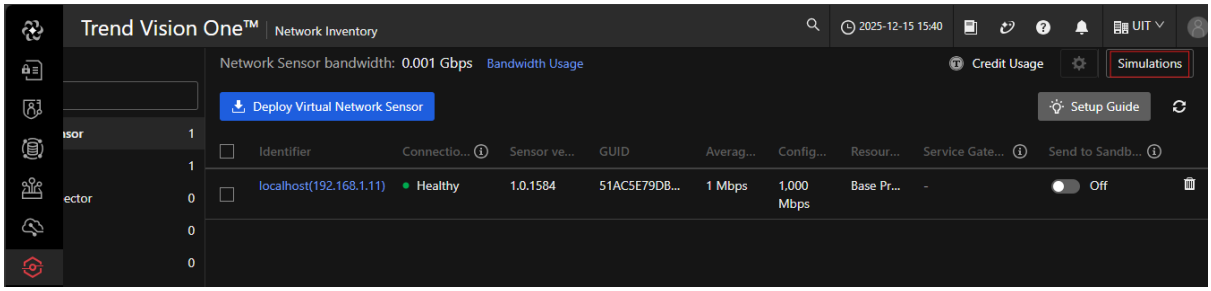
KỸ THUẬT TẤN CÔNG ĐƯỢC GHI NHẬN: OBSERVED ATTACK TECHNIQUE

Mục lục:

Observed Attack Technique (OAT) là tập hợp các kịch bản mô phỏng hành vi tấn công đã được quan sát trong thực tế, nhằm tái hiện chuỗi kỹ thuật của tác nhân đe dọa trên môi trường thử nghiệm. Việc chạy OAT giúp tạo dữ liệu và dấu vết tấn công có kiểm soát để kiểm chứng khả năng phát hiện, tương quan sự kiện và hỗ trợ điều tra trên nền tảng giám sát bảo mật.

I. Kịch bản sử dụng mạng

Chọn mục “Simulations” để triển khai các kịch bản tấn công - **Observed Attack Technique (OAT)**



1. Giao thức lớp ứng dụng và Khai thác các dịch vụ từ xa

- Mô tả kịch bản:

T1071 - Giao thức lớp ứng dụng

Đối thủ có thể giao tiếp bằng các giao thức lớp ứng dụng để tránh bị phát hiện/lọc mạng bằng cách trộn lẫn với lưu lượng truy cập hiện có. Các lệnh đến hệ thống từ xa, và thường là kết quả của các lệnh đó, sẽ được nhúng trong lưu lượng giao thức giữa máy khách và máy chủ.

T1210 - Khai thác các dịch vụ từ xa

Đối thủ có thể khai thác các dịch vụ từ xa để truy cập trái phép vào các hệ thống nội bộ khi đã vào trong mạng. Khai thác lỗ hổng phần mềm xảy ra khi kẻ thù lợi dụng lỗi lập trình trong chương trình, dịch vụ hoặc trong phần mềm hoặc hạt nhân của hệ điều hành để thực thi mã do đối thủ kiểm soát. Mục tiêu chung của việc khai thác các dịch vụ từ xa sau khi thỏa hiệp là di chuyển ngang để cho phép truy cập vào hệ thống từ xa.

Kỹ thuật mô phỏng:

- Cobalt Strike: Yêu cầu HTTP (biến thể 3)
- MS17-010: Thực thi mã từ xa thông qua yêu cầu SMB

Kết quả dự kiến:

- Bàn làm việc - Mô hình:
  - Demo - Kết nối Cobalt Strike có thể có
  - Demo - Chuyển động nhiều bên thông qua giao thức SMB
- Kỹ thuật tấn công quan sát - Bộ lọc:
  - Demo - Kết nối Cobalt Strike có thể có
  - Demo - Giao tiếp chỉ huy và điều khiển có thể qua HTTP
  - Bản demo - COBALTSTRIKE HTTP (Yêu cầu) Biến thể 3 - Gửi đi
  - Demo - Chuyển động ngang thông qua khai thác thông qua giao thức SMB
  - Demo - Có thể di chuyển ngang thông qua khai thác
  - Demo - Phát hiện đáng ngờ trong mạng riêng
  - Demo - MS17-010 Metasploit SMB (Yêu cầu) - Gửi đi
  - Demo - Phát hiện mạng ưu tiên loại mối đe dọa

Yêu cầu về môi trường:

- Một thiết bị Deep Discovery Inspector hoặc thiết bị Cảm biến mạng ảo đã triển khai
- Hai điểm cuối Windows để mô phỏng chuyển động ngang

Các bước

1. Truy cập Kiểm kê mạng để tải xuống hình ảnh đĩa và triển khai thiết bị Deep Discovery Inspector hoặc thiết bị Cảm biến mạng ảo trong môi trường của bạn.
   Lưu ý: Bạn có thể kết nối các thiết bị Deep Discovery Inspector đã triển khai của mình với Trend Vision One thông qua Network Inventory để chạy mô phỏng tấn công mạng.
2. Tải tập lệnh demo xuống một trong các điểm cuối Windows của bạn. Chạy tập lệnh demo bằng địa chỉ IP của cả hai điểm cuối.

