

**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**



**ĐỒ ÁN  
HỆ THỐNG TÌM KIẾM, PHÁT HIỆN VÀ  
NGĂN NGỪA XÂM NHẬP  
-&-**

**ĐỀ TÀI: TÌM HIỂU GIẢI PHÁP IDS THƯƠNG MẠI  
SECURITY ONION**

Giảng viên hướng dẫn: **Đỗ Thị Phương Uyên**

Thực hiện bởi Nhóm 12, gồm:

- |                                |                 |                    |
|--------------------------------|-----------------|--------------------|
| • <b>LẠI QUAN THIÊN</b>        | <b>22521385</b> | <b>Trưởng nhóm</b> |
| • <b>MAI NGUYỄN NAM PHƯƠNG</b> | <b>22521164</b> | <b>Thành viên</b>  |
| • <b>HỒ DIỆP HUY</b>           | <b>22520541</b> | <b>Thành viên</b>  |
| • <b>TRẦN THÉ HỮU PHÚC</b>     | <b>22521143</b> | <b>Thành viên</b>  |

Lớp: **NT204.P21.ANTT**

*TP. Hồ Chí Minh, tháng 02 năm 2025*



## MỤC LỤC

<b>CHƯƠNG 1. GIỚI THIỆU TỔNG QUAN VỀ SECURITY ONION .....</b>	<b>1</b>
<b>1.1. Định nghĩa và mục đích .....</b>	<b>1</b>
<b>1.2. Tại sao Security Onion được sử dụng trong an ninh mạng? .....</b>	<b>1</b>
<b>CHƯƠNG 2. KIẾN TRÚC VÀ THÀNH PHẦN CỦA SECURITY ONION .....</b>	<b>3</b>
<b>2.1. Kiến trúc tổng thể.....</b>	<b>3</b>
<b>2.2. Các thành phần chính.....</b>	<b>5</b>
2.2.1. Thu thập dữ liệu và giám sát mạng .....	5
2.2.2. Xử lý, lưu trữ và trực quan hóa dữ liệu.....	5
2.2.3. Quản lý sự cố và hỗ trợ điều tra .....	5
2.2.4. Hạ tầng Server ( Trung tâm xử lý ) .....	6
<b>2.3. Vai trò và tương tác giữa các thành phần .....</b>	<b>6</b>
<b>CHƯƠNG 3. TÍNH NĂNG NỐI BẬT .....</b>	<b>7</b>
<b>3.1. Giám sát an ninh mạng (Network Security Monitoring - NSM) .....</b>	<b>7</b>
<b>3.2. Phân tích lưu lượng mạng (Packet Capture và Analysis).....</b>	<b>7</b>
<b>3.3. Phát hiện xâm nhập (Intrusion Detection).....</b>	<b>7</b>
<b>3.4. Quản lý log tập trung (Centralized Log Management) .....</b>	<b>7</b>
<b>3.5. Phát hiện, phản ứng và phân tích với các mối đe dọa an ninh mạng .....</b>	<b>8</b>
<b>CHƯƠNG 4. MÔ HÌNH VÀ KỊCH BẢN TRIỂN KHAI.....</b>	<b>9</b>
<b>4.1. Kịch Bản 1: Standalone Mode với Dual NIC (Quản Lý &amp; Giám Sát Riêng Biệt) 9</b>	<b>9</b>
4.1.1. Mục tiêu.....	9
4.1.2. Ngữ cảnh và Mô hình triển khai.....	9
4.1.3. Quy trình triển khai .....	11
4.1.4. Kết quả và đánh giá .....	14
<b>4.2. Kịch bản 2: Tích hợp Security Onion với Firewall (pfSense) .....</b>	<b>20</b>
4.2.1. Mục tiêu.....	20
4.2.2. Ngữ cảnh và Mô hình triển khai.....	20

4.2.3. Quy trình triển khai .....	22
4.2.4. Kết quả và đánh giá .....	30
<b>4.3. Kịch Bản 3: Triển khai Mô hình Mạng Nội Bộ Với Security Onion .....</b>	<b>33</b>
4.3.1. Mục tiêu.....	33
4.3.2. Ngữ cảnh và Mô hình triển khai.....	33
4.3.3. Quy trình triển khai .....	36
4.3.4. Kết quả và đánh giá .....	36
<b>CHƯƠNG 5. TÌM HIỂU CÁC GIẢI PHÁP LIÊN QUAN TRONG HỆ SINH THÁI CỦA SECURITY ONION .....</b>	<b>44</b>
<b>5.1. Giải pháp 1: Triển Khai Security Onion Trên Cloud (Cloud-Native SIEM) .....</b>	<b>44</b>
5.1.1. Mục tiêu.....	44
5.1.2. Ngữ cảnh và Mô hình triển khai.....	44
5.1.3. Quy trình triển khai .....	46
5.1.4. Kết quả và đánh giá .....	50
<b>5.2. Giải pháp 2: Threat Hunting với Security Onion &amp; Threat Intelligence.....</b>	<b>51</b>
5.2.1. Mục tiêu.....	51
5.2.2. Ngữ cảnh và Mô hình triển khai.....	51
5.2.3. Quy trình triển khai .....	52
5.2.4. Kết quả và đánh giá .....	55
<b>CHƯƠNG 6. ĐÁNH GIÁ CHUNG .....</b>	<b>56</b>
<b>6.1. Ưu điểm nổi bật của Security Onion .....</b>	<b>56</b>
6.1.1. Tích hợp toàn diện các công cụ an ninh mạng .....	56
6.1.2. Chi phí thấp .....	56
6.1.3. Khả năng mở rộng linh hoạt.....	56
6.1.4. Giao diện trực quan và khả năng phân tích mạnh mẽ .....	56
6.1.5. Cộng đồng hỗ trợ mạnh mẽ và tài liệu phong phú .....	56
<b>6.2. Các hạn chế và thách thức.....</b>	<b>57</b>
6.2.1. Độ phức tạp trong triển khai và quản lý.....	57
6.1.2. Yêu cầu tài nguyên hệ thống cao.....	57
6.1.3. Khó khăn trong việc scale hệ thống .....	57

6.1.4. Khả năng tùy chỉnh hạn chế .....	57
6.1.5. Cảnh báo nhiễu (False Positives) .....	57
<b>CHƯƠNG 7. KẾT LUẬN.....</b>	<b>58</b>
<b>7.1. Tóm tắt giá trị của Security Onion .....</b>	<b>58</b>
<b>7.2. Triển vọng ứng dụng trong tương lai .....</b>	<b>58</b>
<b>7.3. Kết luận chung.....</b>	<b>58</b>
<b>DANH MỤC TÀI LIỆU THAM KHẢO .....</b>	<b>59</b>

## **CHƯƠNG 1. GIỚI THIỆU TỔNG QUAN VỀ SECURITY ONION**

### **1.1. Định nghĩa và mục đích**

Security Onion là một bản phân phối Linux mã nguồn mở chuyên dụng cho việc giám sát an ninh mạng (Network Security Monitoring - NSM), phát hiện xâm nhập (Intrusion Detection) và phản ứng sự cố (Incident Response). Nó cung cấp các công cụ mạnh mẽ để giúp các tổ chức phát hiện, điều tra và khắc phục các mối đe dọa an ninh mạng một cách hiệu quả.

Security Onion được phát triển dựa trên việc tích hợp nhiều công cụ bảo mật phổ biến như Suricata, Zeek (trước đây là Bro), Elasticsearch, Logstash, Kibana (ELK Stack), Wazuh, CyberChef và nhiều công cụ khác, giúp cung cấp khả năng giám sát và phân tích bảo mật một cách toàn diện.

Mục đích chính của Security Onion bao gồm:

- Giám sát lưu lượng mạng để phát hiện các hoạt động đáng ngờ.
- Phát hiện tấn công mạng thông qua hệ thống phát hiện xâm nhập (IDS).
- Phân tích log và lưu lượng mạng để điều tra sự cố bảo mật.
- Hỗ trợ phản ứng sự cố thông qua giao diện tập trung.

### **1.2. Tại sao Security Onion được sử dụng trong an ninh mạng?**

#### **1.2.1. Nền tảng mã nguồn mở và miễn phí**

Security Onion là một dự án mã nguồn mở, có thể được sử dụng miễn phí và cộng đồng có thể đóng góp vào sự phát triển của hệ thống. Điều này giúp các tổ chức tiết kiệm chi phí mà vẫn có thể triển khai một hệ thống giám sát mạng mạnh mẽ.

#### **1.2.2. Tích hợp nhiều công cụ bảo mật mạnh mẽ**

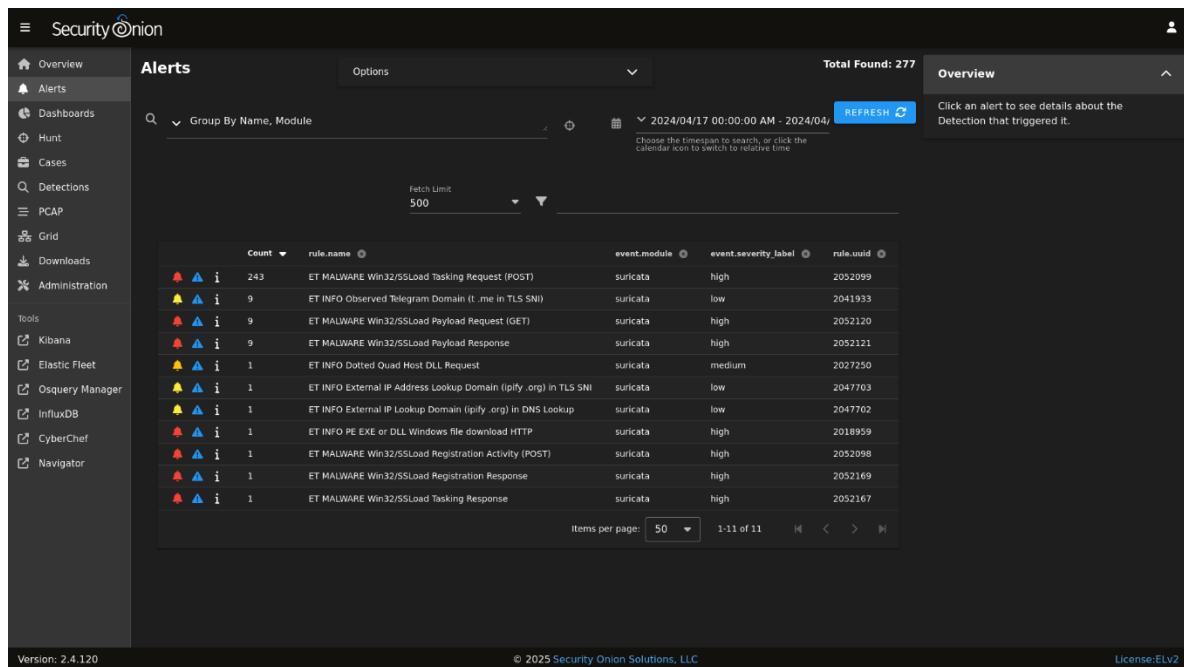
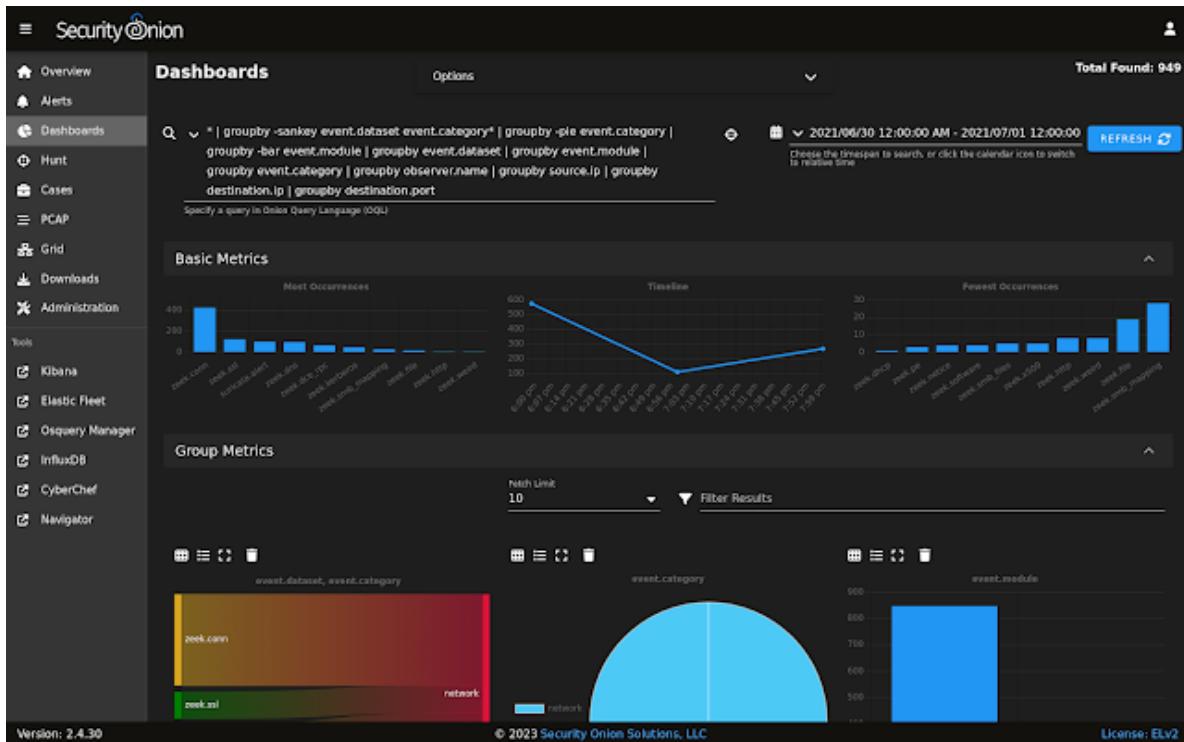
Security Onion không chỉ là một hệ thống đơn lẻ mà là một tập hợp các công cụ bảo mật phổ biến, giúp người dùng có đầy đủ các tính năng để giám sát, phát hiện và điều tra sự cố an ninh mạng.

#### **1.2.3. Khả năng triển khai linh hoạt**

Security Onion có thể được triển khai theo nhiều mô hình khác nhau, từ một hệ thống nhỏ chạy trên một máy đơn lẻ (Standalone) đến hệ thống giám sát mạng lớn với nhiều cảm biến (Distributed Deployment).

## 1.2.4. Giao diện trực quan, dễ sử dụng

Giao diện Security Onion Console (SOC) giúp quản trị viên mạng dễ dàng xem xét dữ liệu giám sát, điều tra các sự cố bảo mật và phản ứng nhanh chóng với các mối đe dọa.



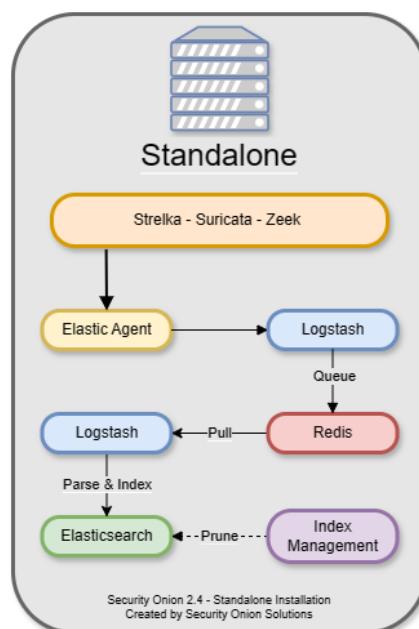
## CHƯƠNG 2. KIẾN TRÚC VÀ THÀNH PHẦN CỦA SECURITY ONION

### 2.1. Kiến trúc tổng thể

Security Onion có thể được triển khai theo bốn kiến trúc chính:

- **Standalone:** Tất cả các thành phần của hệ thống được cài đặt và chạy trên một máy duy nhất. Kiến trúc này phù hợp cho môi trường nhỏ hoặc mục đích đánh giá

- + **Cảm biến (Sensor):** Thu thập và phân tích lưu lượng mạng
- + **Máy chủ (Server):** Xử lý, lưu trữ, và hiển thị dữ liệu
- + **Giao diện quản lý:** Cung cấp công cụ để giám sát và phân tích
- + **Ưu điểm:** Đơn giản và dễ triển khai, Có chi phí thấp, Dễ bảo trì
- + **Nhược điểm:** Hạn chế về khả năng mở rộng và có rủi ro cao về hiệu suất



- **Distributed:** Các thành phần của hệ thống được phân chia trên nhiều máy khác nhau để tăng khả năng mở rộng và hiệu suất. Ví dụ, các cảm biến (sensors) có thể được triển khai trên nhiều máy để giám sát lưu lượng mạng, trong khi máy chủ chính quản lý và phân tích dữ liệu

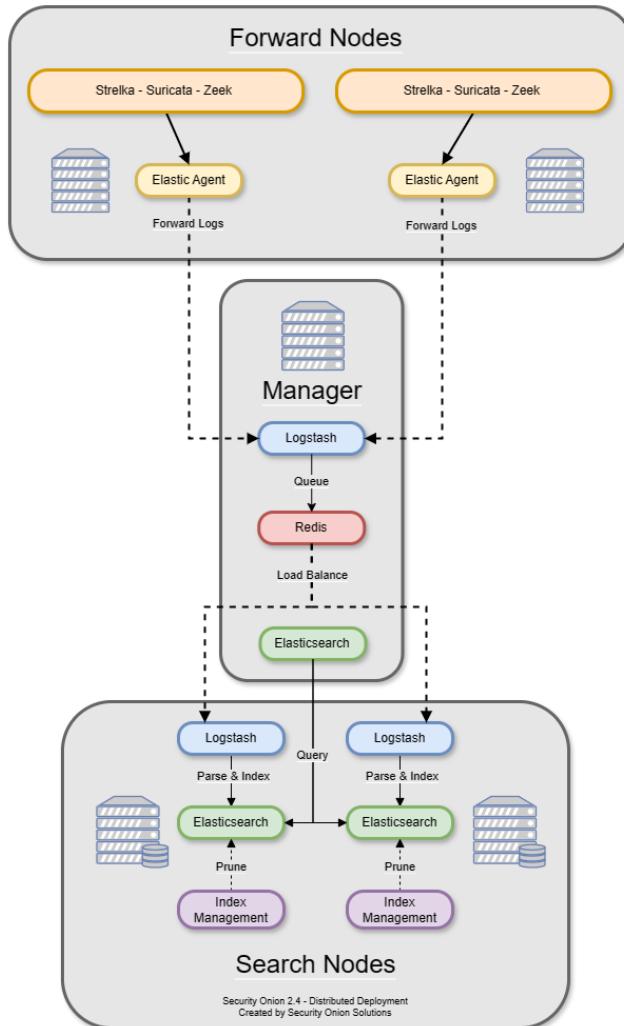
+ **Cảm biến (Sensor):** Được triển khai trên các máy riêng biệt, đặt tại các vị trí chiến lược trong mạng (ví dụ: trước firewall, giữa các VLAN)

+ **Máy chủ (Server):** Xử lý và lưu trữ dữ liệu từ các cảm biến, thường được đặt trong mạng nội bộ

+ **Giao diện quản lý:** Cung cấp công cụ để quản trị viên giám sát và phân tích dữ liệu từ xa

+ **Ưu điểm:** Có khả năng mở rộng cao, Giúp tăng cường hiệu suất, Tính linh hoạt cao

+ Nhược điểm: Phức tạp trong việc triển khai, Chi phí cao, Khó bảo trì



- **Hybrid:** Là hệ thống được kết hợp giữa Standalone và Distributed, tức một số thành phần được triển khai trên một máy chủ, trong khi các thành phần khác được phân tán

+ Ví dụ: Cảm biến được triển khai riêng biệt, trong khi máy chủ và giao diện quản lý chạy trên một máy duy nhất

+ Ưu điểm: Cân bằng giữa hiệu suất và chi phí

- **Evaluation Mode:** là một chế độ cài đặt được thiết kế chủ yếu cho mục đích thử nghiệm, đánh giá và môi trường phòng thí nghiệm, các thành phần được cài đặt với cấu hình mặc định trên một máy duy nhất (hoặc VM), được thiết kế cho mục đích thử nghiệm, đánh giá và học tập

+ **Dịch vụ giám sát (IDS/IPS):** Các công cụ như Snort, Bro (Zeek), netsniffng, pcap\_agent, snort\_agent, barnyard2 và ELSA được kích hoạt mặc định để thu thập và phân tích lưu lượng mạng

+ **Cấu hình sẵn:** Thiết lập mặc định giúp cài đặt nhanh chóng và giảm bớt yêu cầu cấu hình phức tạp cho người dùng mới

+ **Giao diện quản lý:** Tích hợp truy cập đến các công cụ như Kibana, Squert và Sguil, cho phép giám sát và phân tích dữ liệu một cách trực quan

+ **Ưu điểm:** Dễ cài đặt và triển khai nhanh chóng; chi phí thấp; phù hợp cho môi trường phòng lab, lớp học hoặc thử nghiệm ban đầu

+ **Nhược điểm:** Không tối ưu cho môi trường sản xuất; khả năng mở rộng hạn chế; hiệu năng có thể bị giới hạn khi xử lý lưu lượng mạng lớn

## 2.2. Các thành phần chính

### 2.2.1. Thu thập dữ liệu và giám sát mạng

**Sensor:** Thành phần này chịu trách nhiệm thu thập dữ liệu mạng và hệ thống, bao gồm lưu lượng mạng, nhật ký hệ thống và các sự kiện bảo mật khác

**Suricata:** Là công cụ phát hiện xâm nhập mạng và ngăn chặn xâm nhập mạng mạnh mẽ. Giúp phân tích lưu lượng mạng và phát hiện các cuộc tấn công mạng mạnh mẽ như malware, **tấn công DDoS**,...

