |
| | | | | 15706171377B8D10F47B8 | E8 a | agent-core-mac | 127.0.0.1, 192.168.6.2. | . no_group | ● Offlin | | | | |
| | | | | | | | | < 1 2 | 4 5 3 | | | | |
| | | | | | | | | | 2 | | | | |
| | | | | | | | | Can | el Ada | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | Cancel | (Printle | | | | | |
| | | | | | | | Curren | Contract (| | | | | |
| | | | | | | | | | | | | | |

• Tìm kiếm máy trạm:

 Tại popup Add agent(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: AgentID, Computer name, IP Adress, Group, Status, …

Người dùng chọn icon A hoặc nhấn nút Enter để xác nhận tìm

kiếm;

- Hệ thống sẽ hiển thị danh sách máy trạm theo truy vấn.
- Tích chọn một hoặc nhiều các máy trạm để thực thi lập lịch quét:



| Q Search | | | | Create new | v task | | × | | | | | |
|----------------------------|--------|-------------|-------|-------------------------|-------------------------|------------------------|----------------|-----------|---------------|--------------|------------------------------|----------|
| Showing 11 of 11 result(s) | | | Add | d agent(s) | | | | × | | Show only | my schedule | New tasi |
| Task name | Author | Created tin | fx | Search by queries | | | | Q | Next run time | Expired time | Status | Action |
| ubuntu 2 | root | 06/10/202 | Selec | cted (1) | | | | | N/A | N/A | Finished | |
| Ubuntu | root | 06/10/202 | pl | hula-redhat7.7 \times | | | | 0 ~ | N/A | N/A | Finished | |
| Quick Win 11 | root | 06/10/202 | | | | | | | N/A | N/A | Finished | |
| Task win 11 | root | 06/10/202 | 38 re | sult(s) | | | | | N/A | N/A | Finished | |
| Task 456 | root | 06/10/ | | Agent ID | Computer name | IP Address | Group | Status | N/A | N/A | Finished | |
| Task 123 | root | 06/10/202 | 0 | 06A6927157E4EEE09A0C76. | ajiant-agent-centos6 | 127.0.0.1, 10.255.250. | _ maitest1_2_3 | e Offline | N/A | N/A | Finished | |
| éwewe | root | 06/10/202 | 0 | 0715289C3AB47DF72E6E6C. | phula-viettelos1018 | 127.0.0.1, 192.168.12. | default | e Offline | N/A | N/A | Finished | |
| Task 1 | root | 06/10/202 | 0 | 0A691ACC638F0D4E54CA75 | Win7x64-A-PC | 10.0.2.15, 127.0.0.1 | maitest1 | e Offline | N/A | N/A | Finished | |
| Task mai | root | 06/10/202 | | 0AC36E41E40C67DE5A1EF8. | phula-redhat7.7 | 127.0.0.1, 192.168.12. | . chuyen_test | e Offline | N/A | N/A | Finished | |
| maitest | root | 06/10/202 | 0 | 0B726365F86EBFF5000E6B2 | _ localhost.localdomain | 127.0.0.1, 192.168.19. | . no_group | • Offline | N/A | N/A | Finished | |
| Task 2 | root | 06/10/202 | | 0E1CBE9249C35DCDF763F2 | ubuntu | 127.0.0.1, 192.168.12. | maitest1_1 | • Offline | N/A | N/A | Finished | |
| | | | | 155E59FAED2450B5750CEF. | phula.redhat8.4 | 127.0.0.1, 192.168.12. | global | e Offline | | | | |
| | | | | 15706171377B8D10F47BE8 | agent-core-mac | 127.0.0.1, 192.168.6.2 | _ no_group | e offline | | | | |
| | | | - | | | | | | | | | |
| | | | | | | | | 4 3 7 | | | | |
| | | | | | | | Cancel | Add | 2 | | | |
| | | | - | _ | | Cancel | Create and | | 1 | | | |
| | | | | | | Guiner | | | | | | |
| | | | | | | | | | | | | |

- Chọn nút Add để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút Cancel để thực hiện hủy thao tác thêm thông tin Agent/ Group;

➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin máy trạm đã được chọn.

• Add Agents or Group - Người dùng chọn **Add Group**. Hệ thống hiển thị popup lựa chọn group:

• Tìm kiếm group:

 Tại popup Add group(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: Group name

Người dùng chọn icon a hoặc nhấn nút Enter để xác nhận tìm

kiếm;