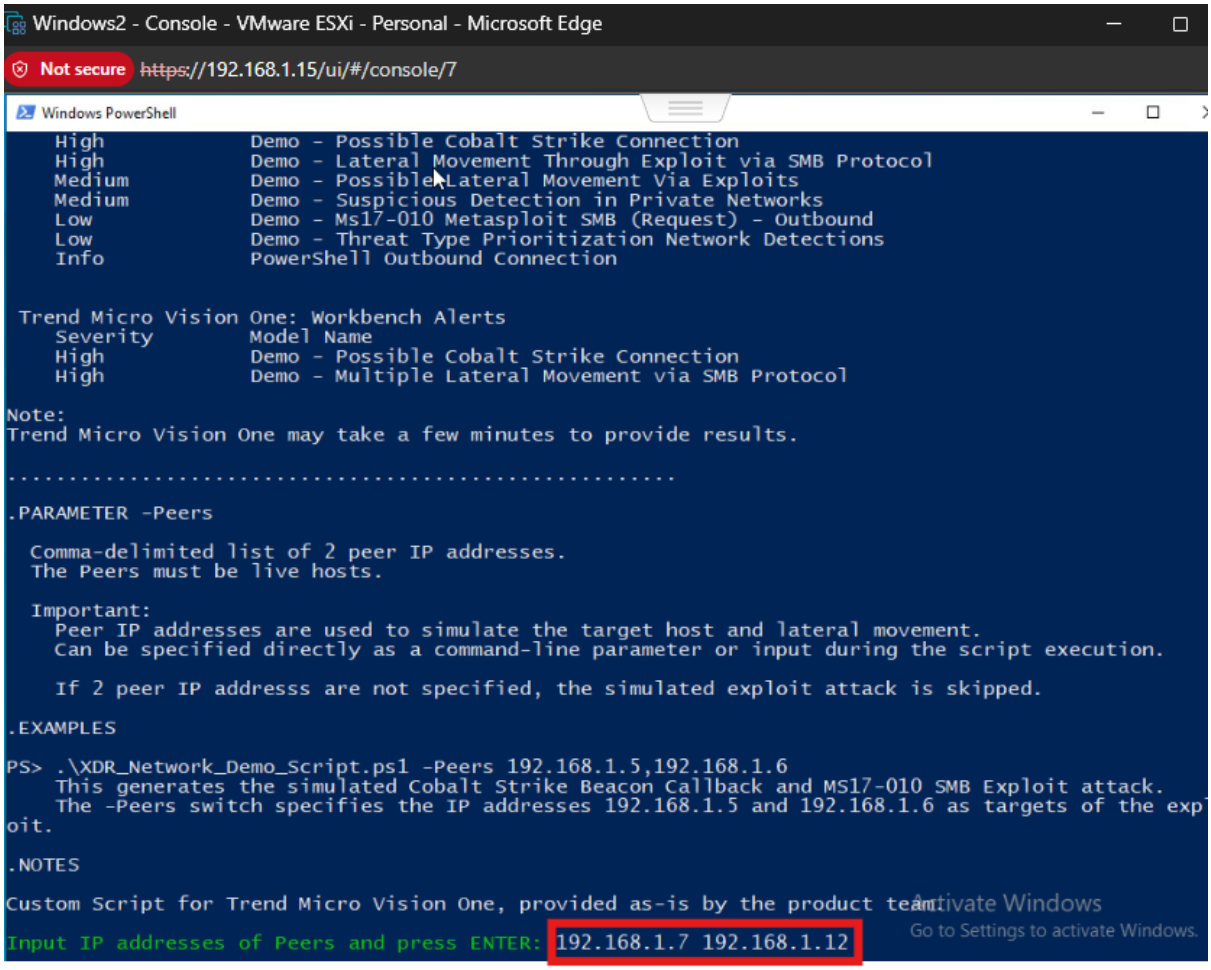
   Tải xuống kịch bản demo

   Tệp lưu trữ được bảo vệ bằng mật khẩu:

   Mật khẩu: Xu hướng MicroBAS

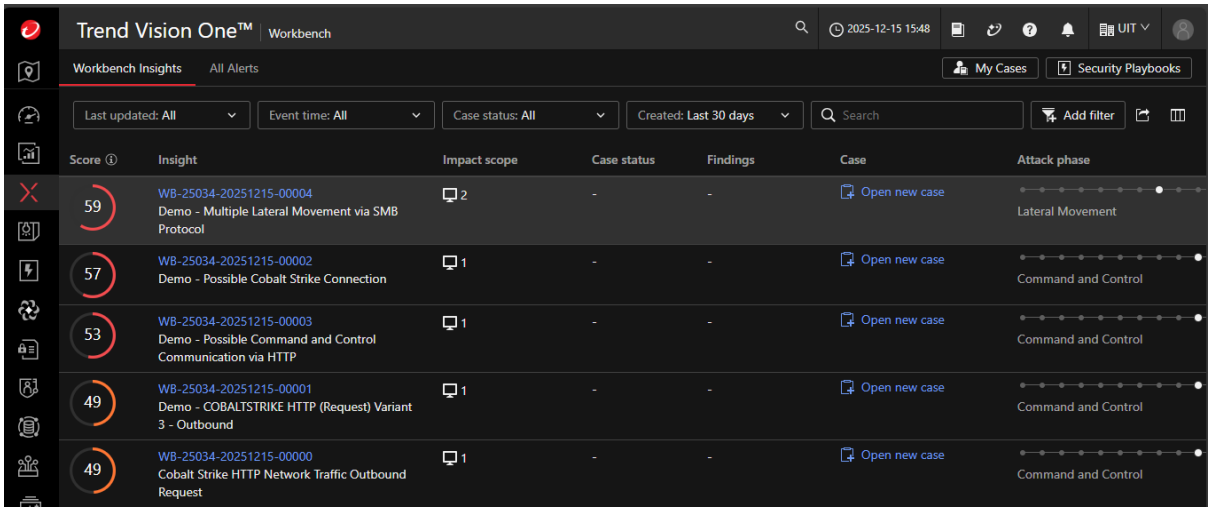
   SHA-256: C728E1FCB8D9F2FD279AAB99BDEF30521AAE11995AE5DD...
3. Kiểm tra kết quả trong Workbench hoặc Observed Attack Techniques sau khi chạy tập lệnh demo. Kết quả có thể mất vài

- Theo như hướng dẫn sẽ tải và chạy script ở máy Windows:



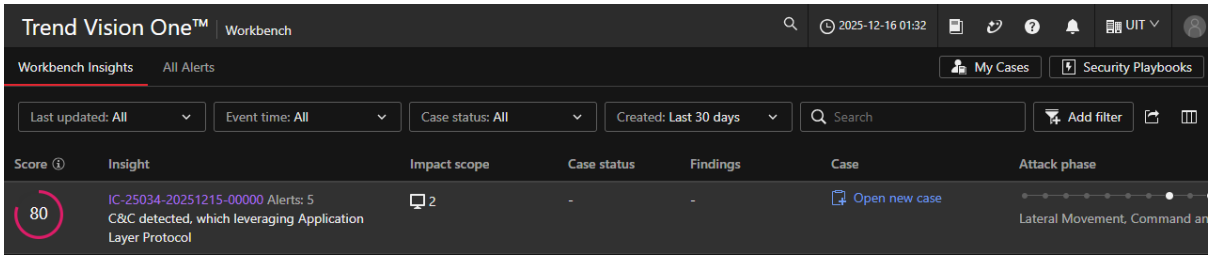
Nhập địa chỉ của máy nạn nhân

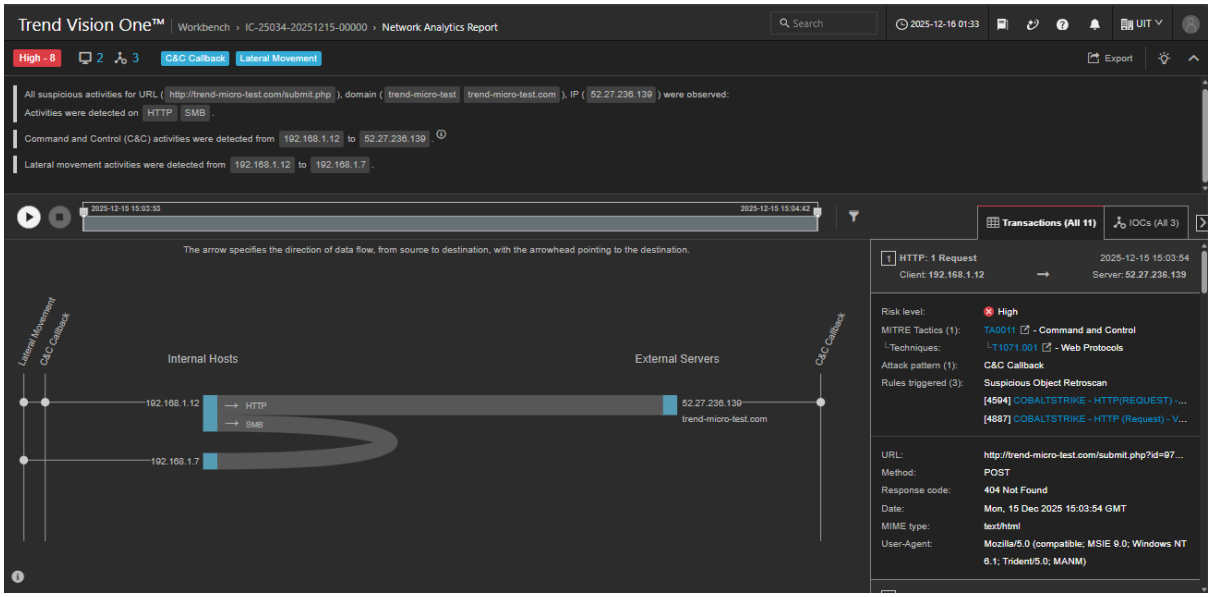
- Kiểm tra trong phần “Workbench” trên Trend Vision One:



Đã phát hiện tấn công

- Sau 1 khoảng thời gian, báo cáo chi tiết được tổng hợp:

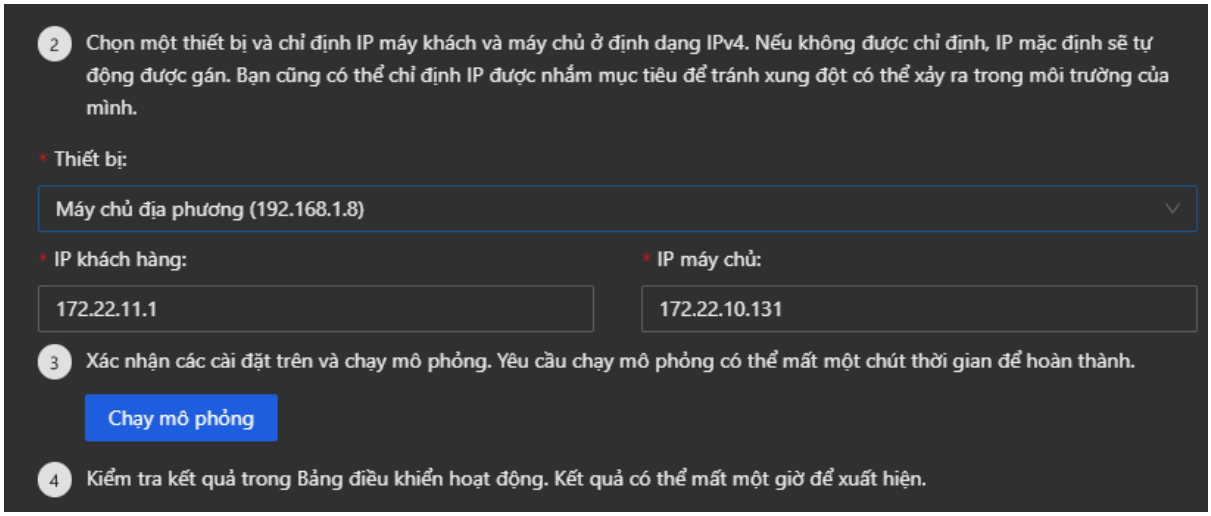




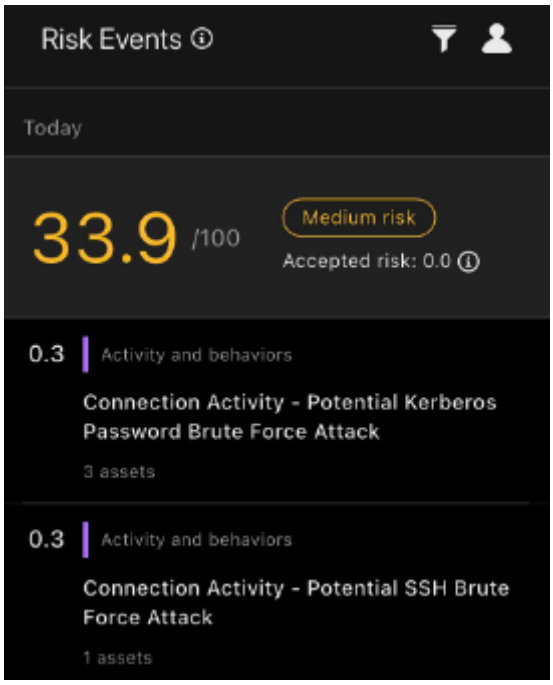
2. Mô phỏng hành vi bất thường

- Mô tả: chọn tấn công Brute Force và SSH

- Chọn VNS và client, server IP (không nhất thiết phải là của các máy trong mạng vì chỉ để mô phỏng):



- Kiểm tra ở mục “Risk events” và sử dụng bộ lọc “Activity and Behaviors” trên điện thoại:



3. Mô phỏng tấn công của tác nhân đe dọa

- Mô tả:

Mô phỏng tấn công của tác nhân đe dọa

Các kịch bản tấn công thực tế có thể được mô phỏng để chứng minh hiệu quả của việc phát hiện mạng trong môi trường của bạn.