**Zeek (Bro):** Đây là một nền tảng mã nguồn mở giúp quản lý bảo mật mạng, nó chủ yếu tập trung vào việc giám sát và phân tích hành vi mạng để phát hiện bất thường, cung cấp dữ liệu chi tiết về giao thức mạng

### 2.2.2. Xử lý, lưu trữ và trực quan hóa dữ liệu

**Logstash:** Xử lý và chuẩn hóa dữ liệu trước khi đưa vào Elasticsearch, thực hiện các tác vụ như phân tách (parsing), định dạng lại và làm giàu dữ liệu (enrichment), giúp dữ liệu trở nên đồng nhất và dễ dàng tìm kiếm

**Elasticsearch:** Công cụ này cho phép lưu trữ, tìm kiếm và phân tích dữ liệu nhật ký nhanh chóng từ các công cụ khác như Zeek và Suricata, hỗ trợ tìm kiếm và phân tích các sự kiện an ninh

**Kibana:** Giao diện trực quan hóa dữ liệu từ Elasticsearch, cho phép tạo biểu đồ và báo cáo dựa trên nhật ký, hỗ trợ phân tích các mối đe dọa và hoạt động đáng ngờ

### 2.2.3. Quản lý sự cố và hỗ trợ điều tra

**CyberChef:** Là một công cụ tích hợp mạnh mẽ để thực hiện các phép biến đổi, giải mã, mã hóa và xử lý dữ liệu trong quá trình điều tra, hữu ích cho việc phân tích dữ liệu dạng thô

#### **2.2.4. Hạ tầng Server (Trung tâm xử lý)**

**Server:** Xử lý dữ liệu (Elasticsearch), hiển thị bảng điều khiển (Kibana), và quản lý cảnh báo (Wazuh)

### **2.3. Vai trò và tương tác giữa các thành phần**

**Thu thập dữ liệu:** Zeek và Suricata giám sát lưu lượng mạng, thu thập dữ liệu và phát hiện các hoạt động bất thường hoặc mối đe dọa.

**Lưu trữ và tìm kiếm:** Dữ liệu từ Zeek và Suricata được gửi đến Elasticsearch để lưu trữ và cho phép truy vấn nhanh chóng.

**Trực quan hóa và phân tích:** Kibana truy cập dữ liệu trong Elasticsearch, cung cấp giao diện để tạo biểu đồ, báo cáo và phân tích các mối đe dọa.

**Xử lý và phân tích dữ liệu:** CyberChef hỗ trợ xử lý và phân tích dữ liệu thô, giúp giải mã và chuyển đổi dữ liệu trong quá trình điều tra.

**Quản lý sự cố:** Security Onion nhận thông tin từ các thành phần khác, giúp nhóm an ninh quản lý, theo dõi và điều tra các sự kiện an ninh một cách hiệu quả thông qua giao diện Hunt/Detections.

## CHƯƠNG 3. TÍNH NĂNG NỘI BẬT

### 3.1. Giám sát an ninh mạng (Network Security Monitoring - NSM)

Security Onion có khả năng ghi lại toàn bộ lưu lượng mạng, giúp phân tích và điều tra khi cần thiết. Hệ thống sử dụng các công cụ bảo mật như:

- Zeek (trước đây là Bro): Phân tích lưu lượng mạng ở cấp độ cao, trích xuất thông tin chi tiết về các giao thức, kết nối và hành vi mạng.

- Suricata: Hệ thống phát hiện xâm nhập (IDS/IPS) giúp nhận diện các mối đe dọa dựa trên chũ ký tấn công và hành vi bất thường.

Bằng cách ghi lại và phân tích lưu lượng, Security Onion giúp các chuyên gia bảo mật phát hiện các dấu hiệu tấn công và hành vi đáng ngờ trong hệ thống.

### 3.2. Phân tích lưu lượng mạng (Packet Capture và Analysis)

Security Onion hỗ trợ lưu trữ và phân tích gói tin mạng nhằm phục vụ điều tra khi xảy ra sự cố bảo mật. Công cụ Stenographer giúp lưu trữ toàn bộ lưu lượng mạng, cho phép nhóm bảo mật tái hiện lại các sự kiện và kiểm tra chi tiết từng gói tin.

Ngoài ra, Security Onion cũng tích hợp với Wireshark và NetworkMiner, giúp phân tích sâu các gói tin để xác định nguồn gốc của cuộc tấn công.

### 3.3. Phát hiện xâm nhập (Intrusion Detection)

Security Onion tích hợp các công cụ mạnh mẽ để phát hiện xâm nhập và đưa ra cảnh báo khi phát hiện dấu hiệu tấn công mạng, cụ thể:

- Suricata và Zeek: Nhận diện các mẫu tấn công phổ biến như tấn công DDoS, brute-force, khai thác lỗ hổng

- Sigma Rules: Hệ thống quy tắc phát hiện mối đe dọa dựa trên các mẫu nhật ký và sự kiện đáng ngờ.

- Hệ thống cảnh báo tự động: Khi phát hiện sự cố, Security Onion sẽ gửi cảnh báo tới đội ngũ bảo mật để xử lý kịp thời.

### 3.4. Quản lý log tập trung (Centralized Log Management)

Security Onion thu thập và phân tích nhật ký từ hệ thống, ứng dụng và thiết bị mạng thông qua các công cụ:

- Logstash: Thu thập và xử lý nhật ký từ nhiều nguồn khác nhau.

- Elasticsearch: Cơ sở dữ liệu mạnh mẽ giúp lưu trữ và tìm kiếm log hiệu quả.

- Kibana: Cung cấp giao diện trực quan hóa dữ liệu, giúp phát hiện những điểm bất thường trong hệ thống.

Nhờ khả năng quản lý log tập trung, Security Onion giúp phát hiện các hành vi bất thường trong hệ thống nhanh chóng và chính xác.

### **3.5. Phát hiện, phản ứng và phân tích với các mối đe dọa an ninh mạng**

Security Onion không chỉ giúp phát hiện mối đe dọa mà còn hỗ trợ xử lý, phân tích sự cố nhanh chóng, nhờ vào công cụ tích hợp như:

- Kibana và Elasticsearch: Giúp truy vết, lọc và phân tích log để xác định nguyên nhân của sự cố an ninh.

- CyberChef: Công cụ hỗ trợ giải mã, phân tích và xử lý dữ liệu trong quá trình điều tra.

- Stenographer: Lưu full-packet capture (PCAP) để truy vết, phân tích hậu kỳ nghiêm ngặt

- Playbook: Hỗ trợ tự động hóa phản ứng với các sự cố để giảm thời gian xử lý.

- Elastic Agent + osquery + Elastic Fleet: Thu thập dữ liệu host-level (system logs, file integrity, live query), bổ sung góc nhìn endpoint

- SOC Cases (SOC interface): Quản lý và phối hợp xử lý sự cố nội bộ.

- CapMe: Hỗ trợ phân tích phiên kết nối mạng, giúp tái hiện lại toàn bộ quá trình tấn công.

- OSQuery: Công cụ giám sát hoạt động của hệ điều hành, giúp phát hiện những thay đổi đáng ngờ trong hệ thống.

## CHƯƠNG 4. MÔ HÌNH VÀ KỊCH BẢN TRIỂN KHAI

### 4.1. Kịch Bản 1: Standalone Mode với Dual NIC (Quản Lý & Giám Sát Riêng Biệt)

Xem Video Demo tại: <https://youtu.be/bWiu8lMXAZk?si=wuvnwz9h18eOClas>

#### 4.1.1. Mục tiêu

Kịch bản này được chọn để triển khai Security Onion ở chế độ Standalone với hai card mạng (NIC) riêng biệt: một cho quản lý và một cho giám sát. Việc tách biệt traffic quản lý và traffic giám sát giúp tăng cường bảo mật và hiệu suất. Trong thực tế, cấu hình này đảm bảo hoạt động quản lý không làm gián đoạn quá trình giám sát và ngược lại, phù hợp cho các hệ thống cần tính ổn định cao.

Đồng thời mục tiêu chính của kịch bản này là để giới thiệu chi tiết cho mọi người những tiện ích trong SideBar của SOC, với mỗi tiện ích sẽ có một nhiệm vụ và vai trò khác nhau.

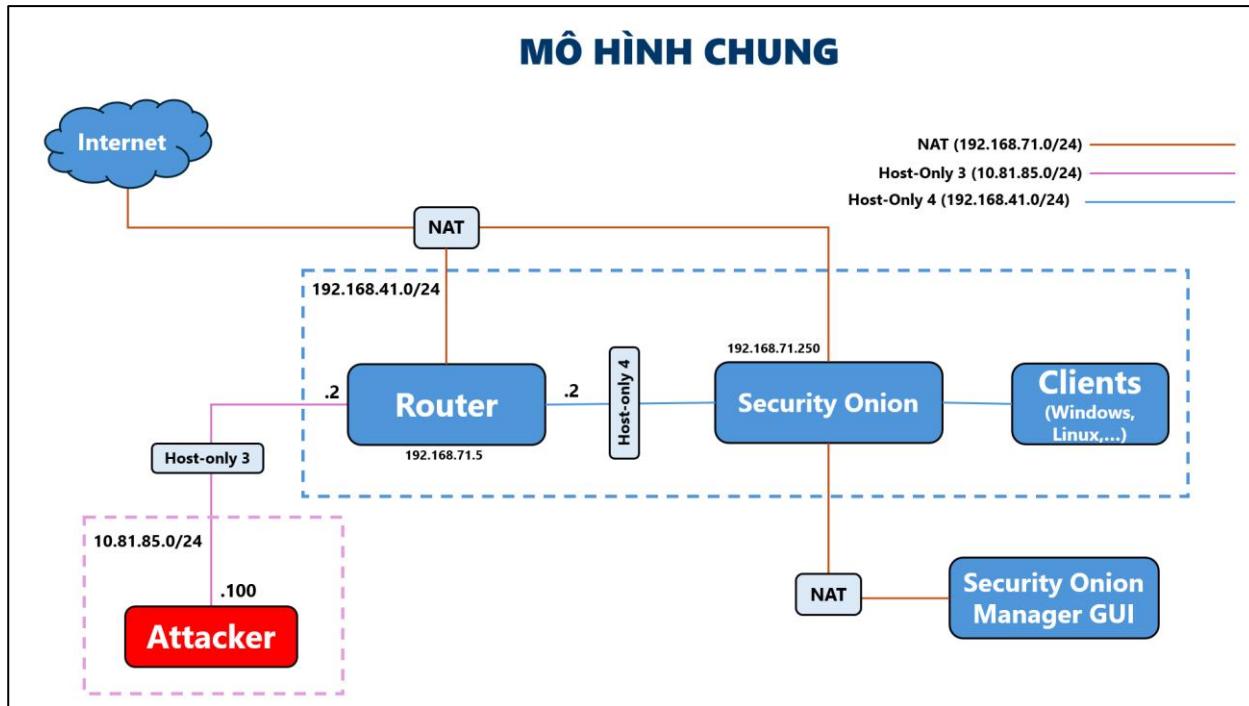
#### 4.1.2. Ngữ cảnh và Mô hình triển khai

##### 4.1.2.1. Ngữ cảnh

Security Onion được triển khai như một máy chủ độc lập (chế độ Standalone) với hai giao diện mạng:

- NIC Quản Lý (Management NIC): Dùng để truy cập giao diện web, cấu hình và quản lý hệ thống.
- NIC Giám Sát (Monitoring NIC): Dùng để thu thập và phân tích traffic mạng từ các thiết bị trong mạng nội bộ.

#### 4.1.2.2. Mô hình triển khai



Mô hình này là một triển khai cơ bản của Security Onion để giám sát traffic trong mạng nội bộ, nhưng thay vì tích hợp với các phương pháp khác, kịch bản 4.1 tập trung vào cấu hình Standalone với Dual NIC để tách biệt chức năng và làm tiền đề cho các kịch bản khác.

#### 4.1.2.3. Mô tả các thành phần

STT	Thành Phần	Mô Tả
1	<b>Internet</b>	<ul style="list-style-type: none"> <li>- Được mô phỏng bằng NAT network của VMware.</li> <li>- Cung cấp kết nối ra ngoài cho pfSense, Security Onion Manager GUI, và có thể cho các client cần update/cập nhật.</li> </ul>
2	<b>Router</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 2 GB RAM; 128GB SSD.</li> <li>- <b>Interface LAN (Host-Only 4: 192.168.41.0/24)</b>: địa chỉ 192.168.41.2.</li> <li>- <b>Interface OPT1 (Host-Only 4: 192.168.71.0/24)</b>: địa chỉ 192.168.71.4.</li> <li>- <b>Interface WAN (NAT: 192.168.71.0/24)</b>: địa chỉ dù 192.168.71.4, dùng để NAT ra Internet.</li> <li>- Nhiệm vụ: phân luồng (routing) giữa 192.168.41.0/24 ↔ 192.168.71.0/24 ↔ 10.81.85.0/24 ↔ Internet.</li> </ul>
3	<b>Security Onion (Standalone)</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 8 Cores vCPU; 16 GB RAM; 1000GB SSD.</li> </ul>

		<ul style="list-style-type: none"> <li>- <b>Interface giám sát (Host-Only 4):</b> 192.168.41.0/24</li> <li>- <b>Interface WAN (NAT):</b> địa chỉ NAT 192.168.71.250 để truy cập Internet, đồng thời để Security Onion Manager GUI publish ra host.</li> <li>- Cài đặt <b>all-in-one mode</b> (sensor + manager) để tự chia Suricata, Zeek, Elasticsearch, Kibana, Fleet Server (8220), v.v.</li> <li>- Ghi lại toàn bộ traffic passed-through pfSense (mirror port qua Host-Only 4) để Suricata/Zeek phân tích.</li> </ul>
4	<b>Attacker</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 4 GB RAM; 128GB SSD.</li> <li>- Nằm trên Host-Only 3 (10.81.85.0/24), địa chỉ 10.81.85.100.</li> <li>- Sử dụng Parrot, thực hiện tấn công (scan nmap, exploit, brute-force SSH, tấn công ứng dụng web) vào Clients.</li> </ul>

#### 4.1.3. Quy trình triển khai

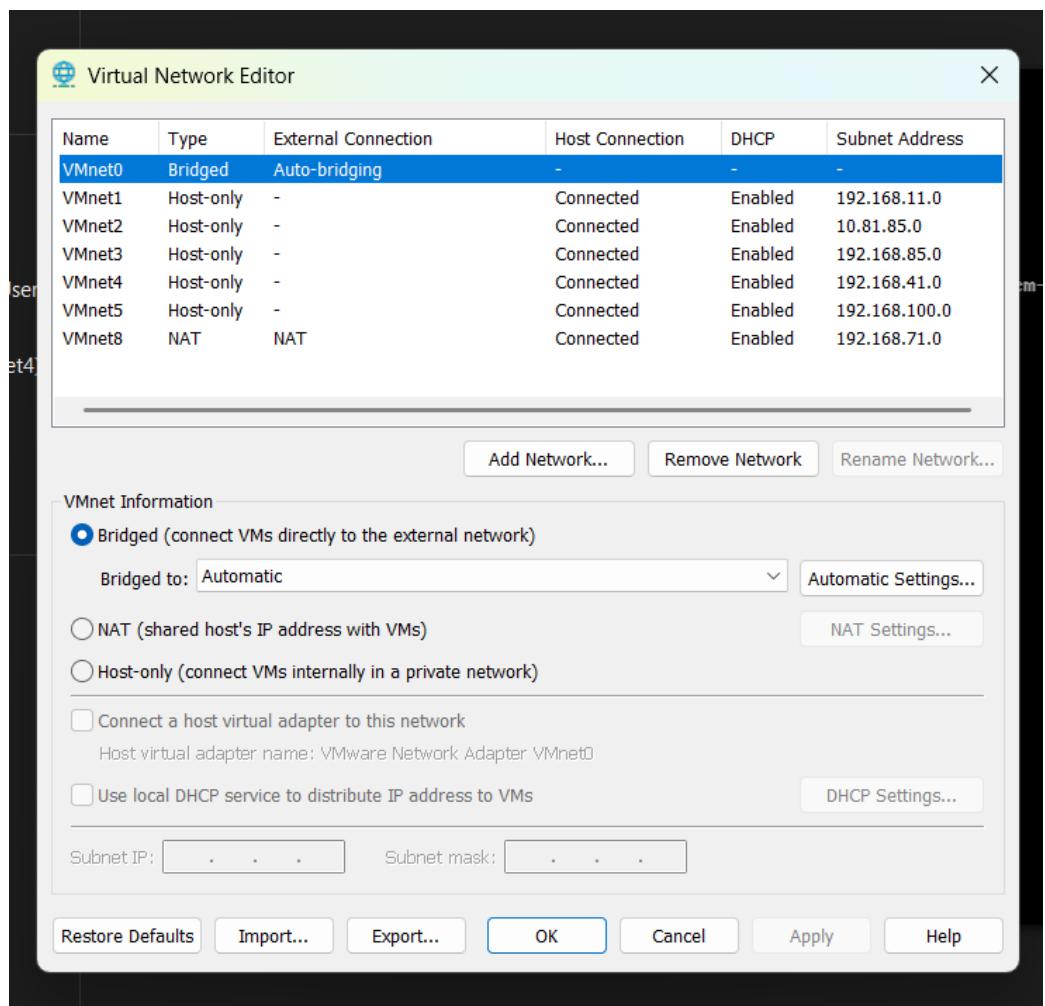
##### 4.1.3.1. Cấu Hình Phần Cứng (VMs)

Sử dụng môi trường Ảo Hoá Loại 2: **VMware Workstation Pro** để thực hiện kịch bản, và nhóm dùng máy chủ vật lý có thông số cấu hình như sau để đảm bảo performance khi chạy nhiều VM cùng lúc:

- Host: Laptop Lenovo LOQ 2024
- CPU: Intel Core i5-12450HX (8 cores/12 threads)
- RAM: 24 GB DDR5
- Ổ cứng: SSD NVMe 1TB
- Hệ điều hành host: Windows 11 Home SL (64-bit)