- → Hệ thống sẽ hiển thị danh sách group
 - Tích chọn một hoặc nhiều group để thực thi lập lịch quét:



| ≡ | aJiant Anti-Malware / Sc | an Scheduler | | | | | | | | | ÷ 0 |
|------------|---------------------------------|--------------|----------------|--------------------------------------|----------|---|----------------------------------|-----------|---------------|--------------|------------------------------|
| | Q Search | | | Add group(s) | | | | × | | | ٩ |
| A | | | _ | Q Search by group name | | | | Q | | | |
| Ρđ | Showing 50 of 759.426 result(s) | | | NOTE: In this interface, users being | nging to | the parent group have full control over all the chi | ild groups of their parent gr Se | e more >> | | Show only | my schedule 🕒 New task |
| 0 | Task name | Author | Created time | TENANT nsm com | ` | A thanhnm18 test | R & liennt | | Next run time | Expired time | Status Action |
| 112000 | Duplicate this task | root_test | 22/09/2022 - 1 | | <i>'</i> | | | | ó N/A | N/A | Finished |
| <u>}-</u> | Test immediately | root_test | 22/09/2022 - 1 | 🗖 💑 global | > | 🖉 💑 no_group 💦 🗲 🗲 | | | N/A | N/A | Finished |
| | Task name immediately main | root_test | 22/09/2022 - 1 | 🗖 🐣 admin | > | n 🖧 phula test | 1 | | N/A | N/A | Finished |
| ж | Task name immediately mai | root_test | 22/09/2022 - 1 | - ••• | | 0.00 | | | 7 N/A | N/A | Finished |
| * | Task name immediately | root_test | 22/09/2022 - 1 | TENANT_edr.com | > | 🗆 💑 new_group | | | 7 N/A | N/A | Finished |
| Ê | Task test immediately | root_test | 22/09/2022 - 1 | TENANT_viettel.c | > | □ 🖧 anhnn_test 🔹 🔉 | | | 5 N/A | N/A | Finished |
| | Task mai test immediately | root_test | 22/09/2022 - 0 | | | | 1 | _ | 5 N/A | N/A | Finished |
| ι <u>φ</u> | data 1 | root_test | 20/09/2022 - 1 | Selected | | | | | 5 N/A | N/A | Finished |
| | test create | root_test | 16/09/2022 - 1 | 3 group(s) | | | | | N/A | N/A | Finished |
| | create test agent edr test 2 | root_test | 14/09/2022 - 1 | Group | Loca | tion | | Action | 2 N/A | N/A | Finished |
| | data-test-1-20-5-9-999 | root_test | 09/09/2022 - 1 | TENANT_nsm.com | | | | | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-998 | root_test | 09/09/2022 - 1 | vcs_server | globa | il | | × | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-997 | root_test | 09/09/2022 - 1 | | | | | | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-996 | root_test | 09/09/2022 - 1 | 💑 no_group | admi | n | | | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-995 | root_test | 09/09/2022 - 1 | | | | | | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-994 | root_test | 09/09/2022 - 1 | | | | | | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-993 | root_test | 09/09/2022 - 1 | | | | | | 5 N/A | N/A | Finished |
| | data-test-1-20-5-9-992 | root_test | 09/09/2022 - 1 | | | | | | i N/A | N/A | Finished |
| | data-test-1-20-5-9-991 | root_test | 09/09/2022 - 1 | | | | | | 5 N/A | N/A | Finished |
| | | | | | | | Cancel | Save | | | |
| | | | | | | | | _ | | | Back to top |
| | | | | | | | | | | | 4 |

- Chọn nút Add để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút Cancel để thực hiện hủy thao tác thêm thông tin Agent/ Group;
- ➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin group đã được chọn.

 + Import from .CSV: Cho phép người dùng tải lên danh sách máy trạm bằng cách:

• Lựa chọn vào nút Import from list;

• Lựa chọn **Download sample file**, cho phép tải xuống file mẫu danh sách máy trạm;

• Người dùng nhập thông tin máy trạm và tải lên file danh sách máy trạm bằng cách chọn nút **Import from .CSV**

Bước 6: Người dùng chọn nút **Create** để hoàn thiện thao tác thêm mới lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác thêm mới lập lịch quét



3.5.1.3 Nhân bản Schedule task

- Mục đích: Cho phép người dùng nhân bản lập lịch quét.
- Các bước thực hiện:

Bước 7: Tại màn hình danh sách task, người dùng chọn **Duplicate** bản ghi task cần nhân bản:

| = | aJiant Anti-Malware / S | Scan Scheduler | | | | | | | | | # 0 |
|----------------|----------------------------|----------------|-----------------------|-------------|--------------------|--------------------------|-----------------------|---------------|--------------|------------------------------|------------|
| <u>∼</u> | Q Search | | | | | | | | | | ٩ |
| T ₂ | Showing 11 of 11 result(s) | | | | | | | | Show only r | ny schedule 🕒 | New task |
| 0 | Task name | Author | Created time | Scan type | Number of agent(s) | Trigger | Start time | Next run time | Expired time | Status | Action |
| | ubuntu 2 | root | 06/10/2022 - 16:15:56 | Quick scan | 1 | Immediately | 06/10/2022 - 16:15:56 | N/A | N/A | • Finished | |
| <u>P-</u> | Ubuntu | root | 06/10/2022 - 16:11:44 | Quick scan | 1 | Immediately | 06/10/2022 - 16:11:44 | N/A | N/A | View report | |
| | Quick Win 11 | root | 06/10/2022 - 16:07:34 | Quick scan | 1 | Immediately | 06/10/2022 - 16:07:34 | N/A | N/A | View detail | |
| | Task win 11 | root | 06/10/2022 - 16:03:41 | Custom scan | 1 | Immediately | 06/10/2022 - 16:03:41 | N/A | N/A | Duplicate this task | |
| - 🐺 - | Task 456 | root | 06/10/2022 - 11:37:08 | Quick scan | 1 | At 06/10/2022 - 12:39:30 | 06/10/2022 - 12:39:30 | N/A | N/A | Delete this task | |
| Ē | Task 123 | root | 06/10/2022 - 11:34:26 | Quick scan | 1 | Immediately | 06/10/2022 - 11:34:26 | N/A | N/A | • Financu | |
| | éwewe | root | 06/10/2022 - 11:17:59 | Quick scan | 2 | Immediately | 06/10/2022 - 11:17:59 | N/A | N/A | Finished | |
| ē | Task 1 | root | 06/10/2022 - 11:14:04 | Quick scan | 2 | Immediately | 06/10/2022 - 11:14:04 | N/A | N/A | Finished | |
| | Task mai | root | 06/10/2022 - 11:10:10 | Quick scan | 1 | Immediately | 06/10/2022 - 11:10:10 | N/A | N/A | Finished | |
| | maitest | root | 06/10/2022 - 10:54:37 | Quick scan | 1 | Immediately | 06/10/2022 - 10:54:37 | N/A | N/A | Finished | |
| | Task 2 | root | 06/10/2022 - 09:09:09 | Custom scan | 1 | Immediately | 06/10/2022 - 09:09:09 | N/A | N/A | Finished | |
| | | | | | | | | | | | |
| | | | | | | | | | | | 4 |

