

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

**SINH VIÊN THỰC TẬP: VƯƠNG ĐÌNH THANH NGÂN**  
**LỚP: NT215.O11.ATCL**

**BÁO CÁO THỰC TẬP DOANH NGHIỆP**  
**GIÁM SÁT AN TOÀN THÔNG TIN**

**TP. HỒ CHÍ MINH, THÁNG 10 NĂM 2023**

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

**BÁO CÁO THỰC TẬP DOANH NGHIỆP**  
**GIÁM SÁT AN TOÀN THÔNG TIN**

<b>Công ty thực tập</b>	<b>: Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT</b>
<b>Người phụ trách</b>	<b>: Phan Văn Hảo</b>
<b>GVHD</b>	<b>: Nghi Hoàng Khoa</b>
<b>Thực tập sinh</b>	<b>: Vương Đình Thanh Ngân</b>

**TP. HỒ CHÍ MINH, THÁNG 10 NĂM 2023**

## LỜI CẢM ƠN

Đầu tiên, em xin gửi lời cảm ơn sâu sắc đến Công ty cổ phần dịch vụ Công nghệ Tin học HPT và các anh chị của phòng HSOC đã tạo điều kiện để em có một kỳ thực tập năm 2023 thật ý nghĩa và thành công.

Quá trình thực tập tại **Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT** đã giúp em học hỏi được rất nhiều kiến thức mới và tiếp cận với các công nghệ phổ biến mà công ty sử dụng. Trong quá trình thực tập vì kinh nghiệm còn hạn chế, em chắc chắn đã gặp một số khó khăn và thiếu sót, vì vậy em mong nhận được sự góp ý từ các anh để em có thể hoàn thiện bản thân và hoàn thành công việc tốt hơn.

Em xin gửi lời cảm ơn chân thành đến thầy Nghi Hoàng Khoa – người hướng dẫn đã hết sức tận tâm, nhiệt tình hỗ trợ và hết lòng giúp đỡ cho em trong suốt quá trình thực tập. Kính chúc thầy tràn đầy sức khỏe, thành công và luôn cháy bỏng ngọn lửa nghề nghiệp để dìu dắt thêm thật nhiều thế hệ sinh viên trong tương lai.

Cuối cùng, em xin chúc Công ty HPT và các anh chị trong phòng HSOC ngày càng phát triển vững mạnh để tiếp tục đem đến những sản phẩm chất lượng cao và dẫn đầu về công nghệ. Bên cạnh đó em cũng xin chúc UIT ngày càng thành công trong sự nghiệp giáo dục và đào tạo.

**TP. Hồ Chí Minh, ngày    tháng 10 năm 2023**

**(Họ và tên)**

Vương Đình Thanh Ngân

# MỤC LỤC

LỜI CẢM ƠN.....	3
DANH MỤC HÌNH ẢNH.....	6
DANH MỤC VIẾT TẮT .....	8
CHƯƠNG I: GIỚI THIỆU VỀ CÔNG TY .....	9
1.1 Giới thiệu chung.....	9
1.2 Lĩnh vực hoạt động.....	9
1.3 Sản phẩm và giải pháp.....	9
1.4 Liên hệ công ty .....	10
CHƯƠNG II: GIỚI THIỆU CHƯƠNG TRÌNH THỰC TẬP .....	11
2.1 Tổng quan về chương trình thực tập.....	11
2.2 Nhật ký thực tập.....	11
CHƯƠNG III: NỘI DUNG THỰC TẬP .....	12
3.1. Cơ sở lý thuyết: .....	12
3.1.1. Tổng quan về SOC .....	12
3.1.2. Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập IDPS .....	13
3.1.3. Hệ thống SIEM.....	14
3.1.4. Hệ thống ELK.....	14
3.1.5. Hệ thống Suricata .....	16
3.1.6. Windows Event Logs .....	16
3.1.7. n8n.....	17
3.1.8. TheHive .....	
3.2 Triển khai thực nghiệm .....	18
3.2.1. Triển khai Suricata .....	19
3.2.2 Triển khai ELK .....	20
3.2.3 Cài đặt Sysmon log và Winlogbeat trên Windows .....	23
3.2.4 Đặt rules trên Suricata .....	26
3.2.6 Trực quan hoá dữ liệu, tạo Dashboard và rules trên ELK .....	30
3.2.7 Ingest Pipelines trên ELK.....	34