##### 4.1.3.2. Cấu hình Mạng

- Cấu hình mạng ảo trong VMWare:



#### **4.1.3.3. Import chứng chỉ từ máy SO**

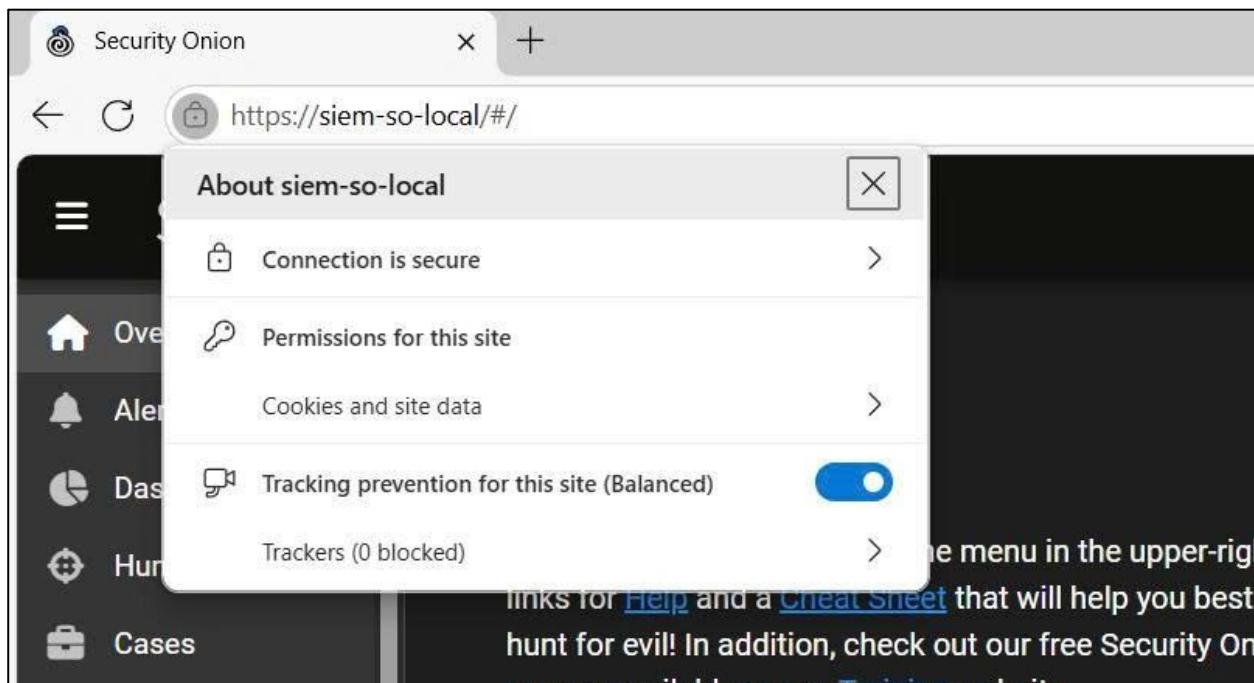
- Ta tiến hành lấy file ca.crt từ máy SO, sau đó gửi chứng chỉ này cho những clients để các clients đó xác thực:

```
[wanthinnn@siem-so-local ~]$ cd /etc/pki/
[wanthinnn@siem-so-local pki]$ ls
ca.crt          elasticfleet-logstash.crt    elasticsearch.crt  issued_certs   rpm-gpg
ca.key          elasticfleet-logstash.key    elasticsearch.key  java           rsyslog
ca-trust        elasticfleet-logstash.p8     elasticsearch.p12 managerssl.crt  swid
elasticfleet-agent.crt elasticfleet-lumberjack.crt filebeat.crt    managerssl.key tls
elasticfleet-agent.key elasticfleet-lumberjack.key filebeat.key    redis.crt
elasticfleet-agent.p8  elasticfleet-lumberjack.p8  filebeat.p8    redis.key
elasticfleet-kafka.crt elasticfleet-server.crt  influxdb.crt   registry.crt
elasticfleet-kafka.key elasticfleet-server.key  influxdb.key   registry.key

[wanthinnn@siem-so-local pki]$ sudo cp ca.crt ~
[wanthinnn@siem-so-local ~]$ cd ~
[wanthinnn@siem-so-local ~]$ ls
ca.crt  SecurityOnion
[wanthinnn@siem-so-local ~]$ chmod 777 ca.crt
chmod: changing permissions of 'ca.crt': Operation not permitted
[wanthinnn@siem-so-local ~]$ sudo chmod 777 ca.crt
[wanthinnn@siem-so-local ~]$ ls
ca.crt  SecurityOnion
[wanthinnn@siem-so-local ~]$ readlink -f *
/home/wanthinnn/ca.crt
/home/wanthinnn/SecurityOnion
[wanthinnn@siem-so-local ~]$ |
```

- Ta sẽ copy file này về máy Windows (cũng là máy để vào giao diện SO Manager):

- Sau khi import chứng chỉ vào, máy Windows đã “tin” được Security Onion:



#### 4.1.4. Kết quả và đánh giá

Đối với những extensions được tích hợp vào trong SOC của Security Onion, mỗi phần sẽ có vai trò riêng và được giới thiệu cụ thể như sau

- Grid: Cung cấp giao diện để quản lý và giám sát các cảm biến trong lưới Security Onion. Người dùng có thể kiểm tra tình trạng hoạt động, cấu hình, và hiệu suất của các cảm biến phân tán trên mạng. Đây thường là mục được chọn khi cần quản lý cơ sở hạ tầng giám sát

The screenshot shows the Security Onion Grid interface. On the left, there's a sidebar with navigation links like Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid (which is selected), Downloads, and Administration. Below that is a Tools section with Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, and Navigator. At the bottom of the sidebar, it says "Version: 2.4.150". The main content area has tabs for Node Status, Container Status, and Appliance Images. The Node Status tab displays detailed information about the local node, including its ID (siem-so-local), role (Standalone), address (192.168.71.250), version (2.4.150), model (N/A), and EPS (3,466). It also shows metrics like OS Uptime (26 minutes) and RAID Status (Feature Unavailable). The Container Status tab lists several containers: so-dockerregistry, so-elastalert, so-elastic-fleet, so-elastic-fleet-package-registry, so-elasticsearch, so-idstools, so-influxdb, so-kibana, so-kratos, and so-logstash, all marked as running and up 4. The Appliance Images tab is currently empty, stating "Appliance images are only displayed for official Security Onion Solut". At the bottom of the main content area, it says "© 2025 Security Onion Solutions, LLC" and "License: ELv2".

**- Detection:** Tập trung vào việc quản lý các quy tắc phát hiện mối đe dọa, bao gồm các quy tắc Suricata (dành cho IDS/IPS), Sigma (dành cho phân tích log), và các quy tắc tùy chỉnh khác. Người dùng có thể xem, chỉnh sửa, hoặc kích hoạt các quy tắc để cải thiện khả năng phát hiện các hành vi nguy hiểm. Trong một số trường hợp, mục này có thể hiển thị biểu tượng đồng hồ cát nhỏ, cho thấy hệ thống đang xử lý hoặc cập nhật dữ liệu

The screenshot shows the 'Detections' section of the Security Onion interface. On the left is a sidebar with navigation links like Overview, Alerts, Dashboards, Hunt, Cases, Detections (which is selected), PCAP, Grid, Downloads, Administration, Tools (Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, Navigator), and a footer with 'Version: 2.4.150'. The main area has a title 'Detections' and a fetch limit of 5000. It lists several events with columns for Title, Enabled, Overrides, Severity, Type, RuleSet, and Timestamp. Most events are from the Sigma rule set and have a medium severity level.

Title	Enabled	Overrides	Severity	Type	RuleSet	Timestamp
The Security Onion grid has returned to a healthy state	false	0	medium	Sigma	securityonion-resources	2025-06-04 15:01
The Security Onion grid has entered an unhealthy state	false	0	medium	Sigma	securityonion-resources	2025-06-04 15:01
The Security Onion grid has nodes that require reboot	false	0	unknown	Sigma	securityonion-resources	2025-06-04 15:01
The Security Onion Detections engine has returned to a healthy state	false	0	medium	Sigma	securityonion-resources	2025-06-04 15:01
The Security Onion Detections engine has entered a failure state	false	0	medium	Sigma	securityonion-resources	2025-06-04 15:01
Security Onion - Grid Node Login Failure (SSH)	true	0	high	Sigma	securityonion-resources	2025-06-04 15:01
Security Onion - SOC Login Failure	true	0	high	Sigma	securityonion-resources	2025-06-04 15:01
Security Onion - Grid Node Login Failure (Console)	true	0	high	Sigma	securityonion-resources	2025-06-04 15:01

The screenshot shows the 'Security Onion IDH - TFTP Requests' detection details page. The sidebar is identical to the previous one. The main area has tabs for OVERVIEW (selected), OPERATIONAL NOTES, DETECTION SOURCE, TUNING (0), and HISTORY. The OVERVIEW tab shows a summary: 'Detects when the TFTP service on a SO Intrusion Detection Honeypot (IDH) node has had requests.' It also includes references to 'openanary.readthedocs.io/en/latest/startng/configuration.html#services-configuration' and 'https://github.com/thinkst/openanary/blob/a0896adfcf0328cf5829fe10d2878c7445138e/openanary/logger.py#L52'. The DETECTION LOGIC section shows the configuration code:

```

logsource:
  product: openanary
detection:
  selection:
    logtype:
      - '10001'
  condition: selection
  
```

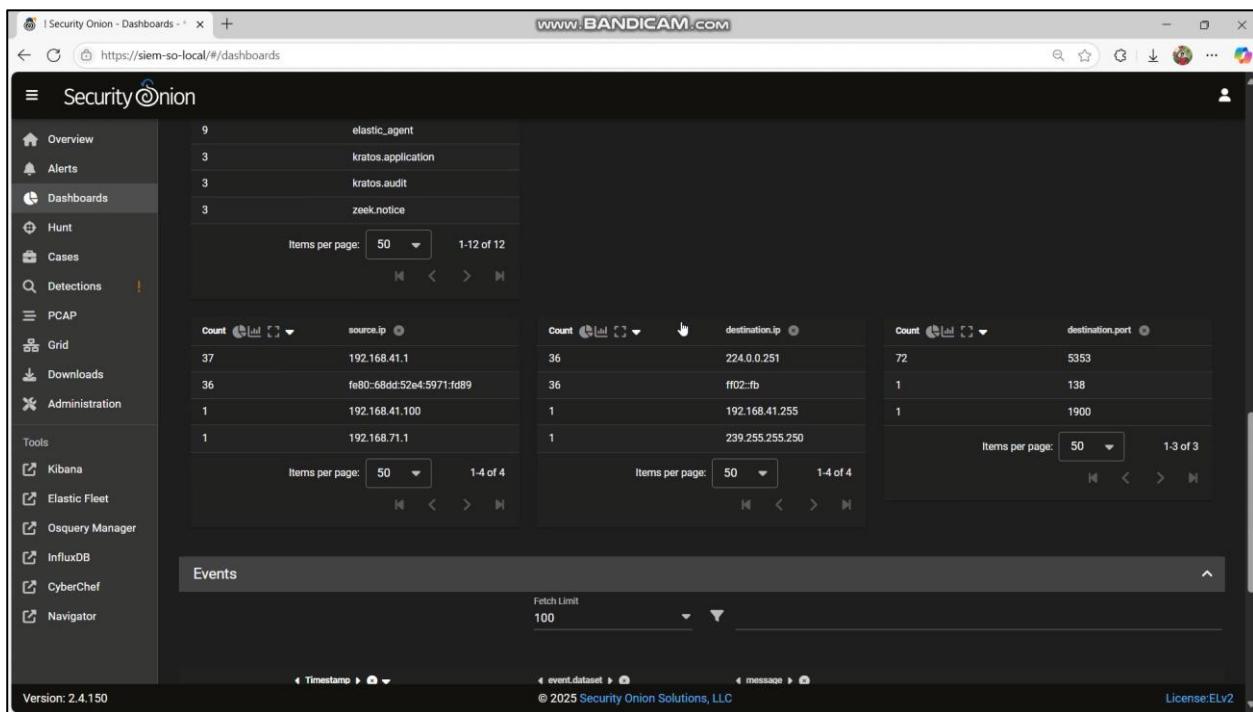
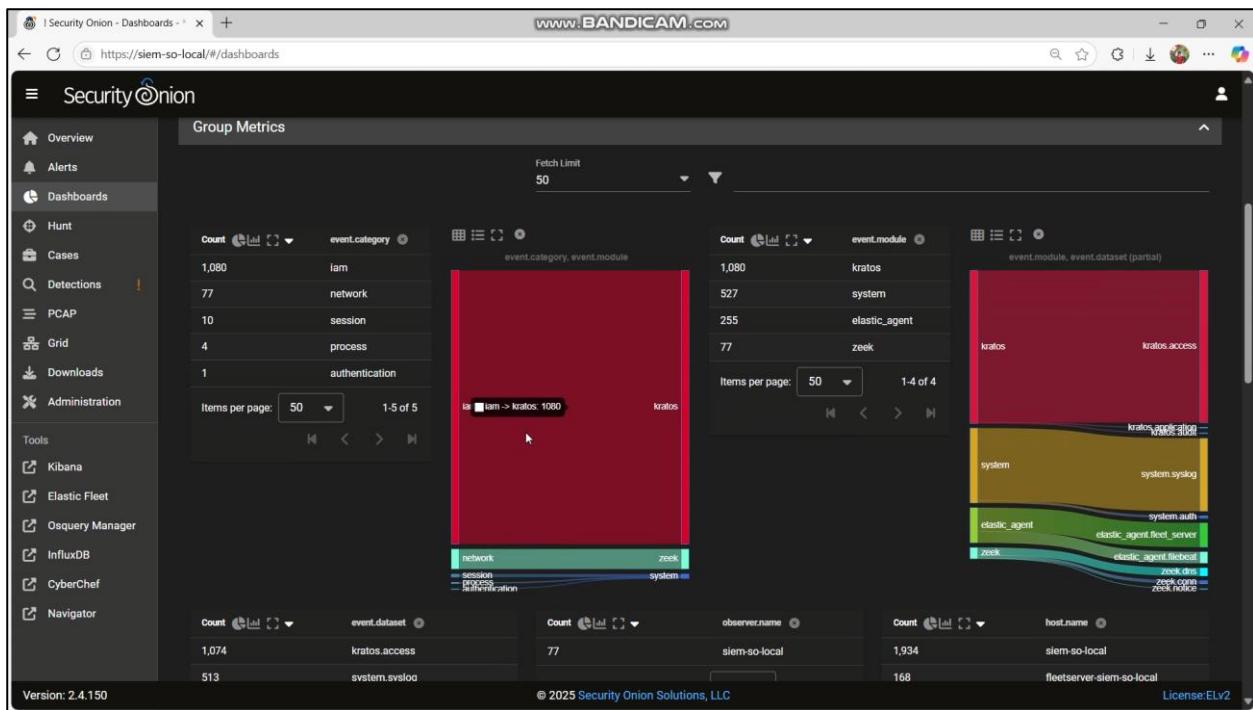
The right side of the screen contains an 'Operations' panel with a status toggle (Enabled), a 'DUPLICATE' button, and a 'DELETE' button. Below it is a 'Details' panel with fields for Public Id, Type, Severity, RuleSet, License, and Created.

Version: 2.4.150      © 2025 Security Onion Solutions, LLC      License: ELv2

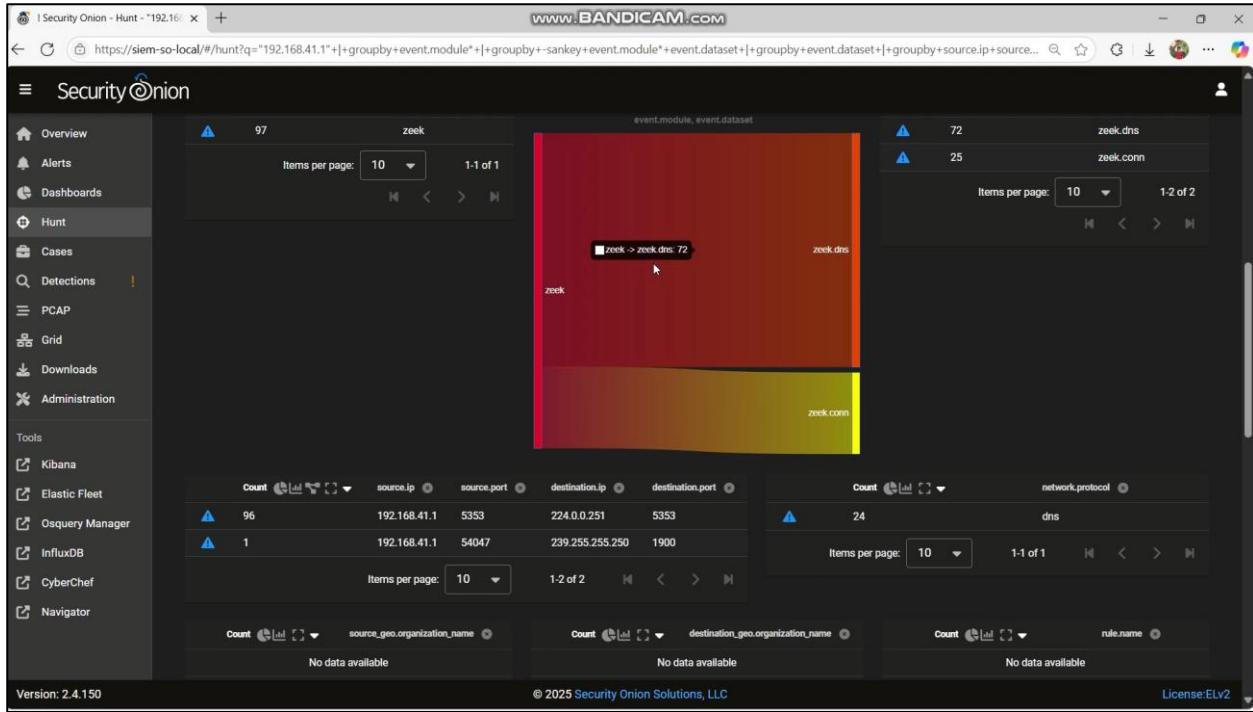
**- Alert:** Hiển thị danh sách các cảnh báo được tạo bởi các công cụ phát hiện xâm nhập như Suricata (IDS/IPS), Zeek (phân tích mạng), hoặc các quy tắc bảo mật khác. Tại đây, người dùng có thể xem chi tiết từng cảnh báo, phân loại chúng (ví dụ: xác nhận hoặc bỏ qua), và thực hiện các hành động xử lý cần thiết

Version: 2.4.150      © 2025 Security Onion Solutions, LLC      License: ELv2

**- Dashboard:** Cung cấp quyền truy cập vào các bảng điều khiển trực quan, được xây dựng bằng Kibana và dựa trên dữ liệu từ Elasticsearch. Các dashboards này có thể được cấu hình sẵn hoặc tùy chỉnh để hiển thị thông tin như lưu lượng mạng, log hệ thống, hoặc các xu hướng sự kiện bảo mật, giúp người dùng dễ dàng theo dõi và phân tích dữ liệu



- Hunt: Đây là công cụ dành cho các hoạt động săn lùng mối đe dọa (threat hunting). Người dùng có thể thực hiện tìm kiếm chủ động trong dữ liệu để phát hiện các hoạt động đáng ngờ, các dấu hiệu của cuộc tấn công, hoặc các mẫu hành vi bất thường mà các quy tắc tự động có thể bỏ sót



- **Cases:** Tính năng này cho phép quản lý các vụ việc bảo mật. Người dùng có thể tạo mới, theo dõi tiến trình, và ghi chép chi tiết về các cuộc điều tra. Cases hỗ trợ tổ chức thông tin một cách có hệ thống và thúc đẩy sự hợp tác giữa các thành viên trong nhóm SOC

- **PCAP:** Cho phép người dùng truy cập và phân tích các tệp PCAP – bản ghi lưu lượng mạng được thu thập từ các cảm biến. Tính năng này rất hữu ích để điều tra chi tiết các sự kiện mạng, xác minh cảnh báo, hoặc tái tạo lại các cuộc tấn công

## 4.2. Kịch bản 2: Tích hợp Security Onion với Firewall (pfSense)

Xem Video Demo tại: <https://youtu.be/HT8qZro5x00?si=-r-8OZ2qNsrbV93Q>

### 4.2.1. Mục tiêu

Xây dựng một kịch bản mô phỏng tấn công mạng đơn giản, trong đó **pfSense** đóng vai trò firewall ghi nhận sự kiện mạng, gửi log về **Security Onion** để phân tích và hiển thị trên **Kibana Dashboard**. **Thành phần hệ thống:**

- **pfSense**: tường lửa mạng, ghi log truy cập đến các cổng dịch vụ.
- **Security Onion**: hệ thống SIEM, phân tích log nhận được từ pfSense.
- **Công cụ sinh lưu lượng**: hping3 trên máy Attacker để mô phỏng các truy cập hợp lệ và bị chặn.

