TẠP CHÍ KHOA HỌC
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP HỒ CHÍ MINH
Tập 22, Số 1 (2025): 27-38
Website: https://journal.hcmue.edu.vn
ISSN: 2734-9918

HO CHI MINH CITY UNIVERSITY OF EDUCATION
JOURNAL OF SCIENCE
Vol. 22, No. 1 (2025): 27-38
https://doi.org/10.54607/hcmue.js.22.1.4352(2025)

Bài báo nghiên cứu

KHUNG GIÁM SÁT VÀ PHẢN ỨNG SỰ CỐ AN NINH TỰ ĐỘNG: THỰC TIỄN TỐT CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

Nguyễn Hoàng Thành*, Huỳnh Trọng Thưa
Học viện Công nghệ Bưu chính Viễn thông, Việt Nam
**Tác giả liên hệ: Nguyễn Hoàng Thành – Email: thanhnh@ptit.edu.vn*
Ngày nhận bài: 17-6-2024; ngày nhận bài sửa: 13-9-2024;ngày duyệt đăng: 16-9-2024

TÓM TẮT

Trong bối cảnh kĩ thuật số hiện nay, việc ứng phó sự cố trong các doanh nghiệp vừa và nhỏ (SME) chủ yếu dựa vào nguồn lực nội bộ hạn chế hoặc sự trợ giúp từ bên ngoài. Trong khi các tập đoàn lớn thường tuân theo các tiêu chuẩn như ISO 2700x, các SME lại đối mặt với những thách thức riêng khi phải thích nghi với các mối đe dọa mạng đang phát triển nhanh chóng. Các hệ thống giám sát và phản ứng sự cố tự động trở nên thiết yếu để bảo vệ thông tin nhạy cảm, duy trì hoạt động liên tục của doanh nghiệp và đảm bảo tuân thủ quy định. Tuy nhiên, hầu hết các nền tảng giám sát an ninh và xử lí sự cố hiện có đều đắt đỏ, thiếu tính tự động hóa và đòi hỏi nhân sự có trình độ cao, khiến chúng không phù hợp với các SME. Nghiên cứu này đề xuất một khung giải pháp giải quyết những thách thức này bằng cách kết hợp dữ liệu nhật kí từ các hệ thống giám sát hiện có với các kĩ thuật phản ứng sự cố tự động hiện đại. Giải pháp được đề xuất được thiết kế để tiết kiệm chi phí và dễ sử dụng cho các SME, giúp họ phát triển và triển khai hệ thống giám sát và phản ứng tự động mà không cần đến nguồn lực hoặc chuyên môn sâu rộng. Bằng cách đưa ra một cách tiếp cận thực tế và dễ tiếp cận đối với an ninh mạng, khung giải pháp này nhằm nâng cao hiệu quả của các SME trong việc bảo vệ hệ thống thông tin của họ, thúc đẩy tính chủ động và khả năng tự quản lí các sự cố an ninh thông tin.

Từ khóa: tự động; mối đe dọa; phản ứng sự cố; giám sát; phát hiện; SME

1. Giới thiệu

Với sự gia tăng các mối đe dọa an ninh mạng như lừa đảo và mã độc, các phương pháp giám sát thủ công trở nên không hiệu quả do thời gian phản ứng chậm và thiếu nhân lực chuyên môn. Để giảm thiểu rủi ro, giảm thiệt hại và tiết kiệm chi phí, các hệ thống phản ứng sự cố tự động đã ra đời, giúp tự động hóa các nhiệm vụ lặp lại, nâng cao hiệu quả và giảm sai sót con người. Các giải pháp này còn cung cấp dữ liệu giá trị để cải thiện an ninh lâu dài.

Các SME ngày càng trở thành mục tiêu của tội phạm mạng. Theo báo cáo của Verizon về các vụ vi phạm dữ liệu, tập trung vào các SME (Verizon, 2024), hiện nay trên toàn cầu đã chứng kiến sự gia tăng của các cuộc tấn công mạng vào các SME khoảng 30% so với năm 2023. Điều này chủ yếu là do các SME thường có hệ thống bảo mật yếu hơn so với các doanh

Cite this article as: Nguyen Hoang Thanh, & Huynh Trong Thua (2025). Automatic incident monitoring and response framework: Best practices for small and medium-sized enterprises. *Ho Chi Minh City University of Education Journal of Science, 22*(1), 27-38.

nghiệp lớn, tổng thiệt hại kinh tế do các cuộc tấn công mạng gây ra cho các SME trên toàn cầu ước tính khoảng 250 tỉ USD, tăng 35% so với năm trước, hơn 1 tỉ hồ sơ thông tin của các SME bị rò rỉ hoặc đánh cắp trong các cuộc tấn công mạng, và khoảng 40% các SME không thể khôi phục sau một cuộc tấn công mạng nghiêm trọng, dẫn đến việc phải đóng cửa hoạt động hoặc bị ảnh hưởng nặng nề về tài chính. Tại Việt Nam, theo báo cáo (Authority of Information Security, 2024) ngày 19/04/2024 của Cục An toàn thông tin về tình hình an ninh mạng tại Việt Nam, xu hướng tấn công mã hóa tống tiền tăng mạnh, với các mục tiêu như VNDirect, PVOIL và Vietnam Post, gây gián đoạn hoạt động và tổn thất lớn. Trong tháng 3/2024, Trung tâm Giám sát An ninh mạng Quốc gia phát hiện hơn 1600 lỗ hổng trên 5000 hệ thống công khai, trong đó có 12 lỗ hổng nghiêm trọng, tiềm ẩn nguy cơ bị khai thác.".

