viettel
security

Viettel Endpoint Detection & Response (VCS-aJiant)

Phiên bản 3.3.0 – Năm 2021
Ngày cập nhật: 29/11/2021

Tài liệu Hướng dẫn sử dụng

Mục lục

Thuật ngữ

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

1. GIỚI THIỆU

1.1 Thực trạng hiện nay

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

1.2 Sự phát triển của công nghệ

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

1.3 VCS-aJiant

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

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

1.4 Các thông tin nâng cấp

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

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

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

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

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

2. TỔNG QUAN

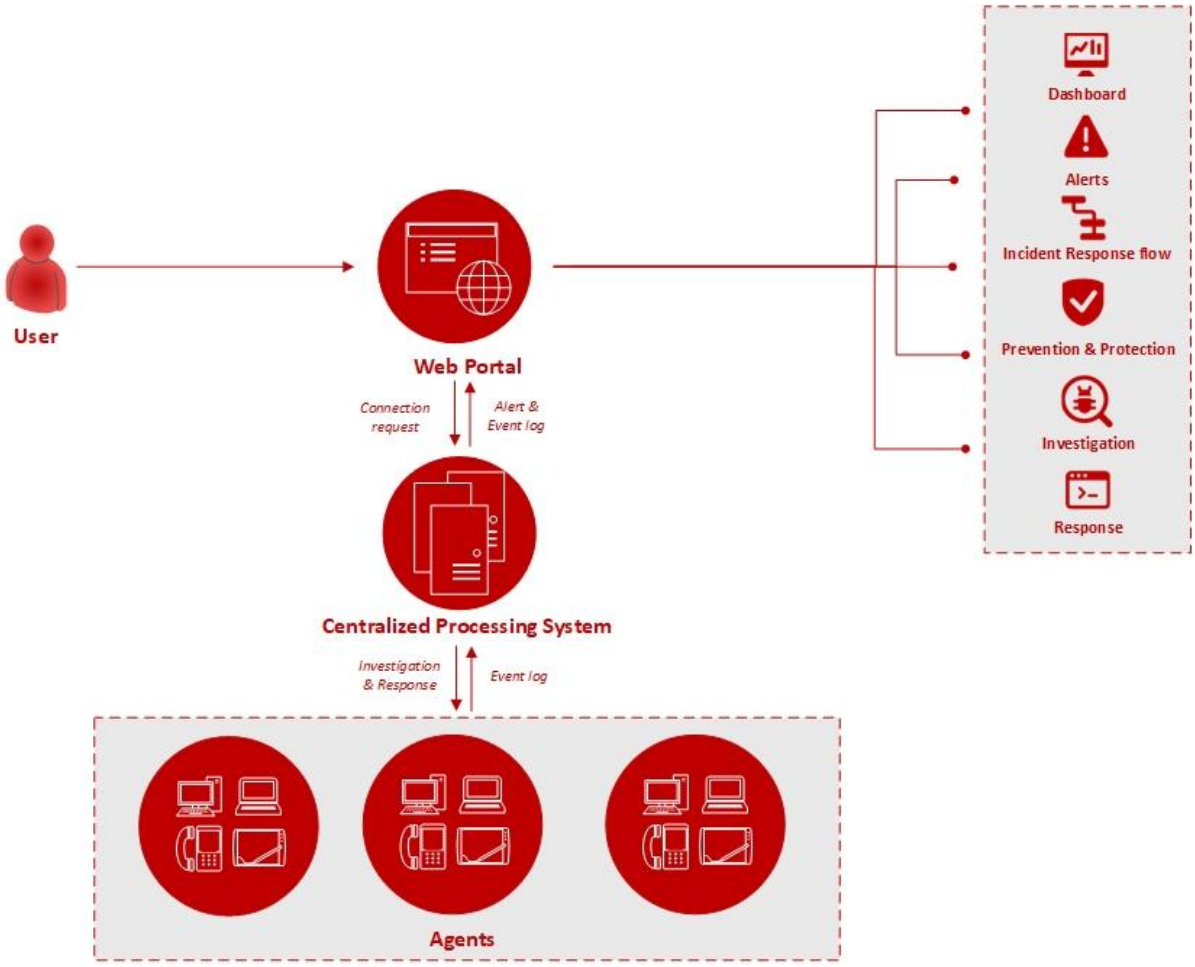
2.1 Công nghệ

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

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

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

2.2 Kiến trúc hạ tầng



Có 3 thành phần chính:

- **Agents**: Là thành phần được cài đặt trên từng máy trạm, máy chủ, có nhiệm vụ giám sát các dấu hiệu bất thường trên các máy trạm, máy chủ, gửi log về máy chủ quản trị tập trung.
- **Cụm máy chủ quản trị, xử lý tập trung và lưu trữ**: Là thành phần xử lý dữ liệu được gửi về từ các agent, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực.
- **Web-Portal:** Là thành phần mà người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích các thông tin của hệ thống.

2.3 Làm việc với giao diện quản trị

Hiện tại VCS-aJiant cung cấp 02 giao diện

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

- Dashboard: thống kê, biểu đồ trực quan về tình hình an toàn thông tin của tổ chức.
- Alert management: danh sách các alert về các dấu hiệu xuất hiện mã độc trên máy người dùng.
- IR flow management: danh sách các IR flow được tạo bởi người quản trị trong quá trình điều tra. Luồng xử lý bao gồm: Detection, Containment, Investigation, Response
- Investigation: danh sách các công cụ phục vụ điều tra (Process Analysis, Event search và Deploy tools)
- Response: danh sách các công cụ phục vụ phản ứng, xử lý sự cố (Live response)
- Protect & Prevention: danh sách các tính năng phòng chống và bảo vệ máy trạm (Application control và Endpoint firewall)
- Setting: danh sách các chức năng cài đặt hệ thống (Policy management, Agent management, Group management, Rule correlation và Account management: User, Role, Permission management)

2. Giao diện phía Agent bao gồm các giao diện chức năng và các luồng xử lý sau

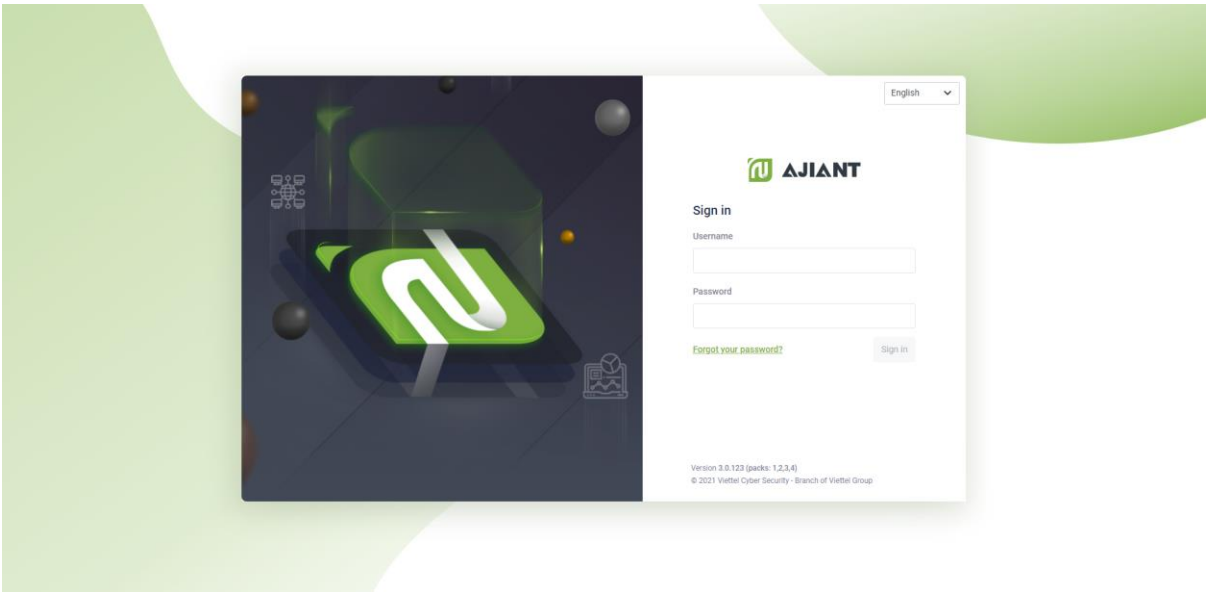
- Main: Trang chủ cho phép xem nhanh tình trạng an toàn thông tin máy cài agent
- Reports: Báo cáo tình hình xử lý mã độc phát hiện tại máy
- Scan: Cho phép người dùng chủ động quét mã độc với các file, folder trong máy gồm 03 cơ chế Quick Scan, Full Scan và Custom Scan
- About: Cung cấp thông tin phiên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

3. HƯỚNG DẪN SỬ DỤNG

GIAO DIỆN WEB-PORTAL

3.1 Đăng nhập

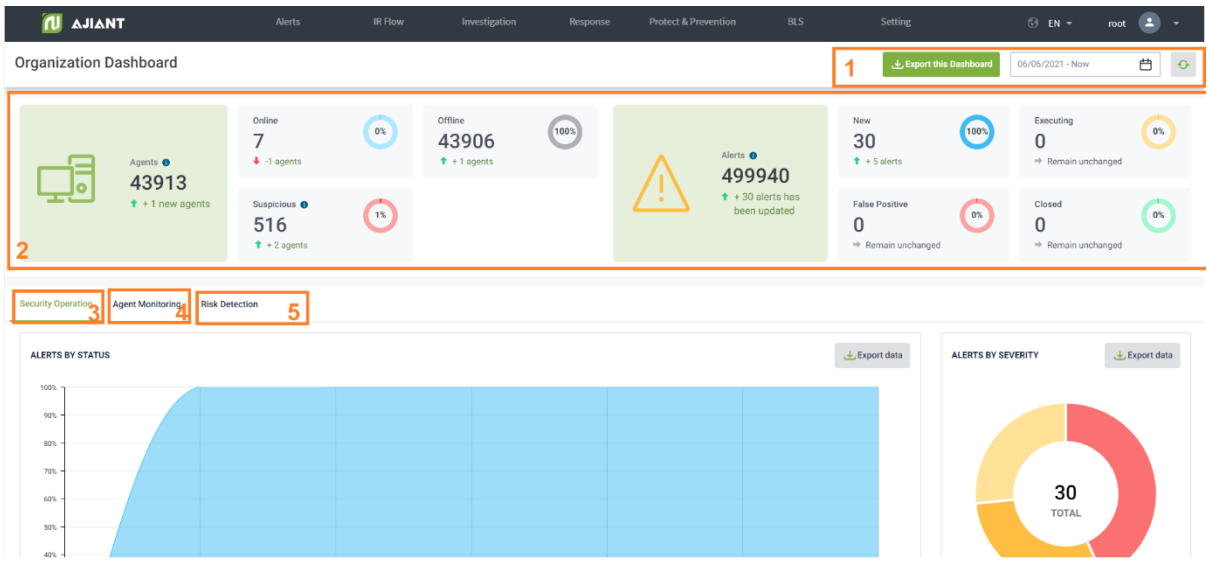
- Truy cập vào hệ thống tại địa chỉ được cung cấp



- Đăng nhập với user/pass được cấp

3.2 Dashboard VCS-aJiant (default)

- Các tính năng chính gồm có:



1 – Các thao tác với dữ liệu trên Dashboard

+ Trích xuất dữ liệu trên dashboard

+ Tìm kiếm dữ liệu tối đa 90 ngày gần đây.

+ Làm mới dữ liệu.

2 - Overview: Thống kê tổng quan tình hình an toàn thông tin tổ chức (thông qua trạng thái agents và alerts)

3 - Security Operation: Theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành alert)

4 - Agent Monitoring: Theo dõi tình hình cài đặt và trạng thái agents

5 - Risk Detection: Theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều alert chưa xử lý nhất hệ thống)

Phân quyền dữ liệu tại tính năng như sau:

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

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

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

3.2.1 Thao tác với dữ liệu

3.2.1.1 Xuất dữ liệu

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

, ngoài ra bổ sung các sheet dữ liệu chi tiết hỗ trợ báo cáo.

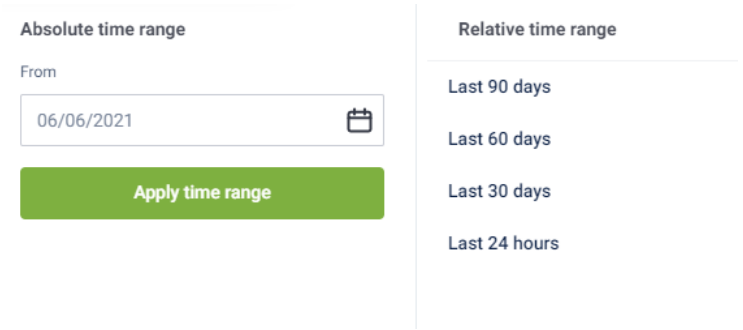
  + Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi.

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

3.2.1.2 Tìm kiếm theo ngày

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

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



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

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

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

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

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

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

+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn 

để tải lại dữ liệu tương ứng.

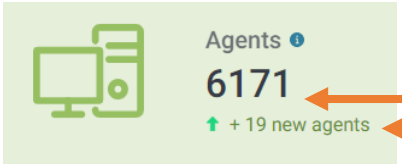
3.3.1.3 Làm mới dữ liệu

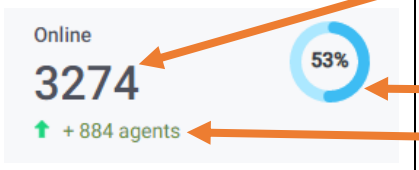
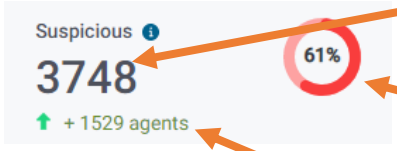
- Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.2.2 Thống kê Overview

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

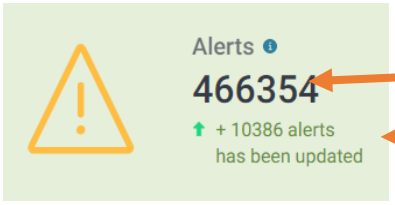
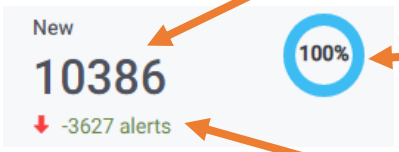
+ Thống kê liên quan đến agents

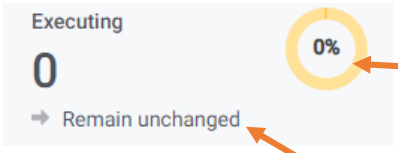
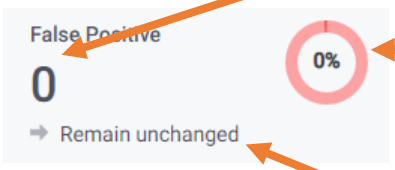
Số thống kê	Ý nghĩa
	Bao gồm 02 chỉ số Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm (+: Máy mới cài đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)

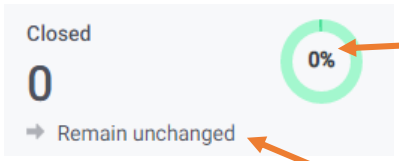
	Bao gồm 03 chỉ số Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00) Tỷ lệ máy Online trung bình so với toàn hệ thống Số lượng máy Online trung bình chênh lệch so với chu kỳ trước. (+: Số lượng máy Online trung bình tăng so với giai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

	(+: Máy mới phát sinh alert, Remain unchanged: Không có máy mới phát sinh alert trong khoảng thời gian tìm kiếm)

+ Thống kê liên quan đến alerts

Số thống kê	Ý nghĩa
	Bao gồm 02 chỉ số Tổng số alert trên toàn bộ hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm (+: Alert mới phát sinh, Remain unchanged: Không có alert mới phát sinh trong khoảng thời gian tìm kiếm)
	Bao gồm 03 chỉ số Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW Tỷ lệ alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW so với toàn bộ alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm Tổng số alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW chênh lệch so với chu kỳ trước. (+: Tổng số alert mới tăng so với giai đoạn trước, Remain unchanged: Tổng số alert mới không thay đổi so với giai đoạn trước)
	Bao gồm 03 chỉ số

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

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

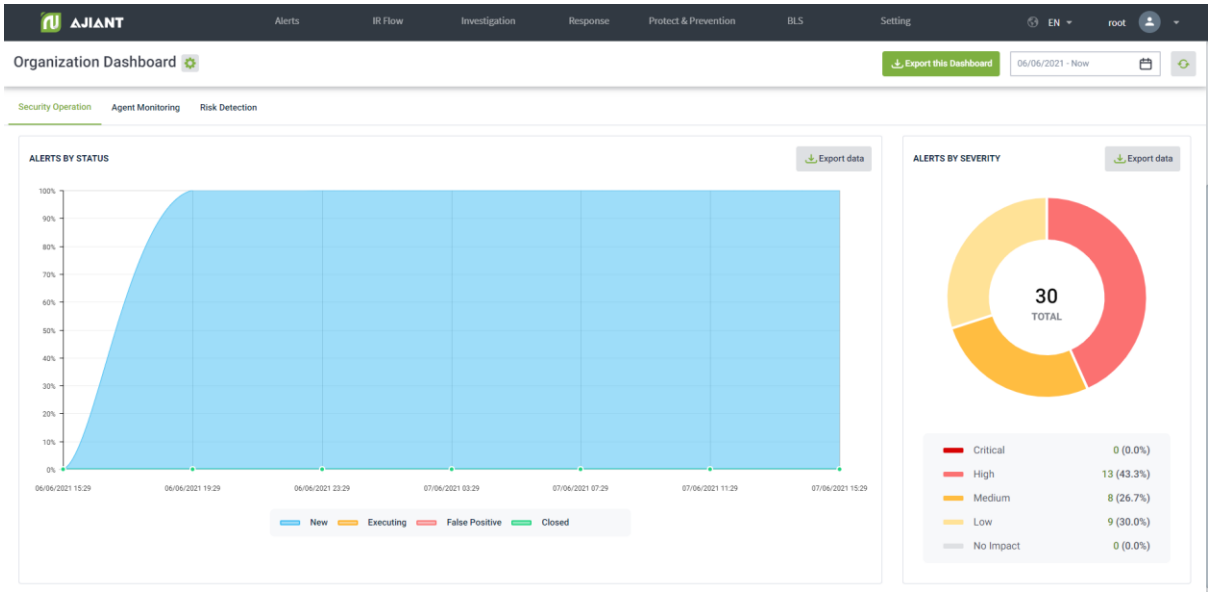
3.2.3 Theo dõi Security Operation

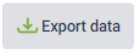
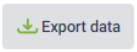
- Cho phép theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành alert) theo khoảng thời gian đã chọn trong phần tìm kiếm

  + Thống kê tình trạng xử lý alert theo trạng thái

  + Thống kê alert theo mức độ nguy hại

  + Trích xuất dữ liệu tương ứng trong các biểu đồ


AJIANT
Alerts
IR Flow
Investigation
Response
Protect & Prevention
BLS
Setting
EN
root
Organization Dashboard
Export this Dashboard
06/06/2021 - Now
Security Operation
Agent Monitoring
Risk Detection
ALERTS BY STATUS
Export data
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
06/06/2021 15:29
06/06/2021 19:29
06/06/2021 23:29
07/06/2021 03:29
07/06/2021 07:29
07/06/2021 11:29
07/06/2021 15:29
New
Executing
False Positive
Closed
ALERTS BY SEVERITY
Export data
30
TOTAL
Critical 0 (0.0%)
High 13 (43.3%)
Medium 8 (26.7%)
Low 9 (30.0%)
No Impact 0 (0.0%)

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

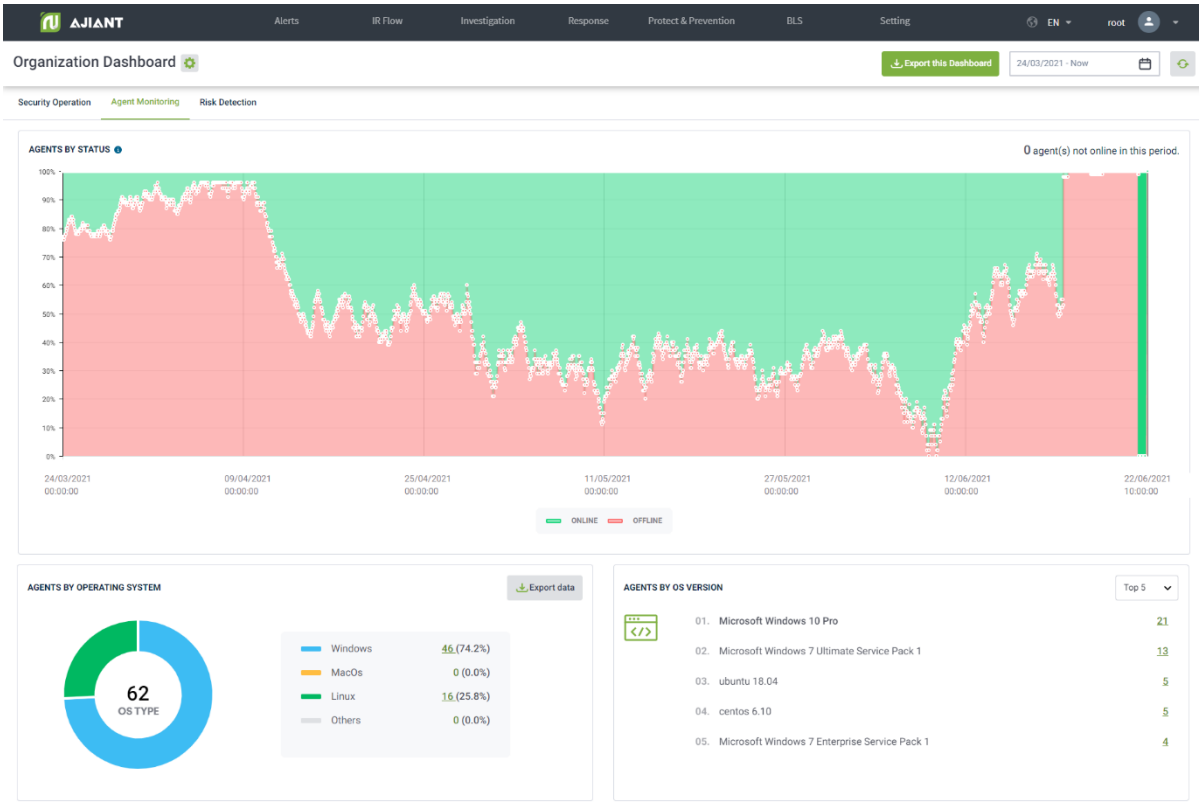
3.2.4 Theo dõi Agent Monitoring

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

  + Thống kê trạng thái agent (Trực tuyến, ngoại truyến)

  + Thống kê agent theo hệ điều hành, phiên bản hệ điều hành

  + Trích xuất dữ liệu thông tin agent



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

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

3.2.5 Theo dõi Risk Detection

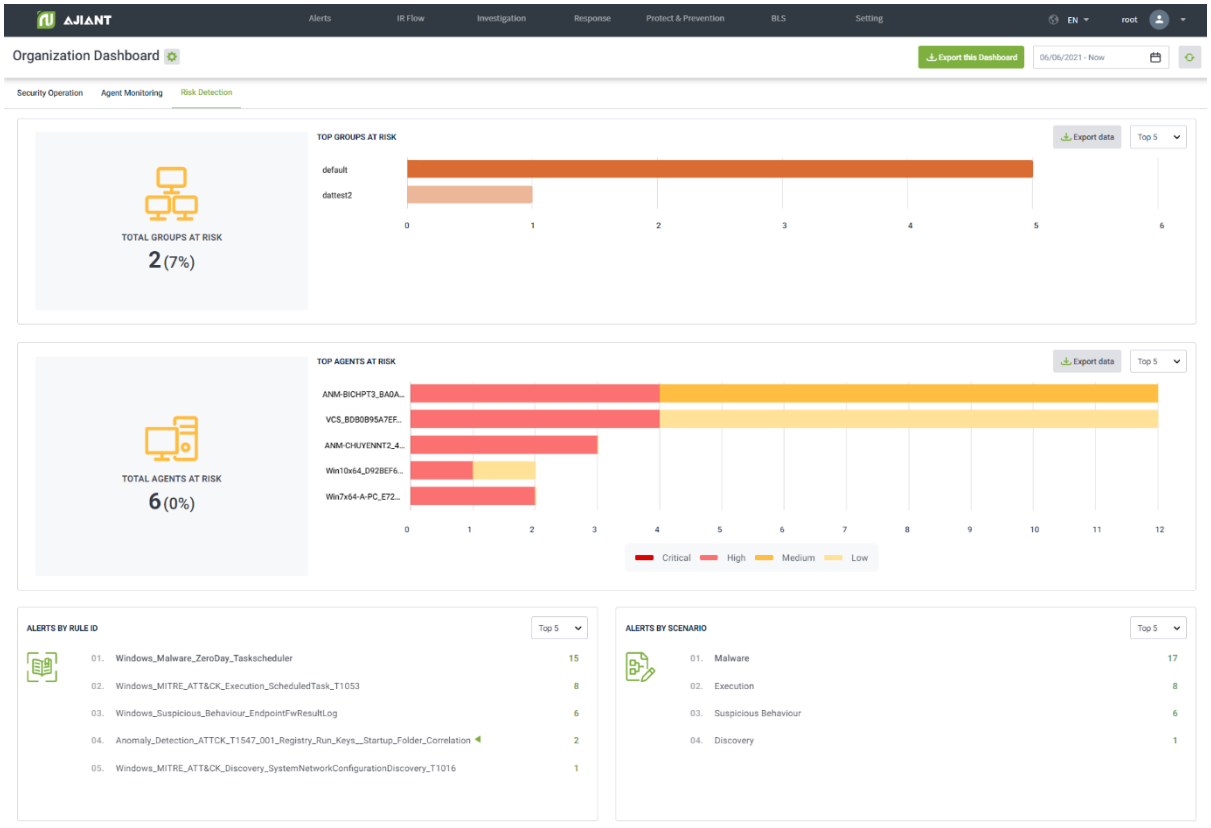
- Cho phép theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều alert chưa xử lý nhất hệ thống)

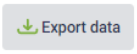
  + Thống kê top các nhóm phát sinh nhiều alert nhất

  + Thống kê top agent phát sinh nhiều alert nhất

  + Thống kê top các ruleid và scenario phát sinh nhiều cảnh bsao nhất

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

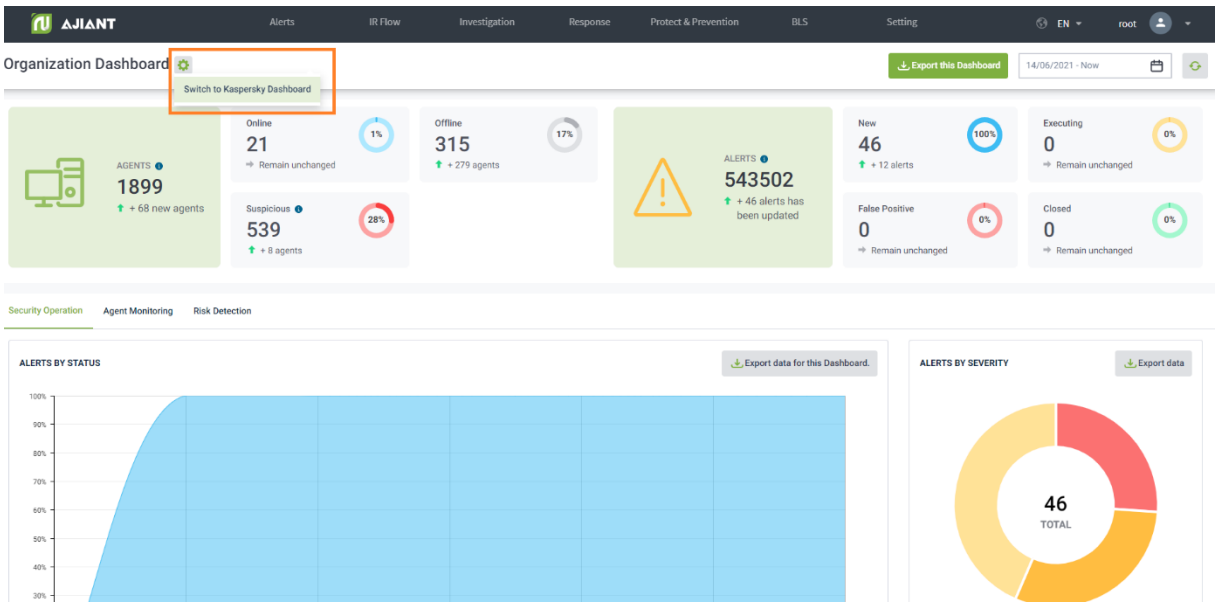


Biểu đồ/thống kê	Ý nghĩa
Total groups at risk	Tổng số nhóm có chứa máy tính phát sinh alert mới ghi nhận hoặc có cập nhật (không kể alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm. Tỷ lệ nhóm khả nghi so với toàn bộ nhóm trên hệ thống (không kể nhóm đã bị xóa)
Top groups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

	- Cho phép chọn Export data để tải về danh sách máy tính phát sinh alert
Alerts by RuleID	Thống kê top rule Id phát sinh nhiều alert mới ghi nhận hoặc có cập nhật nhất trong thời gian tìm kiếm - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 15, Top 20. Mặc định chọn Top 5
Alerts by scenarios	Thống kê top Scenario phát sinh nhiều alert mới ghi nhận hoặc có cập nhật nhất trong chu kỳ báo cáo tính đến thời điểm hiện tại: - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 15, Top 20. Mặc định chọn Top 5

3.3 Dashboard Kaspersky (optional)

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



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

- Các tính năng chính gồm có:

1 – Các thao tác với dữ liệu trên Dashboard

+ Trích xuất dữ liệu trên dashboard

+ Tìm kiếm dữ liệu tối đa 90 ngày gần đây.

Làm mới dữ liệu.

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

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

Phân quyền dữ liệu tại tính năng như sau:

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

3.3.1 Thao tác với dữ liệu

3.3.1.1 Xuất dữ liệu

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

, ngoài ra bổ sung các sheet dữ liệu chi tiết hỗ trợ báo cáo.

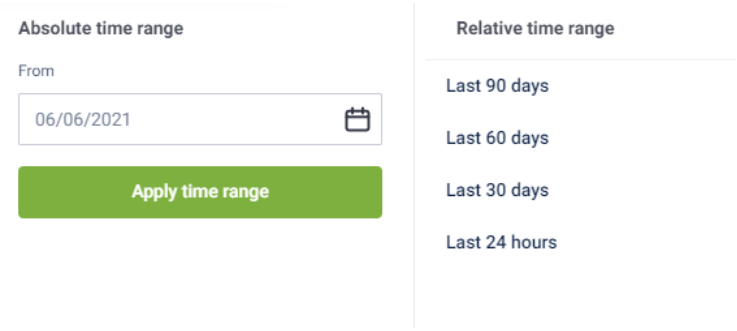
  + Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi.

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

3.3.1.2 Tìm kiếm theo ngày

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

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



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

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

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

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

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

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

+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn 

để tải lại dữ liệu tương ứng.

3.3.1.3 Làm mới dữ liệu

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

3.3.2 Thống kê Overview

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

+ Thống kê liên quan đến agents

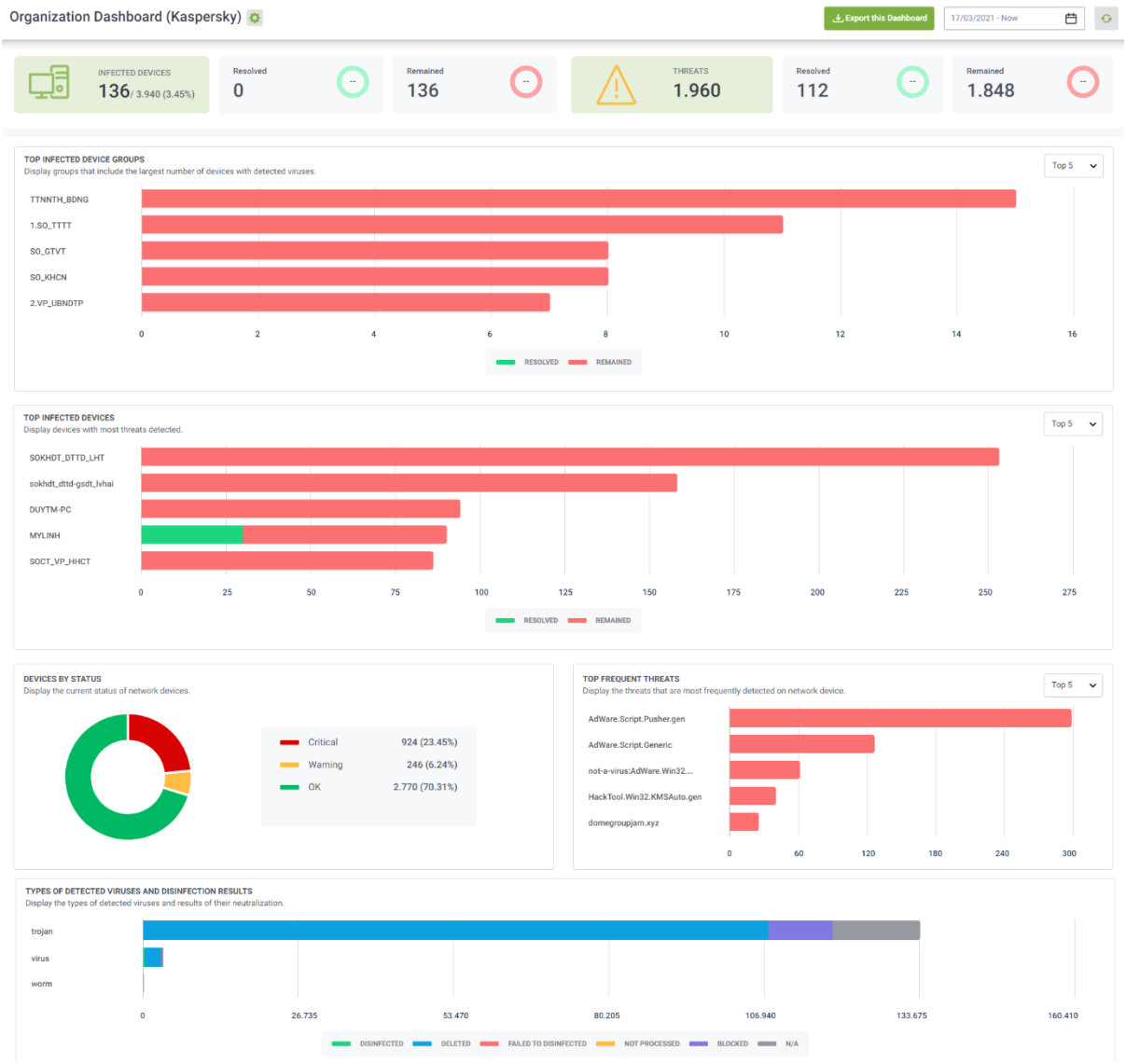
Số thống kê	Ý nghĩa
	Bao gồm 03 chỉ số Tổng số máy bị lây nhiễm trên hệ thống trong khoảng thời gian tìm kiếm Tổng số máy cài đặt agent trong hệ thống (***không kể thời gian tìm kiếm***) Tỷ lệ máy bị lây nhiễm so với toàn bộ máy cài đặt agent trong hệ thống
	Bao gồm 02 chỉ số Tổng số máy bị lây nhiễm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

+ Thống kê liên quan đến alerts

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

3.3.3 Theo dõi Risk Detection

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

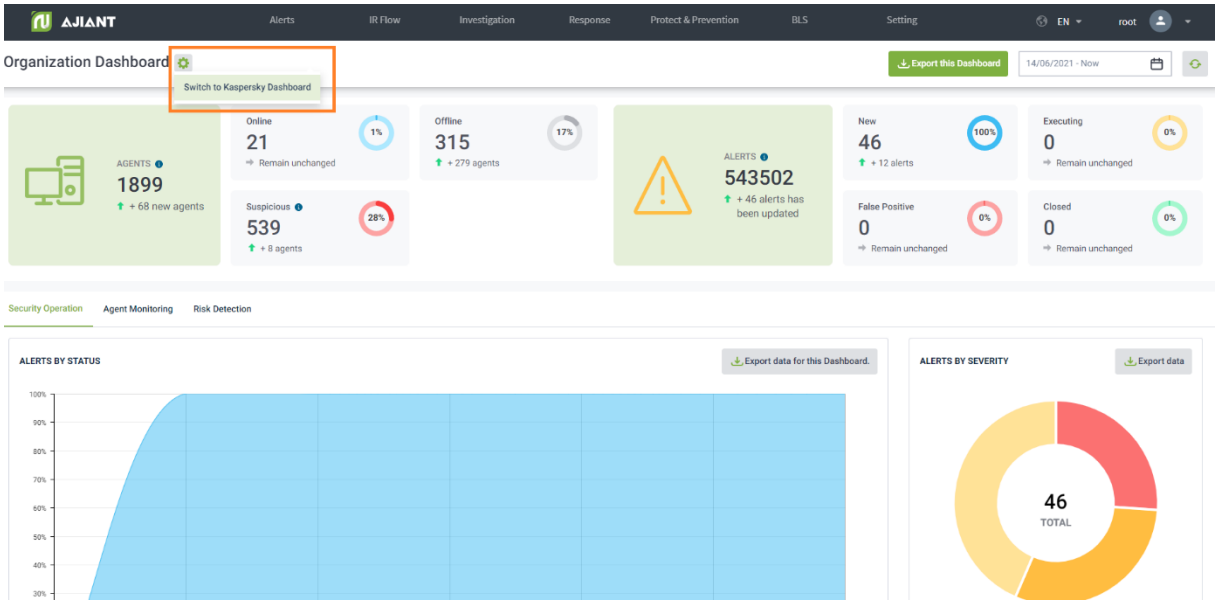


Biểu đồ/thống kê	Ý nghĩa
Top infected device groups	Biểu đồ cột liệt kê nhóm máy có nhiều máy lây nhiễm mã độc nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng máy lây nhiễm mã độc tại từng nhóm theo trạng thái xử lý (Resolved - máy có toàn bộ mã độc đã xử lý và Remain -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

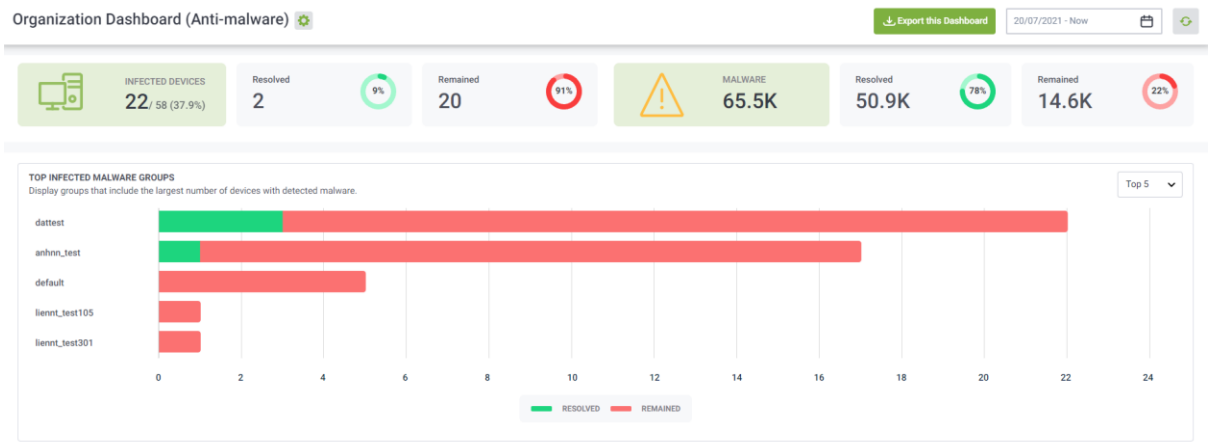
	- Trục y: Tên nhóm máy tương ứng - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5
Top infected devices	Biểu đồ cột liệt kê máy bị lây nhiễm mã độc nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc lây nhiễm theo trạng thái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

3.3 Dashboard Anti-malware (optional)

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



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



- Các tính năng chính gồm có:

1 – Các thao tác với dữ liệu trên Dashboard

+ Trích xuất dữ liệu trên dashboard

+ Tìm kiếm dữ liệu tối đa 90 ngày gần đây.

Làm mới dữ liệu.

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

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

Phân quyền dữ liệu tại tính năng như sau:

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

3.3.1 Thao tác với dữ liệu

3.3.1.1 Xuất dữ liệu

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

, ngoài ra bổ sung các sheet dữ liệu chi tiết hỗ trợ báo cáo.

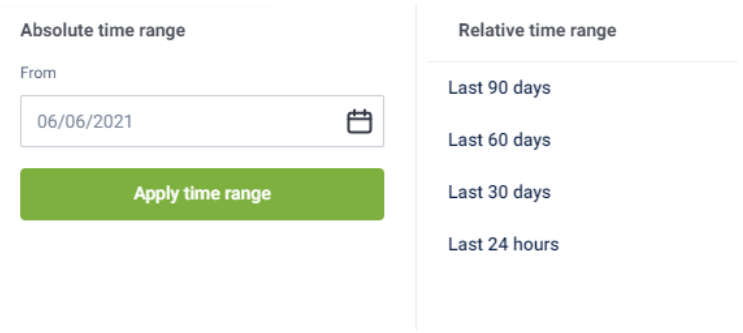
  + Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi.

  + 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:



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

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

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

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

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

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

+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn 

để tải lại dữ liệu tương ứng.

3.3.1.3 Làm mới dữ liệu

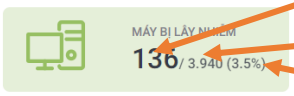
- Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.3.2 Thống kê Overview

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

+ Thống kê liên quan đến agents

Số thống kê	Ý nghĩa

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

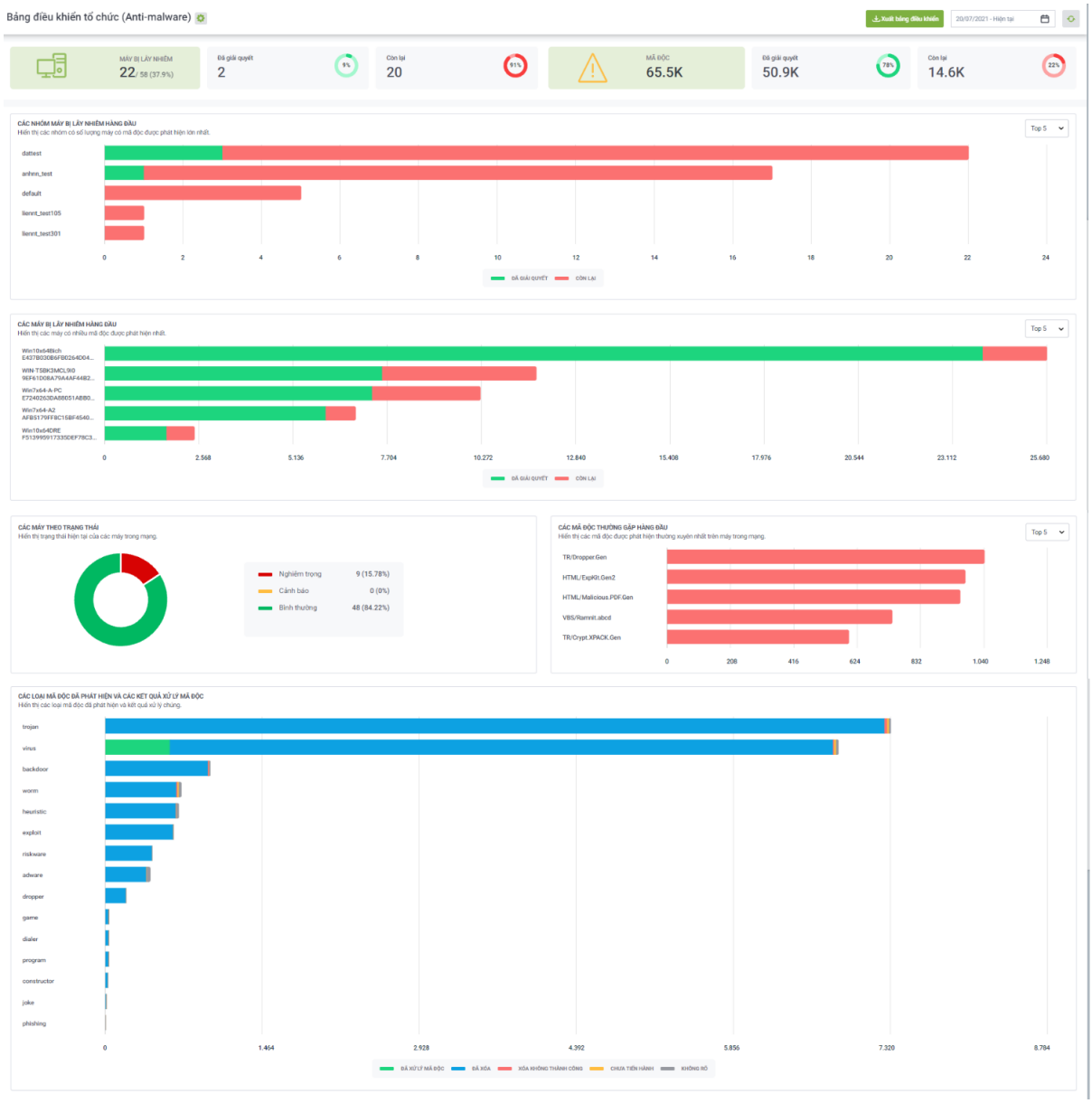
+ Thống kê liên quan đến alerts

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

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

3.3.3 Theo dõi Risk Detection

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

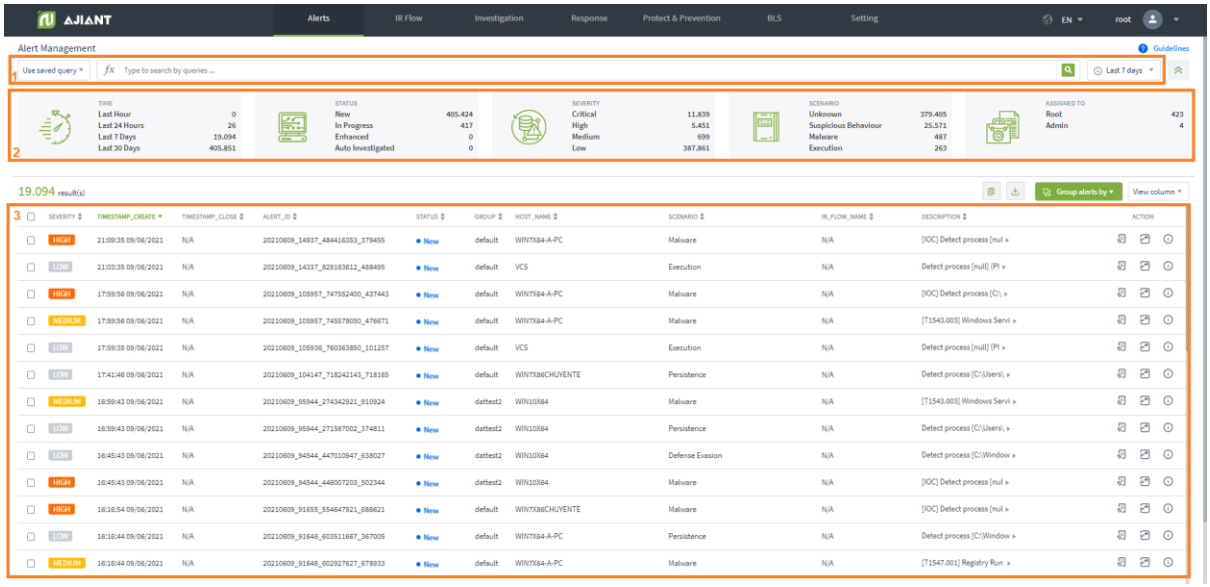


Biểu đồ/thống kê	Ý nghĩa
Top infected device groups	Biểu đồ cột liệt kê nhóm máy có nhiều máy lây nhiễm mã độc nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng máy lây nhiễm mã độc tại từng nhóm theo trạng thái xử lý (Resolved - máy có toàn bộ mã độc đã xử lý và Remain -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

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

3.4 Quản lý alert

- Các tính năng chính gồm có:



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

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

+ Tìm kiếm dữ liệu theo thời gian

2 – Tìm kiếm nhanh

3 - Danh sách alert và các thao tác với alert

+ Xem danh sách alert

+ Gom nhóm alert

+ Xem tóm tắt alert

+ Xem chi tiết 01 alert

+ Xem biểu đồ điều tra (Investigation Graph)

+ Đánh dấu không nguy hiểm (Set False Positive) cho 01/nhiều alert

+ Tạo IR flow từ 01/nhiều alert

+ Thêm 01/nhiều alert vào IR flow

- Phân quyền dữ liệu tại tính năng như sau:

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

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

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

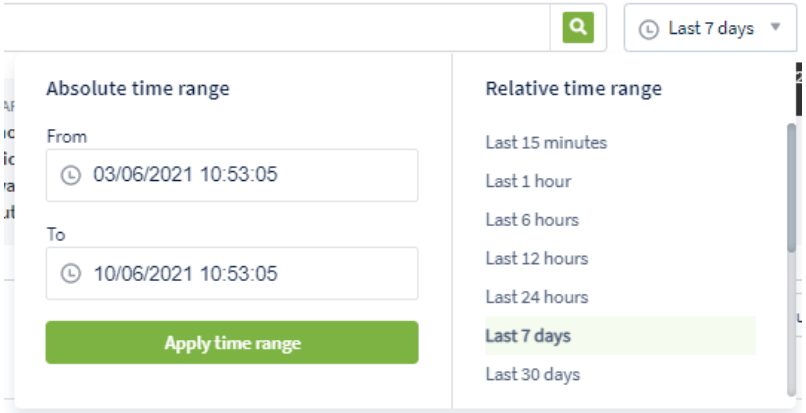
+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả alert thuộc group của user đang login

3.4.1 Tìm kiếm alert

- Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn đã lưu hoặc tìm kiếm nhanh để tìm kiếm alert theo thời gian phát sinh alert.

3.4.1.1 Tìm kiếm theo thời gian

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



- Cho phép thay đổi giá trị thời gian bằng cách chọn thời gian tuyệt đối hoặc thời gian tương đối

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

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

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

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

3.4.1.2 Tìm kiếm nhanh

- Hỗ trợ tìm kiếm alert nhanh theo các trường:

  + Time: thời gian phát sinh alert

  + Status: trạng thái của alert

  + Severity: mức độ nguy hại của alert

  + Scenario: kịch bản sinh ra alert

+ Assigned to: người được phân công xử lý alert

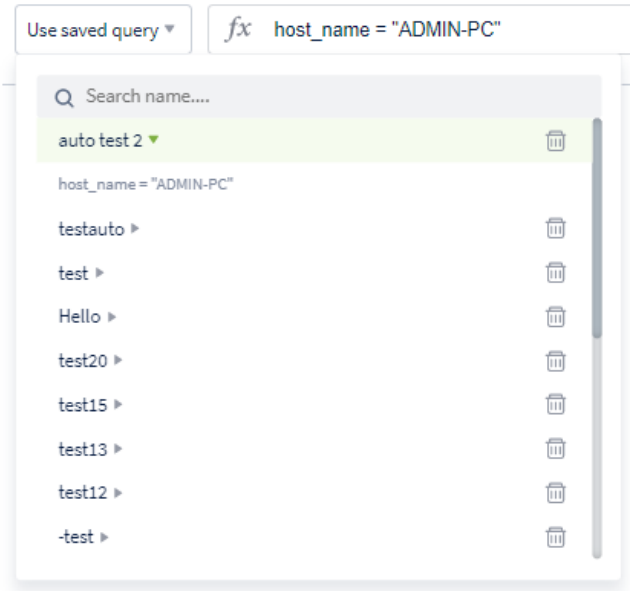
3.4.1.3 Tìm kiếm theo câu query

1 – Sử dụng câu query đã lưu trước đó để tìm kiếm

2 – Nhập câu query để tìm kiếm

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

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



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

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

(*) Nhập câu query để tìm kiếm

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

<tên_trường> <toán tử> “<value>” AND/OR <tên_trường> <toán tử> “<value>”…..

Trong đó:

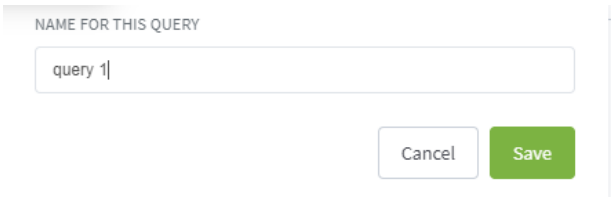
- <tên_ trường> là các giá trị sau:
  - severity: độ nghiêm trọng của alert
  - alert_id: mã alert
  - status: trạng thái của alert
  - group: nhóm của sự kiện sinh alert
  - hostname: Tên của máy trạm
  - scenario: kịch bản sinh ra alert dựa theo MITRE ATT&CK
  - ir_flow_name: tên IR flow mà alert thuộc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

- Bước 2: Click on Search.

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

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

- Bước 3: Trường hợp câu query đúng cấu trúc và muốn lưu lại để sử dụng cho các lần tiếp theo, chọn Save query và nhập tên gợi nhớ cho query:

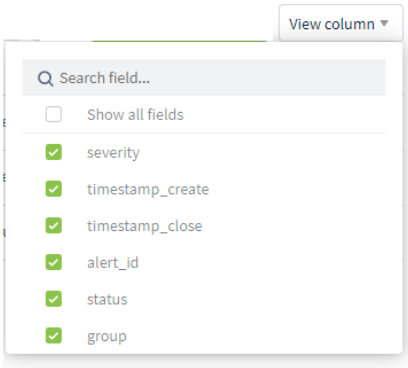


Lưu ý: nút Save query chỉ hiển thị khi câu lệnh query đúng cấu trúc.

3.4.2 Danh sách alert

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

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



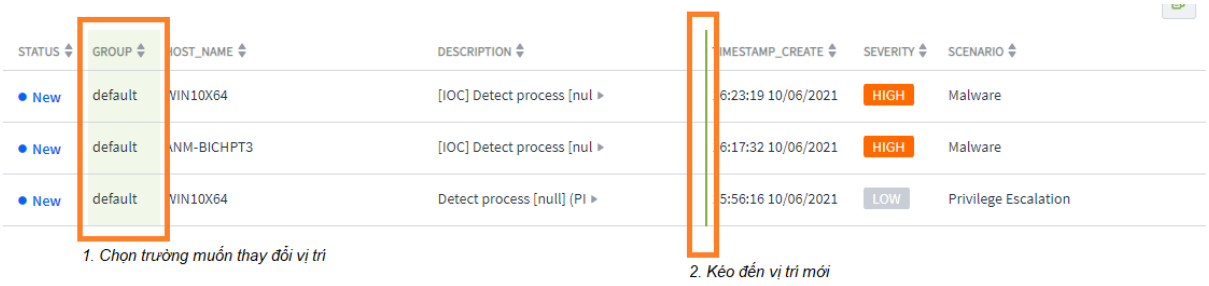
Tại đây có thể tìm kiếm trường thông tin theo tên trường, hỗ trợ chọn/bỏ chọn tất cả các trường.

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

+ Sắp xếp theo dữ liệu tại từng cột

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

+ Kéo thả trường thông tin đến vị trí mong muốn



1. Chọn trường muốn thay đổi vị trí

2. Kéo đến vị trí mới

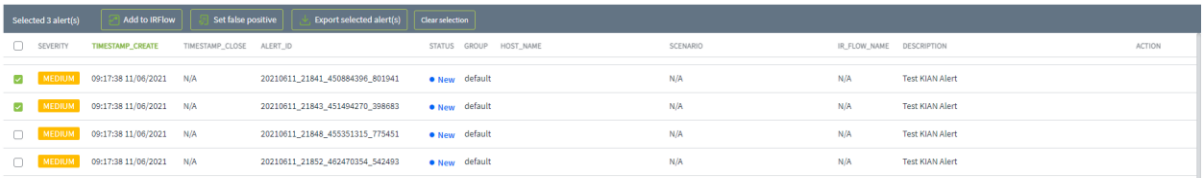
+ Click 01 lần để xem thông tin tóm tắt, chi tiết xem trong 3.3.4 Xem tóm tắt alert
+ Click 02 lần hoặc chọn ⓘ để xem thông tin chi tiết, chi tiết xem trong 3.3.4 Xem chi tiết alert

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

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

+ Chọn để xem lý do đánh dấu không nguy hiểm tại các alert đang ở trạng thái "FALSE POSITIVE"

- Bước 3: Sau khi đã thao tác trên các bản ghi xong, cho phép chọn 01 hoặc nhiều bản ghi bằng cách click chọn tại đầu mỗi alert để tiếp tục thao tác, hỗ trợ các thao tác sau



+ Chọn Add to IRFlow để thêm alert vừa chọn vào IR flow để xử lý.

Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ alert được chọn đều ở trạng thái = "NEW", nếu có ít nhất một alert đang ở trạng thái khác "NEW", thao tác sẽ bị ẩn đi Add to IRFlow. Chi tiết xem trong trường hợp đưa 01 alert vào IR flow mới trong 3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert hoặc thêm vào IR flow đã tồn tại trong 3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR fLow đã có

+ Chọn Set false positive để đánh dấu không nguy hiểm cho alert.

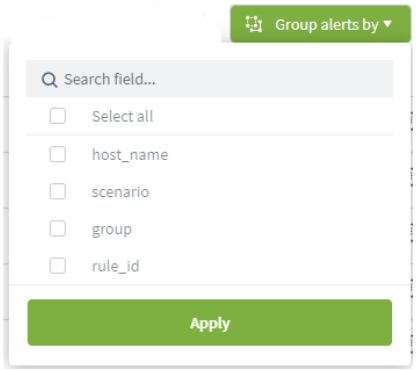
Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ alert được chọn đều ở trạng thái = "NEW", nếu có ít nhất một alert đang ở trạng thái khác "NEW", thao tác sẽ bị ẩn đi Set false positive. Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 alert trong 3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert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

+ Chọn Export selected alert(s) để trích xuất các alert đang được chọn.

3.4.3 Gom nhóm alert

- Cho phép gom nhóm các alert theo 01 hoặc nhiều tiêu chí: hostname, scenario, group, ruleid

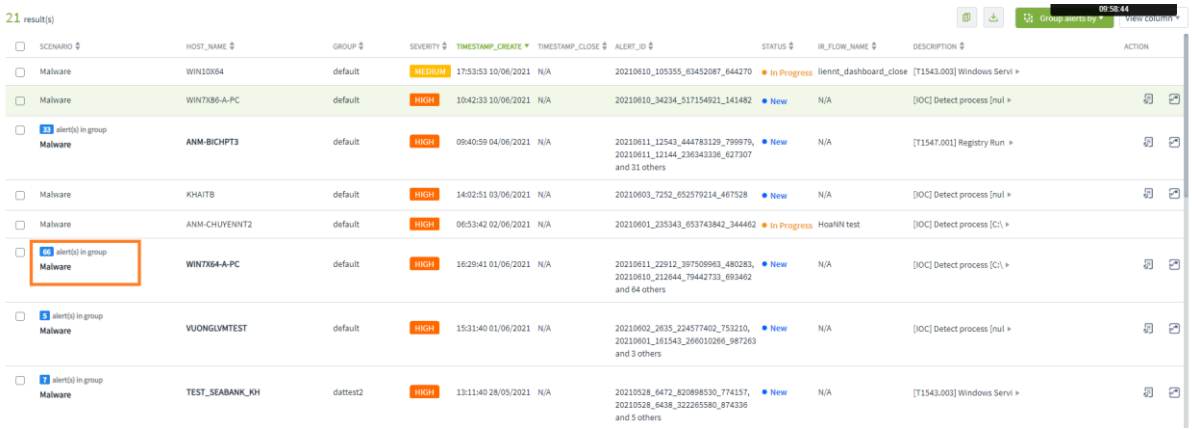
- Bước 1: Sau khi tìm kiếm có thể gom nhóm alert lại, chọn Group alerts by để lựa chọn các tiêu chí muốn sử dụng làm tiêu chí gom nhóm alert.



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

- Bước 2: Chọn  để áp dụng.

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

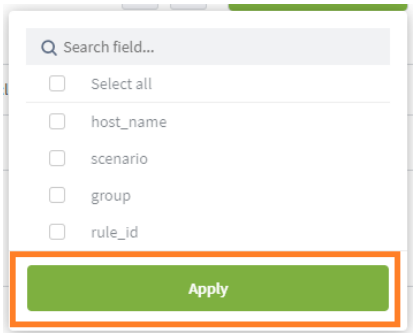


- Trong đó:

  + Các trường được sử dụng làm tiêu chí gom nhóm sẽ được bôi đậm

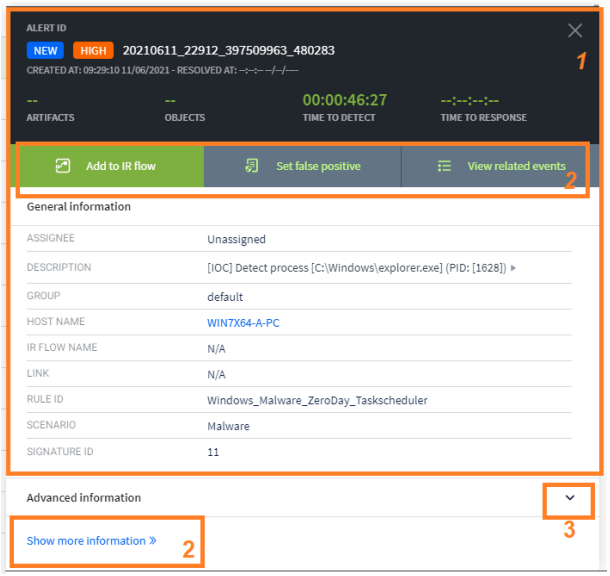
  + Hiển thị số lượng các alert được gom nhóm tại tiêu chí đã chọn

- Bước 3: Để bỏ gom nhóm, thực hiện tương tự nhưng không chọn tiêu chí nào và chọn Apply



3.4.4 Xem tóm tắt alert

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



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

+ Artifacts: Danh sách các đối tượng khả nghi được đánh dấu tự động/thủ công trong alert

+ Objects: Danh sách các đối tượng trong alert

+ Time to detect: Tổng thời gian phát hiện và điều tra alert, tình từ khi alert sinh ra đến khi được đưa vào IR flow hoặc đánh dấu “FALSE POSITIVE”

+ Time to response: Tổng thời gian xử lý alert, tình từ khi alert được được vào IR flow đến khi đóng IR flow

2 – Nhóm các thao tác với alert

+ Chọn 

để đưa alert vào IR flow, xem trường hợp đưa 01 alert vào IR flow đã tồn tại trong 3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR fLow đã có hoặc vào IR flow mới trong 3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert

+ Chọn 

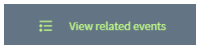
để đánh dấu không nguy hiểm cho alert, xem trường hợp đánh dấu 01 alert trong 3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert

+ Chọn 

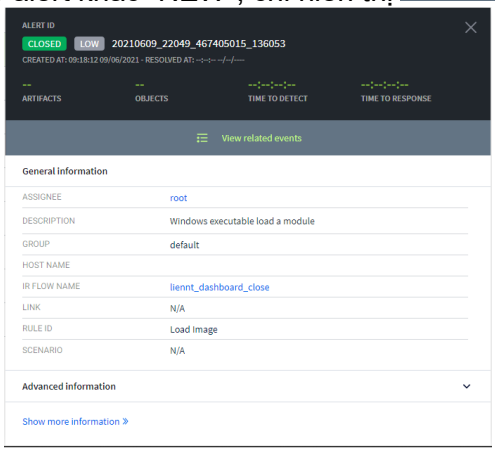
để chuyển đến tính năng Event Search với thời gian mặc định là 04 tiếng trước và sau thời gian phát sinh alert

Lưu ý: Chỉ hiển thị thao tác 

và 

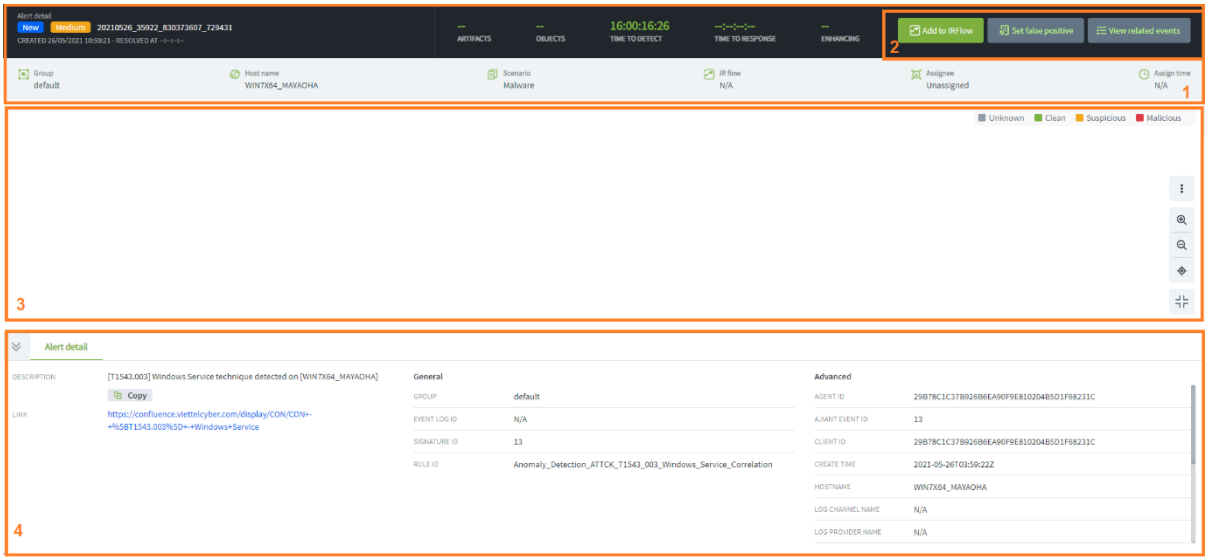
đối với alert đang ở trạng thái "NEW", trường hợp alert khác "NEW", chỉ hiển thị 

như sau:



3.4.5 Xem chi tiết alert

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



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

+ Artifacts: Danh sách các đối tượng khả nghi được đánh dấu tự động/thủ công trong alert

+ Objects: Danh sách các đối tượng trong alert

+ Time to detect: Tổng thời gian phát hiện và điều tra alert, tình từ khi alert sinh ra đến khi được đưa vào IR flow hoặc đánh dấu "FALSE POSITIVE"

+ Time to response: Tổng thời gian xử lý alert, tình từ khi alert được được vào IR flow đến khi đóng IR flow

+ Enhancing: Tỷ lệ hoàn thành quá trình tự động làm giàu thông tin của hệ thống

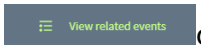
2 – Nhóm các thao tác với alert

+ Chọn 

để đưa alert vào IR flow, xem trường hợp đưa 01 alert vào IR flow đã tồn tại trong 3.3.7 Thêm 01/nhiều alert hoặc nhóm alert vào IR fLow đã có hoặc vào IR flow mới trong 3.3.6 Tạo IR flow từ 01/nhiều alert hoặc nhóm alert

+ Chọn 

để đánh dấu không nguy hiểm cho alert, xem trường hợp đánh dấu 01 alert trong 3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert

+ Chọn 

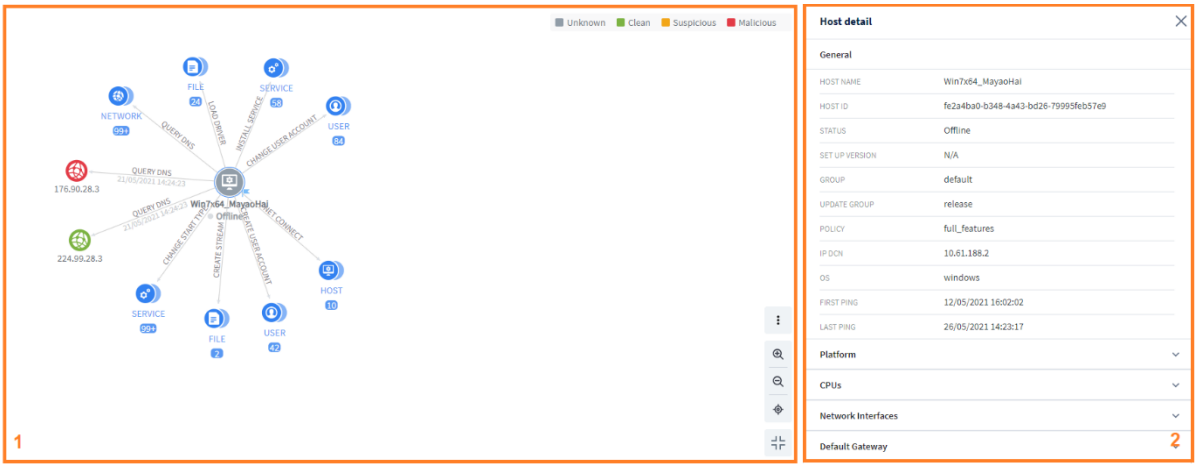
để chuyển đến tính năng Event Search với thời gian mặc định là 04 tiếng trước và sau thời gian phát sinh alert

3 – Biểu đồ điều tra (Investigaton Graph): Chi tiết xem trong 3.3.5 Biểu đồ điều tra (Investigation Graph)

4 – Tab các thông tin liên quan đến alert: Hiện tại chỉ hỗ trợ Alert Detail

3.4.6 Biểu đồ điều tra (Investigation Graph)

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

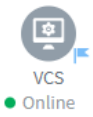


1 – Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ

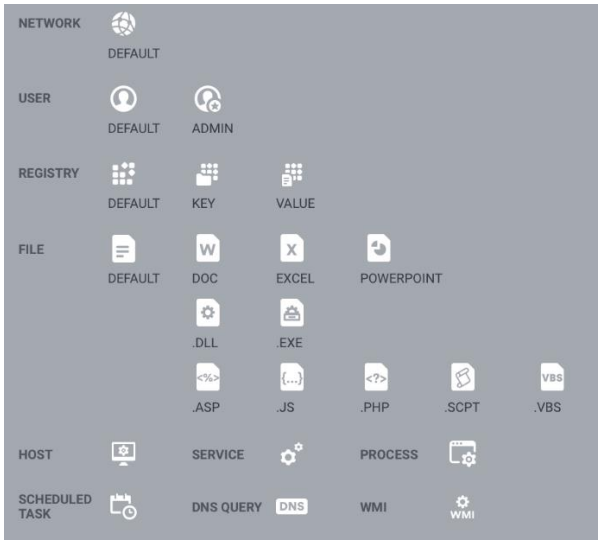
2 – Khu vực hiển thị thông tin chi tiết các đối đượng trên biểu đồ

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

- Cho phép hiển thị trực quan các đối tượng trong alert phục vụ xem thông tin và điều tra.
- Mặc định khi vừa truy cập, biểu đồ hiển thị thông tin liên quan đến máy gốc phát sinh alert, cụ thể như sau:



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



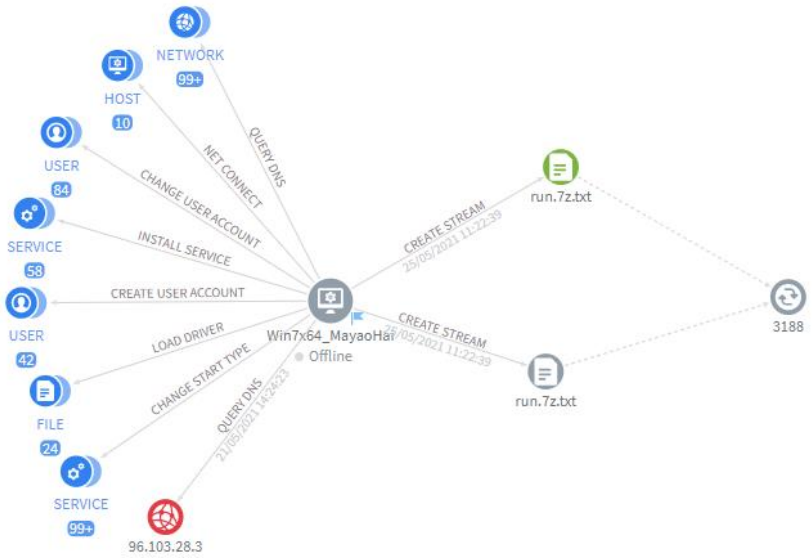
- Mỗi đối tượng bao gồm các trạng thái như sau: 

- Giữa các đối tượng, hiển thị mối quan hệ bao gồm:

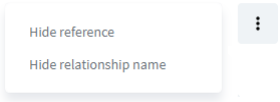
  + Relationship: Mối quan hệ định nghĩa theo các sự kiện phát sinh trong vòng 01 ngày từ thời điểm phát sinh alert (trong đó tên mối quan hệ nằm phía trên mũi tên nối liên 02 đối tượng)

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

+ Ví dụ:



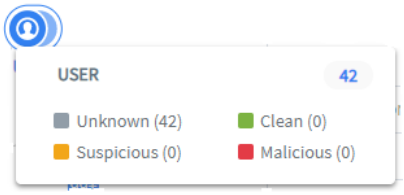
- Các thao tác hỗ trợ hiển thị biểu đồ bao gồm:

Thao tác hỗ trợ hiển thị	Ý nghĩa
	Cho phép ẩn/hiện các thông tin trên biểu đồ: + Reference: Khi chọn, cho phép ẩn/hiện thông tin tham chiếu bao gồm mũi tên nét đứt và đối tượng tham chiếu tại tất cả các đối tượng hiện có trên biểu đồ + Relationship name: Khi chọn, cho phép ẩn/hiện thông tin tên mối quan hệ phía trên tất cả các mũi tên nét liền hiện có trên biểu đồ
	Cho phép zoom in/zoom out biểu đồ tương ứng tại vị trí đang trỏ chuột Ngoài ra có thể lăn chuột tại vị trí muốn zoom in/out để thao tác nhanh
	Cho phép quay lại vị trí trung tâm của biểu đồ (máy gốc)
	Cho phép mở rộng màn hình tối đa để xem biểu đồ và thao tác trên biểu đồ

- Ví dụ một biểu đồ mặc định như sau:

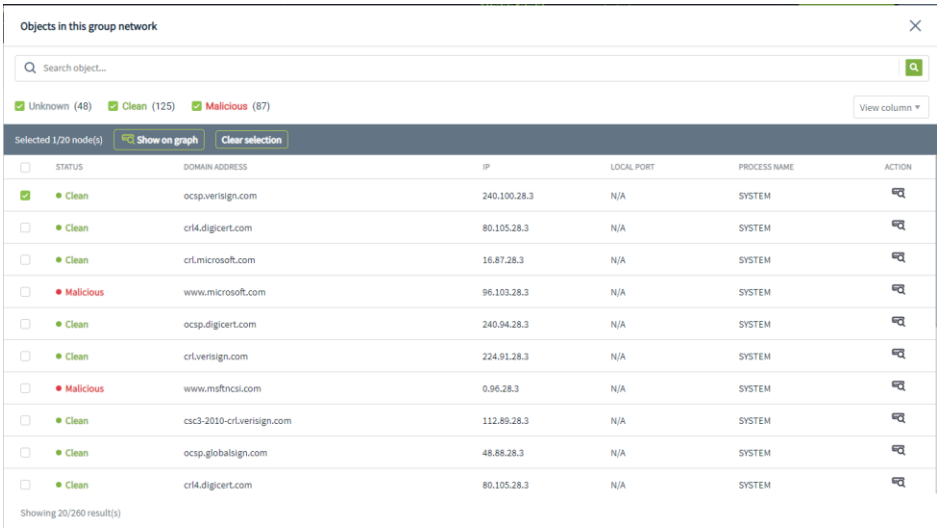
Trường hợp tại mỗi loại đối tượng có nhiều hơn 01 đối tượng trực thuộc, các đối tượng sẽ được tự động nhóm lại.