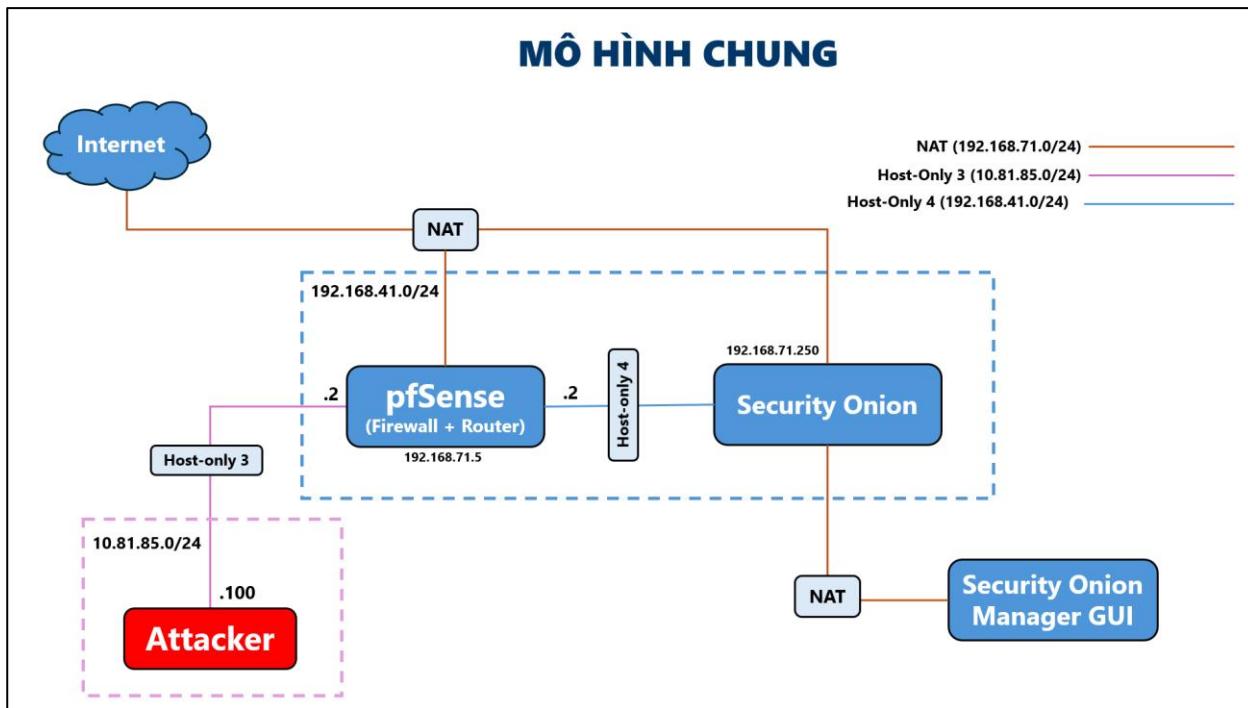
### 4.2.2. Ngữ cảnh và Mô hình triển khai

#### 4.2.2.1. Ngữ Cảnh

- Đây là tiền đề cho việc ta thiết kế một mô hình “Mạng Nội Bộ” cho kịch bản 3, do đó, ta cần giả lập đầy các thành phần như sau:

- + **pfSense** hoạt động như Firewall + Router, phân chia hai VLAN (192.168.41.0/24 và 192.168.71.0/24), cấp NAT ra Internet.
- + **Security Onion** vừa nhận traffic giám sát từ pfSense, vừa chạy các sensor Suricata, Zeek, Filebeat, Winlogbeat, và ES/Logstash/Kibana để phân tích, phát hiện.
- + **Attacker** nằm trên một host khác (Host-Only 3: 10.81.85.0/24), dùng để phát sinh cuộc tấn công (scan, exploit, brute force) vào mạng 192.168.41.0/24.
- Mục tiêu chính: minh họa cách traffic giữa pfSense với Security Onion để phát hiện intrusion, đồng thời cũng thể hiện cách pfSense route/NAT traffic đến Internet (West-East).

#### 4.2.2.2. Mô hình triển khai



#### 4.2.2.3. Mô tả các thành phần

STT	Thành Phần	Mô Tả
1	<b>Internet</b>	<ul style="list-style-type: none"> <li>- Được mô phỏng bằng NAT network của VMware.</li> <li>- Cung cấp kết nối ra ngoài cho pfSense, Security Onion Manager GUI, và có thể cho các client cần update/cập nhật.</li> </ul>
2	<b>pfSense (Firewall + Router)</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 2 GB RAM; 128GB SSD.</li> <li>- <b>Interface LAN (Host-Only 4: 192.168.41.0/24)</b>: địa chỉ 192.168.41.2.</li> <li>- <b>Interface OPT1 (Host-Only 4: 192.168.71.0/24)</b>: địa chỉ 192.168.71.4.</li> <li>- <b>Interface WAN (NAT: 192.168.71.0/24)</b>: địa chỉ dù 192.168.71.4, dùng để NAT ra Internet.</li> <li>- Nhiệm vụ: phân luồng (routing) giữa 192.168.41.0/24 ↔ 192.168.71.0/24 ↔ 10.81.85.0/24 ↔ Internet.</li> </ul>
3	<b>Security Onion (Standalone)</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 8 Cores vCPU; 16 GB RAM; 1000GB SSD.</li> <li>- <b>Interface giám sát (Host-Only 4): 192.168.41.0/24</b></li> </ul>

		<ul style="list-style-type: none"> <li>- <b>Interface WAN (NAT)</b>: địa chỉ NAT 192.168.71.250 để truy cập Internet, đồng thời để Security Onion Manager GUI publish ra host.</li> <li>- Cài đặt <b>all-in-one mode</b> (sensor + manager) để tự chứa Suricata, Zeek, Elasticsearch, Kibana, Fleet Server (8220), v.v.</li> <li>- Ghi lại toàn bộ traffic passed-through pfSense (mirror port qua Host-Only 4) để Suricata/Zeek phân tích.</li> </ul>
4	<b>Attacker</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 4 GB RAM; 128GB SSD.</li> <li>- Nằm trên Host-Only 3 (10.81.85.0/24), địa chỉ 10.81.85.100.</li> <li>- Sử dụng Parrot, thực hiện tấn công (scan nmap, exploit, brute-force SSH, tấn công ứng dụng web) vào Clients.</li> </ul>

#### 4.2.3. Quy trình triển khai

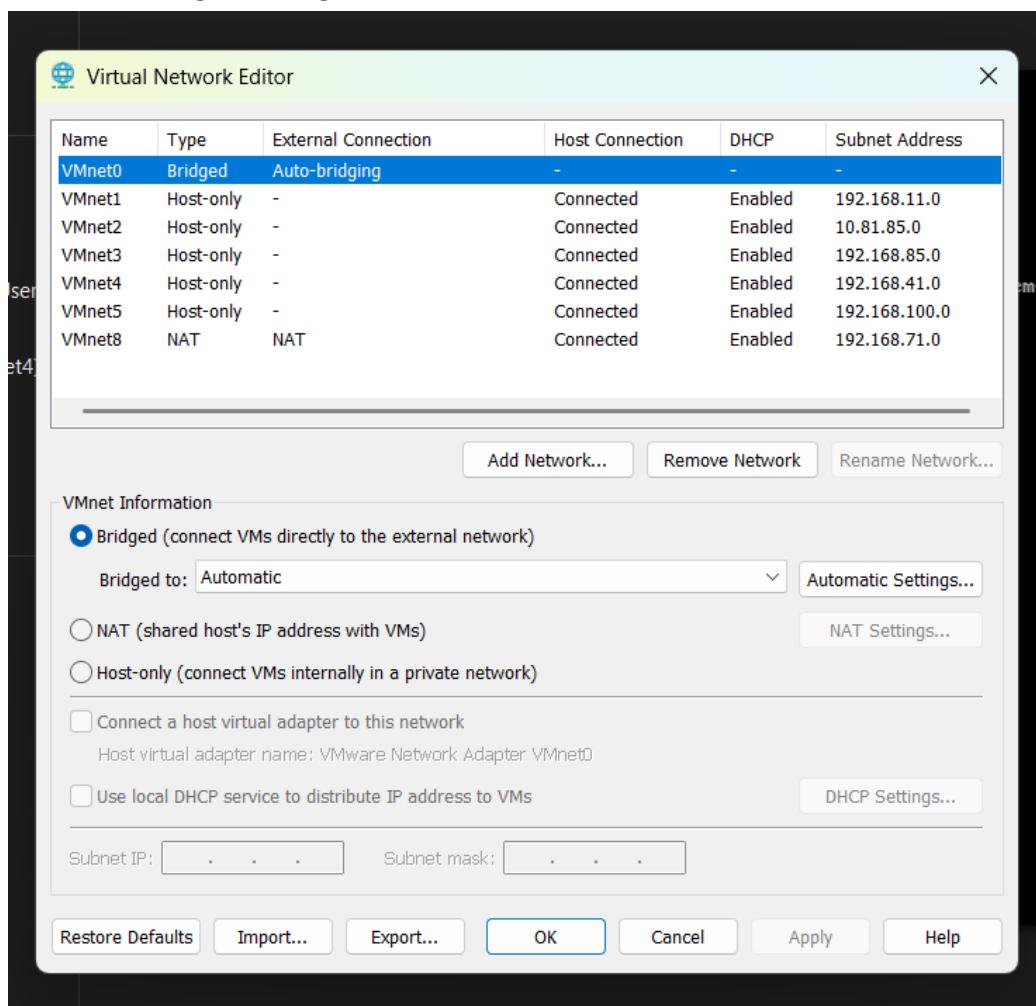
##### 4.2.3.1. Cấu Hình Phần Cứng (VMs)

Sử dụng môi trường Ảo Hoá Loại 2: **VMware Workstation Pro** để thực hiện kịch bản, và nhóm dùng máy chủ vật lý có thông số cấu hình như sau để đảm bảo performance khi chạy nhiều VM cùng lúc:

- Host: Laptop Lenovo LOQ 2024
- CPU: Intel Core i5-12450HX (8 cores/12 threads)
- RAM: 24 GB DDR5
- Ổ cứng: SSD NVMe 1TB
- Hệ điều hành host: Windows 11 Home SL (64-bit)

#### 4.2.3.2. Cấu hình Mạng

- Cấu hình mạng ảo trong VMWare:



- Thông tin mạng trong pfSense:

The screenshot shows the pfSense Status / Dashboard interface. It includes sections for System Information, Netgate Services And Support, and Interfaces.

**System Information** (Left Panel):

- Name: pfSense.home.arpa
- User: admin@192.168.41.1 (Local Database)
- System: VMware Virtual Machine  
Netgate Device ID: 4e036efda3092747eff4
- BIOS: Vendor: Phoenix Technologies LTD  
Version: 6.00  
Release Date: Thu Nov 12 2020  
Boot Method: BIOS
- Version: 2.8.0-RELEASE (amd64)  
built on Thu May 22 6:12:00 +07 2025  
FreeBSD 15.0-CURRENT
- CPU Type: 12th Gen Intel(R) Core(TM) i5-12450HX  
2 CPUs | 1 package(s) | x 2 core(s)  
AES-NI CPU Crypto: Yes (inactive)  
QAT Crypto: No
- Hardware crypto: Inactive
- Kernel PTI: Enabled
- MDS Mitigation: Inactive
- Uptime: 04 Hours 10 Minutes 20 Seconds
- Current date/time: Sun Jun 1 21:09:18 +07 2025
- DNS server(s): 127.0.0.1  
..  
8.8.8  
1.1.1.1
- Last config change: Sun Jun 1 20:10:35 +07 2025
- State table size: 0% (17/199000) Show states
- MBUF Usage: 3% (4318/124490)
- Load average: 0.46, 0.40, 0.37
- CPU usage: 0%
- Memory usage: 12% of 1997 MiB
- SWAP usage: 0% of 1024 MiB

**Netgate Services And Support** (Top Right Panel):

- Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES** (Bottom Right Panel):

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

**Interfaces** (Bottom Right Panel):

WAN	1000baseT <full-duplex>	192.168.71.5
LAN	1000baseT <full-duplex>	192.168.41.2
OPT1	1000baseT <full-duplex>	10.81.85.2

#### 4.2.3.4. Cấu hình HTTPS cho giao diện quản lý pfSense

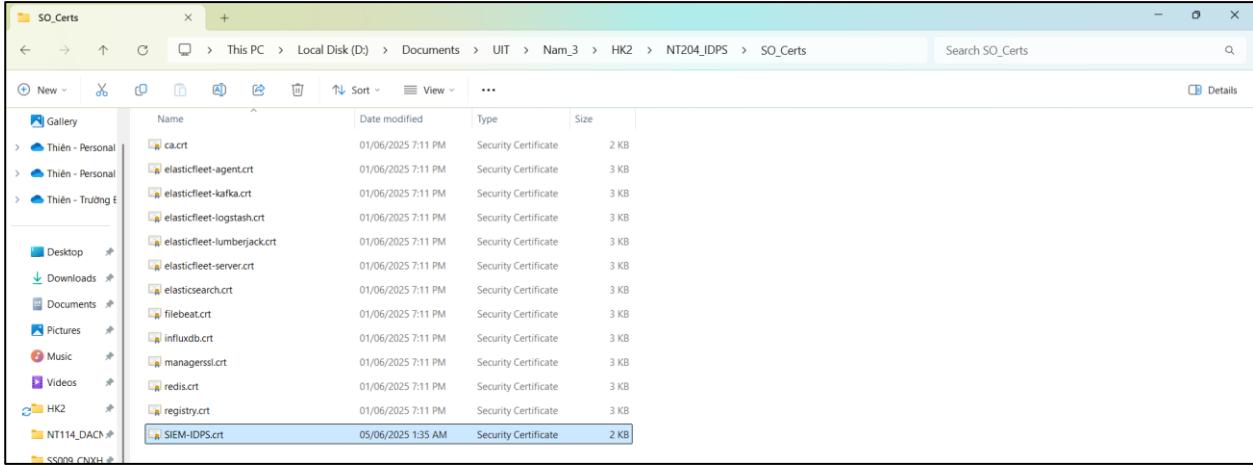
- Tạo chứng chỉ tự ký:

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
SIEM-IDPS	✓	self-signed	1	ST=Ho Chi Minh, OU=UIT, O=Nhom12, L=Thu Duc, CN=siem-idps-internal-ca, C=VN	<a href="#">i</a>	<a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>
SO-CA	✗	self-signed	0	ST=Utah, L=Salt Lake City, CN=siem-so-local, C=US	<a href="#">i</a>	<a href="#"></a> <a href="#"></a> <a href="#"></a>

- Sau đó sử dụng chứng chỉ tự ký trên ký cho siem-idps.local:

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (683accaff3e9d) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-683accaff3e9d	<a href="#">i</a>	<a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>
siem-dacn-local Server Certificate CA: No Server: Yes	external	ST=Ho Chi Minh, OU=VNU, O=UIT, L=Ho Chi Minh City, CN=siem-dacn-pfsense.local, C=VN	<a href="#">i</a>	<a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>
siem-idps-local Server Certificate CA: No Server: Yes	SIEM-IDPS	ST=Ho Chi Minh, OU=UIT, O=Nhom12, L=Thu Duc, CN=siem-idps.local, C=VN	<a href="#">i</a>	webConfigurator <a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>

- Xuất chứng chỉ trên cho máy Manager để import vào:



- Kết quả ta được HTTPS:

#### 4.2.3.5. Cấu hình pfSense gửi log đến Security Onion

- Vào pfSense → Status > System Logs > Settings
- Ta chọn Log Format là syslog cho phù hợp với định dạng json của SO:

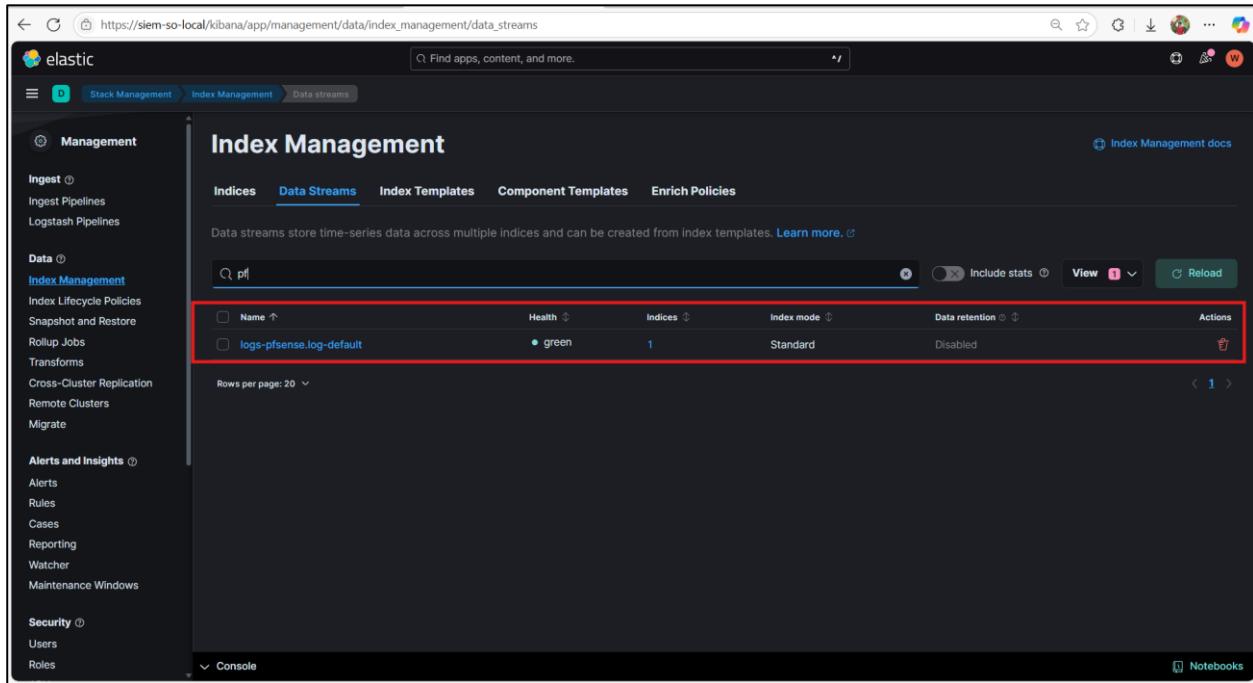
#### - Mục Remote Logging Options:

- + Enable:
- + IP: 192.168.71.250 (Security Onion)
- + Port: 9001
- + Contents: chọn Everything ( hoặc tùy chỉnh theo ý muốn)
- Save.