3.2.7 Triển khai n8n .....	37
3.2.7 Triển khai TheHive .....	33
CHƯƠNG IV: KẾT QUẢ ĐẠT ĐƯỢC .....	44
4.1 Kết quả đạt được .....	44
4.2 Những khó khăn và hạn chế .....	44

## DANH MỤC HÌNH ẢNH

Hình a	<i>Cơ cấu của SOC</i>
Hình 2	<i>Cách IDS hoạt động</i>
Hình 3	<i>Hệ thống ELK</i>
Hình 3	<i>Mô hình tổng quan</i>
Hình 4	<i>Cấu hình file yaml cho Suricata</i>
Hình 5	<i>Cấu hình file yaml cho Suricata</i>
Hình 6	<i>Khởi động Elasticsearch service</i>
Hình 7	<i>Khởi động kibana service</i>
Hình 8	<i>Chỉnh sửa cấu hình của filebeat</i>
Hình 9	<i>Khởi động filebeat</i>
Hình 10	<i>Tạo file sysmon-config.xml như trong hình ở thư mục cùng với cái file sysmon.exe</i>
Hình 11	<i>Sysmon log đã cài đặt thành công trên Windows 10</i>
Hình 12	<i>Cài đặt winlogbeat</i>
Hình 13	<i>Cấu hình các thông số liên quan cho winlogbeat trong file yml</i>
Hình 14	<i>Sửa đổi phần setup Kibana, thêm địa chỉ ip của máy và port Kibana</i>
Hình 15	<i>Sửa đổi phần setup Kibana, thêm địa chỉ ip của máy và port Elasticsearch</i>
Hình 16	<i>Kiểm tra winlogbeat đã hoạt động hay chưa với câu lệnh test config -c</i>
Hình 17	<i>Đường dẫn chứa các rules của Suricata</i>
Hình 18	<i>Rule DoS cho Suricata</i>
Hình 19	<i>Rule nmap cho Suricata</i>
Hình 20	<i>Sử dụng công cụ hping tấn công tới máy victim</i>
Hình 21	<i>Sử dụng công cụ nmap tấn công tới máy victim</i>
Hình 22	<i>Đường dẫn chứa log của Suricata</i>
Hình 23	<i>Log của tấn công DoS trong file fast.log</i>
Hình 24	<i>Log của tấn công nmap trong file fast.log</i>
Hình 25	<i>Cấu hình filebeat</i>

Hình 26	<i>Log của Suricata được hiển thị trên elk với index filebeat</i>
Hình 27	<i>Bật audit log trên máy Windows 10</i>
Hình 28	<i>Log được thu từ máy Windows, bao gồm cả audit log hiển thị trên elk với index winlogbeat</i>
Hình 29	<i>Sử dụng Dashboard có sẵn xem alert là Suricata alert overview để trực quan hoá dữ liệu</i>
Hình 30	<i>Dashboard tự tạo</i>
Hình 31	<i>Một số loại rules mà ELK hỗ trợ</i>
Hình 32	<i>Các rules đã tạo</i>
Hình 33	<i>Alert security thu được sau khi chạy các rules trên</i>
Hình 34	<i>Pipelines có sẵn và create Pipeline</i>
Hình 35	<i>Giao diện sau khi tạo Pipeline</i>
Hình 36	<i>Index và id của một log trong phần discovery</i>
Hình 37	<i>Test Pipelines</i>
Hình 38	<i>Cài đặt SQLite cho n8n</i>
Hình 39	<i>Hoàn thành cài đặt n8n</i>
Hình 40	<i>Đăng nhập vào n8n thông qua port 5678</i>
Hình 41	<i>Workflow đơn giản trên n8n</i>
Hình 42	<i>Đăng nhập vào TheHive</i>
Hình 43	<i>Giao diện TheHive</i>