Bước 8: Hệ thống hiển thị màn hình Duplicate task, người dùng nhập lại task name và kiểm tra lại toàn bộ thông tin trước khi nhân bản



| = | aJiant Anti-Malware / Sc | an Scheduler | | | | | | | | | | | | # 0 |
|--------------|---------------------------------|--------------|-----------------------|-------|---|---------|---------------|---------------|---------|--------------------|---------------|--------------|------------------------------|------------|
| E. | O Search | | | | | | | | | | | | | |
| Δ | | | | - | Duplicate task | | | | × | | | | | |
| - | | | | | Task name | | | | | | | | _ | |
| H | Showing 50 of 759.426 result(s) | | | | (<u>[</u> | | | | | | | Show only | my schedule | New task |
| 0 | Task name | Author | Created time | Scar | A View and Blazer this Reid blazer | | | | | rt time | Next run time | Expired time | Status | Action |
| Ŭ | Duplicate this task | root_test | 22/09/2022 - 17:25:36 | Quic | Scan type 0 | \$ | Priority 🕚 | | | 09/2022 - 17:25:36 | N/A | N/A | • Finished | |
| >- | Test immediately | root_test | 22/09/2022 - 10:56:27 | Cust | Quick scan | ~ | Low | | ~ | 09/2022 - 10:56:27 | N/A | N/A | Finished | |
| 0 | Task name immediately main | root_test | 22/09/2022 - 10:27:27 | Cust | Trigger | | | | | 09/2022 - 10:30:47 | N/A | N/A | · Finished | |
| | Task name immediately mai | root_test | 22/09/2022 - 10:19:37 | Cust | When this task is created | | | | | 09/2022 - 10:19:37 | N/A | N/A | Finished | |
| * | Task name immediately | root_test | 22/09/2022 - 10:17:37 | Cust | Run immediately | | | | | 09/2022 - 10:17:37 | N/A | N/A | · Finished | |
| rft. | Task test immediately | root_test | 22/09/2022 - 10:05:35 | Cust | Run on a schedule | | | | | 09/2022 - 10:05:35 | N/A | N/A | Finished | |
| - <u>1</u> | Task mai test immediately | root_test | 22/09/2022 - 09:53:55 | Cust | Assignee(s) | | | | | 09/2022 - 09:53:55 | N/A | N/A | Finished | |
| <u>م</u> | data 1 | root_test | 20/09/2022 - 17:42:46 | Quic | All agents (total 836 agents) | | | | | 09/2022 - 17:42:46 | N/A | N/A | • Finished | |
| | test create | root_test | 16/09/2022 - 15:04:59 | Quic | Choose group(s) and agent(s) | s) | | | | 09/2022 - 15:04:59 | N/A | N/A | • Finished | |
| | create test agent edr test 2 | root_test | 14/09/2022 - 10:08:36 | Cust | 4 assignee(s) | G Add | l agent/group | p Import fro | om list | 09/2022 - 10:10:42 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-999 | root_test | 09/09/2022 - 18:54:45 | Quic | Assignee Type | Comput | ter name | IP Address | Action | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-998 | root_test | 09/09/2022 - 18:54:45 | Quic | 1FBAFFB82BBC6 agent | virtual | agent_phul | 172.17.0.22 | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-997 | root_test | 09/09/2022 - 18:54:45 | Quic | 09D9E77F49E63 agent | virtual | agent_phul | 172.17.0.2 | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-996 | root_test | 09/09/2022 - 18:54:45 | Quic | 504615DE542C6 agent | Win10x | 64MAINTN | 192.168.74.12 | 8 | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-995 | root_test | 09/09/2022 - 18:54:45 | Quic | EC8EB5F0DAB21 agent | Win10x | 64_MaiNTN | 192.168.74.12 | 8 | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-994 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-993 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | 1 | · • • · | 09/2022 - 18:54:45 | N/A | N/A | • Finished | |
| | data-test-1-20-5-9-992 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | Canaal | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-991 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | Cancel | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | | | 40.00.0000 AD.54.15 | A.1.5 | 4.8 | 6 8.6 | | | | | MAR | | the set of | |