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



Từ đây, muốn điều tra loang tiếp các đối tượng thực hiện các bước như sau:

- Bước 1: Click chọn nhóm đối tượng muốn xem, hiển thị giao diện như sau:



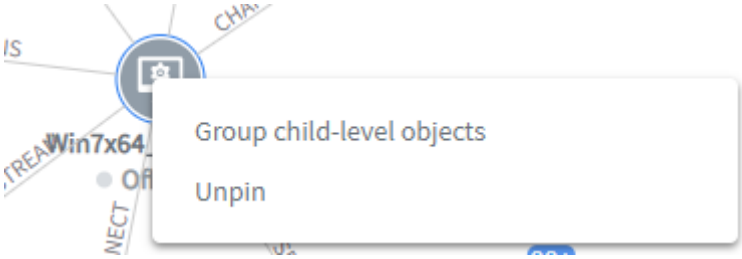
+ Cho phép lọc các đối tượng trong nhóm theo trạng thái Unknown Clean Suspicious Malicious hoặc tìm kiếm nhanh bằng cách nhập nhập dữ liệu muốn tìm kiếm trong tất cả các trường

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

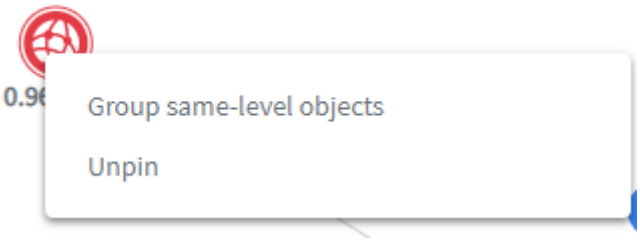
Lưu ý: Nếu đối tượng được mở rộng là một máy tính, mặc định khi hiển thị đối tượng, cũng tự động hiển thị các đối tượng các quan hệ trực tiếp đến máy tính trong vòng 01 ngày kể từ thời điểm phát sinh alert

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

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

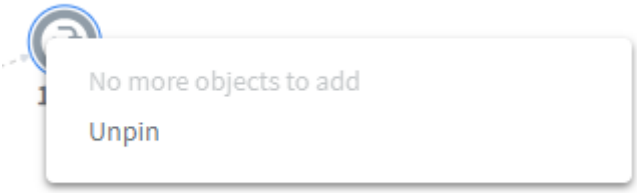


+ Tại các đối tượng khác: Hỗ trợ thu gọn bằng cách nhóm lại theo loại đối tượng và loại quan hệ với các đối tượng cùng cấp bằng cách chọn chuột phải tại đối tượng, sau đó chọn “Group same-level objects”

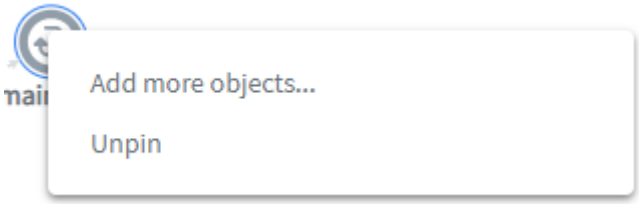


+ Tại đối tượng là tiến trình (process) cho phép mở rộng để điều tra loang bằng cách chọn chuột phải tại đối tượng,

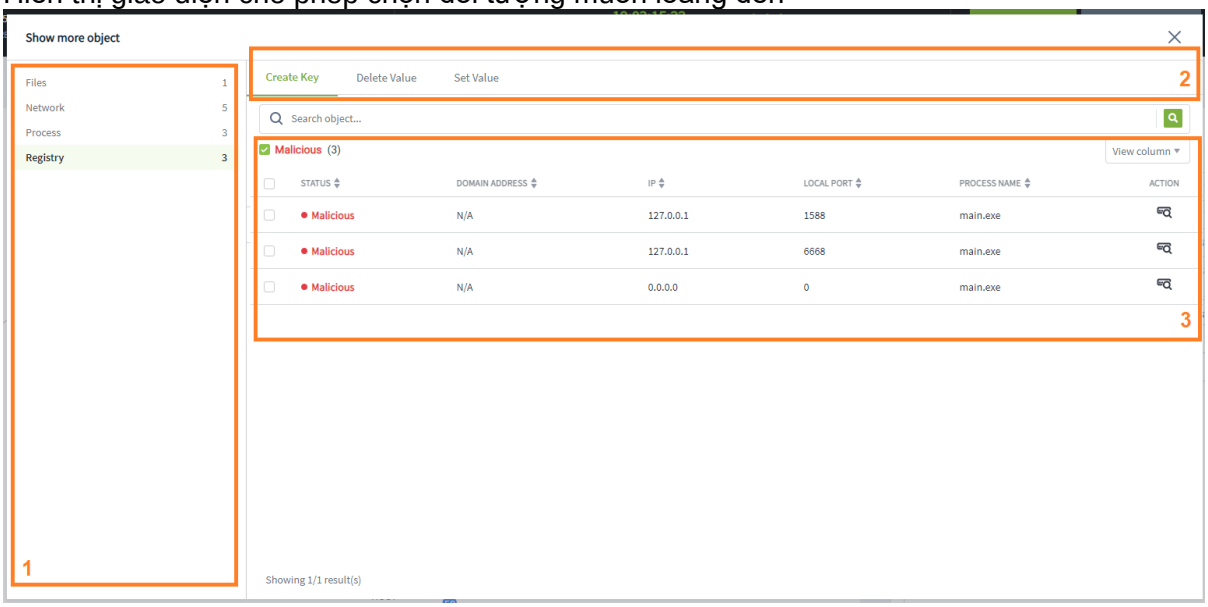
Trường hợp không thể tiếp tục loang, hiển thị:



Trường hợp có thể loang, chọn “Add more objects…”



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



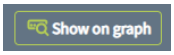
1 – Chọn loại đối tượng

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

3 – Chọn trực tiếp đối tượng muốn hiển thị. Hỗ trợ tìm kiếm theo trạng thái độc/sạch của đối tượng hoặc tìm kiếm theo nội dung có tại các trường thông tin của đối tượng.

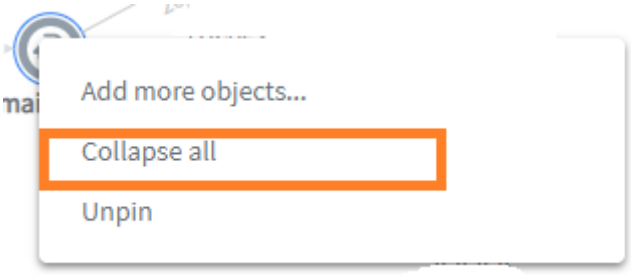
Chọn

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

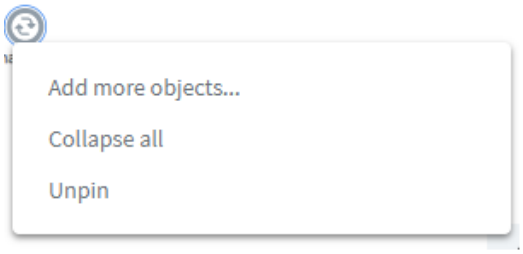
Khi đã chọn được đối tượng phù hợp, chọn  để hiển thị 01 đối tượng lên biểu đồ hoặc chọn 

để chọn tối đa 20 đối tượng lên biểu đồ

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

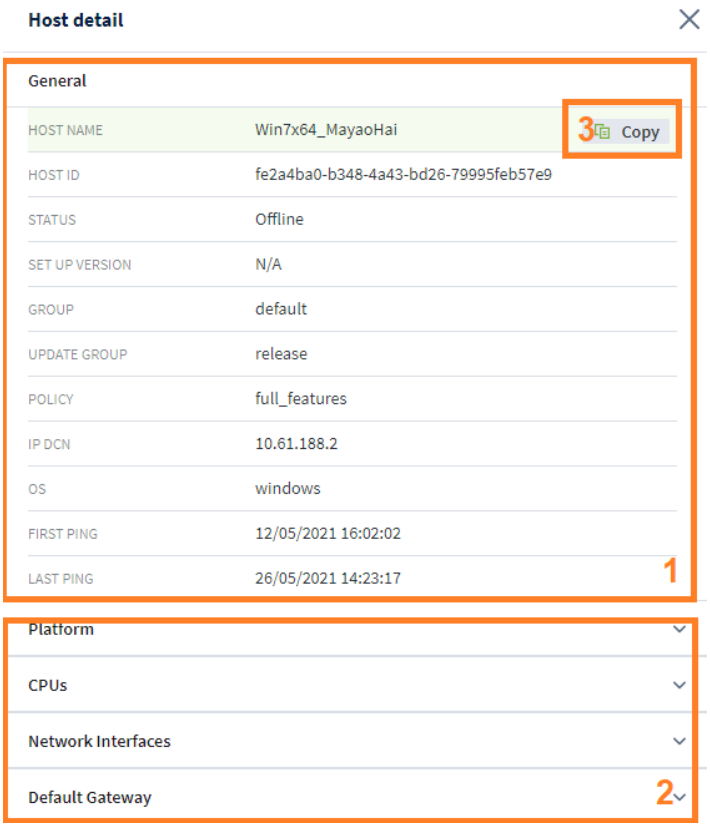


+ Mặc định tại biểu đồ, các đối tượng tự động chạy và giữ khoảng cách với nhau khi bị di chuyển. Trường hợp dùng chuột chọn và kéo thả các đối tượng, sau khi bỏ chuột đối tượng tự động được Pin vào vị trí mới. Để hủy thao tác Pin, chọn Unpin



3.4.6.2 Khu vực hiển thị thông tin chi tiết

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

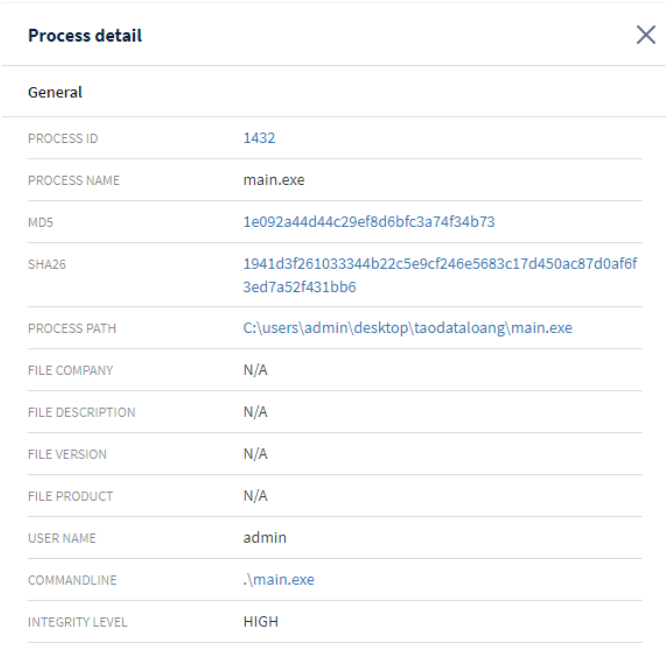


1 - Nhóm thông tin chung: Bao gồm các thông tin chung/thông tin định danh của đối tượng, mặc định luôn hiển thị khi vừa truy cập

2 - Nhóm thông tin chi tiết: Bao gồm các thông tin chi tiết của đối tượng, được phân thành các nhóm thông tin khác nhau, mặc định các nhóm thông tin này sẽ được đóng lại, chọn ˅ để mở rộng và hiển thị nhóm thông tin.

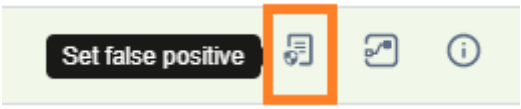
Thao tác Copy hỗ trợ sao chép nội dung trường thông tin

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

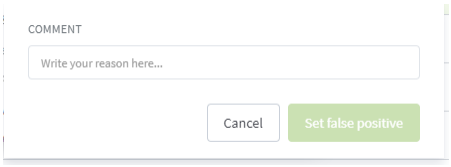


3.4.7 Đánh dấu không nguy hiểm cho 01/nhiều alert hoặc nhóm alert

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

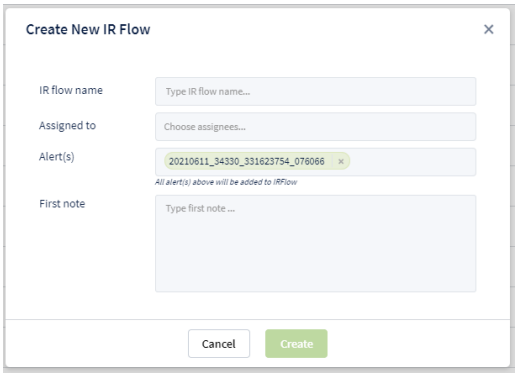


- Bước 3: Nhập lý do đánh dấu không nguy hiểm và chọn 



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

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



Dữ liệu hiển thị trong Combobox Assigned to bao gồm:

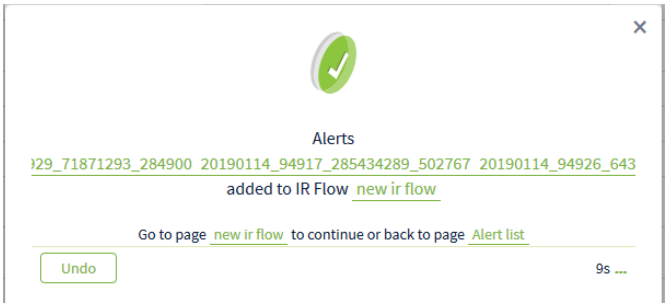
+ User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống

+ User đăng nhập thuộc group default: Hiển thị tên User đang login

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

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

- Bước 3: Sau khi tạo xong hiện cửa sổ sau để có thể hoàn tác trong 10s



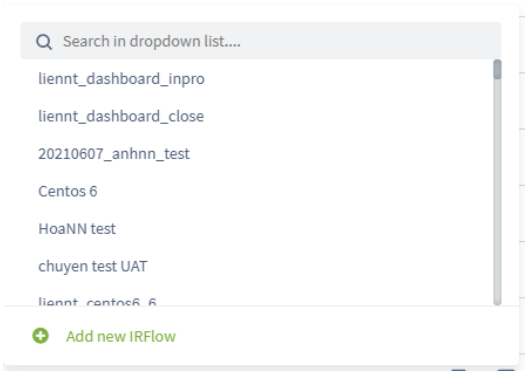
+ Để hoàn tác: chọn “Undo” trong 10 s

+ Để tạo ngay IR flow và chuyển sang màn hình IR flow chọn tên IR flow vừa tạo: chọn “new ir flow”

+ Để quay về màn hình alert chọn “Alert list”

3.4.9 Thêm 01/nhiều alert hoặc nhóm alert vào IR fLow đã có

- Tương tự như 3.3.5 nhưng không chọn “Add new IRFlow” mà chọn IR flow đã có từ danh sách chọn



3.5 Màn hình IRFLow

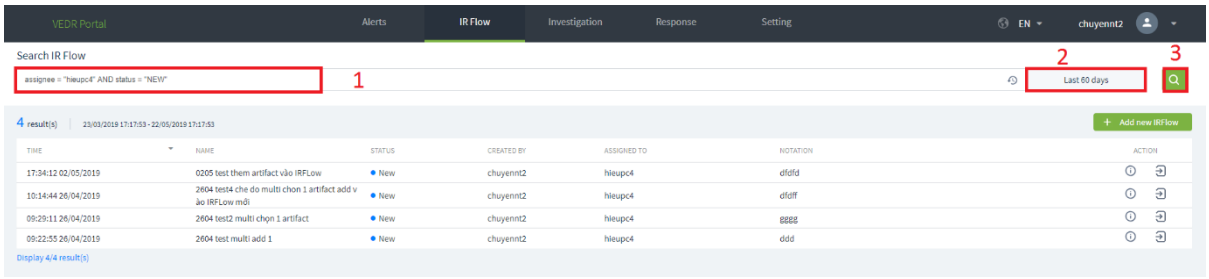
3.5.1 Danh sách hiển thị

- User đăng nhập thuộc group root: Hiển thị tất cả IRFlow trong hệ thống
- User đăng nhập thuộc group default: Hiển thị tất cả IRFlow được assign cho user đang login
- User đăng nhập thuộc group cha: Hiển thị tất cả IRFlow được assign cho user đang login và các user thuộc group con tương ứng
- User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả IRFlow được assign cho user đang login

3.5.2 Tìm kiếm IRFLow

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

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



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

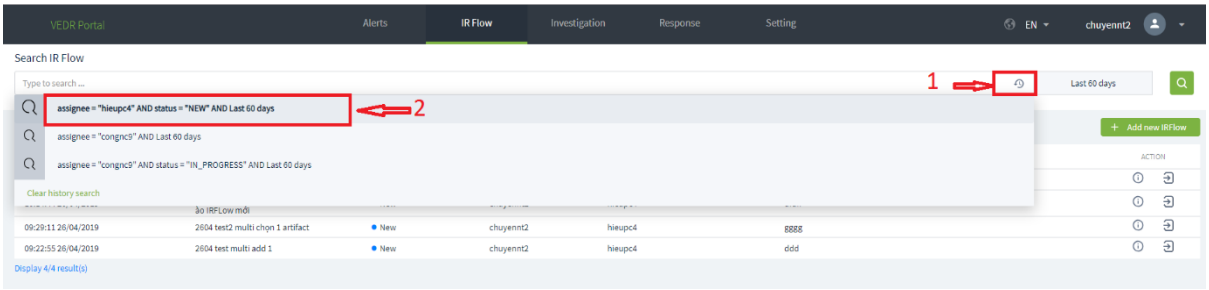
  <tên_trường> <toán tử> “<value>” AND/OR <tên_trường> <toán tử> “<value>”…..

  Trong đó:

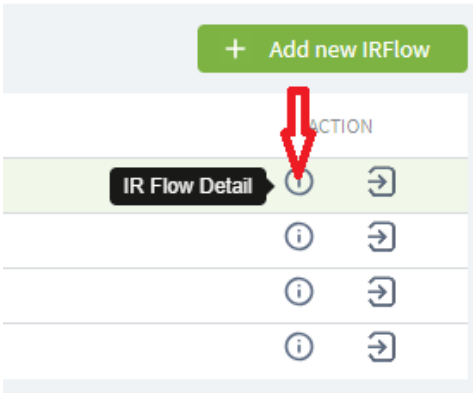
- <tên_ trường> là các giá trị sau:
  - assignee: người được phân công xử lý alert
  - created_by: tài khoản tạo IRFLow
  - name: Tên của IRFLow
  - notation: lưu ý của IRFlow
  - status: trạng thái của IRFlow
- <toán_tử> là các giá trị sau:
  - = : tìm chính xác giá trị là value
  - != : tìm giá trị khác với value
  - ~: tìm giá trị like với value
  - AND/OR: toán tử kết hợp để kết hợp 2 câu query.

- Bước 2: chọn khoảng thời gian tìm kiếm bằng cách click vào button Date & Time và chọn khoảng thời gian tùy ý. Nếu không chọn mặc định là Last 7 days
- Bước 3: Click on Search

Ngoài ra hỗ trợ tìm kiếm theo lịch sử tìm kiếm

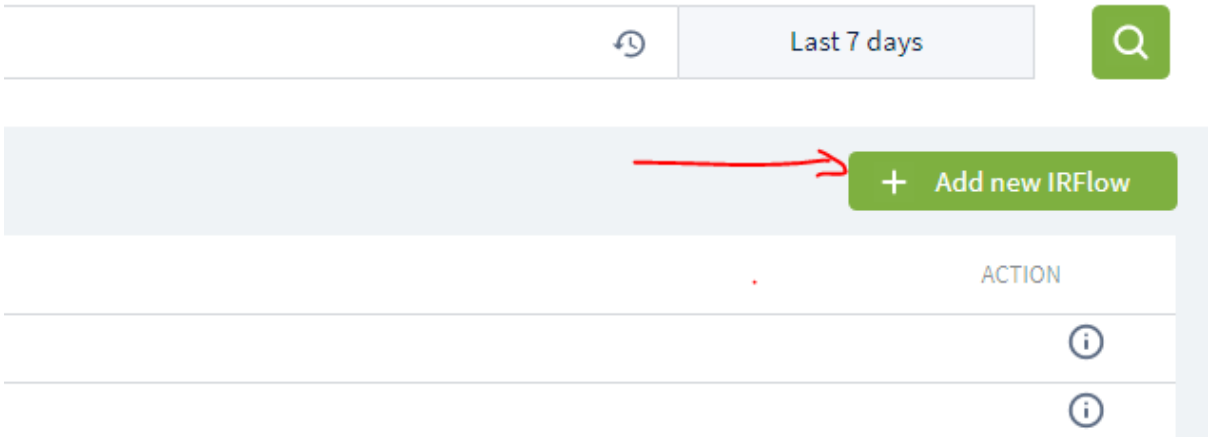


Để vào xem thông tin chi tiết 1 IRFlow và thực hiện các hành động điều tra, xử lý người dùng chọn “IRFLow Detail”



3.5.3 Cách tạo IRFlow

- Bước 1: Click vào Add new IRFlow



- Bước 2: Nhập thông tin hợp lệ

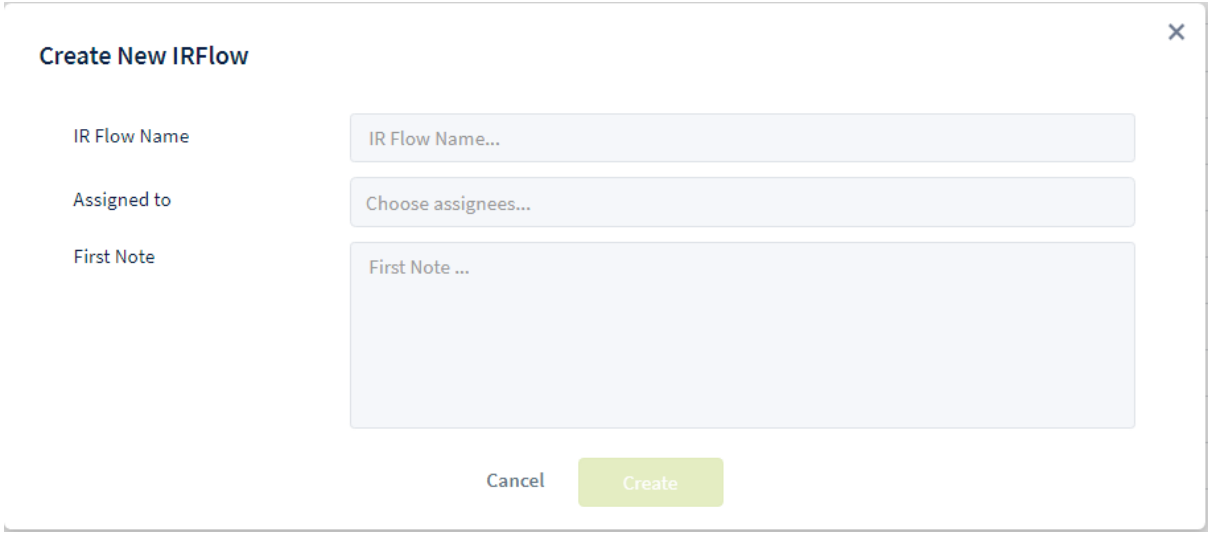
  Dữ liệu hiển thị trong Combobox Assigned to:

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

  + User đăng nhập thuộc group default: Hiển thị tên User đang login

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

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



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

3.5.4 Các bước thực hiện trong IRFlow

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

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

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

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

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

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

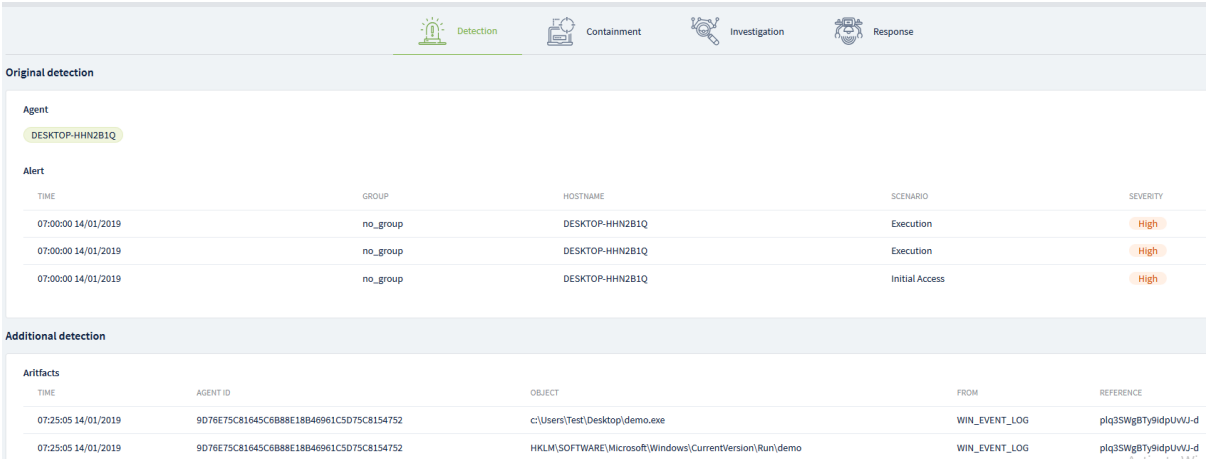
3.5.5 IRFLow – Detection

- Tab Detection hiển thị các đối tượng liên quan đến alert như:

  + Danh sách máy tính có alert

  + Danh sách alert

  + Danh sách artifacts được phát hiện trong quá trình điều tra (investigation)



- Các đối tượng thuộc phần “Original Detection”: là các alert (Alert) và máy tính (Agent) ban đầu khi IRFlow được tạo.
- Còn các đối tượng thuộc phần “Additional Detection”: là các alert, máy tính, artifacts được thêm vào ở bước điều tra (Investigation)
- Ý nghĩa một số trường trên màn hình detection:

  + Time: thời gian thêm agent/artifact vào màn hình detection

  + Object: đường dẫn file/registry của artifact

  + From: nguồn phát sinh artifact (Event log hoặc Process Analysis)

  + Reference: ID của event log hoặc ID của phiên kết nối Process Analysis

3.5.6 IRFlow – Containment

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

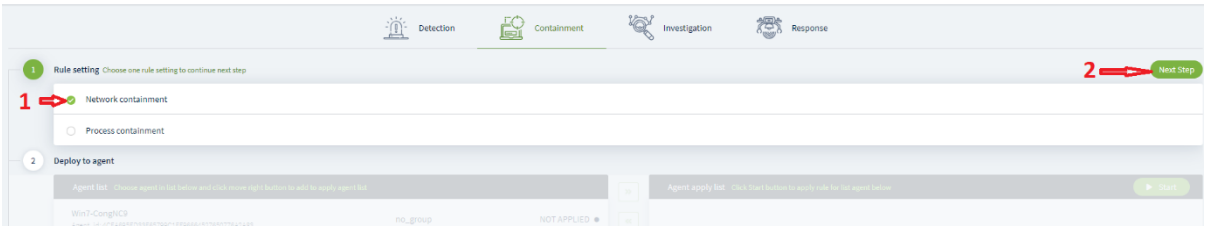
  + NOT APPLIED: chưa gửi lệnh xuống Agent

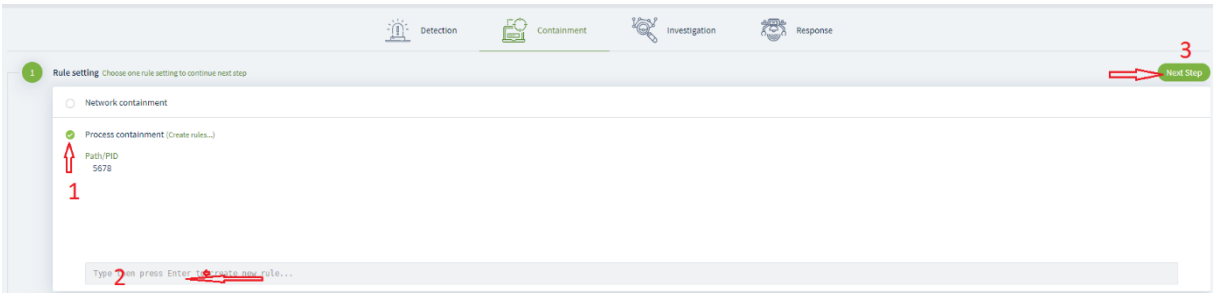
  + APPLYING: đang gửi lệnh xuống agent

  + APPLIED: đã gửi lệnh cô lập thành công

  + STOPPING: đang gửi lệnh dừng cô lập

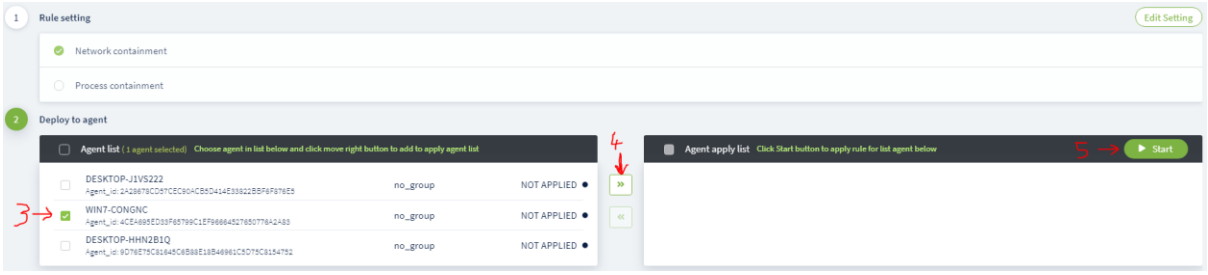
  + STOPPED: đã gửi lệnh dừng cô lập thành công
- Bước 1: lựa chọn hình thức điều tra: cô lập mạng hoặc suspend tiến trình sau đó chọn "Next Step"



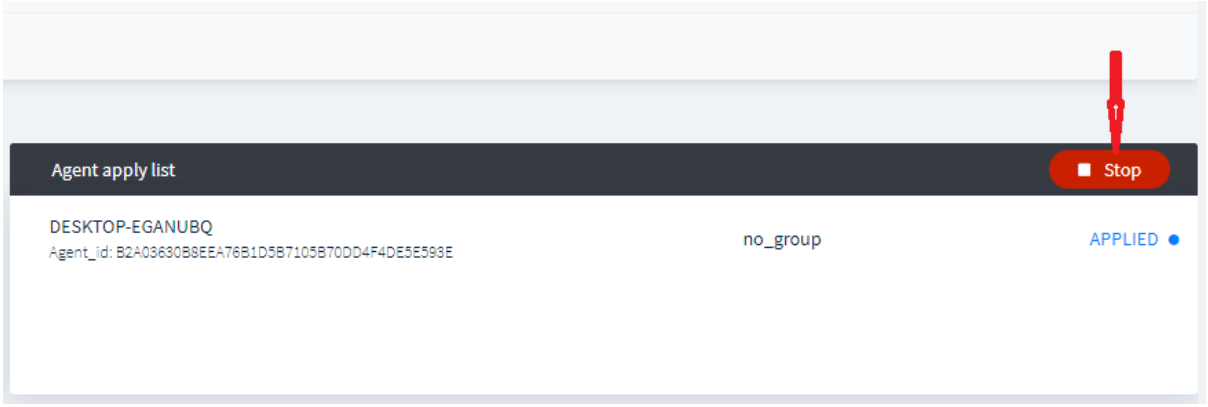


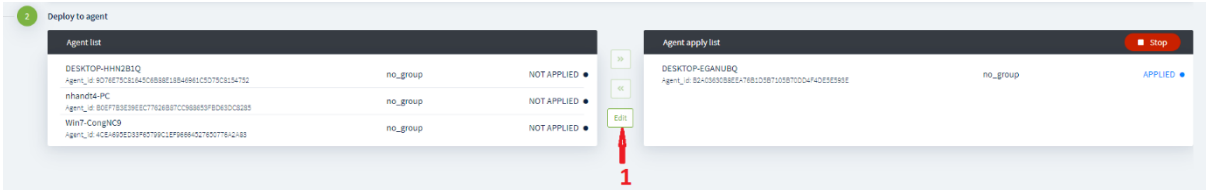
<u>Lưu ý:</u> sau khi nhập Path/PID thì phải ấn Enter để lưu lại cấu hình. Có thể suspend cùng lúc nhiều tiến trình

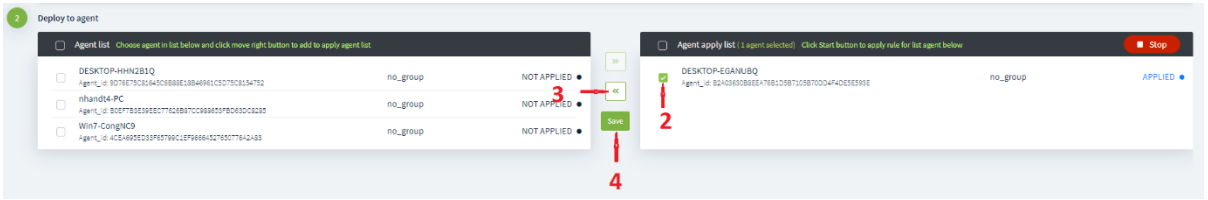
- Bước 2: chọn danh sách Agent cần cô lập và chọn "Start" để bắt đầu cô lập



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







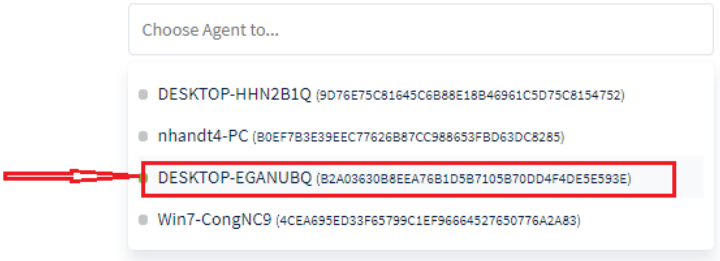
- Trong trường hợp người quản trị không chủ động dừng việc cô lập trên Portal thì sau thời gian mặc định (24h) thì Agent cũng tự động gỡ cô lập dưới Agent.

3.5.7 IRFLow – Investigation

3.5.7.1 Process Analysis

3.5.7.1.1 Xem thông tin process

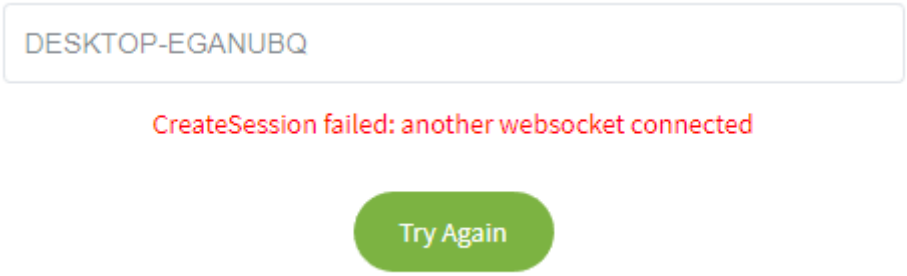
- Đây là quá trình phân tích các tiến trình trên máy người dung có trong tab Detection theo thời gian thực nhằm tìm kiếm các dấu hiệu bất thường
- Bước 1: Chọn agent để kết nối, sau đó click “Start”. Danh sách Agent là các Agent trong IRFLow



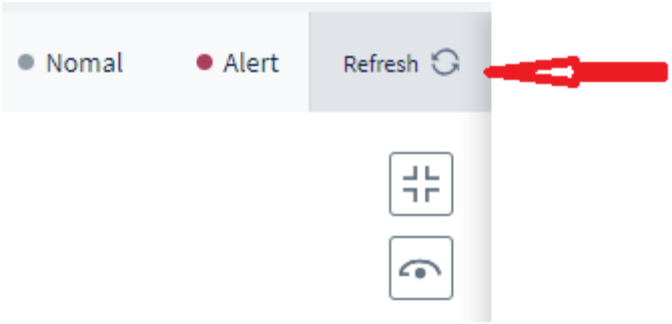
- *Lưu ý:*

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

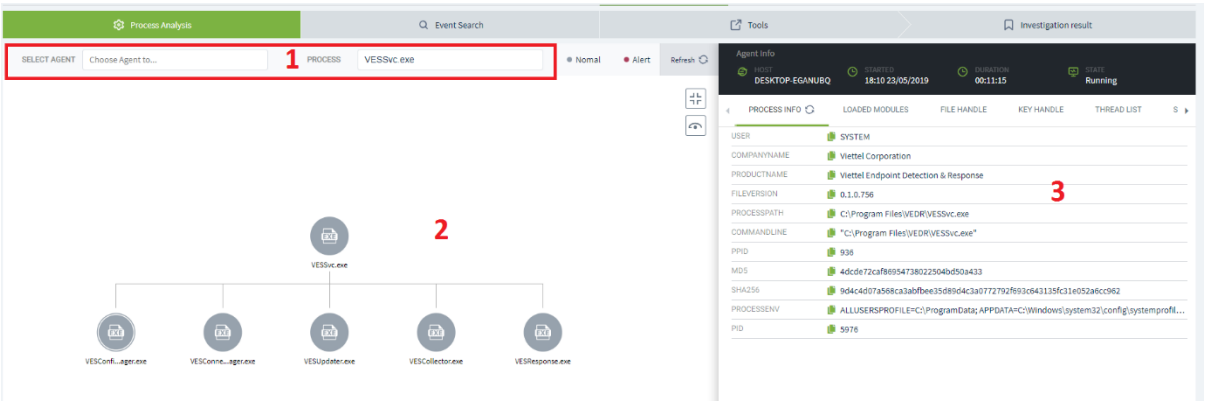
  + Tại 1 thời điểm trong 1 IRFLow chỉ có thể tạo 1 kết nối tới Agent. Trong trường hợp có tài khoản khác đang kết nối với Agent trong cùng IRFLow thì sẽ thông báo lỗi



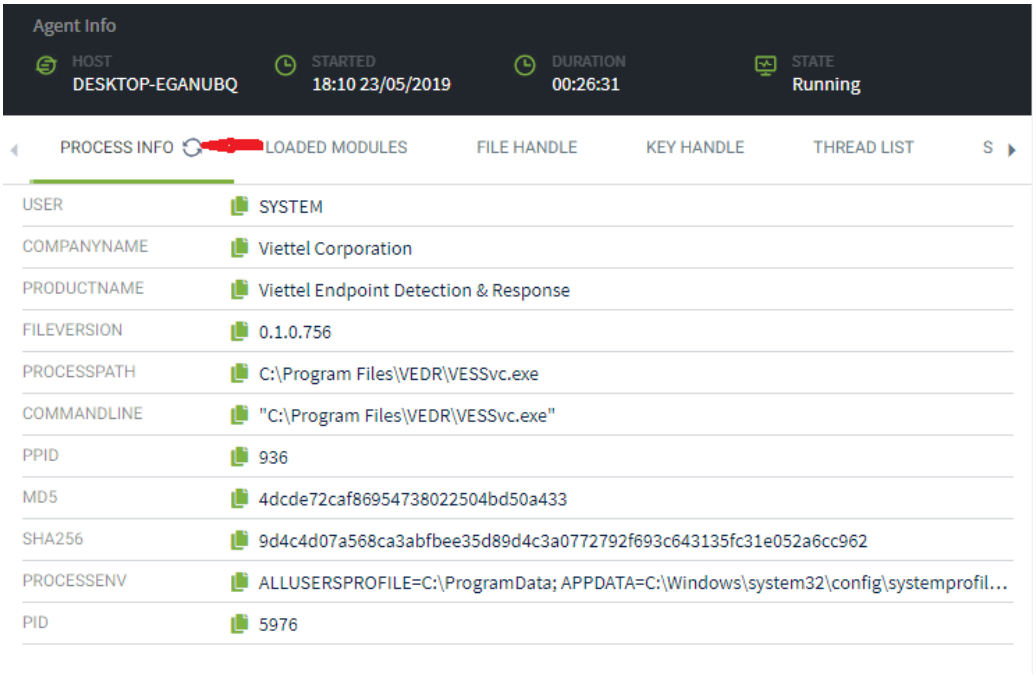
- Bước 2: Click “Refresh” để lấy danh sách process mới nhất dưới Agent



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



- Vùng 1: chọn agent và chọn process
- Vùng 2: hiển thị thông tin cây process, mặc định hiển thị 1 cấp cha và 1 cấp con. Cho phép mở thêm/thu nhỏ các cấp khi click vào process trong cây. Process được focus trong cây sẽ hiển thị icon khác so với process không được focus
- Vùng 3: hiển thị thông tin process được focus trong cây bao gồm thông tin trên các tab: Process info, Modules (loaded dll), File handles, Key handles, Thread List, Section handles, Network Connection
- Bước 4: để lấy thông tin mới nhất của process, click icon Refresh trên mỗi tab



- *Lưu ý:*

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

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

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

3.5.7.1.2 Marking/Get artifact

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

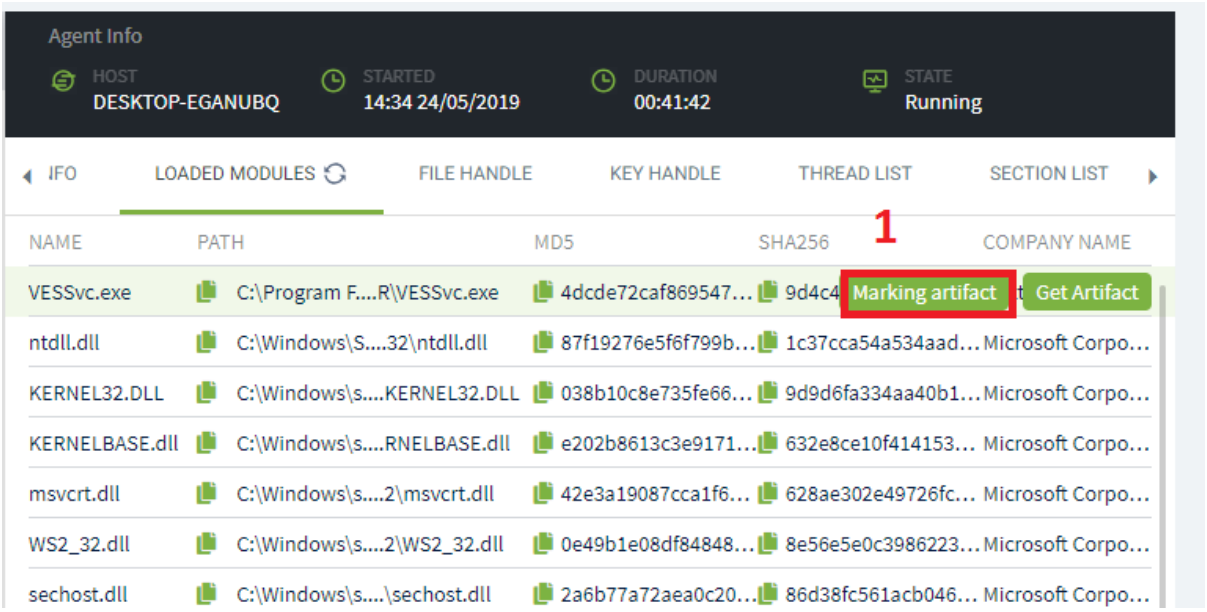
  + Process Info: ProcessPath

  + Loaded module: Path

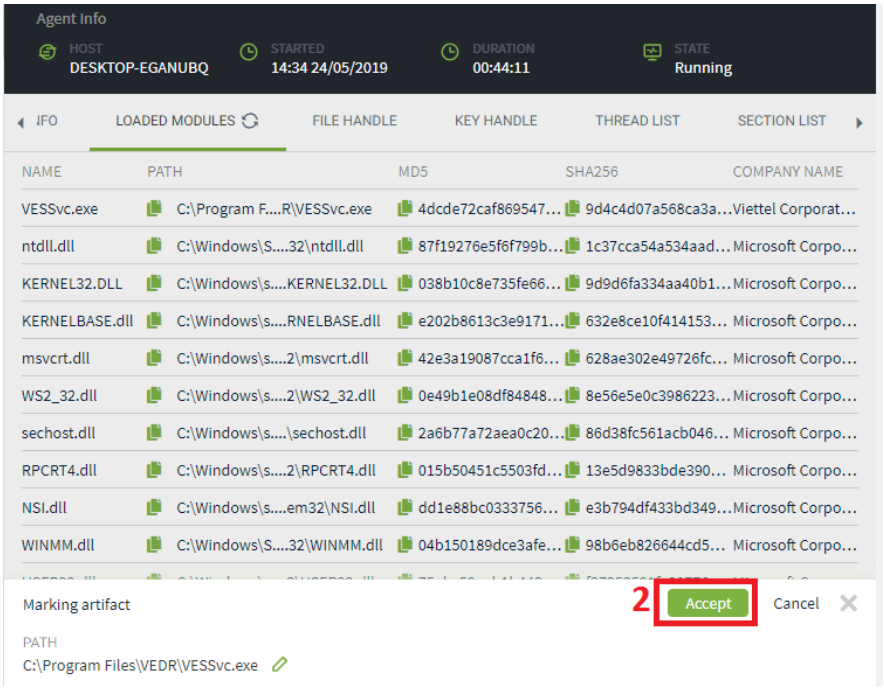
  + File Handle: Path

  + Key Handle: Key path, Value

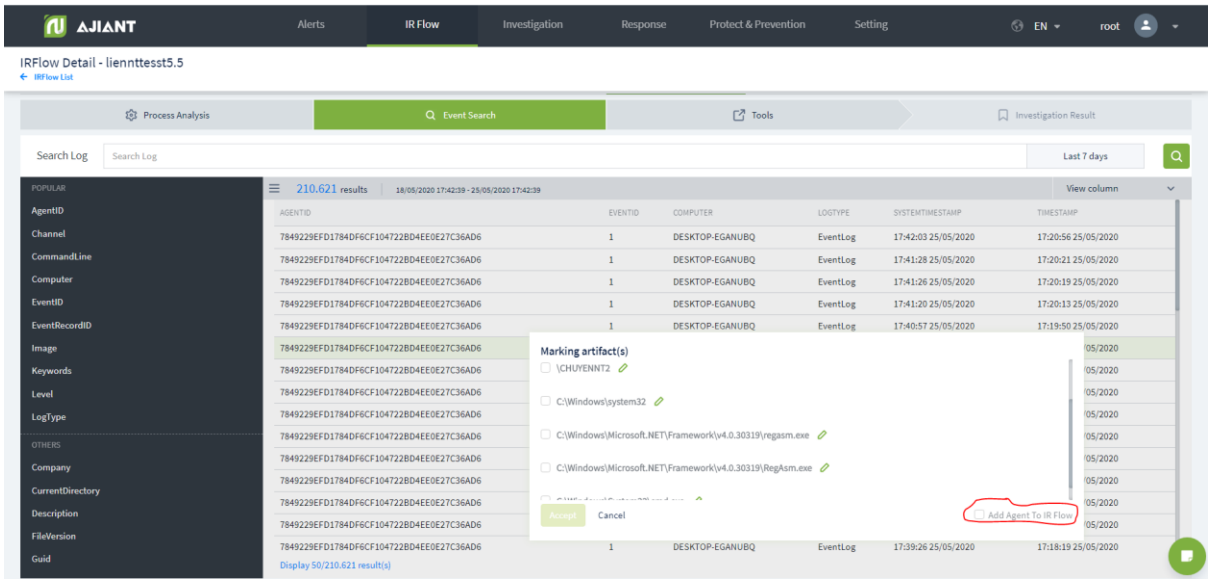
- Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào button “Marking artifact”



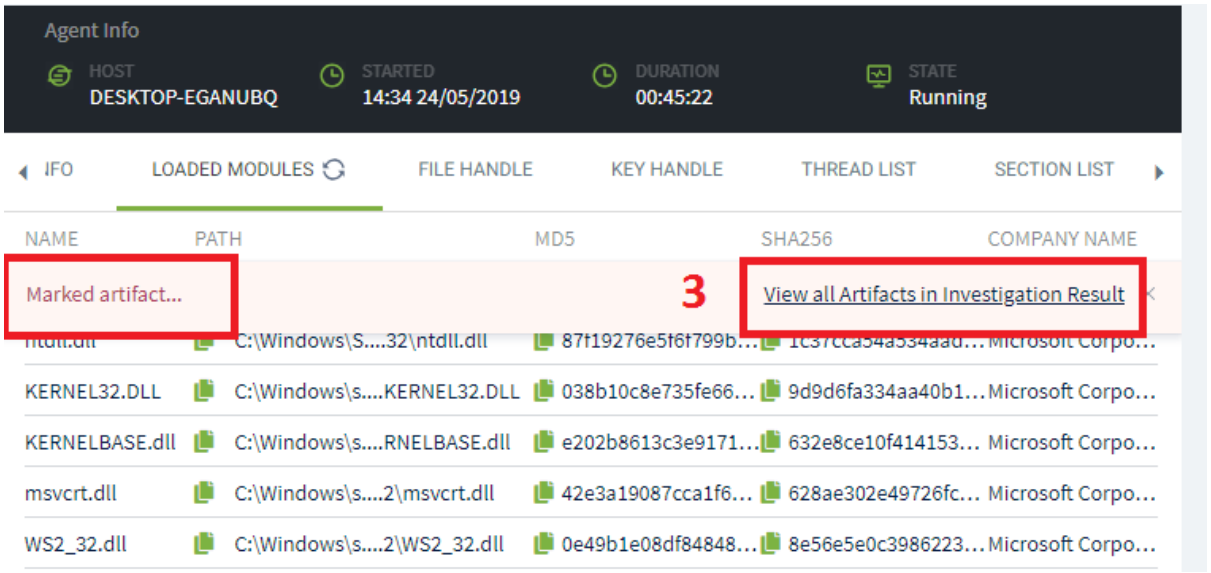
- Bước 2: Click vào button “Accept”, có thể chỉnh sửa đường dẫn file khi click vào icon Edit

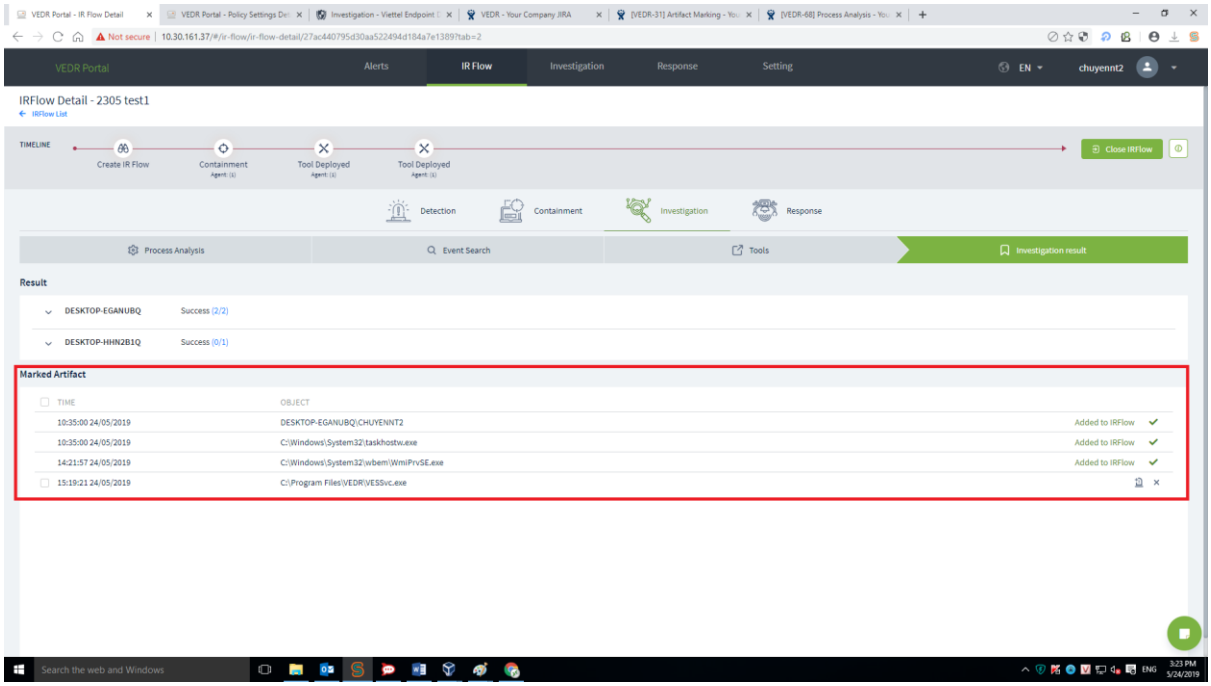


Trường hợp chọn bản ghi có Agent chưa tồn tại trong Detection sẽ có them check box Add Agent to IRFlow. Khi thực hiện Accept thì Agent tương ứng sẽ được add vào Detection

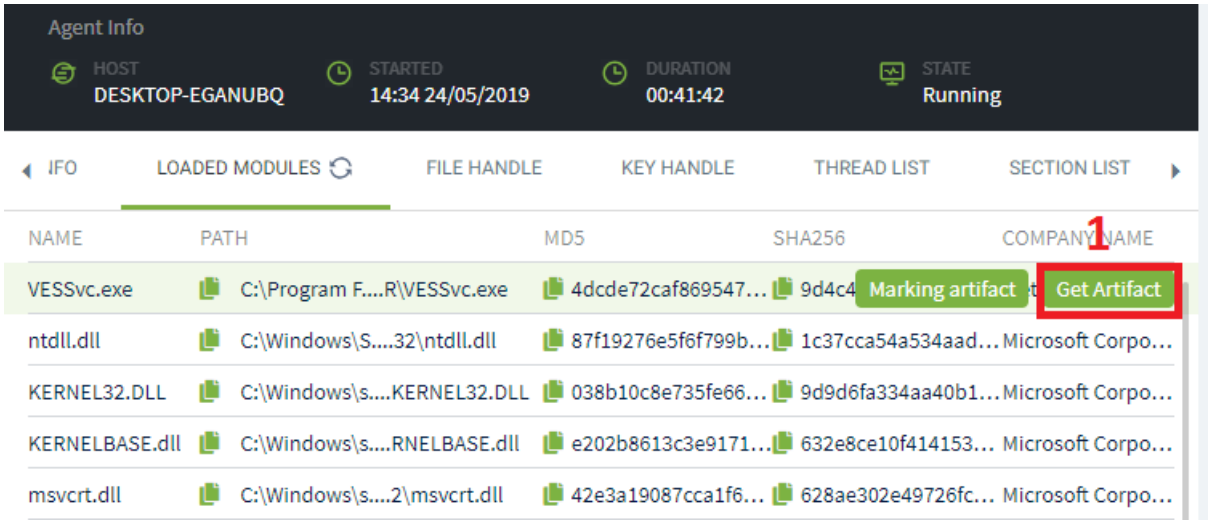


- Sau khi marking thành công, hiển thị thông báo. Click vào button “View all artifacts in Investigation Result” để chuyển đến màn hình Investigation Result. Artifact được marking sẽ hiển thị trên màn hình này





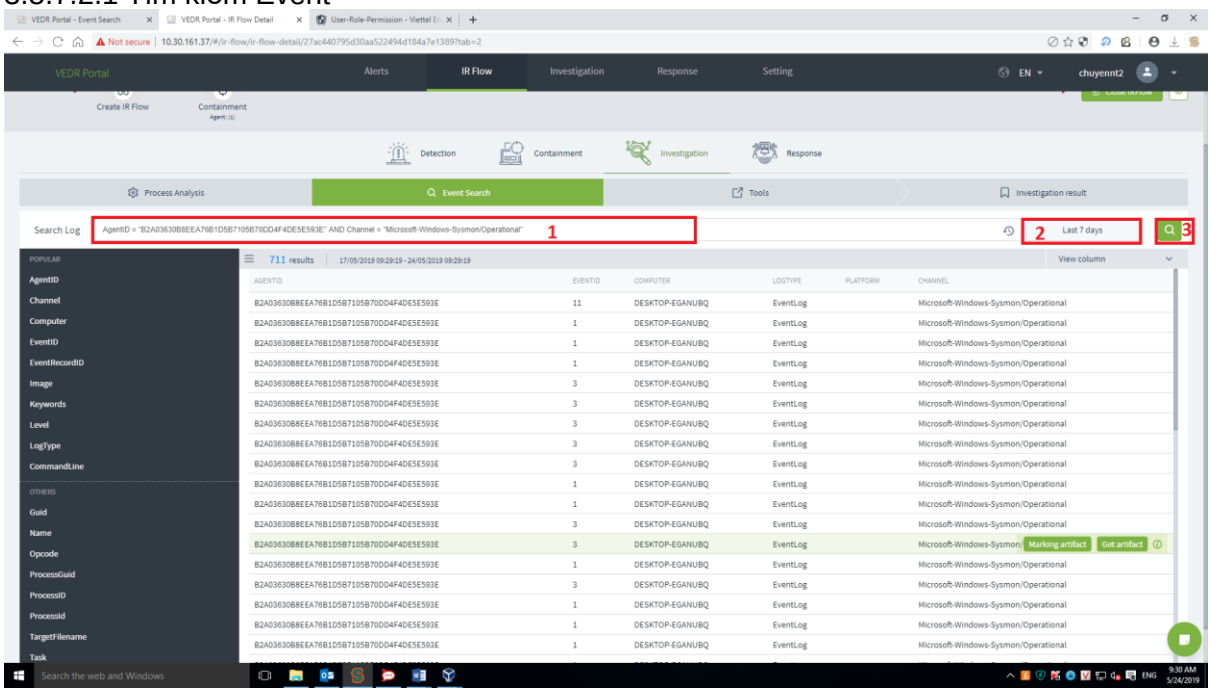
- Chức năng Get Artifact cho phép lấy thông tin file/registry dưới Agent phục vụ cho việc điều tra
- Chọn 1 bản ghi và hover vào bản ghi đó. Click button “Get artifact” > Lựa chọn loại artifact (File/Registry) > Click “Accept”. Sau đó kiểm tra kết quả thực hiện Get artifact trên màn hình Investigation Result



3.5.7.2 Event Search

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

3.5.7.2.1 Tìm kiếm Event



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

<tên_trường> <toán tử> “<value>” AND/OR <tên_trường> <toán tử> “<value>”…..

- Trong đó:

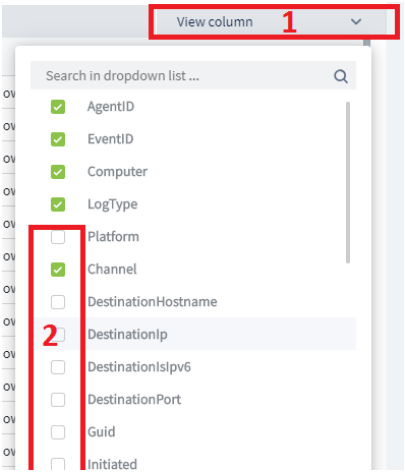
- <tên_ trường> là các giá trị sau:
  - AgentID: ID của agent
  - EventID: ID của event
  - Computer: Tên của computer
  - LogType: Loại log
  - Channel: Channel của event
- <toán_tử> là các giá trị sau:
  - = : tìm chính xác giá trị là value
  - != : tìm giá trị khác với value
  - ~: tìm giá trị like với value
  - AND/OR: toán tử kết hợp để kết hợp 2 câu query

- Bước 2: Chọn khoảng thời gian tìm kiếm bằng cách click vào button Date & Time và chọn thời gian tùy ý. Nếu không chọn thời gian thì hệ thống chọn mặc định là Last 7 days.
- Bước 3: Click on Search.

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

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

  + Để thêm cột hiển thị click vào “View Column” và tích chọn các trường cần thiết

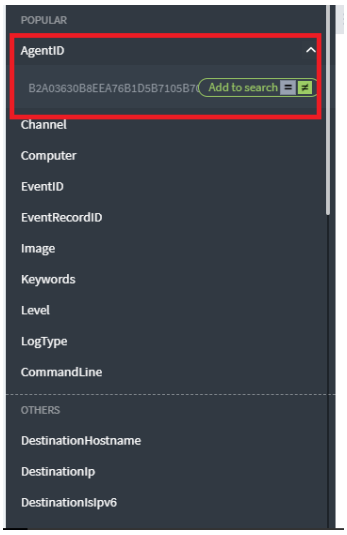


- Ngoài ra, người dùng có thể tìm kiếm các trường trong phần Popular và Others bằng cách show các value của các trường và hover vào value trong Popular/Others, bản ghi đó sẽ hiển thị 2 icon là: “=” và “!=”.

  + Nếu người dùng chọn “=” thì trên phần textbox Search sẽ hiện câu query tương ứng với toán tử “=”.

  + Nếu người dùng chọn “!=” thì trên phần textbox Search sẽ hiện câu query tương ứng với toán tử “!=”.

  + Nếu trong textbox Search đã có dữ liệu và người dùng chọn thêm các value trong phần Popular/Others thì 2 vế của câu query được kết nối với nhau bởi toán tử AND.



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

- Khi người dùng load more thì cập nhật bản ghi từng trường theo số lượng bản ghi hiển thị trên màn hình.

  + Ở phần Popular hiển thị 10 trường phổ biến của log được tìm kiếm nhiều nhất

  + Nếu có >=10 trường thì hiển thị 10 trường có số lượng tìm kiếm nhiều nhất, nếu có ít hơn 10 trường thì hiển thị toàn bộ các trường đó ra.