#### 4.3.4.6. Cấu hình Elastic Agent trên Security Onion để nhận log pfSense

- Ta cấu hình theo hướng dẫn của Security Onion: [Ingesting PFsense Logs with Security Onion 2.4](#)

- Sau khi thành công, trong phần [https://siem-so-local/kibana/app/management/data/index\\_management/data\\_streams](https://siem-so-local/kibana/app/management/data/index_management/data_streams) sẽ hiện lên index logs của pfsense:



The screenshot shows the Elasticsearch Index Management interface. On the left, there's a sidebar with navigation links for Management, Ingest Pipelines, Logstash Pipelines, Data (Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Cross-Cluster Replication, Remote Clusters, Migrate), Alerts and Insights (Alerts, Rules, Cases, Reporting, Watcher, Maintenance Windows), and Security (Users, Roles). The main area is titled 'Index Management' and has tabs for Indices, Data Streams, Index Templates, Component Templates, and Enrich Policies. The 'Data Streams' tab is selected. A search bar at the top has 'pf' entered. Below it is a table with one row, 'logs-pfsense.log-default', highlighted with a red border. The table columns are Name, Health, Indices, Index mode, Data retention, and Actions. The 'logs-pfsense.log-default' row shows 'green' under Health, '1' under Indices, 'Standard' under Index mode, and 'Disabled' under Data retention. The Actions column contains a delete icon. At the bottom of the table, it says 'Rows per page: 20'.

#### 4.2.4.6. Tạo Rule trên pfSense để sinh log

- Vào Firewall > Rules:

+ Rule 1 – Cho phép port 8080 -> Action: Pass -> Destination port: 8080 -> Enable logging -> Save -> Apply changes

The screenshot shows the 'Edit Firewall Rule' configuration page. The rule is being created for port 8080 on the LAN interface, using UDP protocol, with an action of 'Pass'. Logging is enabled. The rule is set to apply to IPv4 traffic on the LAN interface. The destination port is also set to 8080. A description 'Allow port 8080' is provided. The 'Save' button is at the bottom.

**Action:** Pass

**Disabled:**  Disable this rule

**Interface:** LAN

**Address Family:** IPv4

**Protocol:** UDP

**Source:** Source: any / Source Address

**Destination:** Destination: This firewall (self) / Destination Address

**Extra Options:**

- Log:**  Log packets that are handled by this rule
- Description:** Allow port 8080
- Advanced Options:** Display Advanced

**Buttons:** Save, Cancel, Help, Delete

**Bottom Status Bar:** 0/0 B, IPv4, TCP, This Firewall, 8080, none

+ Rule 2 – Chặn port 23 (telnet) -> Action: Block -> Destination port: 23 -> Enable logging -> Save -> Apply changes

The screenshot shows the pfSense Firewall Rules configuration interface. A new rule is being created:

- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP/UDP
- Source:** Source: any, Destination: This firewall (self)
- Destination Port Range:** Telnet (23) (From: Custom, To: Custom)
- Extra Options:**
  - Log:** Log packets that are handled by this rule (unchecked)
  - Description:** A description may be entered here for administrative reference.
  - Advanced Options:** Display Advanced
- Action:** Block traffic to pfSense on port 23

#### 4.2.4. Kết quả và đánh giá

##### 4.2.4.1. Kiểm thử hệ thống

###### a. Sinh log bằng cách gửi gói tin từ Security Onion

Bên máy Attacker, ta tấn công bằng cách gửi gói tin vào port 23:

```
(kali㉿kali)-[~]
$ sudo hping3 -S 10.81.85.2 -p 23
HPING 10.81.85.2 (eth0 10.81.85.2): S set, 40 headers + 0 data bytes
^C
--- 10.81.85.2 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

###### b. Phân tích log trên Kibana hoặc Hunt

- Ta vào Hunt để xem tóm tắt logs:

Count: 117

event.module: pfSense

event.dataset: pfSense.log

Items per page: 10

Fetch Limit: 5000

Timestamp	event.dataset	source.ip	source.port	destination.ip	destination.port	network.transport	network.type
2025-06-05 03:00:47.697 +07:00	pfSense.log	10.81.85.100	1875	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:46.697 +07:00	pfSense.log	10.81.85.100	1874	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:45.699 +07:00	pfSense.log	10.81.85.100	1873	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:44.691 +07:00	pfSense.log	10.81.85.100	1872	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:43.690 +07:00	pfSense.log	10.81.85.100	1871	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:42.697 +07:00	pfSense.log	10.81.85.100	1870	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:41.691 +07:00	pfSense.log	192.168.41.1	51904	192.168.41.2	443	tcp	ipv4
2025-06-05 03:00:41.691 +07:00	pfSense.log	10.81.85.100	1869	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:40.696 +07:00	pfSense.log	10.81.85.100	1868	10.81.85.2	23	tcp	ipv4
2025-06-05 03:00:40.696 +07:00	pfSense.log	192.168.41.1	51903	192.168.41.2	443	tcp	ipv4

Version: 2.4.150 License: ELv2

- Sau đó truy cập giao diện Kibana để xem chi tiết:

tags : pfSense and source.ip : "10.81.85.100"

Jun 4, 2025 @ 03:01:06.301 - Jun 5, 2025 @ 03:01:06.301 (interval: Auto + 30 minutes)

Documents (41) Patterns Field statistics

```

o-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:56.86
c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
se.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.86
o-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:55.86
c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
se.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.86
o-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:54.86
c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
se.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.86
o-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:53.86
c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
se.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.86
o-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:52.86
c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
se.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.86
o-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:51.84
c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
se.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.84
tags pfSense forwarded elastic-agent input-siem-so-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:50.88
lebeat.agent.version 8.17.3 data_stream.dataset pfSense.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.88
tags pfSense forwarded elastic-agent input-siem-so-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:51.84
2 version 1 agent.ephemeral_id 42b9c38e-b38c-4054-81c7-d39ad679df5c agent.id e093e4e-8651-4db8-9db5-0fc81d34360c agent.name siem-so-local agent.type fi
lebeat.agent.version 8.17.3 data_stream.dataset pfSense.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.88
tags pfSense forwarded elastic-agent input-siem-so-local beats_input_codec_plain_applied log @timestamp Jun 5, 2025 @ 03:00:50.88
lebeat.agent.version 8.17.3 data_stream.dataset pfSense.log data_stream.namespace default data_stream.type logs destination.address 10.81.85.88

```

- + Tìm kiếm log theo IP nguồn: event.dataset: "pfSense.log" AND source.ip: "10.81.85.100"
- + Kiểm tra trường event.action: "pass" → cho phép | "block" → bị chặn
- + Sau khi thực hiện lệnh nc ta quan sát được các log sau tương ứng với các rules đã tạo:

#### **4.2.4.2. Kết quả**

- **Thu thập log:** pfSense ghi nhận chính xác log truy cập port 8080 (pass) và port 23 (block) từ Attacker (10.81.85.100), gửi syslog về Security Onion (192.168.71.250:9001).
- **Phân tích log:** Kibana hiển thị log chi tiết (event.dataset: "pfsense.log" AND source.ip: "10.81.85.100"), phân biệt rõ hành động "pass"/"block".
- **Phát hiện bất thường:** Security Onion phát hiện và cảnh báo truy cập trái phép (port 23) qua Hunt và Kibana.
- **Tích hợp ổn định:** pfSense và Security Onion hoạt động mượt mà, không mất log, hỗ trợ giám sát hiệu quả.
- **Mô phỏng tấn công:** hping3 tạo lưu lượng tấn công thành công, kiểm tra tốt khả năng phát hiện của hệ thống.

#### **4.2.4.3. Đánh giá**

##### **a. Ưu điểm:**

- Tái hiện thực tế môi trường giám sát mạng doanh nghiệp.
- Có thể áp dụng kiến thức firewall, IDS/IPS, SIEM.
- Dễ mô phỏng, test nhiều loại tấn công thực tế.
- Tận dụng được log từ pfSense để nâng cao chất lượng cảnh báo.

##### **b. Nhược điểm**

- Cần cấu hình nhiều adapter mạng → dễ gây lỗi route hoặc NAT.
- Security Onion yêu cầu cấu hình phần cứng cao → tốn RAM.
- Phải hiểu rõ cách định tuyến nếu dùng nhiều VMnet (Host-only, NAT, Bridge).

##### **c. Khó khăn khi triển khai trên môi trường ảo hóa loại 2 (như VMware Workstation Pro)**

- VMware Workstation không hỗ trợ port mirroring thật → phải dùng bridge ảo.
- Cần thao tác cấu hình nhiều card mạng ảo thủ công.
- Nếu dùng NAT, có thể gây lỗi không vào được GUI do chưa bật port forwarding.
- Giới hạn tài nguyên (RAM/CPU) khi dùng nhiều máy ảo trên 1 host.

##### **d. Tính ứng dụng thực tế:**

- Dùng pfSense làm firewall thực tế cho công ty nhỏ.
- Dùng SO giám sát các hoạt động trong mạng nội bộ.
- Phát hiện tấn công nội bộ hoặc từ internet → nâng cao khả năng phát hiện sớm sự cố.

=> **Kết luận:** Tích hợp pfSense-Security Onion hiệu quả, giám sát và phát hiện bất thường tốt, phù hợp cho mạng doanh nghiệp nhỏ.

### **4.3. Kịch Bản 3: Triển khai Mô hình Mạng Nội Bộ Với Security Onion**

Xem Video Demo tại: [https://youtu.be/\\_C9MXBDSYEU?si=vYywR-h7iumJpBQG](https://youtu.be/_C9MXBDSYEU?si=vYywR-h7iumJpBQG)

#### **4.3.1. Mục tiêu**

**Giám sát và Phát hiện Tấn công:** Mô hình mạng nội bộ này đặt **Security Onion** vào vị trí trung tâm, nhận toàn bộ traffic nội bộ (từ Clients, Attacker) để thực hiện giám sát (IDS), phân tích log (SIEM), và phát hiện sớm các hoạt động độc hại. Qua đó, đội SOC có thể luyện tập kịch bản tấn công – phát hiện – phản ứng, đồng thời thu thập evidences phục vụ báo cáo, đồ án và học tập chuyên môn.

**Tính Ứng Dụng Thực Tế:** Mô phỏng một dạng “SOC in a box” (Security Onion + pfSense) phù hợp môi trường doanh nghiệp nhỏ. Cho thấy cách triển khai Security Onion kiểu **all-in-one** hoặc **distributed** (độc lập manager GUI + sensor) để quản lý tập trung, phân tách traffic mgmt, traffic giám sát.

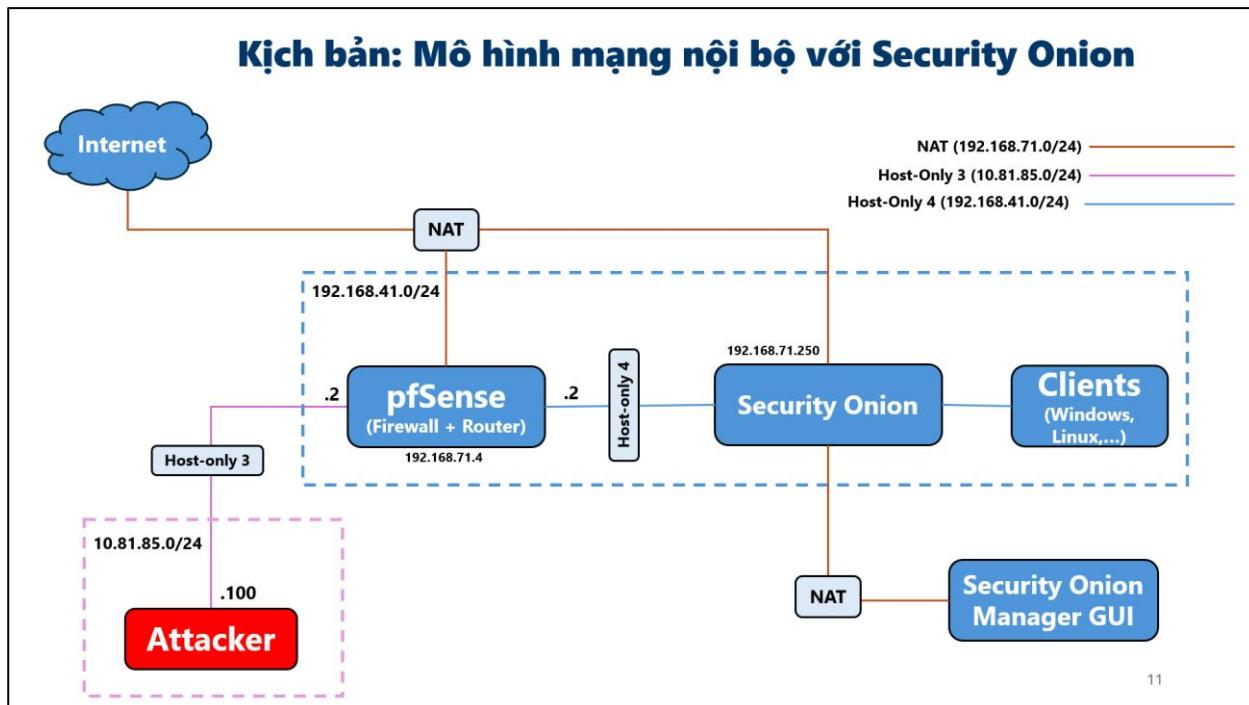
**Lý Do Chọn Kịch Bản Này:** Liên quan chặt chẽ đến đồ án “Hệ Thống Quản Lý và Xử Lý Tập Trung Các Sự Kiện Tấn Công Mạng”: cần mô hình mạng đủ phức tạp, có segment, có attacker giả lập, để test rules Suricata, quy trình phản ứng SIEM/ELK. Môi trường ảo hóa (VMware Workstation Pro) đã sẵn sàng nhiều Host-Only networks, NAT networks, thuận tiện để dựng mô hình 3 – 4 lớp mạng cách ly, giống hệt môi trường doanh nghiệp.

#### **4.3.2. Ngữ cảnh và Mô hình triển khai**

##### **4.3.2.1. Ngữ Cảnh**

- Đây là giai đoạn “Mạng Nội Bộ”: nghĩa là giả lập đầy đủ các thành phần:
  - + **pfSense** hoạt động như Firewall + Router, phân chia hai VLAN (192.168.41.0/24 và 192.168.71.0/24), cấp NAT ra Internet.
    - + **Security Onion** vừa nhận traffic giám sát từ pfSense, vừa chạy các sensor Suricata, Zeek, Filebeat, Winlogbeat, và ES/Logstash/Kibana để phân tích, phát hiện.
    - + **Clients** (Windows, Linux) nằm cùng VLAN 192.168.41.0/24, chịu NAT qua pfSense để truy cập Internet.
    - + **Attacker** nằm trên một host khác (Host-Only 3: 10.81.85.0/24), dùng để phát sinh cuộc tấn công (scan, exploit, brute force) vào mạng 192.168.41.0/24.
  - Mục tiêu chính: minh họa cách traffic đầu cuối (East-West) giữa các client-server, rồi flow đến Security Onion để phát hiện intrusion, đồng thời thể hiện cách pfSense route/NAT traffic đến Internet (West-East).

#### 4.3.2.2. Sơ đồ triển khai



#### 4.3.2.3. Mô tả các thành phần

STT	Thành Phần	Mô Tả
1	<b>Internet</b>	<ul style="list-style-type: none"> <li>- Được mô phỏng bằng NAT network của VMware.</li> <li>- Cung cấp kết nối ra ngoài cho pfSense, Security Onion Manager GUI, và có thể cho các client cần update/cập nhật.</li> </ul>
2	<b>pfSense (Firewall + Router)</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 2 GB RAM; 128GB SSD.</li> <li>- <b>Interface LAN (Host-Only 4: 192.168.41.0/24)</b>: địa chỉ 192.168.41.2.</li> <li>- <b>Interface OPT1 (Host-Only 4: 192.168.71.0/24)</b>: địa chỉ 192.168.71.4.</li> <li>- <b>Interface WAN (NAT: 192.168.71.0/24)</b>: địa chỉ dù 192.168.71.4, dùng để NAT ra Internet.</li> <li>- Nhiệm vụ: phân luồng (routing) giữa 192.168.41.0/24 ↔ 192.168.71.0/24 ↔ 10.81.85.0/24 ↔ Internet.</li> </ul>
3	<b>Security Onion (Standalone)</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 8 Cores vCPU; 16 GB RAM; 1000GB SSD.</li> <li>- <b>Interface giám sát (Host-Only 4): 192.168.41.0/24</b></li> </ul>

		<ul style="list-style-type: none"> <li>- <b>Interface WAN (NAT):</b> địa chỉ NAT 192.168.71.250 để truy cập Internet, đồng thời để Security Onion Manager GUI publish ra host.</li> <li>- Cài đặt <b>all-in-one mode</b> (sensor + manager) để tự chừa Suricata, Zeek, Elasticsearch, Kibana, Fleet Server (8220), v.v.</li> <li>- Ghi lại toàn bộ traffic passed-through pfSense (mirror port qua Host-Only 4) để Suricata/Zeek phân tích.</li> </ul>
4	<b>Clients (Windows, Linux)</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 4 GB RAM; 128GB SSD.</li> <li>- Nằm trên cùng VLAN LAN với Security Onion (192.168.41.0/24).</li> <li>- 1 máy Windows – 192.168.41.101 cài Elastic Agent (Defend) để gửi log Winlog, Sysmon, event, đồng thời tạo traffic (truy cập web, SMB, RDP) để test detection.</li> <li>- 1 máy Metasploitable2 – 192.168.41.100 để cho Attacker khai thác được nhiều lỗ hổng trên máy này.</li> </ul>
5	<b>Attacker</b>	<ul style="list-style-type: none"> <li>- Phần cứng ảo: 2 Cores vCPU; 4 GB RAM; 128GB SSD.</li> <li>- Nằm trên Host-Only 3 (10.81.85.0/24), địa chỉ 10.81.85.100.</li> <li>- Sử dụng Parrot, thực hiện tấn công (scan nmap, exploit, brute-force SSH, tấn công ứng dụng web) vào Clients.</li> </ul>

### 4.3.3. Quy trình triển khai

Đây là kịch bản được phát triển từ 2 kịch bản trước, vui lòng xem chi tiết phần này tại phần 4.1.3 và 4.2.3 đã được trình bày trước đó rất cụ thể.

### 4.3.4. Kết quả và đánh giá

Giao diện quản lý sau khi cấu hình xong:

The screenshots demonstrate the configuration and monitoring capabilities of the Security Onion system.

**Grid Page Screenshot:**

ID	Role	Address	Version	Model	EPS	Age	Status
siem-so-local	Standalone	192.168.71.250	2.4.150	N/A	3,466	5 days	OK

**Detections Page Screenshot:**

Count	RuleSet	Enabled	Category	Count	Logsource - Product
1,305	core	false	process_creation	737	windows
375	emerging_threats_addon	false	file_event	127	linux
53	core	true	registry_set	109	azure
19	securityonion-resources	true	webserver	74	openconnect
5	securityonion-resources	false	ps_script	58	rpc_firewall
			image_load	52	aws

#### 4.3.4.1. Kiểm thử hệ thống

Ta tiến hành thực hiện 2 kịch bản nhỏ để kiểm tra hiệu quả của Security Onion, cụ thể như sau:

##### a. Kịch bản 3.1: Nmap Scan từ Attacker bên ngoài mạng

- Từ máy Attacker 10.81.85.100, ta sử dụng công cụ Nmap để scan máy Victim 192.168.85.100:

```
[root@parrot] ~
# nmap -sS -sV -O 192.168.41.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 18:30 UTC
Nmap scan report for 192.168.41.100
Host is up (0.0019s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7.1p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      ?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5980/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8089/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at h
https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 26.18 seconds
[=root@parrot] ~
```

- Ngay vừa khi Attacker scan xong, thì bên máy Security Onion lập tức hiện cảnh báo với các mức độ khác nhau:

Count	rule.name	event.module	ever
4	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	me
3	GPL ICMP PING *NIX	suricata	low
2	ET INFO RMI Request Outbound	suricata	high
2	ET SCAN Suspicious inbound to MySQL port 3306	suricata	me
2	GPL DNS named version attempt	suricata	me
1	ET CHAT IRC authorization message	suricata	low
1	ET INFO GIOP/IOP Request Outbound	suricata	high
1	ET INFO Outbound MSSQL Connection to Non-Standard Port - Likely Malware	suricata	me
1	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	me
1	ET SCAN Potential VNC Scan 5800-5820	suricata	me
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	me
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	me

- Ta chọn 1 cảnh báo và đọc chi tiết về nó:

The screenshot shows the Security Onion web interface. On the left, a sidebar lists various modules like Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, Tools, Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, and Navigator. The main area displays a table of alerts with columns for Count, rule.name, event.module, event.type, and ever. One specific alert is highlighted: "ET INFO RMI Request Outbound". To the right of this alert, there is a detailed summary box with the title "ET INFO RMI Request Outbound". The summary text describes how this rule detects an outbound Java Remote Method Invocation (RMI) request, which is a mechanism allowing a Java program to invoke methods on an object located remotely. It mentions that the detection is triggered for TCP traffic from specified internal servers to an external network, where the communication is established towards the server, and the server's response is very small, less than 5 bytes. It looks for a specific pattern at the start of the content that matches certain byte sequences indicative of RMI traffic. This could potentially indicate unusual or unauthorized usage of RMI, which may involve.

## b. Kịch bản 3.2: Sử dụng Elastic Defend để giám sát thiết bị đầu cuối khi thiết bị mở những file mã độc.

- Ta sử dụng Elastic Security để tạo 1 Policy giám sát những thiết bị cuối Elastic Agent, sau đó ta thêm Elastic Defend Integration lên Policy này (trong ảnh là thiết bị Windows có tên DESKTOP-DDGUTK5 đã được thêm vào danh sách giám sát)

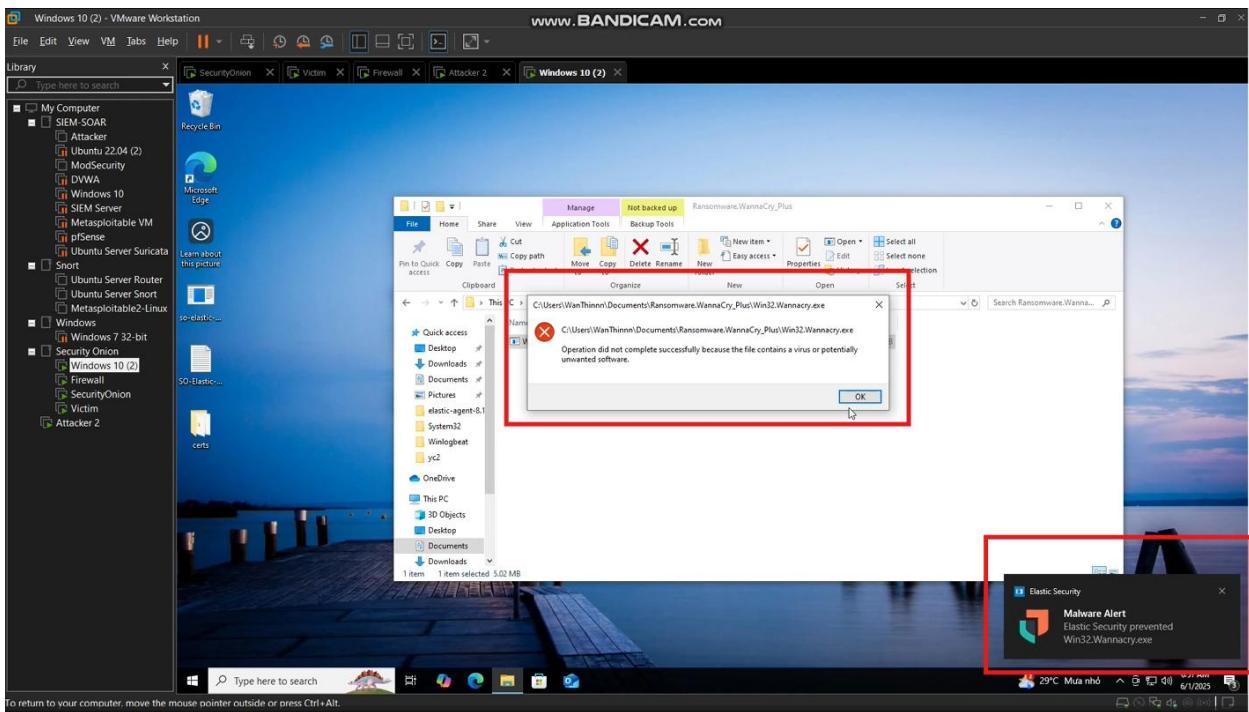
The screenshot shows the Kibana Fleet interface. At the top, there are tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. The Agents tab is selected. Below the tabs, there are two cards: "Ingest Overview Metrics" and "Agent Info Metrics". A search bar and filter buttons for Status (Healthy, Unhealthy, Updating, Offline, Inactive, Unenrolled), Tags, Agent policy, and Upgrade available are present. A table below lists three agents: DESKTOP-DDGUTK5, siem-so-local, and FleetServer-siem-so-local. Each row includes columns for Status, Host, Agent policy, CPU, Memory, Last activity, Version, and Actions. The DESKTOP-DDGUTK5 row shows it is healthy, running endpoints-initial rev.14, with 1.33% CPU usage, 244 MB memory, last active 10 seconds ago, and version 8.17.3. Buttons for "Upgrade available" and "Actions" are shown. At the bottom, there is a pagination control with "Rows per page: 20" and a link "https://siem-so-local/kibana/app/fleet/policies/so-grid-nodes\_general".

The screenshot shows the 'Agent details' tab for the host 'DESKTOP-DDGUTK5'. The 'Integrations' section lists several endpoint monitoring integrations, with 'elastic-defend-endpoints' highlighted by a red box.

- Bên máy Clients sau khi ta kết nối thành công với máy Security Onion, thì giao diện Windows Defender, phần Virus & threat protection được thay thế như sau:

The screenshot shows the Windows 10 desktop environment with the Microsoft Defender Antivirus interface open. The 'Virus & threat protection' section indicates that 'Elastic Security' is turned on. The interface also includes links for 'Windows Community videos', 'Have a question?', 'Who's protecting me?', and 'Change your privacy settings'.

- Mở thử mã độc Wana Cry Plus, thao tác liền bị chặn, file mã độc cũng được cách ly ngay lập tức, logs cảnh báo hiện lên Clients và cũng gửi về Server:



This screenshot shows the 'Logs' section of the Elastic Stack interface. The logs table has columns for 'Timestamp', 'event.dataset', 'component.id', 'Message', and 'error.message'. The 'Message' column contains detailed log entries from the 'elastic\_agent.endpoint\_security' component. One entry, highlighted with a red box, shows the system sending a diagnostic alert for the WannaCry file. The 'error.message' column also shows the alert message. The interface includes a search bar, dataset and log level filters, and a link to 'Open in Logs Explorer'.

Timestamp	event.dataset	component.id	Message	error.message
20:55:44.264	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] BulkQueueConsumer.cpp:3	
20:56:14.689	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] BulkQueueConsumer.cpp:3	
20:56:45.220	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] BulkQueueConsumer.cpp:3	
20:56:54.182	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] BulkQueueConsumer.cpp:3	
20:56:54.182	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] FilterLib.cpp:2929 Load	
20:56:54.182	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] FilterLib.cpp:2929 Load	
20:56:54.261	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] FileScore.cpp:1281 Send	
20:56:55.341	elastic_agent.endpoint_security		[elastic_agent.endpoint_security][info] BulkQueueConsumer.cpp:3	

#### **4.3.4.3. Đánh giá**

Dựa trên các kết quả thu được từ hai kịch bản kiểm thử và các phân tích ở trên, hệ thống Security Onion đã thể hiện được hiệu quả trong việc phát hiện, giám sát và phản ứng với các mối đe dọa an ninh mạng. Cụ thể, đánh giá được thực hiện dựa trên các khía cạnh sau:

##### **a. *Khả năng phát hiện mối đe dọa (Threat Detection)***

- Trong kịch bản 3.1 (Nmap Scan), Security Onion với Suricata đã phát hiện nhanh chóng và chính xác các hoạt động quét cổng từ máy Attacker (10.81.85.100) nhắm vào máy Victim (192.168.85.100). Các cảnh báo được hiển thị với các mức độ ưu tiên khác nhau, giúp quản trị viên dễ dàng nhận diện và phân tích các sự kiện bất thường.

- Trong kịch bản 3.2 (Elastic Defend), hệ thống đã phát hiện và chặn ngay lập tức hành vi mã độc (Wana Cry Plus) trên thiết bị đầu cuối. Elastic Defend không chỉ cách ly file mã độc mà còn gửi log cảnh báo về máy chủ Security Onion, thể hiện khả năng giám sát thời gian thực hiệu quả.

##### **b. *Tích hợp và tương quan dữ liệu (Log Correlation)***

- Hệ thống Filebeat và Winlogbeat hoạt động tốt trong việc thu thập và chuyển log từ các thiết bị đầu cuối về Security Onion. Việc tương quan giữa các sự kiện mạng (network alerts từ Suricata) và sự kiện trên thiết bị đầu cuối (endpoint events từ Sysmon, Elastic Defend) giúp phát hiện các hành vi đáng ngờ một cách toàn diện, ví dụ như hành vi mã hóa giả trong kịch bản fake-ransomware (T1486 – Data Encrypted for Impact).

- Dashboard trên Kibana cung cấp cái nhìn tổng quan và chi tiết về các sự kiện như “Intrusion Events”, “Zeek Conn”, và “Suricata Alerts”, hỗ trợ quản trị viên phân tích và ra quyết định nhanh chóng.

##### **c. *Quản lý tập trung và khả năng mở rộng (Centralized Management & Scalability)***

- Elastic Fleet Server trên Security Onion đã quản lý thành công các Elastic Agent trên các thiết bị đầu cuối, đảm bảo việc triển khai và áp dụng các chính sách bảo mật (Policy) được thực hiện mượt mà. Tính năng remote isolation cho phép cách ly thiết bị bị nhiễm mã độc từ xa, tăng cường khả năng phản ứng với sự cố.

- Hệ thống cho phép quản lý tập trung nhiều thiết bị đầu cuối, hiển thị trạng thái của các Agent (version, modules, enrollment status), giúp dễ dàng mở rộng quy mô giám sát trong môi trường doanh nghiệp.

#### **d. Hạn chế và đề xuất cải tiến**

- Mặc dù hệ thống hoạt động tốt, việc cấu hình ban đầu của Security Onion và các thành phần như Elastic Defend, Fleet Server yêu cầu kiến thức kỹ thuật nhất định. Cần có tài liệu hướng dẫn chi tiết hơn hoặc giao diện cấu hình đơn giản hơn để hỗ trợ người dùng mới.

- Trong môi trường lớn với số lượng thiết bị đầu cuối nhiều, cần tối ưu hóa hiệu suất của Fleet Server để đảm bảo khả năng xử lý đồng thời nhiều Agent.

- Nên tích hợp thêm các công cụ AI/ML để tự động hóa việc phân tích và phát hiện các mẫu hành vi bất thường, giúp giảm tải cho quản trị viên.

=> **Kết luận:** Hệ thống Security Onion, với sự kết hợp của Suricata, Zeek, Elastic Stack và Elastic Defend, đã chứng minh được khả năng phát hiện, giám sát và phản ứng hiệu quả với các mối đe dọa an ninh mạng. Việc tích hợp các công cụ này vào một nền tảng quản lý tập trung giúp tăng cường khả năng bảo mật và giảm thiểu rủi ro trong môi trường mạng. Tuy nhiên, để phù hợp với các môi trường phức tạp hơn, cần cải tiến thêm về giao diện người dùng và khả năng tự động hóa.

#### **4.3.4.2. Kết quả đạt được**

##### **a. Traffic Capture & Alert**

- Suricata trên Security Onion đã phát hiện thành công các cuộc **scan port** từ Kali (alert SBSCAN, portscan).
- Zeek ghi nhận các kết nối midstream (OTH), các kết nối SMB, Notice SSL invalid cert khi Windows client truy cập Internet.
- Elastic Stack (Kibana) hiển thị Dashboard “Intrusion Events”, “Zeek Conn”, “Suricata Alerts” kịp thời.

##### **b. Log Aggregation và Correlation**

- **Filebeat/Winlogbeat** trên Windows client đã chuyển log hệ thống (VD: Sysmon process create, Windows event) về SO, cho phép correlation giữa network alert (Suricata) và endpoint event (Process tạo file mã hóa giả).

- Khi chạy script fake-ransomware, Elastic Defend phát hiện hành vi “T1486 – Data Encrypted for Impact” (với rule “Possible Ransomware File Modification”), đồng thời Suricata alert phát hiện truy cập SMB/Azure?

##### **c. Quản lý tập trung (Fleet)**

- Elastic Fleet Server (port 8220) trên SO xử lý enrollment Agent từ Windows Client thành công, policies được push xuống (Defend, logs, metrics).
- Kibana hiển thị các máy enrolled, version Agent, modules, cho phép remote isolation nếu cần.

## CHƯƠNG 5. TÌM HIỂU CÁC GIẢI PHÁP LIÊN QUAN TRONG HỆ SINH THÁI CỦA SECURITY ONION

### 5.1. Giải pháp 1: Triển Khai Security Onion Trên Cloud (Cloud-Native SIEM)

Xem Video Demo tại: <https://youtu.be/W58uNYqI-xU?si=tZ9231kaII02CNko>

#### 5.1.1. Mục tiêu

Mục tiêu của giải pháp này là thiết lập một hệ thống giám sát an ninh mạng hiệu quả trên hạ tầng điện toán đám mây AWS, sử dụng Security Onion – một nền tảng mã nguồn mở SIEM (Security Information and Event Management) để thu thập, phân tích và đồng bộ log, traffic mạng và phát hiện xâm nhập.

Việc triển khai trên Cloud mang lại nhiều lợi ích:

- Linh hoạt trong việc mở rộng tài nguyên (scale-out/scale-up) khi lưu lượng mạng tăng cao.
- Tích hợp nhanh với các nguồn log và dịch vụ góc AWS như: CloudTrail, VPC Flow Logs, GuardDuty.
- Tối ưu chi phí: chỉ tạo instance khi cần, dễ tạo/làm mới/rollback nhanh hệ thống SOC khi cần.
- Phù hợp cho các lab nghiên cứu, mô hình dạy học hoặc triển khai SOC nhỏ vào môi trường doanh nghiệp vừa và nhỏ.

#### 5.1.2. Ngữ cảnh và Mô hình triển khai

##### 5.1.2.1. Ngữ cảnh

Trong bối cảnh doanh nghiệp sử dụng AWS làm hạ tầng chính, các thành phần như Web Server, hệ thống backend và tường lửa được triển khai trong VPC riêng. Tuy nhiên, doanh nghiệp muốn thêm một tầng giám sát truy cập mạng và hành vi truy cập từ xa vào hệ thống.

Giải pháp sử dụng EC2 instance cài đặt Security Onion trong chế độ all-in-one (bao gồm Suricata, Zeek, Elasticsearch, Kibana...), kèm theo hai giao diện mạng:

- Monitoring Interface: nhận mirrored traffic từ Web Server.
- Management Interface: giao diện truy cập giao diện SOC qua Bastion Host.

##### 5.1.2.2. Mô hình triển khai

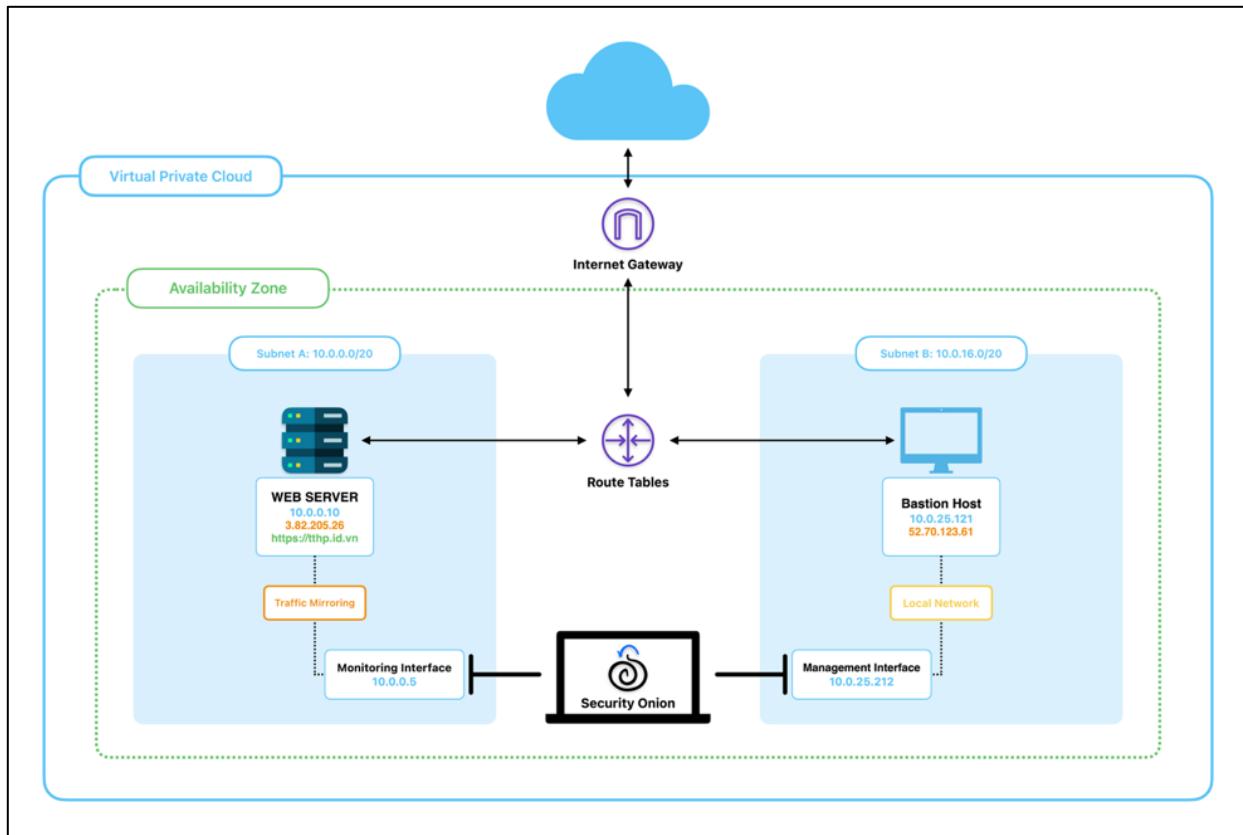
Mô hình sử dụng một VPC (10.0.0.0/16) chia làm hai subnet:

- Subnet A (10.0.0.0/20): Web Server + Monitoring Interface của Security Onion.
- Subnet B (10.0.16.0/20): Bastion Host + Management Interface của Security Onion.

Tổng quan bao gồm:

- Web Server hoạt động công khai qua IP public, xử lý yêu cầu từ người dùng.

- Bastion Host dùng để SSH nội bộ đến Security Onion.
- Security Onion được gắn hai ENI tương ứng với hai subnet, xử lý lưu lượng mirrored và cung cấp giao diện phân tích trên Kibana, Hunt,...



#### 5.1.2.3. Mô tả các thành phần trong hệ thống

STT	Thành Phần	Mô Tả
1	<b>Internet Gateway</b>	<ul style="list-style-type: none"> <li>- Được thiết lập mặc định khi tạo VPC và các Subnet.</li> <li>- Thiết bị gateway nối VPC với Internet, cho phép Web Server &amp; Bastion Host giao tiếp bên ngoài Internet.</li> </ul>
2	<b>Route Table</b>	<ul style="list-style-type: none"> <li>- Được thiết lập mặc định khi tạo VPC và các Subnet.</li> <li>- Routing nội bộ giữa các subnet và ra ngoài Internet, gán với cả Subnet A và Subnet B.</li> </ul>
3	<b>Web Server</b>	<ul style="list-style-type: none"> <li>- Ubuntu Server 24.04 LTS cấu hình t3.micro: 2 vCPU, 1 GB RAM, 256 GB SSD;</li> </ul>

		<ul style="list-style-type: none"> <li>- Public IP: 3.82.205.26, Private IP: 10.0.0.10;</li> <li>- Nhiệm vụ: Chạy dịch vụ web (Apache), là nguồn phát sinh traffic.</li> </ul>
4	<b>Bastion Host</b>	<ul style="list-style-type: none"> <li>- Ubuntu Server 24.04 LTS cấu hình t2.micro: 1 vCPU, 1 GB RAM, 128 GB SSD;</li> <li>- Public IP: 52.70.123.61, Private IP: 10.0.25.121;</li> <li>- Nhiệm vụ: Là điểm truy cập SSH từ xa và truy cập nội bộ đến Management Interface của SO.</li> </ul>
5	<b>Security Onion (SO)</b>	<ul style="list-style-type: none"> <li>- Được phát hành bởi Security Onion Solution, LLC.</li> <li>- OtherLinux 9 cấu hình t3a.2xlarge: 8 vCPU, 32 GB RAM, 512 GB SSD;</li> <li>- 2 ENI: Monitoring Interface (10.0.0.5) và Management Interface (10.0.25.212);</li> <li>- Cài đặt Standalone mode.</li> </ul>

### 5.1.3. Quy trình triển khai

#### 5.1.3.1. Thiết lập hạ tầng cơ bản AWS

- Tạo VPC mới: CIDR 10.0.0.0/16.
- Tạo Subnet A: 10.0.0.0/20 và Subnet B: 10.0.16.0/20.
- Tạo key pair để truy cập các EC2: ED25519.

#### 5.1.3.2. Khởi tạo các máy chủ EC2

- Security Onion:

+ Khởi chạy Security Onion 2 AMI từ AWS Marketplace với cấu hình t3a.2xlarge, 512 GB SSD;

+ Gán key pair được tạo trước đó để truy cập từ xa;

+ Tạo 2 network interface với Security Group:

- Monitoring Interface (Private IP: 10.0.0.5): Inbound và Outbound: cho phép tất cả lưu lượng;
- Management Interface (Private IP: 10.0.25.212): Inbound: chỉ cho phép SSH, HTTP, HTTPS từ Bastion Host (10.0.25.121).

+ Truy cập bằng SSH và tiến hành cài đặt với mode Standalone.

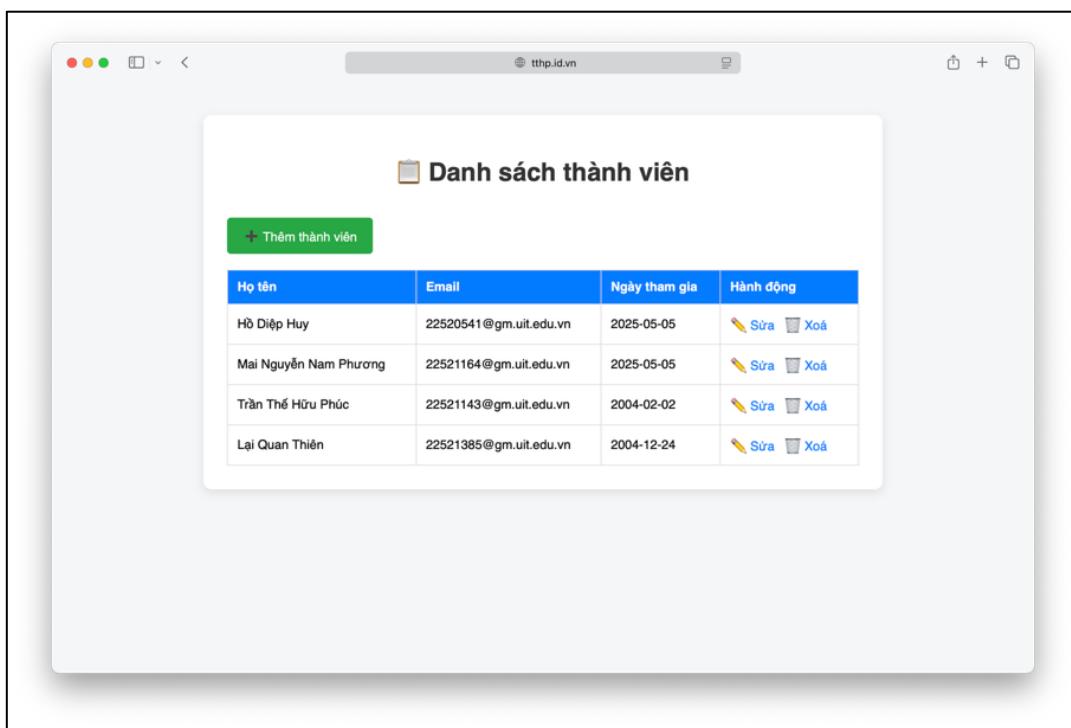
**- Bastion Host:**

- + Khởi chạy Ubuntu Server 24.04 LTS cấu hình t2.micro, 128 GB SSD;
- + Gán key pair được tạo trước đó để truy cập từ xa;
- + Tạo 1 network interface với Security Group:

- Public IP: 52.70.123.61, Private IP: 10.0.25.121;
- Inbound: Chỉ cho phép SSH từ máy tính cá nhân;
- Outbound: Cho phép tất cả lưu lượng.

**- Web Server:**

- + Khởi chạy Ubuntu Server 24.04 LTS cấu hình t3.micro, 256 GB SSD;
- + Gán key pair được tạo trước đó để truy cập từ xa;
- + Tạo 1 network interface với Security Group:
  - Public IP: 3.82.205.26, Private IP: 10.0.0.10;
  - Inbound: Cho phép HTTP, HTTPS từ tất cả nguồn truy cập và chỉ cho phép SSH từ máy tính cá nhân;
  - Outbound: Cho phép tất cả lưu lượng.
- + Tiến hành truy cập bằng SSH và triển khai website đơn giản.



#### **5.1.3.3. Thiết lập Traffic Mirroring**

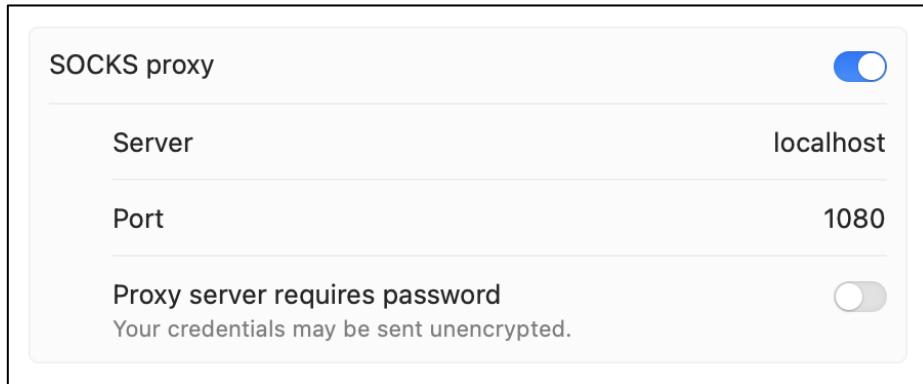
- Vào VPC Console => Traffic Mirroring.
- Tạo Mirror Target: gán ENI Monitoring của SO (10.0.0.5).
- Tạo Mirror Filter: full packet.
- Tạo Mirror Session: từ ENI Web Server đến Monitoring Interface của SO.

#### 5.1.3.4. Truy cập giao diện quản lý Security Onion

- Tạo SSH tunnel từ máy tính cá nhân đến Bastion Host:

**ssh -i {public-key} -D {SOCKs-proxy-port} {remote-host}@{remote-ip}**

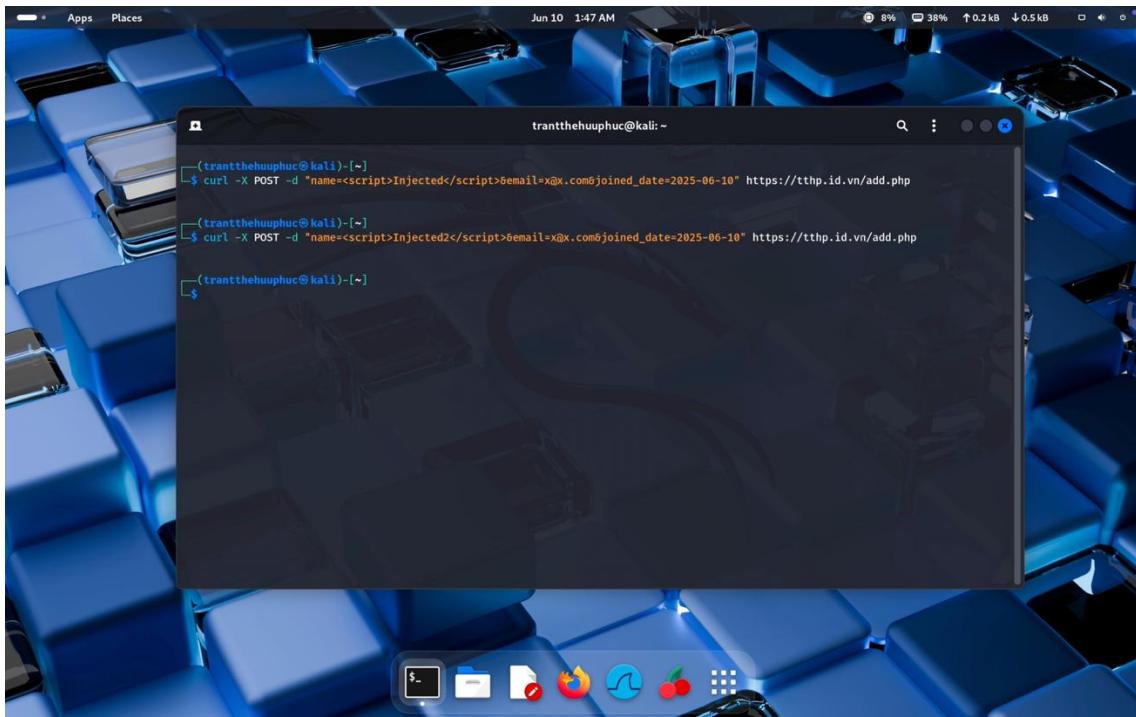
- Tạo SOCKs proxy trên máy tính cá nhân với **port** được chỉ định trong phần tạo SSH tunnel và server là **localhost**.



- Mở trình duyệt và truy cập <https://10.0.25.212> để truy cập giao diện quản lý Security Onion.

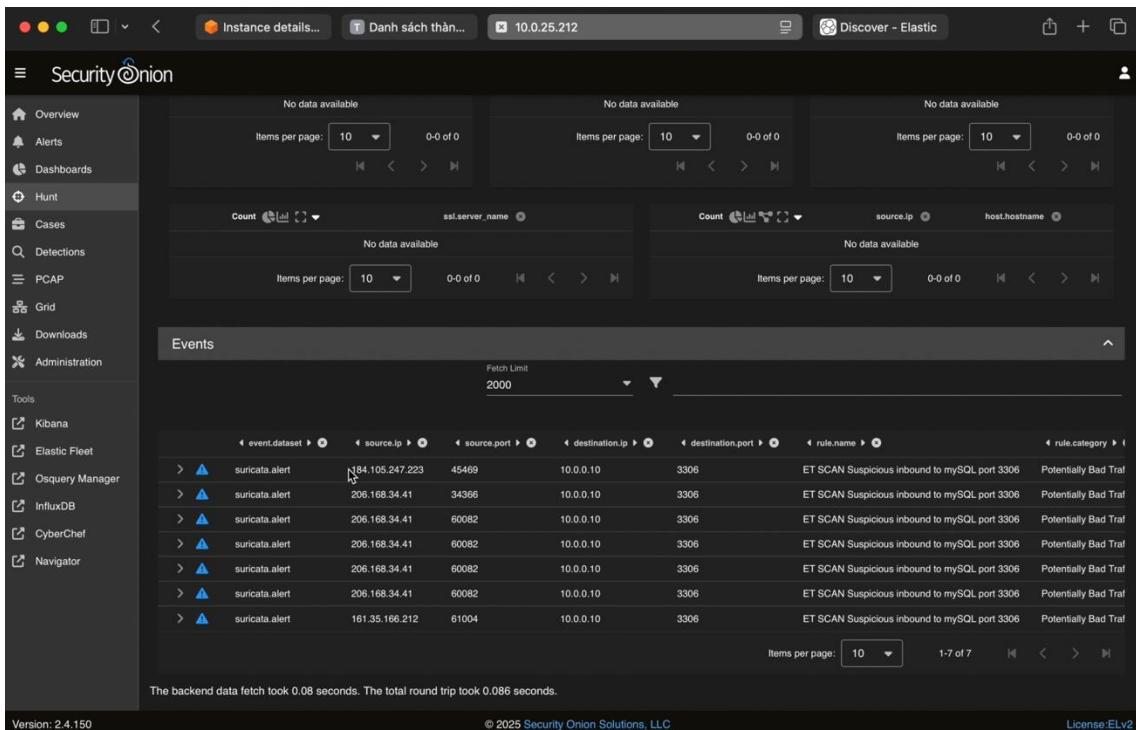
### 5.1.3.5. Kiểm thử

- Sinh traffic bằng cách truy cập nhiều lần vào website.
- Thực hiện tấn công SQL Injection từ máy ảo Kali Linux:



```
trantthehuuphuc@kali:~$ curl -X POST -d "name=<script>Injected</script>&email=x@x.com&joined_date=2025-06-10" https://tthp.id.vn/add.php
(trantthehuuphuc@kali)~$ curl -X POST -d "name=<script>Injected2</script>&email=x@x.com&joined_date=2025-06-10" https://tthp.id.vn/add.php
(trantthehuuphuc@kali)~$
```

- Cảnh báo trong Security Onion:



The screenshot shows the Security Onion interface. On the left, there's a sidebar with navigation links like Overview, Alerts, Dashboards, Hunt, Cases, Detections, PCAP, Grid, Downloads, Administration, Tools, Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, and Navigator. The main area has three search panels at the top: 'Instance details...', 'Danh sách thành...', and 'Discover - Elastic'. Below these are sections for 'Count' and 'source.ip' and 'host.hostname'. At the bottom, there's a large 'Events' section with a table of log entries. The table has columns for event.dataset, source.ip, source.port, destination.ip, destination.port, rule.name, and rule.category. The table shows multiple entries for 'suricata.alert' from various IP addresses (e.g., 184.105.247.223, 206.168.34.41) to port 3306, categorized as 'Potentially Bad Traf'.

event.dataset	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category
> suricata.alert	184.105.247.223	45469	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf
> suricata.alert	206.168.34.41	34366	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf
> suricata.alert	206.168.34.41	60082	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf
> suricata.alert	206.168.34.41	60082	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf
> suricata.alert	206.168.34.41	60082	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf
> suricata.alert	206.168.34.41	60082	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf
> suricata.alert	161.35.166.212	61004	10.0.0.10	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traf

#### **5.1.4. Kết quả và đánh giá**

##### **a. Ưu điểm**

- Mô hình linh hoạt, có thể mở rộng theo vùng (multi-AZ, multi-VPC).
- Không cần đầu tư phần cứng vật lý.
- Giao diện trực quan, hỗ trợ đầy đủ chức năng SOC.
- Tích hợp tốt với log hệ thống AWS.

##### **b. Nhược điểm**

- Chi phí lớn.
- Tốn tài nguyên máy chủ nếu traffic lớn (cần nhiều RAM/CPU).
- Traffic Mirroring có thể tốn băng thông và phát sinh chi phí.
- Cần người có kinh nghiệm quản lý Cloud + SIEM.

##### **c. Tính ứng dụng**

- Triển khai mô hình SOC mini phục vụ doanh nghiệp SME.
- Làm lab học tập, giảng dạy an ninh mạng.
- Đóng vai trò như hệ thống honeypot kiểm tra tấn công từ Internet.

##### **d. Kết luận**

Giải pháp triển khai Security Onion trên AWS Cloud là lựa chọn phù hợp để giám sát an ninh mạng hiện đại, đặc biệt trong bối cảnh chuyển đổi số. Với khả năng mở rộng, tích hợp tốt và dễ quản lý, giải pháp này cung cấp một nền tảng SOC mạnh mẽ, chuyên nghiệp cho các môi trường cloud-native.

## 5.2. Giải pháp 2: Threat Hunting với Security Onion & Threat Intelligence

Xem Video Demo tại: <https://youtu.be/oGU8ufvFnPQ?si=wVdn9oKTDtf2mBLm>

### 5.2.1. Mục tiêu

Mục tiêu của giải pháp này là mô phỏng quá trình Threat Hunting – săn tìm mối đe dọa – bằng cách sử dụng thông tin Threat Intelligence (IOC như IP/domain độc hại), tích hợp với hệ thống giám sát mạng **Security Onion**.

Lý do chọn kịch bản:

- Áp dụng khả năng phát hiện tấn công của Suricata thông qua IOC.
- Kết hợp Threat Intelligence và phân tích log trên Kibana để tìm kiếm hành vi tấn công.
- Mô phỏng tình huống thực tế: Attacker cố gắng brute force SSH và tải mã độc về từ server.

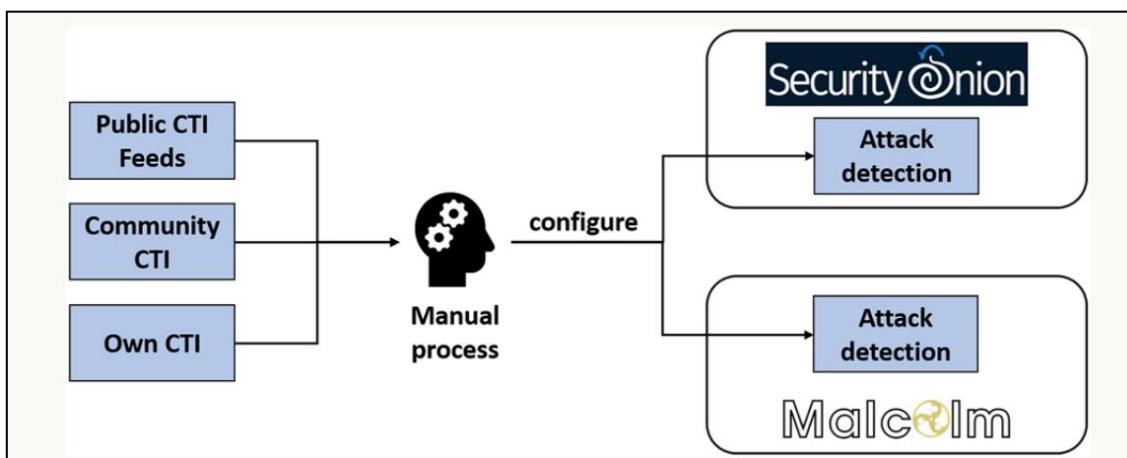
Qua đó, nhóm muốn thể hiện khả năng xây dựng hệ thống SOC có thể: Phát hiện sớm mối đe dọa dựa trên IOC và hỗ trợ phân tích viên trong quá trình threat hunting.

### 5.2.2. Ngữ cảnh và Mô hình triển khai

#### 5.2.2.1. Ngữ cảnh

- Một attacker từ bên ngoài mạng cố gắng brute-force vào SSH server và tải mã độc về.
- Máy nạn nhân (victim) ở đây chính là **Security Onion** để kiểm tra khả năng giám sát và phát hiện.
- IOC được thu thập từ nguồn công khai và tự động cập nhật vào Suricata.

#### 5.2.2.2. Mô hình triển khai



### **5.2.3. Quy trình triển khai**

#### **5.2.3.1. Thông tin phản ứng:**

- **Attacker (Kali Linux)**: 4 vCPU, 4GB RAM, 128GB disk
  - **Security Onion**: 4 vCPU, 8GB RAM, 60GB disk (yêu cầu tối thiểu để chạy Suricata + Elasticsearch + Kibana)
    - **Phần mềm ảo hóa**: VMware Workstation Pro (loại 2)

#### **5.2.3.2. Các bước thực hiện**

### Bước 1: Tự động tải IOC và sinh rule Suricata.

## Viết script Python để:

- Tải IOC từ <https://danger.rulez.sk/projects/bruteforceblocker/blist.php>
  - Sinh rule Suricata từ IOC
  - Reload Suricata với so-rule-update và so-suricata-restart

SecurityOnion3 - VMware Workstation www.BANDICAM.com

File Edit View VM Tabs Help

Attacker\_DAN SecurityOnion3