Mặc dù, đối mặt với nhiều rủi ro an ninh mạng, nhiều SME vẫn chưa có sự chuẩn bị đầy đủ để xử lí các sự cố do hạn chế về tài chính, nhân lực và chuyên môn. Tình trạng này trở nên nghiêm trọng hơn khi phần lớn SME không có đội ngũ an ninh thông tin chuyên trách, trong khi sự phức tạp của các giải pháp an ninh hiện đại đòi hỏi kiến thức kĩ thuật cao. Phụ thuộc vào dịch vụ thuê ngoài cũng không phải lúc nào đảm bảo ưu tiên hoặc hiệu quả về an ninh mạng. Các nền tảng như Enterprise Security (Splunk, 2024), Qradar SIEM (IBM, 2024), ArcSight Enterprise Security Manager (OpenText, 2024), và XDR Platform (Trellix, 2024) tuy mạnh mẽ nhưng có chi phí cao và yêu cầu hạ tầng phức tạp, khiến việc triển khai trở nên khó khăn, đặc biệt là tại Việt Nam. Vì vậy, các SME rất cần những giải pháp an ninh mạng linh hoạt, dễ triển khai và tiết kiệm chi phí hơn để đáp ứng nhu cầu bảo mật và bảo vệ hoạt động của mình.

Mục tiêu của nghiên cứu này là thiết kế và phát triển một khung giải pháp phản ứng sự cố an ninh thông tin vừa đơn giản vừa hiệu quả, được thiết kế riêng để đáp ứng nhu cầu của các SME là điều cần thiết. Khung giải pháp này sẽ bao gồm các đặc điểm như chi phí đầu tư và triển khai thấp, dễ cấu hình, tích hợp và vận hành, nhưng phải bảo vệ an toàn chống lại nhiều mối đe dọa và phản ứng hiệu quả với các sự cố an ninh thông tin. Chúng tôi sử dụng phương pháp nghiên cứu phân tích thực trạng các mối đe dọa an ninh mạng đối với các SME, đánh giá hiệu quả của các hệ thống phản ứng sự cố hiện tại, và đề xuất mô hình tự động hóa nhằm giảm thiểu thiệt hại và tăng cường khả năng bảo vệ.

Nghiên cứu này đuọc trình bày thành 3 phần, ngoài phần giới thiệu, các phần còn lại được trình bày như sau. Phần 2 trình bày các nội dung chính gồm các công trình liên quan, Thiết kế và triển khai khung giám sát và phản ứng sự cố an ninh tự động. Phần 3 là kết luận và hướng phát triển.

2. Nội dung

2.1. Các công trình liên quan

Nghiên cứu (William et al., 2021) đề xuất thiết kế một hướng dẫn cho việc triển khai đội ứng cứu sự cố máy tính (CIRT) tại các trường đại học. Bằng cách thành lập CIRT trong các trường đại học, các cơ sở này không chỉ bảo vệ được cơ sở hạ tầng kĩ thuật số của mình mà còn đóng góp vào một phản ứng phối hợp lớn hơn đối với các sự cố an ninh trên phạm vi quốc gia. Nghiên cứu (Ashley O'Neil, 2021) cho rằng khả năng của một tổ chức trong việc phát hiện, ngăn chặn và phục hồi từ sự cố an ninh chủ yếu phụ thuộc vào năng lực của

đội phản ứng sự cố (IR). Họ phát triển một phương pháp đào tạo dựa trên kịch bản để hỗ trợ các tổ chức vượt qua các rào cản kĩ thuật-xã hội trong việc phản ứng sự cố. Nghiên cứu (Avi, Yulia, Pete, & Peter, 2023) đề xuất cải tiến sách hướng dẫn phản ứng sự cố bằng cách bổ sung ngữ cảnh vận hành, chuyển từ mô hình quy trình sang tích hợp mô hình vận hành, giúp nâng cao hiệu quả. Tuy nhiên, cả ba cách tiếp cận trên chủ yếu dựa vào đội ngũ nhân sự chuyên môn cao và các quy trình nhiều bước phức tạp, tạo ra nhiều thách thức có thể làm giảm hiệu quả việc quản lí và phản ứng sự cố an ninh thông tin.

Nghiên cứu (Huynh , 2020) đề xuất mô hình kết hợp mạng nơ-ron nhiều lớp với huấn luyện nhiều giai đoạn DSD để cải tiến đồng thời các tiêu chí liên quan đến hiệu quả thực thi của các hệ thống phát hiện xâm nhập đạt được độ chính xác cao nhất. Trong nghiên cứu (Tanwir & Dragos, 2023), tác giả đề xuất một phương pháp phát hiện xâm nhập dựa trên sự bất thường có khả năng phát hiện các cuộc tấn công trong thời gian thực khi chúng đang diễn ra. Mô hình CNN với số lượng tham số tương đối nhỏ được sử dụng cho việc huấn luyện và giám sát được chọn để phương pháp này có thể nhanh chóng và sử dụng được trong các thiết lập thời gian thực. Tuy nhiên, cả hai mô hình đề xuất đều chỉ tập trung vào việc phát hiện sự cố, việc phản ứng vẫn để lại cho các xử lí thủ công.