## **DANH MỤC VIẾT TẮT**

CNTT	<i>Công Nghệ Thông Tin</i>
SOC	<i>Security Operations Center</i>
ELK	<i>Elasticsearch - Logstash - Kibana</i>
SIEM	<i>Security Information and Event Management</i>
IDPS	<i>Intrusion Detection/Prevention System</i>
CIA	<i>Confidentiality-Integrity-Availability</i>
DoS	<i>Denial of Service attack</i>



## **CHƯƠNG I: GIỚI THIỆU VỀ CÔNG TY**

### **1.1. Giới thiệu chung**

Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT được thành lập vào ngày 13 tháng 01 năm 1995. HPT hiện nay đã phát triển khắp Việt Nam và từng bước vươn ra thị trường thế giới: Trụ sở chính tại TP.HCM, Chi nhánh tại Hà Nội, Văn phòng đại diện tại Đà Nẵng và Campuchia. Với triết lý kinh doanh bằng năng lực, sự tận tụy với khách hàng, hợp tác chặt chẽ với các hãng CNTT hàng đầu thế giới, HPT đã thúc đẩy các doanh nghiệp và tổ chức trên khắp Việt Nam ứng dụng giải pháp, dịch vụ CNTT tiên tiến trên thế giới, mang lại hiệu quả thiết thực cho tất cả các lĩnh vực mũi nhọn của nền kinh tế cũng như hỗ trợ công tác quản lý của các cơ quan Nhà nước.

Ban lãnh đạo công ty gồm:

Chủ tịch Hội đồng Quản trị	: Ông Ngô Vi Đồng
Phó Chủ tịch Hội đồng Quản trị	: Bà Đinh Hà Duy Trinh
Tổng Giám Đốc	: Ông Đinh Hà Duy Linh
Phó Tổng Giám Đốc	: Ông Nguyễn Quyền

### **1.2. Lĩnh vực hoạt động**

- Giải pháp và Dịch vụ Tích hợp hệ thống
- Giải pháp và Dịch vụ Phần mềm
- Giải pháp và Dịch vụ An toàn thông tin
- Giải pháp và Dịch vụ mang lại giá trị gia tăng cho khách hàng

### **1.3. Sản phẩm và giải pháp**

- SAALEM - Giải pháp số hóa quy trình nghiệp vụ tín dụng
- HPT SmartNOC – Giải pháp giám sát hệ thống CNTT toàn diện, tùy biến cao
- Giải pháp quản lý vận hành kho
- HPT Cyber Intelligence – Phần mềm quản lý thông tin tình báo
- HCapollo – Giải pháp giám sát và cảnh báo ATTT
- HCriffin – Giải pháp giám sát lớp mạng
- HPT Mavex – Nền tảng sẵn lòng các mối đe dọa

- Giải pháp truy xuất & xác thực nguồn gốc

#### *1.4. Liên hệ công ty*

- Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT (HPT Vietnam Corporation)
- Địa chỉ: Lô E2a3 Đường D1, Khu Công nghệ Cao, Phường Long Thạnh Mỹ, TP. Thủ Đức, TP.HCM.
- Website: <https://www.hpt.vn>

## CHƯƠNG II: GIỚI THIỆU CHƯƠNG TRÌNH THỰC TẬP

### 2.1. Tổng quan về chương trình thực tập

Đối tượng tham gia: Các sinh viên đang theo học ngành công nghệ thông tin, có kiến thức cơ bản về bảo mật và mạng máy tính.

Mục đích: Trang bị cho thực tập sinh các kiến thức cơ bản về sản phẩm và các giải pháp bảo mật của công ty HPT.