Bước 9: Người dùng chọn nút **Create** để hoàn thiện thao tác nhân bản lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác nhân bản lập lịch quét.

| Q Search | | | 1 | 2 1 1 1 1 1 1 1 | | | | 1 | | | | |
|---------------------------------|-----------|-----------------------|------|---|------------------|------------------|-----------|--------------------|---------------|--------------|------------------------------|------|
| | | | | Duplicate task | | | × | | | | | |
| Showing 50 of 759.426 result(s) | | | | Task name | | | | | | Show only | my schedule | New |
| Task name | Author | Created time | Scar | Task 1 | | | | rt time | Next run time | Expired time | Status | Acti |
| Duplicate this task | root test | 22/09/2022 - 17:25:36 | Ouic | Scan type 🚯 | Priority (| | | 09/2022 - 17:25:36 | N/A | N/A | Einished | |
| Test immediately | root test | 22/09/2022 - 10:56:27 | Cust | Quick scan | ✓ Low | | ~ | 09/2022 - 10:56:27 | N/A | N/A | Finished | |
| Task name immediately main | root_test | 22/09/2022 - 10:27:27 | Cust | Tripper | | | | 09/2022 - 10:30:47 | N/A | N/A | Finished | |
| Task name immediately mai | root_test | 22/09/2022 - 10:19:37 | Cust | When this task is created | | | | 09/2022 - 10:19:37 | N/A | N/A | Finished | |
| Task name immediately | root_test | 22/09/2022 - 10:17:37 | Cust | Run immediately | | | | 09/2022 - 10:17:37 | N/A | N/A | · Finished | |
| Task test immediately | root_test | 22/09/2022 - 10:05:35 | Cust | Run on a schedule | | | | 09/2022 - 10:05:35 | N/A | N/A | Finished | |
| Task mai test immediately | root_test | 22/09/2022 - 09:53:55 | Cust | Assignee(s) | | | | 09/2022 - 09:53:55 | N/A | N/A | Finished | |
| data 1 | root_test | 20/09/2022 - 17:42:46 | Quic | All agents (total 836 agents) | | | | 09/2022 - 17:42:46 | N/A | N/A | Finished | |
| test create | root_test | 16/09/2022 - 15:04:59 | Quic | Choose group(s) and agent(s) | i) | | | 09/2022 - 15:04:59 | N/A | N/A | Finished | |
| create test agent edr test 2 | root_test | 14/09/2022 - 10:08:36 | Cust | 4 assignee(s) | Add agent/g | import fro | om list v | 09/2022 - 10:10:42 | N/A | N/A | Finished | |
| data-test-1-20-5-9-999 | root_test | 09/09/2022 - 18:54:45 | Quic | Assignee Type | Computer name | IP Address | Action | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-998 | root_test | 09/09/2022 - 18:54:45 | Quic | 1FBAFFB82BBC6 agent | virtual_agent_ph | ıl 172.17.0.22 | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-997 | root_test | 09/09/2022 - 18:54:45 | Quic | 09D9E77F49E63 agent | virtual_agent_ph | ul 172.17.0.2 | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-996 | root_test | 09/09/2022 - 18:54:45 | Quic | 504615DE542C6 agent | Win10x64MAINT | N 192.168.74.12 | 28 | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-995 | root_test | 09/09/2022 - 18:54:45 | Quic | EC8EB5F0DAB21 agent | Win10x64_MaiN | IN 192.168.74.12 | 28 | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-994 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-993 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | · • | 2/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-992 | root_test | 09/09/2022 - 18:54:45 | Quic | | | Cancel | Create | /2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-991 | root_test | 09/09/2022 - 18:54:45 | Quic | | | Cancel | Greate | 09/2022 - 18:54:45 | N/A | N/A | Finished | |

3.5.1.4 Xem chi tiết

- Mục đích: Cho phép người dùng xem thông tin chi tiết lập lịch quét
- Các bước thực hiện:





Bước 10: Tại màn hình danh sách task, người dùng chọn **View Detail** bản ghi task cần xem chi tiết;