```
[root@securityonion kb5]# python3 generate_ioc_rules.py
[*] Downloading IOC feed...
[*] Saved IOC feed to /home/huy/kb5/ioc.txt
[*] Parsed 453 IPs from IOC
[*] Adding attacker IP 10.81.85.100 to IOC list
[*] Generating Suricata rules...
[*] Wrote 454 rules to /opt/so/rules/nids/suri/local.rules
[*] Running so-rule-update...
2025-06-03 11:44:39,125 - <DEBUG> - This is idstools-rulecat version 0.6.5: Python: 3.13.0 (main, Dec 3 2024, 02:26:48) |GCC 12.2.01
2025-06-03 11:44:39,126 - <INFO> - Forcing Suricata version to 7.8.3.
2025-06-03 11:44:39,126 - <INFO> - Fetching https://rules.emergingthreats.net/open/suricata-7.8.3/emerging.rules.tar.gz.
100% - 4945750/4945758 - <INFO> - Done.
```

To return to your computer, press Ctrl+Alt.

- Hình ảnh chạy thành công:

```
ID: surirulereload
Function: cmd.run
  Name: /usr/sbin/so-suricata-reload-rules >> /opt/so/log/suricata/reload.log 2>&1
  Result: True
  Comment: State was not run because none of the onchanges reqs changed
  Started: 11:45:34.080453
  Duration: 0.004 ms
  Changes:

ID: delete_so-suricata_so-status.disabled
Function: file.uncomment
  Name: /opt/so/conf/so-status/so-status.conf
  Result: True
  Comment: Pattern already uncommented
  Started: 11:45:34.080526
  Duration: 2.975 ms
  Changes:

ID: clean_suricata_eve_files
Function: cron.present
  Name: /usr/sbin/so-suricata-eve-clean > /dev/null 2>&1
  Result: True
  Comment: Cron /usr/sbin/so-suricata-eve-clean > /dev/null 2>&1 already present
  Started: 11:45:34.084198
  Duration: 5.0 ms
  Changes:

Summary for local
Succeeded: 25
Failed: 0
Total states run: 25
Total run time: 2.530 s
[+] Suricata restarted successfully
[root@securityonion kb5]#
```

- Hình ảnh rules được load thành công vào suricata:

```
(msg:"[T1] Malicious IP - 94.70.236.210 # 2025-05-10 16:18:33      3    2756219"; si d:1000442; rev:1;)
alert ip any any -> 172.234.162.31 # 2025-06-01 02:28:43      3    2755199 any
(msg:"[T1] Malicious IP - 172.234.162.31 # 2025-06-01 02:28:43      3    2755199 any
199"; sid:1000443; rev:1;)
alert ip any any -> 182.44.72.96 # 2025-05-30 22:36:12      3    2759583 any
(msg:"[T1] Malicious IP - 182.44.72.96 # 2025-05-30 22:36:12      3    2759583"; si d:1000444; rev:1;)
alert ip any any -> 172.104.241.98 # 2025-05-20 01:39:31      3    2755176 any
(msg:"[T1] Malicious IP - 172.104.241.98 # 2025-05-20 01:39:31      3    2755176
176"; sid:1000445; rev:1;)
alert ip any any -> 196.283.106.97 # 2025-05-24 08:16:03      3    2758185 any
(msg:"[T1] Malicious IP - 196.283.106.97 # 2025-05-24 08:16:03      3    2758185
185"; sid:1000446; rev:1;)
alert ip any any -> 49.0.85.146 # 2025-05-12 05:14:23      3    2756116 any (msg:"[T1]
11 Malicious IP - 49.0.85.146 # 2025-05-12 05:14:23      3    2756116"; sid:100044
7; rev:1;)
alert ip any any -> 95.182.115.26 # 2025-06-02 23:46:46      3    2768503 any
(msg:"[T1] Malicious IP - 95.182.115.26 # 2025-06-02 23:46:46      3    2768503"; si d:1000448; rev:1;)
alert ip any any -> 23.236.143.222 # 2025-05-22 23:18:05      3    2754888 any
(msg:"[T1] Malicious IP - 23.236.143.222 # 2025-05-22 23:18:05      3    2754888
888"; sid:1000449; rev:1;)
alert ip any any -> 107.173.37.111 # 2025-06-03 04:19:05      3    2758810 any
(msg:"[T1] Malicious IP - 107.173.37.111 # 2025-06-03 04:19:05      3    2758810
810"; sid:1000450; rev:1;)
alert ip any any -> 103.205.60.32 # 2025-05-29 21:21:27      3    2758010 any
(msg:"[T1] Malicious IP - 103.205.60.32 # 2025-05-29 21:21:27      3    2758010"; si d:1000451; rev:1;)
alert ip any any -> 134.199.236.87 # 2025-05-14 18:49:16      3    2756999 any
(msg:"[T1] Malicious IP - 134.199.236.87 # 2025-05-14 18:49:16      3    2756999
999"; sid:1000452; rev:1;)
alert ip any any -> 8.209.214.165 # 2025-05-09 20:10:17      3    2756047 any
(msg:"[T1] Malicious IP - 8.209.214.165 # 2025-05-09 20:10:17      3    2756047"; si d:1000453; rev:1;)
alert ip any any -> 10.81.85.100 any (msg:"[T1] Malicious IP - 10.81.85.100"; sid:1000454; rev:1;)
[root@securityonion kb5]#
```

## Bước 2: Tấn công brute-force SSH + tải mã độc

- Dùng Kali SSH brute-force vào Security Onion (dùng hydra).
- Trên attacker: chạy server python3 -m http.server 80 chứa file malware giả lập.
- Trên Security Onion: dùng curl tải file từ attacker.

The terminal window shows the following session:

```
(hohuy㉿kali)-[~]
$ cd kb5/
(hohuy㉿kali)-[~/kb5]
$ ls
attack_demo.py  hydra.restore
(hohuy㉿kali)-[~/kb5]
$ python3 attack_demo.py
[*] Bắt đầu tấn công SSH brute-force với hydra (chạy nén)...
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-03 08:22:49
[WARNING] Restoredfile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:i:p:i:14344399), -3586100 tries per task
[DATA] attacking ssh://[10.81.85.10]:22/
[*] Tao file malware giả và khởi chạy web server...
[*] Web server đang chạy trên http://10.81.85.10:80/
[STATUS] 36.00% (4/11) tasks completed, 44344363 to do in 6640:55h, 4 active
[*] Thực hiện tải file malware giả từ attacker sang target...
Warning: Permanently added '10.81.85.10' (ED25519) to the list of known hosts.
#####
#####
### UNAUTHORIZED ACCESS PROHIBITED ###
#####
#####
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total Spent   Left Speed
0       0     0       0      0      0 0 ---:---:---:---:---:--- 010.81.85.10  -- [03/Jun/2025 08:23:53] "GET /badfile.exe HTTP/1.1" 200 -
100  20 100  20 0 2000 0 ---:---:---:---:---:--- 2000
[*] Đã tải file malware giả thành công.
[*] Demo tấn công hoàn tất.

(hohuy㉿kali)-[~/kb5]
$ The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Bước 3: Quan sát cảnh báo trên Kibana

Truy vấn:

- alert.signature: "\*SimpleHTTP\*" để bắt cảnh báo từ rule Suricata
- source.ip: <IP\_attacker> để lọc log theo attacker

Ta thấy có các alert về SimpleHTTP hay SSH...

The Kibana interface displays a table of alerts from the Security Onion log. The table includes columns for Timestamp, event.dataset, rule.name, event.severity\_label, and event\_data.event.dataset. The alerts listed are primarily suricata.alert entries, mostly of medium severity, related to various SSH and SimpleHTTP events.

Timestamp	event.dataset	rule.name	event.severity_label	event_data.event.dataset
2025-06-03 19:23:52.448 +07:00	suricata.alert	ET-HUNTING curl User-Agent to Dotted Quad	medium	
2025-06-03 19:23:52.448 +07:00	suricata.alert	ET INFO Executable Download from dotted-quad Host	medium	
2025-06-03 19:23:52.448 +07:00	suricata.alert	ET INFO Python SimpleHTTP ServerBanner	low	
2025-06-03 19:23:52.438 +07:00	suricata.alert	[T1] Malicious IP - 10.81.85.100	low	
2025-06-03 19:23:52.286 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:52.236 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:52.227 +07:00	suricata.alert	[T1] Malicious IP - 10.81.85.100	low	
2025-06-03 19:23:52.227 +07:00	suricata.alert	ET SCAN Potential SSH Scan OUTBOUND	medium	
2025-06-03 19:23:43.057 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:43.041 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:43.015 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:43.014 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:42.995 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:42.988 +07:00	suricata.alert	[T1] Malicious IP - 10.81.85.100	low	
2025-06-03 19:23:42.969 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:42.969 +07:00	suricata.alert	ET INFO Server Responded with Vulnerable OpenSSH Version (CVE-2024-6409)	medium	
2025-06-03 19:23:42.961 +07:00	suricata.alert	[T1] Malicious IP - 10.81.85.100	low	
2025-06-03 19:23:42.961 +07:00	suricata.alert	[T1] Malicious IP - 10.81.85.100	low	
2025-06-03 19:23:42.961 +07:00	suricata.alert	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	high	

## Bước 4: Kiểm tra IOC match

Xác nhận Suricata đã tạo alert với IP trong IOC nếu attacker nằm trong danh sách



### 5.2.4. Kết quả và đánh giá

#### a. Ưu điểm

- Cho thấy khả năng phát hiện tấn công nhờ cập nhật IOC.
- Hỗ trợ threat hunting thủ công bằng Kibana dễ dàng.
- Có thể mở rộng để tích hợp nhiều nguồn Threat Intelligence.

#### b. Nhược điểm

- Chưa phát hiện được payload cụ thể (nếu chỉ dựa vào IP).
- Rule chưa đủ sâu để bắt các hành vi ẩn/tấn công tinh vi.

#### c. Tính ứng dụng thực tế

- Mô hình này có thể áp dụng vào các tổ chức nhỏ hoặc doanh nghiệp vừa muôn triển khai SOC nội bộ.
- Có thể tích hợp thêm log từ endpoint, firewall để tăng khả năng giám sát.

#### d. Khó khăn khi làm trên môi trường ảo hóa loại 2 (VMware Workstation):

- Hiệu năng hạn chế, đặc biệt với Security Onion cần tài nguyên lớn.
- Giới hạn về networking (host-only đôi khi bị lỗi nếu không cấu hình đúng).
- Giới hạn đồng bộ thời gian, dẫn đến log không chính xác về timestamp.

## CHƯƠNG 6. ĐÁNH GIÁ CHUNG

### 6.1. Ưu điểm nổi bật của Security Onion

#### 6.1.1. Tích hợp toàn diện các công cụ an ninh mạng

Security Onion kết hợp nhiều công cụ mã nguồn mở mạnh mẽ như Zeek, Suricata, Elasticsearch và Kibana, tạo nên một giải pháp giám sát an ninh mạng toàn diện.

- Không cần triển khai và cấu hình riêng lẻ từng công cụ
- Tiết kiệm thời gian và công sức cho quản trị viên

#### 6.1.2. Chi phí thấp

Security Onion là mã nguồn mở, miễn phí sử dụng

- Phù hợp với các tổ chức có ngân sách hạn chế
- Giảm chi phí đầu tư vào các giải pháp thương mại đắt đỏ

#### 6.1.3. Khả năng mở rộng linh hoạt

Hỗ trợ triển khai theo các mô hình Standalone, Hybrid và Distributed, phù hợp với nhu cầu và quy mô của các tổ chức khác nhau

- Phù hợp với mọi quy mô tổ chức, từ nhỏ đến lớn
- Dễ dàng mở rộng khi nhu cầu tăng lên

#### 6.1.4. Giao diện trực quan và khả năng phân tích mạnh mẽ

Với Kibana, người dùng có thể trực quan hóa dữ liệu, tạo biểu đồ và báo cáo, giúp việc phân tích và đồng thời nó còn cung cấp khả năng giám sát an ninh mạng (NSM), phát hiện xâm nhập (IDS/IPS), và quản lý log tập trung (SIEM)

- Phát hiện sớm các mối đe dọa và phản ứng kịp thời
- Cung cấp dữ liệu chi tiết để điều tra sâu

#### 6.1.5. Cộng đồng hỗ trợ mạnh mẽ và tài liệu phong phú

Là một dự án mã nguồn mở phổ biến, Security Onion có một cộng đồng người dùng và nhà phát triển đông đảo, cung cấp tài liệu phong phú và hỗ trợ kỹ thuật

- Dễ dàng tìm kiếm tài liệu, hướng dẫn, và hỗ trợ kỹ thuật
- Thường xuyên được cập nhật và cải tiến

## **6.2. Các hạn chế và thách thức**

### **6.2.1. Độ phức tạp trong triển khai và quản lý**

Việc triển khai và cấu hình các thành phần của Security Onion có thể phức tạp, đòi hỏi kiến thức chuyên sâu về an ninh mạng và các công cụ liên quan

- Khó khăn cho người mới bắt đầu hoặc tổ chức không có chuyên gia bảo mật
- Cần thời gian để làm quen và tối ưu hóa hệ thống

### **6.1.2. Yêu cầu tài nguyên hệ thống cao**

Để xử lý và lưu trữ lượng lớn dữ liệu mạng, Security Onion cần cấu hình phần cứng mạnh mẽ, đặc biệt trong môi trường mạng lớn

- Chi phí đầu tư phần cứng có thể tăng lên đáng kể
- Khó triển khai trong môi trường hạn chế tài nguyên

### **6.1.3. Khó khăn trong việc scale hệ thống**

Khi lưu lượng mạng tăng lên, việc mở rộng hệ thống (đặc biệt là Elasticsearch) có thể phức tạp

- Cần tối ưu hóa cấu hình để đảm bảo hiệu suất
- Quản lý nhiều cảm biến và máy chủ đòi hỏi công sức và thời gian

### **6.1.4. Khả năng tùy chỉnh hạn chế**

Mặc dù tích hợp nhiều công cụ, việc tùy chỉnh sâu các thành phần có thể gặp khó khăn do sự phụ thuộc lẫn nhau và cấu trúc phức tạp của hệ thống

- Phụ thuộc vào cộng đồng và tài liệu tự học
- Khó khăn khi gặp sự cố nghiêm trọng cần hỗ trợ nhanh chóng hoặc tùy chỉnh theo nhu cầu cá nhân gặp khó khăn

### **6.1.5. Cảnh báo nhiễu (False Positives)**

Các công cụ như Suricata và Zeek có thể tạo ra nhiều cảnh báo không chính xác

- Cần điều chỉnh rule và cấu hình để giảm thiểu cảnh báo nhiễu
- Đòi hỏi kiến thức để phân biệt giữa cảnh báo thật và giả

## CHƯƠNG 7. KẾT LUẬN

### 7.1. Tóm tắt giá trị của Security Onion

Security Onion là một nền tảng mã nguồn mở được thiết kế để giám sát và bảo vệ an ninh mạng. Nó tích hợp nhiều công cụ mạnh mẽ như Zeek, Suricata, ELK Stack, giúp các tổ chức phát hiện, phân tích và phản ứng nhanh chóng với các mối đe dọa an ninh mạng. Khả năng triển khai linh hoạt và giao diện trực quan giúp Security Onion trở thành một giải pháp hiệu quả cho việc giám sát an ninh mạng.

### 7.2. Triển vọng ứng dụng trong tương lai

Với sự tăng của các mối đe dọa an ninh mạng, nhu cầu về các giải pháp giám sát và phản ứng nhanh chóng ngày càng tăng. Security Onion, với khả năng tích hợp và mở rộng, có triển vọng được áp dụng rộng rãi trong các tổ chức để tăng cường khả năng bảo vệ mạng. Việc liên tục cập nhật và cải tiến các công cụ tích hợp sẽ giúp Security Onion duy trì vị thế là một giải pháp hàng đầu trong lĩnh vực an ninh mạng. Các giải pháp phát triển bao gồm

- Tích hợp AI/ML để nâng cao khả năng phân tích
- Hỗ trợ điện toán đám mây và container hóa
- Tăng cường khả năng tự động hóa
- Mở rộng hỗ trợ cho các thiết bị IoT và OT
- Cải thiện hiệu suất và khả năng mở rộng
- Tăng cường bảo mật và tuân thủ

### 7.3. Kết luận chung

Security Onion đã và đang chứng minh là một giải pháp giám sát an ninh mạng mạnh mẽ, linh hoạt, và tiết kiệm chi phí. Với những ưu điểm vượt trội như tích hợp đa công cụ, khả năng phát hiện sớm các mối đe dọa, và cộng đồng hỗ trợ mạnh mẽ, Security Onion là lựa chọn hàng đầu cho các tổ chức cần hệ thống NSM toàn diện.

Trong tương lai, với sự phát triển của AI/ML, điện toán đám mây, và IoT, Security Onion hứa hẹn sẽ tiếp tục được cải tiến và mở rộng, đáp ứng nhu cầu ngày càng cao về an ninh mạng trong bối cảnh kỹ thuật số hiện đại.

## DANH MỤC TÀI LIỆU THAM KHẢO

- [1] **Security Onion Solutions**, “Security Onion Documentation v2.4”, Security Onion Documentation, Online. <https://docs.securityonion.net> [Truy cập 2/2025].
- [2] **Burks, Doug & Bejtlich, Richard**, “Security Onion Documentation (Paperback Edition)”, Security Onion Solutions, May 11, 2020. <https://www.amazon.com/Security-Onion-Documentation-Doug-Burks/dp/B088GGHDV6> [Truy cập 6/2025].
- [3] **Ackermann T., Karch M., Kippe J.**, “Integration of Cyber Threat Intelligence into Security Onion and Malcolm for the use case of industrial networks”, *Automatisierungstechnik*, 2023. DOI: 10.1515/auto-2023-0057.  
[https://www.researchgate.net/publication/373790735\\_Integration\\_of\\_Cyber\\_Threat\\_Intelligence\\_into\\_Security\\_Onion\\_and\\_Malcolm\\_for\\_the\\_use\\_case\\_of\\_industrial\\_networks](https://www.researchgate.net/publication/373790735_Integration_of_Cyber_Threat_Intelligence_into_Security_Onion_and_Malcolm_for_the_use_case_of_industrial_networks) [Truy cập ngày 5/2025].
- [4] **Barraza Tudela, K. N. & Patilla, H. J.**, “Security Onion as a Network Auditing Tool at the San Cristóbal de Huamanga National University”, *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 3, 2025.  
[https://thesai.org/Downloads/Volume16No3/Paper\\_14-Security\\_Onion\\_as\\_a\\_Network\\_Auditing\\_Tool.pdf](https://thesai.org/Downloads/Volume16No3/Paper_14-Security_Onion_as_a_Network_Auditing_Tool.pdf) [Truy cập ngày 2/2025].
- [5] **Heikkinen, R.**, “Information Security Case Study with Security Onion at Kajaani UAS Datacentre Laboratory”, Bachelor Thesis, Kajaani University of Applied Sciences, 2018.  
[https://www.theseus.fi/bitstream/handle/10024/145362/Heikkinen\\_Raimo.pdf](https://www.theseus.fi/bitstream/handle/10024/145362/Heikkinen_Raimo.pdf) [Truy cập ngày 2/2025].

---- HẾT ----