Vị trí thực tập: SOC - Analyst

### 2.2. Nhật ký thực tập

Thời gian thực tập: 21/8/2023 - 21/10/2023

Tuần	Thời gian	Nội dung
Tuần 1, 2	21/8 - 3/9	Tìm hiểu về ELK Tìm hiểu về Suricata Dựng mô hình thực nghiệm ELK và Suricata
Tuần 3, 4	4/9 - 17/9	Triển khai ELK Triển khai Suricata Thực hiện tấn công trên máy Suricata Thu log, đọc hiểu log
Tuần 5, 6	18/9 - 1/10	Tấn công trên máy victim Viết rules trên ELK Tạo Dashboard Trực quan hoá dữ liệu
Tuần 7, 8	2/10 - 20/10	Tìm hiểu n8n, TheHive Dựng n8n, TheHive

## CHƯƠNG III: NỘI DUNG THỰC TẬP

### 3.1. Cơ sở lý thuyết

#### 3.1.1. Tổng quan về SOC

##### a. Giới thiệu chung về SOC

SOC (Security Operations Center) là một giải pháp dịch vụ bao gồm dịch vụ giám sát an ninh 24/7 sử dụng công nghệ SIEM (Security Information and Event Management), giúp người dùng nhận biết các cuộc tấn công thông tin, các mối đe dọa nhắm mục tiêu, quản lý lỗ hổng thông tin và ứng cứu kịp thời các sự cố quan trọng.

##### b. Chức năng của SOC

Phát hiện mối đe dọa bảo mật: SOC chịu trách nhiệm theo dõi các mạng và hệ thống máy tính của tổ chức để phát hiện các mối đe dọa bảo mật, bao gồm các cuộc tấn công, sự xâm nhập, phần mềm độc hại, và hành vi đáng ngờ.

Phân tích và ứng phó: Khi một mối đe dọa được phát hiện, nhóm chuyên gia của SOC tiến hành phân tích để hiểu rõ hơn về tấn công, xác định mục tiêu, và đưa ra các biện pháp ứng phó như cách ngăn chặn tấn công và khắc phục hậu quả.

Giám sát hệ thống và mạng: SOC liên tục theo dõi các sự kiện và log từ các hệ thống và thiết bị mạng để phát hiện sự không bình thường và các dấu hiệu của tấn công.

Báo cáo và ghi lại: SOC tạo ra các báo cáo chi tiết về các sự kiện bảo mật và lưu trữ thông tin liên quan đến các sự kiện này để hỗ trợ việc phân tích sau này và tuân thủ quy định bảo mật.

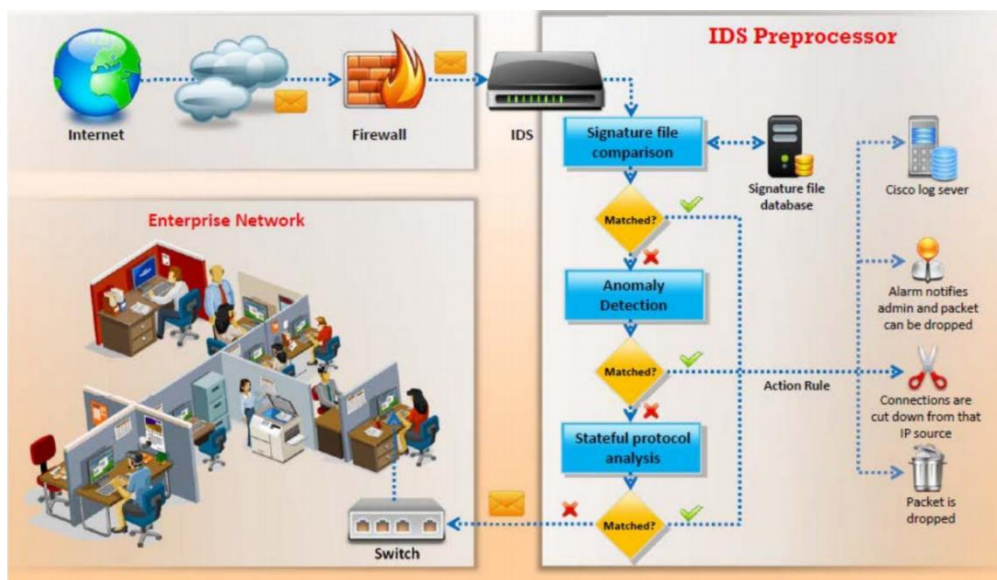


Hình a: Cơ cấu của SOC

### 3.1.2. Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập IDPS

Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập (IDPS) chủ yếu tập trung vào xác định các sự cố có thể xảy ra, ghi nhận các thông tin liên quan, cố gắng ngăn chặn và báo cáo cho các quản trị viên bảo mật. Mục tiêu là đảm bảo an toàn cho mạng hoặc hệ thống máy tính theo bộ ba CIA.