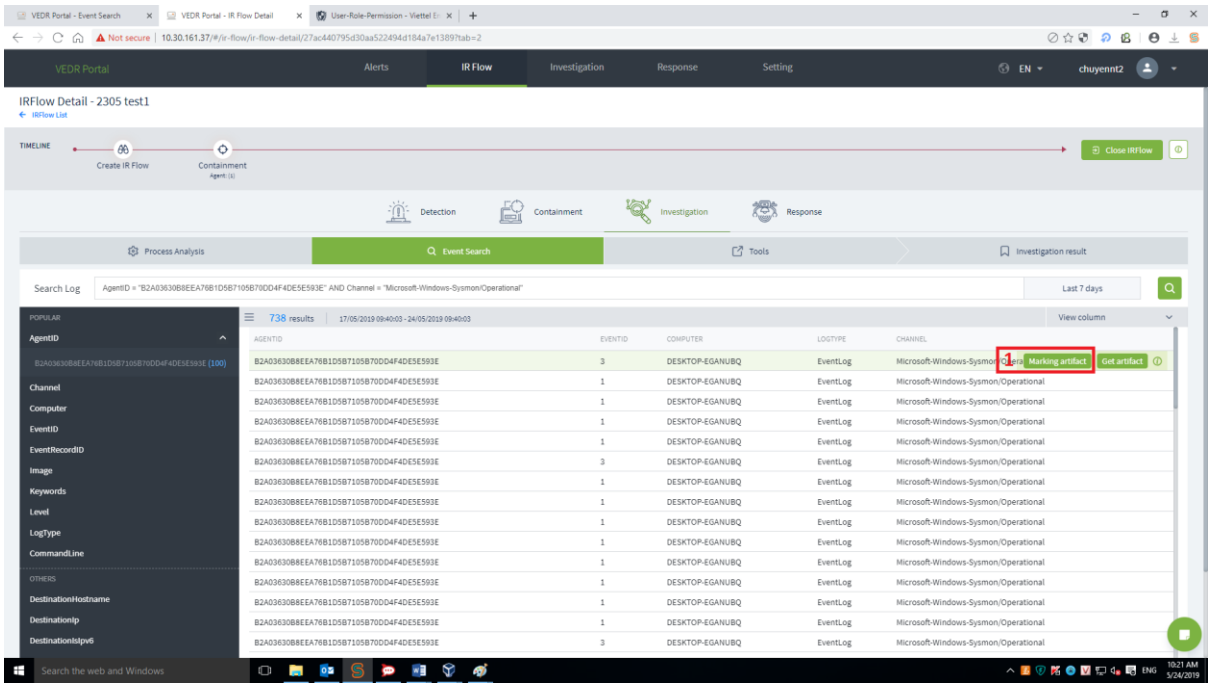
- Khi show/hide 1 trường sẽ hiển thị 5 trường có số lượng bản ghi nhiều nhất, sắp xếp từ cao xuống thấp.
- Khi người dùng load more thì cập nhật bản ghi từng trường theo số lượng bản ghi hiển thị trên màn hình.
- Khi kích đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó

  + Tab thông tin chi tiết hiển thị là dạng Table, dữ liệu hiển thị dưới dạng bảng

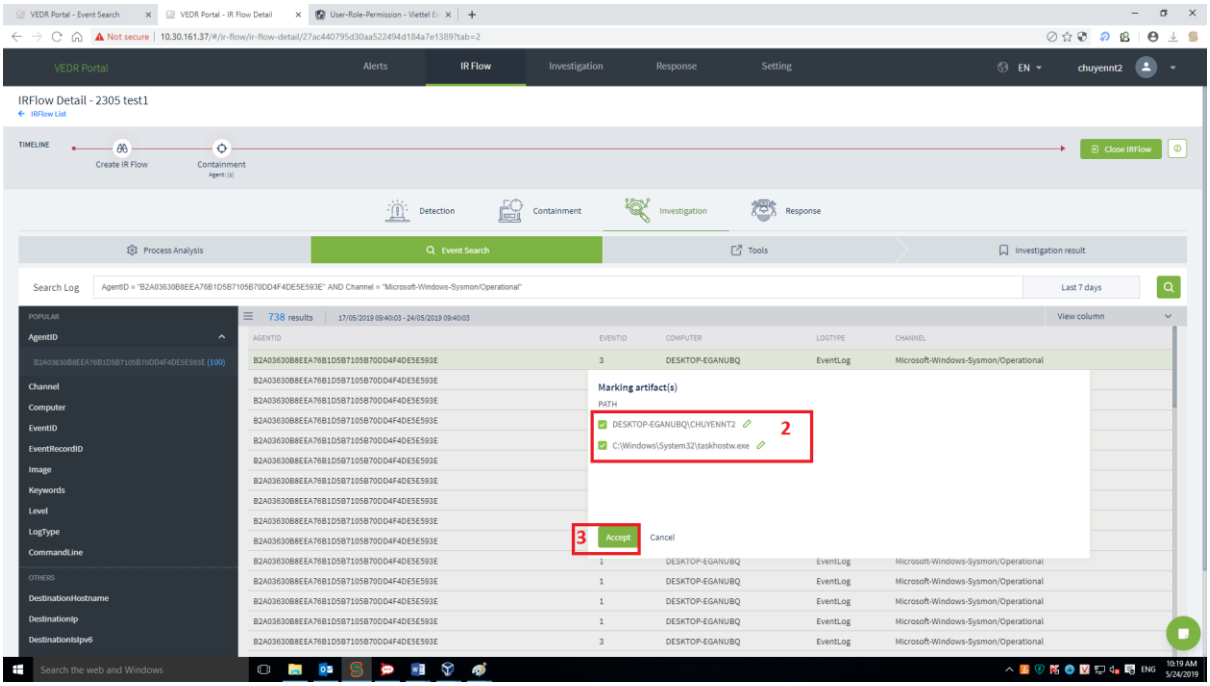
  + Khi chọn tab JSON thì dữ liệu hiển thị dưới dạng JSON

3.5.7.2.2 Xử lý Event

- Marking artifact: Đánh dấu artifact

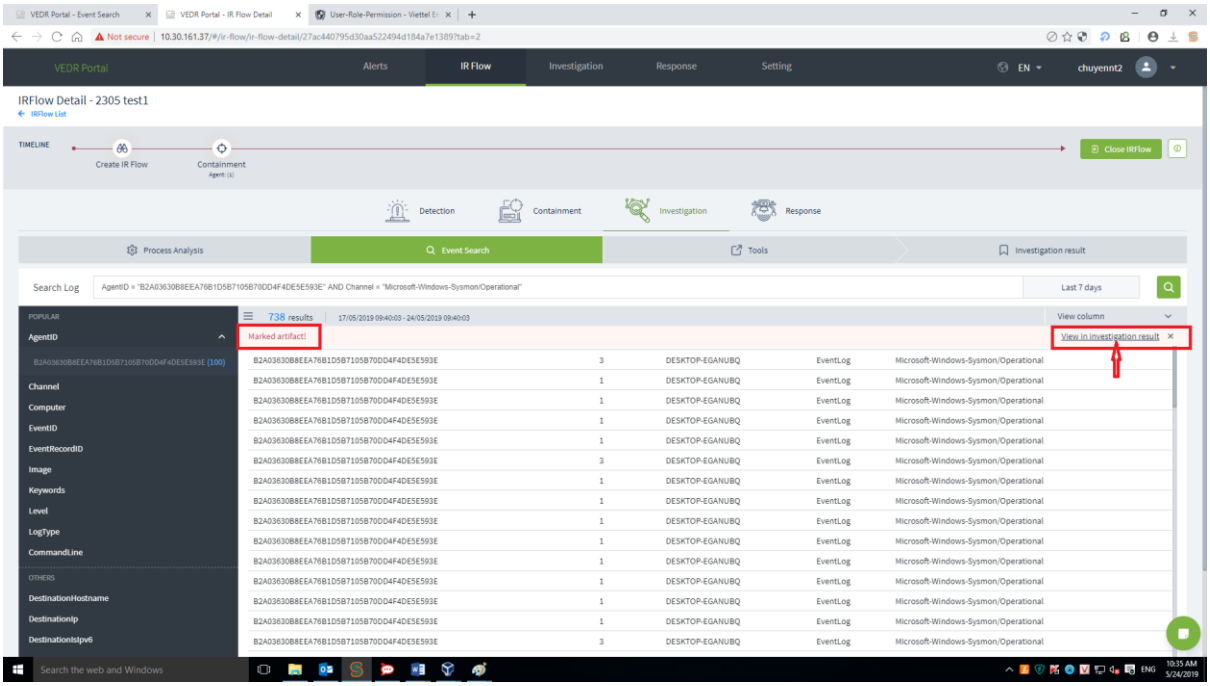


- Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào button Marking artifact. Trên màn hình sẽ hiển thị popup như sau:

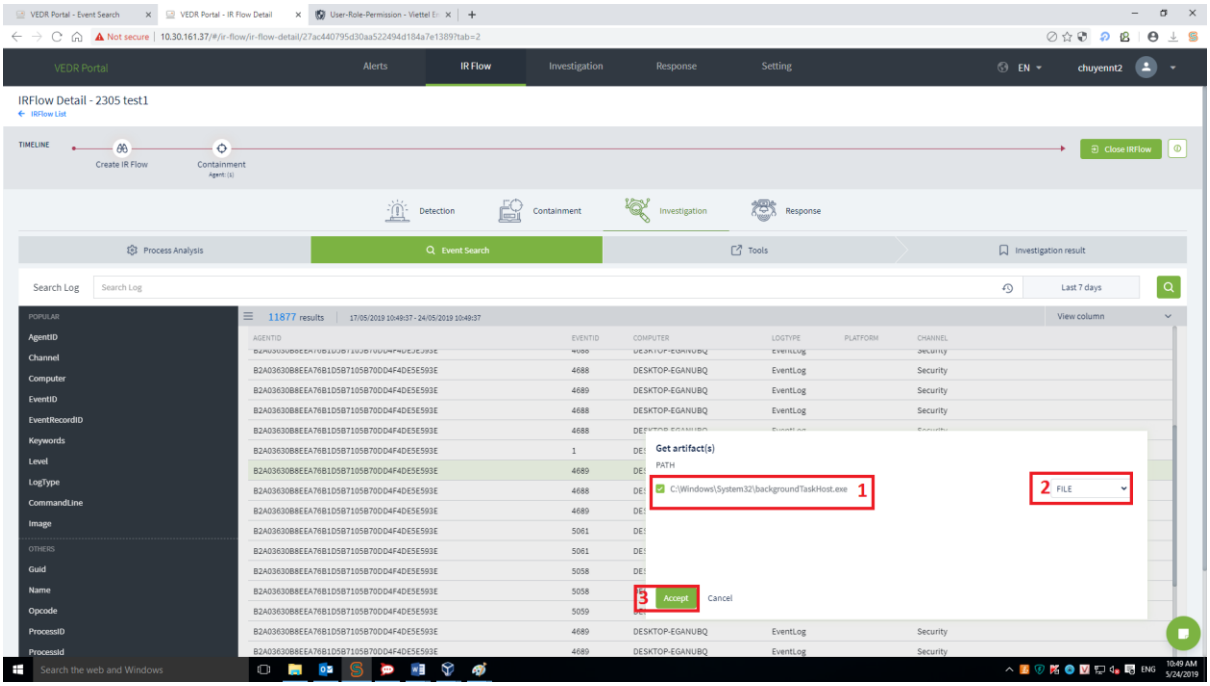


- Trường hợp chọn event của Agent không thuộc IRFLow thì sẽ có lựa chọn để người dùng add Agent vào IRFLow. Agent sẽ được thêm vào màn hình Detection của IRFlow đang thao tác

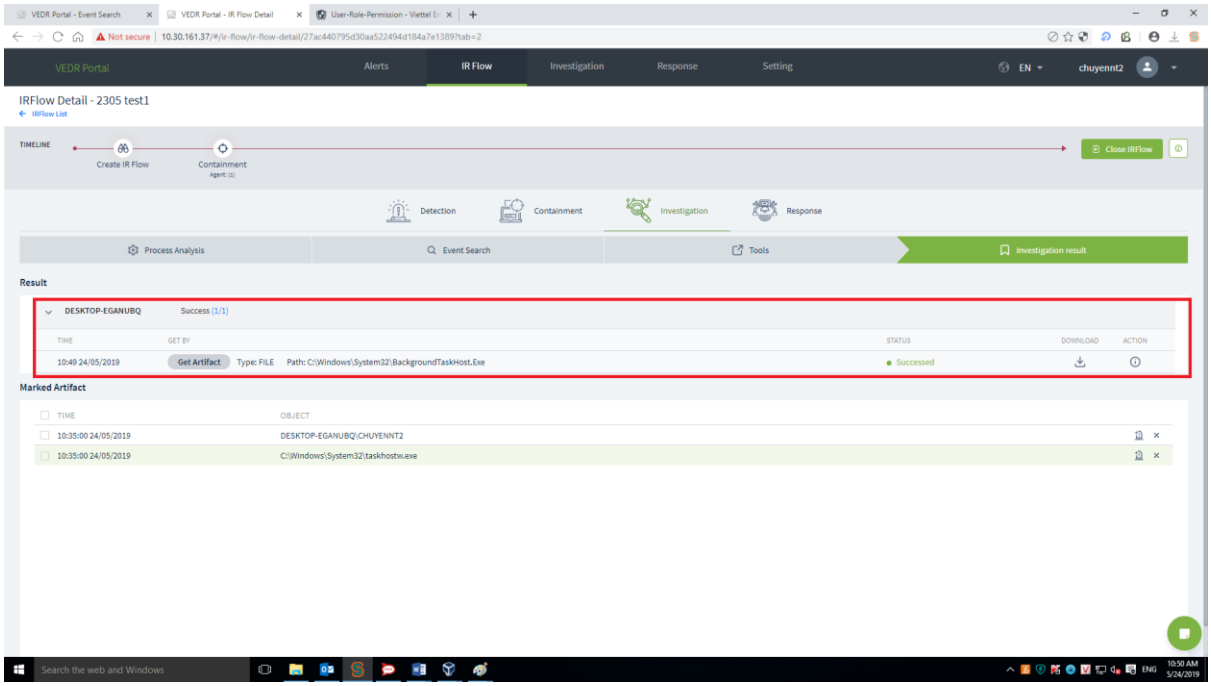
- Bước 2: Chọn path phù hợp để marking artifact. Sau đó nhấn vào Accept để thực hiện marking. Nếu chọn Cancel thì việc marking artifact sẽ bị trì hoãn.
- Khi marking artifact thành công màn hình sẽ hiển thị thông báo. Click vào “View in investigation result” để chuyển đến màn hình Investigation Result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



- Get artifact: thực hiện get file/registry dưới Agent lên server để phục vụ cho quá trình điều tra
- Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào button “Get artifact” Trên màn hình sẽ hiển thị popup như sau:



- Bước 2: chọn artifact sau đó chọn loại artifact (File/Registry) và click “Accept”
- Khi marking artifact thành công màn hình sẽ hiển thị thông báo. Click vào “View in investigation result” để chuyển đến màn hình Investigation Result. Kết quả của việc Get artifact sẽ hiển thị trên tab này



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

3.5.7.2.3 Deploy Tools

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

  Với agent Windows:

  + Listdlls: lấy thông tin các processs và dll đang được load lên

  + Autorunsc: lấy thông tin các tiến trình, dịch vụ khởi động cùng hệ thống

  Với agent Linux:

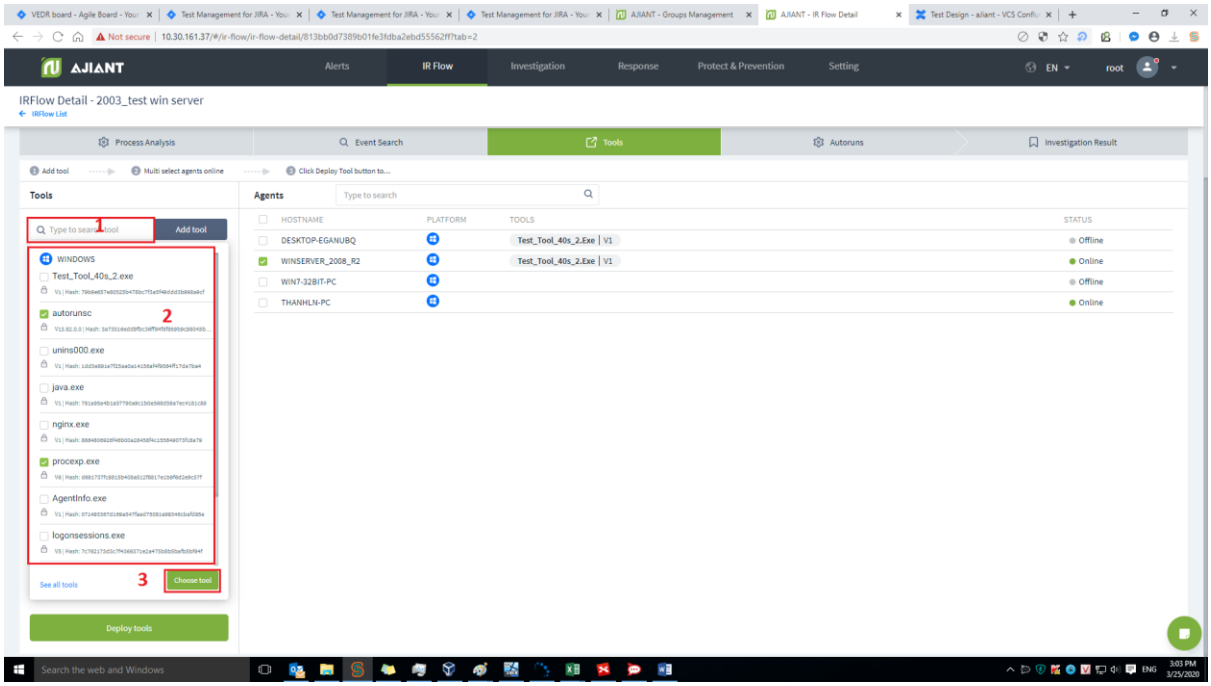
  + ListService: lấy danh sách service dưới máy agent

  Luồng thực hiện chức năng này như sau:

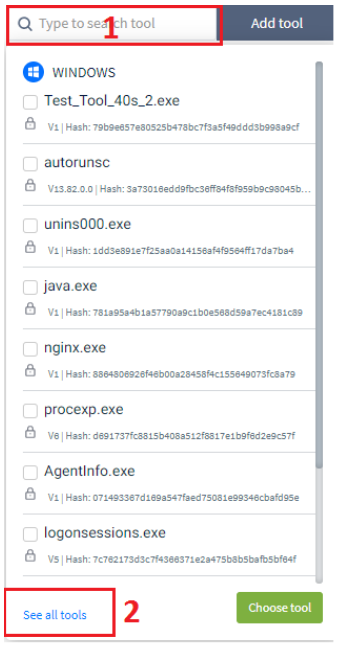
  Thực hiện lựa chọn tool > Chọn agent > click “Deploy tools”

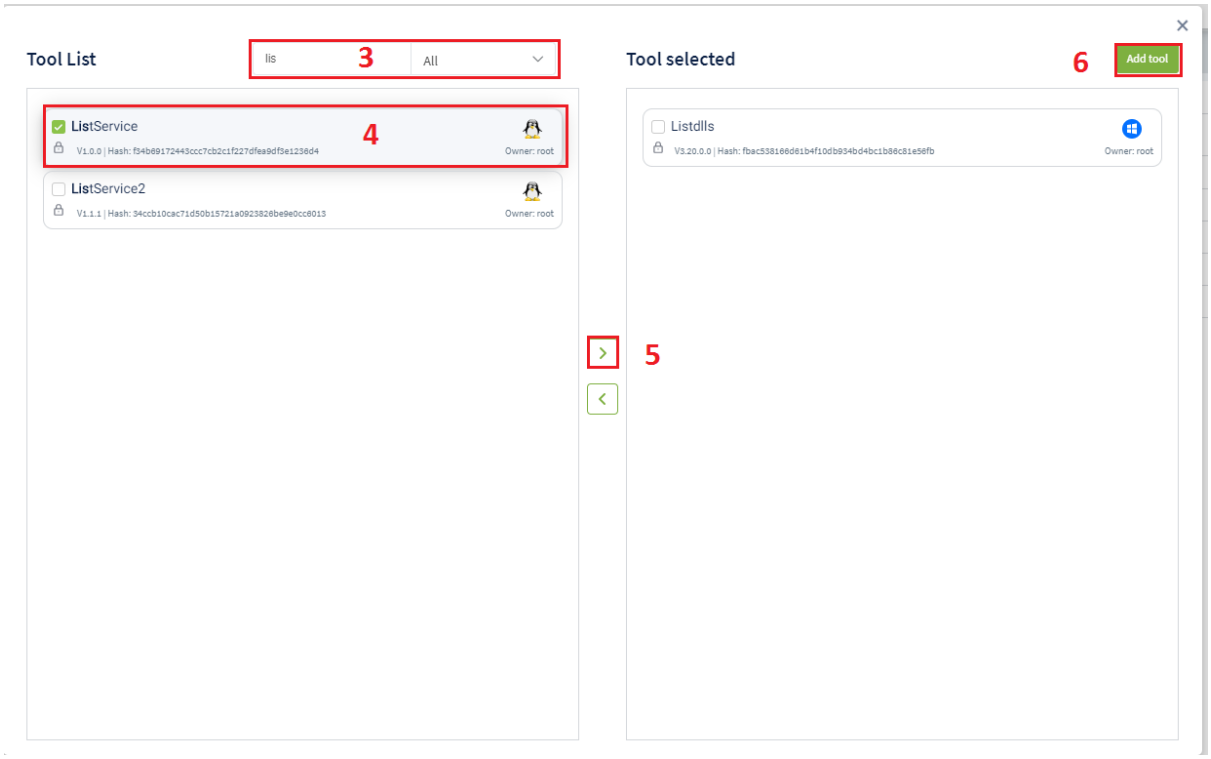
  Để lựa chọn tool thích hợp có 2 cách sau:

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

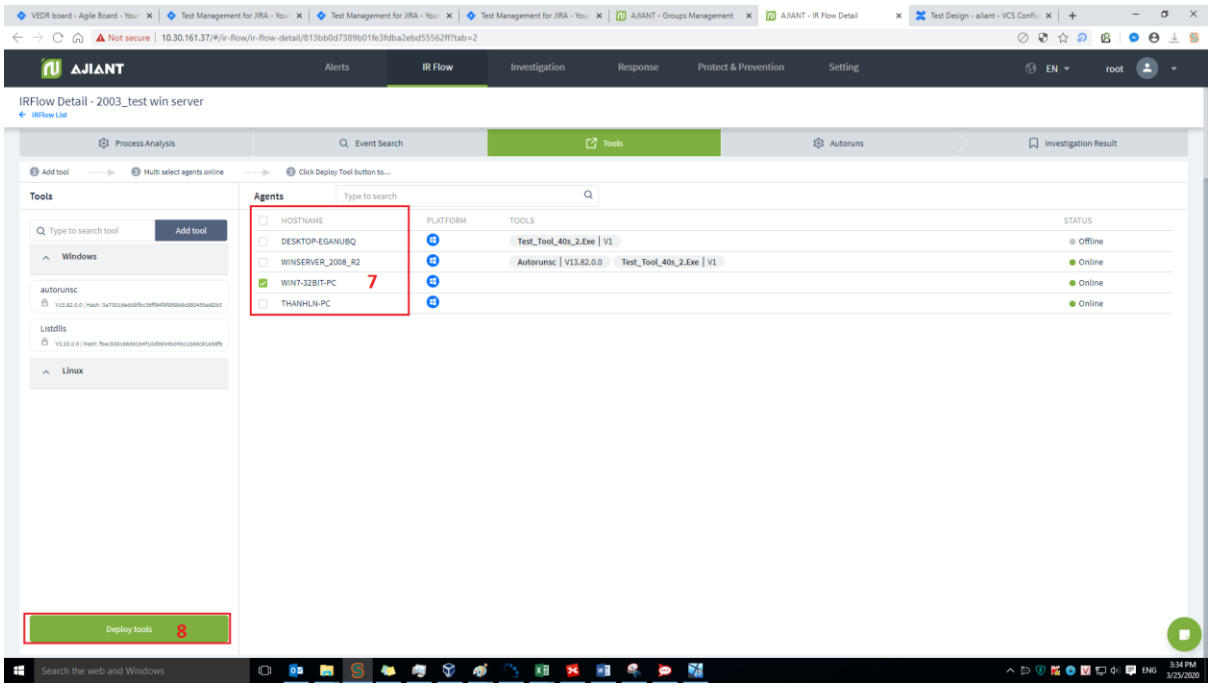


- Cách 2: Click vào textbox search tool > click “See all tools” => hiện ra màn hình danh sách tool đầy đủ >Tìm kiếm và lựa chọn tool cần deploy > click “Add tool”

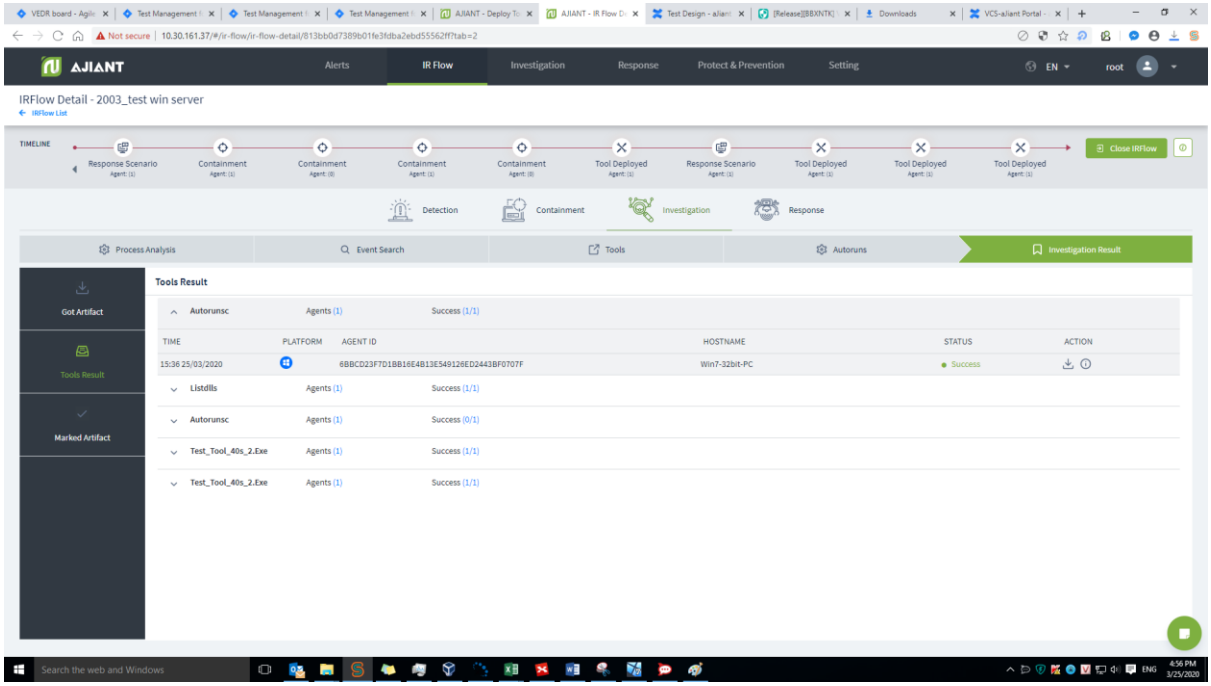




- Sau bước tìm kiếm tool thực hiện chọn agent và click “Deploy tools”



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



3.5.7.2.4 Xử lý Event

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

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

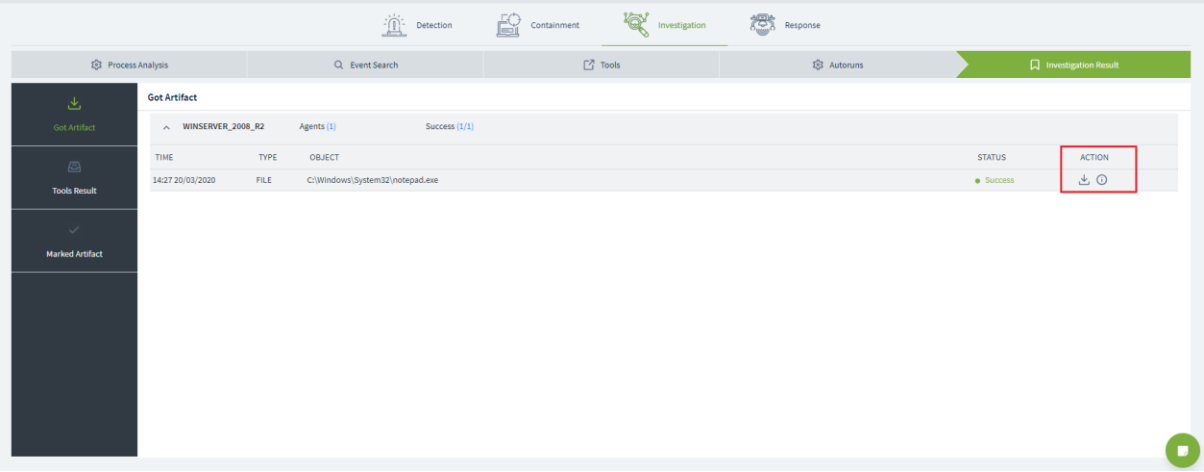
  + Tab Tool Results: kết quả thực hiện lệnh Deploy tools

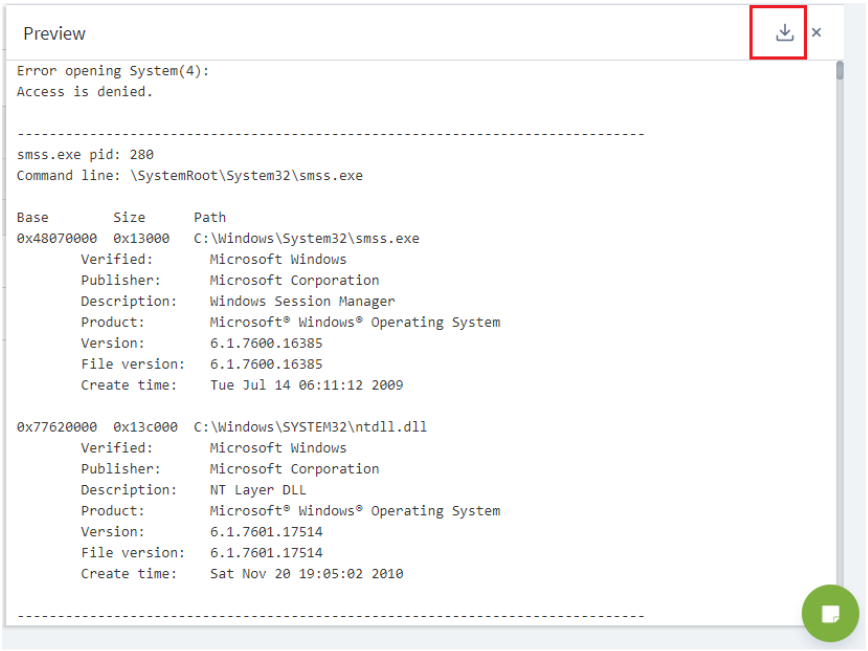
  + Tab Marked Artifact: các artifact đã marking

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

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

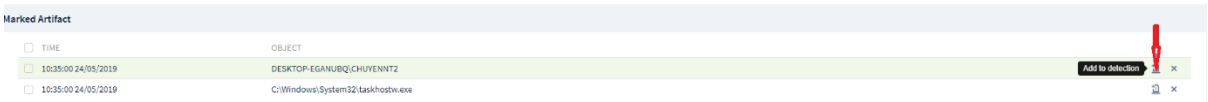
  + Download artifact hoặc kết quả chạy tool. Có 2 cách Download: click icon Download trên giao diện hoặc click icon Xem chi tiết > click icon Download trên màn hình này



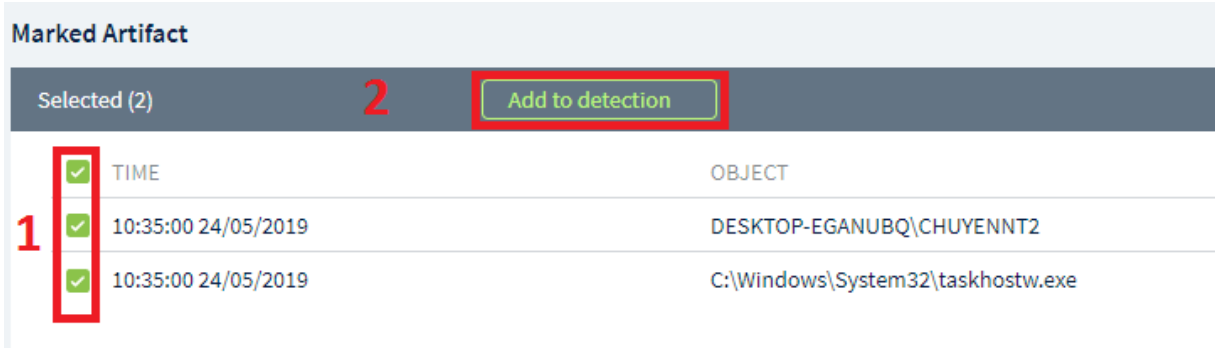


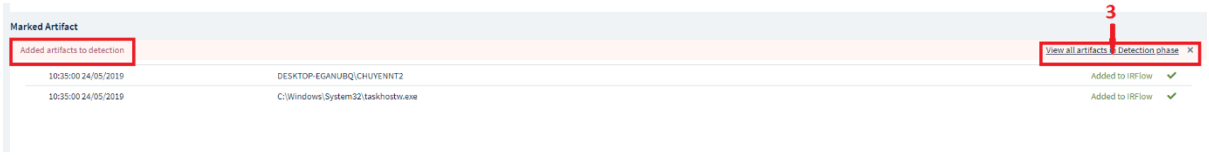
- Trong Tab Marked artifact, lựa chọn artifact để thêm vào màn hình Detection

  Chọn 1 artifact và click “Add to detection”

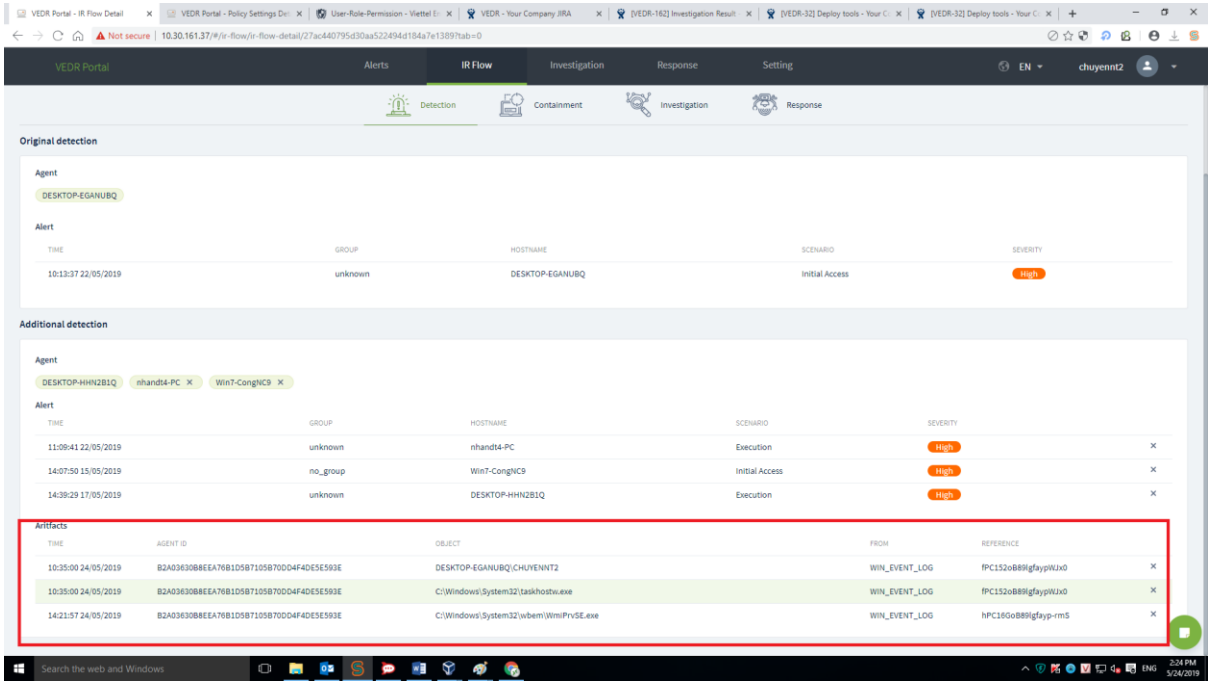


Chọn nhiều artifact và click “Add to detection”





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

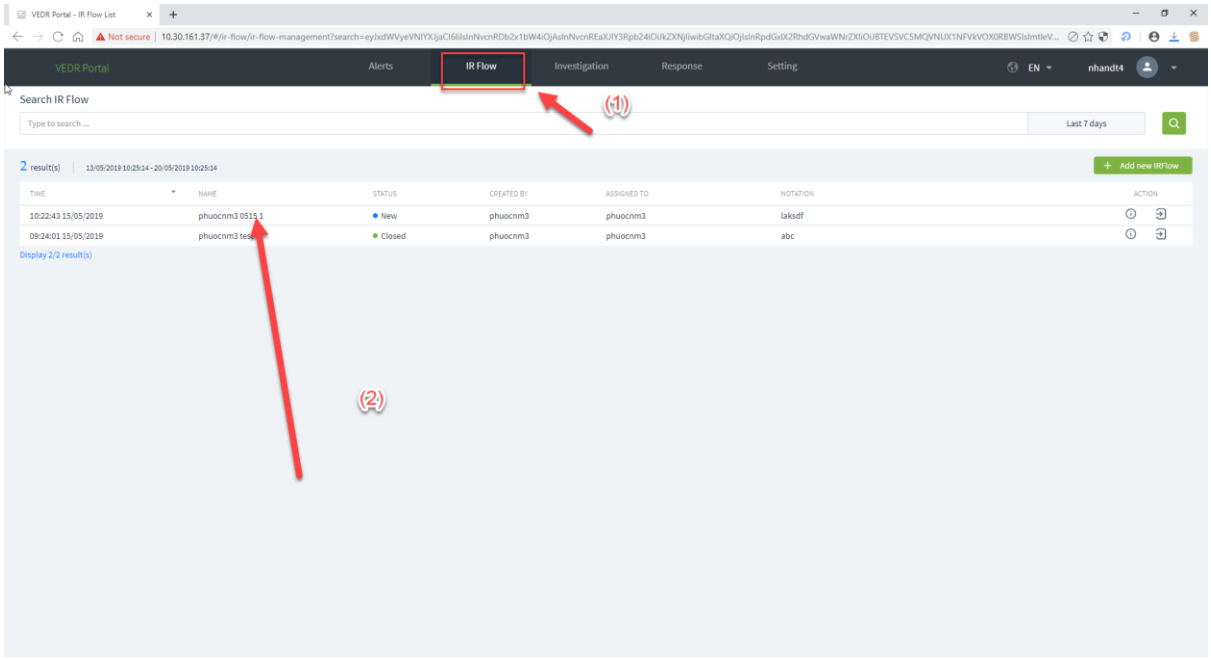


3.5.8. IRFlow – Response

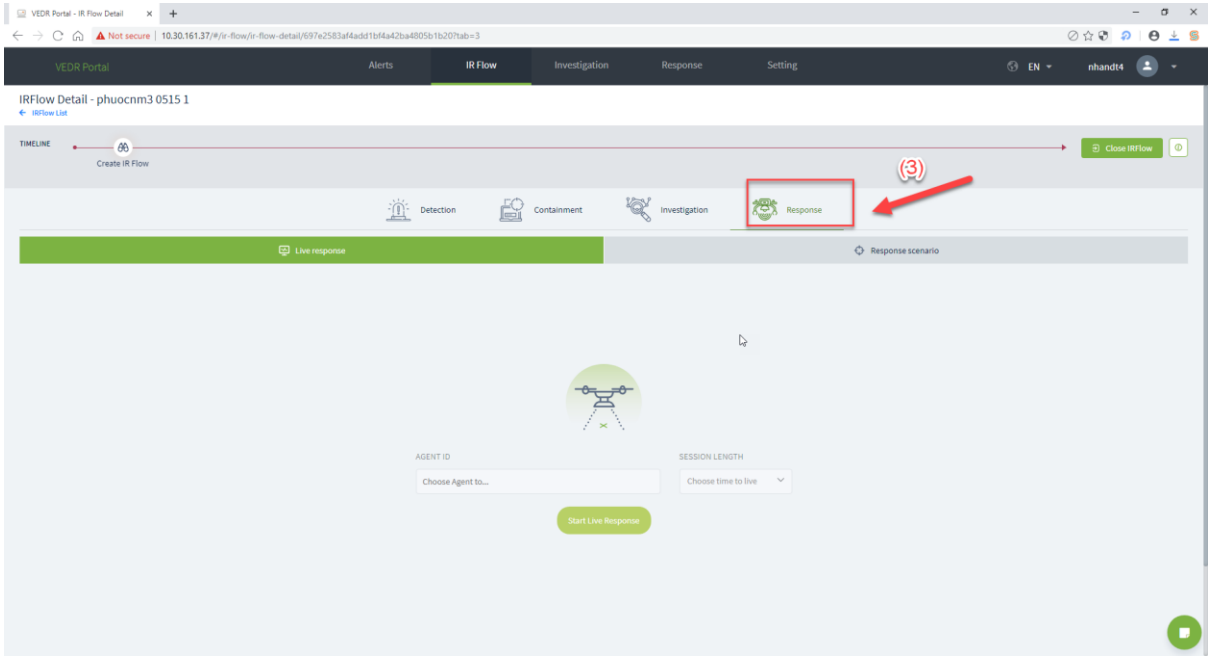
3.5.8.1 Live Response

- Chức năng Live response cung cấp khả năng xử lý một tập các command từ xa theo phiên làm việc nhằm cho biết các thông tin hoặc xử lý yêu cầu trên host.

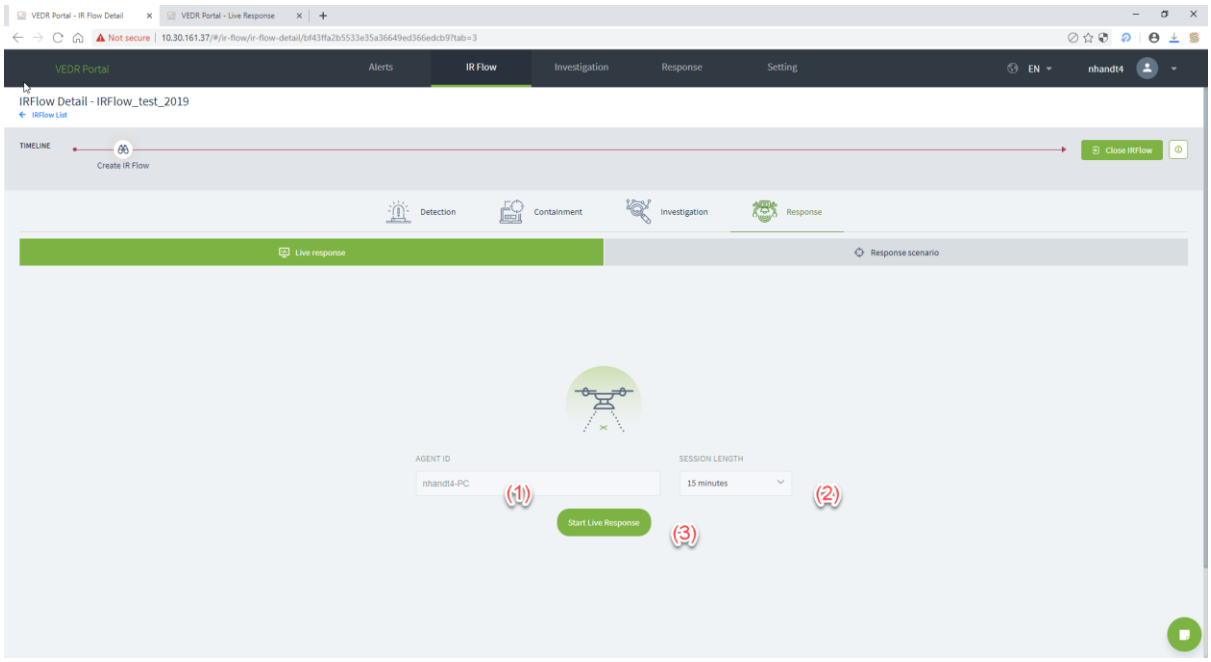
- Các bước thực hiện chức năng Live Response trong IRFlow:
- Bước 1: Click tab IRFlow
- Bước 2: Click duplicate vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Live Response)



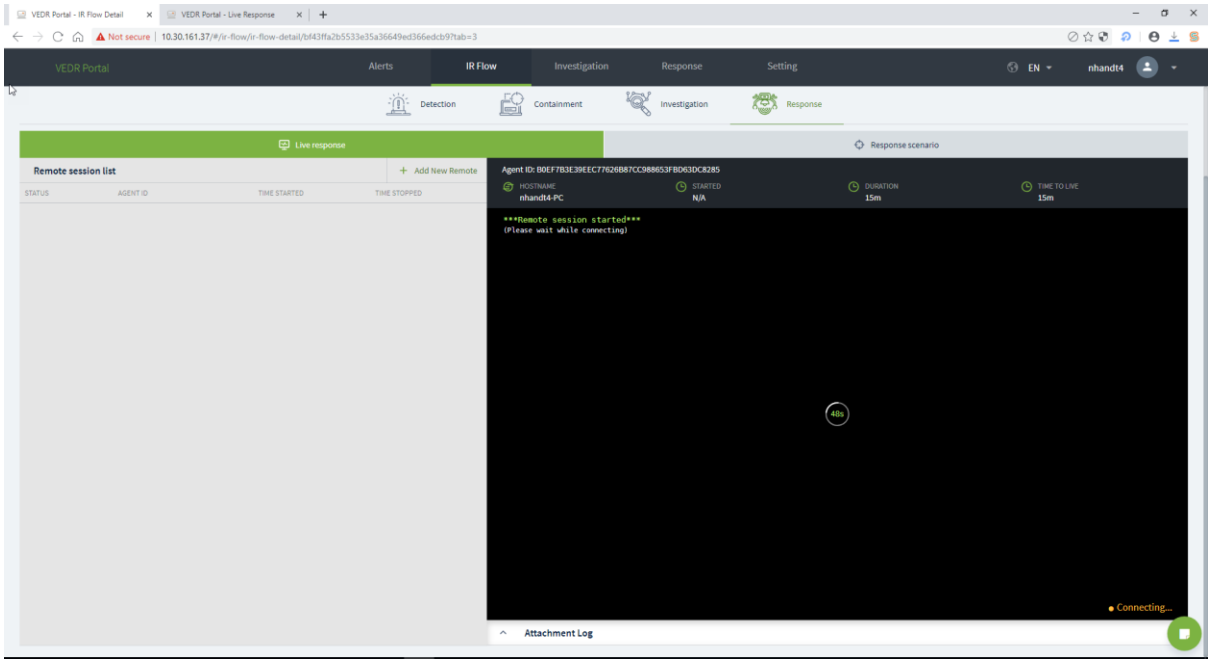
- Bước 3: Click tab con Response



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



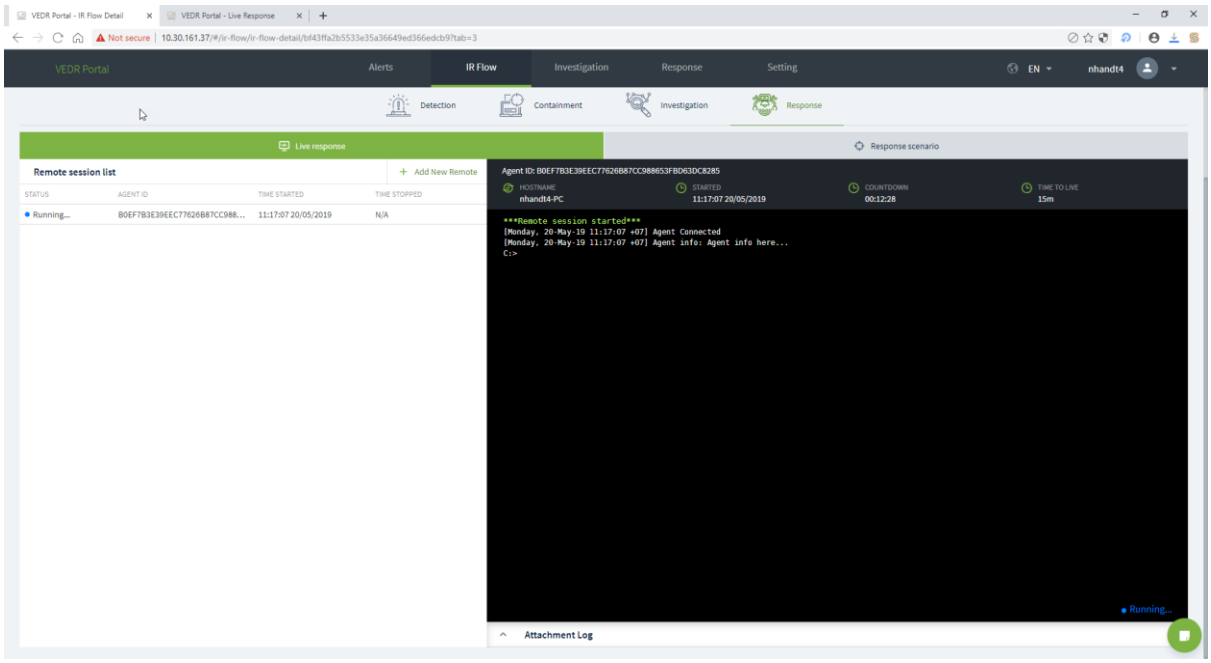
- Sau đó, người dùng cần chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là “connecting”.



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

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

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



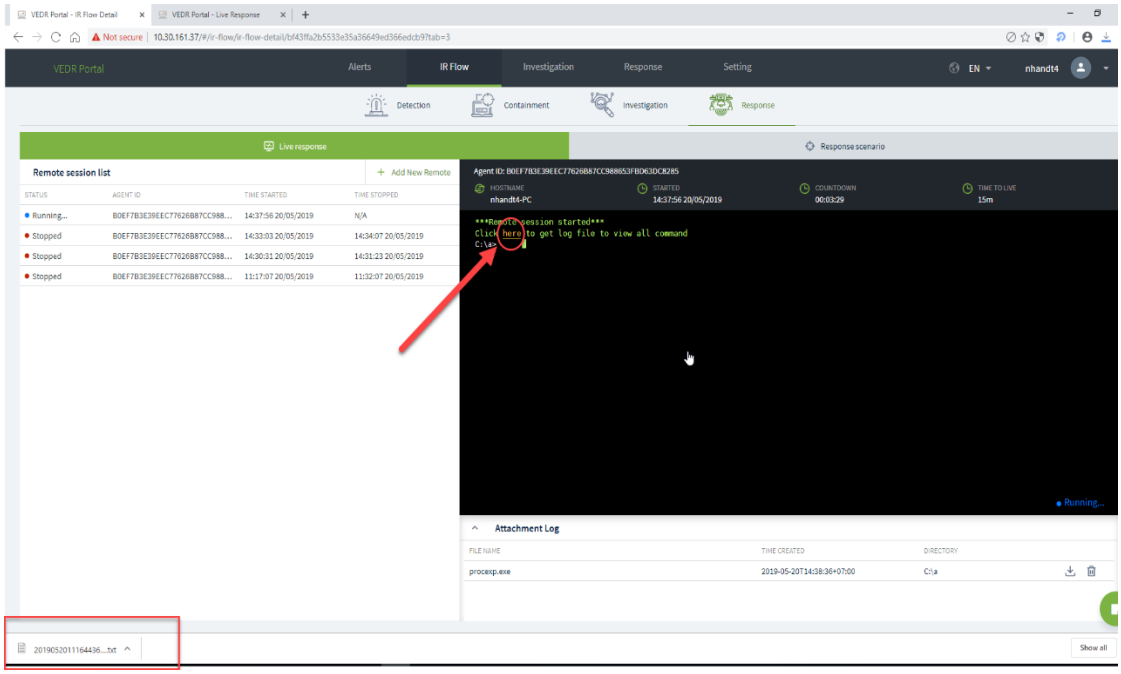
- Người dùng có thể thực hiện các lệnh tại màn hình console như sau:

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

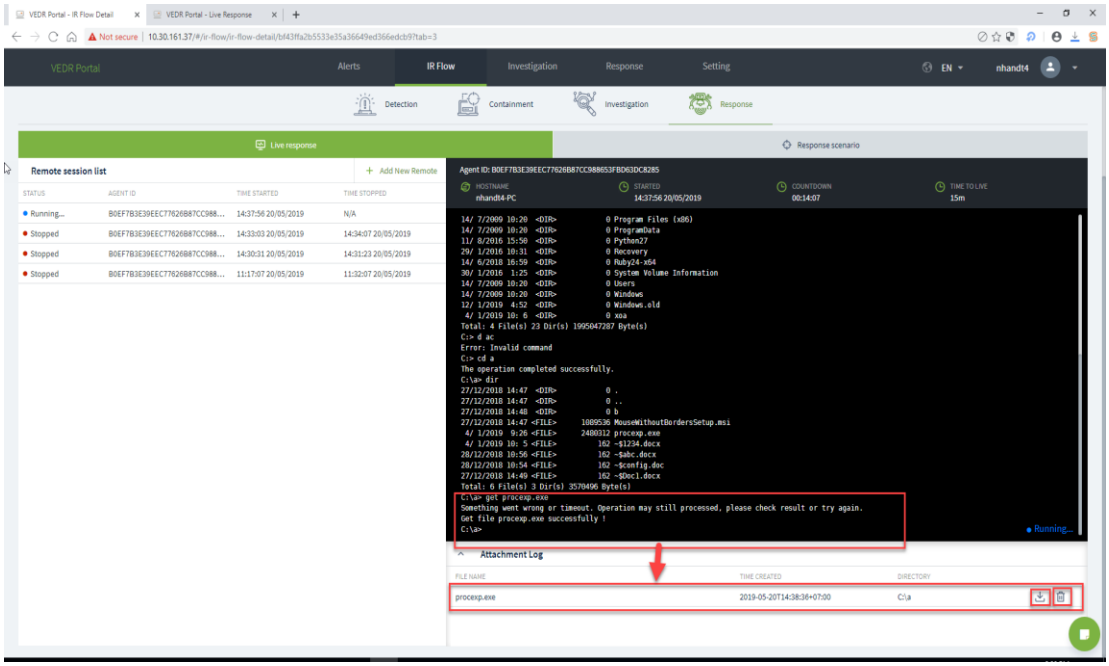
		delete -folder temp\axvers	
		delete –all <folderpath> ví dụ: delete –all c:\temp	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
6	viewfile	<filepath><sizeinbytes>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	get	<filepath>	Upload 1 file từ host lên server
8	put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

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

- Một số lưu ý khi làm việc với các lệnh trên màn hình console:
- Lệnh Clear: Sau khi thực hiện lệnh clear thì hệ thống sẽ hỗ trợ người dùng download toàn bộ log đã thực hiện trên màn hình console trước đấy, bằng thao tác click vào link “here”

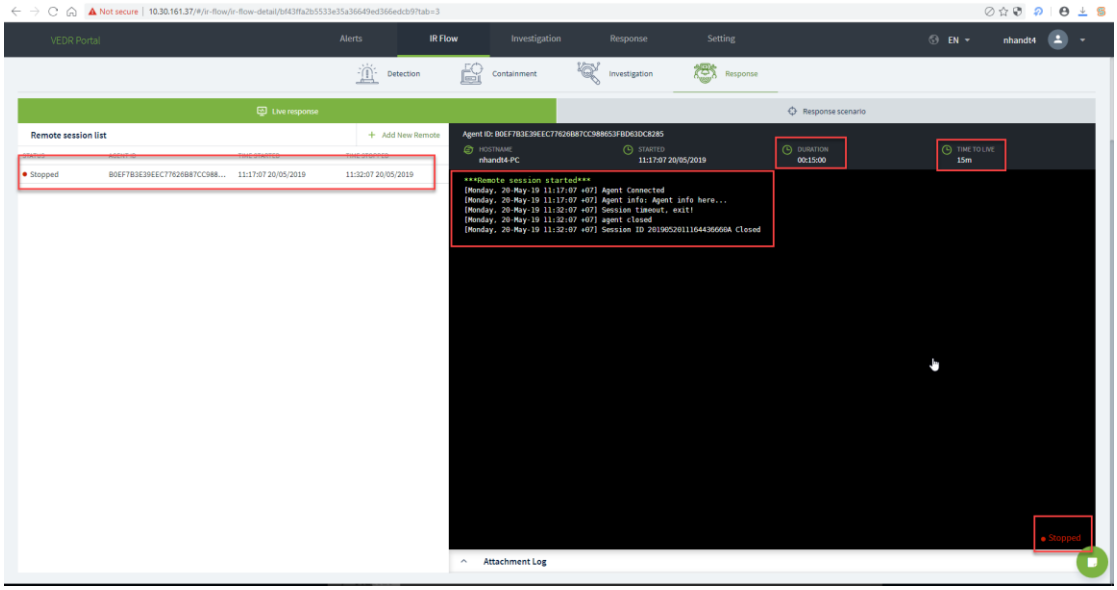


- Lệnh get <filepath>: ví dụ: get procexp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình Attachment Log ở phía dưới góc bên phải của màn hình. Người dùng được phép tải file về trình duyệt hoặc xóa file đã lấy về server.

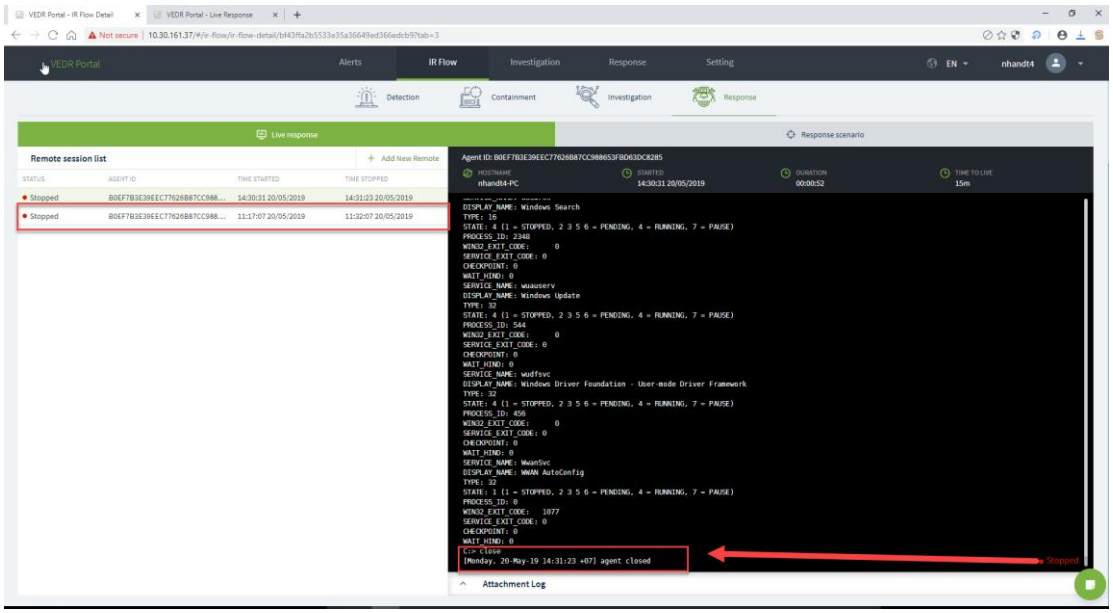


- Bước 6: Phiên làm việc của Live Response kết thúc khi:

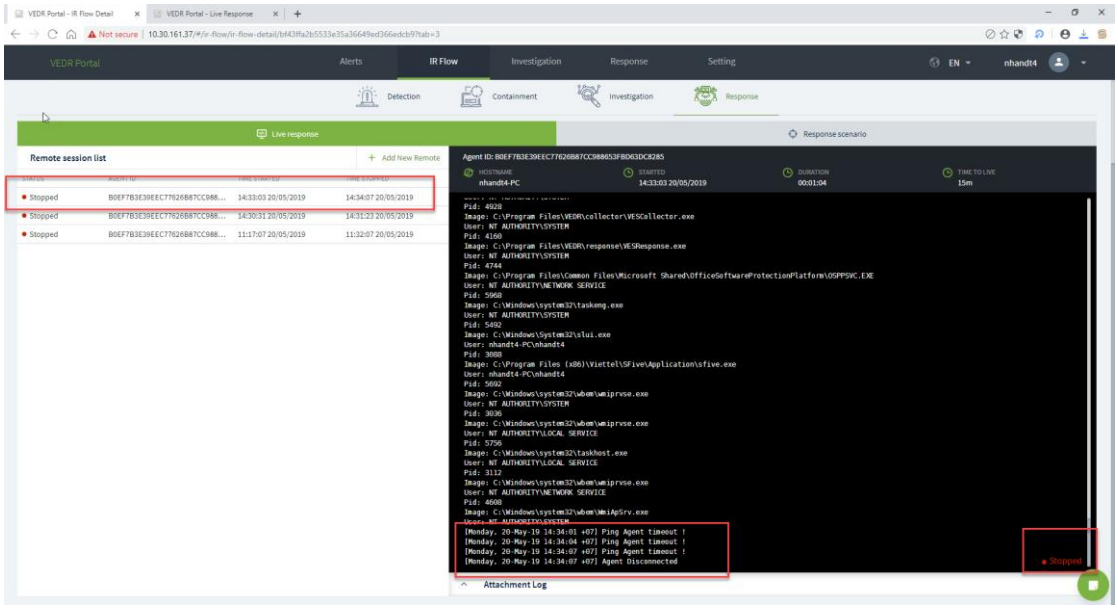
- Thời gian của phiên hết hiệu lực: Khi trường “Duration” bằng thời gian với trường “Time To Live”.



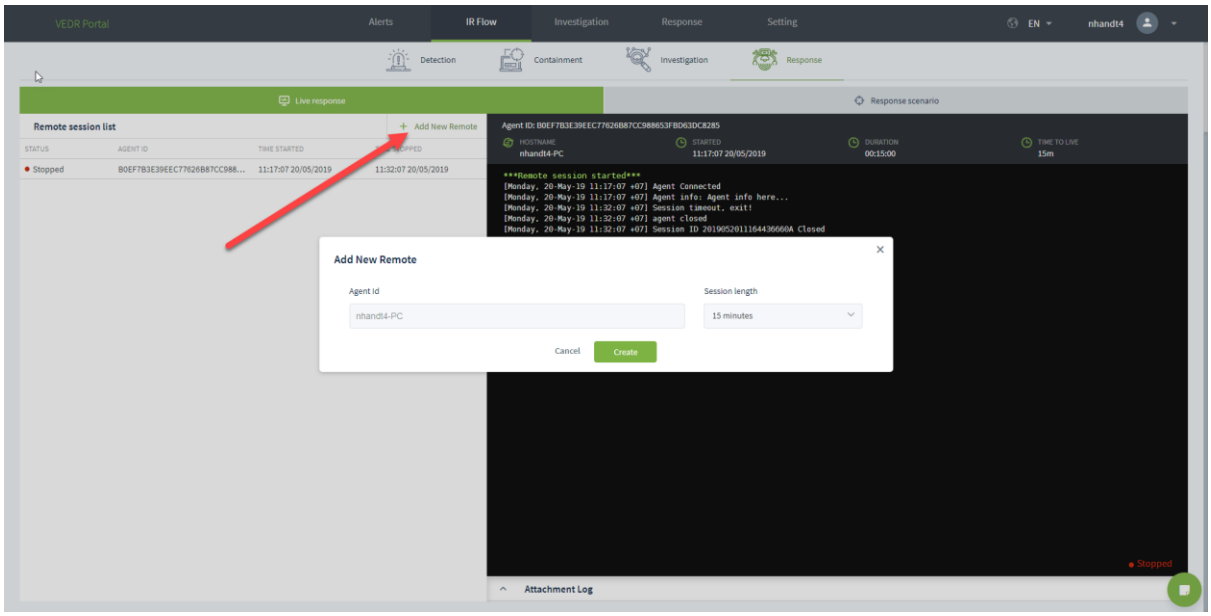
- Người dùng chủ động yêu cầu đóng kết nối bằng lệnh “close”.



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

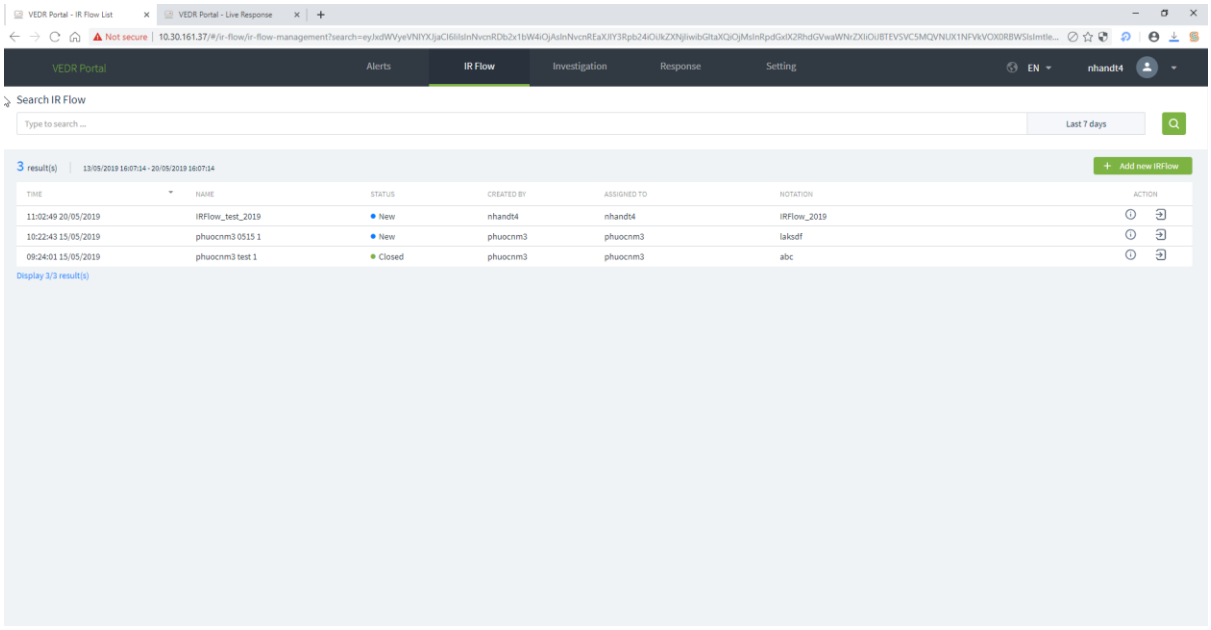


- Ngoài ra, người dùng có thể click nút “+ Add New Remote” để tạo 1 phiên live response mới:

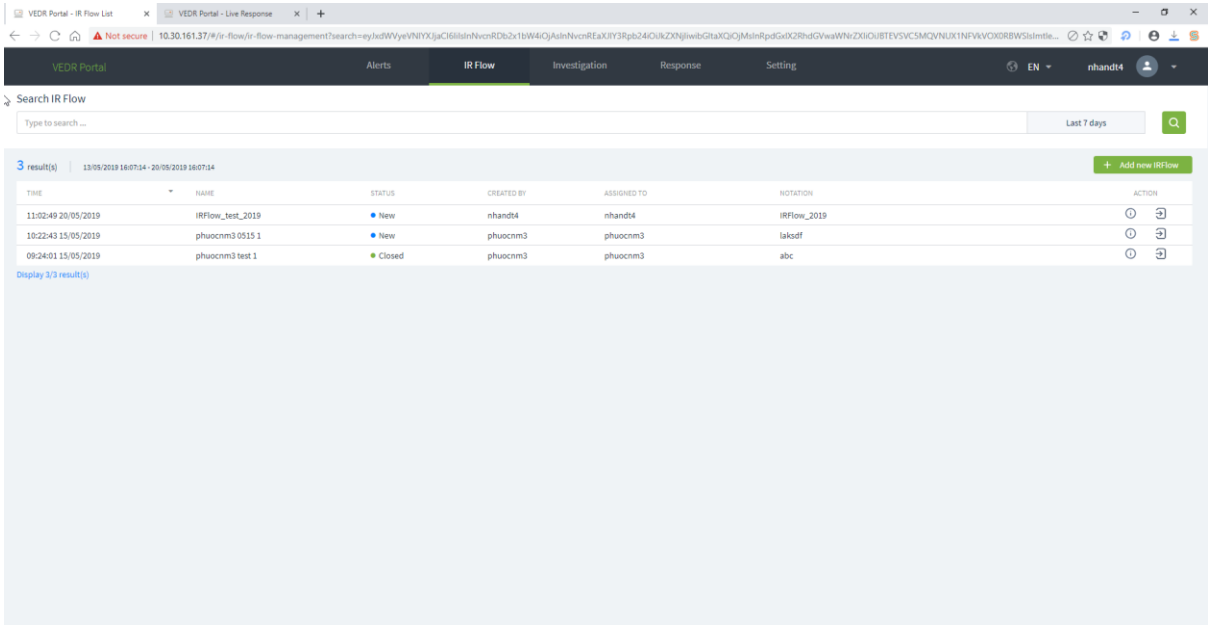


3.5.8.2 Response Scenario

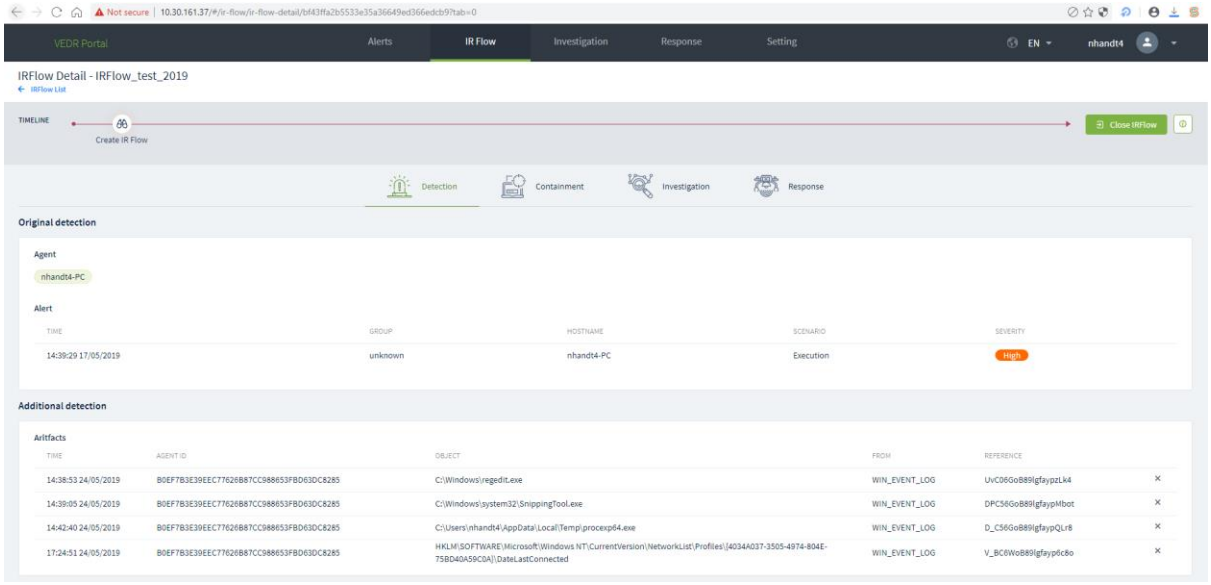
- = Chức năng Response scenario cung cấp khả năng cài đặt một kịch bản Response và thực hiện phản ứng trên một hoặc nhiều Agent.
- Các bước thực hiện chức năng Response Scenario trong IRFlow:
- Bước 1: Click tab IRFlow



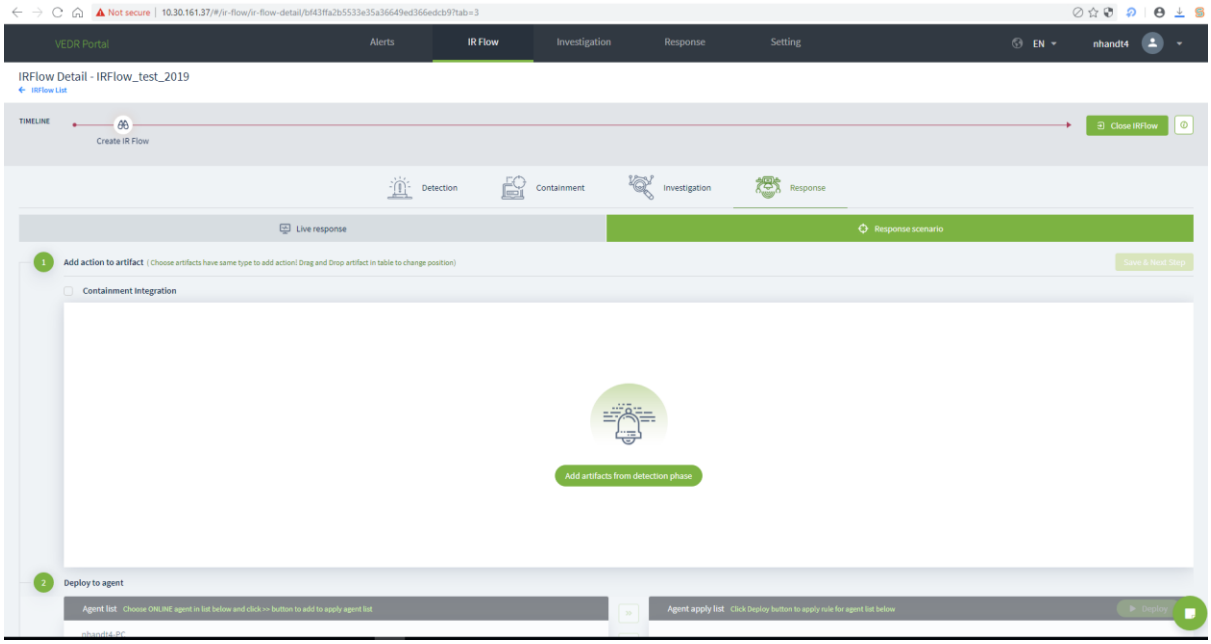
- Bước 2: Click duplicate vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Response Scenario)



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



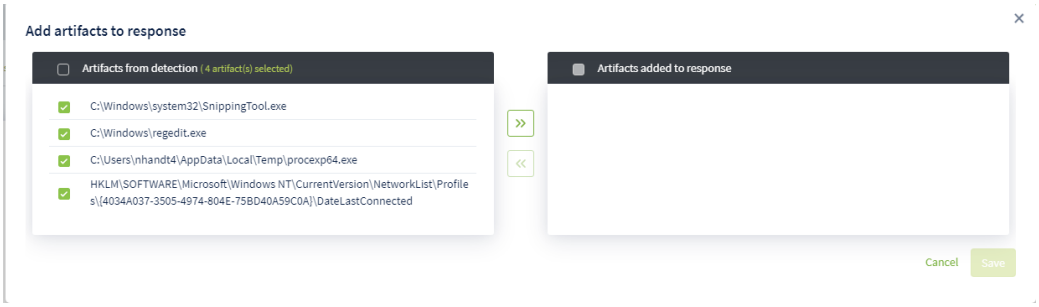
- Bước 3: Click Response Tab >> Response Scenario



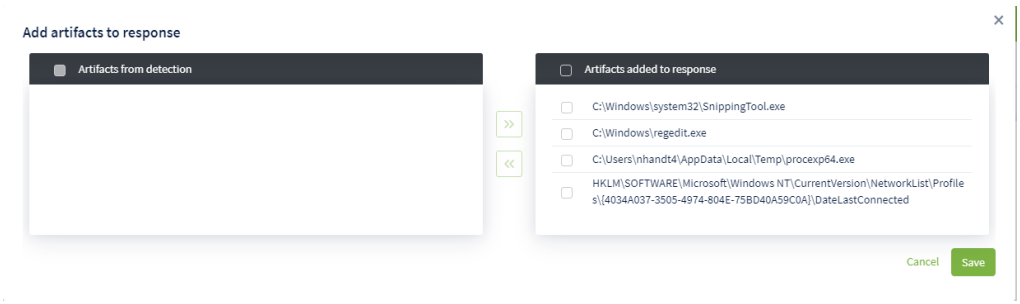
- Bước 4: Thực hiện các cấu hình chi tiết:

  Add action to Artifact

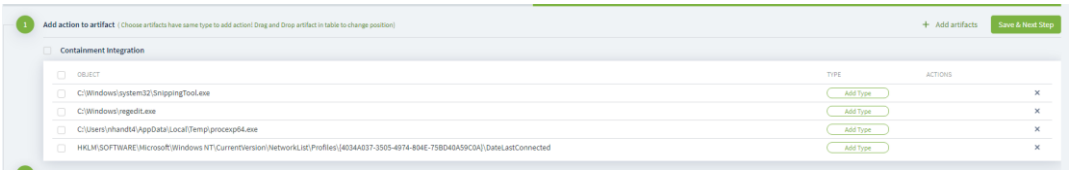
- Click button Add artifacts from detection phase để bắt đầu thêm artifacts vào kịch bản phản ứng.
- Danh sách Artifact hiển thị từ tab Detection



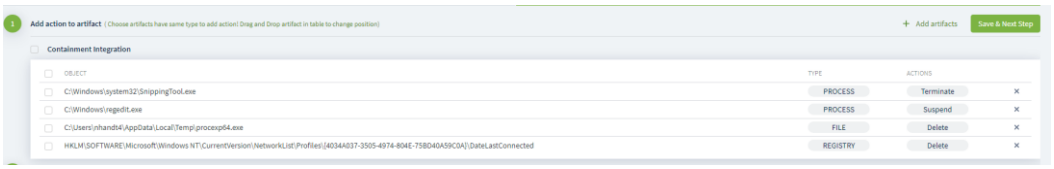
- Click button » để chuyển sang phần các artifact trong kịch bản phản ứng



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

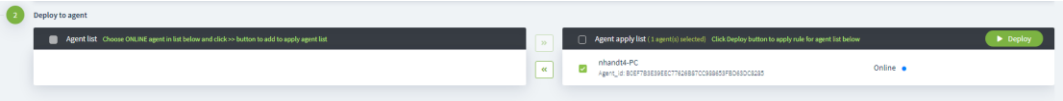


- Lựa chọn Type cho các Artifact. Hệ thống hỗ trợ gán từng type và action cho từng Artifact hoặc 1 type/action cho nhiều Artifact. Có 3 type: File, Process, Registry. Mỗi Type lại có 1 action riêng.