Việc tích hợp các công nghệ tiên tiến, chẳng hạn như phát hiện dựa trên học máy, trong khung làm việc của Trung tâm điều hành an ninh (SOC) cho phép phân tích thời gian thực lưu lượng mạng và các bất thường. Trong nghiên cứu (Zafar Iqbal, 2020), Iqbal và công sự đã sử dụng phương pháp học máy để cho phép phát hiện nhanh chóng và tự động cảnh báo cho phản ứng ngay lập tức với các sự cố an ninh. Trong nghiên cứu (Islam et al., 2022), Islam và cộng sự đã đề xuất một khung làm việc mới dựa trên trí tuệ nhân tạo gọi là SmartValidator nhằm tự động hóa quá trình xác thực các cảnh báo bằng cách sử dụng về các mối hiểm họa trong hệ thống SOC. Khung này được phát triển nhằm khắc phục quá trình cập nhật thủ công gây ra sự chậm trễ trong việc phản ứng với các cuộc tấn công. SmartValidator sử dụng các kĩ thuật học máy, bao gồm ba lớp: thu thập dữ liệu, xây dựng mô hình và xác thực cảnh báo. Tuy vậy, việc kiểm chứng hiệu quả phát hiện và phản ứng khi áp dụng các mô hình học máy, học sâu và trí tuệ nhân tạo vào hệ thống SOC vẫn còn nhiều thách thức, chưa đầy đủ.

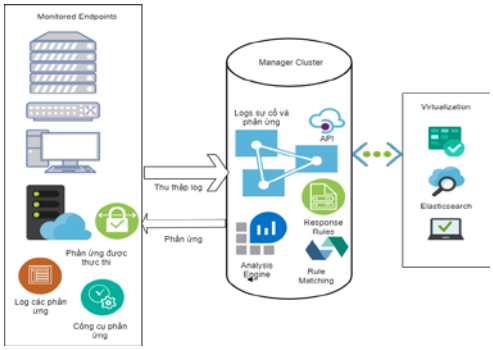
Ti Dun và cộng sự đã nghiên cứu cách mà các Trung tâm điều hành an ninh thế hệ mới (NGSOC) phản ứng với các hoạt động độc hại trong nghiên cứu (Dun et al., 2022) nhằm phát hiện phần mềm độc hại Hermes Ransomware. Tuy nhiên, khung kiến trúc này có một hạn chế vì thiếu tính phổ quát, chỉ có thể áp dụng cho một vài trường hợp cụ thể. Trong nghiên cứu (Rajesh et al., 2022), bằng cách tích hợp các kĩ thuật botnet vào ma trận MITRE ATT&CK, giúp doanh nghiệp có thể lập bản đồ các chiến thuật, kĩ thuật và quy trình cụ thể liên quan đến botnet, nâng cao khả năng phát hiện mối đe dọa tổng thể. Wang và cộng sự (Wang et al., 2021) đã giới thiệu một SOC toàn diện để giải quyết và giảm thiểu các vấn đề đã được xác định. Khung này bao gồm thành phần phân tích hành vi và nền tảng SOC tích hợp với dữ liệu lớn. Tuy nhiên, các giải pháp SOC tổng thể thường phức tạp và khó triển khai, không phù hợp với SME.

Tại Việt Nam, nghiên cứu (Nguyen et al., 2022) phân tích các nguy cơ an ninh mạng tại Việt Nam và đề xuất các giải pháp như tường lửa đa tầng và hệ thống bảo mật cho tập đoàn FPT, mang tính thực tiễn cao cho doanh nghiệp Việt Nam và thị trường mới nổi. Tuy nhiên, nghiên cứu chưa đề cập đến phản ứng thông minh với sự cố. Trong một nghiên cứu khác (Le et al., 2017), tác giả giới thiệu mô hình đánh giá an ninh mạng (CSAM) dựa trên kiến trúc ISO 2700x và NIST SP 800-53 Rev.4. Nghiên cứu này giúp đánh giá toàn diện cho các tổ chức trong việc xác định điểm mạnh và điểm yếu về an ninh mạng. Tuy nhiên, nghiên cứu có thể cần thêm dữ liệu định lượng hoặc các trường hợp điển hình cụ thể hơn để minh chứng cho tính hiệu quả của mô hình đề xuất khi áp dụng trong thực tế.

2.2. Thiết kế khung giám sát và phản ứng sự cố an ninh tự động

2.2.1. Thiết kế tổng quan

Khung giải pháp chúng tôi đề xuất gọi là AIMRF (Automatic Incident Monitoring and Response Framework) dựa trên các Agents, chạy trên các điểm cuối được giám sát, chuyển tiếp dữ liệu bảo mật đến một máy chủ trung tâm. Các thiết bị không có Agent có thể gửi dữ liệu qua Syslog, SSH hoặc API. Máy chủ trung tâm giải mã, phân tích dữ liệu và chuyển kết quả đến cụm Elasticsearch để lập chỉ mục và lưu trữ. Cụm Elasticsearch hỗ trợ từ cụm đơn (xử lí dữ liệu nhỏ) đến cụm nhiều nút (với dữ liệu lớn hoặc yêu cầu sẵn sàng cao). Filebeat được sử dụng để chuyển tiếp an toàn dữ liệu và cảnh báo tới Elasticsearch qua mã hóa TLS, đảm bảo hiệu quả và an toàn trong môi trường sản xuất.



Hình 1. *Mô hình kiến trúc tổng thể*

Hình 1 mô tả kiến trúc triển khai khung giám sát được chúng tôi đề xuất với các thành phần chính. Trong đó các máy chủ giám sát và Elasticsearch có thể được định cấu hình như một cụm, cung cấp khả năng cân bằng tải và tính sẵn sàng cao.