Mô phỏng tấn công mạng:

APT28

Chi tiết mô phỏng:

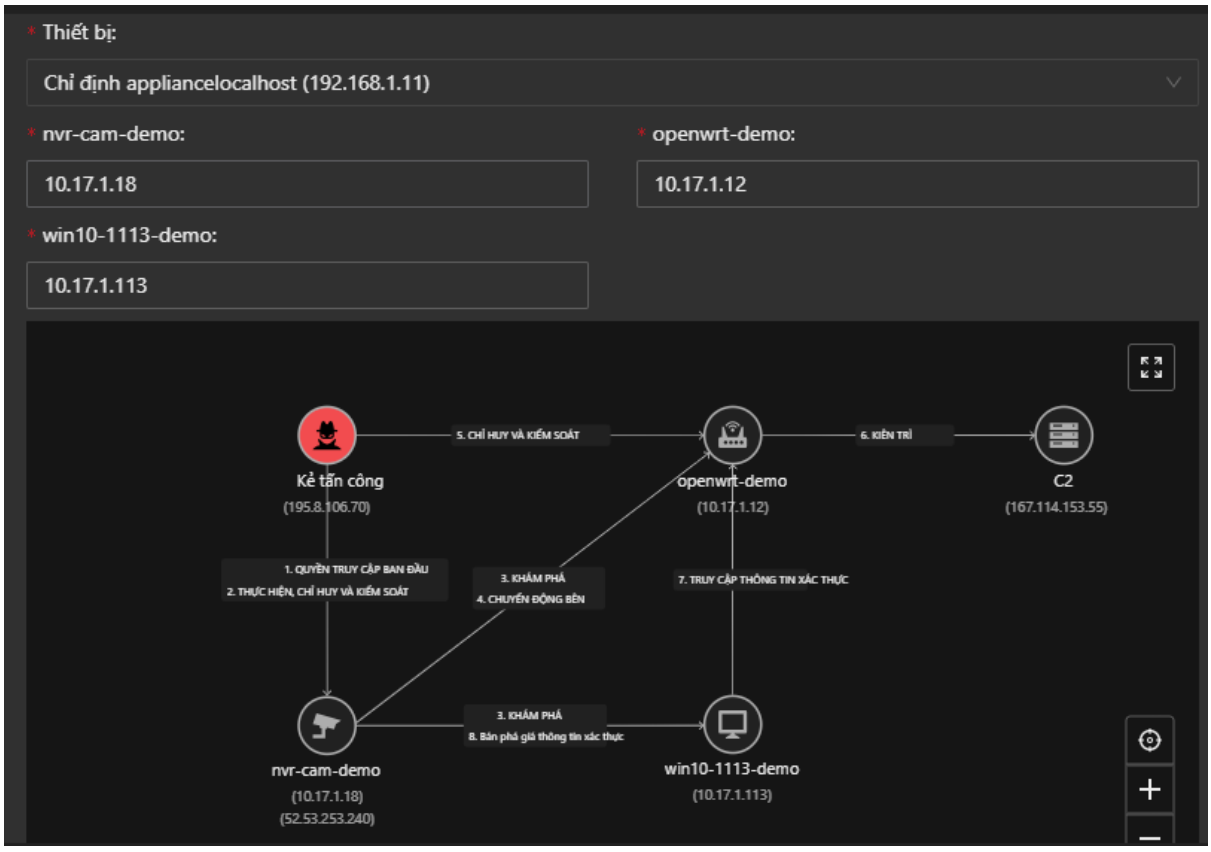
APT28, còn được gọi là Strontium, Sednit, Fancy Bear và Sofacy, là một nhóm gián điệp mạng có liên quan đến cơ quan tình báo quân sự Nga GRU. Hoạt động ít nhất từ năm 2004, APT28 nhắm mục tiêu vào các tổ chức chính phủ, quân đội và an ninh bằng cách sử dụng các kỹ thuật như khai thác zero-day, spear phishing và phần mềm độc hại.

Trong mô phỏng cuộc tấn công APT28 thực sự này, các lỗ hổng phần mềm được khai thác để truy cập vào thiết bị IoT (Network Video Recorder). SSH được bật và có quyền truy cập vào root shell. Chuyển động ngang đạt được thông qua proxy SOCKS và proxychains để quét cổng và tấn công brute-force vào hệ thống SSH.