| Q Search | | | | | | | | | | | | | |
|---------------------------------|-----------|-----------------------|------|---|-------|------------|----------------|--------|--------------------|---------------|--------------|------------------------------|-----|
| | | | | View task detail | | | | × | | | | | |
| Showing 50 of 759.426 result(s) | | | | Task name | | | | | | | Show only | my schedule | New |
| Task name | Author | Created time | Scar | Task test immediately | | | | | rt time | Next run time | Expired time | Status | Act |
| Duplicate this task | root_test | 22/09/2022 - 17:25:36 | Quic | Scan type 🚯 | | Priority 😝 | | | 09/2022 - 17:25:36 | N/A | N/A | Finished | |
| Test immediately | root_test | 22/09/2022 - 10:56:27 | Cust | Custom soon | | Low | | | 09/2022 - 10:56:27 | N/A | N/A | Finished | |
| Task name immediately main | root_test | 22/09/2022 - 10:27:27 | Cust | custom scan | Ť | LOW | | Ť | 09/2022 - 10:30:47 | N/A | N/A | Finished | |
| Task name immediately mai | root_test | 22/09/2022 - 10:19:37 | Cust | Target(s) | | | | | 09/2022 - 10:19:37 | N/A | N/A | Finished | |
| Task name immediately | root_test | 22/09/2022 - 10:17:37 | Cust | Application Data $	imes$ | | | | ~ | 09/2022 - 10:17:37 | N/A | N/A | Finished | |
| Task test immediately | root_test | 22/09/2022 - 10:05:35 | Cust | Trigger | | | | | 09/2022 - 10:05:35 | N/A | N/A | Finished | |
| Task mai test immediately | root_test | 22/09/2022 - 09:53:55 | Cust | When this task is created | | | | | 09/2022 - 09:53:55 | N/A | N/A | Finished | |
| data 1 | root_test | 20/09/2022 - 17:42:46 | Quic | Run immediately | | | | | 09/2022 - 17:42:46 | N/A | N/A | Finished | |
| test create | root_test | 16/09/2022 - 15:04:59 | Quic | Run on a schedule | | | | | 09/2022 - 15:04:59 | N/A | N/A | Finished | |
| create test agent edr test 2 | root_test | 14/09/2022 - 10:08:36 | Cust | Assignee(s) | | | | | 09/2022 - 10:10:42 | N/A | N/A | Finished | |
| data-test-1-20-5-9-999 | root_test | 09/09/2022 - 18:54:45 | Quic | All agents (total 836 agent | ts) | | | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-998 | root_test | 09/09/2022 - 18:54:45 | Quic | Choose group(s) and ager | it(s) | | | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-997 | root_test | 09/09/2022 - 18:54:45 | Quic | 1 assignee(s) | 0/ | | | m list | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-996 | root_test | 09/09/2022 - 18:54:45 | Quic | Assignee Type | Com | puter name | IP Address | Action | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-995 | root_test | 09/09/2022 - 18:54:45 | Quic | AE6C56DE45F9A agent | Main | tnWinx64 | 192.168.74.128 | 8 | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-994 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | < | 1 > | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-993 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | | _ | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-992 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | | Cancel | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-991 | root_test | 09/09/2022 - 18:54:45 | Quic | | | | | | 09/2022 - 18:54:45 | N/A | N/A | Finished | |
| 1 | | | ~ | | | | | | | | | | |

→ Hệ thống hiển thị màn hình chi tiết lập lịch quét

Bước 11: Người dùng chọn nút **Cancel** hoặc icon **Close** để hủy thao tác xem chi tiết lập lịch quét

3.5.1.5 Xóa Schedule task

- Mục đích: Cho phép xóa lập lịch quét trong danh sách task;
- Các bước thực hiện:
- **Bước 12:** Tại màn hình danh sách task, người dùng chọn **Delete this task** bản ghi task cần xóa;



| aJiant Anti-Malware / Sc | an Scheduler | | | | | | | | | - |
|---------------------------------|--------------|-----------------------|-------------|--------------------|--------------------------|-----------------------|---------------|--------------|------------------------------|-----------|
| Q Search | | | | | | | | | | |
| | | | | | | | | | | |
| Showing 50 of 759.426 result(s) | | | | | | | | Show on | ly my schedule |) New ta: |
| Task name | Author | Created time | Scan type | Number of agent(s) | Trigger | Start time | Next run time | Expired time | Status | Action |
| Duplicate this task | root_test | 22/09/2022 - 17:25:36 | Quick scan | 5 | Immediately | 22/09/2022 - 17:25:36 | N/A | N/A | Finished | |
| Test immediately | root_test | 22/09/2022 - 10:56:27 | Custom scan | 1 | Immediately | 22/09/2022 - 10:56:27 | N/A | N/A | Finished | |
| Task name immediately main | root_test | 22/09/2022 - 10:27:27 | Custom scan | 1 | At 22/09/2022 - 10:30:47 | 22/09/2022 - 10:30:47 | N/A | N/A | Finished | |
| Task name immediately mai | root_test | 22/09/2022 - 10:19:37 | Custom scan | 1 | Immediately | 22/09/2022 - 10:19:37 | N/A | N/A | Finished | |
| Task name immediately | root_test | 22/09/2022 - 10:17:37 | Custom scan | 1 | Immediately | 22/09/2022 - 10:17:37 | N/A | N/A | View report | |
| Task test immediately | root_test | 22/09/2022 - 10:05:35 | Custom scan | 1 | Immediately | 22/09/2022 - 10:05:35 | N/A | N/A | View detail | |
| Task mai test immediately | root_test | 22/09/2022 - 09:53:55 | Custom scan | 1 | Immediately | 22/09/2022 - 09:53:55 | N/A | N/A | Duplicate this tas | k |
| data 1 | root_test | 20/09/2022 - 17:42:46 | Quick scan | 1 | Immediately | 20/09/2022 - 17:42:46 | N/A | N/A | Delete this task | |
| test create | root_test | 16/09/2022 - 15:04:59 | Quick scan | 0 | Immediately | 16/09/2022 - 15:04:59 | N/A | N/A | • Finished | _ |
| create test agent edr test 2 | root_test | 14/09/2022 - 10:08:36 | Custom scan | 1 | At 29/09/2022 - 10:10:42 | 29/09/2022 - 10:10:42 | N/A | N/A | Finished | |
| data-test-1-20-5-9-999 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-998 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-997 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-996 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-995 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-994 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-993 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-992 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-991 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | | | - · · · | ** | 1. B. 1. 1 | | | | 100 - 10 - 1 | |