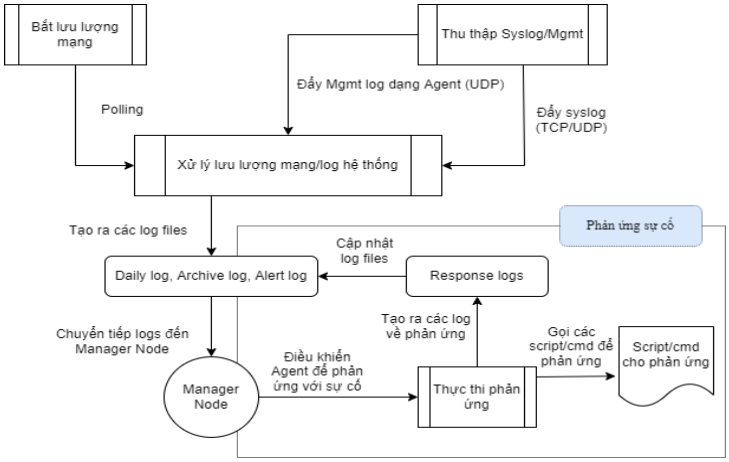
Kiến trúc của khung gồm 3 phần chính: (1) Thành phần thu thập dữ liệu, là nơi giám sát và thực thi phản ứng sự cố an ninh theo điều khiển từ Manager Cluster, có thể là server, máy trạm, thiết bị mạng hoặc đám mây. (2) Máy chủ xử lí, phân tích dữ liệu log để tạo cảnh báo sự cố và thiết lập các rule, mã lệnh điều khiển từ xa để xử lí sự cố tại các Agents. (3) Thành phần dành cho người giám sát an ninh hoặc hệ thống ngoài, nhận cảnh báo và kết quả xử lí các sự cố an ninh.

2.2.2. Các luồng xử lí chính

Thiết kế luồng xử lí cho Agent như Hình 2. Agent bắt lưu lượng mạng qua cơ chế Polling hoặc thu thập thông các giao thức khác như Syslog, SNMP theo dạng Agent hoặc giao thức dựa trên UDP/TCP. Sau đó là xử lí lưu lượng mạng hoặc log hệ thống để tạo ra

các dữ liệu logs. Cuối cùng là Agent chuyển các logs này đến Manager.

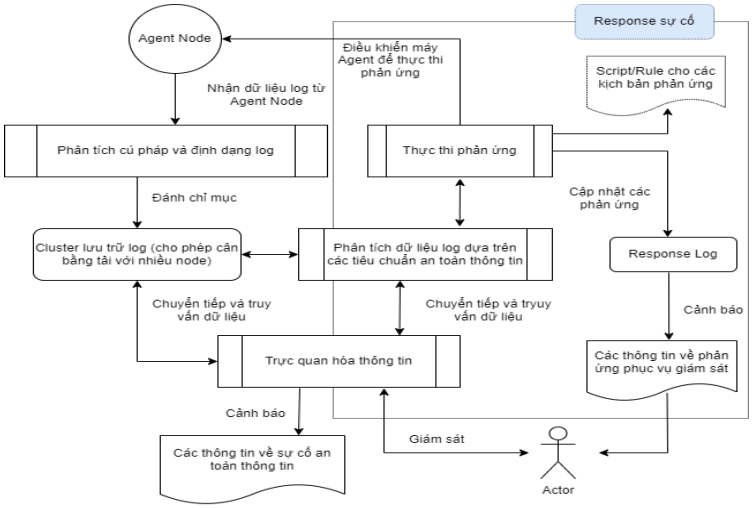
Trong trường hợp Manager phân tích log và cho kết quả là có sự cố an ninh và gửi điều khiển về Agent. Agent sẽ thực thi các phản ứng với sự cố tương ứng dựa trên các script hoặc command tương ứng, đồng thời nó cũng tạo các log phản ứng để gửi về Manager nhằm cập nhật thông tin về kết quả sự cố cho bộ phận giám sát.



Hình 2. *Luồng xử lí tại Agent*

Luồng xử lí của Manager hoạt động như sau: Manager nhận log từ Agent, phân tích cú pháp và định dạng lại log theo cấu trúc phù hợp. Sau đó, log được đánh chỉ mục và đưa vào cơ sở dữ liệu tìm kiếm. Tiếp theo, Manager phân tích dữ liệu log dựa trên các tiêu chuẩn an toàn, chuyển dữ liệu đã xử lí đến khối trực quan hóa, và cuối cùng cung cấp giao diện hoặc công cụ cảnh báo giúp giám sát viên dễ dàng theo dõi và truy vấn thông tin.

Bên cạnh đó, Manager dựa trên kết quả phân tích logs để phát hiện sự cố an ninh, sau đó kích hoạt phản ứng sự cố dựa trên các rule hoặc script phù hợp. Các script này có thể điều khiển từ xa đến Agents để thực thi commands tương ứng. Đồng thời, trong quá trình xử lí, Manager có khả năng liên kết với các đối tác bên thứ ba để thực hiện phân tích chuyên sâu, tùy thuộc vào từng loại sự cố.