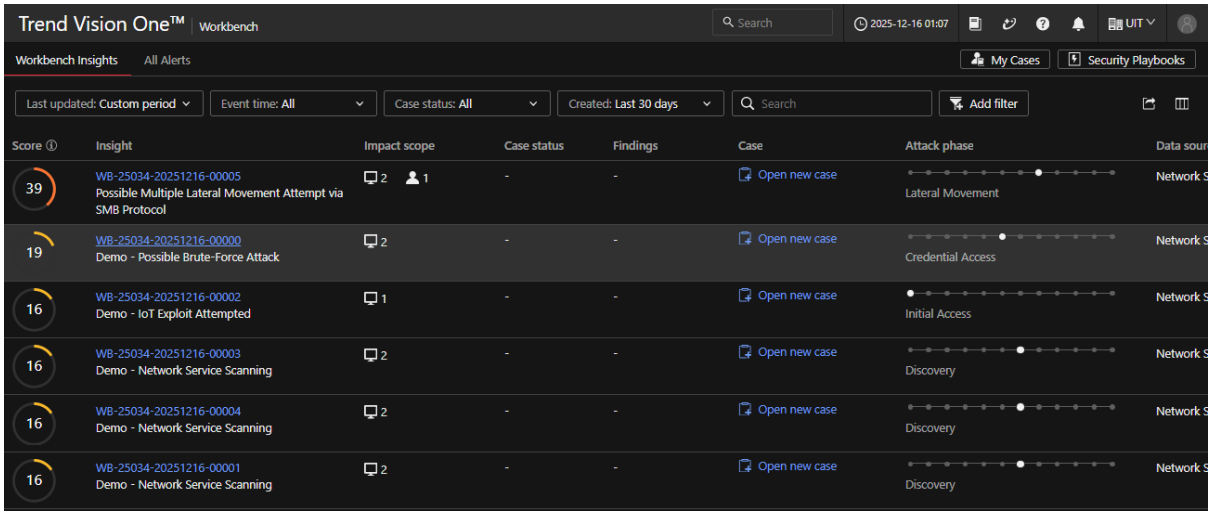
Các phương pháp khác bao gồm xâm nhập bộ định tuyến, cài đặt OpenVPN và tải lên các công cụ như Mimikatz. Với quyền truy cập VPN, quyền truy cập mạng không hạn chế đạt được và Responder được sử dụng để giả mạo NetBIOS và tiến hành các cuộc tấn công chuyển tiếp SMB để thu thập thông tin đăng nhập.

Thông tin đăng nhập được thu thập được sử dụng để tải xuống và thực thi Mimikatz từ xa với winexe để kết xuất thông tin xác thực thêm. Các tập lệnh shell đơn giản được triển khai để thiết lập tính bền vững của mạng, đảm bảo quyền truy cập mở rộng.

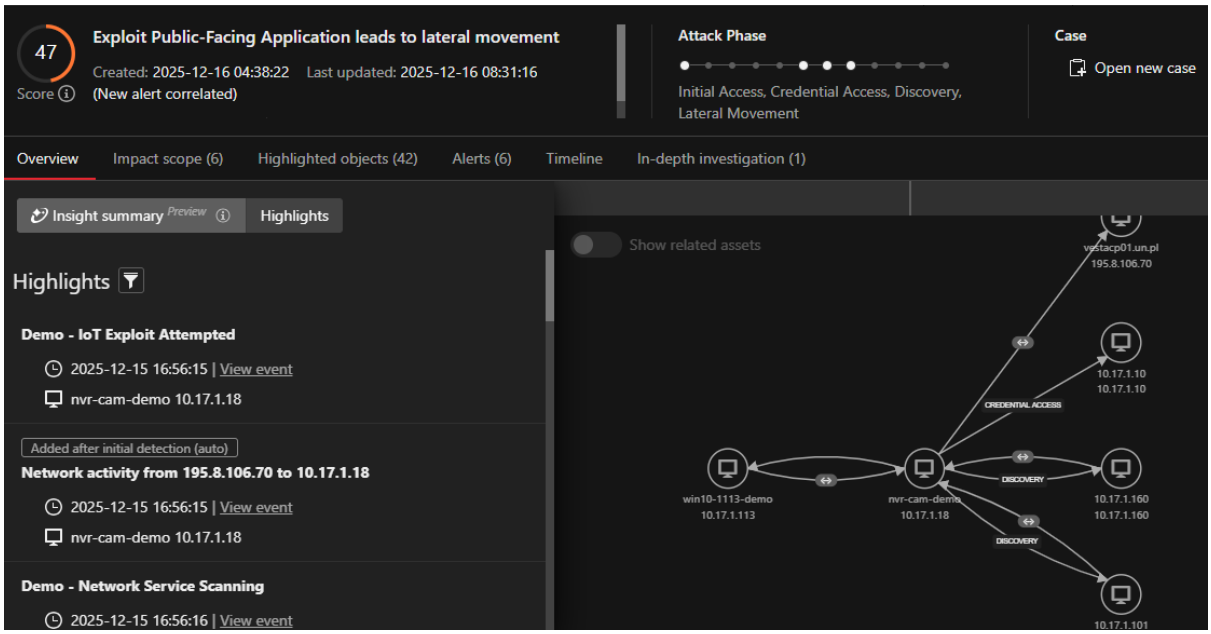
- Chọn IP của thiết bị VNS, còn các thiết bị khác chỉ là demo nên để IP mặc định (cùng mạng) để mô phỏng dữ liệu rồi chạy:



- Kiểm tra “Workbench”:



- Sau 1 khoảng thời gian, báo cáo chi tiết được tổng hợp:

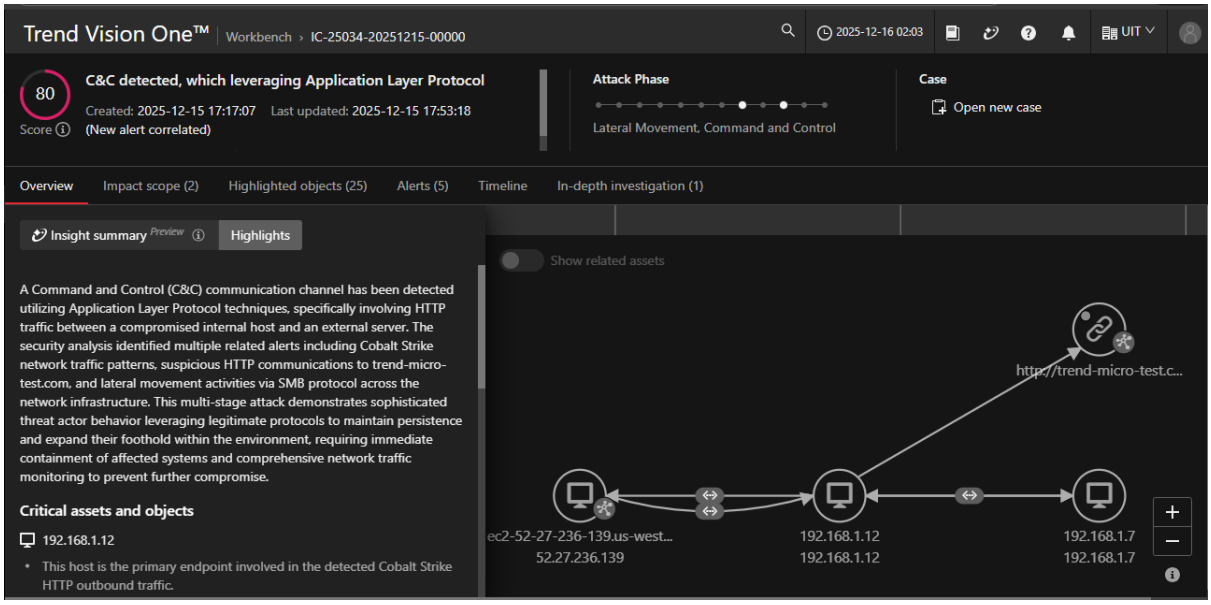


II. Phân tích kịch bản

Trong phần này, ta sẽ phân tích tấn công "**Giao thức lớp ứng dụng và Khai thác các dịch vụ từ xa**"

1. Điều tra Workbench tổng quan

- Tổng quan:



- Tổng kết: Hệ thống đã phát hiện một kênh liên lạc Command & Control (C&C) sử dụng các kỹ thuật ở tầng ứng dụng, cụ thể là lưu lượng HTTP giữa một máy nội bộ đã bị xâm nhập và một máy chủ bên ngoài. Phân tích bảo mật ghi nhận nhiều cảnh báo liên quan, bao gồm mẫu lưu lượng Cobalt Strike, giao tiếp HTTP đáng ngờ tới trend-micro-test.com, và hoạt động di chuyển ngang (lateral movement) thông qua giao thức SMB trong hạ tầng mạng. Đây là một cuộc tấn công nhiều giai đoạn, cho thấy tác nhân đe doạ lợi dụng các giao thức hợp lệ để duy trì hiện diện và mở rộng phạm vi xâm nhập, vì vậy cần cô lập ngay các hệ thống bị ảnh hưởng và giám sát lưu lượng mạng toàn diện để ngăn xâm nhập tiếp diễn.
- Đối tượng:
  + 192.168.1.12: máy bị **ảnh hưởng chính**, có lưu lượng HTTP outbound liên quan Cobalt Strike; là máy khởi tạo liên lạc tới C&C.
  + http://trend-micro-test.com/submit.php?id=97219: URL đích C&C mà máy bị xâm nhập đang liên lạc; gắn với mẫu giao tiếp Cobalt Strike.
  + trend-micro-test.com: tên miền đóng vai trò domain C&C, xuất hiện trong các hoạt động mạng đáng ngờ.
  + 192.168.1.7: liên quan đến di chuyển ngang qua SMB; là một phần của chuỗi tấn công có nhiều endpoint bị ảnh hưởng.
  + trend-micro-test: hostname liên quan tới máy bị xâm nhập và hạ tầng nội bộ; có liên hệ với hoạt động lateral movement qua SMB.

2. Điều tra Workbench – execution profile trên máy Victim

a) Tổng quan

- Victim chính: 192.168.1.12
- Trong Workbench, Execution Profile thể hiện:

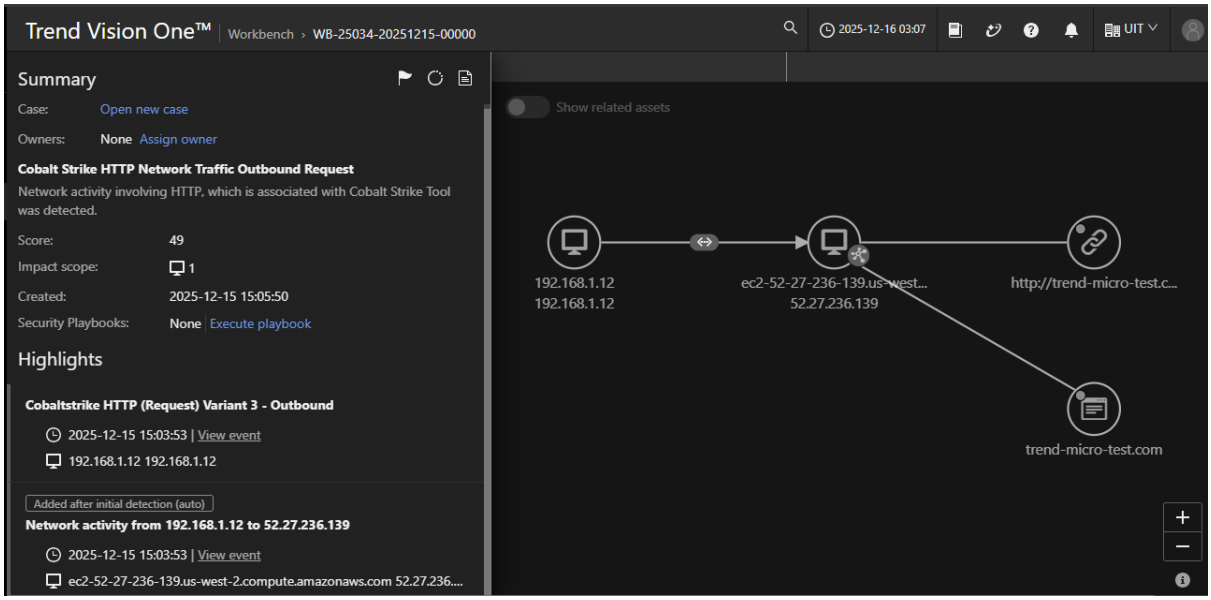
  + Chuỗi network-based execution (do mô phỏng không có agent EDR)
  + Các hành vi được ánh xạ theo MITRE ATT&CK
  + Quan hệ giữa Victim → C2 → Internal host