Bước 13: Hệ thống hiển thị màn hình popup Xác nhận xóa. Người dùng chọn No để hủy thao tác xóa lập lịch quét hoặc chọn Yes, keep delete để tiếp tục thao tác xóa

| ₹ | aJiant Anti-Malware / Sca | in Scheduler | | | | | | | | | | # 0 |
|------------|---------------------------------|--------------|-----------------------|-------------|--------------------|--|---|-----------------------|---------------|--------------|------------------------------|------------|
| (1) (1) | Q Search | | | | | | | | | | | Q |
| A | | | | | | | | | | | | |
| ۴t | Showing 50 of 759.426 result(s) | | | | | | | | | Show only | my schedule 🕒 N | ew task |
| 0 | Task name | Author | Created time | Scan type | Number of agent(s) | Trigger | | Start time | Next run time | Expired time | Status | Action |
| | Duplicate this task | root_test | 22/09/2022 - 17:25:36 | Quick scan | 5 | Immediately | | 22/09/2022 - 17:25:36 | N/A | N/A | Finished | |
| <u>}-</u> | Test immediately | root_test | 22/09/2022 - 10:56:27 | Custom scan | 1 | Immediately | | 22/09/2022 - 10:56:27 | N/A | N/A | Finished | |
| | Task name immediately main | root_test | 22/09/2022 - 10:27:27 | Custom scan | 1 | At 22/09/2022 - 10:30:47 | | 22/09/2022 - 10:30:47 | N/A | N/A | Finished | |
| | Task name immediately mai | root_test | 22/09/2022 - 10:19:37 | Custom sca | | | ~ | 22/09/2022 - 10:19:37 | N/A | N/A | Finished | |
| | Task name immediately | root_test | 22/09/2022 - 10:17:37 | Custom sca | | • | | 22/09/2022 - 10:17:37 | N/A | N/A | Finished | |
| Ē | Task test immediately | root_test | 22/09/2022 - 10:05:35 | Custom sca | | Delete this task? | | 22/09/2022 - 10:05:35 | N/A | N/A | Finished | |
| | Task mai test immediately | root_test | 22/09/2022 - 09:53:55 | Custom sca | | | | 22/09/2022 - 09:53:55 | N/A | N/A | Finished | |
| ě | data 1 | root_test | 20/09/2022 - 17:42:46 | Quick scan | | | _ | 20/09/2022 - 17:42:46 | N/A | N/A | Finished | |
| | test create | root_test | 16/09/2022 - 15:04:59 | Quick scan | Are you sure yo | ou want to delete the task "Task name immediately mai"? | | 16/09/2022 - 15:04:59 | N/A | N/A | Finished | |
| | create test agent edr test 2 | root_test | 14/09/2022 - 10:08:36 | Custom sca | | infine diatery man | | 29/09/2022 - 10:10:42 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-999 | root_test | 09/09/2022 - 18:54:45 | Quick scan | | No Yes, keep delete | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-998 | root_test | 09/09/2022 - 18:54:45 | Quick scan | | | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-997 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-996 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-995 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-994 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-993 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-992 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | data-test-1-20-5-9-991 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | | | | ~ 11 | ** | | _ | | | | | |
| | | | | | | | | | | | | k to top |
| | | | | | | | | | | | | 4 |

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



3.5.1.6 Xem báo cáo

- Mục đích: Cho phép người dùng xem báo cáo lập lịch quét;
- Các bước thực hiện:

Bước 14: Tại màn hình danh sách task, người dùng chọn **View report** bản ghi task cần xem báo cáo;