Hình 3. *Luồng xử lí tại Manager*

2.2.3. Các thành phần chính của khung giải pháp

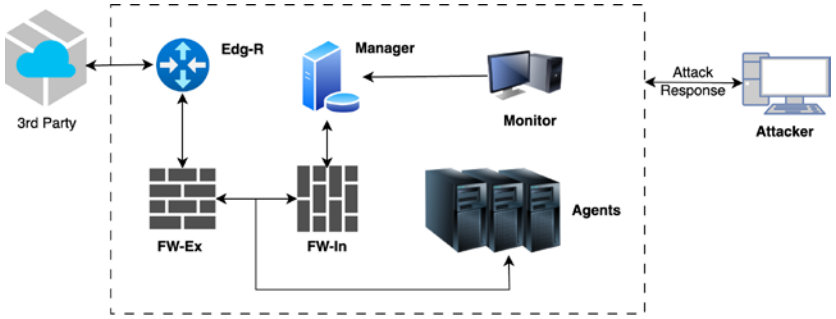
Hệ thống gồm hai thành phần chính là Agent và Manager. Agent thu thập dữ liệu và log từ các máy chủ, thiết bị đầu cuối, thiết bị mạng, bao gồm log hệ thống, log mạng và các sự kiện an ninh, sau đó gửi đến Manager để phân tích. Khi nhận lệnh từ Manager, Agent thực hiện phản ứng sự cố như chạy scripts hoặc lệnh và gửi lại log phản ứng. Manager phân tích, đánh chỉ mục và lưu trữ log, giúp phát hiện mối đe dọa và sự cố an ninh, đồng thời gửi lệnh đến Agent để xử lí sự cố. Ngoài ra, Manager cung cấp giao diện trực quan để giám sát và tích hợp với hệ thống bên ngoài nhằm nâng cao hiệu quả xử lí. Mối quan hệ chính giữa Agent và Manager là trao đổi log và lệnh, giúp tối ưu hóa khả năng phản ứng nhanh và chính xác đối với các mối đe dọa an ninh.

2.2.4. Giải pháp kĩ thuật, công nghệ cho các chức năng thiết kế

Dưới đây là các kĩ thuật và công nghệ được sử dụng cho các chức năng được thiết kế cho Agent và Manager ở trên.

- Mã hóa: AES (Advanced Encryption Standard);
- Thu thập log: Netsniff-ng, Snort/Suricata, OSSEC (hệ thống phát hiện xâm nhập dựa trên máy chủ), Syslog-ng, Wazuh Agent (Wazuh là nền tảng mã nguồn mở hỗ trợ thu thập và phân tích dữ liệu như log hệ thống, thông tin về quá trình và các sự kiện bảo mật);
- Giao thức trao đổi log: Syslog, PF_RING (giúp tăng tốc độ và hiệu suất thu thập dữ liệu mạng), SNMP;
- Các loại log: Event log (archive), monitoring log (daily), alert log;
- Trực quan hóa thông tin: Kibana;
- Cảnh báo: Email, Slack (nền tảng nhắn tin và cộng tác);
- Truy vấn dữ liệu và thông tin giám sát: Elasticsearch;
- Đẩy dữ liệu sau khi phân tích đến công cụ giám sát: Filebeat;
- Công cụ phân tích bảo mật (Decode, Rule Matching): Wazuh Server;
- Phản ứng sự cố: Scripts, mã lệnh bằng C/C++ hoặc Python.

2.2.5. Triển khai khung giám sát và phản ứng sự cố an ninh tự động



Hình 4. *Mô hình triển khai tại PTIT.HCM*

Chúng tôi triển khai các kịch bản thực tế nhằm kiểm thử khả năng giám sát và phản ứng tự động sự cố an ninh tại Học viện Công nghệ Bưu chính Viễn thông cơ sở Thành phố Hồ Chí Minh (PTIT.HCM). Phần tiếp theo, chúng tôi sẽ trình bày 3 trong số 6 kịch bản đã thử nghiệm, gồm:

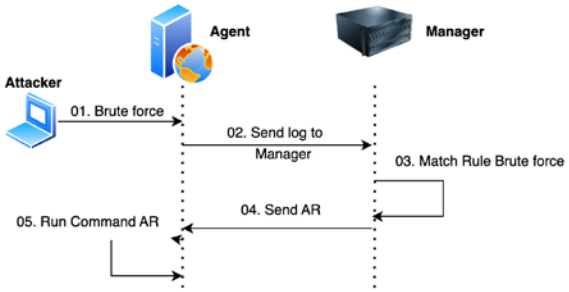
- Phát hiện và chặn IP tấn công Brute force;
- Phát hiện và loại bỏ mã độc;
- Cô lập server bị tấn công.

Các thông tin cấu hình về 3 kịch bản chúng tôi cũng đã đưa lên Github tại (Thanh, 2024). Mô hình hệ thống triển khai đánh giá khung giám sát và phản ứng sự cố an ninh như hình 4. Hệ thống bao gồm 1 Manager và 3 Agents. Manager đảm nhiệm việc thu thập log từ các Agent, dùng các công cụ phân tích log tự động, phát hiện các sự kiện khớp với các luật được định nghĩa, từ đó tạo ra các cảnh báo, email cảnh báo tới người quản trị, đồng thời dựa trên các script và các command tương ứng để phản ứng lại với các sự cố an ninh. Các Agent làm nhiệm vụ thu thập sự kiện và gửi về Manager, đồng thời nó cũng thực thi các yêu cầu được điều khiển từ Manager để ngăn chặn các tấn công cụ thể.

- Manager có chức năng quản lí việc thu thập và phân tích dữ liệu từ Agents;
- Elasticsearch thực hiện chức năng đánh chỉ mục và tìm kiếm;
- Filebeat có nhiệm vụ chuyển tiếp an toàn các cảnh báo và sự kiện đã lưu trữ đến Elasticsearch;
- Agents được triển khai trên hệ điều hành Linux và Windows;

Thực tiễn 1: Phát hiện và chặn IP tấn công Brute force

Mô hình triển khai cho kịch bản 1 như Hình 5.