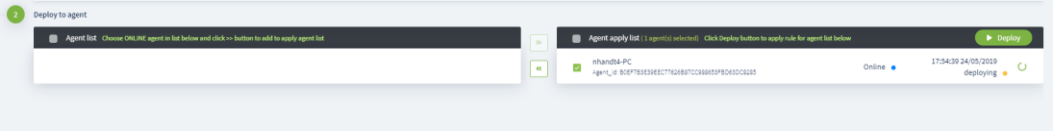


- Sau khi hoàn tất phần gán Type và Action, Click Save & Next Step để lưu và chuyển sang bước tiếp hoặc Click + Add artifacts để tiếp tục thêm Artifact.
- Deploy to Agent: Danh sách Agent được lấy từ tab Detection
- Tích chọn Agent đang online trong List Agent của IRFlow để thực hiện chuyển sang List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

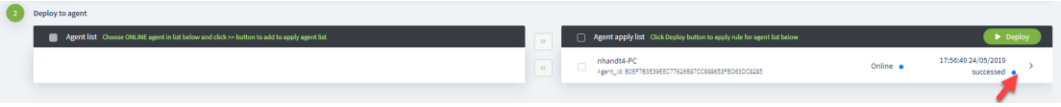
- Click » để chuyển sang List các agent có thể deploy
- Tích chọn Agent để Deploy



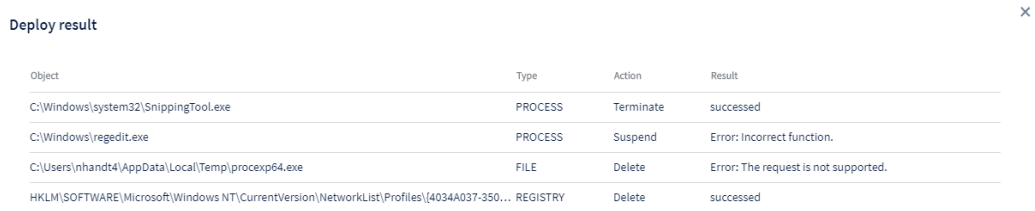
- Bấm nút Deploy
- Sau khi bấm nút Deploy, có các trạng thái:
- Deploying



- Successed



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

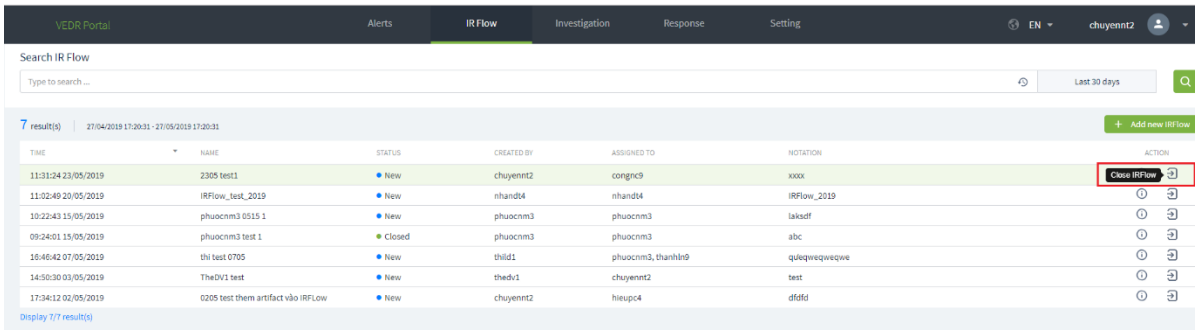


Deploy result

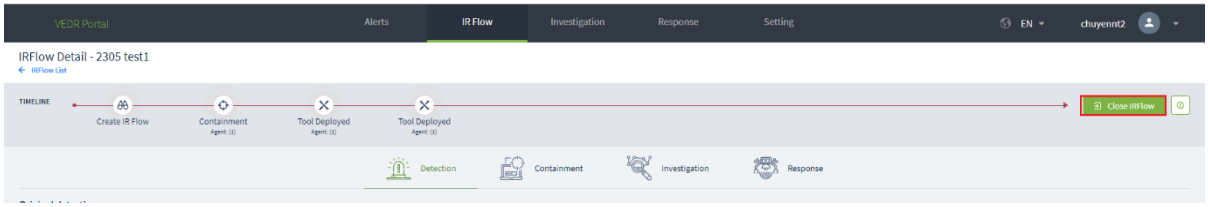
Object	Type	Action	Result
C:\Windows\system32\SnippingTool.exe	PROCESS	Terminate	successed
C:\Windows\regedit.exe	PROCESS	Suspend	Error: Incorrect function.
C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe	FILE	Delete	Error: The request is not supported.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{4034A037-350...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

3.5.9 Close IRFLow

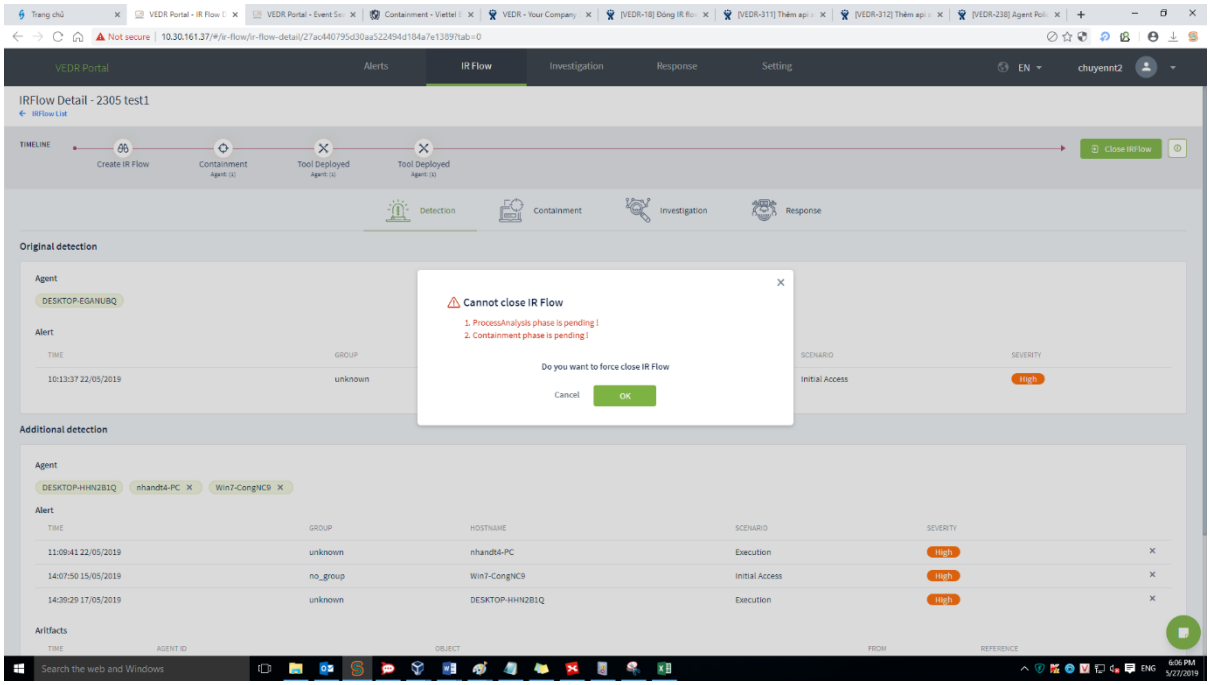
- Đóng IRFLow sau khi đã điều tra và xử lý xong
- Để thực hiện close IRFlow click “Close IRFlow” trên màn hình danh sách IRFLow



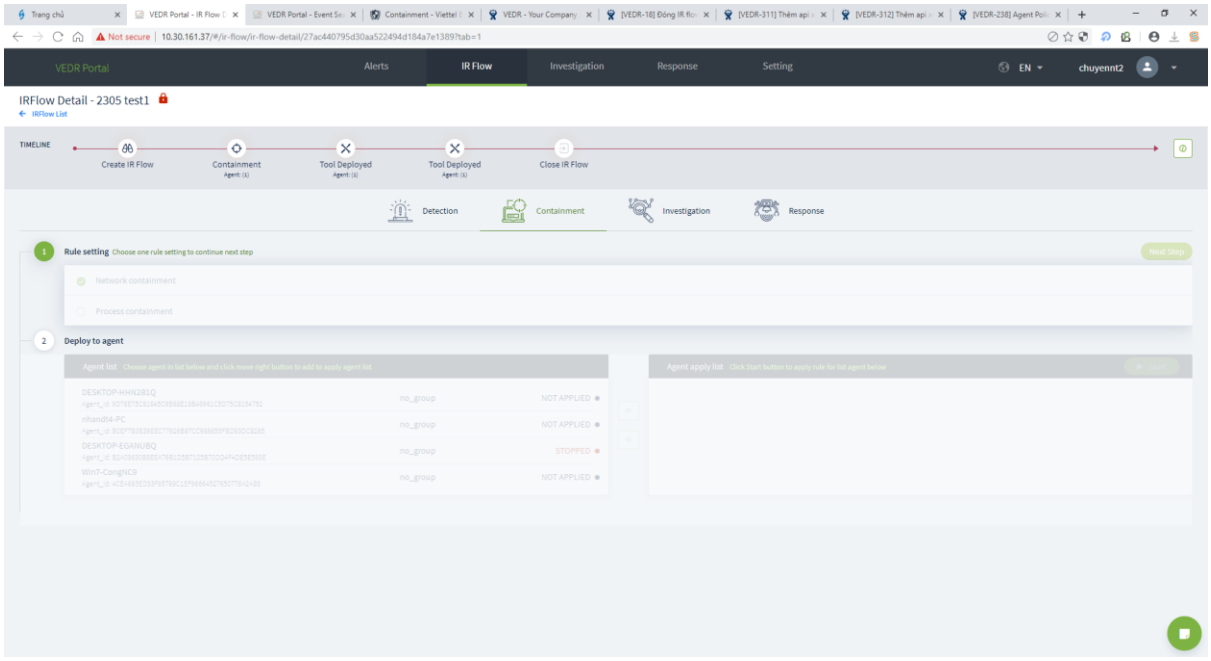
- Hoặc click “Close IRFlow” trên timeline ở bất cứ pha nào trong IRFlow: Detection, Containment, Investigation, Response

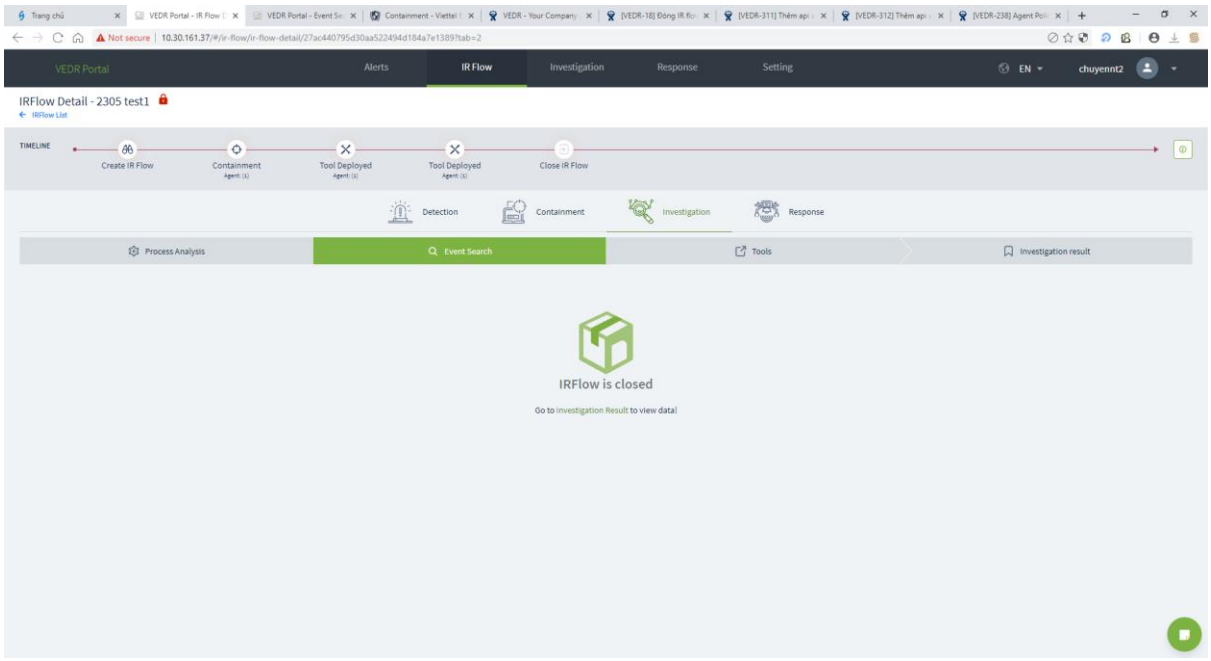


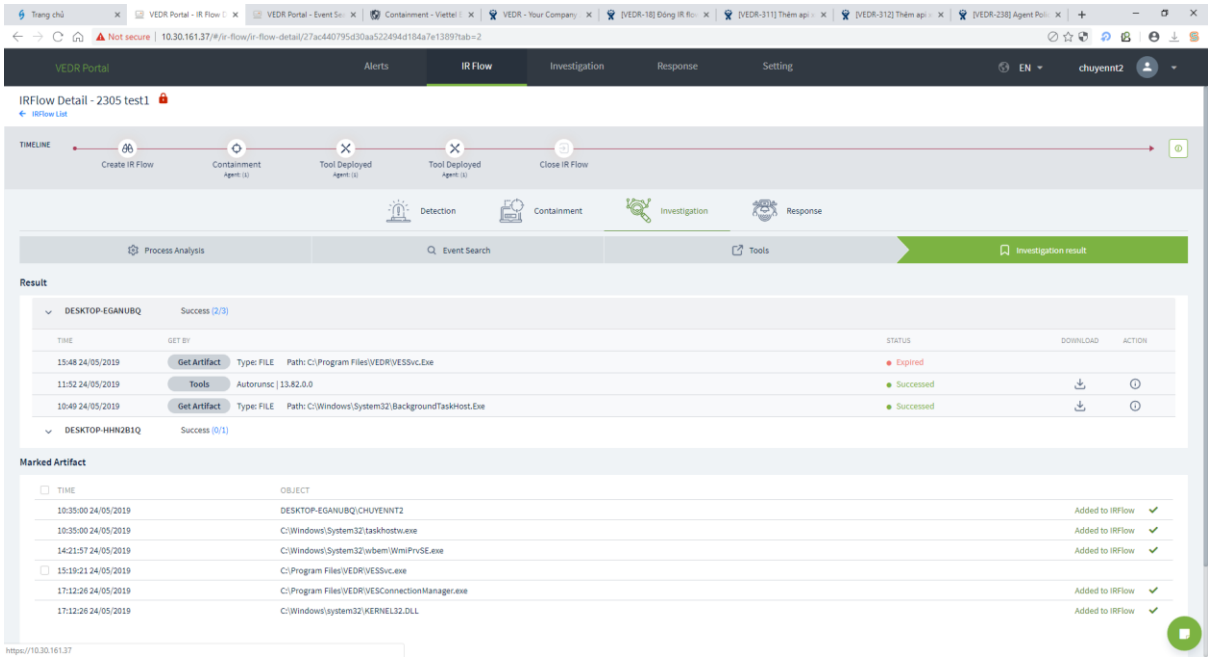
- Nếu khi chọn close IRFLow mà có các tác vụ chưa thực hiện xong như: Containment, Live Response, Response Scenario, Deploy tool… thì sẽ hiện thông báo hỏi người dùng



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


VEDR Portal
Alerts
IR Flow
Investigation
Response
Setting
EN
chuyennt2
IRFlow Detail - 2305 test1
IRFlow List
TIMELINE
Create IR Flow
Containment
Tool Deployed
Tool Deployed
Close IR Flow
Detection
Containment
Investigation
Response
Rule setting
Choose one rule setting to continue next step
Next Step
Network containment
Process containment
Deploy to agent
Agent list
Agent apply list


VEDR Portal
Alerts
IR Flow
Investigation
Response
Setting
EN
chuyennt2
IRFlow Detail - 2305 test1
IRFlow List
TIMELINE
Create IR Flow
Containment
Tool Deployed
Tool Deployed
Close IR Flow
Detection
Containment
Investigation
Response
Process Analysis
Event Search
Tools
Investigation result
IRFlow is closed
Go to Investigation Result to view data!

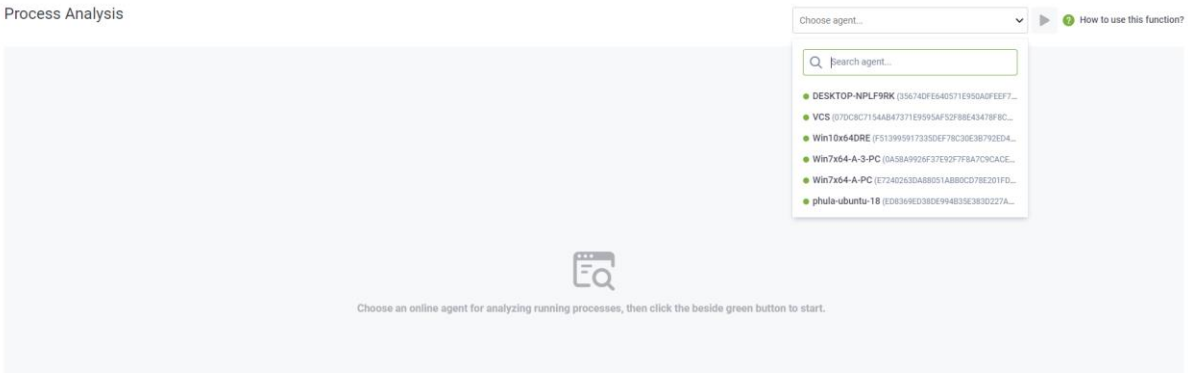


3.6 Màn hình Investigation

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

3.6.1 Investigation_Process Analysis

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



- Danh sách máy người dùng:

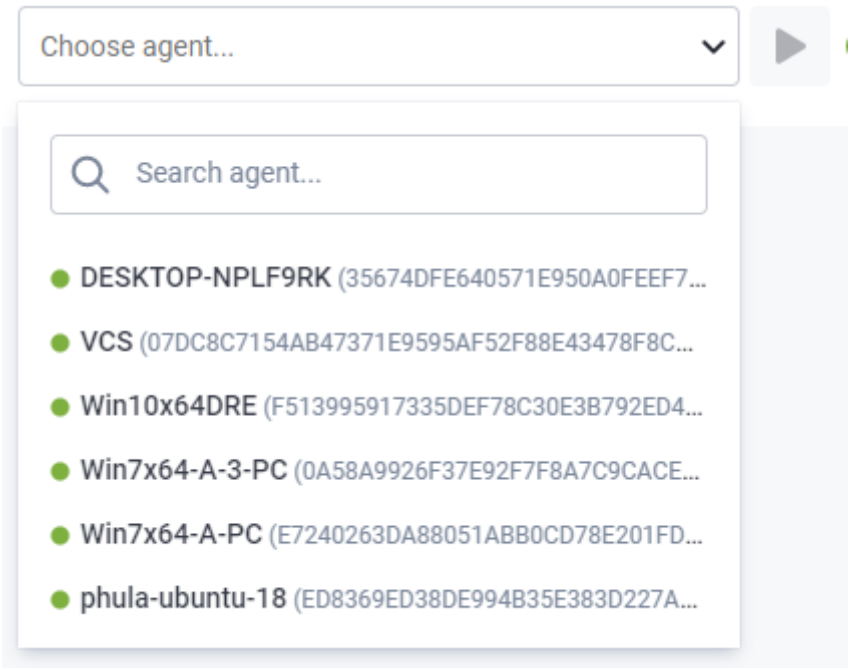
  + User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày

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

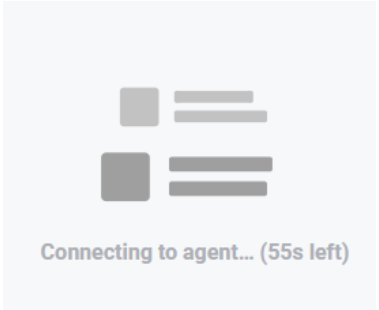
+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng

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

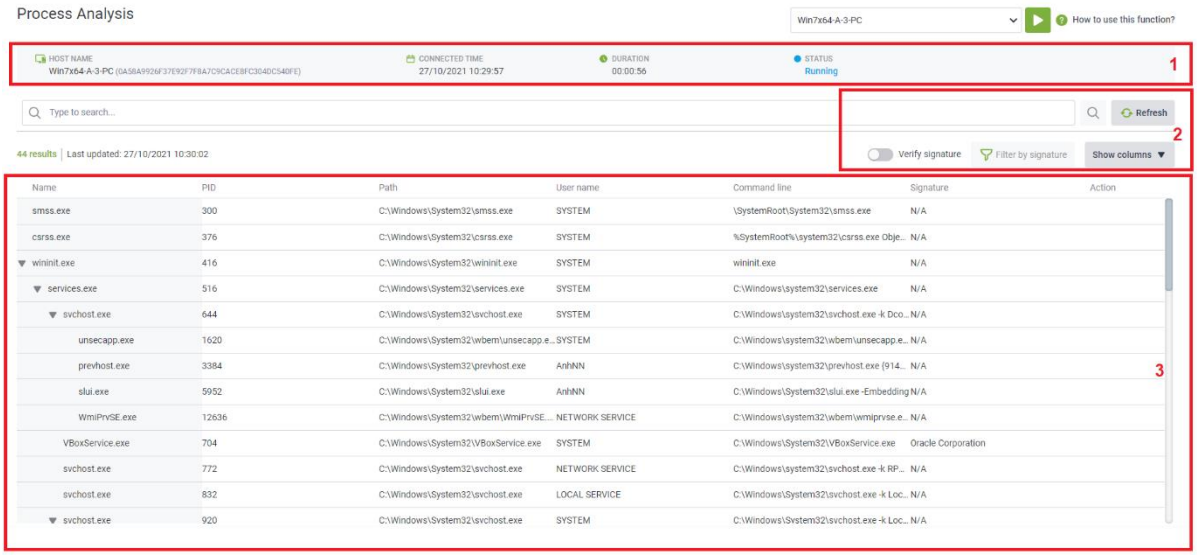
- Bước 1: Tìm kiếm và chọn Agent kết nối (Lưu ý để đảm bao có thể kết nối, danh sách chỉ hiển thị các máy đang Online)



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



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

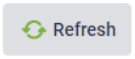


Trong đó giao diện chia làm các nhóm thông tin:

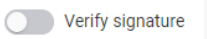
(1) Nhóm thông tin liên quan đến kết nối, bao gồm: Máy đang kết nối, thời gian tạo kết nối, thời lượng kết nối tính đến hiện tại, trạng thá kết nối

(2) Nhóm thông tin hỗ trợ tìm kiếm/làm mới và lọc dữ liệu tại danh sách, bao gồm các thao tác:

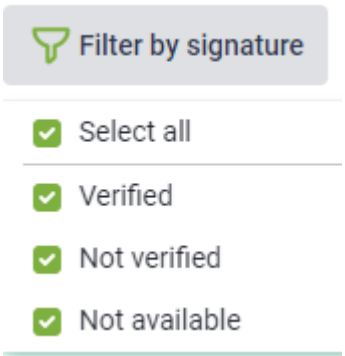
 : Cho phép tìm kiếm theo từ khóa của dữ liệu đang hiển thị trong tất cả các trường trên danh sách



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



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

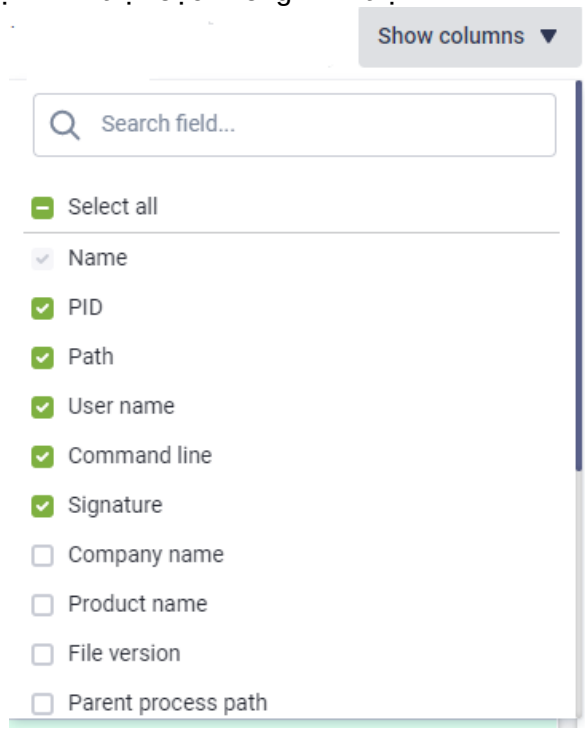


Các trạng thái chữ ký số sẽ quy định màu của bản ghi tương ứng

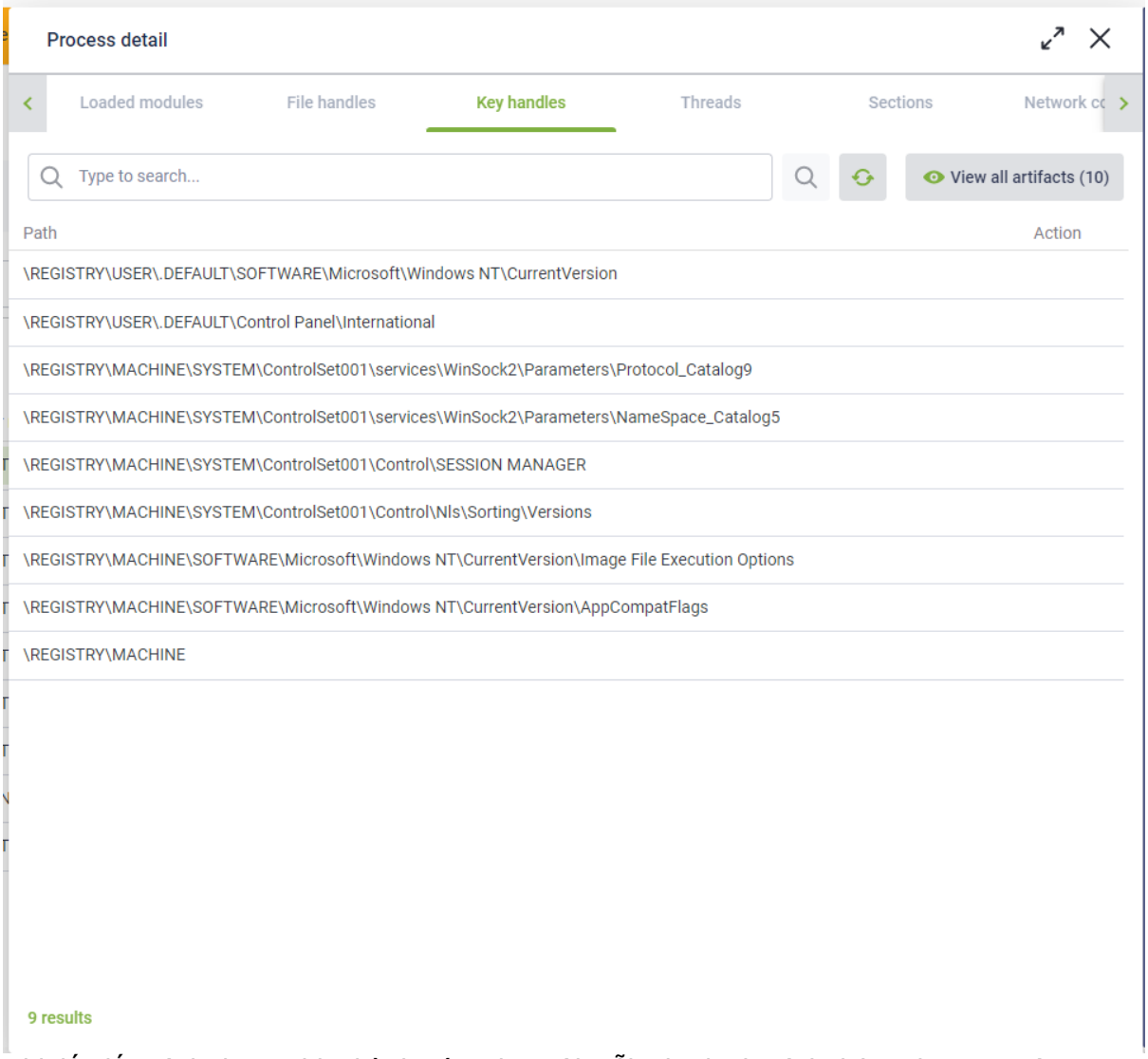
CRYPTSP.dll	C:\Windows\system3...	d0c2fbb6d97416b01...	7eab6c37f0a845e64...	Microsoft Corporation	Microsoft Windows
GDI32.dll	C:\Windows\system3...	1084aa52ccc324ea5...	6e972cf624f7c0de81...	Microsoft Corporation	Microsoft Windows
IMM32.DLL	C:\Windows\system3...	aa2c08ce85653b1a0...	83dfd0c119b20aedb...	Microsoft Corporation	Microsoft Windows
KERNELBASE.dll	C:\Windows\system3...	da68c291b4ef2dec9c...	21aa4779fc21e7621...	Microsoft Corporation	Microsoft Windows
LPK.dll	C:\Windows\system3...	d202223587518b13d...	9db971b866d058adb...	Microsoft Corporation	Microsoft Windows
MSCTF.dll	C:\Windows\system3...	c431eaf5caa1c82cac...	addf850128dc675e6...	Microsoft Corporation	Microsoft Windows
NSI.dll	C:\Windows\system3...	044fe45ffd6ad40e3b...	a1688a5e6e0f7037c...	Microsoft Corporation	Microsoft Windows
PerfCtrl.dll	C:\Program Files\Ajia...	a8a221af714077ec8...	e11aec935d0a34766...	Viettel Corporation	Viettel Group
RPCRT4.dll	C:\Windows\system3...	0611473c1ad9e2d99...	90afcc2a60350ece27...	Microsoft Corporation	Microsoft Windows
USER32.dll	C:\Windows\system3...	fe70103391a64039a...	f7d219d75037bc98f6...	Microsoft Corporation	Microsoft Windows
USP10.dll	C:\Windows\system3...	2f8b1e3ee3545d3b5...	2a3ec01f3bafe7d7d6...	Microsoft Corporation	Microsoft Windows
VESSvc.exe	C:\Program Files\Ajia...	e381c58f04dae8f2a2...	c6510091a2433f918f...	N/A	N/A
advapi32.dll	C:\Windows\system3...	6df46d2bd74e3da1b...	2dc945f6f2c4a82189...	Microsoft Corporation	Microsoft Windows

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

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



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

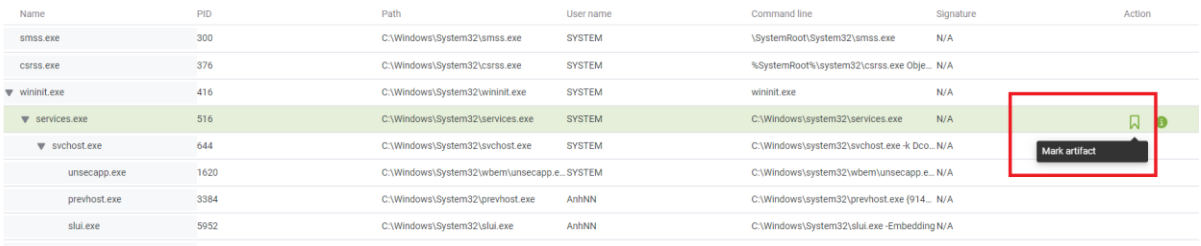


Chi tiết tiến trình được chia thành các tabs, với mỗi tab, danh sách thông tin tương ứng được hiển thị.

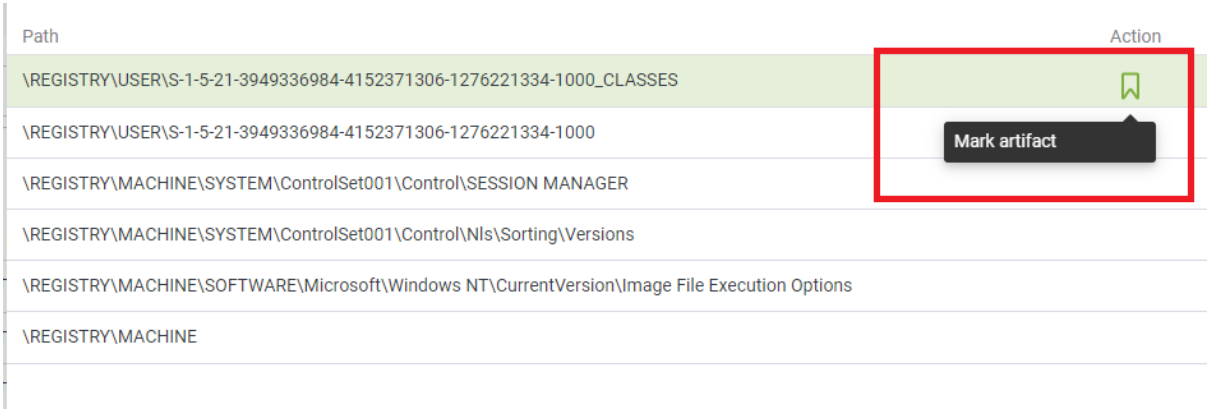
- Bước 3: Marking artifact.

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

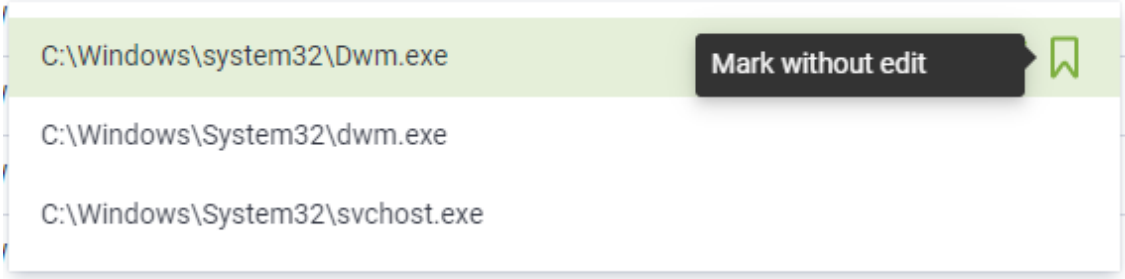
  Người dùng có thể chọn tiến trình từ ngoài danh sách để mark



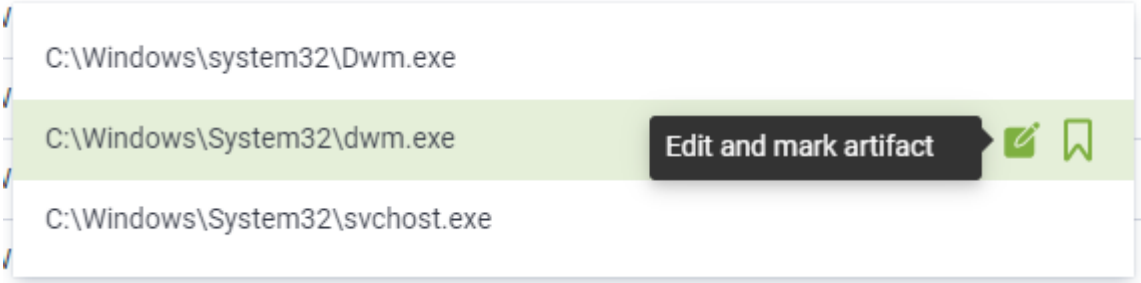
Hoặc mark các đối tượng khả nghi trong chi tiết tiến trình



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

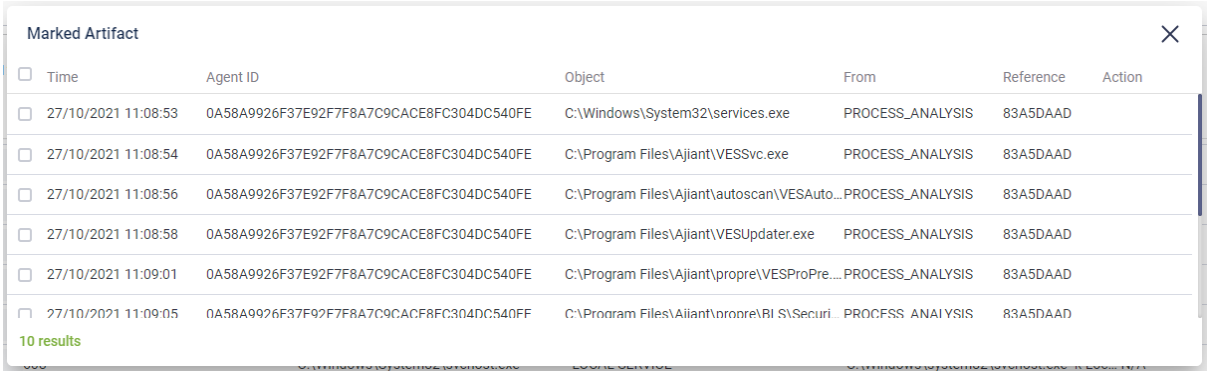


Hoặc người dùng có thể chỉnh sửa nội dung đối tượng trước khi đánh dấu



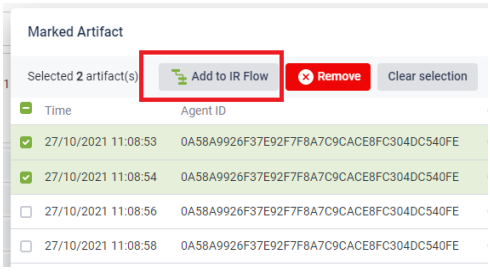
- Sau khi đánh dấu, có thể xem lại danh sách bằng cách click 

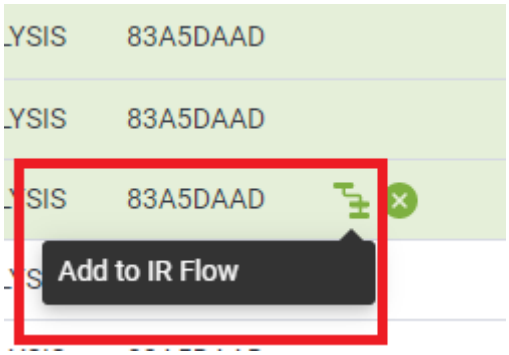
  Lưu ý button này chỉ hiển thị khi có ít nhất 01 artifact được đánh dấu.



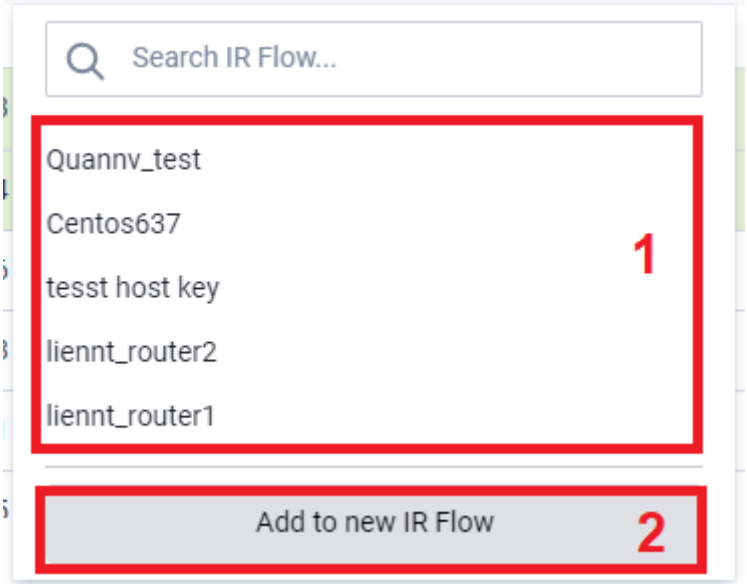
- Bước 4: Thêm artifact vào IRFLow

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





- Lựa chọn IRFlow đã tạo sẵn hoặc tạo mới IRFLow



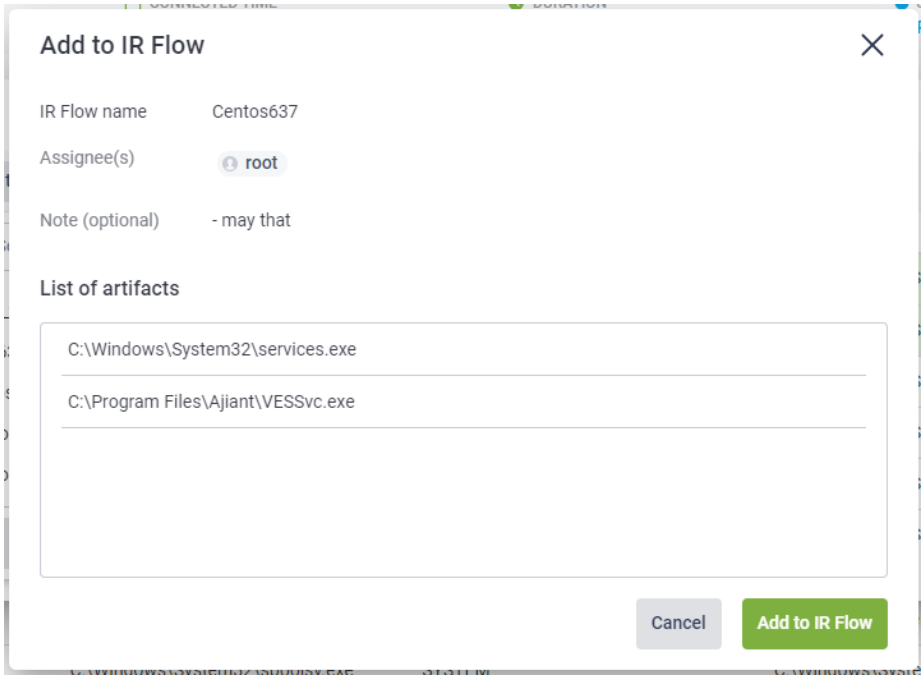
(1) Danh sách IRFlow đã tạo sẵn:

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

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

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

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



- Danh sách assigned to khi tạo mới 1 IRFlow

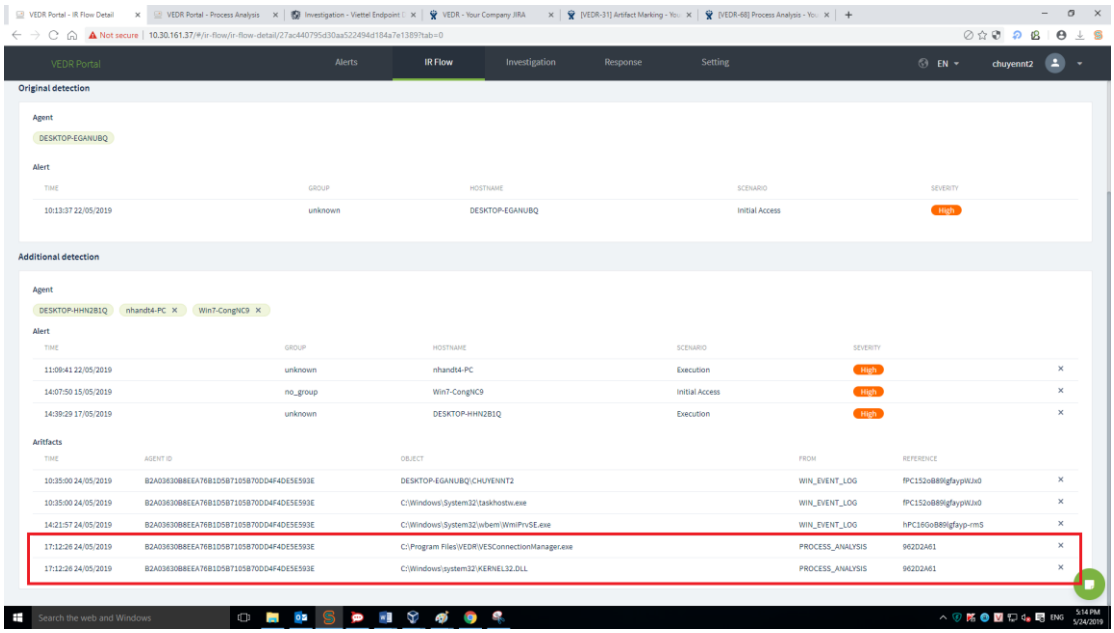
+ User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống

+ User đăng nhập thuộc group default: Hiển thị tên User đang login

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

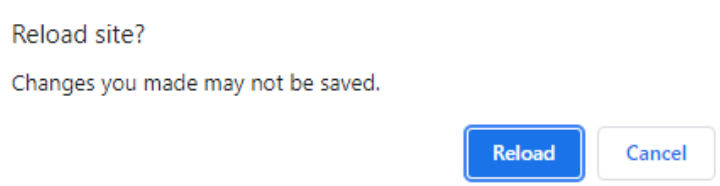
+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tên User đang login

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



- ***Lưu ý:***

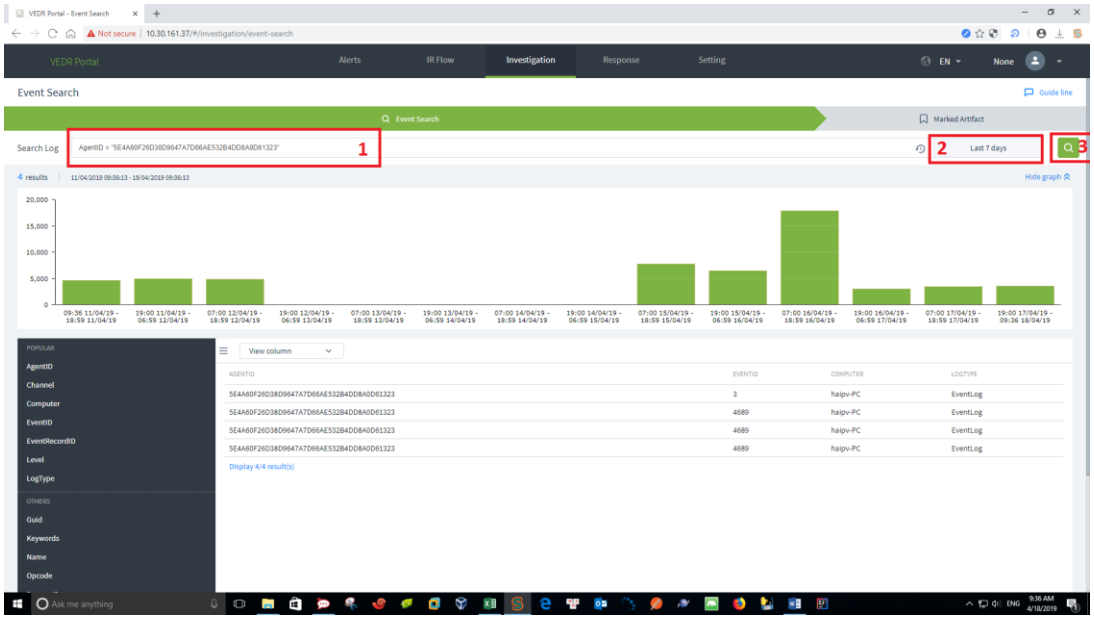
  + Dữ liệu artifacts sẽ không bị mất đi nếu chuyển kết nối đến các máy khác nhau hoặc khi máy hiện tại mất kết nối, trường hợp người dùng tải lại trang hoặc điều hướng đến trang khác, hệ thống yêu cầu xác nhận:



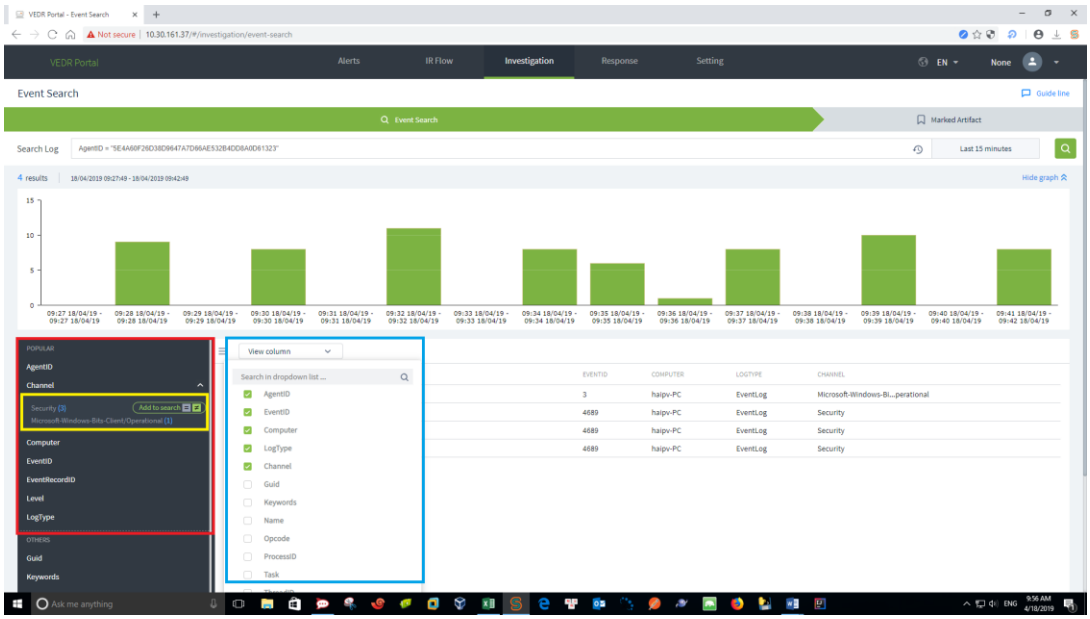
3.6.2 Investigation_Event Search

3.6.2.1 Tìm kiếm Event

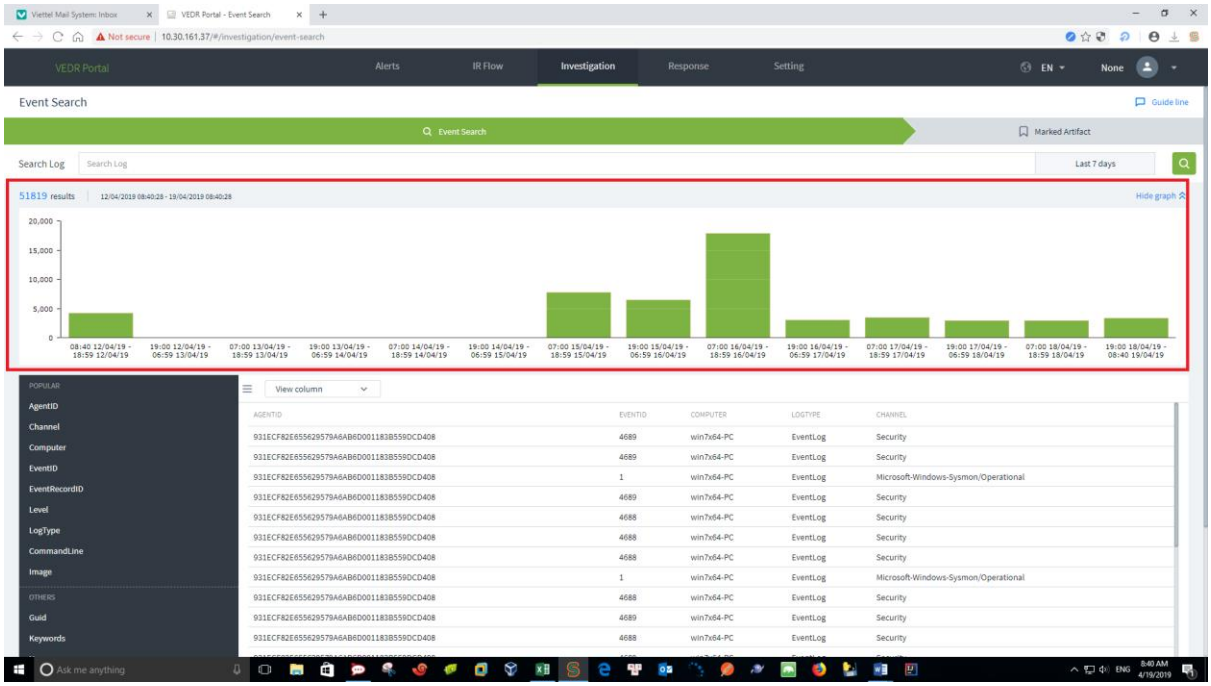
- Chức năng này tương tự trong Event Search của IRFLow:
- Bước 1: Nhập câu query >Chọn khoảng thời gian > Click Search



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



3.6.2.2 Biểu đồ



- Bước 1: Thực hiện tìm kiếm như phần Tìm kiếm event
- Bước 2: Biểu đồ hiển thị thống kê theo khoảng thời gian tìm kiếm. Cách phân chia các khoảng thời gian tương ứng với các cột trên biểu đồ như sau:

  + Thống kê >= 90 ngày, chia 30 khoảng thống kê

  + Thống kê events trong 60 ngày gần đây, thì chia thành 20 khoảng, mỗi khoảng thống kê số event trong 3 ngày

  + Thống kê 30 ngày, chia 15 khoảng, mỗi khoảng 2 ngày

  + Thống kê 7 ngày, chia 14 khoảng, mỗi khoảng 12 giờ

  + Thống kê 1 ngày, chia thành 24 khoảng, mỗi khoảng 1 giờ

  + Thống kê 12 giờ, chia 12 khoảng, mỗi khoảng 1 giờ

  + Thống kê 6 giờ, chia 12 khoảng, mỗi khoảng 30 phút

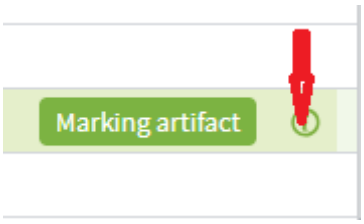
  + Thống kê 1 giờ, chia thành 12 khoảng, mỗi khoảng 5 phút

  + Thống kê 30 phút, chia 15 khoảng, mỗi khoảng 2 phút

  + Dưới 30 phút, chia thành các khoảng thời gian 1 phút
- Khi hover vào mỗi cột sẽ hiển thị Khoảng thời gian và số lượng bản ghi tìm kiếm được trong khoảng thời gian đó.
- *Lưu ý:* Các mốc thời gian trên chart là các thời điểm tính tròn theo ngày/giờ/phút cho phù hợp khoảng thời gian thống kê dài hay ngắn.

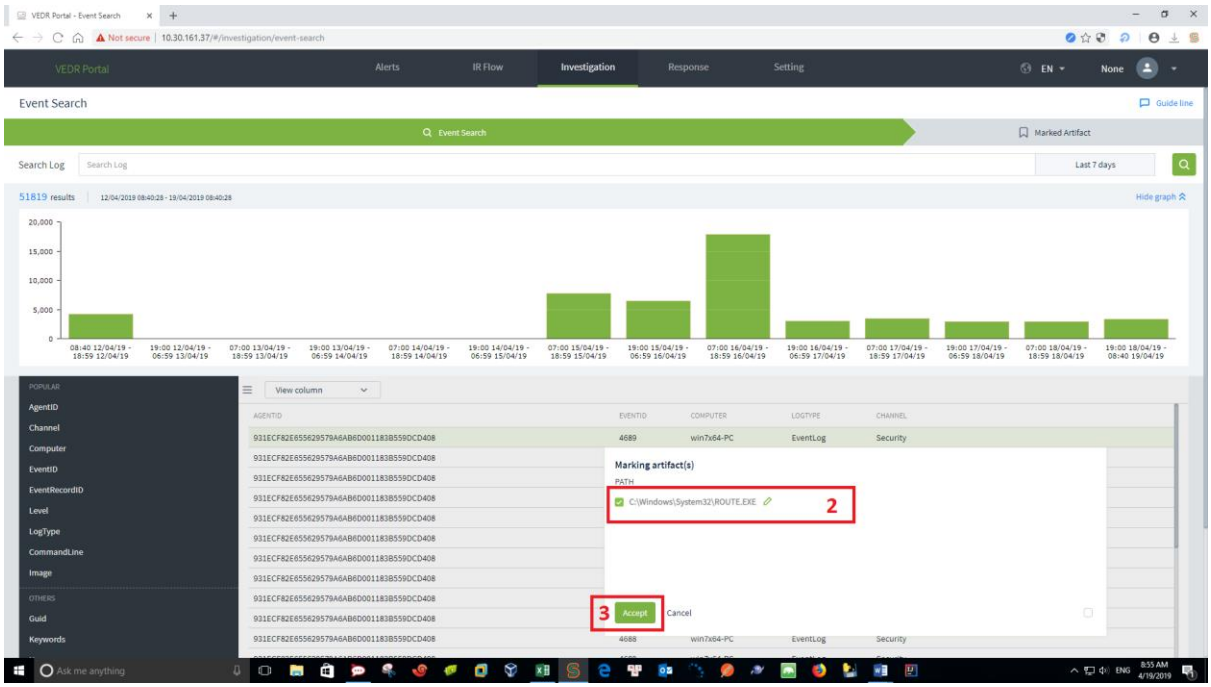
3.6.2.3 Xử lý Event

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



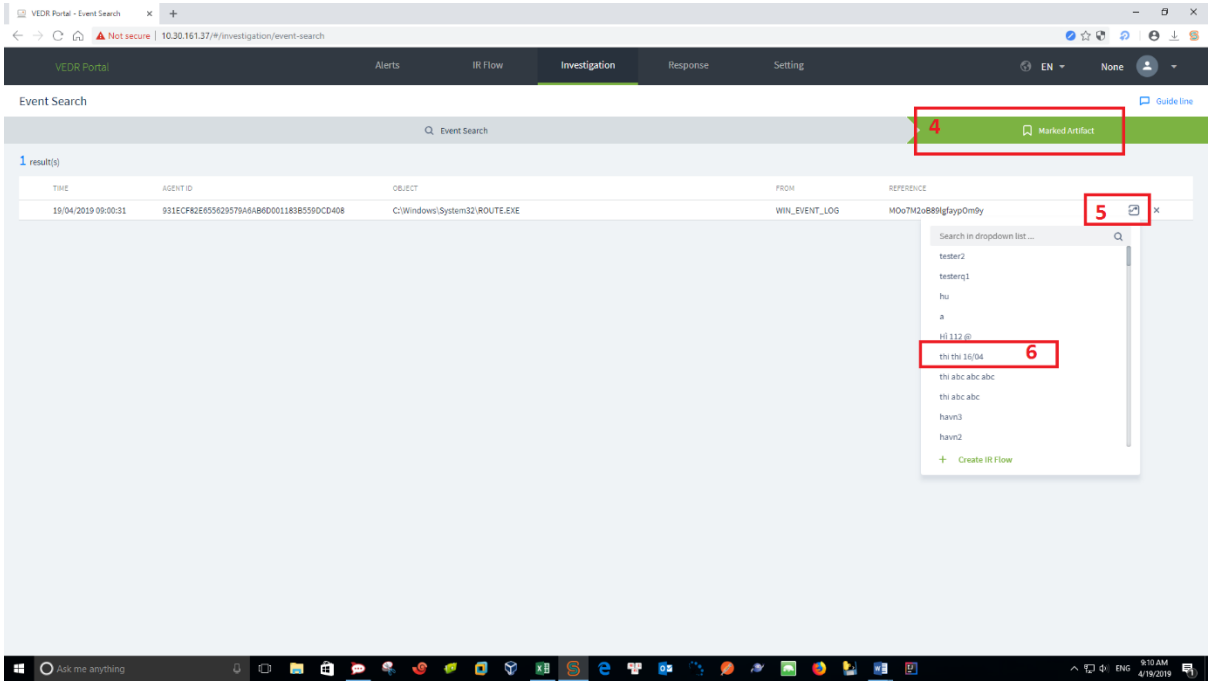
- Marking artifact: Hover vào 1 bản ghi và chọn “Marking artifact”

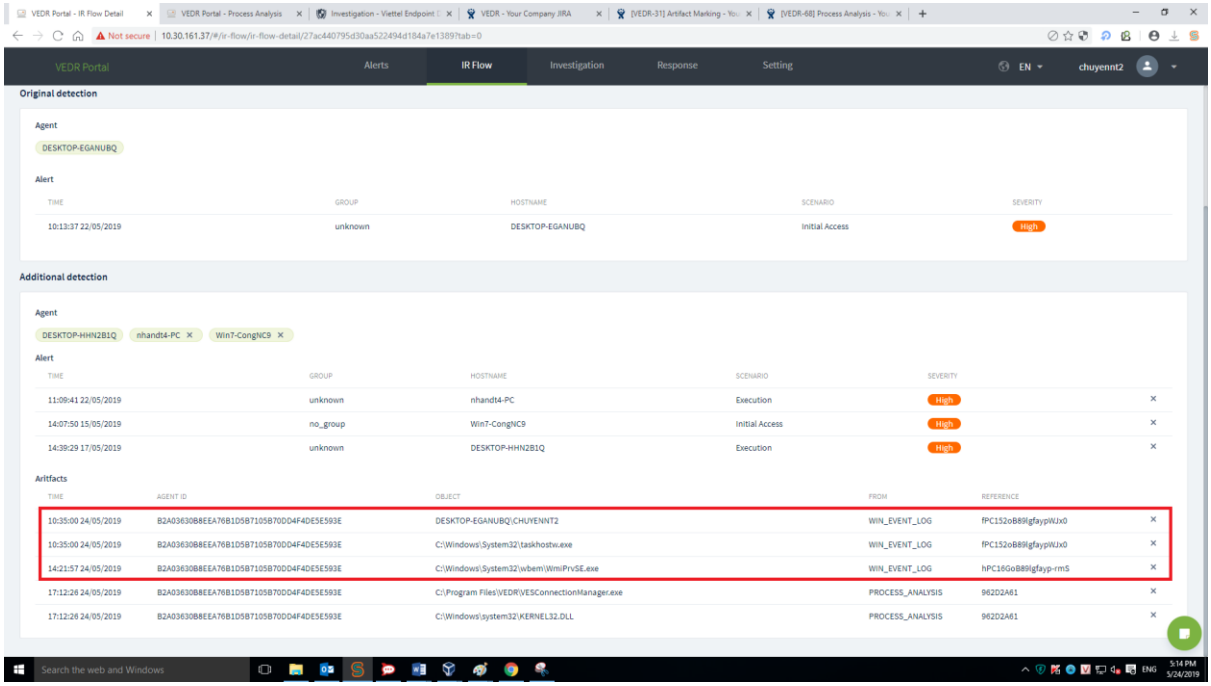
- Lựa chọn path và click “Accept”



Hình 2: Investigation/Event Search_Marking artifact

- Chọn IRFlow và add artifact đó vào Irflow





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

+ Nếu thực hiện chuyển tab giữa Event Search và Marked artifact thì dữ liệu màn Marked artifact sẽ không bị mất đi

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

3.6.3 Investigation_Deploy Tools

3.6.3.1 Tool Management

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

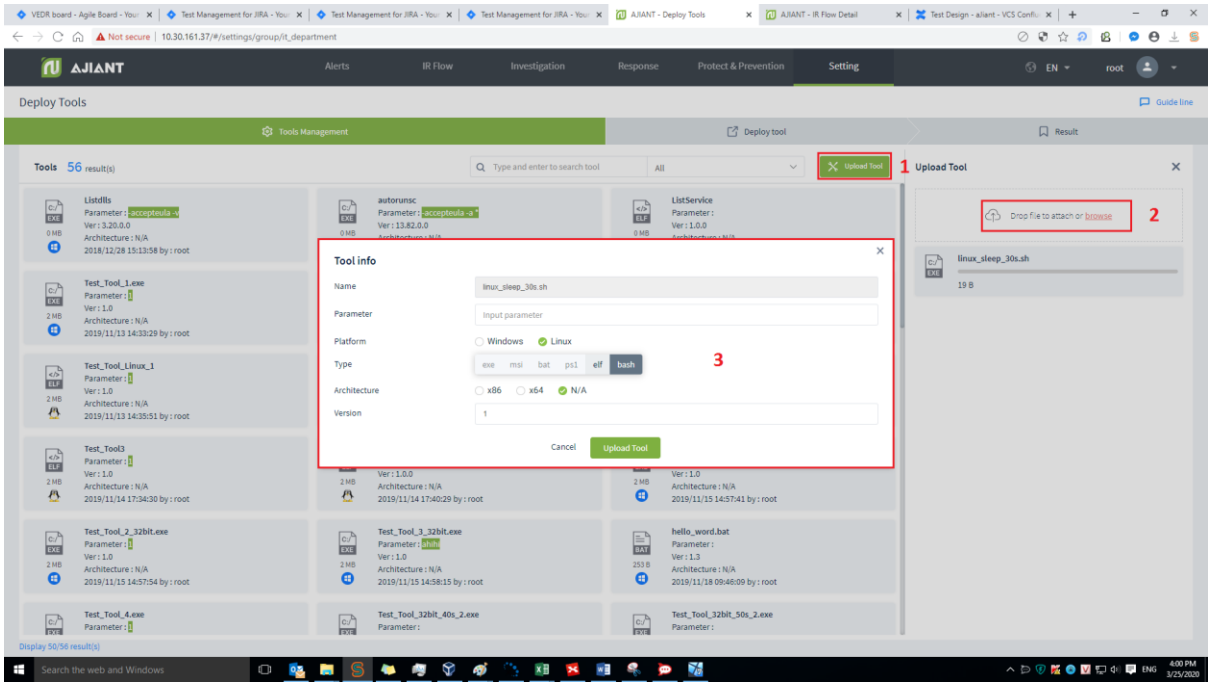
  + Hiển thị danh sách tool cùng các thông tin chi tiết của tool: Tên, Parameter, Version, Architecture, Upload User, Platform, mã Hash.