| Q Search | | | | | | | | | | |
|---------------------------------|-----------|-----------------------|-------------|--------------------|--------------------------|-----------------------|---------------|--------------|------------------------------|-----|
| Showing 50 of 759.426 result(s) | | | | | | | | Show of | nly my schedule | New |
| Task name | Author | Created time | Scan type | Number of agent(s) | Trigger | Start time | Next run time | Expired time | Status | Act |
| Duplicate this task | root_test | 22/09/2022 - 17:25:36 | Quick scan | 5 | Immediately | 22/09/2022 - 17:25:36 | N/A | N/A | Finished | |
| Test immediately | root_test | 22/09/2022 - 10:56:27 | Custom scan | 1 | Immediately | 22/09/2022 - 10:56:27 | N/A | N/A | Finished | |
| Task name immediately main | root_test | 22/09/2022 - 10:27:27 | Custom scan | 1 | At 22/09/2022 - 10:30:47 | 22/09/2022 - 10:30:47 | N/A | N/A | Finished | |
| Task name immediately mai | root_test | 22/09/2022 - 10:19:37 | Custom scan | 1 | Immediately | 22/09/2022 - 10:19:37 | N/A | N/A | Finished | |
| Task name immediately | root_test | 22/09/2022 - 10:17:37 | Custom scan | 1 | Immediately | 22/09/2022 - 10:17:37 | N/A | N/A | Finished | |
| Task test immediately | root_test | 22/09/2022 - 10:05:35 | Custom scan | 1 | Immediately | 22/09/2022 - 10:05:35 | N/A | N/A | Finished | |
| Task mai test immediately | root_test | 22/09/2022 - 09:53:55 | Custom scan | 1 | Immediately | 22/09/2022 - 09:53:55 | N/A | N/A | Finished | ŀ |
| data 1 | root_test | 20/09/2022 - 17:42:46 | Quick scan | 1 | Immediately | 20/09/2022 - 17:42:46 | N/A | N/A | View report | |
| test create | root_test | 16/09/2022 - 15:04:59 | Quick scan | 0 | Immediately | 16/09/2022 - 15:04:59 | N/A | N/A | View detail | - |
| create test agent edr test 2 | root_test | 14/09/2022 - 10:08:36 | Custom scan | 1 | At 29/09/2022 - 10:10:42 | 29/09/2022 - 10:10:42 | N/A | N/A | Duplicate this tas | k |
| data-test-1-20-5-9-999 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Delete this task | |
| data-test-1-20-5-9-998 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | • Financo | |
| data-test-1-20-5-9-997 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-996 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-995 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-994 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-993 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-992 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| data-test-1-20-5-9-991 | root_test | 09/09/2022 - 18:54:45 | Quick scan | 10 | Immediately | 09/09/2022 - 18:54:45 | N/A | N/A | Finished | |
| | | | - · · · | ** | | | | | 100 - 1 - 1 | _ |

Bước 15: Hệ thống hiển thị màn hình View report:

8 – Tìm kiếm:

- Mục đích: Cho phép tìm kiếm truy vấn các thông tin trong báo cáo như: AgentID, Computer name, IP Address, Platform, Group, Status, Result

- Các bước thực hiện:



| View task repo | ort | | | | | | | × |
|-----------------|---------------------------|-----------------------|--|--|---------------|------------------------------------|---|----|
| Task name | Task per | | | Created time | 14/09/202 | 22 14:32:24 | | |
| Author | root_test | | | Scan type | Custom s | can 🔁 | | |
| fx | | | | | | Q 🕁 Export | to Excel | rd |
| 5 result(s) | | | | | -0 | | | |
| Agent ID | | Computer name | IP Address | Platform | Group | Status | Result | |
| FC97D9289BFA70F | 681BB4B8FED595CDEA2CA9AD1 | bich3_win7x86 | 192.168.255.1 36 | Microsoft Windows 7 Ultimate Service Pack 1 | group_windows | Scan skip | Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule | |
| 524B30C4C568F59 | 292D6076E25F4C83AF5C33B5C | EDR-TEST02 | 192.168.133.1, 192.168.255.1, 192.168.6.40 | Microsoft Windows 10 Enterprise | group_1 | Scan completed | Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0 | |
| F2AA317BE87690E | 505BF7D25CA6A7DC68D1FC37D | Blchpt3_Win10Tes t | 192.168.255.1 38 | Microsoft Windows 10 Pro | group_windows | • Scan completed | Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0 | |
| | | | | | | | 🕜 Back to to | p |

+ Người dùng nhập vào thông tin truy vấn và chọn icon <a> hoặc nhấn nút Enter để xác nhận truy vấn;

→ Hệ thống hiển thị danh sách kết quả báo cáo lập lịch quét sau khi truy vấn.

9 - Export to Excel

- Mục đích: Cho phép người dùng tải xuống báo cáo kết quả lập lịch quét theo định dạng file Excel;

| View task repor | rt | | | | | | | × |
|------------------|--------------------------|-----------------------|--|--|---------------|------------------------------------|---|---|
| Task name | Task per | | | Created time | 14/09/202 | 22 14:32:24 | | |
| Author | root_test | | | Scan type | Custom se | can | | |
| fx | | | | | | Q ± Ex | port to Excel | View on Dashboard |
| 5 result(s) | | | | | | | | |
| Agent ID | | Computer name | IP Address | Platform | Group | Status | Result | |
| FC97D9289BFA70F6 | 81BB4B8FED595CDEA2CA9AD1 | bich3_win7x86 | 192.168.255.1 36 | Microsoft Windows 7 Ultimate Service Pack 1 | group_windows | Scan skip | Start time End time: Agent mis | :: 15/09/2022 14:34:52 15/09/2022 14:34:52 ssed this schedule |
| 524B30C4C568F592 | 92D6076E25F4C83AF5C33B5C | EDR-TEST02 | 192.168.133.1, 192.168.255.1, 192.168.6.40 | Microsoft Windows 10 Enterprise | group_1 | Scan completed | Start time End time: Total file s Total male | : 14/09/2022 14:36:18 14/09/2022 14:36:59 scan: 96 ware found: 0 |
| F2AA317BE87690E5 | 05BF7D25CA6A7DC68D1FC37D | Blchpt3_Win10Tes t | 192.168.255.1 38 | Microsoft Windows 10 Pro | group_windows | Scan completed | Start time End time: Total file s Total mah | : 14/09/2022 14:36:18 14/09/2022 14:36:52 scan: 28 ware found: 0 |
| | | | | | | | | Back to top |



viettel

- Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút

Export to Excel

→ Hệ thống cho phép tải xuống file kết quả báo cáo lập lịch quét.