b) Kết luận

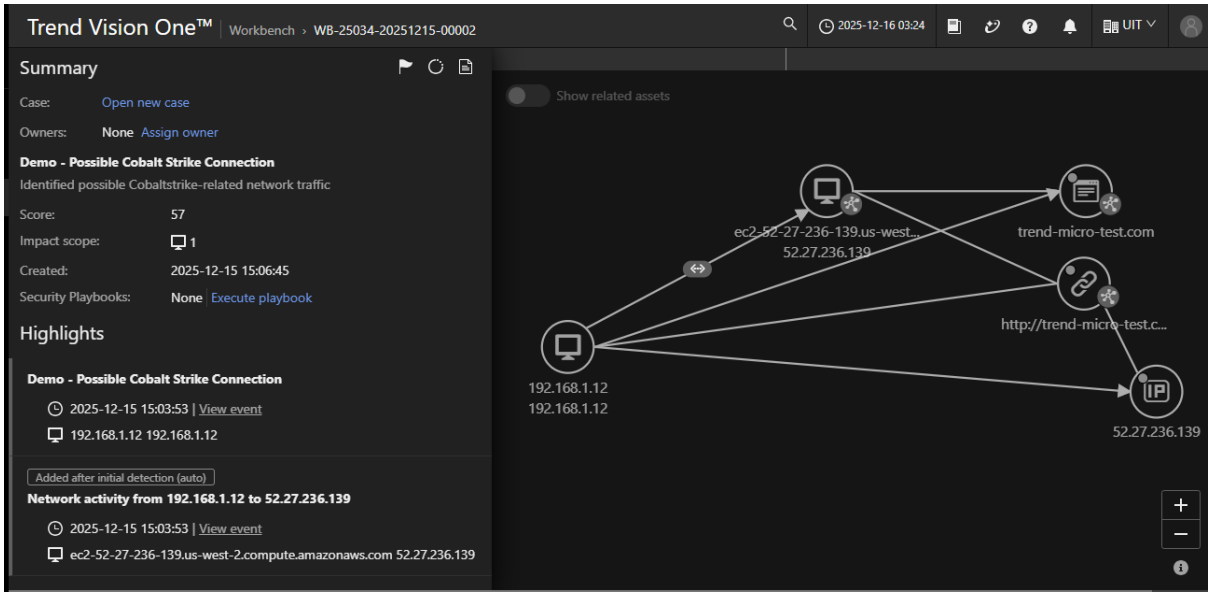
- 192.168.1.12 đã bị xâm nhập, máy này đóng vai trò:
  + Beacon C2 ra Internet
  + Pivot point để di chuyển ngang
- Tấn công mang tính multi-stage, không phải sự kiện đơn lẻ
- Kỹ thuật sử dụng: Application Layer C2 (HTTP), Living-off-the-network (SMB)

3. Điều tra chi tiết các phát hiện

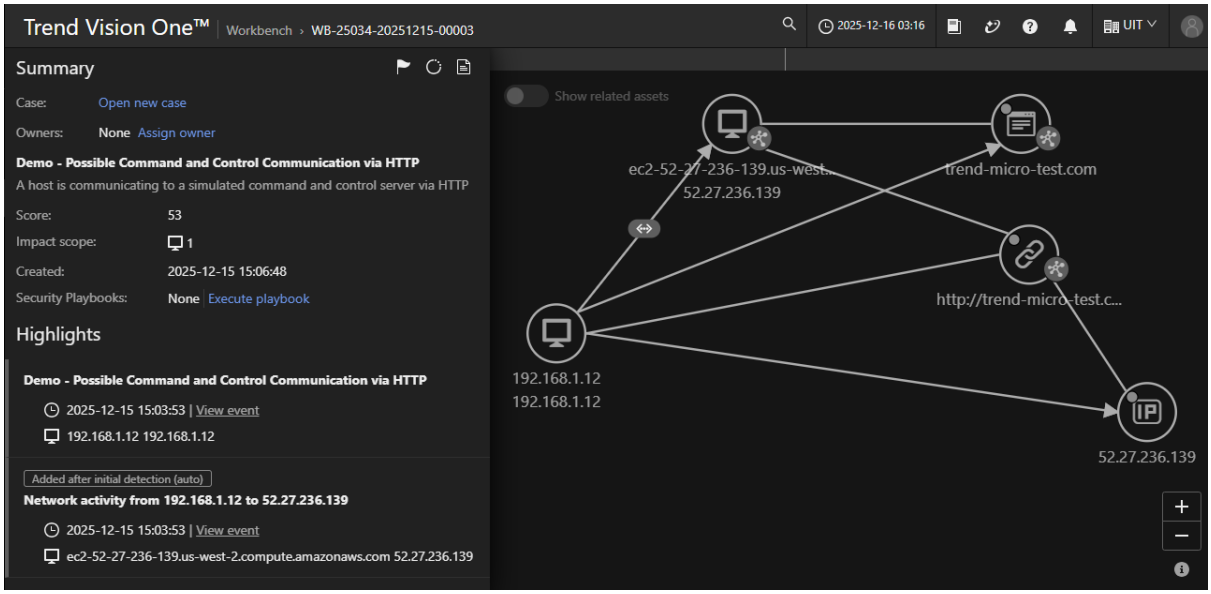
- Cảnh báo đầu tiên: 192.168.1.12 đã **tạo HTTP request** ra ngoài tới một server trên Internet, dùng domain/URL cụ thể; nội dung/mẫu request giống Cobalt Strike, nên bị đánh dấu là C2 (C&C – Command and Control là kênh liên lạc giữa máy bị nhiễm (victim) và máy chủ của kẻ tấn công (C2 server)). beaconing