Cách IDS hoạt động:



Hình 2: Cách IDS hoạt động

Cách IPS ngăn chặn xâm nhập:

+ IPS dừng hoạt động tấn công: Ngắt kết nối (mạng) hoặc phiên làm việc đang bị sử dụng để tấn công. Chặn truy cập vào mục tiêu (hoặc các máy có khả năng là mục tiêu) từ tài khoản người dùng, địa chỉ IP hoặc các yếu tố tấn công khác. Chặn tất cả các truy cập đến host, dịch vụ, ứng dụng hoặc các tài nguyên khác là mục tiêu

+ IPS thay đổi môi trường bảo mật: Tái cấu hình một thiết bị mạng (ví dụ tường lửa, router, switch) để chặn truy cập từ attacker hoặc truy cập đến mục tiêu. Và các lỗ hổng đang có trên host

+ IPS thay đổi nội dung của hoạt động tấn công. Loại bỏ hoặc thay thế những phần độc hại của tấn công để nó thành bình thường. Hoạt động như proxy và bình thường hoá các yêu cầu được gửi đến (đóng gói lại payloads của yêu cầu, bỏ các thông tin header...)

### *3.1.3. Hệ thống SIEM*

Hệ thống SIEM (Security Information and Event Management) là một công cụ hoặc nền tảng dùng để thu thập, phân tích, và báo cáo về thông tin và sự kiện liên quan đến bảo mật từ nhiều nguồn khác nhau trong một hệ thống hoặc mạng. Mục tiêu chính của SIEM là cung cấp một cái nhìn toàn diện về bảo mật hệ thống, giúp người quản trị và nhóm an ninh mạng theo dõi và bảo vệ hệ thống khỏi các mối đe dọa và tấn công mạng.

Các bước triển khai SIEM là:

- + Thu thập dữ liệu
- + Phân tích sự kiện
- + Báo cáo và cảnh báo
- + Tích hợp và ứng phó
- + Một số nhà cung cấp SIEM như: splunk, IBM QRadar, Exabeam...