  + Tìm kiếm tool: Tìm kiếm theo nhiều tiêu chí như All (toàn bộ các trường dữ liệu), theo Name (tên tool), Tool ID, Version, SHA1, Upload User, Platform.

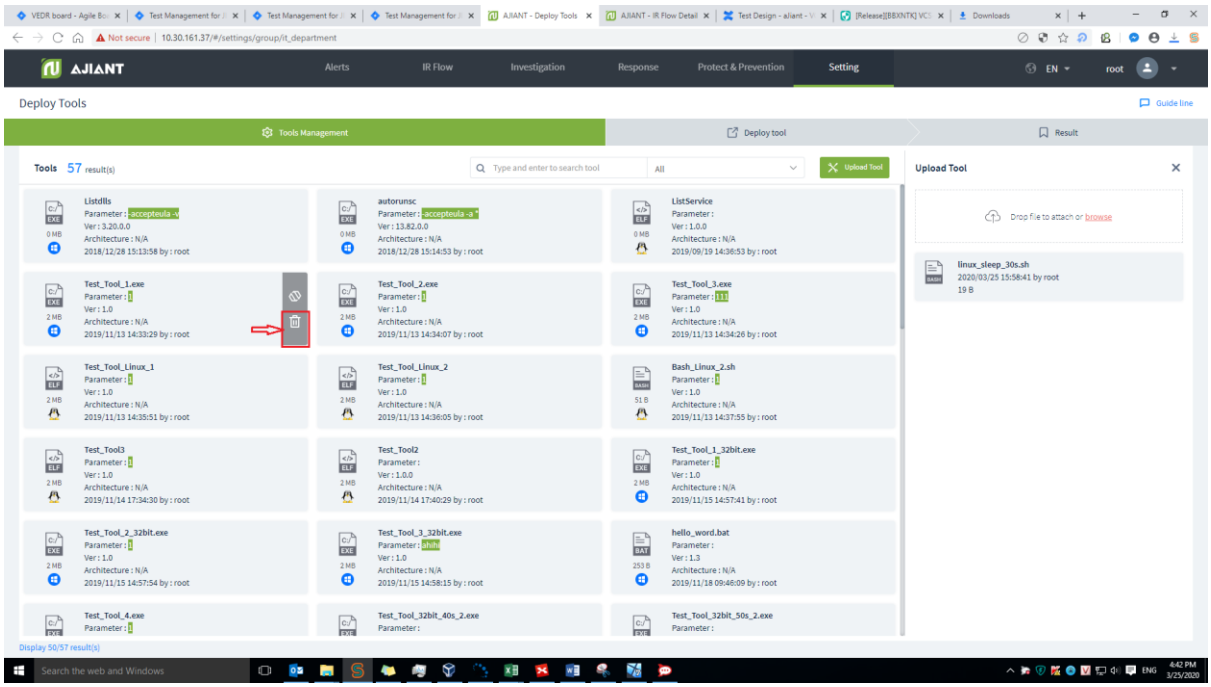
  + Upload tool: upload tool chạy trên agent Windows và Linux có dung lượng tối đa 10MB

  Xóa tool

- Với tính năng Upload tool thao tác theo các bước sau:
- Click vào “Upload tool” > Chọn đường dẫn đến tool cần upload hoặc kéo thả tool vào giao diện > Nhập thông tin vào popup Tool info > click “Upload tool”



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



3.6.3.2 Deploy tool

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

Tuy nhiên có 1 số điểm khác như sau:

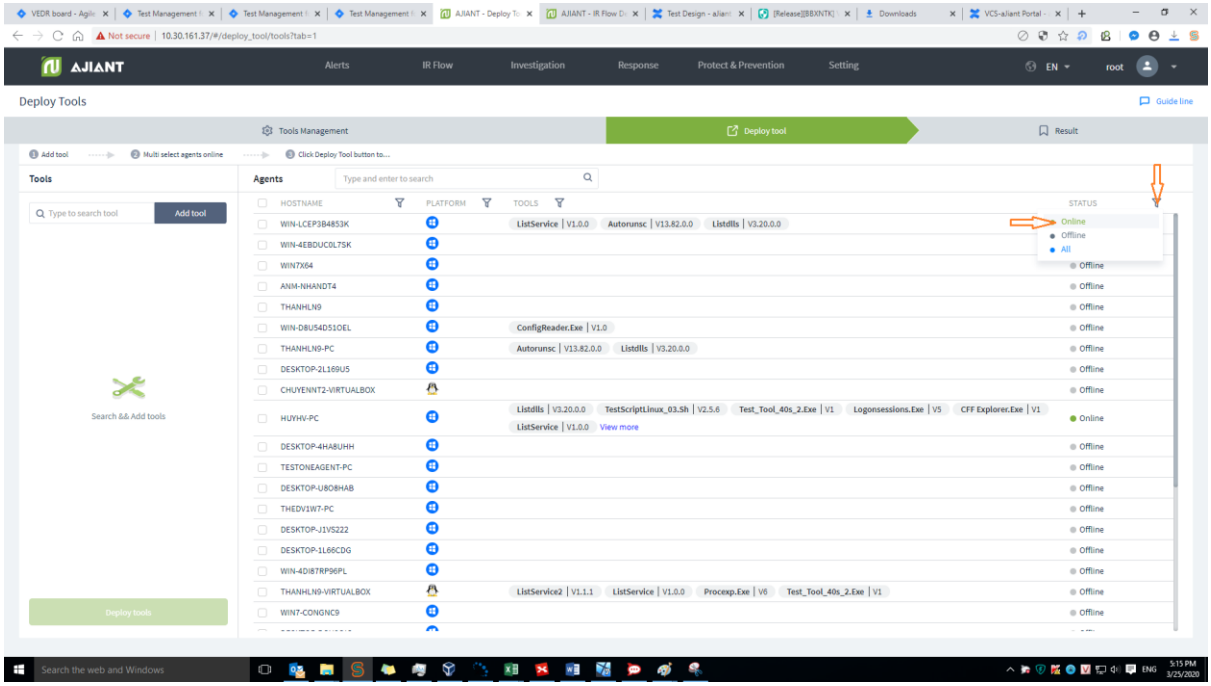
+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày

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

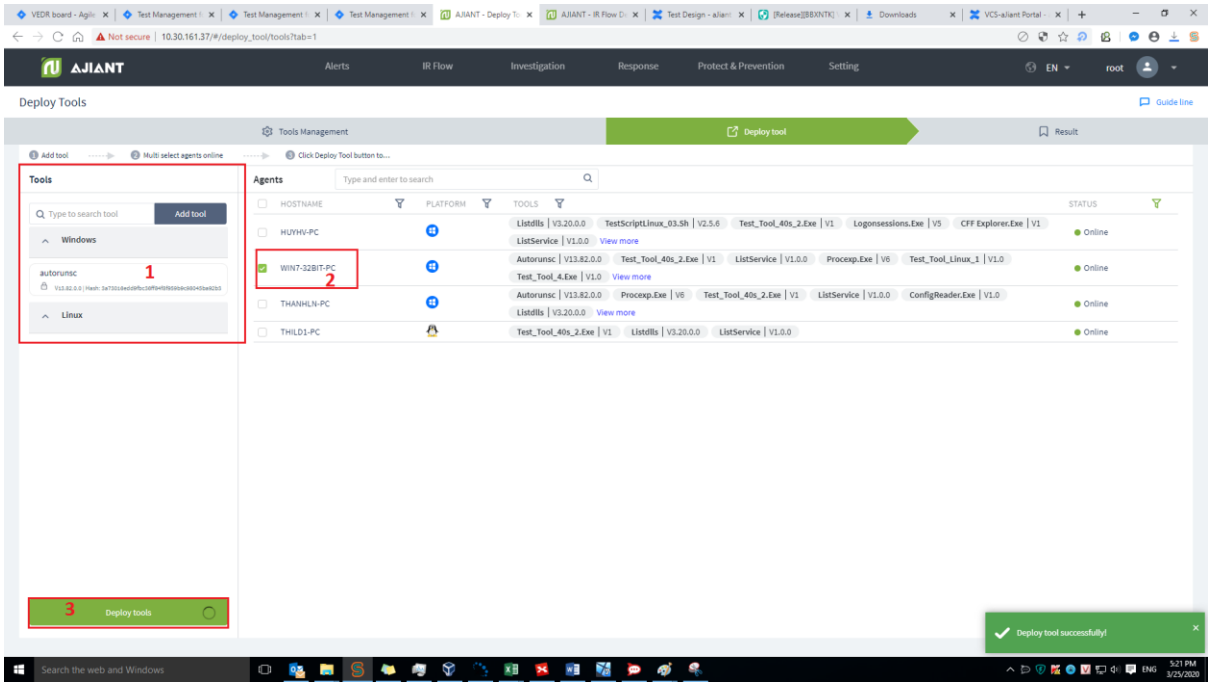
+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng

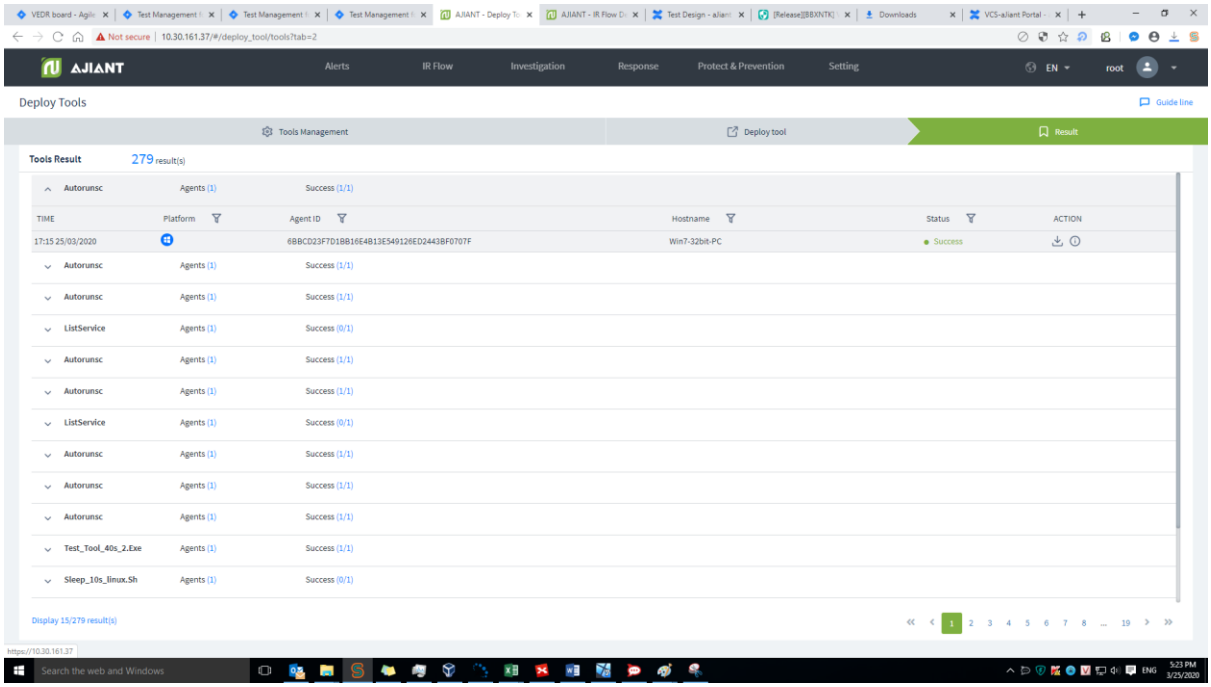
+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login

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



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

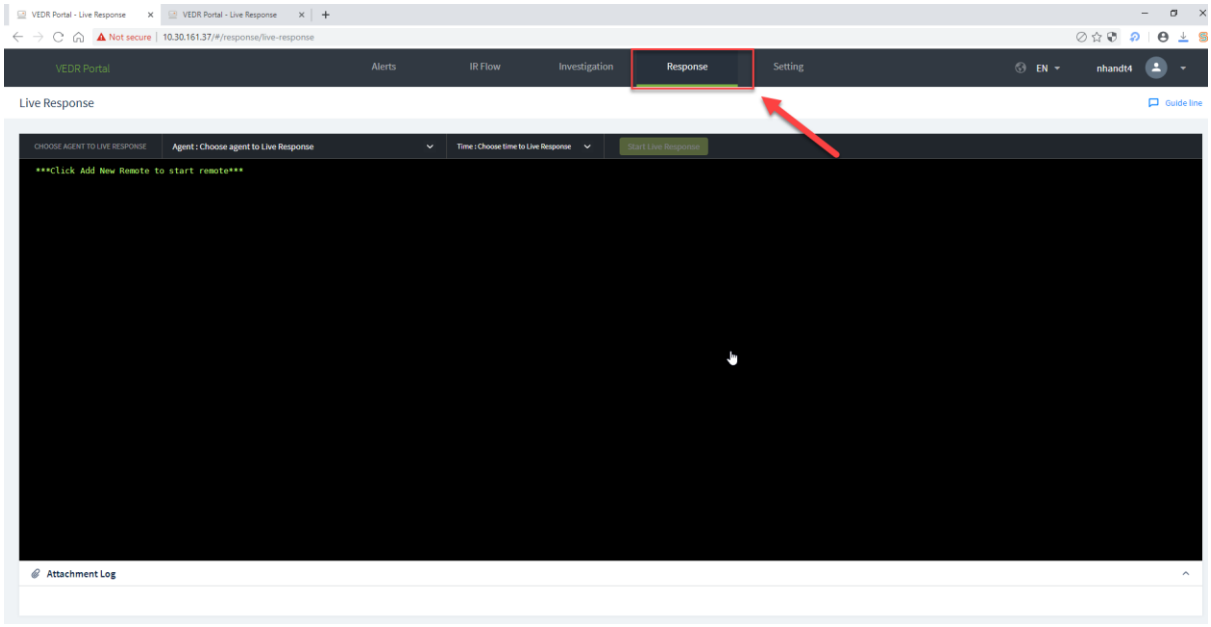

AJIANT
Alerts
IR Flow
Investigation
Response
Protect & Prevention
Setting
Deploy Tools
Tools Management
Deploy tool
Result
Tools
Add tool
Windows
autorunsc
1
Linux
Agents
HOSTNAME
PLATFORM
TOOLS
STATUS
HUYHV-PC
WIN7-32BIT-PC
2
THANHLN-PC
THILD1-PC
Online
3
Deploy tools
Deploy tool successfully!


AJIANT
Deploy Tools
Tools Management
Deploy tool
Result
Tools Result
279 result(s)
Autorunsc
Agents (1)
Success (1/1)
TIME
Platform
Agent ID
Hostname
Status
ACTION
17:15 25/03/2020
6BBCD23F7D1BB16E4B13E549126ED2443BF0707F
Win7-32bit-PC
Success
ListService
Success (0/1)
Test_Tool_40s_2.Exe
Sleep_10s_linux.Sh
Display 15/279 result(s)

3.7 Màn hình Response

3.7.1 Response_Live Response

- Mục đích: Chức năng Live response cung cấp khả năng xử lý một tập các command từ xa theo phiên làm việc nhằm cho biết các thông tin hoặc xử lý yêu cầu trên host.
- Các bước thực hiện chức năng Live Response:
- Bước 1: Click tab Response và chọn Live Response



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

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

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

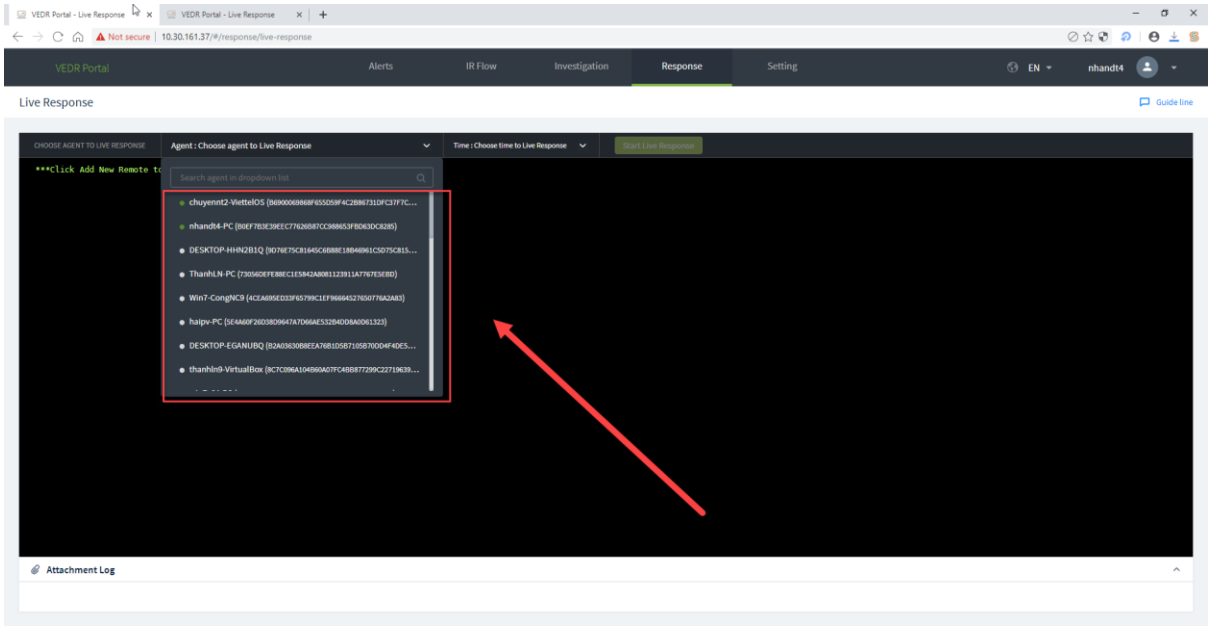
  + User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng

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

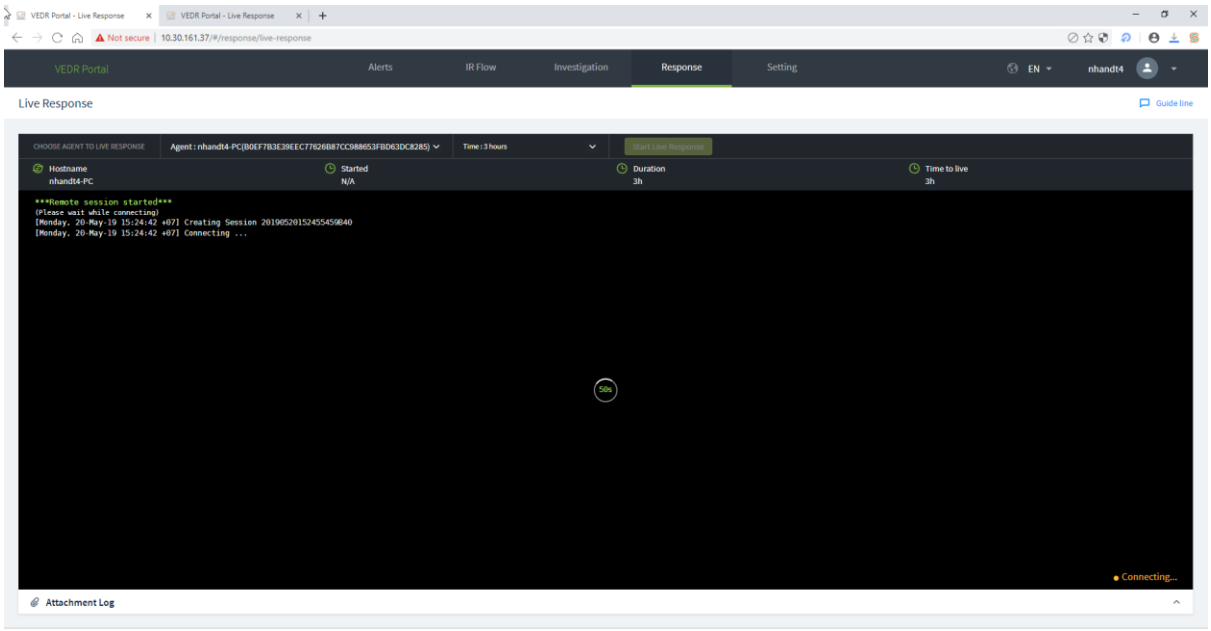
- Người dùng chỉ thực hiện được Live Response với những agent đang có trạng thái online ( ).

  + Chọn Time: có các khoảng thời gian 5 phút, 15 phút, 1 giờ, 3 giờ.

+ Click nút “Start Live Response”

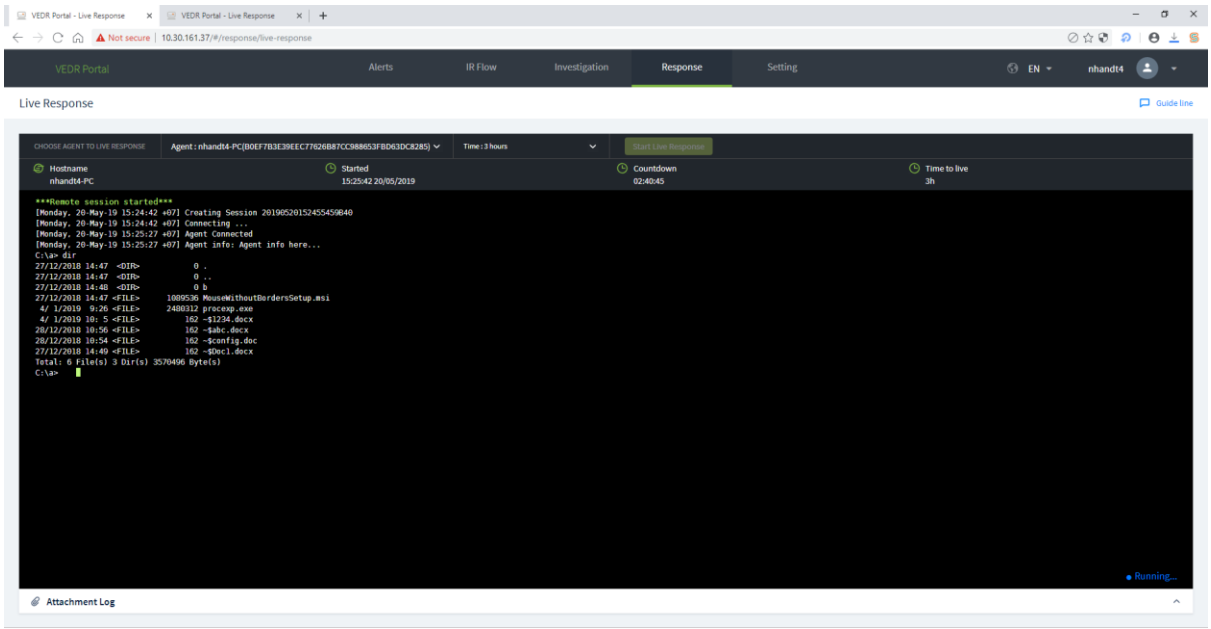


- Bước 3: Chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là “connecting”:



-

- Bước 4: Khi kết nối thành công, người dùng được phép thực hiện các lệnh ở màn hình console và trạng thái của phiên Live response “running”.
- Lưu ý: Mỗi agent tại một thời điểm chỉ có 1 phiên Live response làm việc.



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

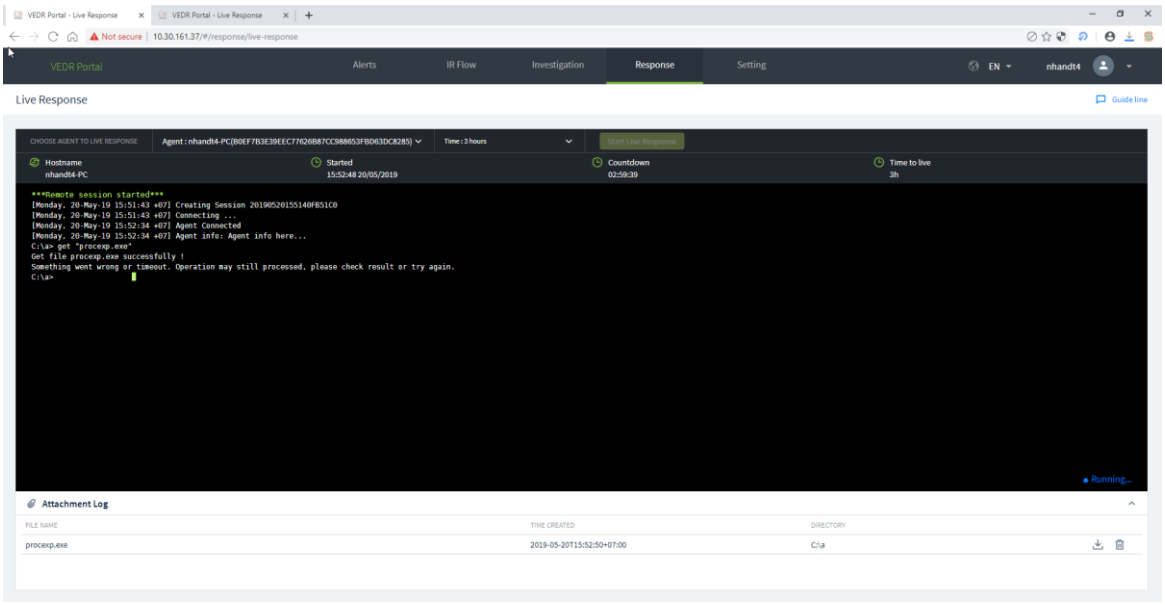
STT	***Các lệnh***	***Tham số***	***Mô tả***
1	cd	cd <dirpath>	Thay đổi thư mục làm việc hiện tại
2		cd.. hoặc cd ..	Chuyển về thư mục cha
3	pwd		In thư mục hiện thời đang làm việc
4	dir		Liệt kê các file/ các thư mục con trong thư mục hiện thời
5	delete	delete –file <path> ví dụ: delete -file "c:\temp\run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

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

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

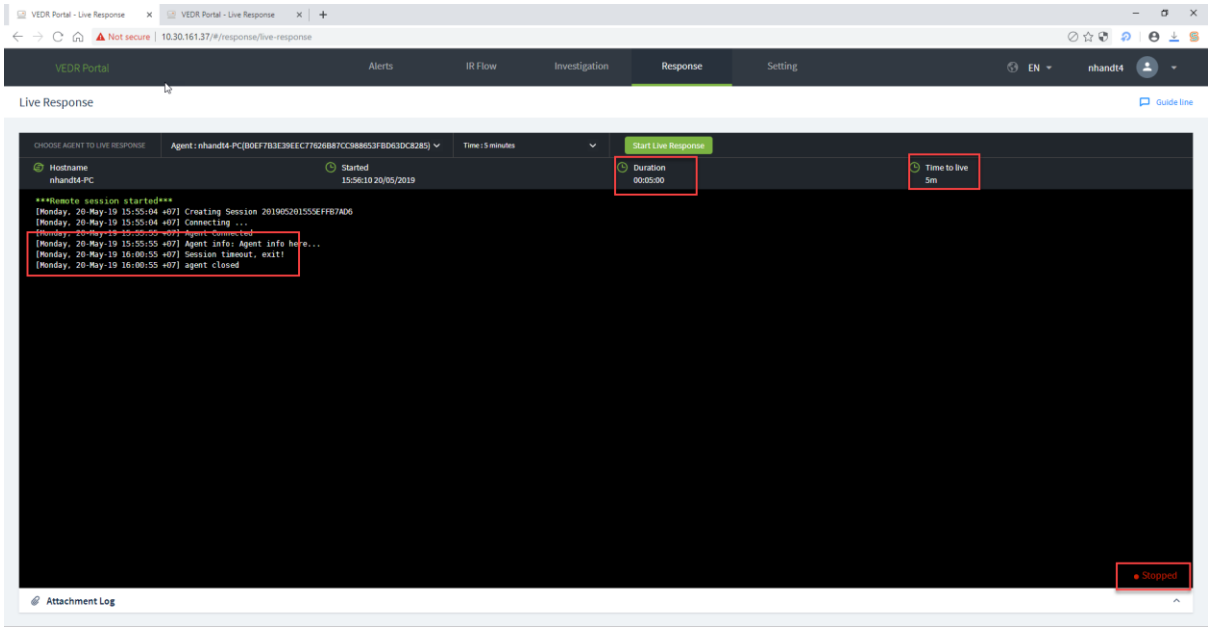
  + Lệnh Clear: Sau khi thực hiện lệnh clear thì hệ thống sẽ hỗ trợ người dùng download toàn bộ log đã thực hiện trên màn hình console trước đấy, bằng thao tác click vào link “here”

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



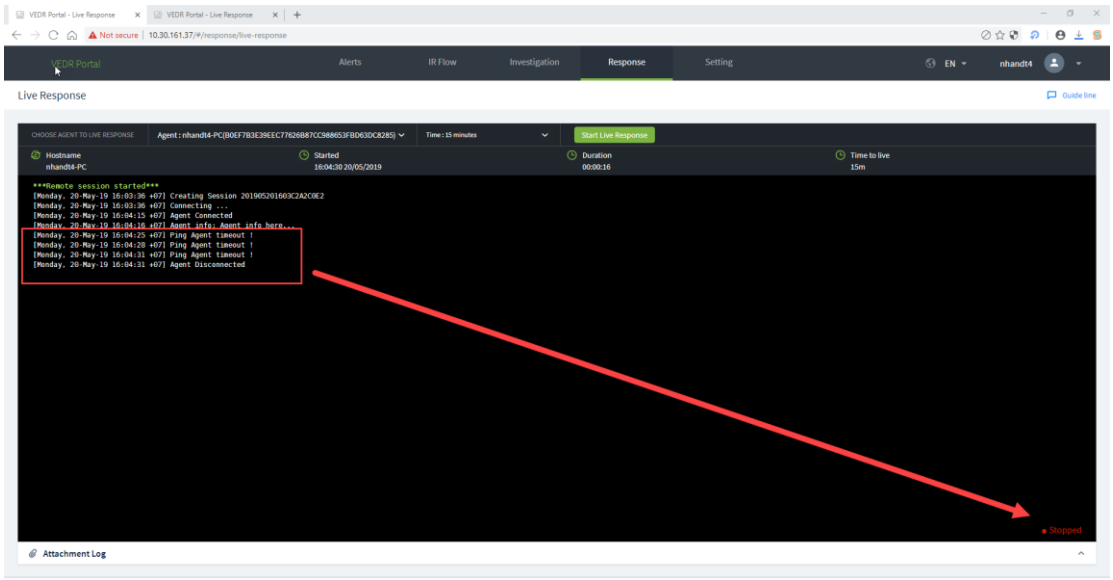
- Bước 6: Phiên làm việc của Live Response kết thúc khi:

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



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

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



3.8 Màn hình Setting

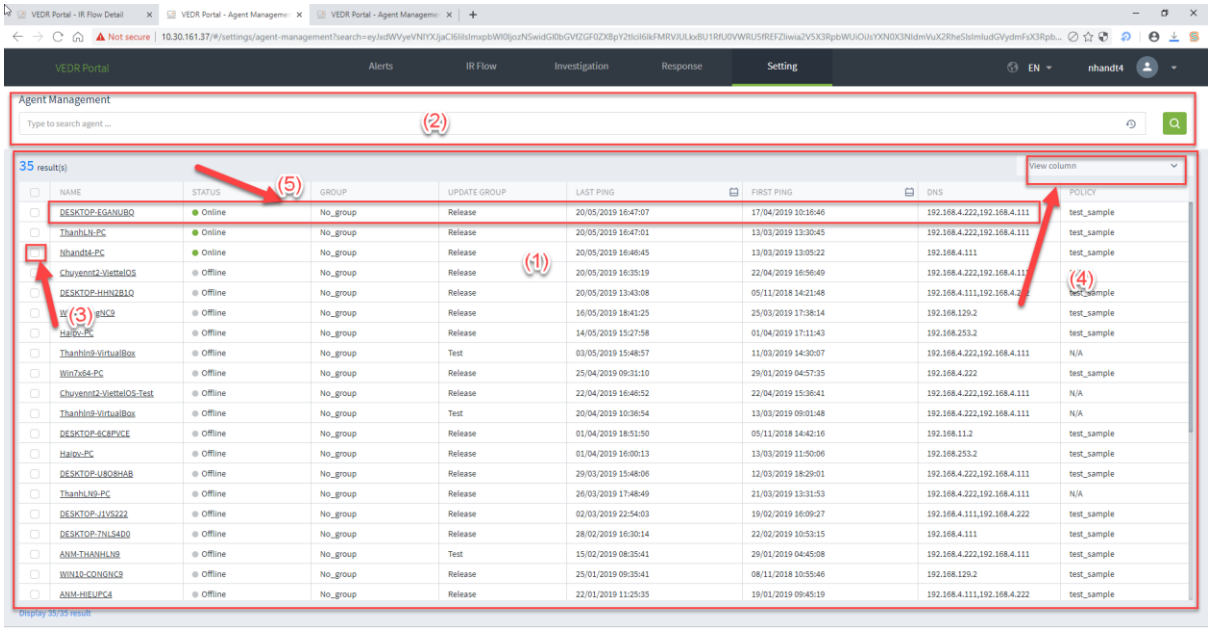
3.8.1 Agent Management

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

  + Xem danh sách các agent và các thông tin chung

+ Xem chi tiết của Agent

+ Chọn nhanh các agent và thiết lập một số cài đặt (policy, update group)



- 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

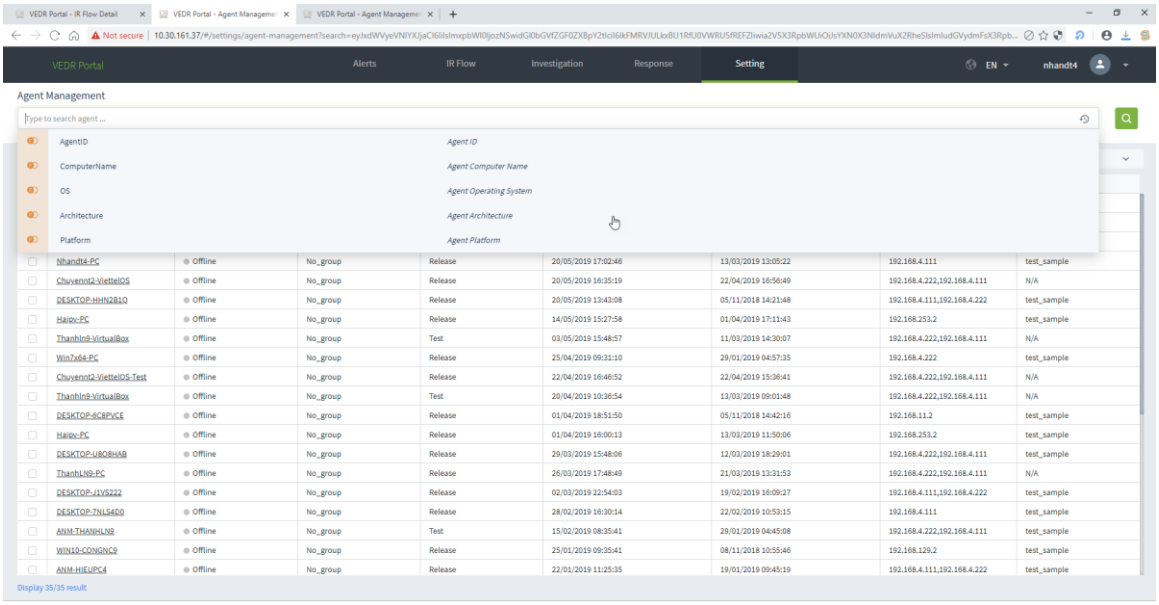
+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default

+ 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

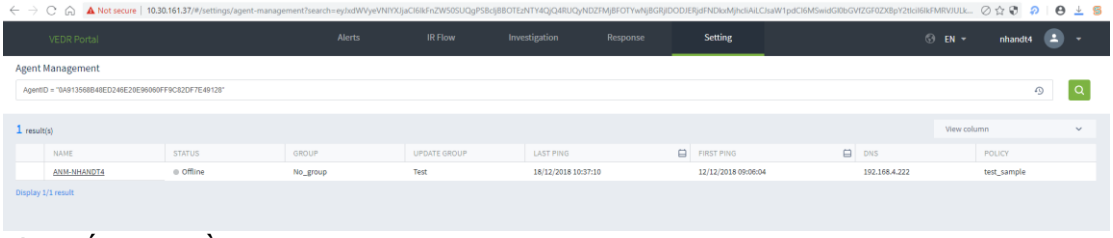
+ Mỗi agent được hiển thị các thông tin chung gồm: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, PlatForm, PlatForm Version, Architecture, DNS, Version.

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 “=”, “!=”, “~”.

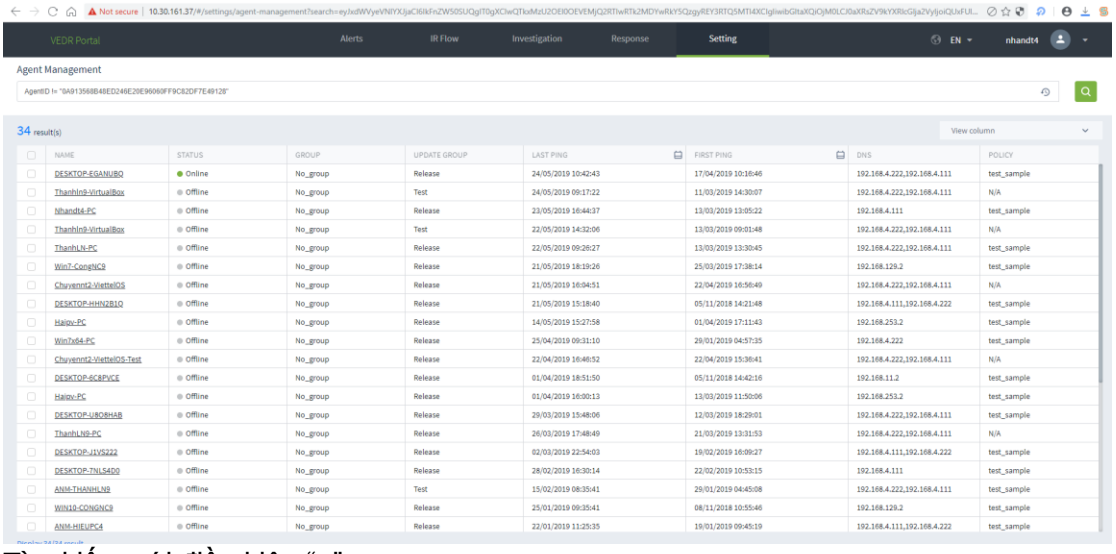


- Ví dụ về các câu tìm kiếm:

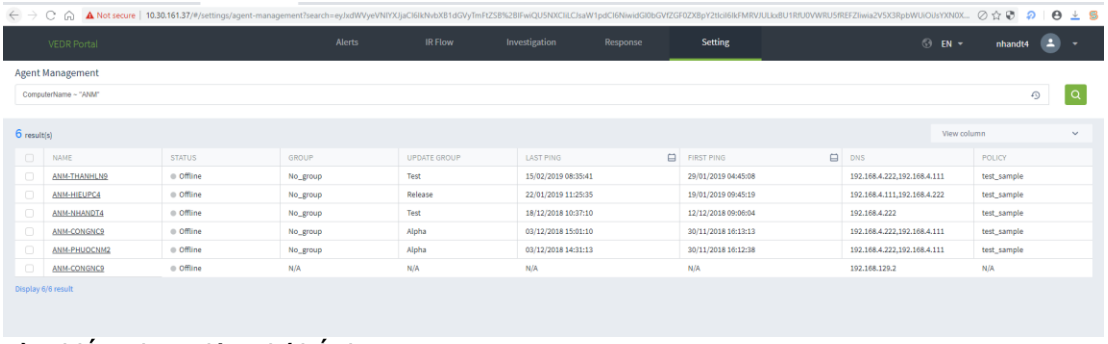
Tìm kiếm với điều kiện “=”



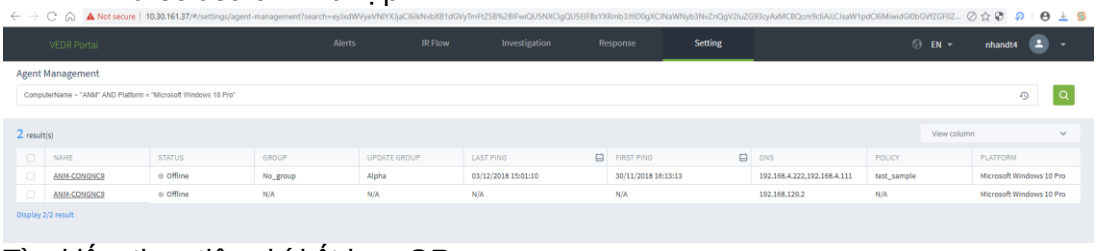
Tìm kiếm với điều kiện “!=”



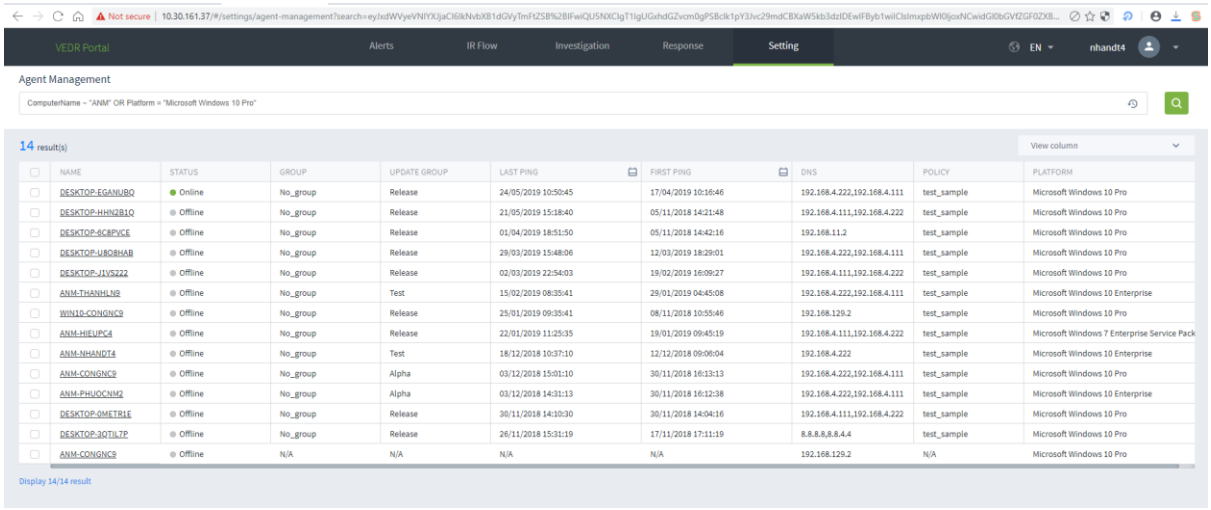
Tìm kiếm với điều kiện “~”



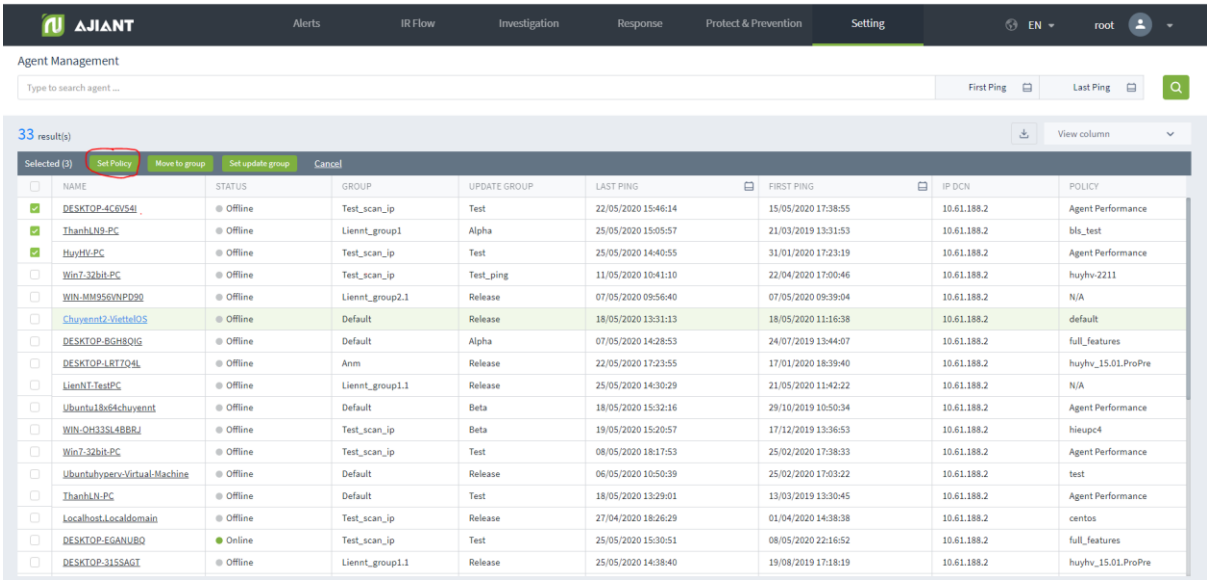
Tìm kiếm theo tiêu chí kết hợp AND



Tìm kiếm theo tiêu chí kết hợp OR

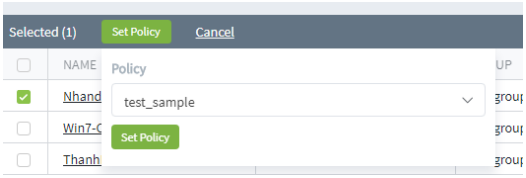


- 3 - Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Policy

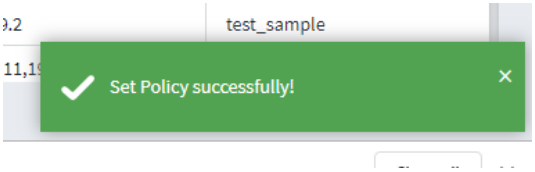


+ Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected

+ Thực hiện Set Policy

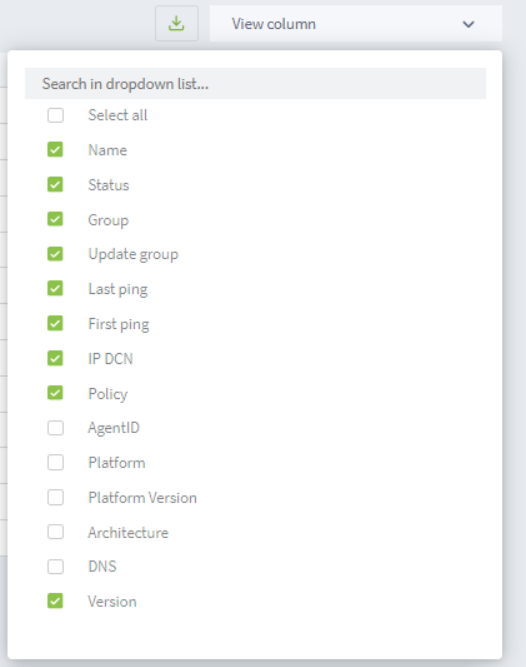


+ Kết quả sau khi set policy



+ Hủy thao tác ở màn hình Multiselected

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



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

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

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

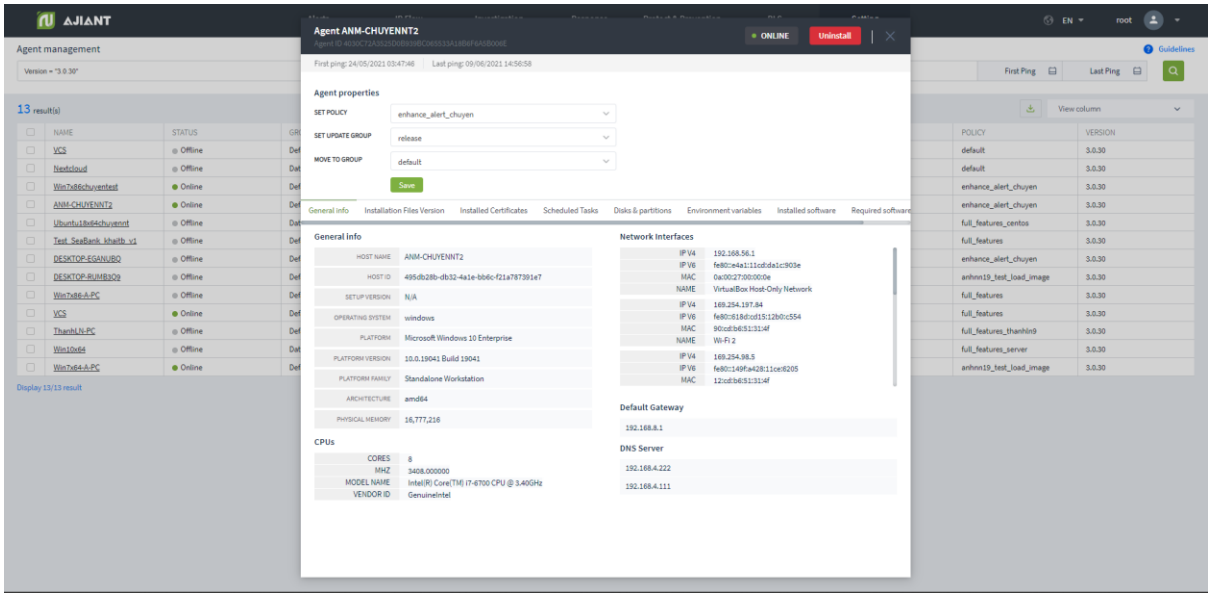
  + User đăng nhập thuộc group default: Hiển thị Group default

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

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

✓ Tab General info

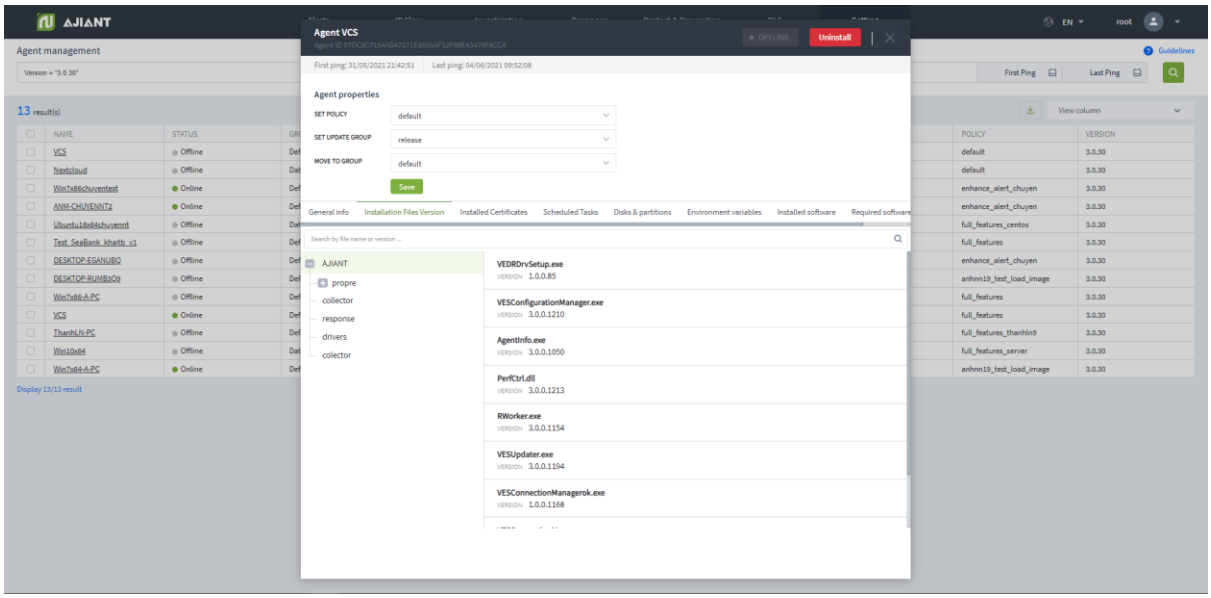
- Hệ thống hiển thị các thông tin chung về agent gồm: Các thông tin chung, CPUs, Network Interfaces, Default Gateway, DNS Server.



✓ Installation Files Version

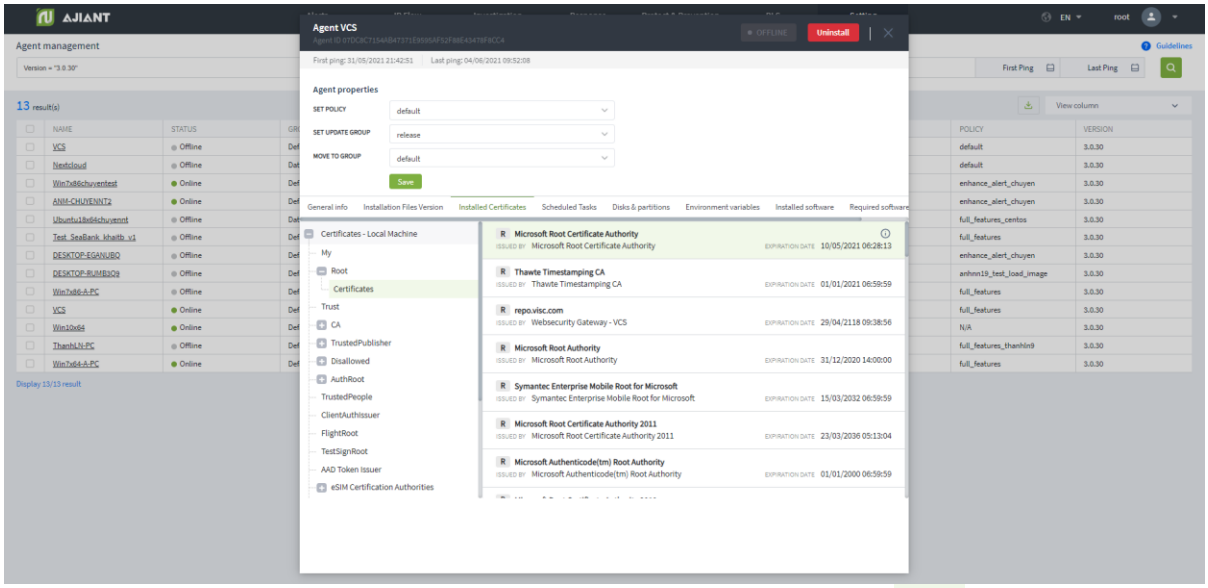
- Thống kê tất cả các file cài agent, bao gồm các thông tin: Tên folder chứa file cài, File name, Version

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

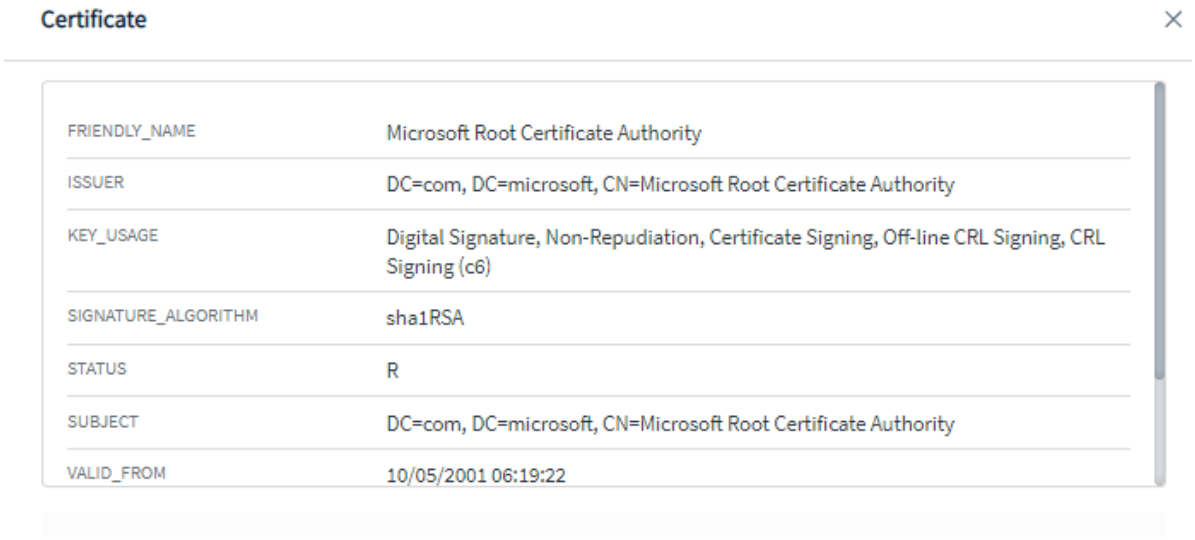


✓ Installed Certificates

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



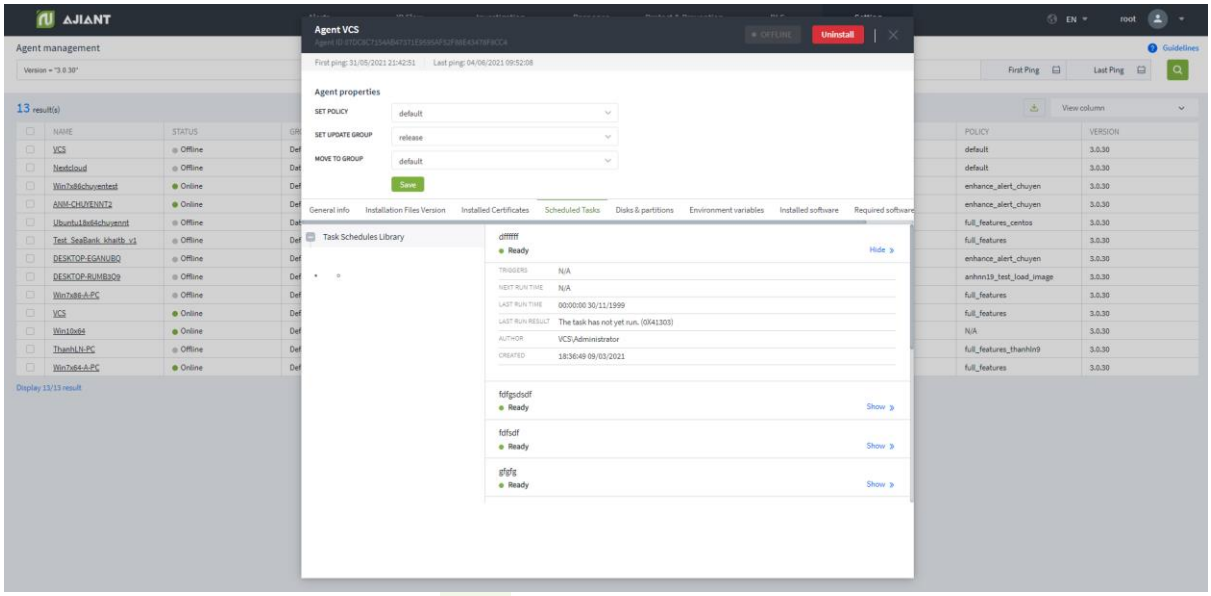
- Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn  , hiển thị màn hình như sau:



✓ Scheduled Tasks

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

  + Chọn Show » hoặc Hide » để tùy chỉnh việc hiển thị thông tin bổ sung cho từng task.

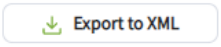


+ Hover vào task và chọn ⓘ để xem thông tin đầy đủ của task dưới dạng xml

XML Detail

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

Export to XML

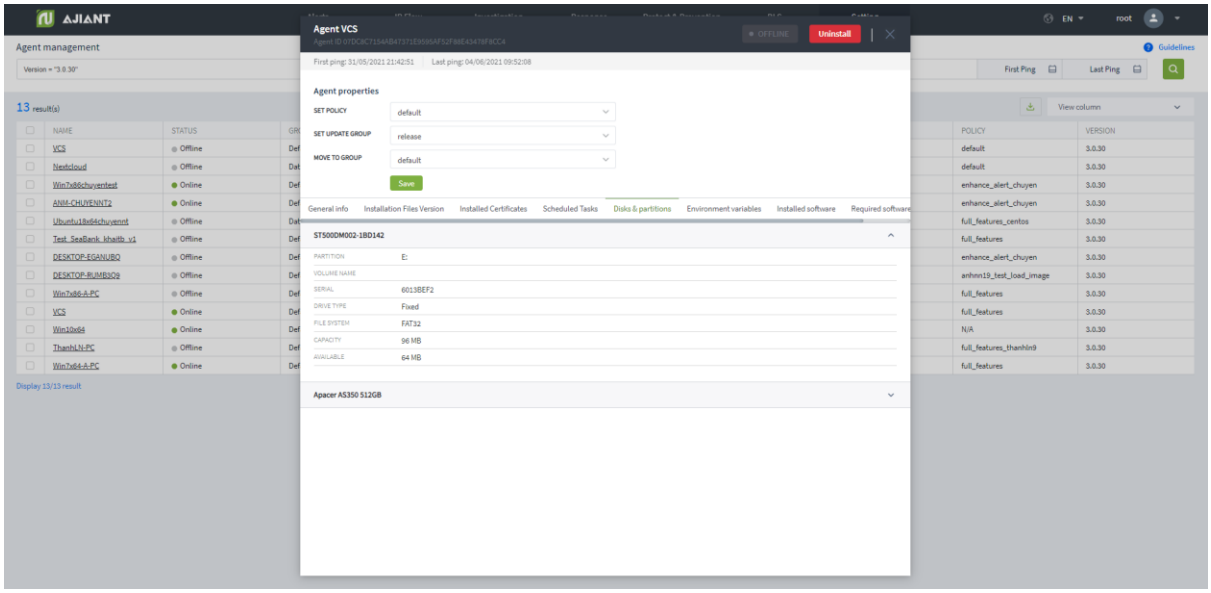
+ Chọn 

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

✓ Disks & partitions

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

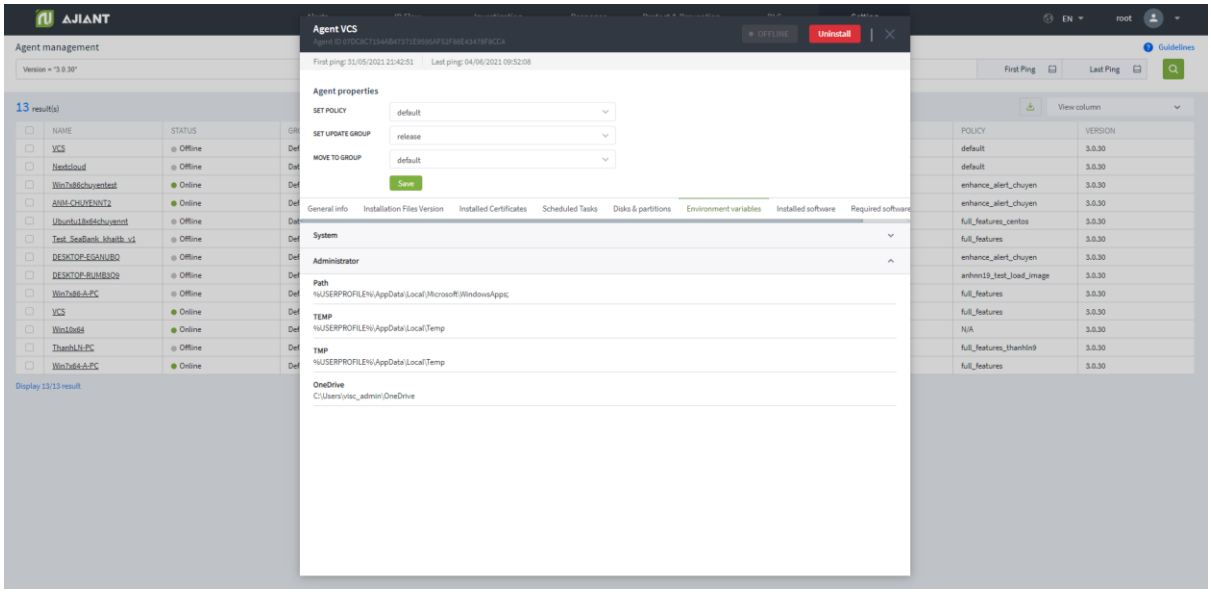
+ Chọn  hoặc  để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



✓ Environment variables

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

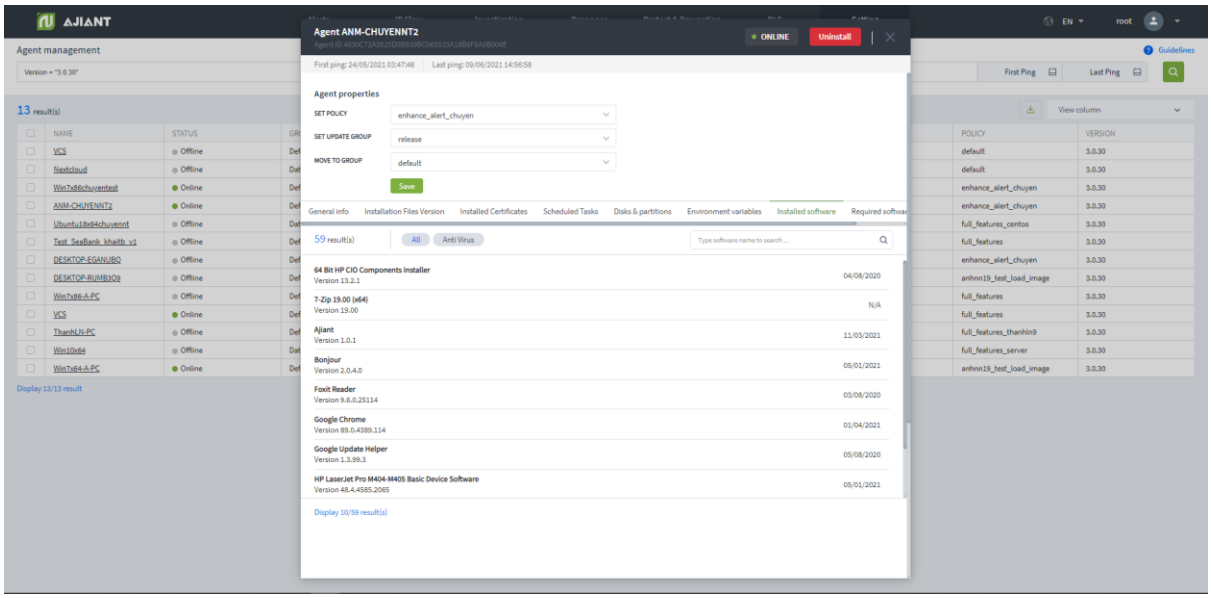
+ Chọn  hoặc  để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



✓ Tab Installed Software

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

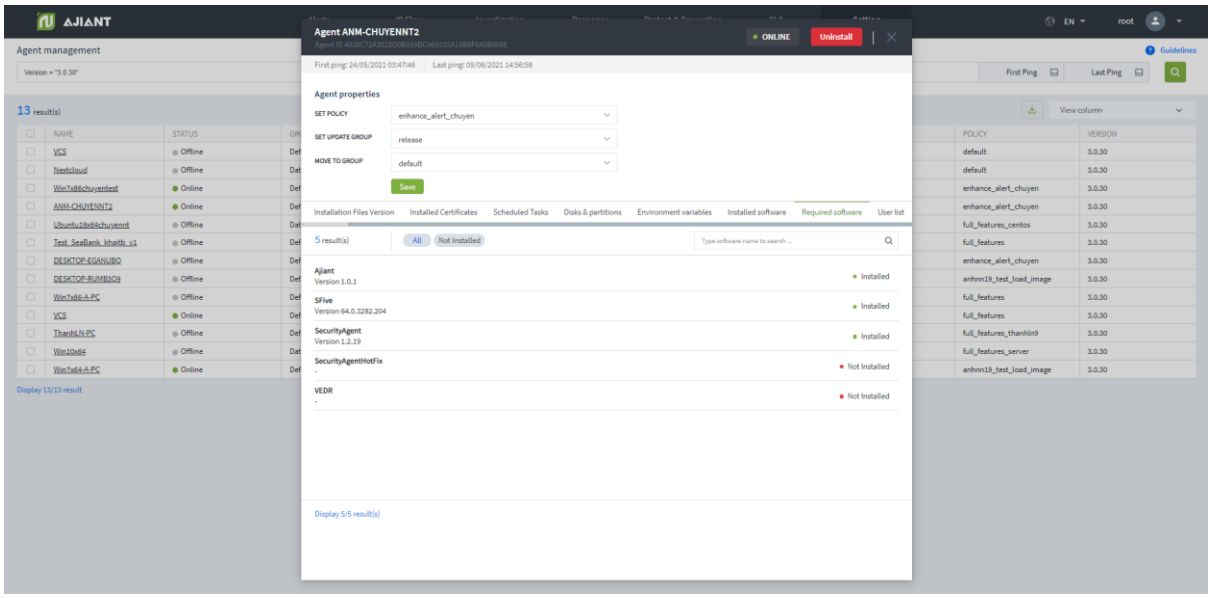
  + Hỗ trợ search nhanh phần mềm Antivirus đã cài hoặc nhập tên phần mềm vào text box search



✓ Tab Required Software

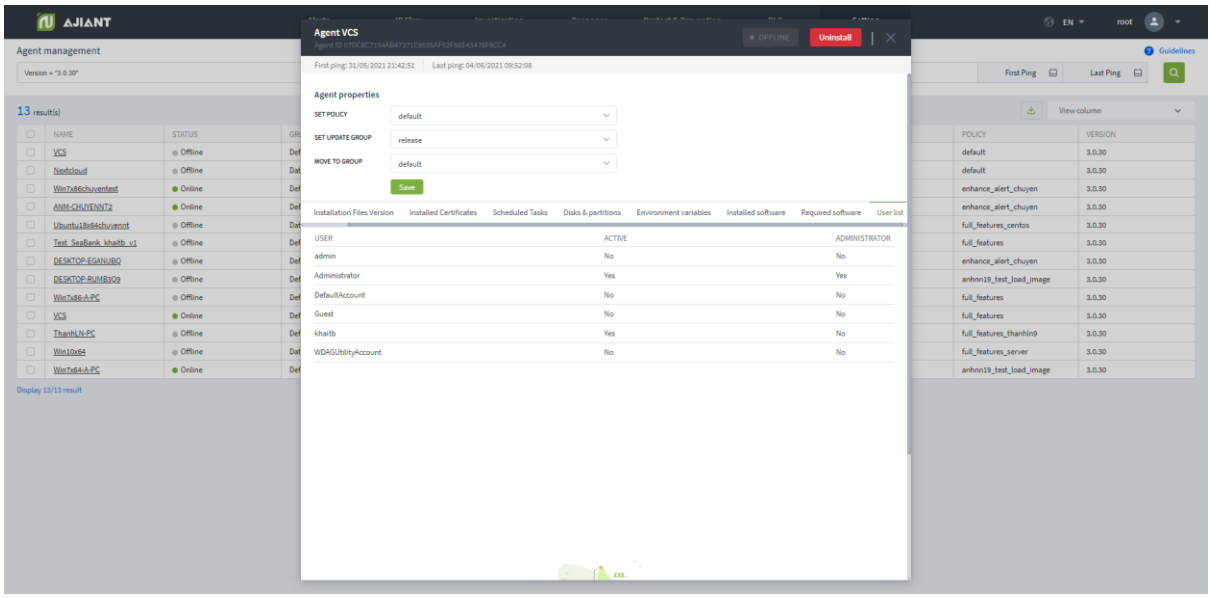
- Thống kê tất cả phần mềm bắt buộc đã cài hoặc chưa cài trong agent bao gồm thông tin: Tên phần mềm, version cài, trạng thái cài

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



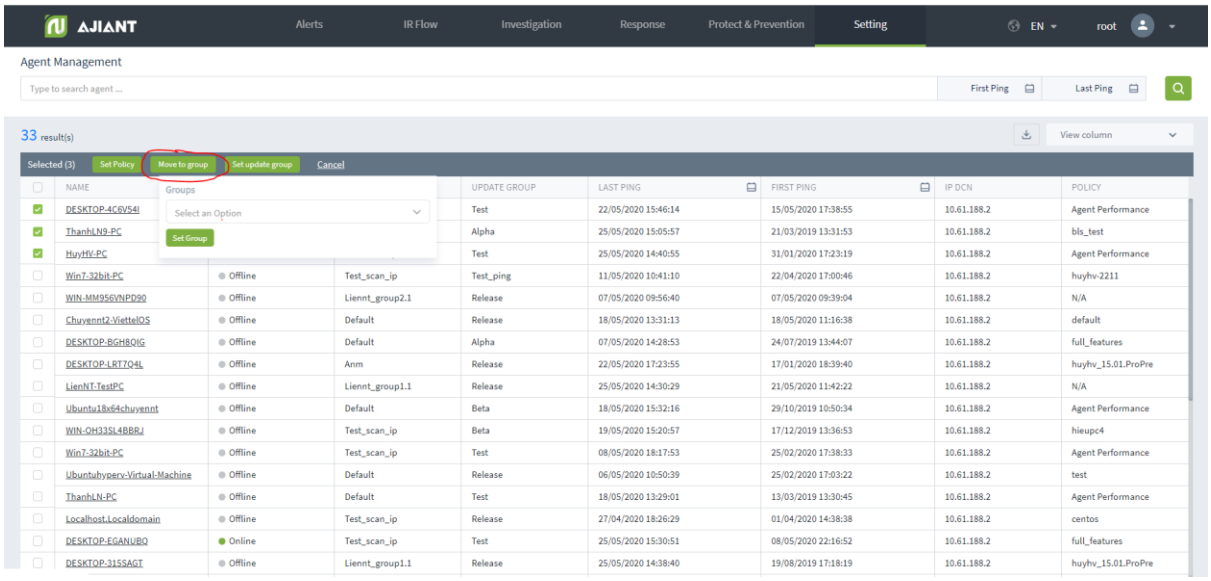
✓ Tab User list

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



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

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



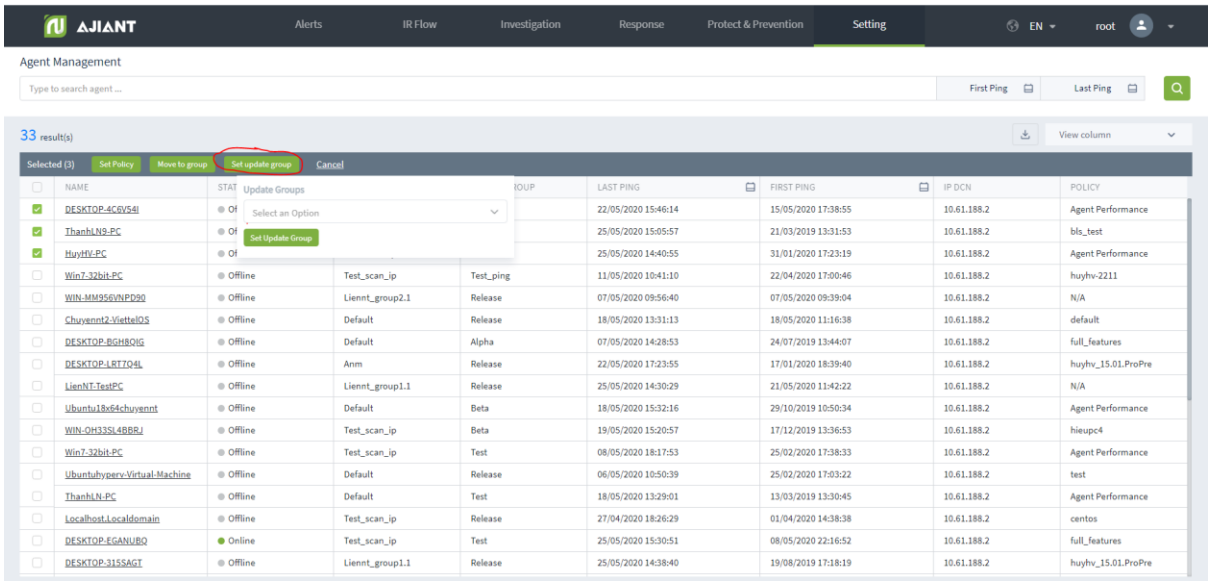
+ Thực hiện Move to group

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



- Thực hiện Set update group

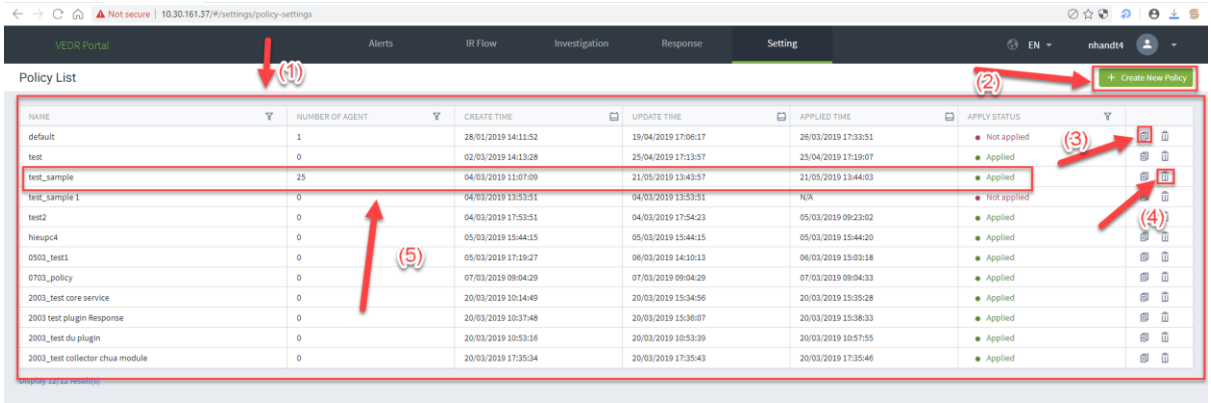
- Lưu ý:

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

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

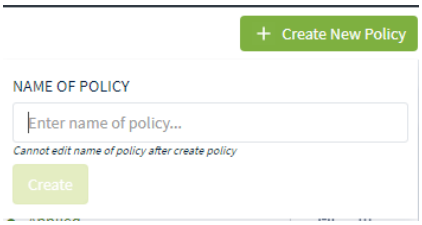
3.8.2 Policy Setting

- Mục đích: Hỗ trợ người dùng quản lý danh sách các chính sách thiết lập cho các Agent.
- Màn hình giao diện khi người dùng truy nhập vào Setting >> Policy Setting:

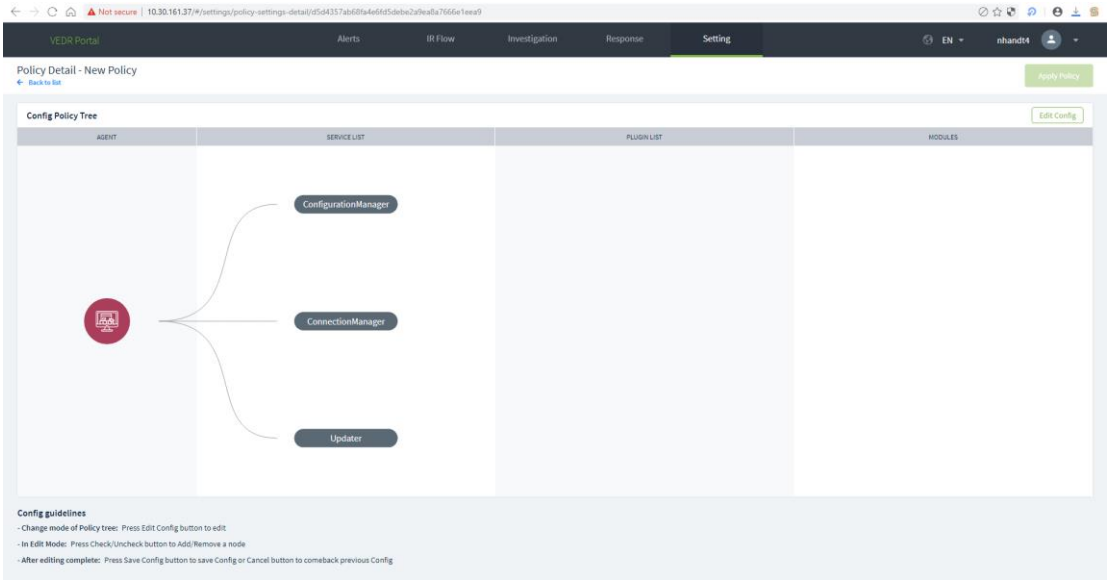


- 1 - Hiển thị danh sách các Policy đã được tạo trên hệ thống. Mỗi 1 policy gồm các thông tin: Tên, số lượng Agent được áp chính sách, Thời gian tạo, thời gian cập nhật, Thời gian áp chính sách, trạng thái (có 2 trạng thái: Applied và Not Applied).