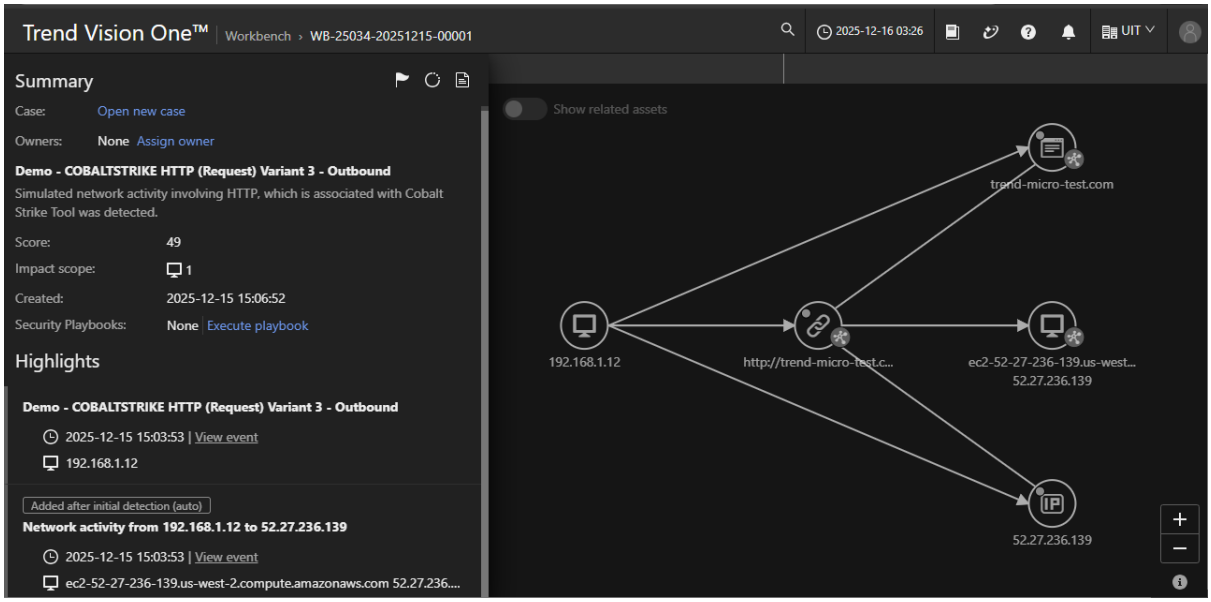
- Cảnh báo thứ 2: 192.168.1.12 **đang có lưu lượng outbound HTTP** tới trend-micro-test.com (52.27.236.139), bị nghi là kết nối Cobalt Strike/C2.



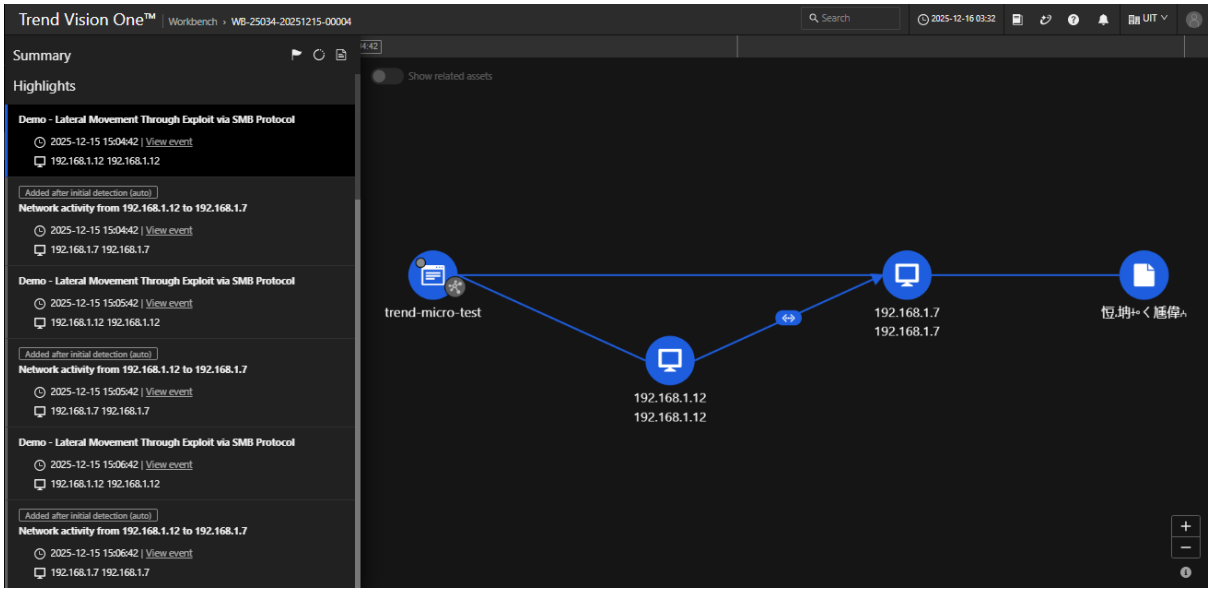
- Cảnh báo thứ 3: Máy 192.168.1.12 đang **giao tiếp C2 qua HTTP** (mô phỏng) tới domain trend-micro-test.com, được resolve về IP 52.27.236.139 (EC2/AWS) — thể hiện kết nối outbound từ máy nội bộ ra "máy chủ điều khiển" bên ngoài.



- Cảnh báo thứ 4: Máy 192.168.1.12 **phát sinh HTTP outbound** (beacon/C2) tới trend-micro-test.com (URL http://trend-micro-test...) được resolve về IP 52.27.236.139 (EC2/AWS), nên bị nhận diện là lưu lượng giống Cobalt Strike (COBEACON).



- Cảnh báo thứ 5: Máy 192.168.1.12 thực hiện **di chuyển ngang (lateral movement)** bằng cách khai thác/ truy cập qua giao thức SMB sang máy 192.168.1.7 (các event "Network activity from 192.168.1.12 to 192.168.1.7"), cho thấy khả năng lan rộng từ máy bị xâm nhập sang máy nội bộ khác.



III. Kết luận

Thông qua các nội dung trên, hệ thống đã được kiểm chứng khả năng giám sát – phát hiện – điều tra theo luồng tác chiến thực tế. Các kịch bản mô phỏng (Simulations/OAT) giúp tạo dữ liệu tấn công có kiểm soát, từ đó đánh giá mức độ quan sát của cảm biến mạng và năng lực tổng hợp sự kiện trên Trend Vision One một cách rõ ràng.

Kết quả điều tra trên Workbench cho thấy nền tảng có thể liên kết và làm nổi bật các dấu hiệu quan trọng của chuỗi tấn công nhiều giai đoạn, điển hình như hoạt động Command & Control qua HTTP (mẫu hành vi tương tự Cobalt Strike) và dấu hiệu di chuyển ngang qua SMB trong nội bộ. Điều này hỗ trợ rút ngắn thời gian khoanh vùng, ưu tiên xử lý sự cố và đưa ra hành động ứng phó phù hợp (cô lập máy bị ảnh hưởng, giám sát mở rộng và chặn các chỉ dấu liên quan).