Hình 5. *Kịch bản Phát hiện và chặn IP tấn công Bruteforce*

Cấu hình trên Manager:

Thông tin cấu hình command và phản hồi tự động chúng tôi đăng tải trên github (Thanh, 2024) tại đường dẫn /Scenario-1/ossec.conf

Cấu hình trên Agent:

Chúng tôi viết một script thực thi firewall-drop-cyber.sh, mã này được đăng tải trên github (Thanh, 2024) tại đường dẫn /Scenario-1/firewall-drop-cyber.sh

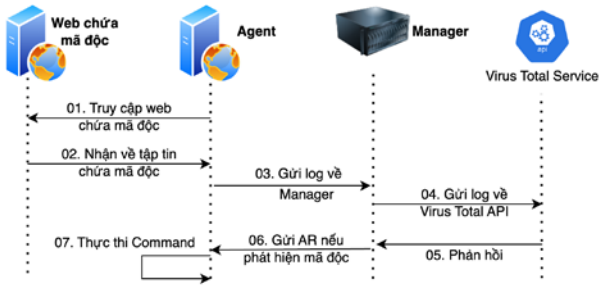
Kết quả thử nghiệm:

Chúng tôi mô phỏng một cuộc tấn công SSH, cuộc tấn công sẽ được thực hiện bằng cách cố gắng kết nối với Agent bằng SSH nhiều lần bằng các người dùng không hợp lệ. Sau một số lần truy cập, chức năng phản ứng chặn IP sẽ được kích hoạt. Khi đó, những nổ lực kết nối Agent từ kẻ tấn công đều bị AR (Active Response) phát hiện và ngăn chặn như minh họa ngay bên dưới.

G:\>ssh root@"địa chỉ IP đã được che vì lí do bảo mật"
root@IP's password:
Permission denied, please try again.
----------(đã lược bỏ bớt)
root@IP's password:
root@IP: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
……
G:\>ssh root@"địa chỉ IP đã được che vì lí do bảo mật"
ssh: connect to host IP port 22: Connection timed out

Thực tiễn 2: Phát hiện và loại bỏ mã độc

Mô hình triển khai cho kịch bản 2 như Hình 6.



Hình 6. *Kịch bản Phát hiện và loại bỏ mã độc*

VirusTotal là một cổng thông tin trực tuyến do Google cung cấp, sử dụng nhiều công cụ để kiểm tra vi-rút và phần mềm độc hại. Nó cung cấp dịch vụ API mà AIMRF sử dụng để quét các tệp băm, tên miền, địa chỉ IP hoặc URL. Để tích hợp, chúng tôi sử dụng thành phần wazuh-integration chạy trên trình quản lí Wazuh.

Định cấu hình Manager:

Trong kịch bản này, chúng tôi giám sát thử nghiệm một thư mục trong thời gian thực và thực hiện quét VirusTotal đối với mọi tệp mới hoặc tệp được sửa đổi. Nếu một tệp được phân loại là độc hại, AR tương ứng sẽ được kích hoạt và tệp sẽ bị xóa ngay. Để thực hiện việc tích hợp, chúng tôi thêm cấu hình sau vào /var/ossec/etc/ossec.conf như sau:

```
<intergration>
    <name>virustotal</name>
    <api_kay> "key đã được ẩn đi vì lí do bảo mật"</api_key>
    <rule_id>100200, 100201</rule_id>#tập luật kiểm tra
    <alert_format>json</ alert_format >
</intergration>
```

Các quy tắc tùy chỉnh để giám sát thư mục /root được tùy chỉnh trong tệp /var/ossec/etc/rules/local_rules.xml.

Cấu hình phản hồi tự động AR để loại bỏ các tập tin độc hại. Sau khi VirusTotal xác định tệp là mối đe dọa, Manager sẽ kích hoạt AR để xóa tệp khỏi hệ thống. Định cấu hình cho Manager trong tệp /var/ossec/etc/ossec.conf.

Phản hồi tự động được kích hoạt theo quy tắc 87105. Quy tắc này được thực thi khi VirusTotal xác định một tệp là độc hại. Khi đó, các quy tắc tùy chỉnh sau được thêm vào /var/ossec/etc/rules/local_rules.xml để thông báo kết quả thực hiện việc xóa tệp và thành

công hay có lỗi.

Định cấu hình Agent:

Thay đổi cài đặt giám sát tính toàn vẹn của tệp trong /var/ossec/etc/ossec.conf để giám sát /root trong thời gian thực.

<syscheck><directories whodata="yes">/root</directories></syscheck>

Đoạn mã thực thi phản hồi tự động được thêm vào /var/ossec/active-response/bin/remove-threat.sh cũng như các tuỳ chỉnh local_rules.xml và ossec.conf. Chúng tôi cũng đăng tải script này trên github (Thanh, 2024) tại đường dẫn /Scenario-2/remove-threat.sh, /Scenario-2/ossec.conf, và /Scenario-2/local_rules.xml

Kết quả thử nghiệm:

Thực hiện tải virus trên Agent, Manager nhận thông tin tệp độc hại từ cảnh báo do VirusTotal (87105) tạo ra, xóa tệp và ghi nhật kí phản hồi tự động. Như vậy, khi một tệp được sửa đổi trong thư mục được giám sát /root, Manager sẽ kích hoạt quá trình quét VirusTotal và tạo cảnh báo nếu bị phát hiện là độc hại.