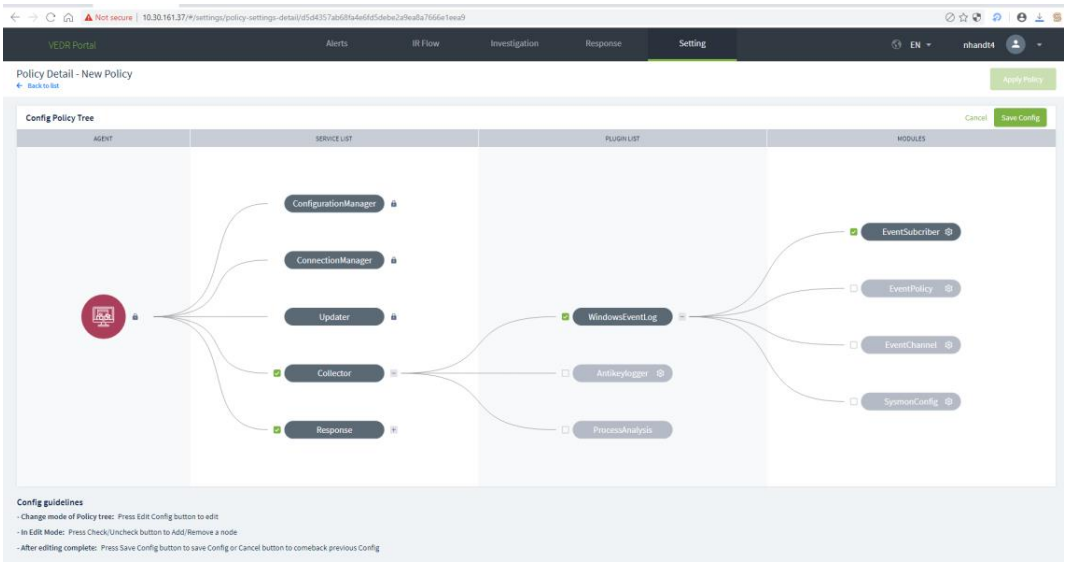
- 2 - Tạo mới một chính sách: Click vào button + Create New Policy hệ thống hiển thị Popup tạo mới chính sách như sau:



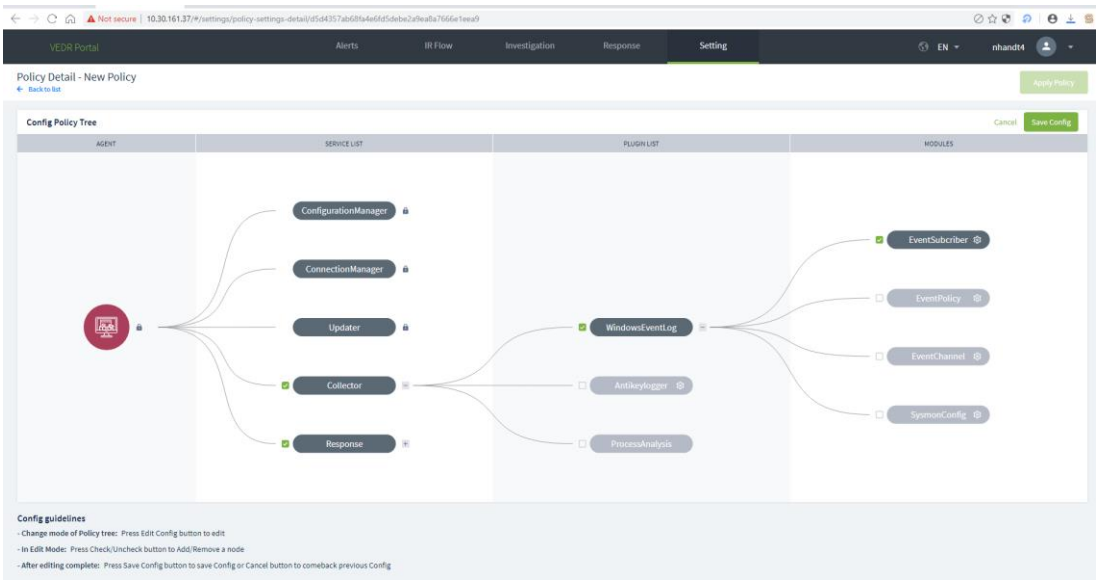
- Lưu ý khi tạo mới: Tên Policy không được trùng với các Policy đã tạo trước đó.
- Sau khi tạo mới policy thành công hệ thống sẽ hiển thị màn hình chi tiết của 1 policy:



- Mỗi 1 policy tạo xong thường có 3 core service mặc định: ConfigurationManager, ConnectionManager, Updater. Lưu ý 3 service này không được phép xóa khỏi hệ thống. Các bước để cấu hình cho 1 policy:
- Bước 1: Click button Edit Config để thay đổi cây Policy
- Bước 2: Khi ở trong chế độ Edit, người dùng được phép Check/Uncheck để Add/Remote các service khác



- Bước 3: Sau khi hoàn thành chế độ edit: Người dùng nhấn nút “Save config” để lưu các thay đổi hoặc nhấn nút “Cancel” để quay lại cấu hình trước 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”: lọc các event có eventID = 4

“-689”: lọc các event có eventID # 689

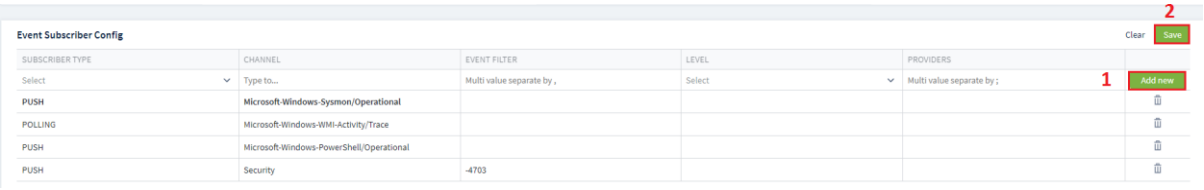
- trường **providers** các string con cách nhau dấu chấm phẩy (;)
- các trường bắt buộc phải điền: **subs_type, channel**
- Channel: nguồn log
- sub_type:

  PUSH: khi có event mới → gọi hàm của VCS-aJiant để xử lý

  POLLING: VCS-aJiant sau 1 khoảng thời gian chủ động lấy log

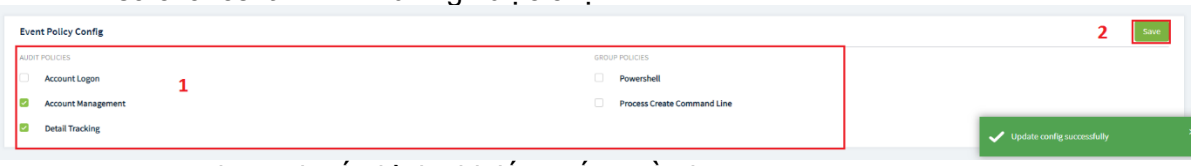
  PULL: VCS-aJiant chủ động lấy log sau 1 khoảng thời gian

Sau khi cấu hình xong cần Save lại



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

Yêu cầu: có ít nhất 1 trường được chọn



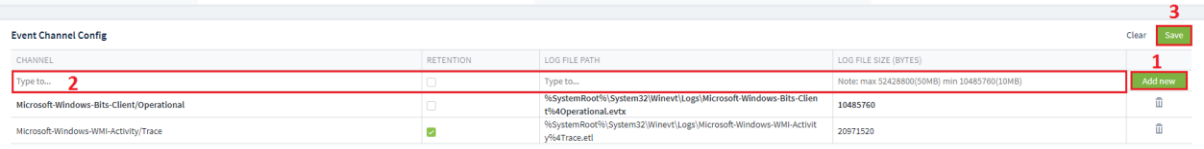
+ EventChannel: cấu hình chi tiết 1 số nguồn log:

Retention: có lưu log xoay vòng hay không (Nếu chọn Rentention thì khi file log đầy có log mới sẽ ghi đè lên log cũ nhất)

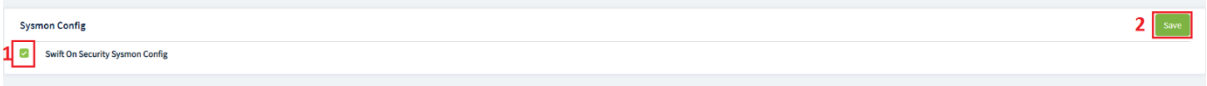
Log file path: đường dẫn file log

Log file size: kích thước file log

Yêu cầu: tất cả dữ liệu đều phải điền



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

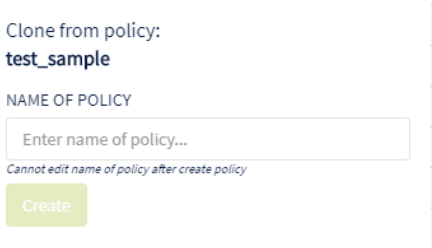


- Antikeylogger: là một SelfRun Plugin của VCS-aJiant, có nhiệm vụ định kỳ quét toàn bộ máy để tìm ra KeyLogger đang chạy trên máy nếu có

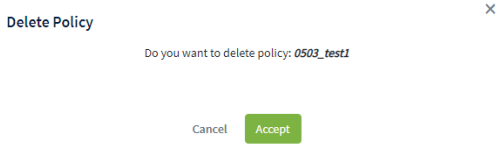
+ Scan setting: cấu hình các loại KeyLogger cần quét
Yêu cầu:
Scan cycle: min là 1 phút, max là 180 phút
Chọn ít nhất 1 loại Keylogger
+ Whitelist setting: cấu hình whitelist 1 số phần mềm theo đường dẫn của file trên ổ đĩa hoặc theo chữ ký số (cert) của file chạy key logger
Yêu cầu: điền đầy đủ các trường
Sau khi nhập xong cần Save lại cấu hình:

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

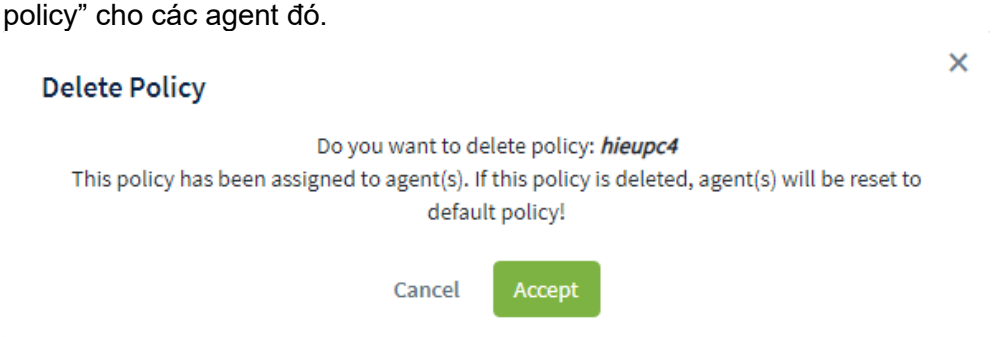
+ Clone chính sách mới: Click vào button hệ thống sao chép toàn bộ chi tiết của policy được clone ngoại trừ tên policy.



+ Xóa chính sách: Click vào button hệ thống hiển thị pop up để người dùng đưa ra quyết định xóa hay không?



Trường hợp Policy đã có agent được áp, sau khi xóa hệ thống tự động gán “default policy” cho các agent đó.



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

3.8.3 Group Management

- Cấu hình luật để tự động chuyển policy và chuyển nhóm cho các agent nếu thỏa mãn luật trên Portal, giảm thời gian chuyển policy và chuyển nhóm cho từng agent và đồng bộ policy cho các agent thỏa mãn luật đã cấu hình.

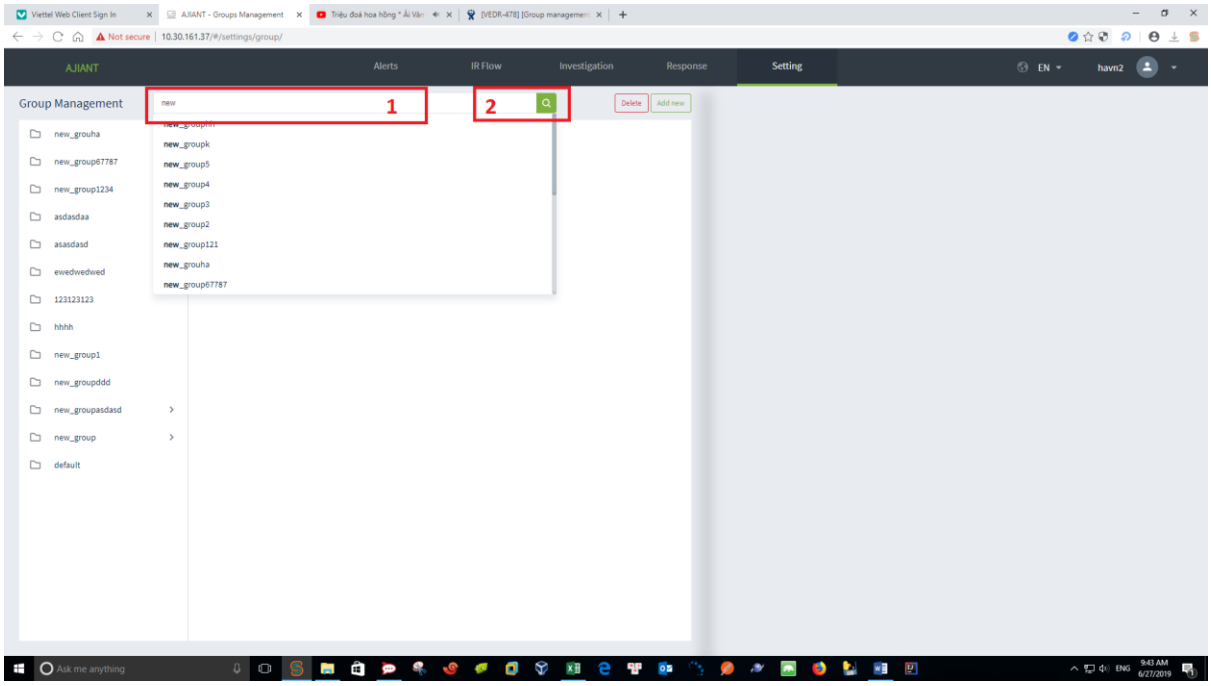
  Các tính năng chính trên màn hình này bao gồm:

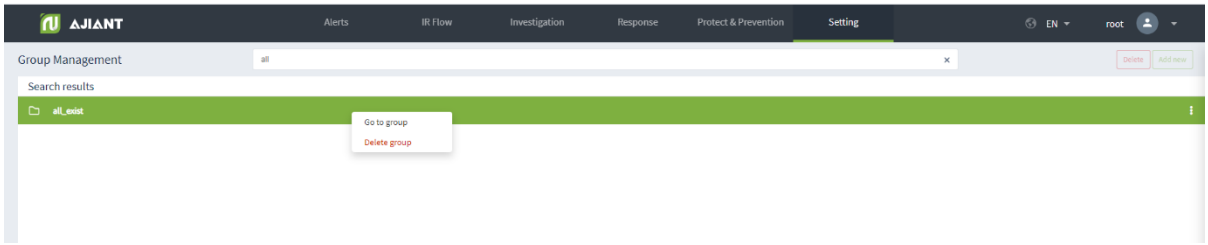
  + Quản lý nhóm theo cây
  + Tìm kiếm nhóm
  + Thêm mới nhóm:
    - Tạo luật tự động chuyển nhóm cho agent
    - Tùy chọn cách thức chuyển nhóm (All existing agents, New agents only, All existing and new agents) và gán policy (gán ngay, không gán)
  + Theo dõi các agent thuộc nhóm, tổng số agent thuộc nhóm
  + Chỉnh sửa nhóm
  + Xóa nhóm, xóa agent thuộc nhóm

(1) Quản lý nhóm theo cây:
+ User đăng nhập thuộc group root: 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

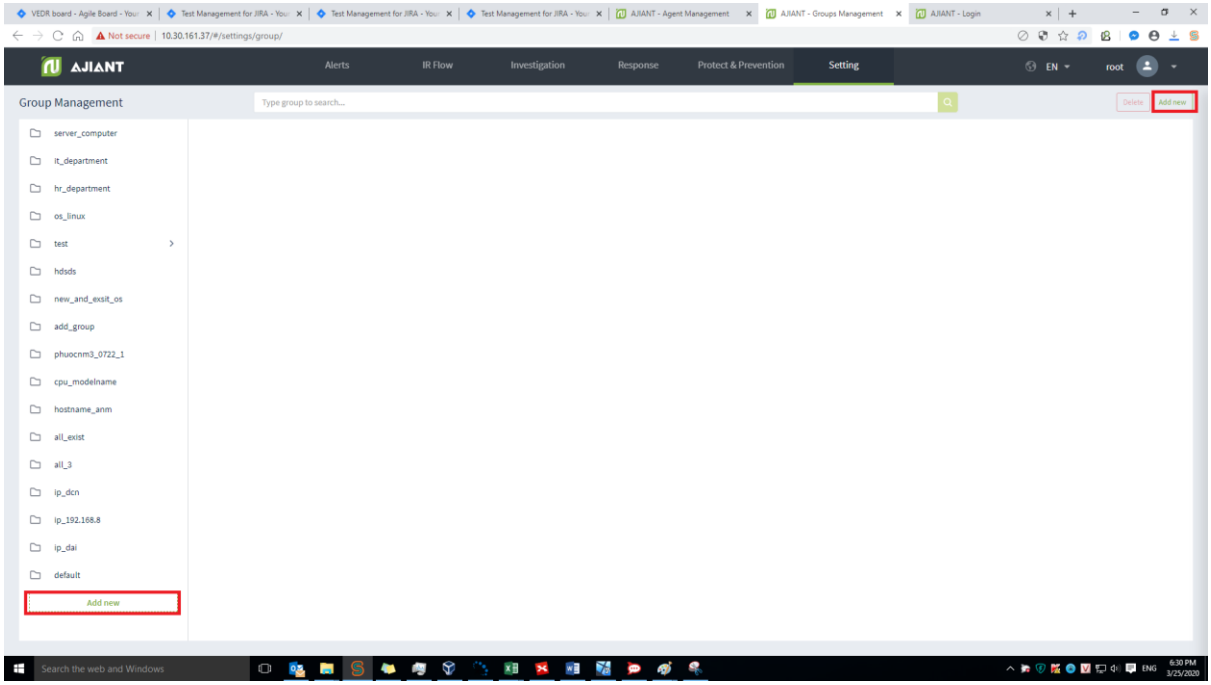




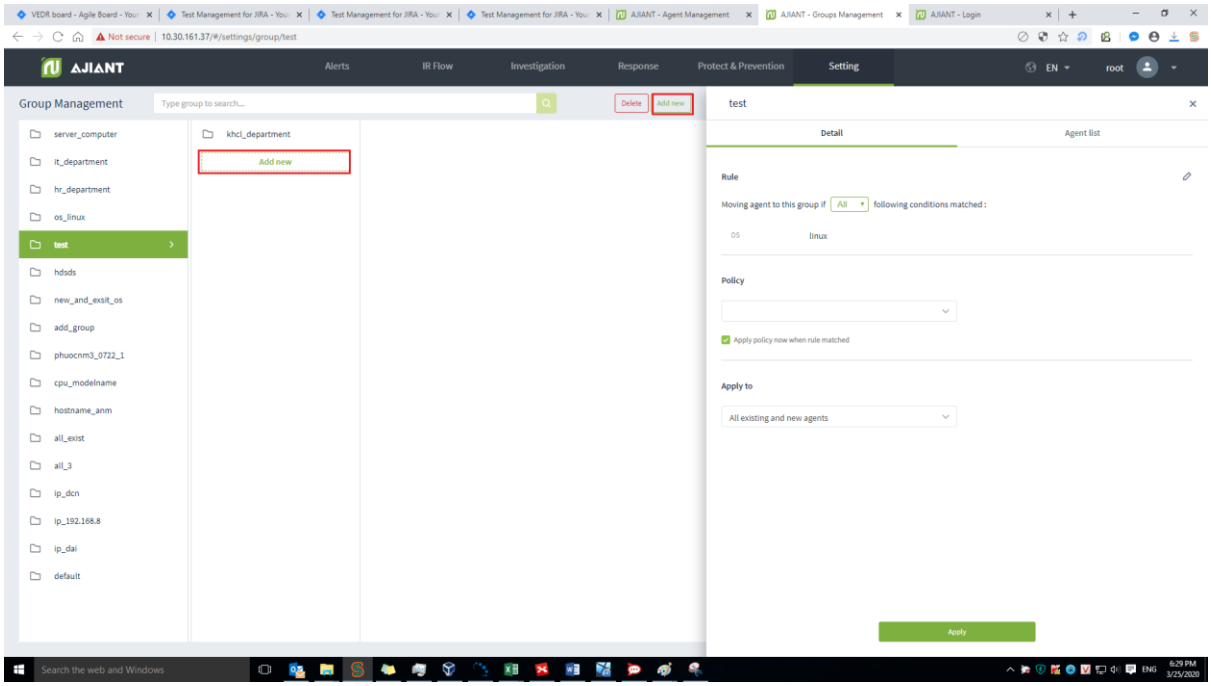
- Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.
  - Tab thông tin chi tiết hiển thị là Detail, dữ liệu của group đó là Rule, Policy, Apply to.
  - Khi chọn tab Agent list thì dữ liệu thông tin các agent match với group đó.
- Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 2 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
B1: Lựa chọn vị trí nhóm sẽ tạo

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

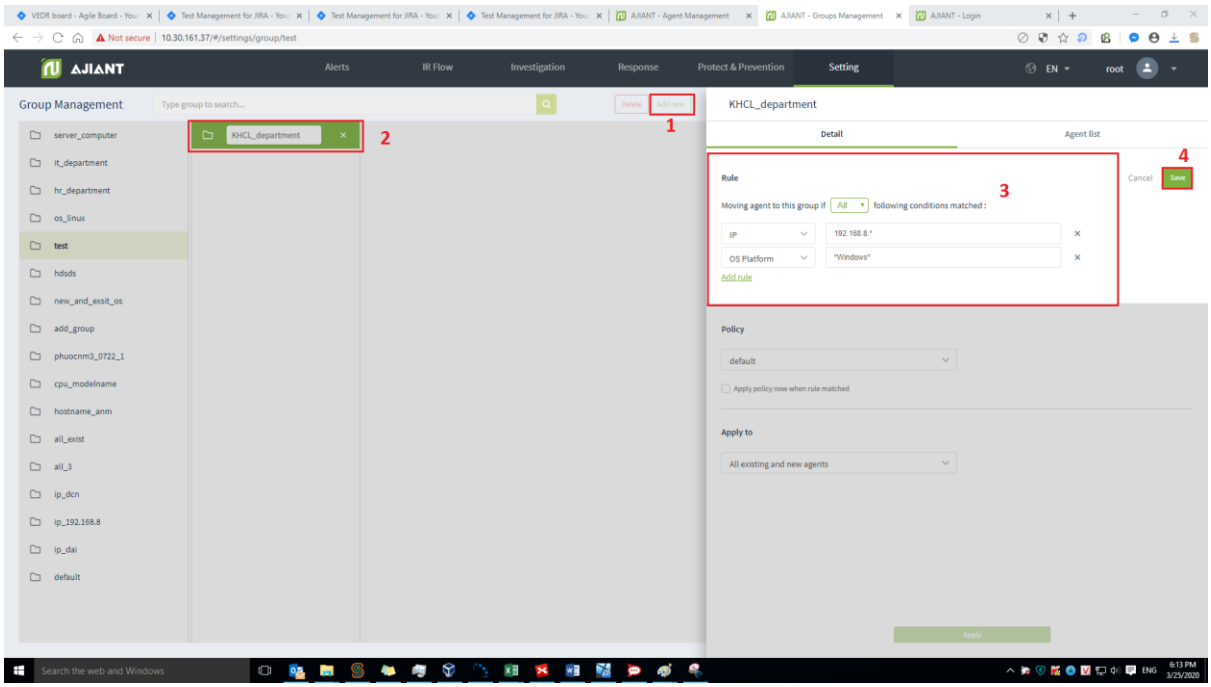


Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2… thì click vào nhóm cha sau đó click “Add new” trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click “Add new”

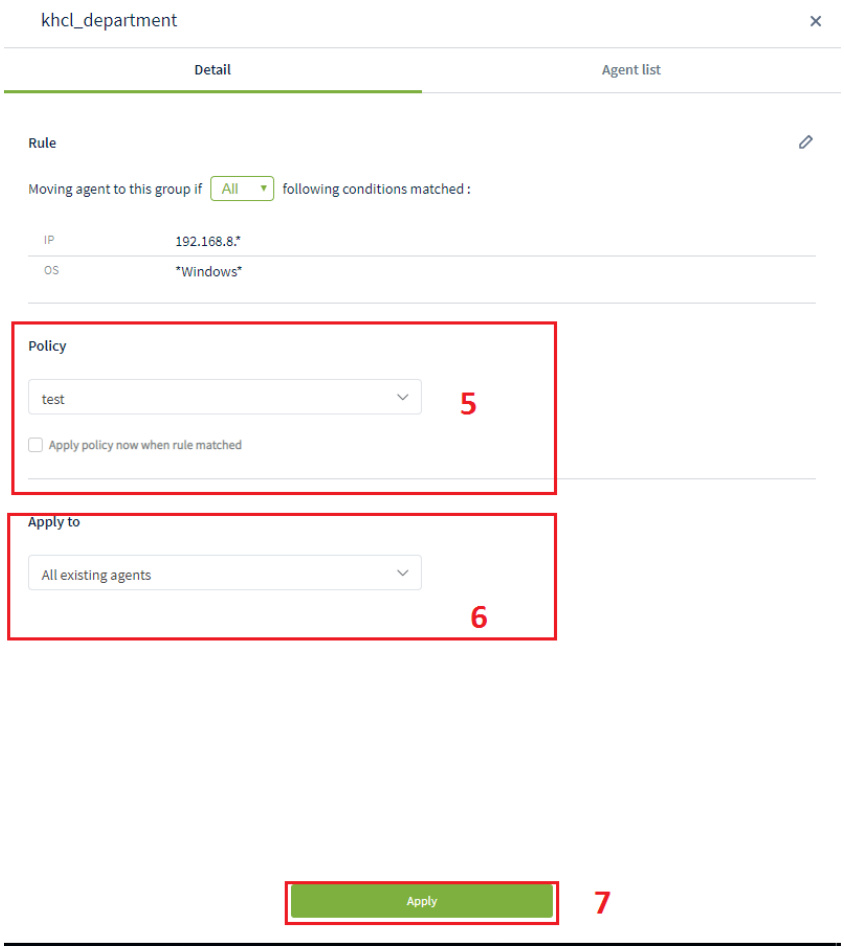


- Bước 2: Nhập tên nhóm và cấu hình luật

Lưu ý: tên và luật cấu hình không được trùng với tên và luật đã có.
Nếu chọn toán tử “All”: luật thỏa mãn khi cả 2 trường được thỏa mãn
Nếu chọn toán tử “Any”: luật thỏa mãn khi 1 trong 2 hoặc cả 2 trường thỏa mãn



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



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

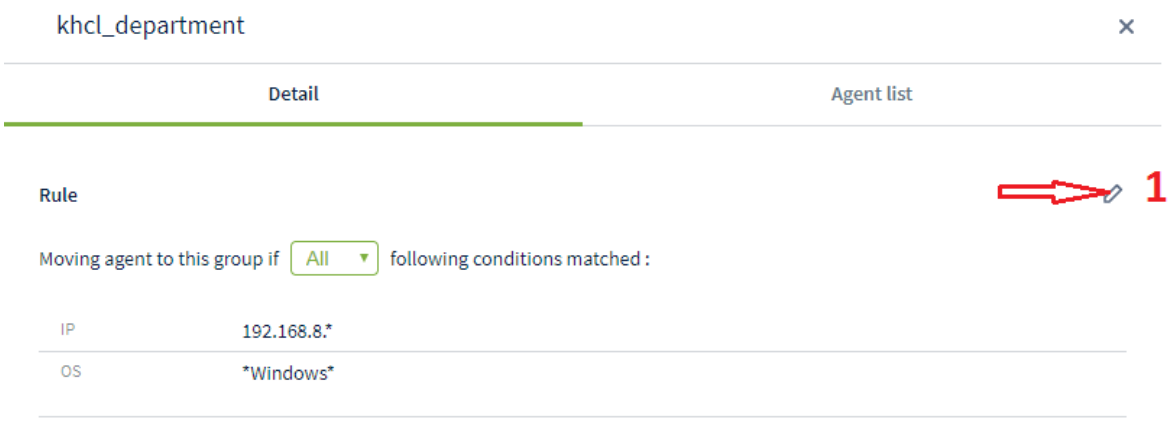
thì chuyển nhóm và được áp policy "**default**" do không chọn checkbox > áp policy mặc định.

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

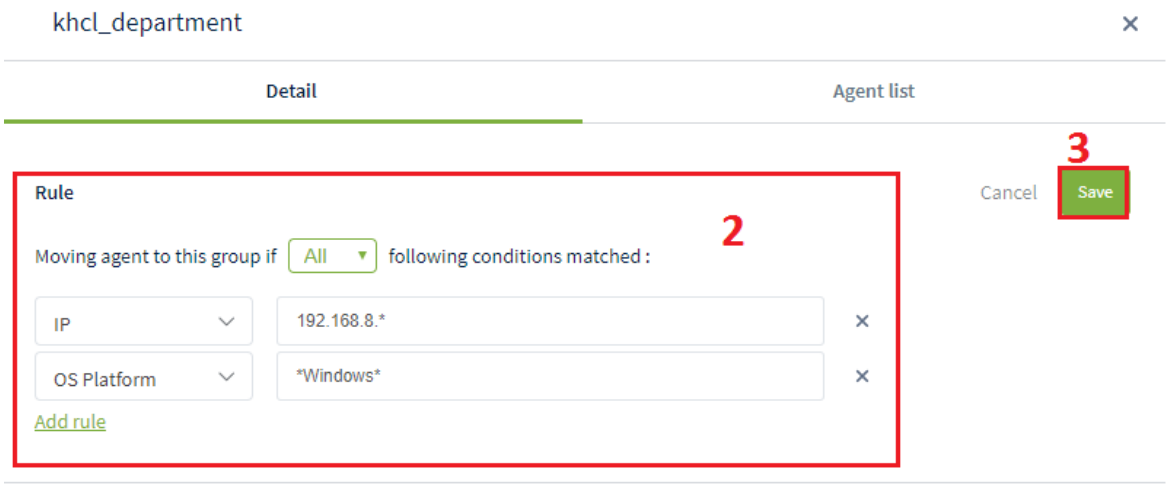
(4) Sửa nhóm: có thể lựa chọn sửa 1 hoặc 2 hoặc cả 3 thành phần trong một nhóm: Rule, Policy, Apply to

+ 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



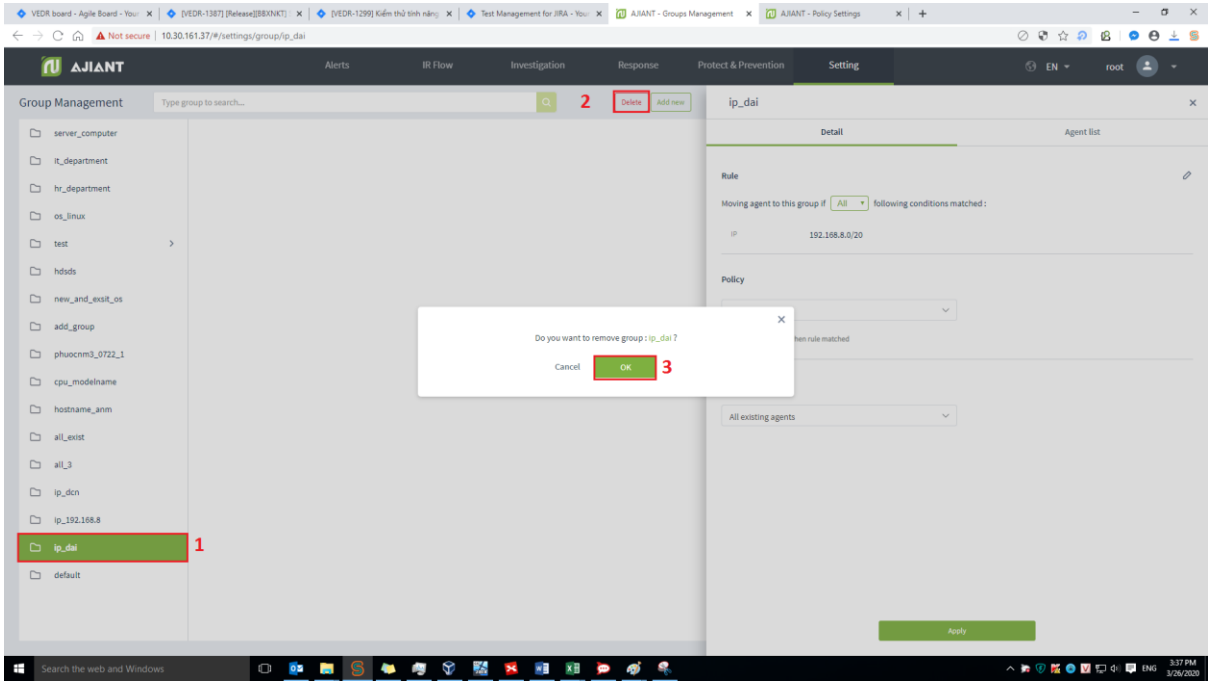
Sau đó có thể chỉnh sửa ở mục “Policy” và “Apply to” rồi click Apply

Lưu ý:

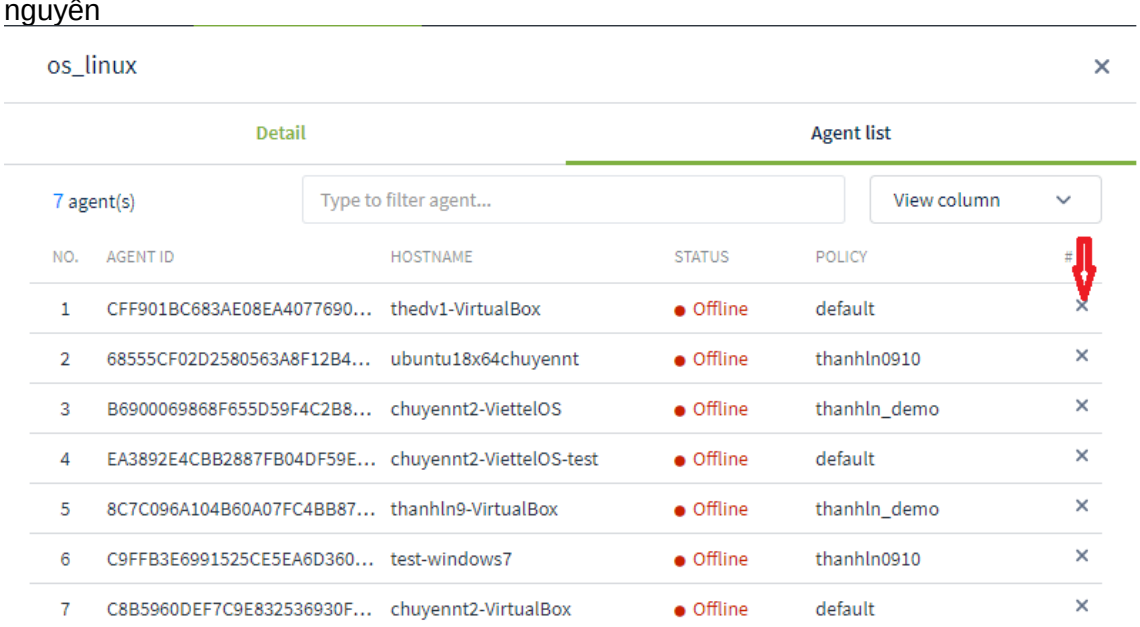
- Trường hợp sửa các thành phần của nhóm (Rule, Policy hoặc Apply to) sau đó ko click Apply thì nội dung chỉnh sửa đã được lưu lại, nhưng không cập nhật Agent list. Với các Agent cài mới thì xử lý như sau:
  + Chuyển nhóm: phụ thuộc Agent mới có được chọn ở mục “Apply to” hay không, nếu được chọn sẽ kiểm tra phía Agent, khớp luật của nhóm sẽ được chuyển vào nhóm
  +Apply policy: policy của agent phụ thuộc việc chọn checkbox “Apply policy now when rule matched”, nếu checkbox được chọn thì sẽ apply policy của nhóm, nếu không được chọn sẽ áp policy “default” do không chọn checkbox sẽ áp policy mặc định.
- Trường hợp sửa xong các thành phần của nhóm rồi click Apply thì nội dung chỉnh sửa được lưu lại, đồng thời nếu có lựa chọn “All existing agents” trong phần “Apply to” thì thực hiện quét thông tin toàn bộ agent trong hệ thống và chuyển nhóm cho agent, sau đó cập nhật Agent list.
  Đối với Agent mới xử lý tương tự như trên.

(5) Xóa nhóm hoặc xóa agent khỏi nhóm
+ User đăng nhập thuộc group root: Có thể xóa tất cả group trong hệ thống
+ User đăng nhập thuộc group default: Không được xóa group default
+ User đăng nhập thuộc group cha: Có thể xóa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login
+ User đăng nhập thuộc group một hoặc nhiều con: Có thể xóa tất cả group thuộc user đang login

Để xóa nhóm click vào nhóm cần xóa, click “Delete” sau đó click “OK” trên màn hình confirm.
Sau khi xóa 1 nhóm thì các agent thuộc nhóm sẽ chuyển về nhóm mặc định, nhóm “default”, policy giữ nguyên



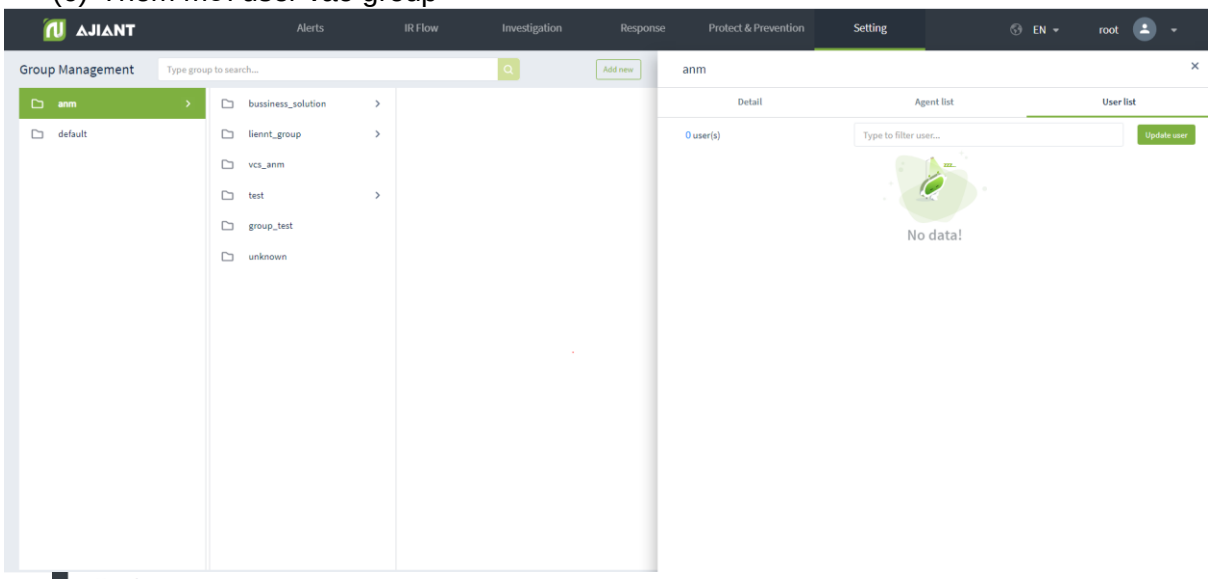
Để xóa Agent khỏi nhóm thì click vào tab Agent list, click icon “x” để xóa agent khỏi nhóm.
Sau khi xóa agent khỏi nhóm thì agent được chuyển về nhóm mặc định: “default”, policy giữ nguyên

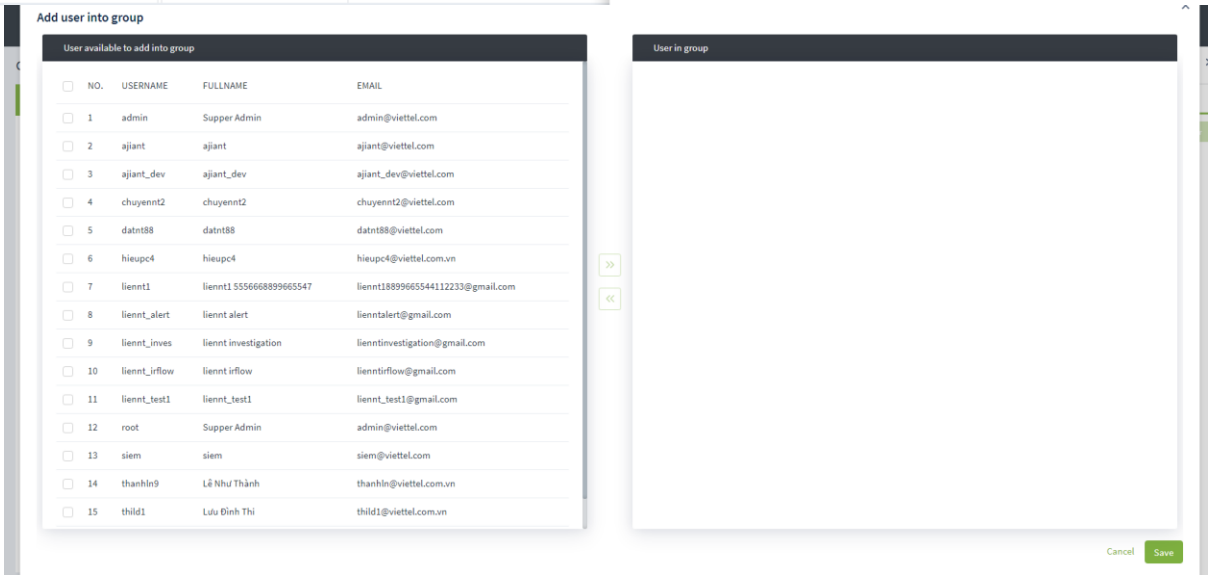


Lưu ý: trường hợp xóa một nhóm cha:

- Xóa tất cả nhóm con
- Chuyển tất cả agent của nhóm cha và các nhóm con về nhóm mặc định: “default”
- Giữ nguyên policy của các agent trong nhóm cha và con

(6) Thêm mới user vào group

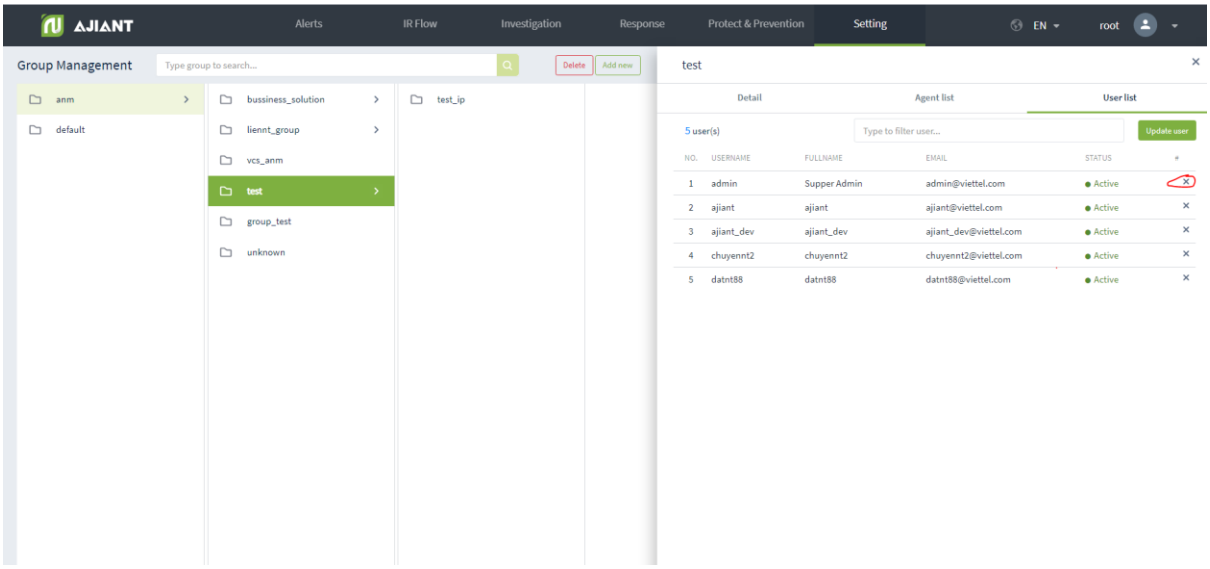




Danh sách user:

+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống
+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default
+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login
+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login

(7) Xóa user



3.8.4 Account Management

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

3.8.4.1 Permission management

- Quản lý các quyền truy cập vào tài nguyên (API) của hệ thống. 1 permission là quyền truy cập vào 1 tài nguyên xác định (API) của hệ thống.
- Các chức năng chính trên màn hình này:

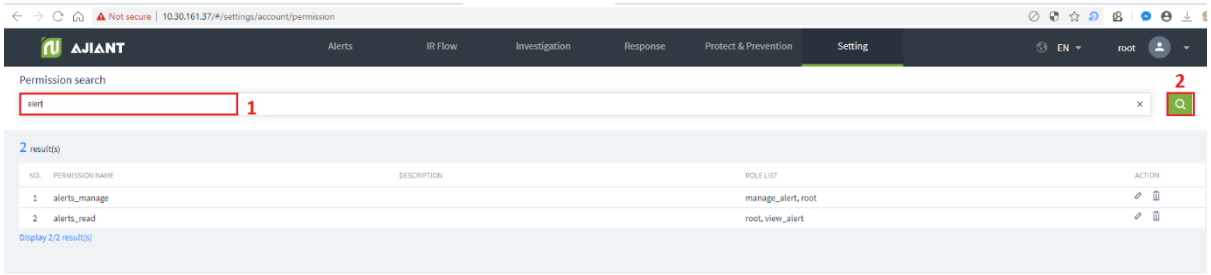
  + Quản lý các permission

  + Tìm kiếm permission

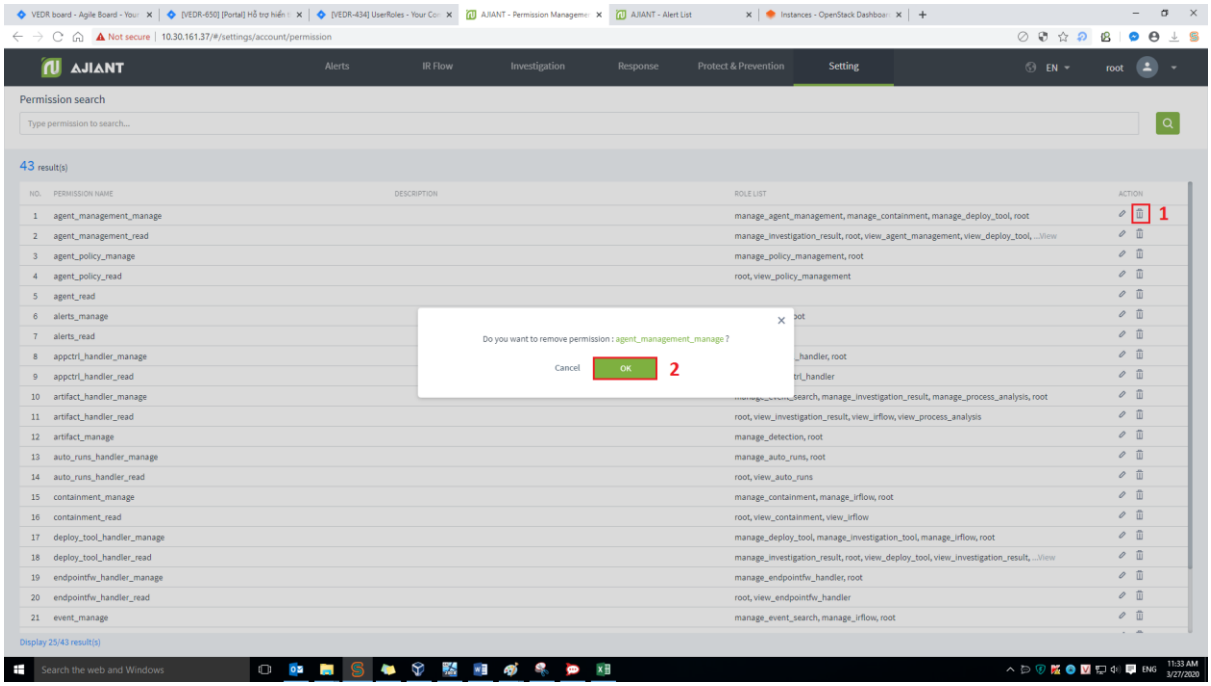
  + Xóa permission

(1) Quản lý các permission: hiển thị toàn bộ các permission của hệ thống. Trong trường hợp xóa permission trên màn hình này, khi thực hiện các chức năng trên portal mà bị thiếu permission thì sẽ tự động thêm permission đã xóa trên màn hình quản lý Permission

(2) Tìm kiếm permission: nhập ký tự tìm kiếm vào texbox Search > click Enter hoặc Search => hiển thị danh sách permission thỏa mãn



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



3.8.4.2 Role Management

- Quản lý các role (nhóm quyền hay nhóm permission) của hệ thống.
- Các chức năng trên màn hình này bao gồm:

  + Quản lý danh sách role:

    - User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống
    - User đăng nhập thuộc Role default: Hiển thị Role default
    - User đăng nhập thuộc Role cha: Hiển thị tất cả Role thuộc của user đang login và group con tương ứng
    - User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login

  + Tìm kiếm role

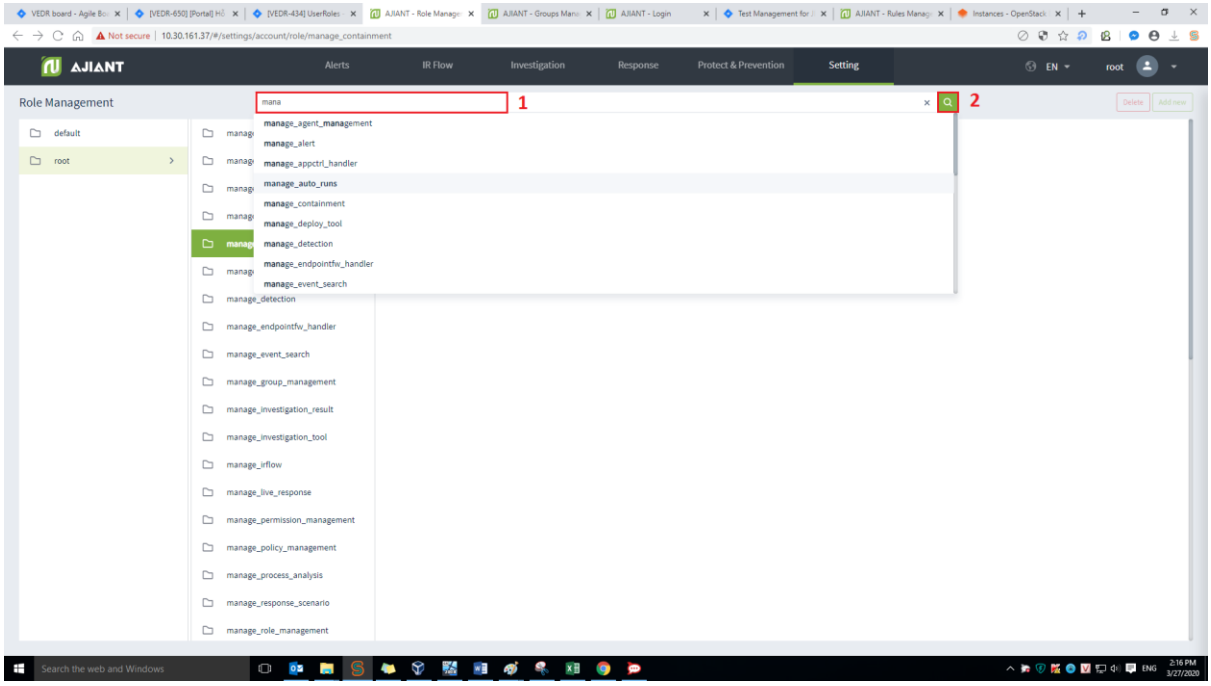
  + Thêm mới role

  + Xóa role

(1) Quản lý danh sách role: quản lý danh sách role theo dạng cây. Có 2 role ở gốc mặc định đã tạo sẵn: role “default” và “root”
Role “default”: User có quyền “default” chỉ có quyền truy cập vào Portal, không có quyền xem dữ liệu hoặc thao tác chức năng
Role “root”: bao gồm toàn bộ các role của hệ thống, User có role “root” có toàn bộ quyền sử dụng tất cả chức năng trên Portal
Click vào 1 role sẽ hiển thị thông tin chi tiết của role. Một role sẽ bao gồm các thông tin: tên role, danh sách các permission, danh sách User (tài khoản) chứa role, role cha hoặc danh sách role con (nếu có)

(2) Tìm kiếm role

- Cách 1: Click vào textbox Search > hiển thị danh sách các role trong hệ thống và có thể scroll được danh sách role > Lựa chọn role trong danh sách hiện ra
- Cách 2: Click vào textbox Search > Nhập ký tự tìm kiếm vào textbox > Hệ thống lọc ra các role chứa ký tự tìm kiếm > chọn role trong danh sách đã lọc hoặc click Enter hoặc click button Search



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

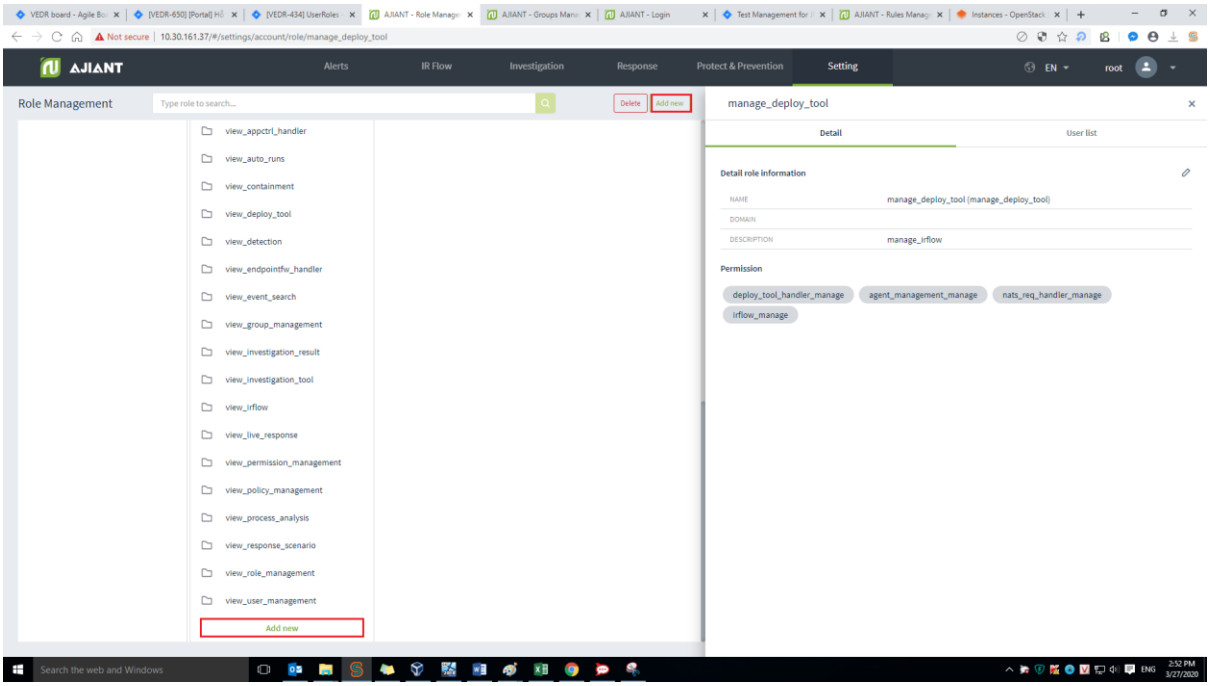
+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị Go to role. Click vào "Go to role" đưa về danh sách role dạng cây ban đầu
+ Khi click vào menu góc phải mỗi bản ghi cũng hiển thị option: Go to role

(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

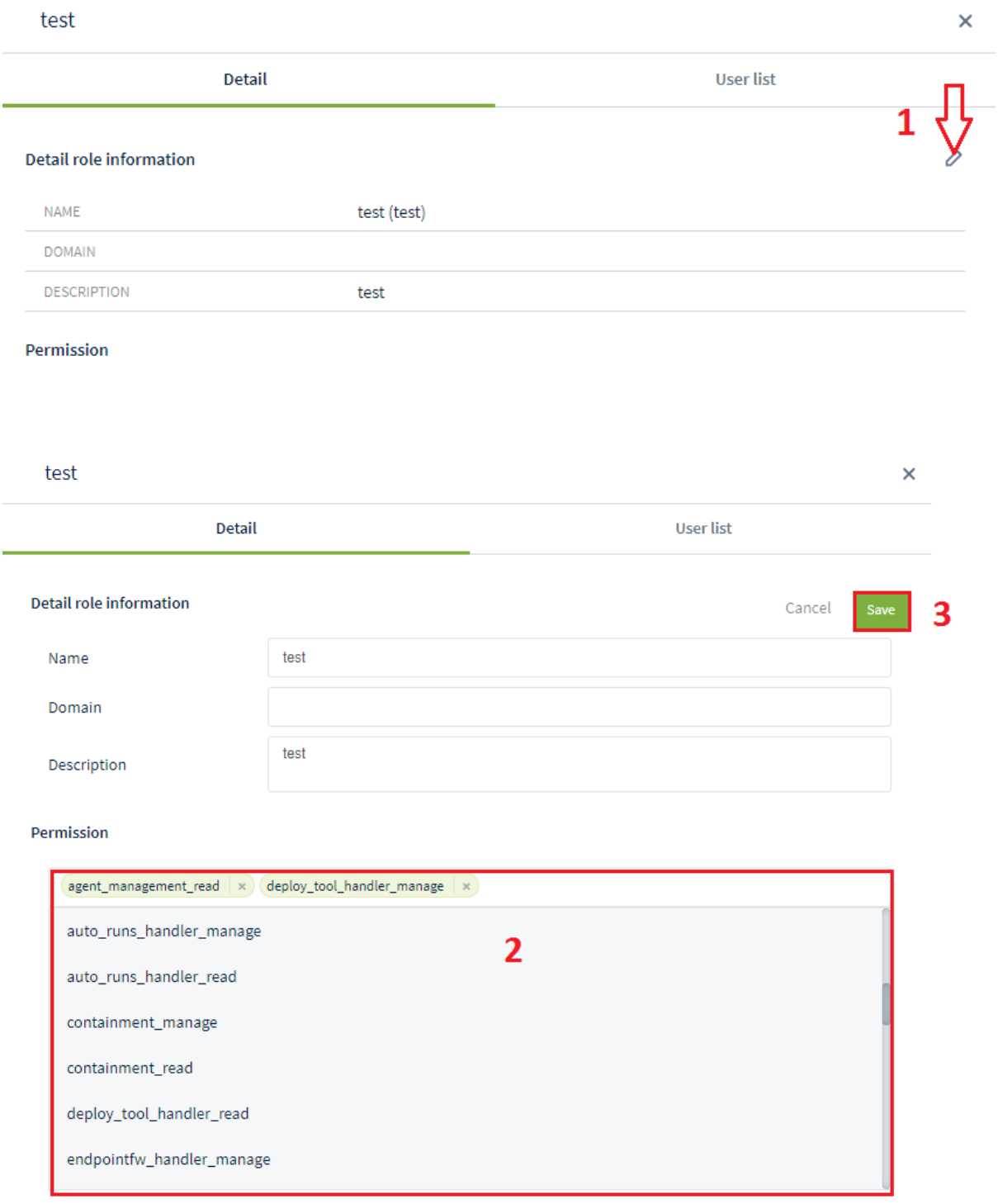
- Bước 1: Có các cách tạo mới role như sau:
- Click vào 1 role sau đó hover vào cuối danh sách role chọn "Add new" để tạo role cùng cấp với role đã chọn

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.