### *3.1.4. Hệ thống ELK*

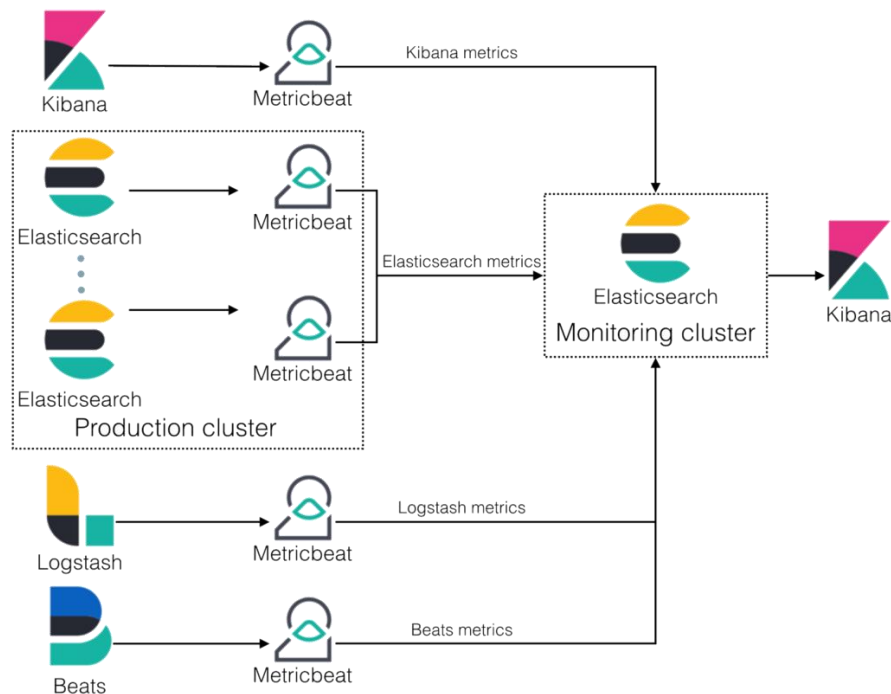
#### a. Khái niệm ELK

ELK tích hợp từ bộ các công cụ Elasticsearch, Logstash, Kibana, bên cạnh đó còn có Beat

Elasticsearch: là hệ thống tìm kiếm và phân tích dữ liệu mã nguồn mã mở với ưu điểm là tìm kiếm nhanh chóng, phân tích văn bản đầy đủ, phân tán và mở rộng, tích hợp linh hoạt, thời gian thực.

Logstash: thu thập, xử lý và chuyển đổi dữ liệu log, ghi vào Elasticsearch

Kibana: là một giao diện người dùng đồ họa cho Elasticsearch để quản lý, thống kê log, đọc thông tin từ Elasticsearch.



Hình 3: Hệ thống ELK

⇒ Điểm mạnh của ELK là khả năng thu thập, hiển thị, truy vấn theo thời gian thực, đáp ứng truy vấn một lượng dữ liệu cực lớn.

#### b. Hoạt động và ứng dụng ELK

Hoạt động	Ứng dụng
Raw log ban đầu sẽ được đưa đến Logstash bằng một số cách như gửi UDP request chứa log tới URL của Logstash Ở Logstash sẽ thêm thông tin về thời gian, IP,.. và ghi xún Elasticsearch	Thu thập và xử lý thông tin, phản ứng, giám sát liên tục, phân tích sự cố và điều tra Netflix, Adobe, Cisco....
Người dùng vào URL của Kibana, Kibana sẽ đọc thông tin log trong Elasticsearch, hiển thị lên giao diện cho người dùng query và xử lý.	Công ty HPT có sử dụng giải pháp HCapollo phát triển từ nền tảng ELF

### 3.1.5. Hệ thống Suricata

Suricata là một hệ thống phát hiện xâm nhập và ngăn chặn mạng mã nguồn mở do Open Information Security Foundation (OISF) phát triển. Nó được thiết kế để giám sát lưu lượng mạng và phát hiện các hoạt động độc hại, chẳng hạn như xâm nhập mạng, nhiễm malware và các mối đe dọa bảo mật khác. Suricata nổi tiếng với kiến trúc đa luồng và hiệu suất cao, cho phép xử lý lưu lượng mạng tốc độ cao một cách hiệu quả. Nó hỗ trợ một loạt các giao thức, bao gồm Ethernet, IP, TCP, UDP, HTTP, ...

### 3.1.6. Windows Event Logs

#### a. Windows Event Logs là gì?

Windows Event Logs (Nhật ký Sự kiện Windows) là một phần quan trọng của hệ điều hành Windows của Microsoft. Chúng được sử dụng để ghi lại các sự kiện, hoạt động và thông tin liên quan đến hệ thống máy tính chạy Windows. Mục đích chính của Windows Event Logs là giúp quản trị viên hệ thống và nhà phát triển xác định và theo dõi sự kiện quan trọng, lỗi, hoặc thông tin khác liên quan đến hoạt động của hệ thống.

Các sự kiện trong Windows Event Logs được chia thành ba loại chính:

- + Sự kiện hệ thống (System Events): Ghi lại thông tin về hoạt động hệ thống tổng quan, chẳng hạn như khởi động, tắt máy, lỗi phần cứng, và thông tin về thiết bị.
- + Sự kiện ứng dụng (Application Events): Ghi lại thông tin về các ứng dụng và dịch vụ cụ thể trên hệ thống, bao gồm cả lỗi và thông báo từ các ứng dụng.
- + Sự kiện bảo mật (Security Events): Ghi lại thông tin về các hoạt động bảo mật trên hệ thống, như đăng nhập, đăng xuất, và quyền truy cập tệp tin và tài nguyên hệ thống.