Kịch bản 3: Cô lập server bị tấn công

Thiết lập Command và AR trên Manager:

Tạo command để thiết lập outbound-drop khi có sự cố cần bảo vệ, cô lập server. Khi rules_id 87105 được kích hoạt, AR sau sẽ được thực thi.

```
<active-response>
  <disabled>no</disabled>
  <command>outbound-drop</command> <location>defined-agent</location>
  <agent_id>014,015</agent_id>    <rules_id>87105</rules_id>
  <timeout>60</timeout>
</active-response>
```

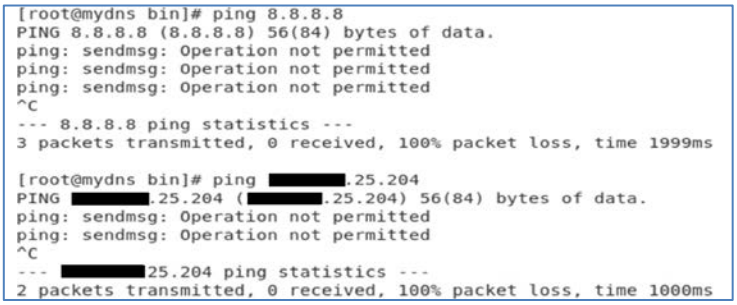
Tạo script outbound-drop.sh trên Linux Agent:

Máy chủ Agent dùng CSF (agentId=014):

```
#!/bin/sh
csf -td 0.0.0.0/0 60 -d out "block all outbound connections for 60 seconds"
csf -td 0.0.0.0/0 60 -d in "block all inbound connections for 60 seconds"
```

Kết quả thử nghiệm:

Thực hiện tải virus trên Linux Agent. Máy tấn công bị bị cô lập như Hình 7.



Hình 7. *Kết nối tới máy chủ bị cô lập từ nhiều phân vùng mạng*

Kiểm tra cấu hình khi máy chủ Agent bị cô lập, chúng ta có kết quả như Hình 8.

Hình 8. *Kiểm tra file cấu hình đã tự động cập nhật*

Bên cạnh các thực tiễn đã trình bày, chúng tôi triển khai thêm 3 kịch bản như sau:

- *Phát hiện và chặn IP lạ:* Tích hợp với AbuseIPDB để phát hiện người dùng đăng nhập từ IP lạ. Khi phát hiện IP độc hại, script sẽ chặn IP và hiển thị cảnh báo trên hệ thống SIRS Manager.
- *Phát hiện và ngăn phần mềm không mong muốn*: Thiết lập danh sách phần mềm tin cậy, tạo rule để phát hiện tiến trình không thuộc danh sách. Manager gửi lệnh để Agent thực hiện script hủy tiến trình bằng PowerShell và gửi cảnh báo.
- *Ngăn chặn truy cập tên miền độc hại*: Tích hợp với Alientvault blacklist để phát hiện domain thuộc danh sách đen. Manager điều khiển Agent thêm domain vào file hosts trên máy Windows, chuyển truy cập đến sinkhole (IP giả).

Việc triển khai hệ thống giám sát và phản ứng sự cố an ninh thông tin tự động cho các SME đã mang lại các kết quả và hiệu quả đáng kể như (1) phát hiện và phản ứng nhanh chóng, (2) tiết kiệm chi phí và tài nguyên, (3) giảm thiểu rủi ro và tổn thất, (4) cải thiện tuân thủ bảo mật, và (5) giải phóng đội ngũ nhân sự, cải thiện hiệu quả quản lí và vận hành.

3. Kết luận và hướng phát triển

Trong kỉ nguyên số hiện nay, an ninh mạng đã trở thành một mối quan tâm cấp thiết đối với các doanh nghiệp thuộc mọi quy mô. Trong khi các tập đoàn lớn thường có đủ nguồn lực để đầu tư vào các giải pháp an ninh mạng phức tạp và các đội ngũ chuyên biệt để quản lí chúng, các SME lại đối mặt với nhiều thách thức đáng kể. Nhiều giải pháp an ninh mạng hiện tại có chi phí cao và đòi hỏi trình độ chuyên môn cao để triển khai và quản lí, khiến chúng không phù hợp với các SME có ngân sách hạn chế và nhân viên ít chuyên môn. Nghiên cứu này đã đề xuất một giải pháp phát hiện và phản ứng sự cố đơn giản và hiệu quả, được thiết kế riêng cho các SME với 3 thực tiễn tốt nhất đã được triển khai cùng, đảm bảo họ có thể bảo vệ tài sản số mà không tốn kém quá nhiều chi phí.

Mặc dù, hệ thống giám sát và phản ứng sự cố an ninh thông tin tự động mang lại nhiều lợi ích cho các SME, nó cũng có một số hạn chế như (1) đòi hỏi sự thiết lập ban đầu phức tạp và quản lí liên tục để đảm bảo hiệu quả do các mối đe dọa an ninh liên tục phát triển, đòi hỏi hệ thống phải được cập nhật và bảo trì thường xuyên để đối phó với các lỗ hổng và mối đe dọa mới, (2) việc tự động hóa có thể không linh hoạt hoặc khó tùy chỉnh theo nhu cầu cụ thể của từng SME và có thể tạo ra nhiều cảnh báo giả, gây khó khăn trong việc phân loại và xử lí sự cố.

Hướng nghiên cứu tiếp theo sẽ là tích hợp các mô hình học sâu và tập luật phức tạp để nâng cao hiệu quả phát hiện và phản ứng sớm hơn nữa với các sự cố an ninh tiềm ẩn.