10 - View on dashboard

- Mục đích: Cho phép xem báo cáo thống kê Anti-malware của hệ thống

| View task repo | ort | | | | | | × |
|-----------------|---------------------------|-----------------------|--|--|---------------|------------------------------------|---|
| Task name | Task per | | | Created time | 14/09/202 | 22 14:32:24 | |
| Author | root_test | | | Scan type | Custom s | can | |
| fx | | | | | | Q Export | to Excel |
| 5 result(s) | | | | | | | |
| Agent ID | | Computer name | IP Address | Platform | Group | Status | Result |
| FC97D9289BFA70F | 681BB4B8FED595CDEA2CA9AD1 | bich3_win7x86 | 192.168.255.1 36 | Microsoft Windows 7 Ultimate Service Pack 1 | group_windows | • Scan skip | Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule |
| 524B30C4C568F59 | 292D6076E25F4C83AF5C33B5C | EDR-TEST02 | 192.168.133.1, 192.168.255.1, 192.168.6.40 | Microsoft Windows 10 Enterprise | group_1 | Scan completed | Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0 |
| F2AA317BE87690E | 505BF7D25CA6A7DC68D1FC37D | Blchpt3_Win10Tes t | 192.168.255.1 38 | Microsoft Windows 10 Pro | group_windows | Scan completed | Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0 |
| | | | | | | | Back to top |

- Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút View on dashboard

→ Hệ thống điều hướng sang trang báo cáo thống kê Anti-malware của hệ thống;

B. Giao diện Agent

3.6 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":



| Viettel Endpoint Detection & Response | |
|---------------------------------------|---|
| Helpdesk support | > |
| Check policy compliance | |
| | |

- Hệ thống hiển thị các thông tin:
 - + Trường hợp máy không có mã độc nào hoặc toàn bộ mã độc đã được xử

lý:

| V | Viettel Endpoint | Detection & Response | - × |
|---|-------------------|----------------------|-----------------|
| | V | Clean | |
| | disinfected (96%) | NOT PR | OCESSED (4%) |
| الله عنها عنها المعالم المعالم المعالم المعالم | an G | Reports | i About |

+ 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;



| V | Viettel | Endpoint Detection & Res | sponse – × |
|---|-----------------------------|--------------------------|--------------------------------|
| | | Critical | |
| | DISINFECTED 52 (96%) | | NOT PROCESSED 2 (4%) |
| | 🕄 Scan | Reports | i About |
| | | | |

+ 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.

3.7 About

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

| V | About | × |
|------------------------------|--|-------------|
| _{viettel} ajiant | Viettel Endpoint Detection & Response VERSION 11.0.2215 | |
| | OPERATION SYSTEM Microsoft Windows 10 x64 | |
| | For more detail, please contact us via <u>cskh_anm@viettel.com.</u> © 2021 Viettel Cyber Security - Branch of Viettel Group | <u>vn</u> . |



3.8 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;

| V | | Reports | – o × | | | | | |
|--|---------------------|----------------------------------|---------------------------------|--|--|--|--|--|
| Copies of disinfected or modified files during disinfection are move to Backup folder. Those files are stored in a dedicated format and do not impose any threats, you can restore, remove or clear all files in Backup folder any time. | | | | | | | | |
| 🔿 Restore 🛛 😣 R | Remove 🗍 前 Clear st | torage | | | | | | |
| Event date | Status | Object | File path | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit.MSOffice.Generic | C:\Windows\System32\svchost.exe | | | | | |
| 27/07/2021 - 15:53:12 | Fail to disinfected | Trojan: Exploit MSOffice Generic | C:\Windows\System32\svchost.exe | | | | | |

- 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:

^{O Restore}: Cho phép lựa chọn 01 file để phục hồi;

^{S Remove}: Cho phép lựa chọn 01 file để xóa khỏi thư mục Backup;

3.9 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 đôc:







Stop scanning

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

^DPause: Cho phép tạm dừng quá trình quét;

: Cho phép kết thúc quá trình quét;

E View report : Trường hợp phát hiện được ít nhất một mã độc, cho phép xem nhanh trạng thái xử lý tại <u>3.14 Reports;</u>

Màn hình khi người dùng chọn tạm dừng quá trình quét

| Q | Paused (33%) ² malware detected | | | | | |
|---|--|-----------------|--------|---------------|--|--|
| | DURATION OBJECTS SCANNED | 00:00:02 868 | | | | |
| | Paused scan. Click 'Resume' to continue your scanning. | | | | | |
| | 🔓 View report | | Resume | Stop scanning | | |
| | | | | | | |

Resume : Cho phép chọn để tiếp tục quét hoặc stop scanning để hoàn thành quá

trình quét.

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