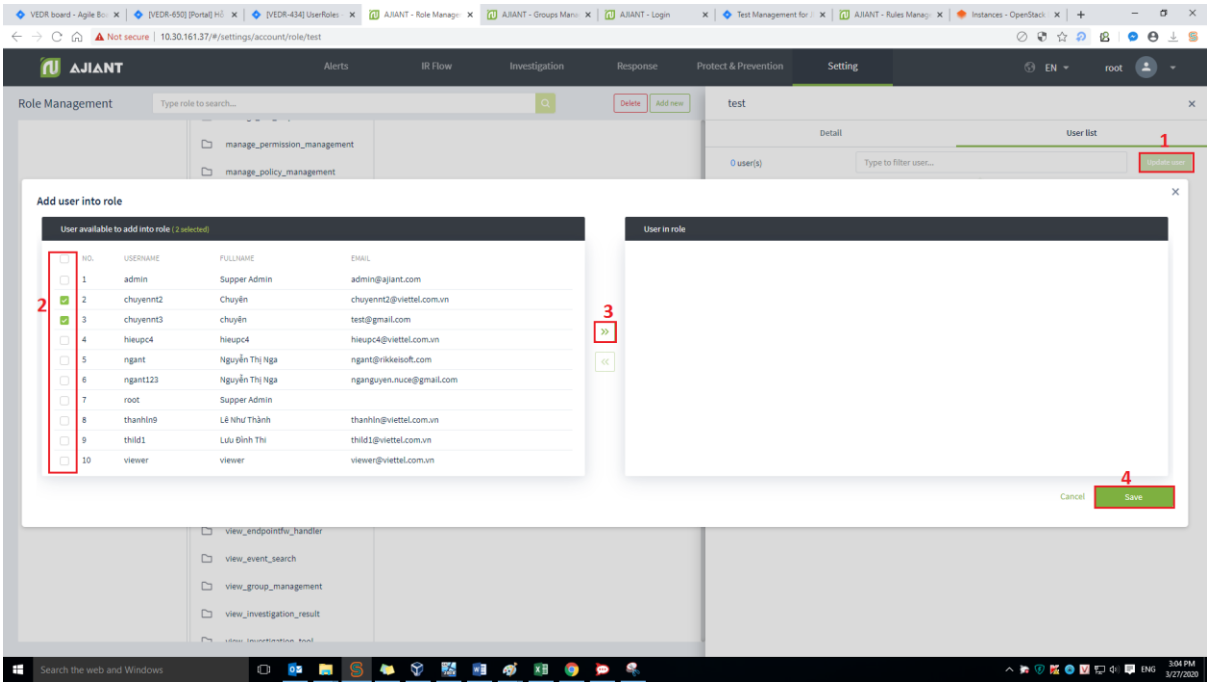
- Bước 2: click icon Edit để thêm thông tin permission cho role > Lựa chọn permission để thêm vào role > click Save

  + 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.

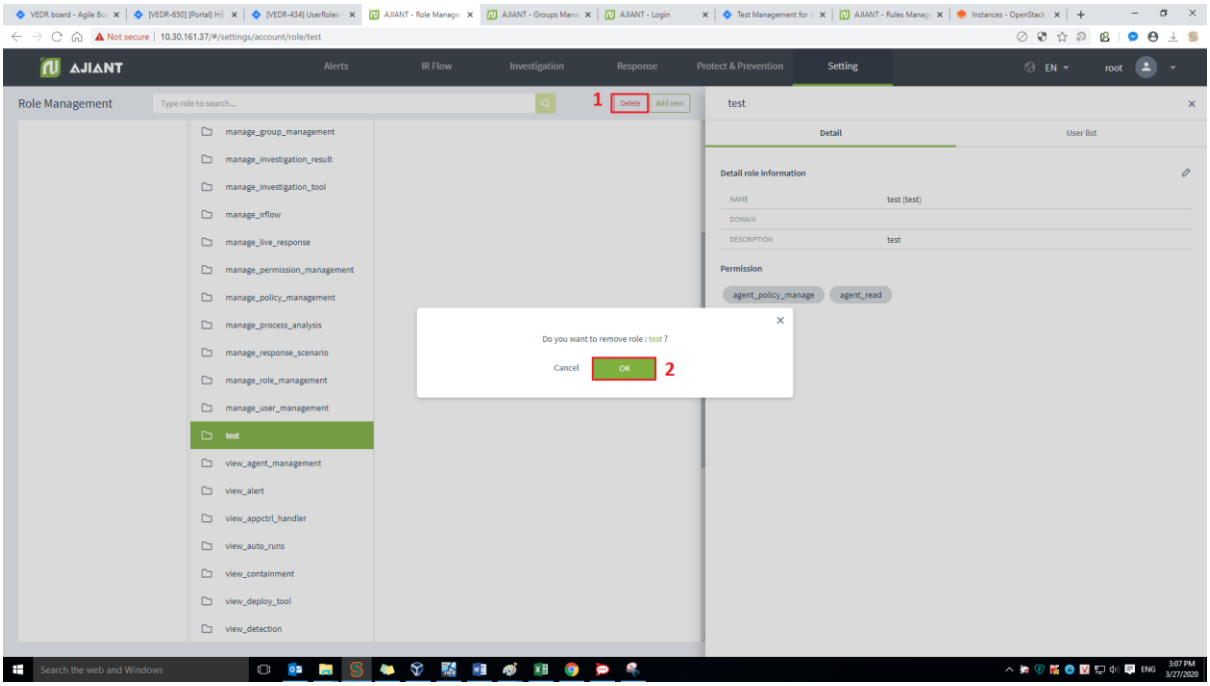


- Bước 3: Chuyển sang tab User list để thêm role vào danh sách role của User
  + User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống

+ 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



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

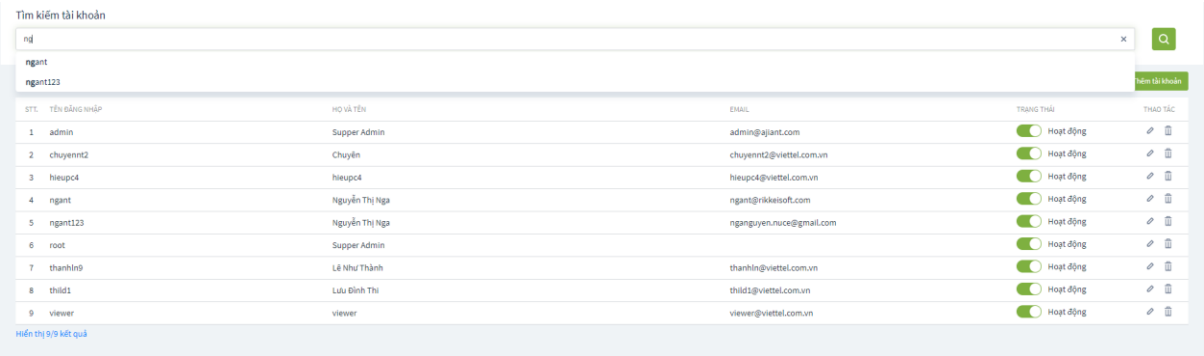


Lưu ý: Sau khi xóa 1 role, tất cả các user sử dụng role này được thay đổi: Nếu user X nằm trong role bị xóa và user X chỉ có 1 role thì chuyển user X về role mặc định, ngược lại, nếu user X có nhiều role thì chỉ loại bỏ role bị xóa ra khỏi danh sách role của user X.

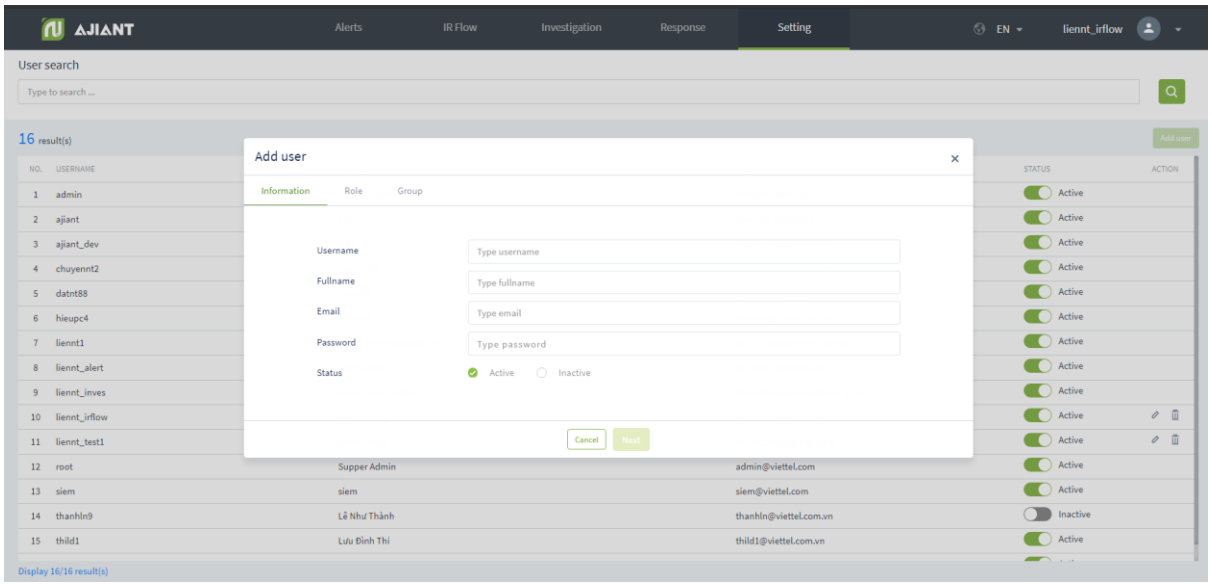
3.8.4.3 User management

- Quản lý các tài khoản đăng nhập vào hệ thống Portal VCS-aJiant.
- Các chức năng chính trên màn hình này gồm có:
  + Tìm kiếm tài khoản
  + Thêm mới tài khoản
  + Chỉnh sửa tài khoản
  + Xóa tài khoản

(1) Tìm kiếm tài khoản: click vào textbox Search > hiện danh sách các tài khoản trong hệ thống > Lựa chọn tài khoản cần tìm kiếm trong danh sách hoặc nhập ký tự <text> vào textbox để lọc bớt các tài khoản> Click “Search” hoặc chọn tài khoản cần tìm trong danh sách các tài khoản đã được lọc



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



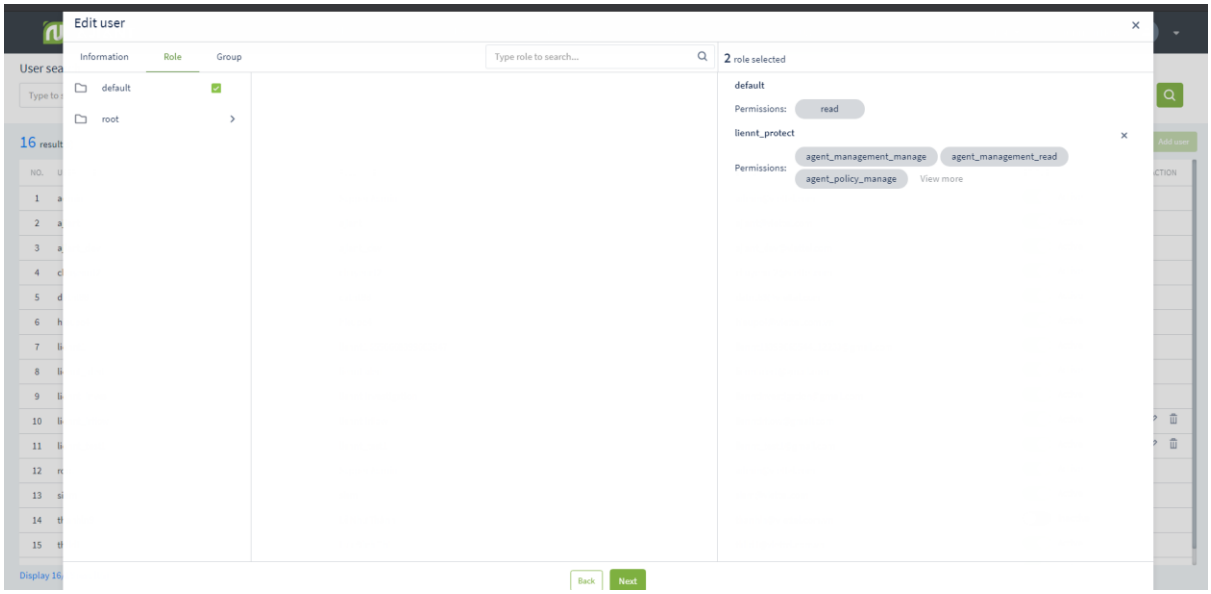
- Lựa chọn role (nhóm quyền) sẽ gán cho tài khoản, sau đó click “next”
- Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó

  + User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống

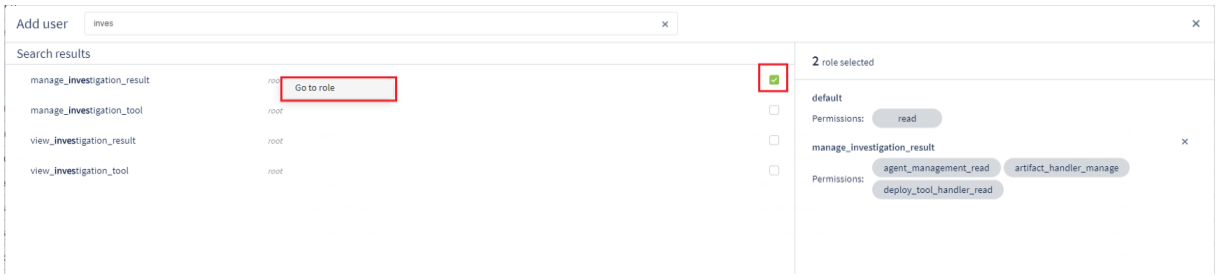
  + User đăng nhập thuộc Role default: Hiển thị Role default

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

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

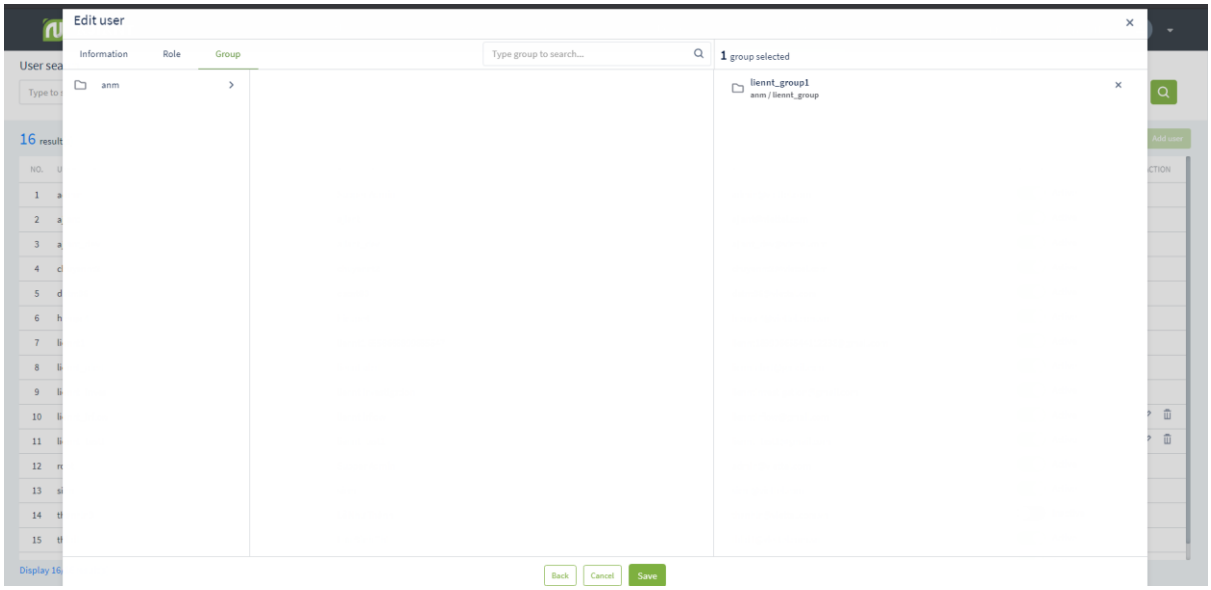


- Trên màn hình add role cho User, có thể tìm kiếm các role tương tự phần tìm kiếm tài khoản, sau khi nhập các ký tự tìm kiếm vào textbox “Search” > click icon Search hoặc Enter hiện màn hình các role thỏa mãn điều kiện tìm kiếm.

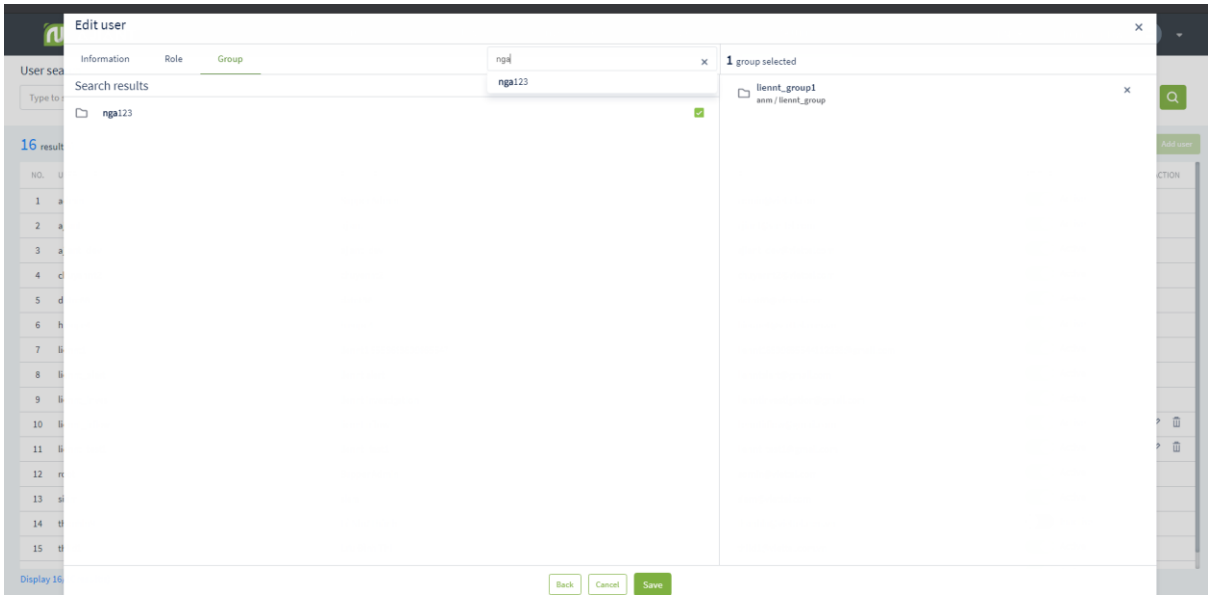


- Click chọn checkbox tương ứng với role cần thêm, sau đó click “Go to role” để về màn hình danh sách role ban đầu, sau đó click “Create” để tạo tài khoản.
- Lưu ý: Tài khoản đang đăng nhập tạo 1 tài khoản mới chỉ tạo được các tài khoản chứa các role con thuộc danh sách role mà tài khoản đang đăng nhập được cấp.
- Lựa chọn group sẽ gán cho tài khoản, sau đó click “Create”
- Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó

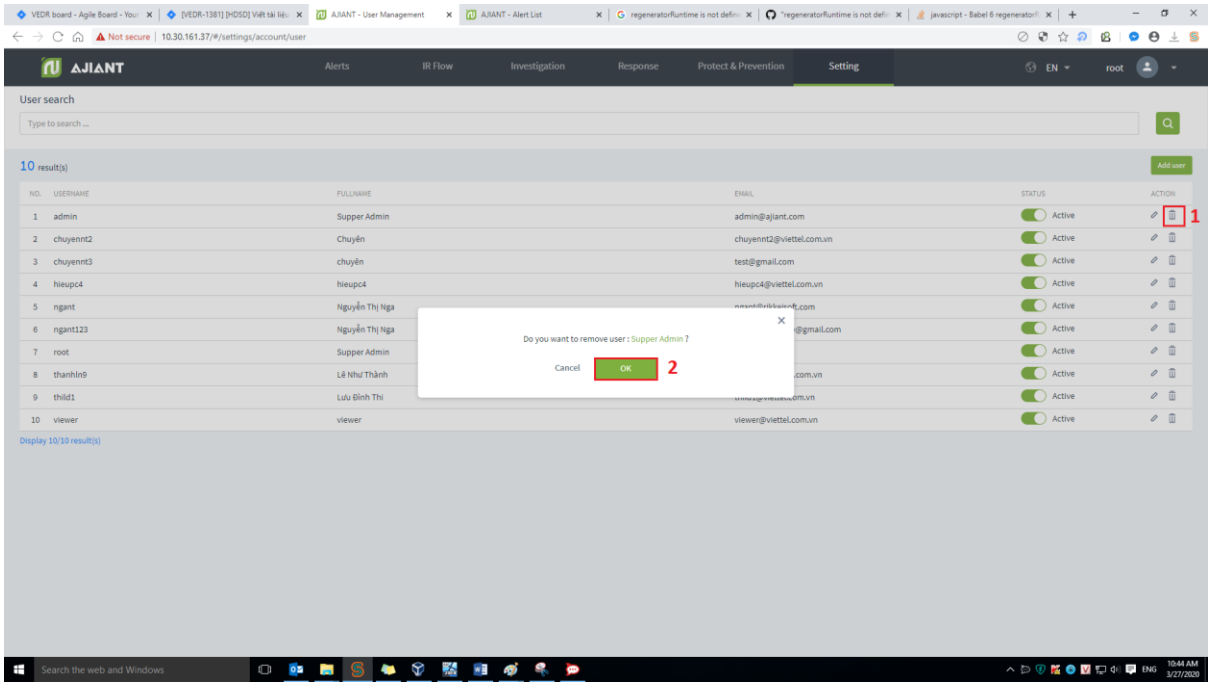
  + User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống
  + User đăng nhập thuộc group default: Hiển thị group default
  + User đăng nhập thuộc group cha: Hiển thị Group thuộc group của user đang login và group con tương ứng
  + User đăng nhập thuộc group một hoặc nhiều con: Hiển thị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



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



(3) Xóa tài khoản: click vào icon Xóa sau đó click OK trên màn hình confirm
Kiểm tra hiển thị icon xóa:
+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống
+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default
+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login
+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login

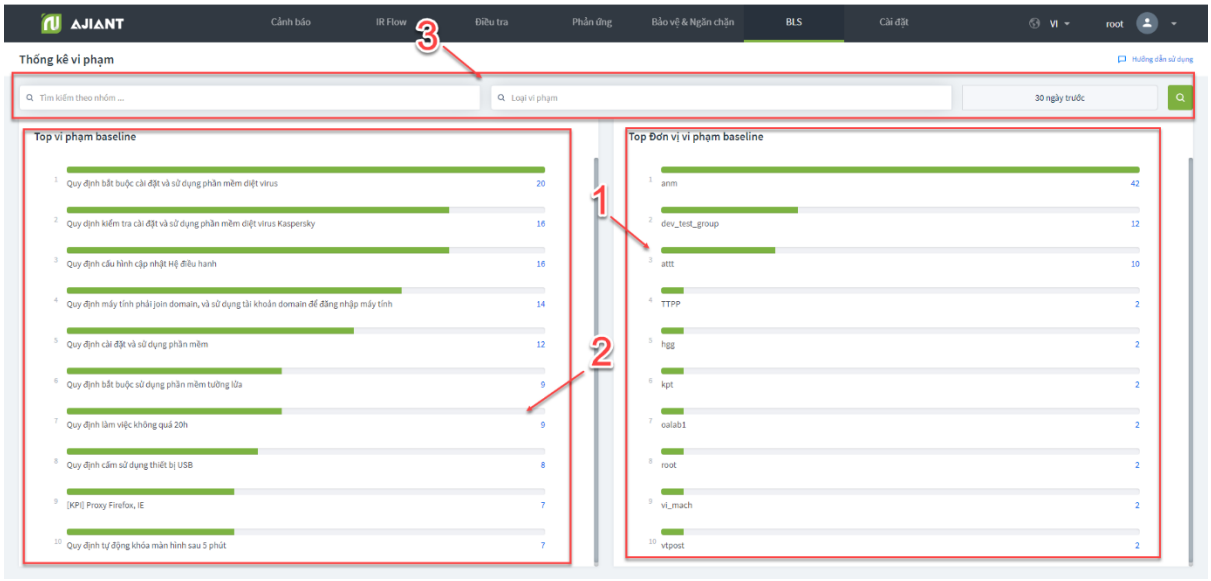


3.9 Màn hình BLS

3.9.1 Thống kê vi phạm (Violation statistic)

- Chức năng Thống kê vi phạm hỗ trợ người quản trị thống kê các vi phạm của agent đã cài đặt bao gồm:
  + Top các vi phạm base line, top đơn vị vi phạm baseline
  + Xem danh sách các vi phạm và danh sách agent vi phạm trong từng đơn vị
  + Xem danh sách các đơn vị vi phạm và danh sách vi phạm trong từng đơn vị
  + Xem chi tiết của Agent
  + Export vi phạm
  + Report vi phạm
- Click vào tab BLS >> Thống kê vi phạm

3.9.1.1 Màn hình Thống kê vi phạm



- Hệ thống hỗ trợ thực hiện các tính năng:

(1) Thống kê Top 10 vi phạm base line nhiều nhất sắp xếp theo thứ tự giảm dần

Mỗi bản ghi được hiển thị các thông tin gồm: Nội dung vi phạm, số lượng máy vi phạm.
Chọn bản ghi bất kì trong Top vi phạm baseline, hệ thống sẽ di chuyển đến màn hình chi tiết tương ứng với vi phạm đã được chọn

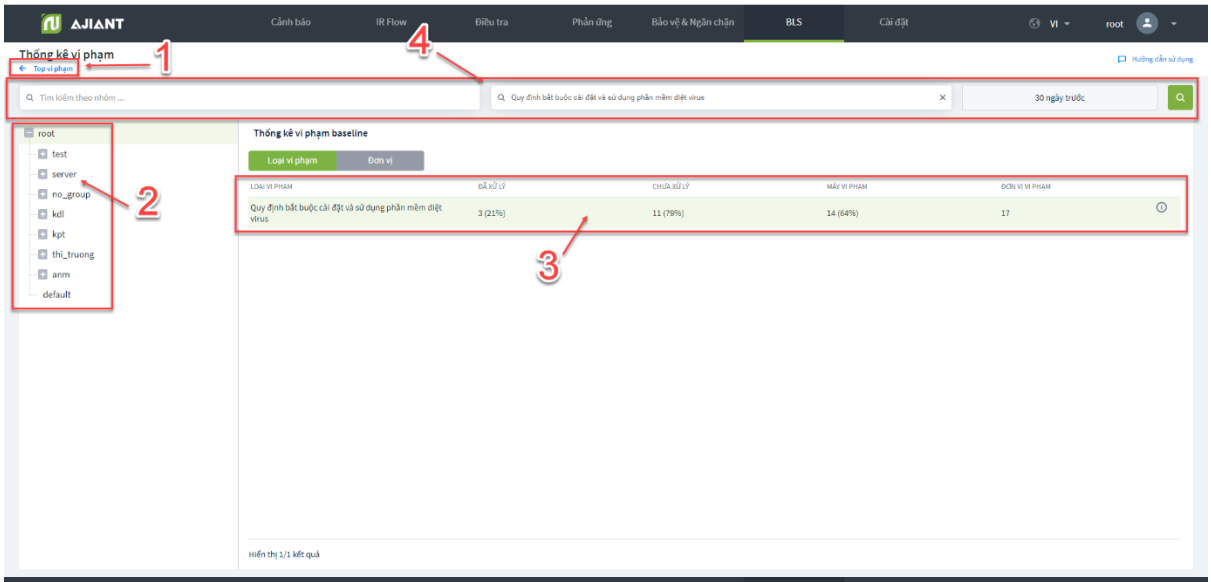
(2) Thống kê Top 10 đơn vị vi phạm base line nhiều nhất sắp xếp theo thứ tự giảm dần

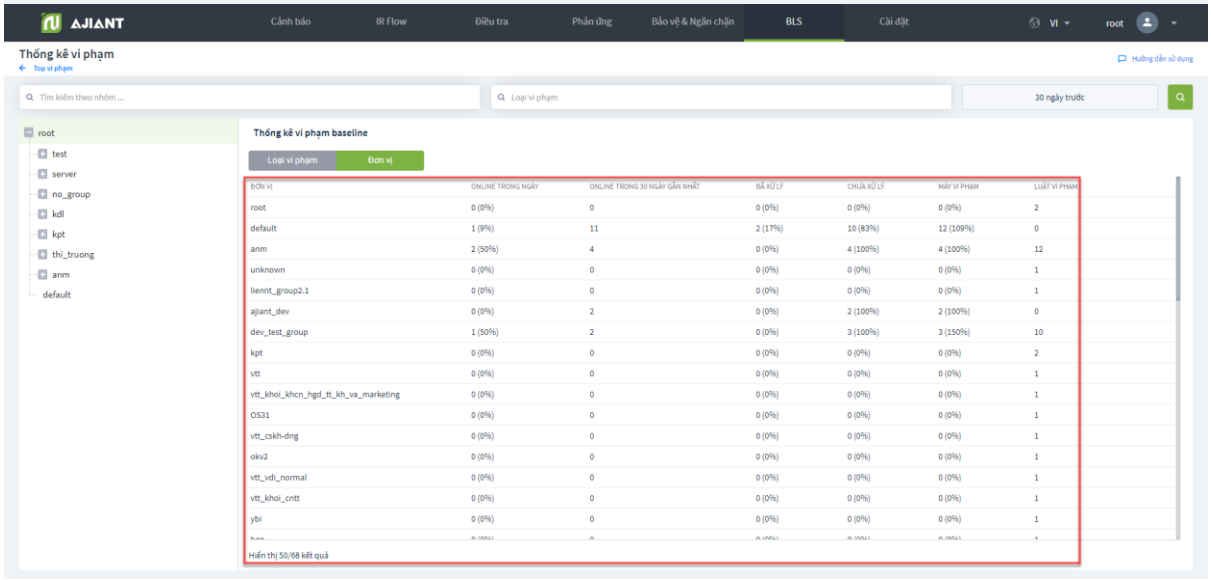
Mỗi bản ghi được hiển thị các thông tin gồm: Tên đơn vị vi phạm, số lượng máy vi phạm.
Chọn bản ghi bất kì trong Top đơn vị vi phạm baseline, hệ thống sẽ di chuyển đến màn hình chi tiết tương ứng với đơn vị đã được chọn

(3) Tìm kiếm

Tìm kiếm riêng lẻ:
+ Tìm kiếm theo Đơn vị
-> Top đơn vị vi phạm hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng (nếu có)
-> Top vi phạm: Hiển thị các vi phạm của đơn vị và đơn vị con (nếu có) tương ứng
+ Loại vi phạm
-> Top đơn vị vi phạm: hiển thị danh sách đơn vị vi phạm Loại vi phạm đã chọn
-> Top vi phạm: Hiển thị vi phạm đã chọn
+ Thời gian bị vi phạm
Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

3.9.1.2 Tab Loại vi phạm





- Hệ thống hỗ trợ thực hiện các tính năng:

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

(2) Cây dữ liệu đơn vị của hệ thống

Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con

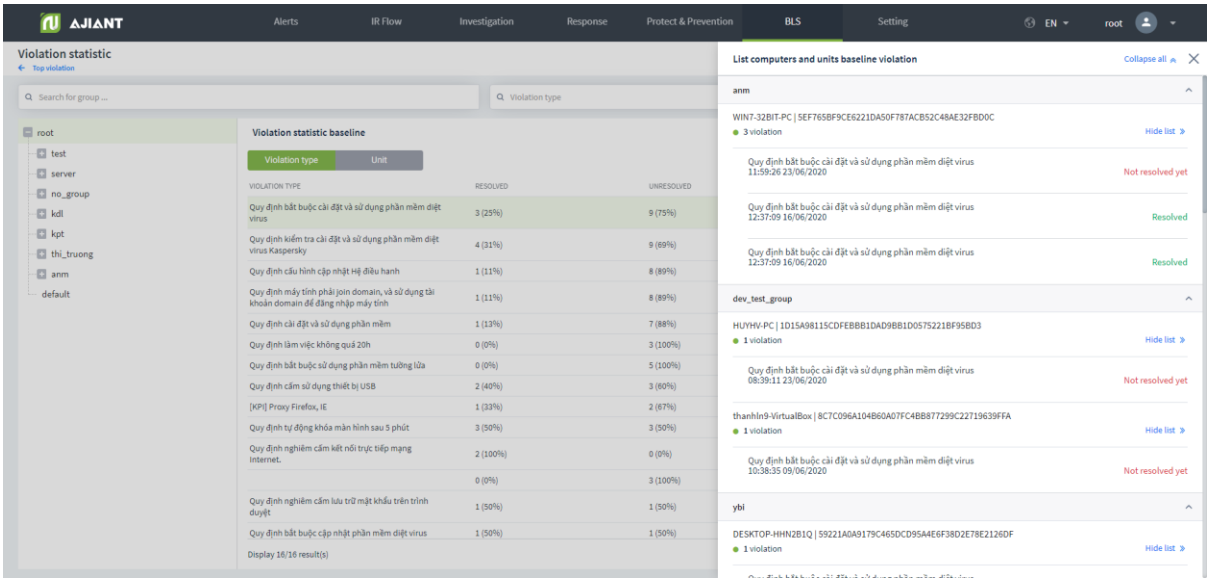
Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc vi phạm

(3) Tab Loại vi phạm

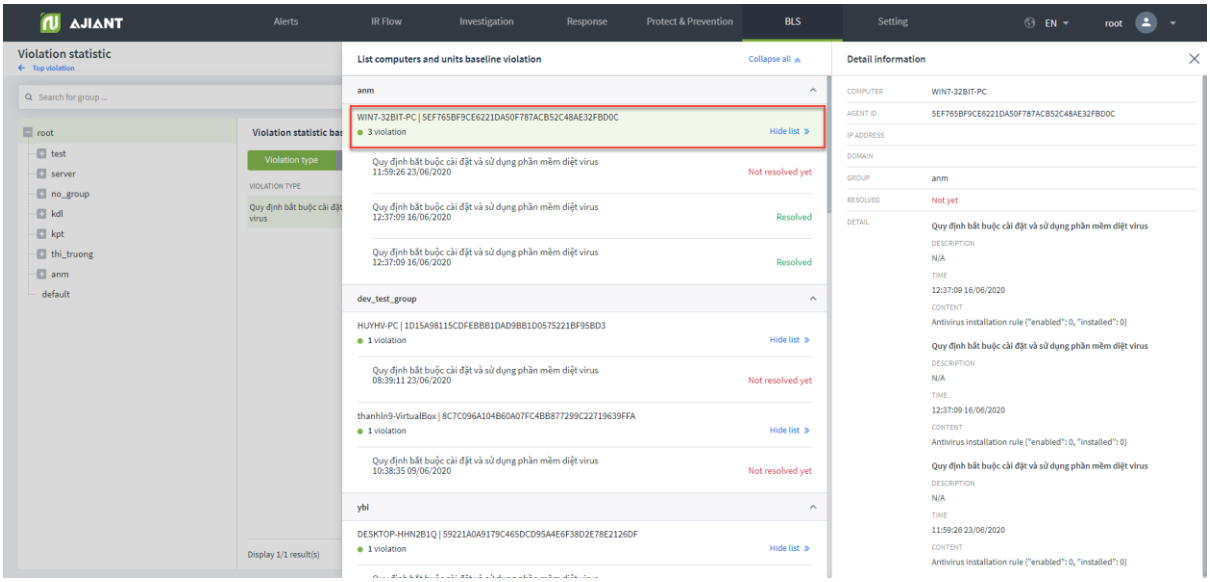
Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Violation type, Resolved, Unresolved, Violation Computer, Violation unit

Chọn bản ghi Loại vi phạm trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm

Chọn máy tính: Hiển thị thông tin chi tiết máy tính và danh sách vi phạm tương ứng của máy tính



Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (tất cả loại vi phạm của máy)



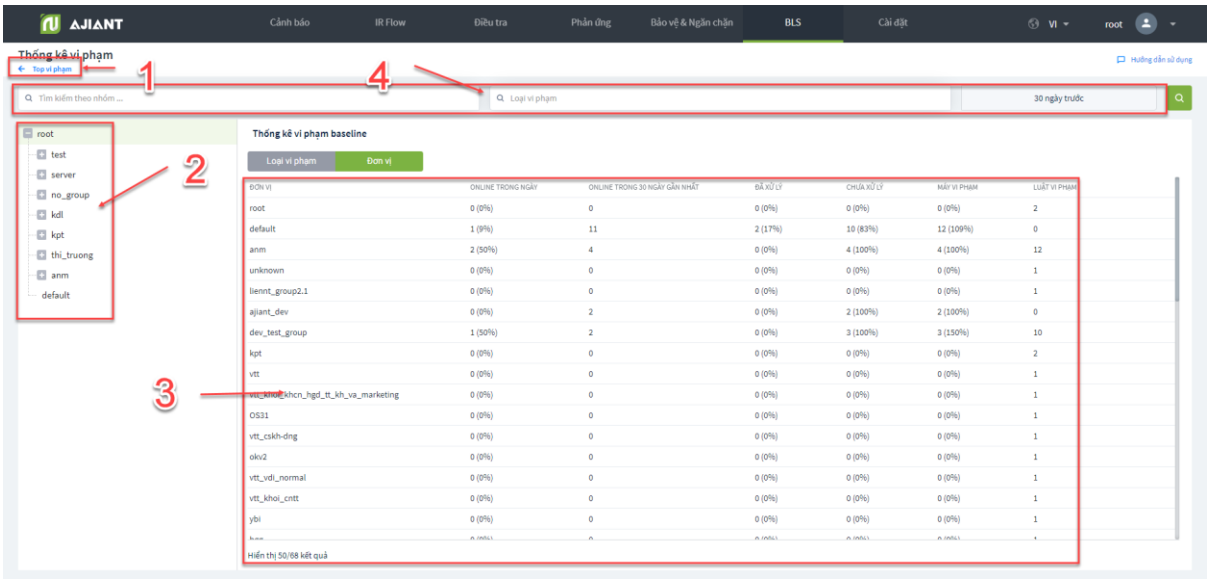
(4) Tìm kiếm

Tìm kiếm riêng lẻ:

+ Tìm kiếm theo Đơn vị: Hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng

+ Loại vi phạm: Hiển thị vi phạm đã chọn
+ Thời gian bị vi phạm
Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

3.9.1.3 Tab Đơn vị



- Hệ thống hỗ trợ thực hiện các tính năng:

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

(2) Cây dữ liệu đơn vị của hệ thống

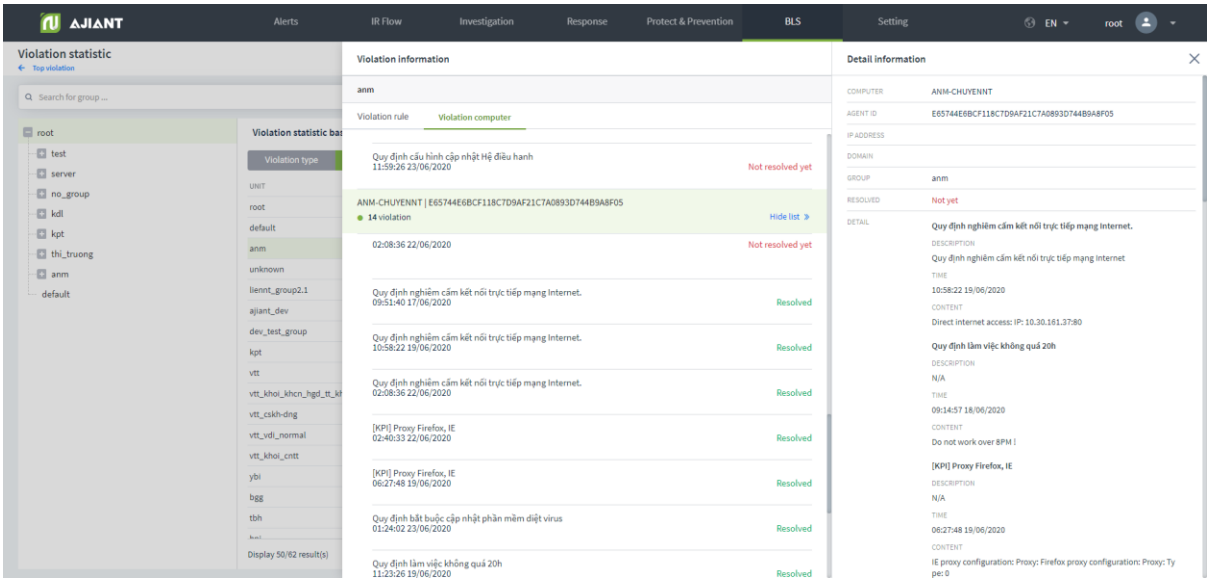
Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con

Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc đơn vị cha - con

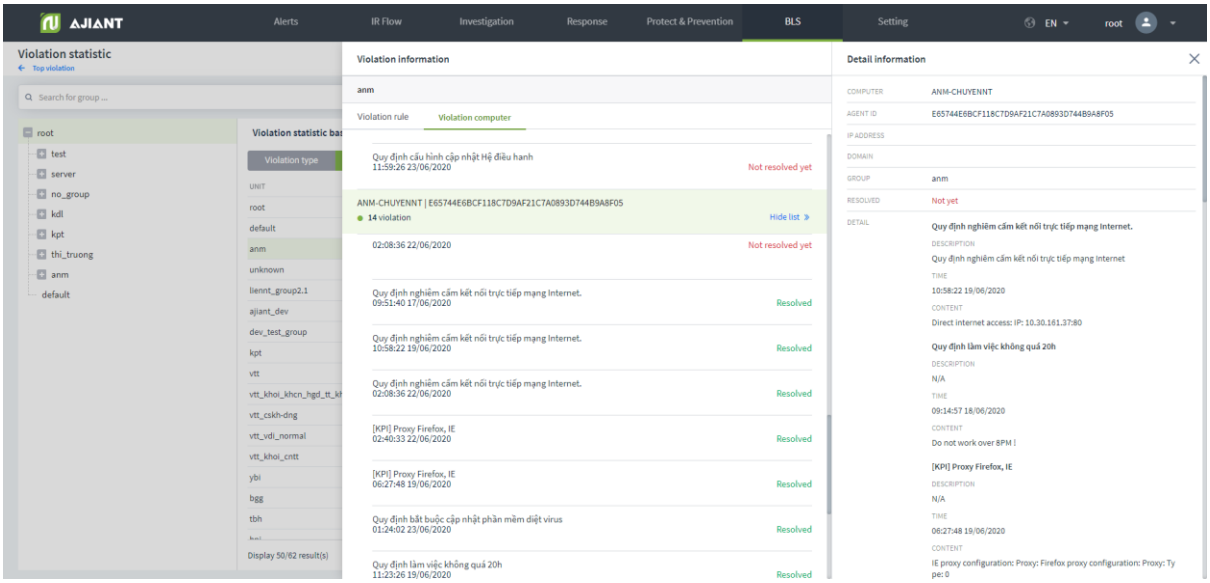
(3) Tab Đon vị

Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Unit, Online in day, Online in 30 days recent, Resolved, Unresolved, Violation computer, Violation rule

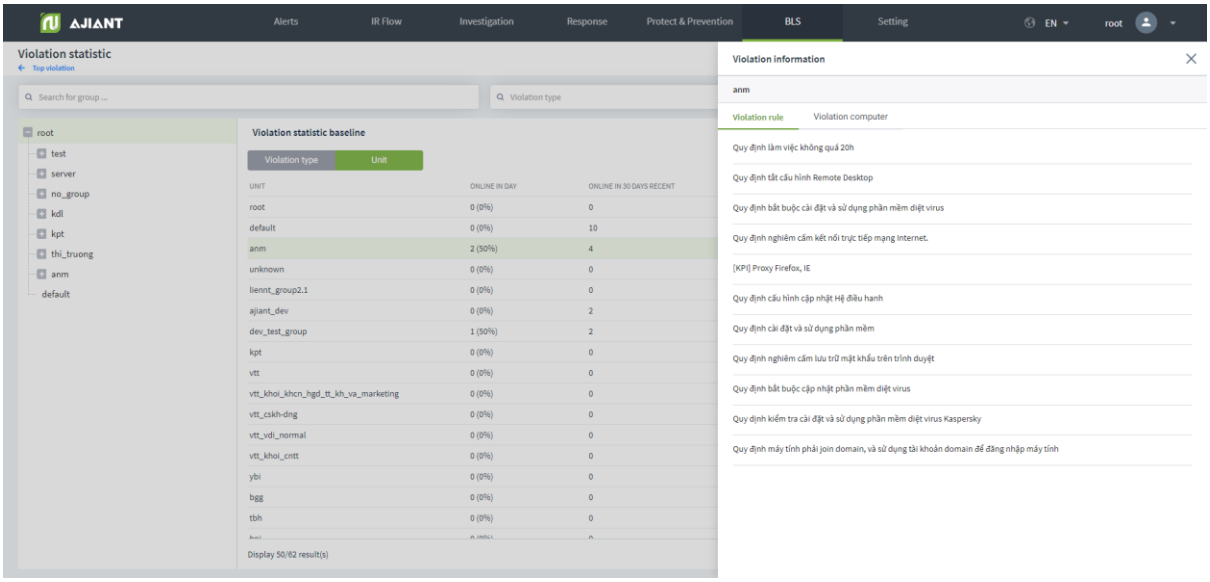
Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm bao gồm Tên đơn vị, Tên máy tính|Agent ID, danh sách vi phạm của từng máy, thời gian vi phạm, trạng thái vi phạm (đã fix hay chưa fix vi phạm)



Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (tất cả loại vi phạm của máy)



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



(4) Tìm kiếm

Tìm kiếm riêng lẻ:
+ Tìm kiếm theo Đơn vị: Hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng
+ Loại vi phạm: Hiển thị vi phạm đã chọn
+ Thời gian bị vi phạm
Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

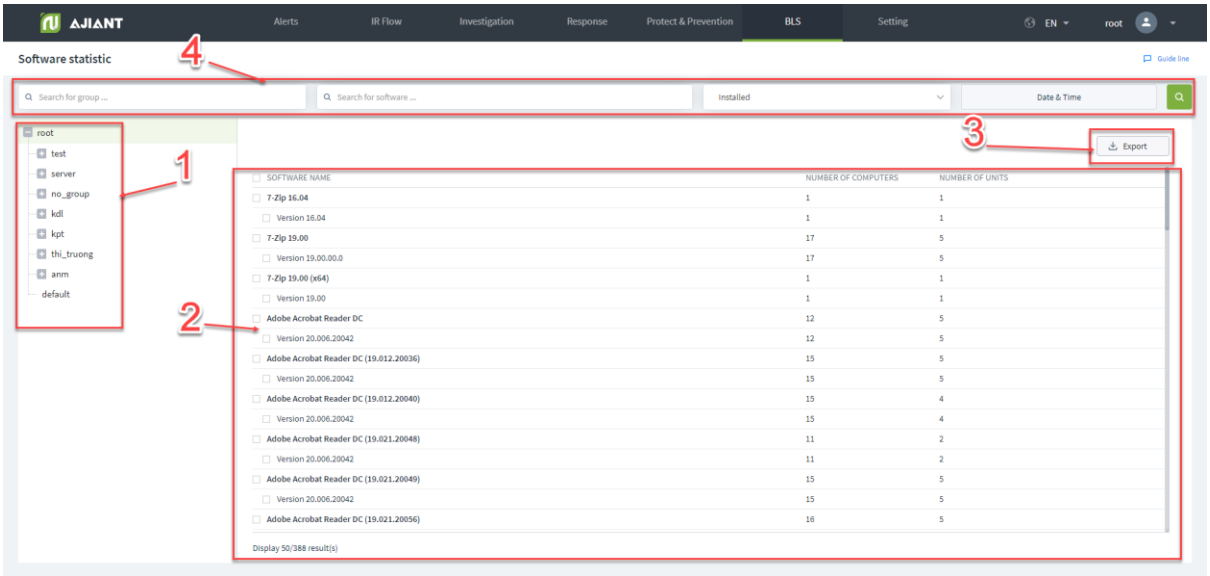
3.9.2 Thống kê phần mềm (Software statistic)

- Chức năng Thống kê phần mềm hỗ trợ người quản trị thống kê các phần mềm đã cài đặt trong một đơn vị bao gồm:

  + Xem danh sách các phần mềm đã cài trong 1 đơn vị được chọn

  + Xem chi tiết của Agent

  + Export phần mềm



- Hệ thống hỗ trợ thực hiện các tính năng:

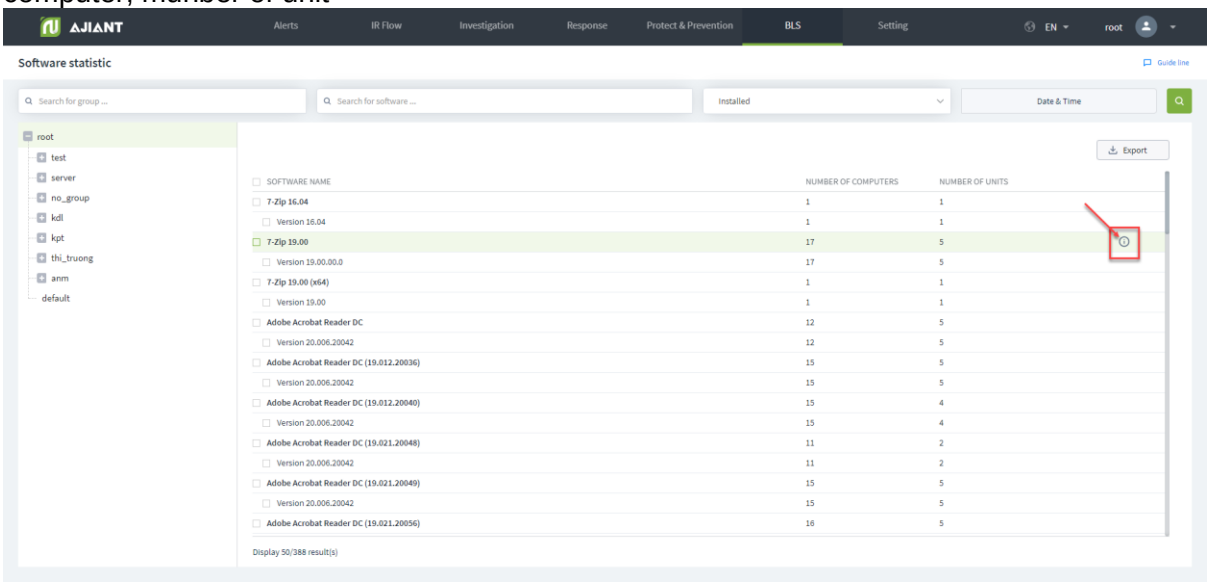
(1) Cây dữ liệu đơn vị của hệ thống

Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con

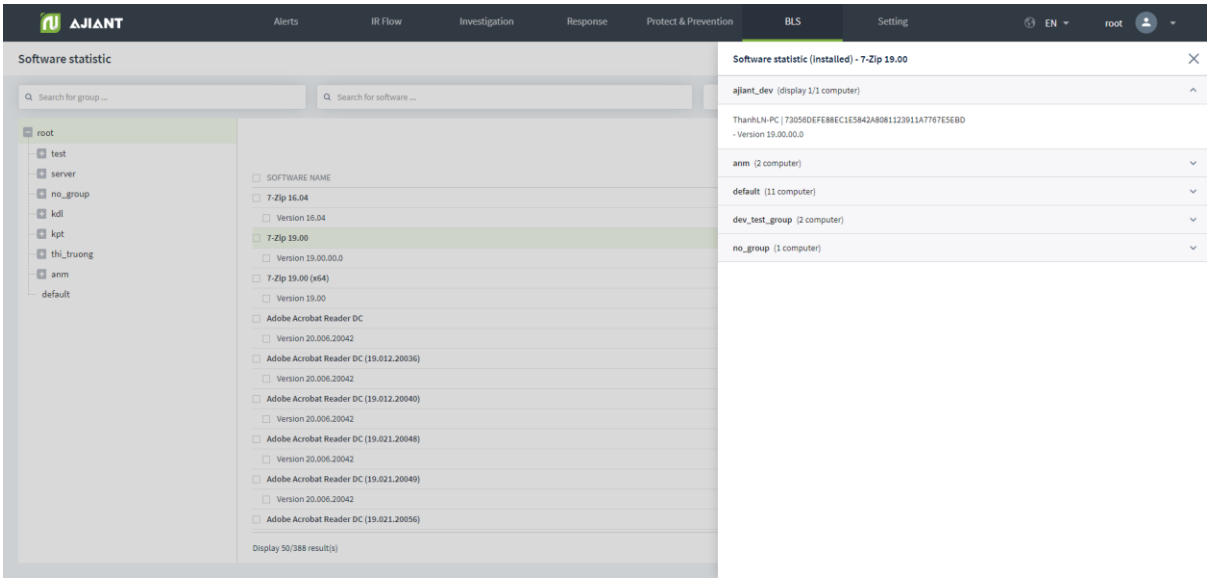
Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc phần mềm

(2) Danh sách phần mềm

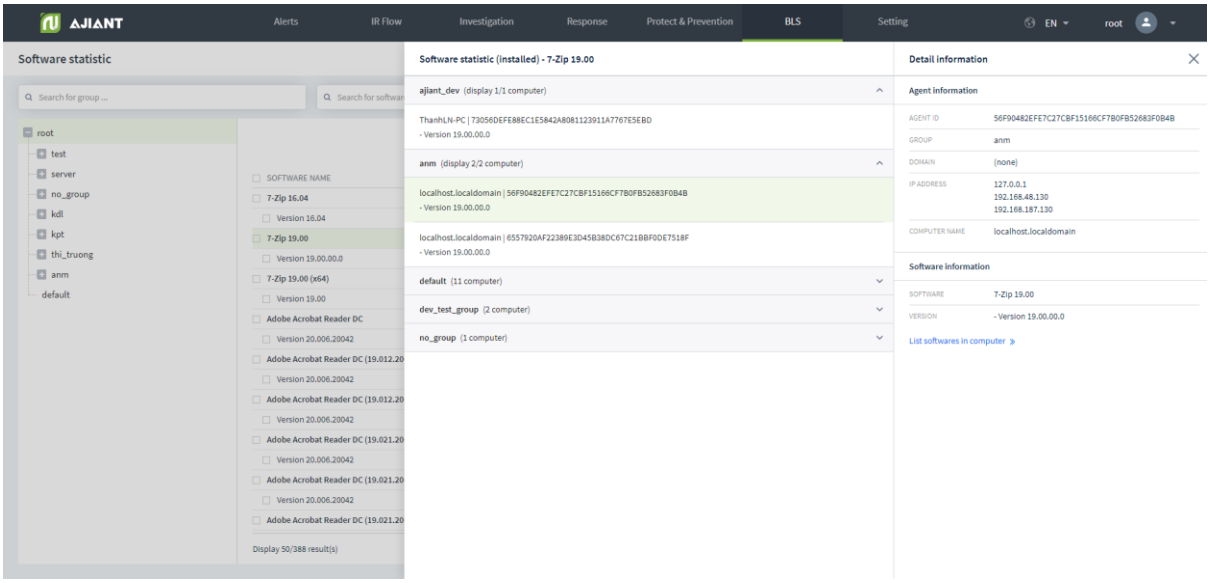
Mỗi phần mềm được hiển thị các thông tin chung gồm: Software name, munber of computer, munber of unit



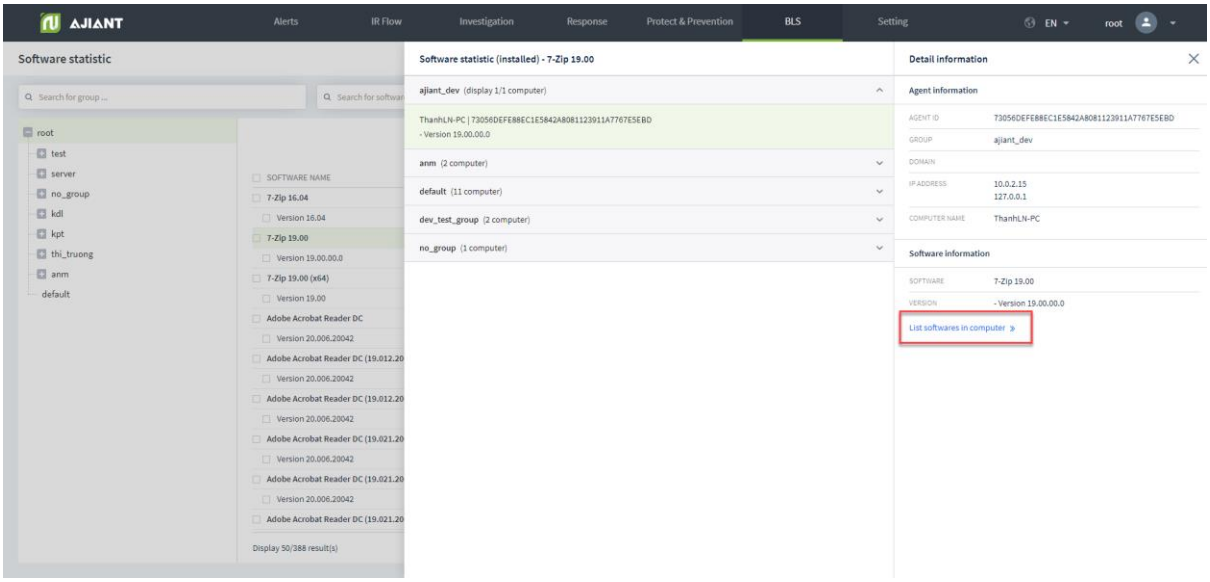
Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị bao gồm Tên đơn vị, Tên máy tính|Agent ID, Version



Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Software information (software name, version)



Chọn link [List softwares in computer]: Hệ thống đi chuyển đến màn hình Agent management và popup chi tiết máy tính tương ứng đã chọn hiển thị



(3) Tìm kiếm

Tìm kiếm riêng lẻ:
+ Tìm kiếm theo Đơn vị: Hiển thị các phần mềm đã cài trong đơn vị
+ Tên phần mềm: hiển thị danh sách phần mềm đã nhập
+ Tìm kiếm theo trạng thái: Installed, uninstalled
+ Thời gian cài
Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

(4) Export

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

3.10 Rules Correlation

3.10.1 Danh sách hiển thị

- Chức năng cho phép người dùng nhập hoặc chọn điều kiện tìm kiếm để thực hiện tìm kiếm rule đang có trên hệ thống, thao tác deploy/undeploy/xóa nhanh với các rule.

  + Bộ lọc FITTER

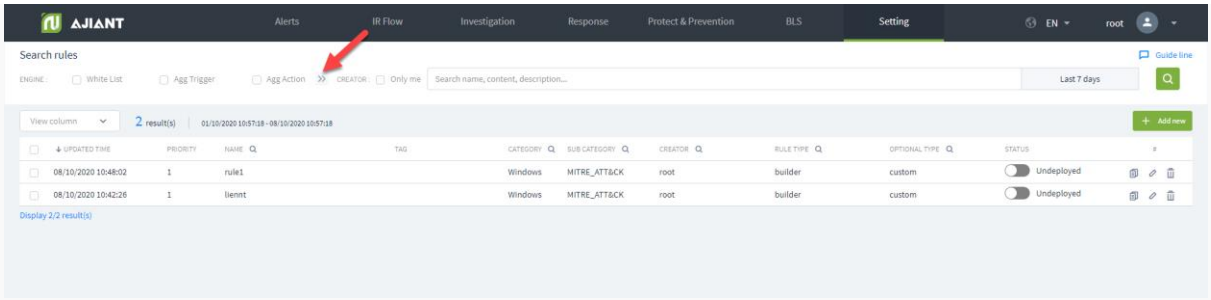
  + Bộ lọc FITTER bao gồm:

- 6 Engine: Whitelist, Agg Trigger, Agg Action, Filter, Indicator, False-Positive.
- Text box search theo các trường: Name, content, description
- Thời gian cập nhật

- Tạo bởi tôi

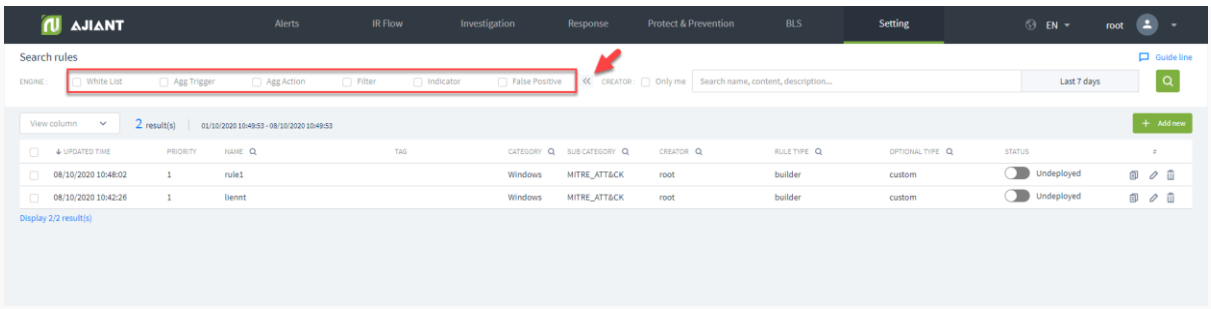
Lọc theo Engine

- Bước 1: Chọn 1 hoặc nhiều Engine mặc định



Màn hình tìm kiếm rule

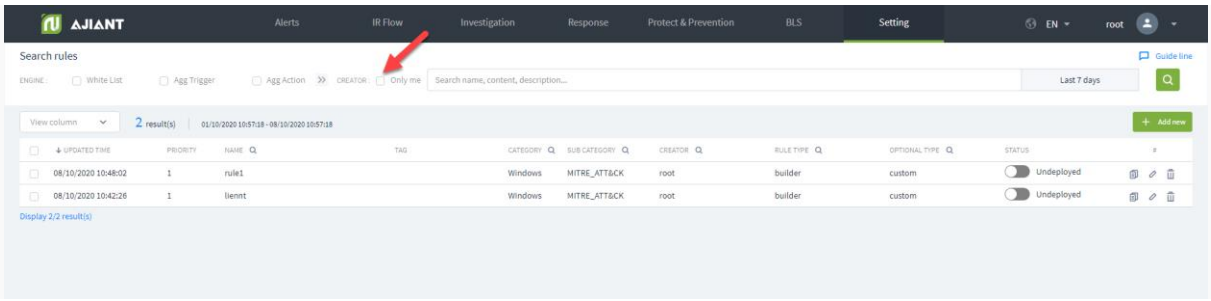
- Bước 2: Chọn Mở rộng để thêm các Engine cần lọc.



Màn hình mở rộng các điều kiện tìm kiếm rule

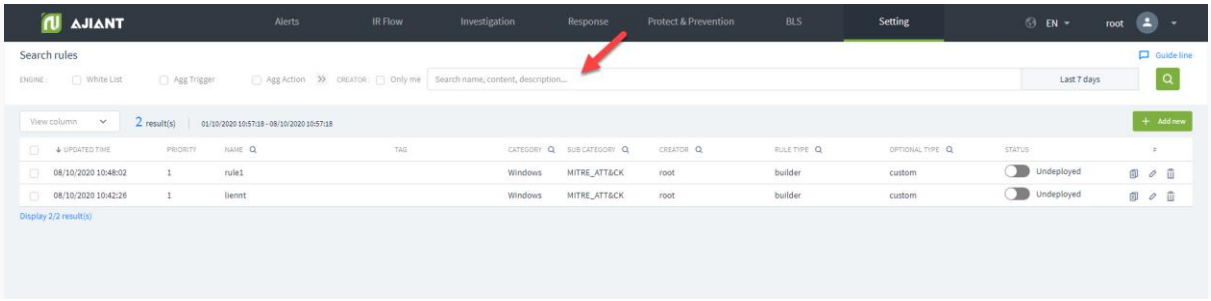
Khi chọn 2 hoặc nhiều Engine, màn hình trả về kết quả được lọc theo phép toán AND.

- Bước 3: Tích chọn người tạo Rules là user đang login vào hệ thống



Màn hình lọc theo Creator

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



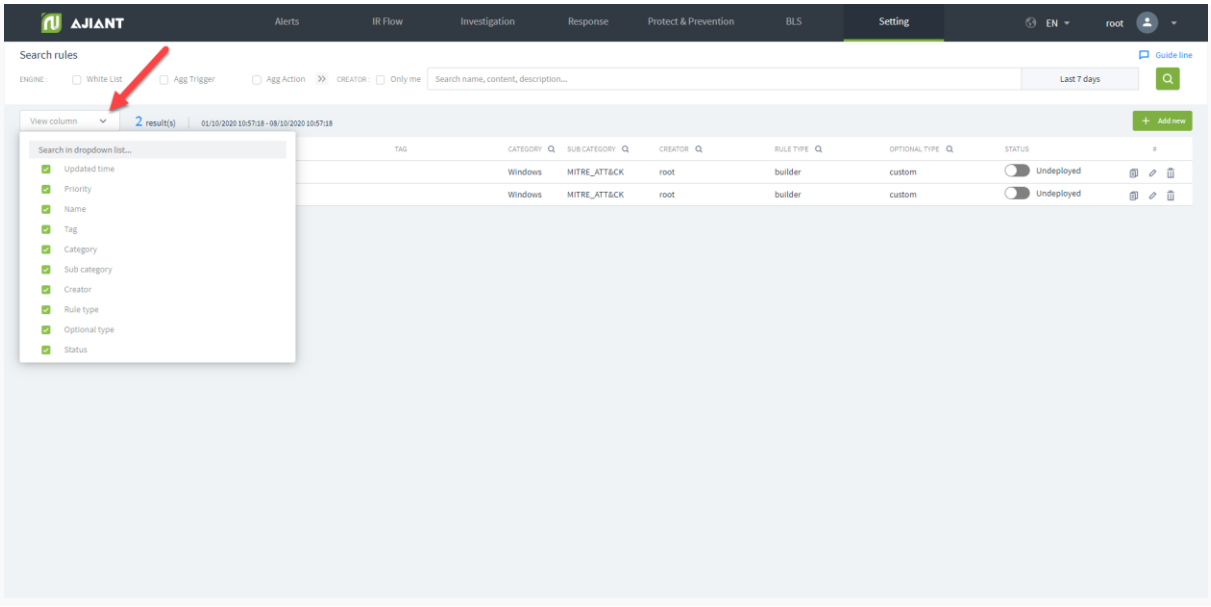
- Bước 5: Nhập thông tin cần tìm kiếm.
- Bước 6: Nhấn Search để hiển thị kết quả tìm kiếm.

Chọn cột

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

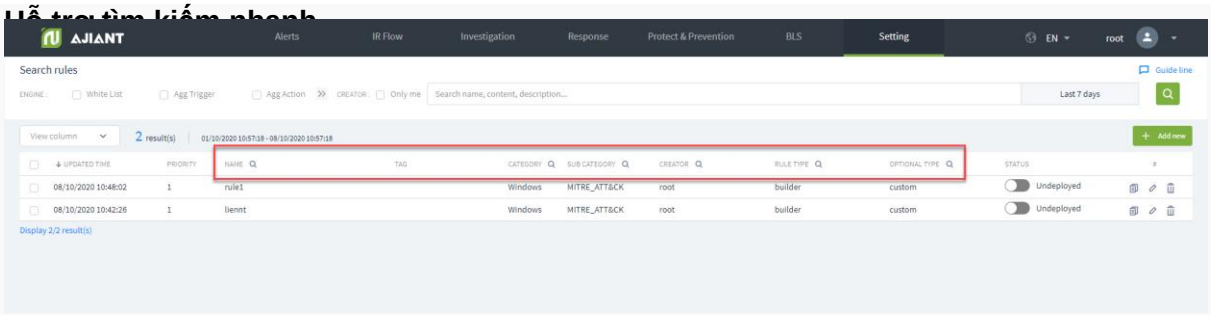
Các bước thực hiện:

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



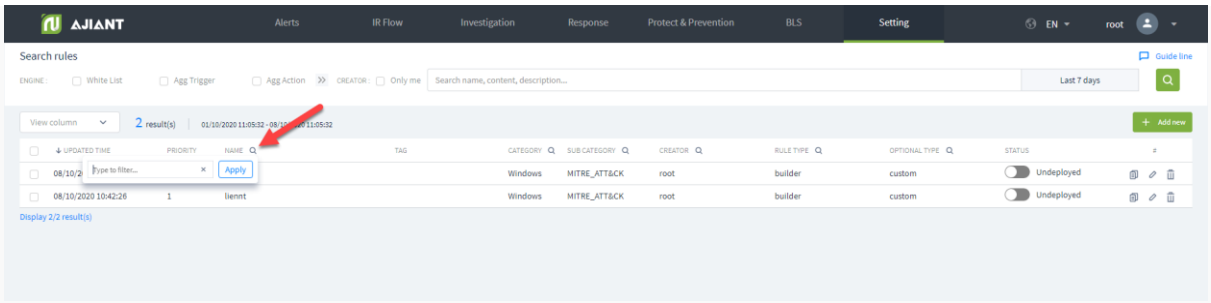
Màn hình Tùy chọn hiển thị thêm cột

Hỗ trợ tìm kiếm nhanh



Tìm kiếm theo tên rule

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



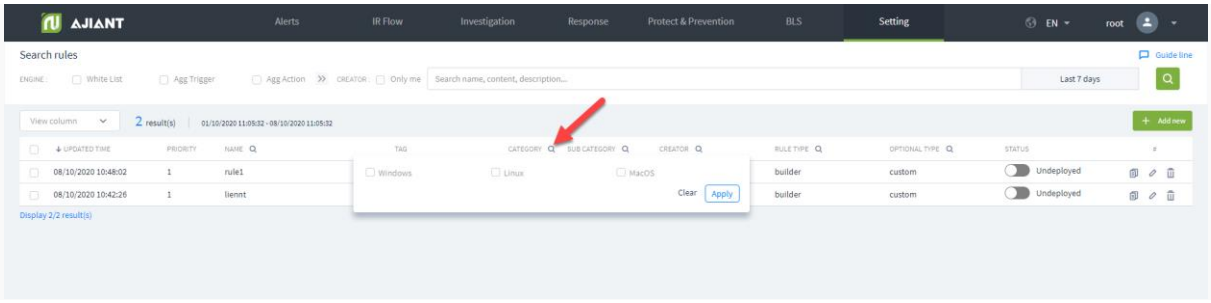
Màn hình tìm kiếm nhanh theo tên rule

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

Tìm kiếm theo Category

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

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



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

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

Tìm kiếm Sub Category

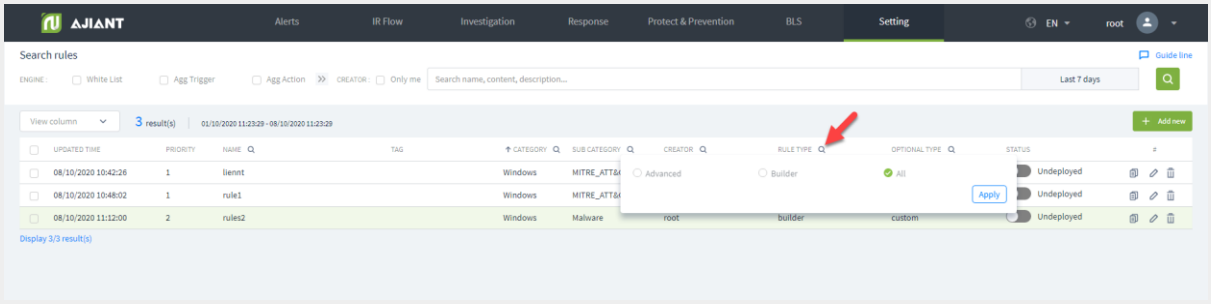
Hỗ trợ tìm kiếm nhanh theo loại triển khai, gồm 3 loại mặc định là: Metre ATT&CK, Malware, Suspicious Behaviour

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

Tìm kiếm Creator

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

Tìm kiếm Rule type

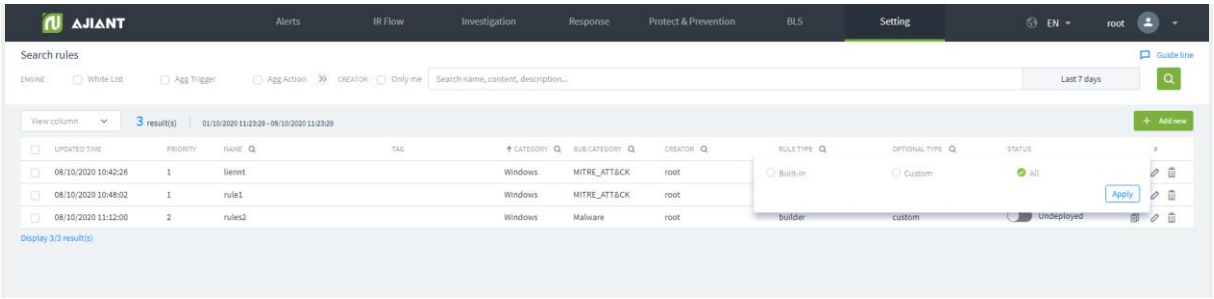


Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Advanced, Builder, All.