❖ ***Tuyên bố về quyền lợi:*** *Các tác giả xác nhận hoàn toàn không có xung đột về quyền lợi.*

❖ ***Lời cảm ơn:*** *Cảm ơn Học viện Công nghệ Bưu chính Viễn thông đã hỗ trợ chúng tôi trong quá trình thực hiện nghiên cứu này.*

TÀI LIỆU THAM KHẢO

Ashley, O., Atif, A., & Sean, M. (2021). Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training. *Australasian Conference on Information Systems, Cryptography and Security,* (pp. 1-11). Sydney. https://doi.org/10.48550/arXiv.2108.04996

Authority of Information Security. (2024). *Báo cáo an toàn thông tin mạng Việt Nam* [*Vietnam network information security report*]*(tháng 3/2024).* Ministry of Information and Communications

Avi, S., Yulia, C., Pete, B., & Peter, M. (2023). Operations-informed incident response playbooks. *Elsevier Journal of Computers & Security, 134*(C). https://doi.org/10.1016/j.cose.2023.103454

Dun, Y., Razak, M., Mohamad, F., Tan, F., & Ahmad, F. (2022). Hermes Ransomware v2.1 Action Monitoring using Next Generation Security Operation Center (NGSOC) Complex Correlation Rules. *International Journal on Advanced Science, Engineering and Information Technology, 12*(3), 1287-1292. https://doi.org/10.18517/ijaseit.12.3.15329

Huynh, T. T, Nguyen, H. T. Thua, H., & Thanh, N. (2020). Nâng cao hiệu quả phát hiện xâm nhập mạng bằng huấn luyện DSD [Enhancing network intrusion detection efficiency using DSD]. *Journal of Science and Technology of Information and Communication, 03*(CS.01), 54-61.

IBM. (2024, Sep 13). *IBM QRadar SIEM*. Retrieved from https://www.ibm.com/products/qradar-siem

Islam, C., Babar, M., Croft, R., & Janicke, H. (2022, June). SmartValidator: A framework for automatic identification and classification of cyber threat data. *Journal of Network and Computer Applications, 202*, 1-24. https://doi.org/10.1016/j.jnca.2022.103370

Le, Q. M., Doan, H. H., Nguyen, N. T., Cu, K. L., & Nguyen, M. P. (2017, June). An Assessment Model for Cyber Security of Vietnamese Organization. *VNU Journal of Science: Policy and Management Studies, 33*(2), 97-103. https://doi.org/10.25073/2588-1116/vnupam.4102

Nguyen, T. P. T., Le, T. H.., Hoang, V, T., & Dinh, T. N. H (2022). Cyber Attacks and Security System Design Solutions in Emerging Markets and Vietnam. *Ambient Communications and Computer Systems* (pp. 521-528). Singapore: Springer. https://doi.org/10.1007/978-981-16-7952-0_49

OpenText. (2024, Sep 13). *ArcSight Enterprise Security Manager*. https://www.opentext.com/products/arcsight-enterprise-security-manager

Rajesh, P., Alam, M., Tahernezhadi, T., Monika, A., & Chanakya, G. (2022). Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework. *International Conference on Intelligent Data Science Technologies and Applications*, (pp. 4-12). San Antonio, Texas, USA. https://doi.org/10.1109/IDSTA55301.2022.9923170

Splunk. (2024, Sep 12). *Splunk Enterprise Security*. https://www.splunk.com/en_us/products/enterprise-security.html

Thanh, N. (2024, July 12). *GitHub*. Retrieved from https://github.com/hthanhsg/automatic-security-incident-response-and-monitoring-framework/

Tanwir, A., & Dragos, T. (2023). Efficient Early Anomaly Detection of Network Security Attacks Using Deep Learning. *IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 154-159). Venice, Italy: IEEE. https://doi.org/10.1109/csr57506.2023.10224923

Trellix. (2024, Sep 13). *XDR Platform*. Retrieved from https://www.trellix.com/platform/

Verizon. (2024). *Data Breach Investigations Report (DBIR) 2024.* California : Verizon Business.

Wang, J., Yan, T., An, D., Liang, Z., Guo, C., Hu, H., Qi, F. (2021). A comprehensive security operation center based on big data analytics and threat intelligence PoS. *International Symposium on Grids & Clouds* (pp. 1-12). Taipei, Taiwan: Proceedings of Science. https://doi.org/10.22323/1.378.0028

William, V. C., Ivan, O. G., & Santiago, S. V. (2021). Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *MDPI Journal on Computers*, *10*(8), 1-23. https://doi.org/10.3390/computers10080102

Zafar, I., & Zahid, A. (2020). SCERM - A novel framework for automated management of cyber threat response activities. *Future Generation Computer Systems, Elsevier Journal*, 687–708. https://doi.org/10.1016/j.future.2020.03.030

AUTOMATIC INCIDENT MONITORING AND RESPONSE FRAMEWORK: BEST PRACTICES FOR SMALL AND MEDIUM-SIZED ENTERPRISES

Nguyen Hoang Thanh*, Huynh Trong Thua

Posts and Telecommunications Institute of Technology, Vietnam

Corresponding author: Nguyen Hoang Thanh – Email: thanhnh@ptit.edu.vn

Received: June 17; Revised: September 13, 2024; Accepted: September 16, 2024

ABSTRACT

In today's digital landscape, small and medium-sized enterprises (SMEs) often rely on limited internal resources or external assistance for incident response. While larger corporations often adhere to standards such as ISO 2700x, SMEs face unique challenges in adapting to rapidly evolving cyber threats. Automated incident monitoring and response systems have become essential for protecting sensitive information, maintaining business continuity, and ensuring regulatory compliance. However, most existing security monitoring and incident handling platforms are costly, insufficiently automated, and require highly skilled personnel, making them impractical for SMEs. This research proposes a framework that addresses these challenges by integrating log data from existing monitoring systems with modern, automated incident response techniques. Designed to be cost-effective and user-friendly, the proposed solution enables SMEs to develop and implement an automated monitoring and response system without extensive resources or expertise. By offering a practical, accessible approach to cybersecurity, this framework aims to enhance SMEs' ability to defend their information systems, fostering a proactive and self-sufficient information security posture.

Keywords: automation; detection; incident response; monitoring; SME; threat