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

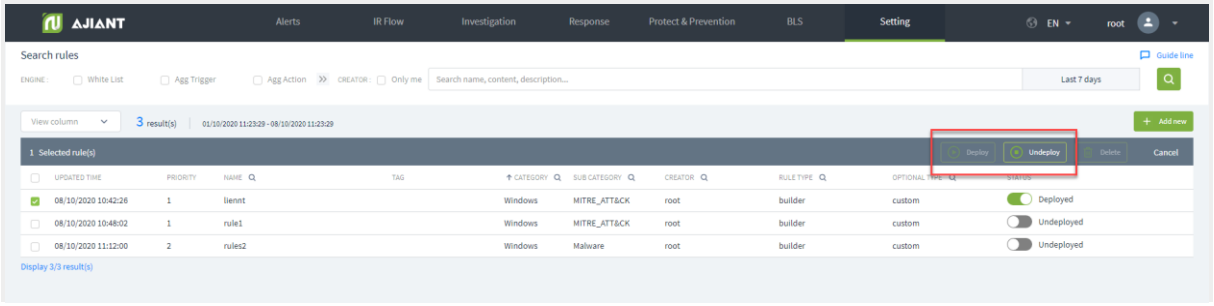
Tìm kiếm Optional type

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

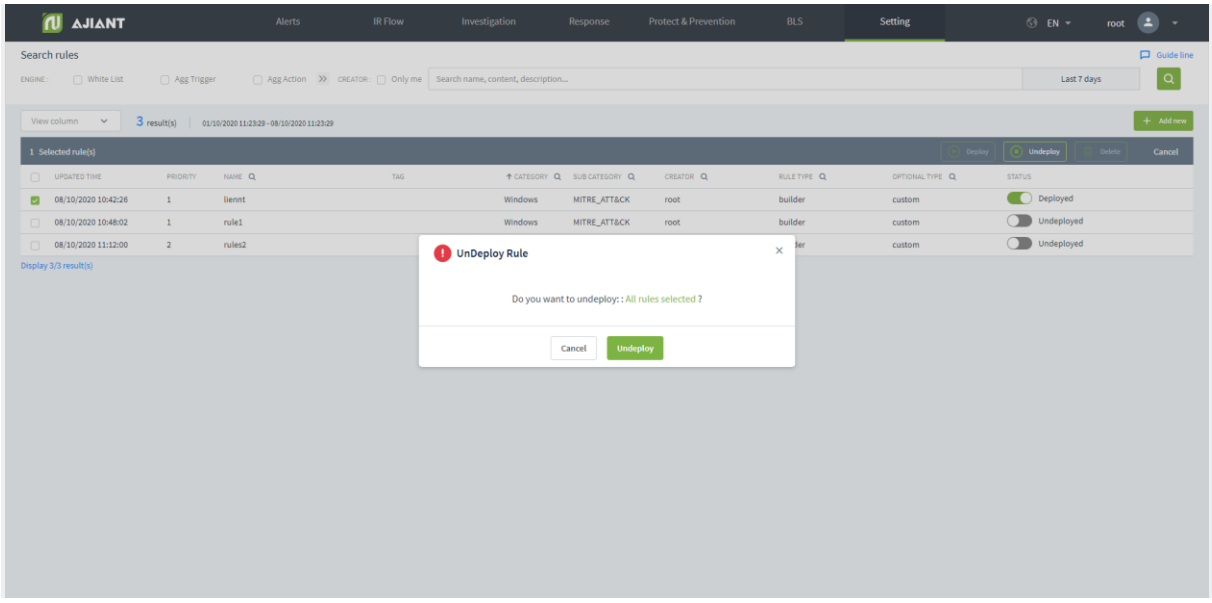


- Bước 1: Click icon  để hiển thị danh sách Optional type
- Bước 2: Click Optional type muốn tìn kiếm
- Bước 3: Click Apply

Hỗ trợ Deploy/Undeploy cho nhiều Rules



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



3.10.2 Thêm mới Rules Correlation

- Chức năng cho phép người dùng cấu hình một rule correlation mới hoàn chỉnh.

Tổng quan

- Engine: Gồm tất cả 6 engine với thông tin chi tiết lần lượt là:
    - Whitelist là một Stateless Engine thực hiện loại bỏ nhanh các event mà hệ thống không cần xử lý. Các event khớp với rule whitelist sẽ bị drop khỏi luồng xử lý.
    - Agg_trigger và Agg_action là một Stateful Engine thực hiện gom nhóm các event tương tự nhau. Mỗi rule aggregate chứa các thông tin về điều kiện gom nhóm (định nghĩa event tương tự nhau), khoảng thời gian gom nhóm (ví dụ 30s, 1 phút, 2 phút,…). Các event khớp điều kiện gom nhóm được lưu lại và chỉ trả về một event có kèm theo số lượng sau một khoảng thời gian. Các event không khớp điều kiện gom nhóm được trả ra ngay lập tức với số lượng là 1.
    - Filter là một Stateless Engine thực hiện lọc các điều kiện để đẩy vào indicator.
    - Indicator là một Stateful Engine thực hiện kiểm tra, thống kê trên các event thỏa mãn Filter. Đầu vào của Indicator là các event thỏa mãn Filter, đầu ra là các Indicator Event hoặc Alert Event. Indicator hỗ trợ các phép thống kê số lượng (count) trong một đơn vị thời gian (time-windows) của cùng một đối tượng, không alert lặp lại đối với cùng một đối tượng trong khoảng thời gian quy định trước. Mỗi rule indicator chỉ thực hiện xét các điều kiện cùng loại, trên cùng một hệ thống.

- FalsePositive engine là một Stateless Engine thực hiện loại bỏ các trường hợp alert bị alert sai. Mỗi alert khi khớp với rule Falsepositive sẽ bị drop.

- Debug/ Not Debug là hai trạng thái của engine. Khi thực hiện thao tác debug, log được đẩy về thoả mãn điều kiện của engine sẽ hiển thị trên màn hình Gỡ rối Correlation.

- Điều kiện: Mỗi engine sẽ hỗ trợ các điều kiện về Event, not Event, Alert Event, not Alert Event, Accumulate, Function, not Function khác nhau . Chi tiết về các điều kiện và cách sử dụng:

  - Event: Được sử dụng cho các trường event.
  - Not Event: Chỉ được tạo ra khi có event.
  - Alert: Được sử dụng cho các trường alert.
  - Not Alert: Xét xem không có alert event trong bao lâu.
  - Accumulate: Thực hiện gom nhóm điều kiện event thoả mãn số lượng từ đó sinh ra alert.
  - Function: Là các hàm. Lưu ý: Vớicác hàm boolean, giá trị trả về là true hoặc false.
  - Not Function: Với not function, các hàm được sử dụng giống với function. Tuy nhiên giá trị trả về sẽ có kết quả true/false ngược lại.

- Toán tử :

  - Các toán tử cơ bản gồm: =, !=, >, <, >=, <= .
  - In: Kiểm tra giá trị của một trường có nằm trong danh sách không.
    - Bên trái toán tử: Tên trường cần kiểm tra.
    - Bên phải toán tử: Danh sách giá trị để kiểm tra được phân cách bởi dấu “,”.
  - Contains: kiểm tra giá trị của một trường có chứa giá trị mà cần kiểm tra.
    - Bên trái toán tử: Tên trường cần kiểm tra (trường này cần có giá trị là mảng hoặc string).
    - Bên phải toán tử: Giá trị để kiểm tra.
  - Assign: để gán giá trị của một trường vào một biến.
    - Bên trái toán tử: Tên trường cần gán.
    - Bên phải toán tử: Tên biến cần gán.
  - Matches: kiểm tra giá trị của một trường có thoả mãn một chuỗi regex.
    - Bên trái toán tử: Tên trường cần kiểm tra.
    - Bên phải toán tử: Chuỗi regex.

- Cấu hình thời gian: Kiểm tra điều kiện trong một khoảng thời gian , chỉ có ở các engine Agg_trigger ,Agg_action và Indicator.
- Count: Kiểm tra số event đếm được trong một khoảng thời gian có thoả mãn điều kiện không.

- Nhóm/ Bỏ nhóm : Cho phép người dùng gộp hoặc tách nhanh các điều kiện trong một toán tử AND hoặc OR.

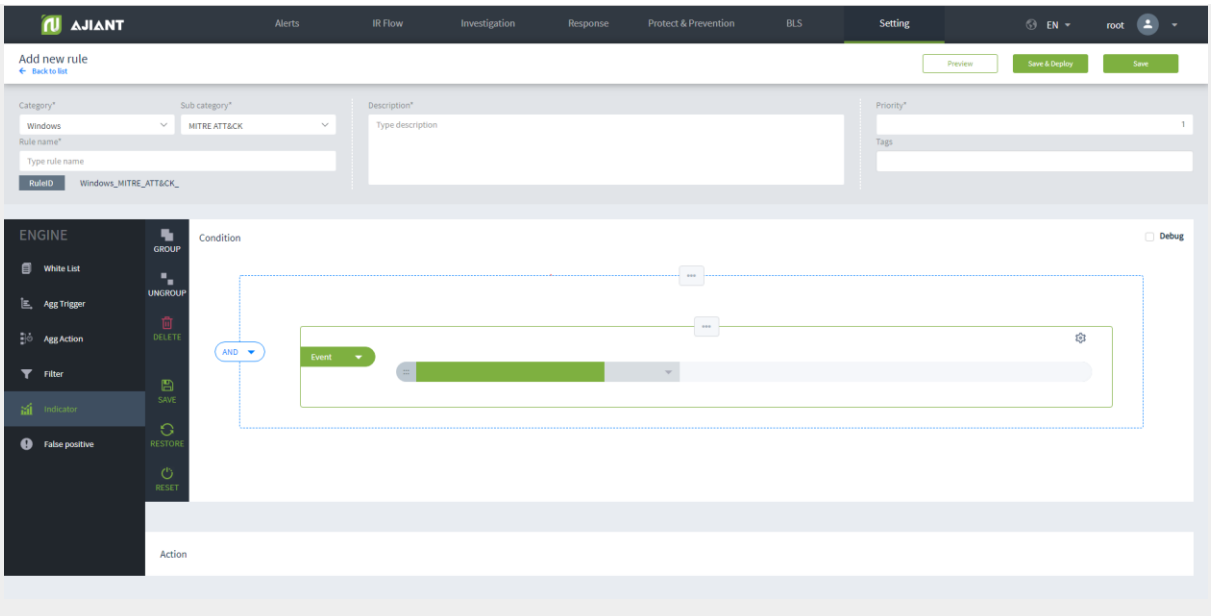
Các bước thực hiện gộp nhóm/ tách nhóm

- Gộp nhóm
  - Bước 1: Click vào vào trường cần gộp nhóm
  - Bước 2: Chọn NHÓM Màn hình chi tiết các bước thực hiện gộp nhóm
- Tách nhóm
  - Bước 1: Click vào các item cần tách nhóm.
  - Bước 2: Chọn BỎ NHÓM Màn hình chi tiết các bước thực hiện tách nhóm

- Restore: Tự động reset lại đến ngay sau khi nhấn SAVE gần nhất
- Reset: Thực hiện reset condition (về trạng thái ban đầu)
- Delete: Xóa Condition đang được focus

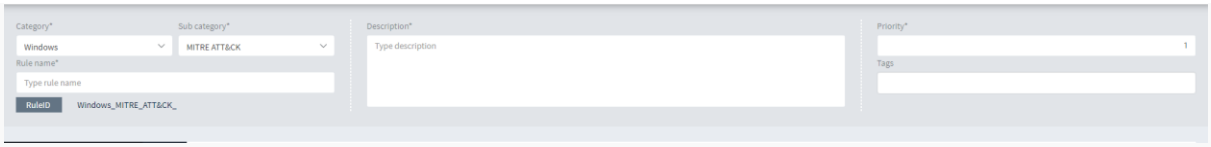
Các bước thêm mới rule correlation:

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



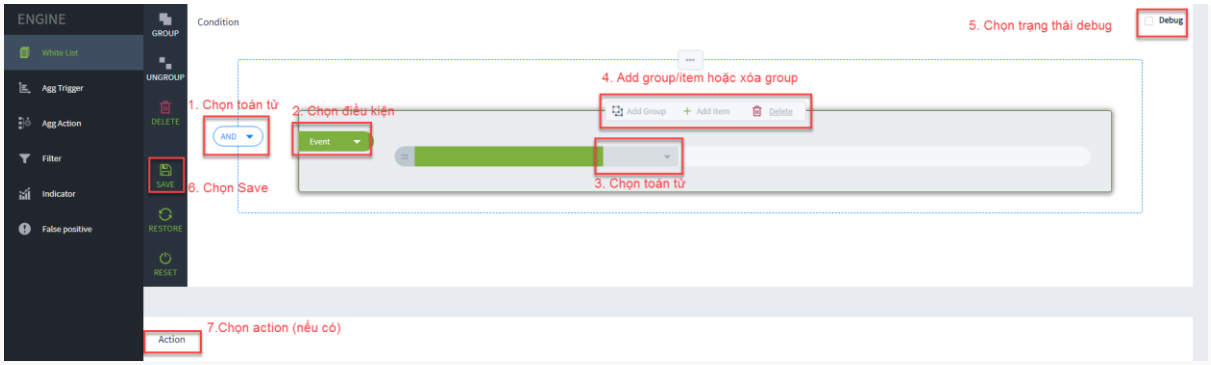
Hình 1: Màn hình thêm mới Rule correlation

- Bước 2: Nhập thông tin của rule.



Lưu ý: Các trường có dấu (*) là các trường bắt buộc nhập.

- Bước 3: Chọn Engine, nhập điều kiện cho các Event, not Event, Alert, not Alert, Accumulate, Function tương ứng.



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

- Bước 4: Nhấn Lưu để lưu lại điều kiện hoặc nhấn Huỷ để trở lại ngay sau bước mới lưu.

- Bước 5: Tại Hành động , chọn hành động cần thực hiện đối với engine đó.

Các bước thực hiện thêm hành động tương ứng với từng engine:

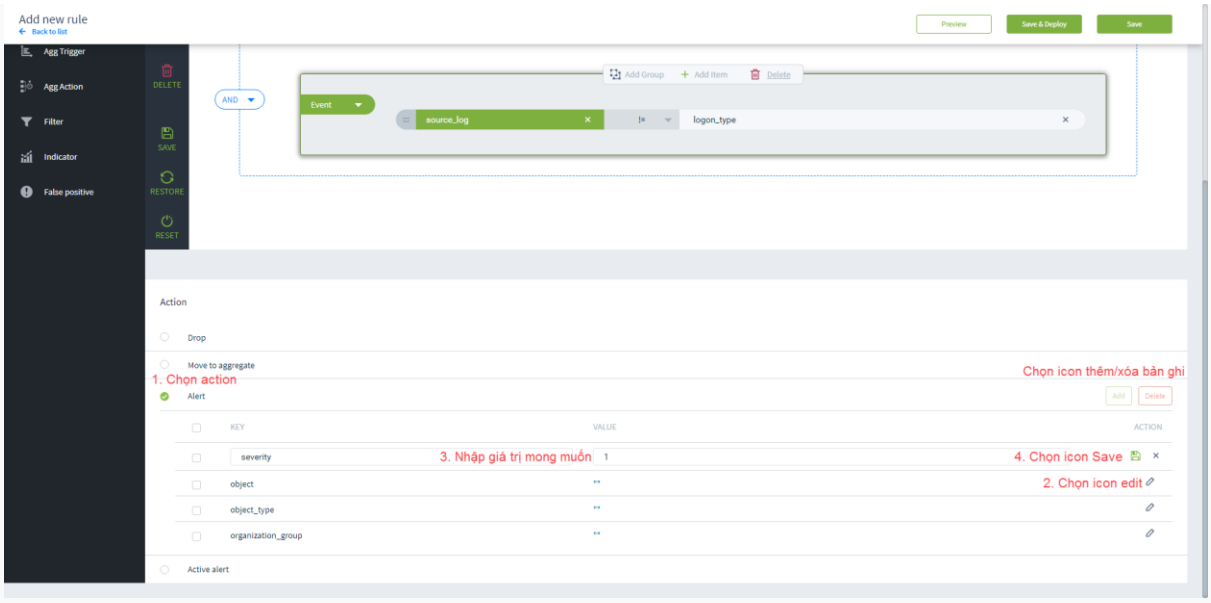
Khi người dùng thực hiện xong các bước tạo điều kiện và nhấn lưu, màn hình sẽ hiển thị các hành động cho từng engine. Mỗi engine sẽ bao gồm các hành động tương ứng. Engine Agg_trigger sẽ không có hành động.

Whitelist: Gồm 4 hành động dưới dạng check box : Drop, Chuyển sang aggregate, Alert và Danh sách Active, người dùng bắt buộc phải chọn 1 trong 4 hành động này. Khi các log đẩy vào thoả mãn điều kiện sẽ thực hiện 1 trong 4 hành động mà người dùng đã tích chọn. Chi tiết chức năng của 4 hành động:

  - Drop: Các log được đẩy vào thoả mãn điều kiện sẽ được loại bỏ khỏi luồng xử lý.
  - Chuyển sang aggregate: Log đẩy vào thoả mãn điều kiện sẽ được chuyển sang engine aggregate để tiếp tục xử lý.
  - Alert: Khi thêm các trường key và value cho alert, các log đẩy vào thoả mãn điều kiện sẽ hiển thị alert tại màn hình quản lý alert.
  - Danh sách Active: Các value của active list sẽ được thêm vào danh sách hiển thị trên màn hình Active List.

Các bước thêm trường cho hành động Alert/ Danh sách active:

- Bước 5.1: Click chọn hành động muốn thêm.
- Bước 5.2: Click button Sửa để nhập giá trị cho trường
- Bước 5.3: Nhập giá trị cho trường
- Bước 5.4: Click Save
- Bước 5.5: Click button Add để thêm mới một trường vào alert.



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

Để xoá hành động vừa tạo, click icon Xoá .

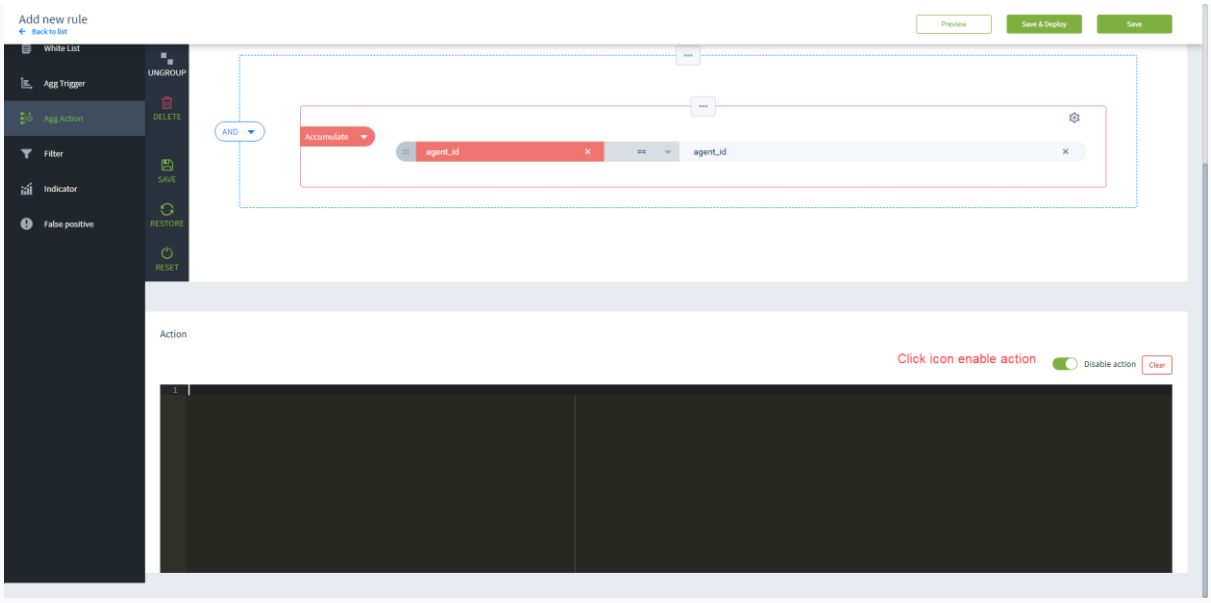
Để chỉnh sửa hành động, Click icon Chỉnh sửa .

Lưu ý: Có thể tạo nhiều hành động với các trường khác nhau tuỳ theo mục đích người sử dụng.

Agg_action: Tại engine này, người dùng có thể thực hiện hành động thêm code.

Các bước thêm trường cho hành động thêm code

- Bước 5.1: Nhập đầy đủ điều kiện và toán tử. Click vào Save
- Bước 5.2: Tại mục Action, click vào icon Enable action
- Bước 5.3: Nhập nội dung của code
- Bước 5.4: Chọn button clear => Nội dung nhập của code sẽ bị xóa toàn bộ



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

Filter : Gồm 3 hành động: Alert, Enrichment và Danh sách Active. Người dùng có thể 1 hoặc nhiều hành động trong cùng engine. Chi tiết chức năng của 3 hành động:

- Enrichment: Thêm trường vào Alert.
- Alert và Danh sách Active (như engine Whitelist).

Các thao tác thêm mới, sửa, xoá cho các hành động của engine filter tương tự với khi thêm mới các trường cho engine whitelist.

Indicator : Hành động alert.
Các thao tác thêm mới, sửa, xoá cho các hành động của engine Indicator tương tự với khi thêm mới các trường cho engine whitelist .

FalsePositive: Hành động Enrichment.
Các thao tác thêm mới, sửa xoá cho các hành động của engine FalsePositive tương tự với khi thêm mới các trường cho engine whitelist .

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

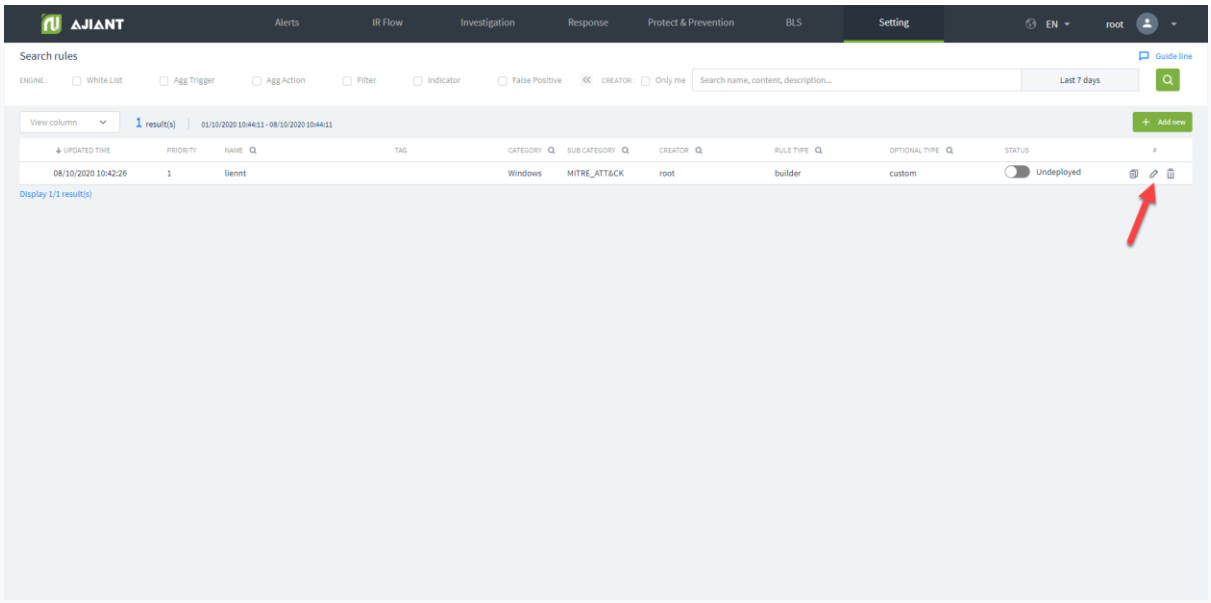
Lưu ý: Khi có lỗi, người dùng có thể nhấn button Preview để xem lỗi.

3.10.3 Sửa Rules Correlation

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

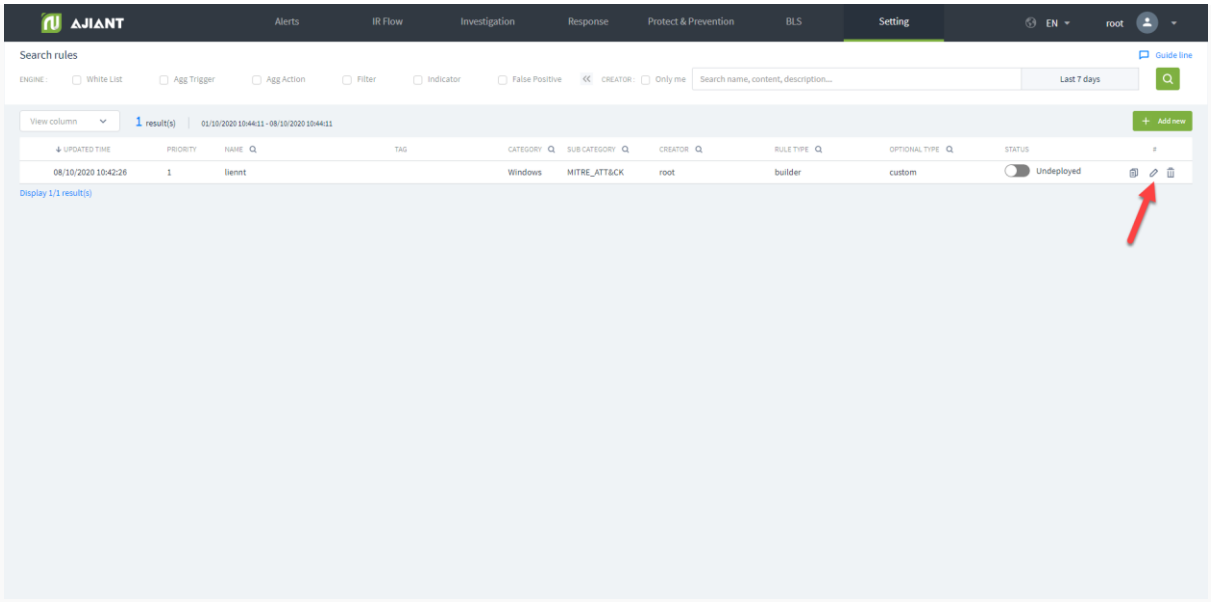
Các bước thực hiện:

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



Hình 5: Màn hình quản lý rule

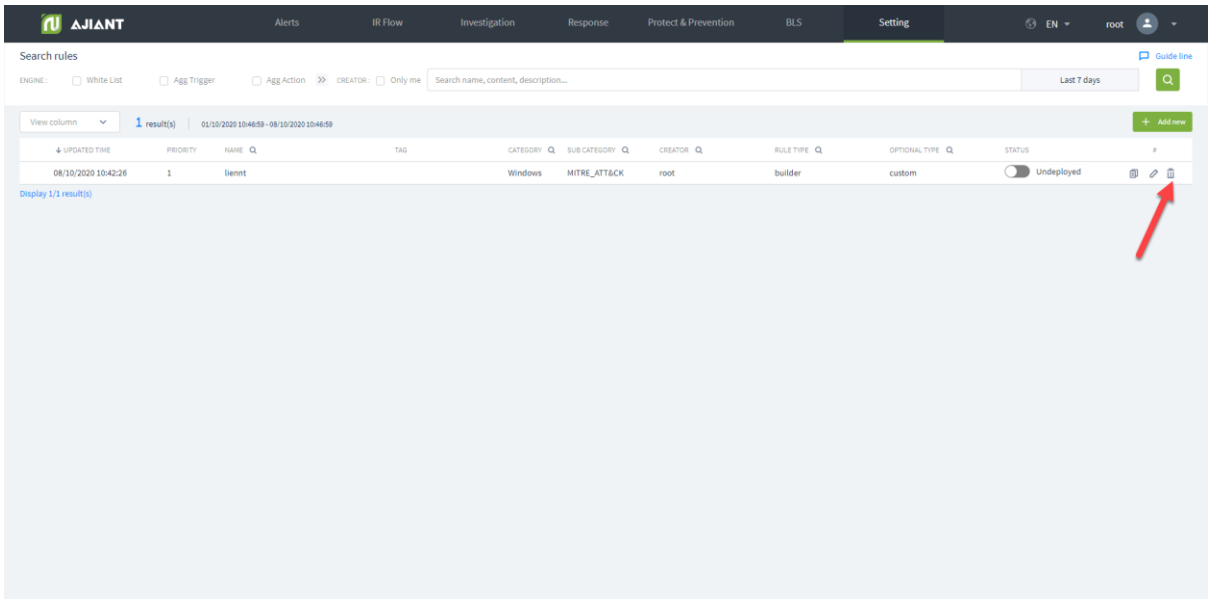
- Bước 2: Tại màn hình chỉnh sửa , nhập thông tin cần chỉnh sửa.



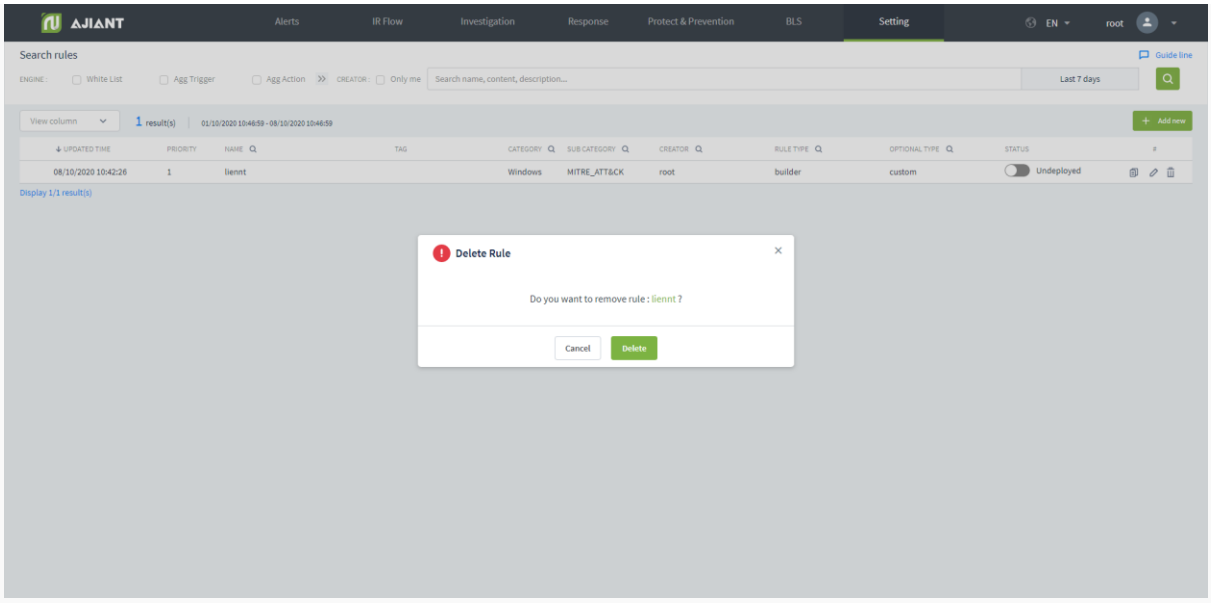
Hình 6: Màn hình thông tin chi tiết của rule

- Lưu ý: Các trường tên rule, category, subcategory là những trường không chỉnh sửa được.
- Bước 3: Nhấn Lưu để lưu rule lại vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống , đồng thời deploy xuống correlation engine thì nhấn Lưu & Deploy.
- Với những rule chỉnh sửa nhưng chỉ Lưu, người dùng phải click Redeploy tại màn hình quản lý rule thì rule mới có tác dụng đối với hệ thống.
- *Lưu ý*: Khi có lỗi, người dùng có thể nhấn Preview để xem lỗi.

3.10.4 Xóa Rules Correlation

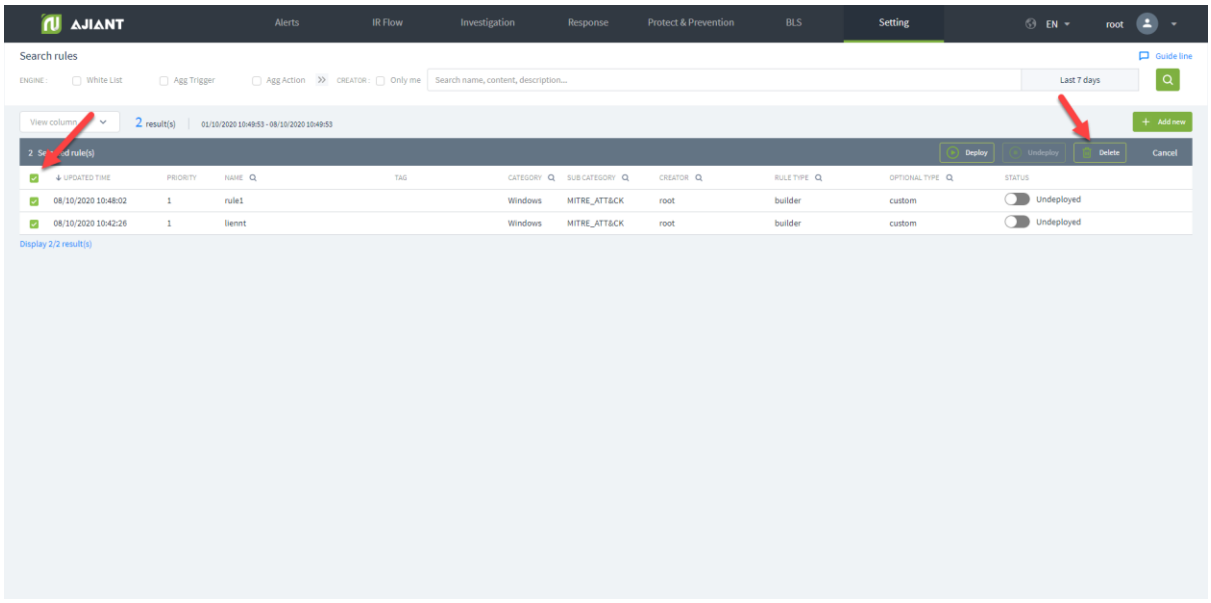


- Các bước thực hiện xóa 01 rule:
- Bước 1: Click icon Xoá tại rule muốn xoá.
- Bước 2: Màn hình hiển thị thông báo xác nhận xoá , chọn HUỶ/ ĐỒNG Ý.



Hình 7: Popup xác nhận xóa rule

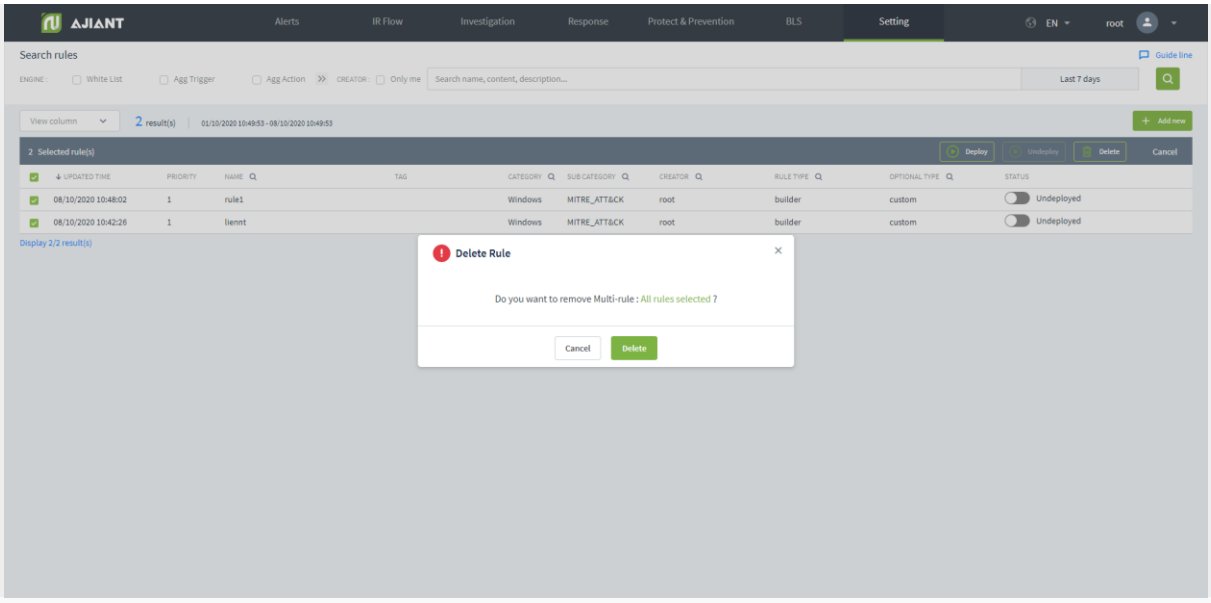
- Nếu chọn ĐỒNG Ý, rule được chọn xoá sẽ biến mất khỏi màn hình hiển thị.



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

Các bước thực hiện xóa nhiều rule:

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



Hình 9: Màn hình xác nhận xóa

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

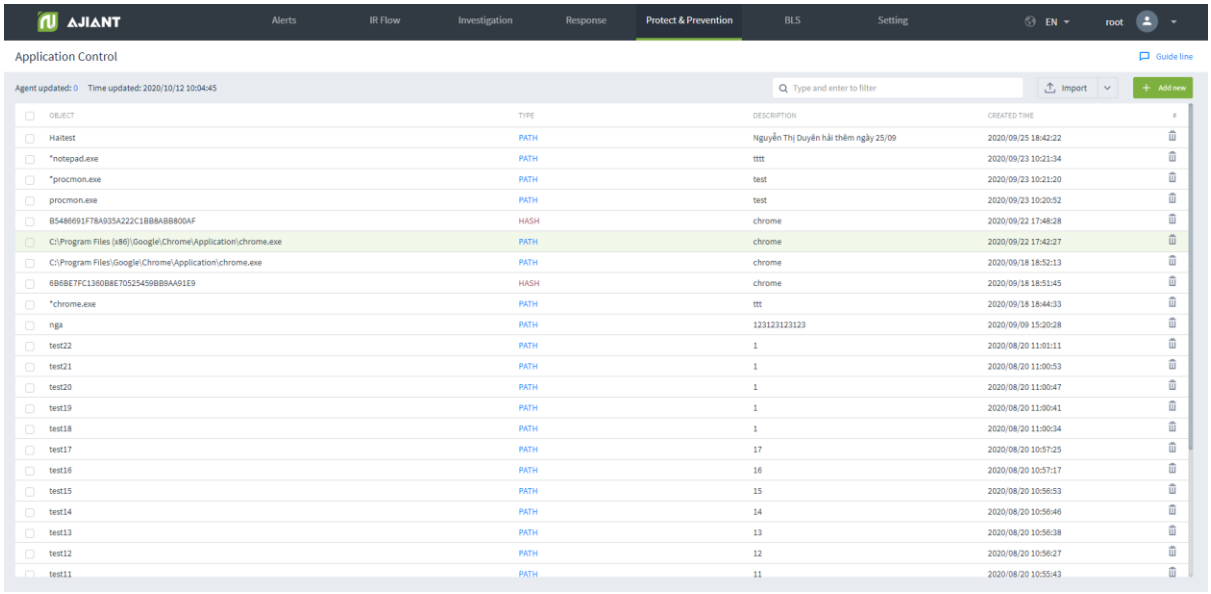
3.11 Protect & Prevention

3.11.1 Application Control

- Chức năng Application Control cho phép cấu hình các ứng dụng/tiến trình (process) sẽ chặn dưới máy người dùng không cho phép chạy (execute). Ứng dụng/tiến trình được nhận dạng dựa vào mã băm (MD5, SHA1, SHA256) hoặc đường dẫn.

3.10.1.1 Hiển thị danh sách các ứng dụng/tiến trình bị chặn

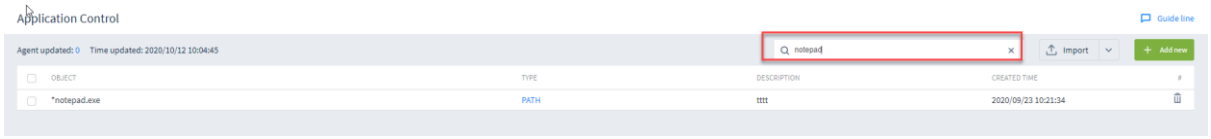
- Click vào tab Protect & Prevention > chọn Application control sẽ hiển thị toàn bộ các ứng dụng/tiến trình dưới máy người dùng không cho sử dụng.



Màn hình danh sách ứng dụng/tiến trình bị chặn

3.10.1.2 Tìm kiếm ứng dụng/tiến trình bị chặn

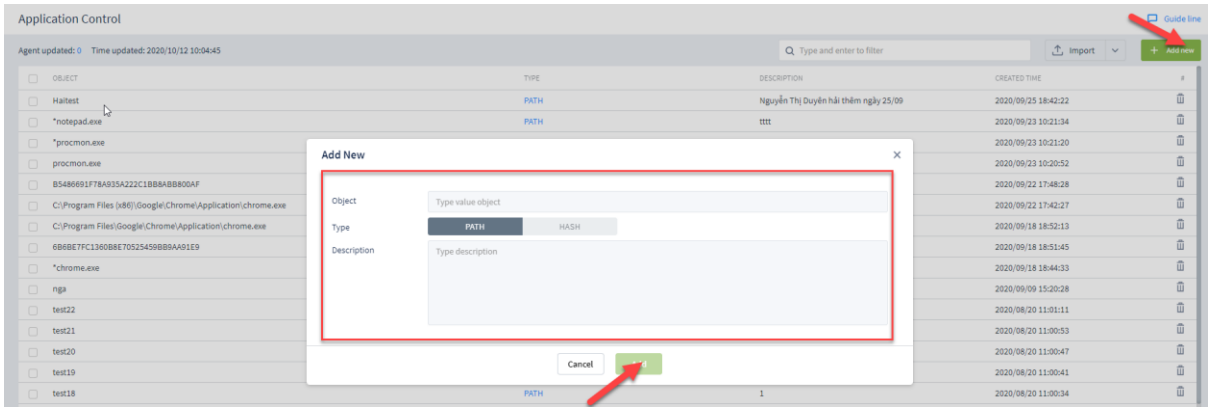
- Người dùng có thể tìm kiếm theo mã băm hoặc đường dẫn của ứng dụng bị chặn



Màn hình tìm kiếm ứng dụng/tiến trình bị chặn

3.10.1.3 Thêm mới ứng dụng/tiến trình bị chặn

- Click vào <Add new> để thêm mới ứng dụng/tiến trình bị chặn, người dùng có thể chọn chặn theo Path hoặc mã Hash (MD5, SHA1, SHA256)



Màn hình thêm mới ứng dụng/tiến trình bị chặn

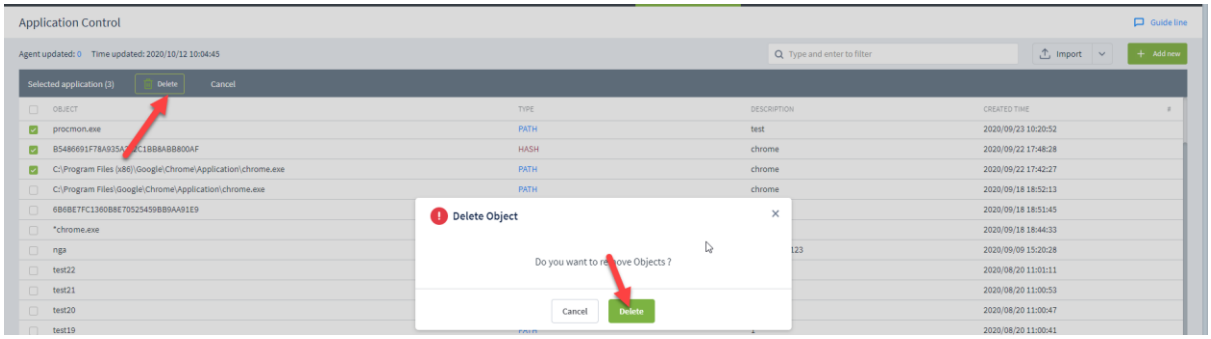
3.10.1.4 Thêm mới ứng dụng/tiến trình từ tập tin có sẵn

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

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

3.10.1.5 Xóa ứng dụng/tiến trình bị chặn trong danh sách

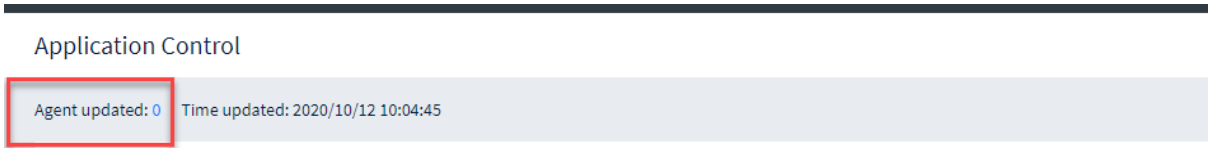
- Hệ thống hỗ trợ xóa 1 hoặc nhiều ứng dụng bị chặn.
- Clik vào từng ứng dụng cần xóa và click icon Delete, hoặc click vào checbox đầu mỗi ứng dụng và click button <Delete>



Màn hình xóa ứng dụng/tiến trình bị chặn

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

- Sau khi người dùng thêm/sửa/xóa danh sách các tiến trình trên giao diện, hệ thống sẽ cập nhật danh sách này xuống dưới các agent theo luồng update file agent (chu kỳ 3 phút/lần). Agent nhận được cấu hình mới, phát sinh log với eventID =101 và đẩy lên server, hiển thị trên màn hình Event search. Sau đó hệ thống sẽ tự động cập nhật số lượng agent đã cập nhật danh sách cấu hình mới trên màn Application control.

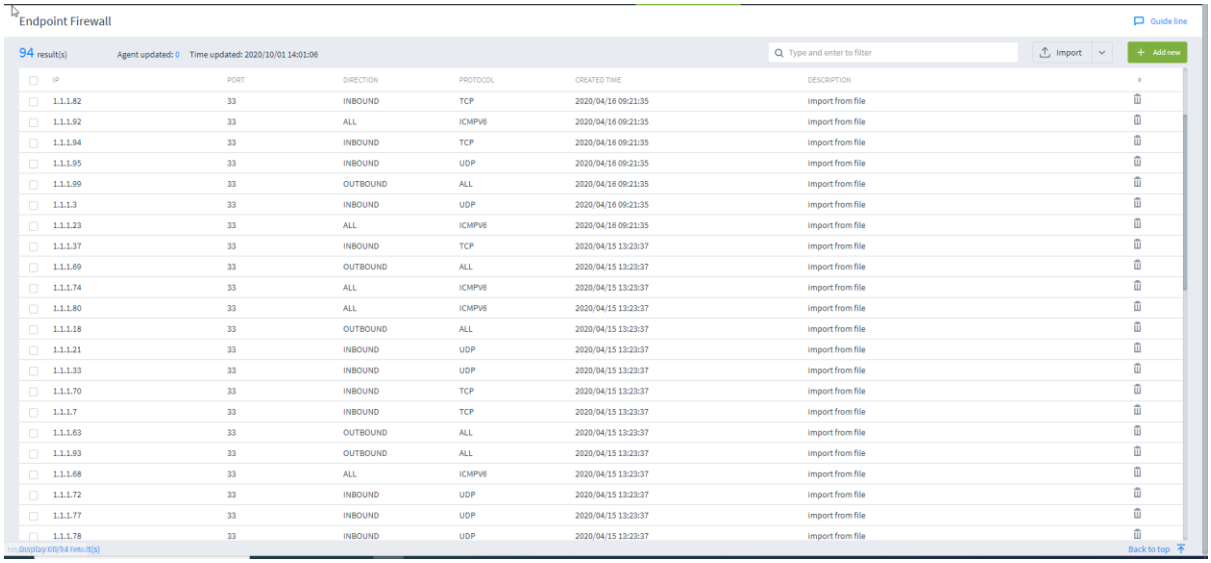


3.11.2 Endpoint Firewall

- Mục đích: Chức năng Endpoint Firewall cho phép cấu hình các kết nối sẽ chặn dưới máy người dùng, bao gồm chặn theo ip, port, hoặc cả ip và port, hỗ trợ các protocol TCP, UDP, ICMP, hỗ trợ Ipv4 và Ipv6, hỗ trợ inbound và outbound connection.

3.11.2.1 Hiển thị danh sách các kết nối bị chặn

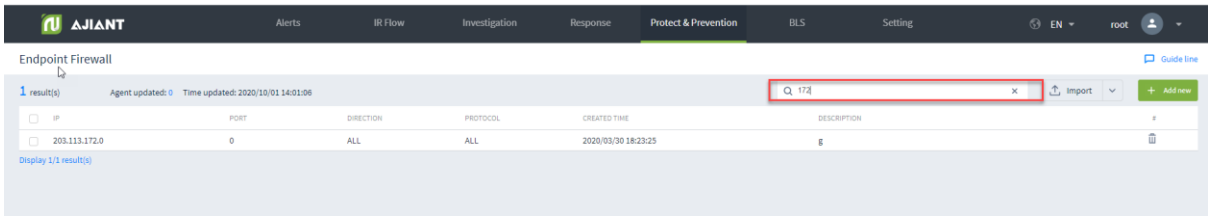
- Click vào tab Protect & Prevention > chọn Endpoint Firewall sẽ hiển thị toàn bộ danh sách các kết nối bị chặn.



Màn hình danh sách các kết nối bị chặn

3.11.2.2 Tìm kiếm các kết nối bị chặn

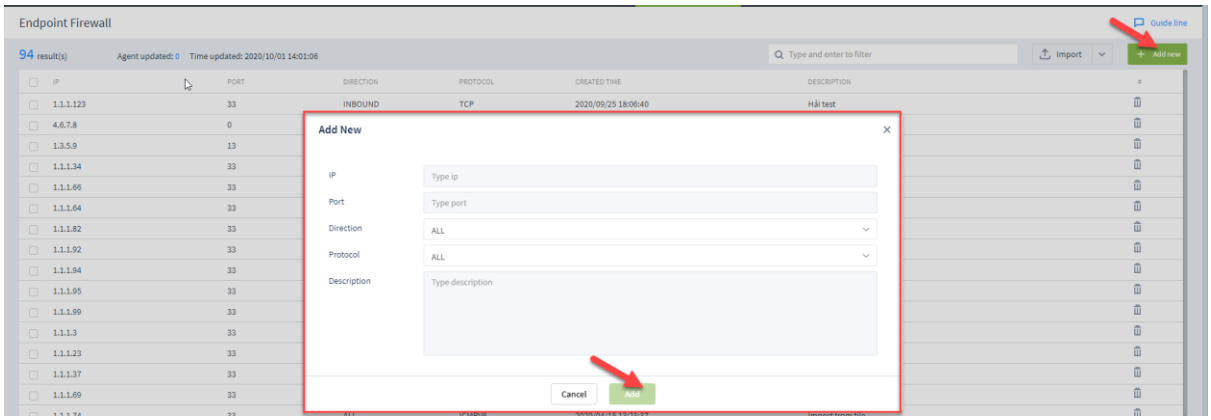
- Người dùng có thể tìm kiếm theo địa chỉ IP và port đã thiết lập



Màn hình tìm kiếm các kết nối bị chặn

3.11.2.3 Thêm mới các kết nối bị chặn

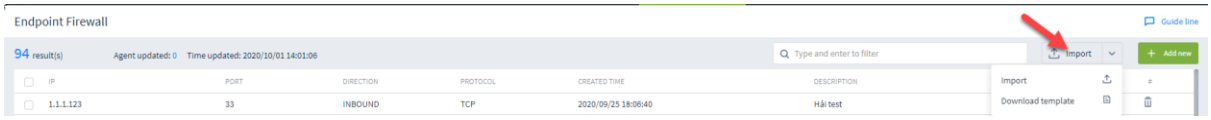
- Click button <Add new>, nhập thông tin trên popup thêm mới kết nối bị chặn
  + IP: địa chỉ IP cần chặn
  + Port: port cần chặn, nếu chặn tất cả port thì nhập 0
  + Direction: inbound, outbound, All (chặn cả 2 chiều)
  + Protocol: ICMP, TCP, UDP, ICMPV6, ALL



Màn hình thêm mới địa chỉ kết nối bị chặn

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

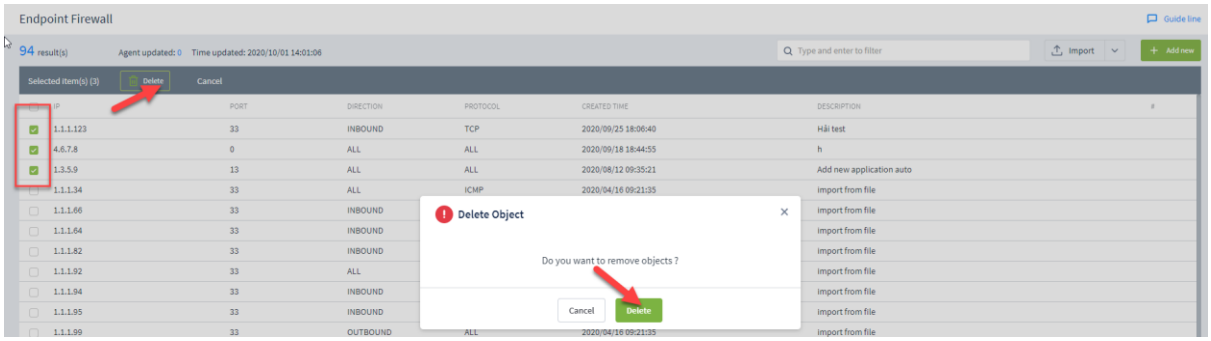
- Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại.
- Click <Import>, chọn đường dẫn đến file cần tải lên và click Open, hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống.



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

3.11.2.5 Xóa kết nối bị chặn trong danh sách

- Hệ thống hỗ trợ xóa 1 hoặc nhiều kết nối bị chặn.
- Click vào từng kết nối cần xóa và click icon Delete, hoặc click vào checbox đầu mỗi kết nối và click button <Delete>



Màn hình xóa kết nối bị chặn

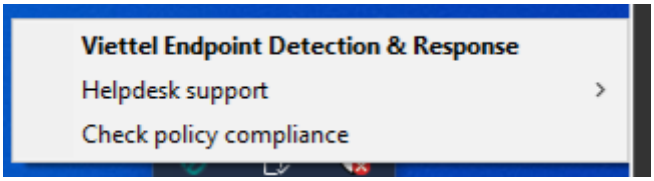
3.11.2.6 Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công

- Sau khi người dùng thêm/sửa/xóa danh sách các kết nối trên giao diện, hệ thống sẽ cập nhật danh sách này xuống dưới các agent theo luồng update file agent (chu kỳ 3 phút/lần). Agent nhận được cấu hình mới, phát sinh log với eventID =201 và đẩy lên server, hiển thị trên màn hình Event search. Sau đó hệ thống sẽ tự động cập nhật số lượng agent đã cập nhật danh sách cấu hình mới trên màn Endpoint Firewall.

GIAO DIỆN PHÍA AGENT

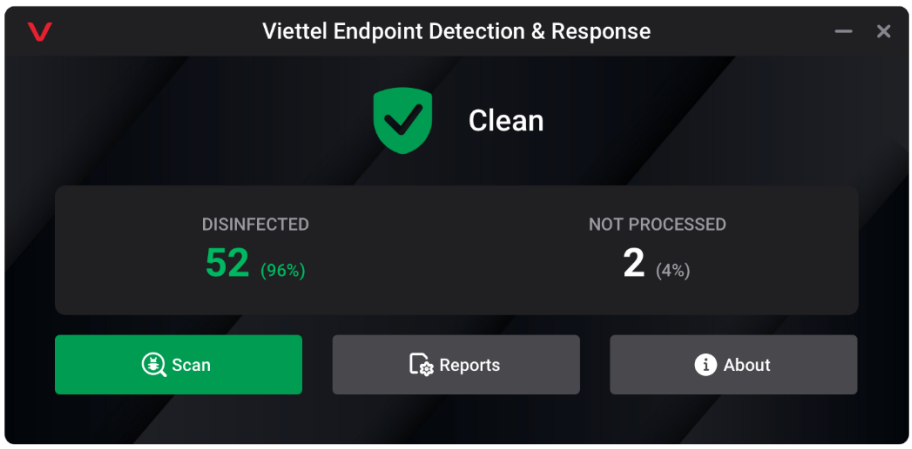
3.12 Main

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

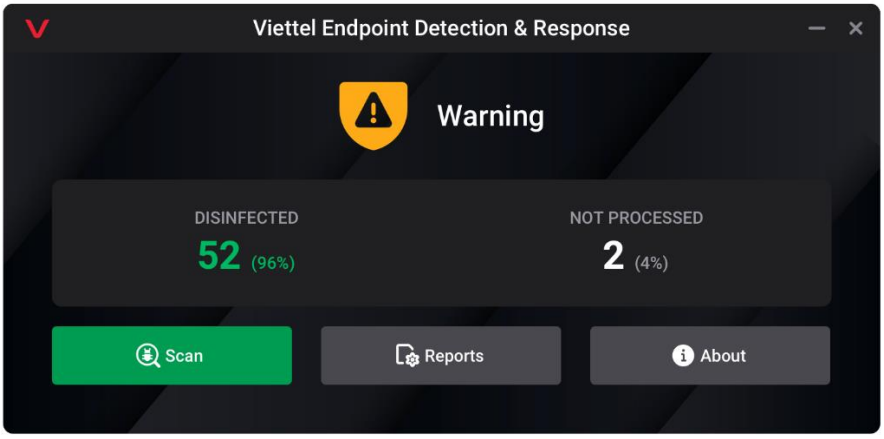


- Hệ thống hiển thị các thông tin

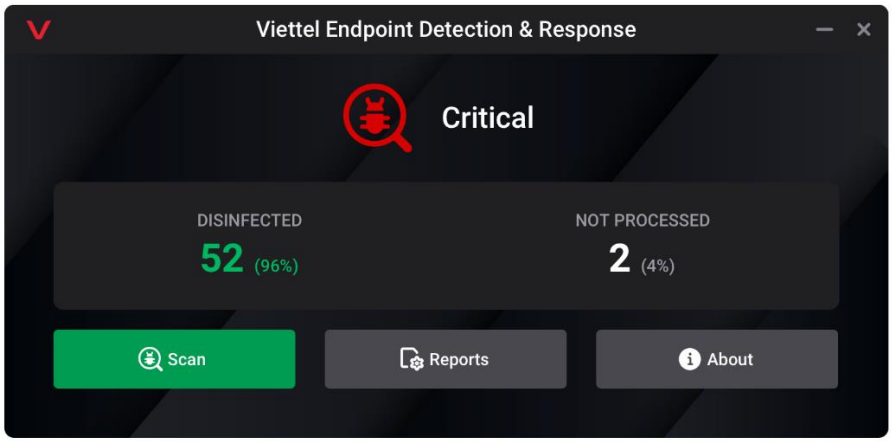
+ Trường hợp máy không có mã độc nào hoặc toàn bộ mã độc đã được xử lý



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



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



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

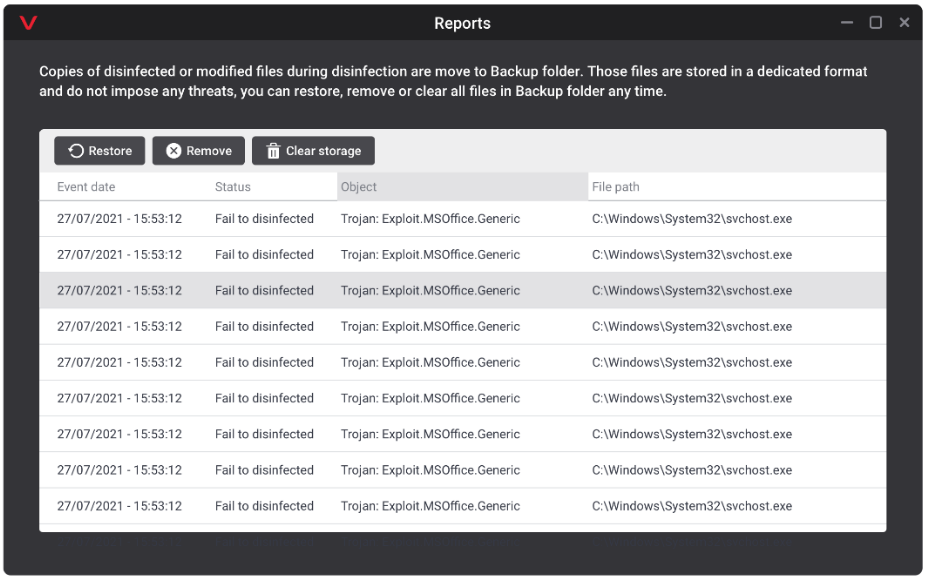
- Disinfected: Tổng số và tỷ lệ mã độc đã phát hiện và được xử lý
- Not processed: Tổng số và tỷ lệ mã độc đã phát hiện nhưng chưa được xử lý

3.13 About

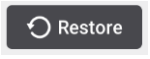
- Chức năng cung cấp thông tin về phiên bản Agent cài trên máy người dùng và thông tin hỗ trợ sản phẩm

3.14 Reports

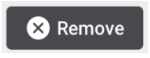
- Chức năng tổng hợp danh sách các mã độc đã được phát hiện trên hệ thống và tình trạng xử lý tính đến thời điểm hiện tại



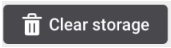
- Các file chứa mã độc trước khi được xử lý đều được lưu trữ bản gốc trong thư mục Backup, để dọn thư mục Backup hoặc phục hồi file, sản phẩm cung cấp các tính năng sau:



: Cho phép lựa chọn 01 file để phục hồi



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



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

3.15 Scan

- Chức năng cho phép người dùng chủ động sử dụng hệ thống để quét và xử lý mã độc trên máy.
- Các phương thức quét được hỗ trợ bao gồm

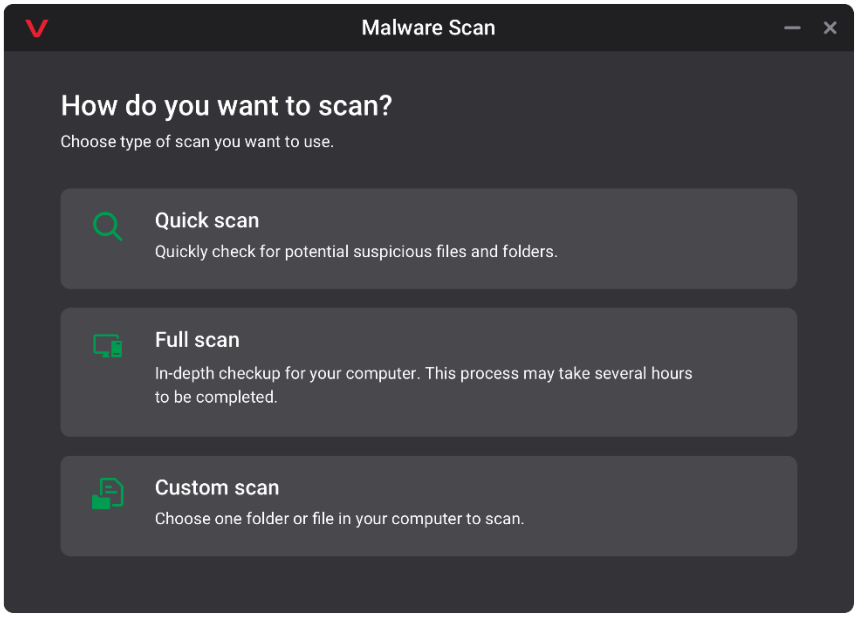
+ Lựa chọn trực tiếp từ file explorer, cho phép chọn nhiều tệp tin và thư mục, chuột phải chọn quét (Context scan)

+ Lựa chọn các hình thức quét từ giao diện phía agent

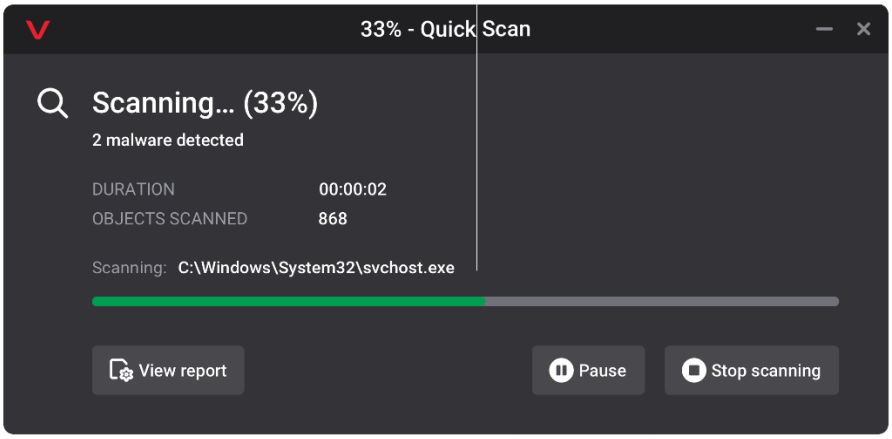
— Quick scan: Quét trên một tập các thư mục được định nghĩa trước, đây là các thư mục thường xuyên phát sinh mã độc, khi chọn quét toàn bộ các tệp tin và thư mục trực thuộc các thư mục đã chọn.

— Full scan: Quét toàn bộ các tệp tin và thư mục có trong máy người dùng.

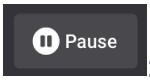
— Custom scan: Tương tự context scan, khi chọn hình thức này agent hiển thị file explorer cho phép người dùng lựa chọn 01 tệp tin hoặc thư mục để quét



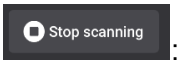
- Sau khi chọn phương thức phù hợp, hệ thống thực hiện quét và xử lý mã độc:



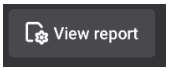
- Hỗ trợ các thao tác trong lúc quét như sau:



: Cho phép tạm dừng quá trình quét

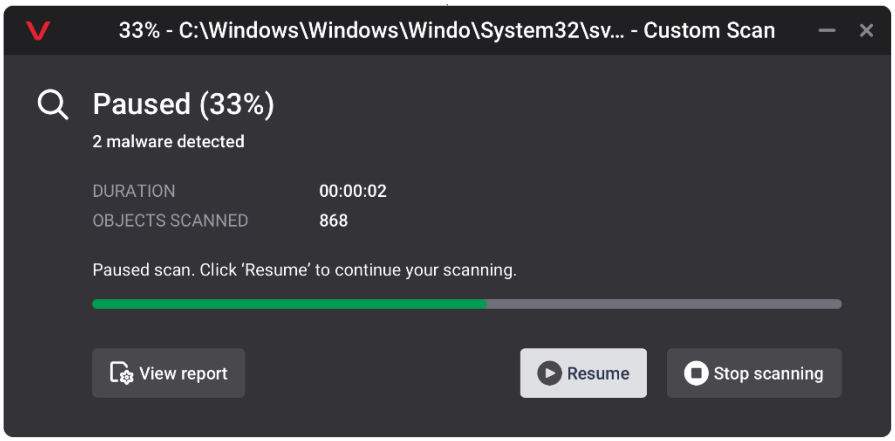


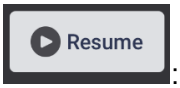
: Cho phép kết thúc quá trình quét

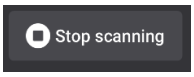


: Trường hợp phát hiện được ít nhất một mã độc, cho phép xem nhanh trạng thái xử lý tại 3.14 Reports

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





: Cho phép chọn để tiếp tục quét hoặc 

để hoàn thành quá trình quét

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