#### b. Một số Windows Event ID

Windows Event ID	Mô tả
Windows Security Log Event ID 4624: An account was successfully	Sự kiện này phát sinh khi phiên đăng nhập được tạo (trên máy đích). Nó tạo trên máy tính đã được truy cập, nơi phiên được tạo. Đây là một sự kiện có giá trị cao vì nó ghi lại từng và mọi nỗ lực đăng nhập thành công vào máy tính cục bộ bất kể loại đăng nhập, vị trí của người dùng hoặc loại tài khoản.



logged on	Ngoài ra, có thể liên kết sự kiện này với các sự kiện đăng xuất 4634 và 4647 bằng ID đăng nhập.
Windows Security Log Event ID 4625: An account failed to log on	Sự kiện này được ghi lại mọi lỗi đăng nhập. Nó tạo ra trên máy tính nơi nỗ lực đăng nhập được thực hiện, ví dụ: nếu nỗ lực đăng nhập được thực hiện trên máy trạm của người dùng, thì sự kiện sẽ được ghi lại trên máy trạm này. Sự kiện này có thể được tạo ra trên bộ điều khiển miền, máy chủ thành viên và máy trạm. Đây là một sự kiện hữu ích vì nó ghi lại từng lần đăng nhập không thành công vào máy tính cục bộ bất kể loại đăng nhập, vị trí của người dùng hoặc loại tài khoản.

### 3.1.7. n8n

n8n là một hệ thống quản lý quy trình làm việc (workflow automation) mã nguồn mở (open-source), cho phép bạn tự động hóa các quy trình công việc và tích hợp các ứng dụng khác nhau trong một quy trình liên tục, giảm thiểu nỗ lực và mang tính sẵn sàng mọi lúc. Tên gọi "n8n" được viết tắt từ "nodemation," trong đó "node" đề cập đến các thành phần xây dựng quy trình. Liên quan tới n8n ta có:

+ Node: Trong n8n, node là một thành phần cơ bản của quy trình làm việc. Mỗi node đại diện cho một công việc cụ thể hoặc một tác vụ, chẳng hạn như gửi email, tạo bản ghi trong cơ sở dữ liệu, gửi thông báo Slack, và nhiều tác vụ khác. Các node có thể được sắp xếp và kết nối lại với nhau để tạo ra một quy trình làm việc.

+ Workflow: Workflow là tổng thể của các node được kết nối lại với nhau để thực hiện một quy trình hoặc một chuỗi các tác vụ liên quan. Trong n8n, bạn có thể xây dựng và tùy chỉnh các workflow theo nhu cầu của bạn.

+ Trigger: Trigger là một loại đặc biệt của node, được sử dụng để kích hoạt (trigger) quy trình làm việc khi có một sự kiện cụ thể xảy ra. Ví dụ, trigger có thể được thiết lập để bắt đầu quy trình khi có một email mới đến hoặc khi có một tệp tin mới được tải lên.

+ Integrations: n8n có khả năng tích hợp với nhiều dịch vụ và ứng dụng bên ngoài. Bạn có thể sử dụng các node tích hợp sẵn để kết nối với các dịch vụ như Gmail, Slack, Dropbox, Google Sheets, và nhiều ứng dụng khác.

#### 3.1.8. TheHive

TheHive là một Nền tảng ứng phó sự cố bảo mật (SIRP) nguồn mở, có thể mở rộng và hợp tác được thiết kế để hỗ trợ quản lý và phân tích các sự cố bảo mật. Được phát triển chủ yếu cho Nhóm ứng phó sự cố bảo mật máy tính (CSIRT) và Trung tâm điều hành bảo mật (SOC), TheHive hợp lý hóa và nâng cao quy trình xử lý sự cố bằng cách cung cấp một nền tảng tập trung để quản lý trường hợp, phân công nhiệm vụ và cộng tác theo thời gian thực. TheHive cung cấp các tính năng trong quy trình SOC như:

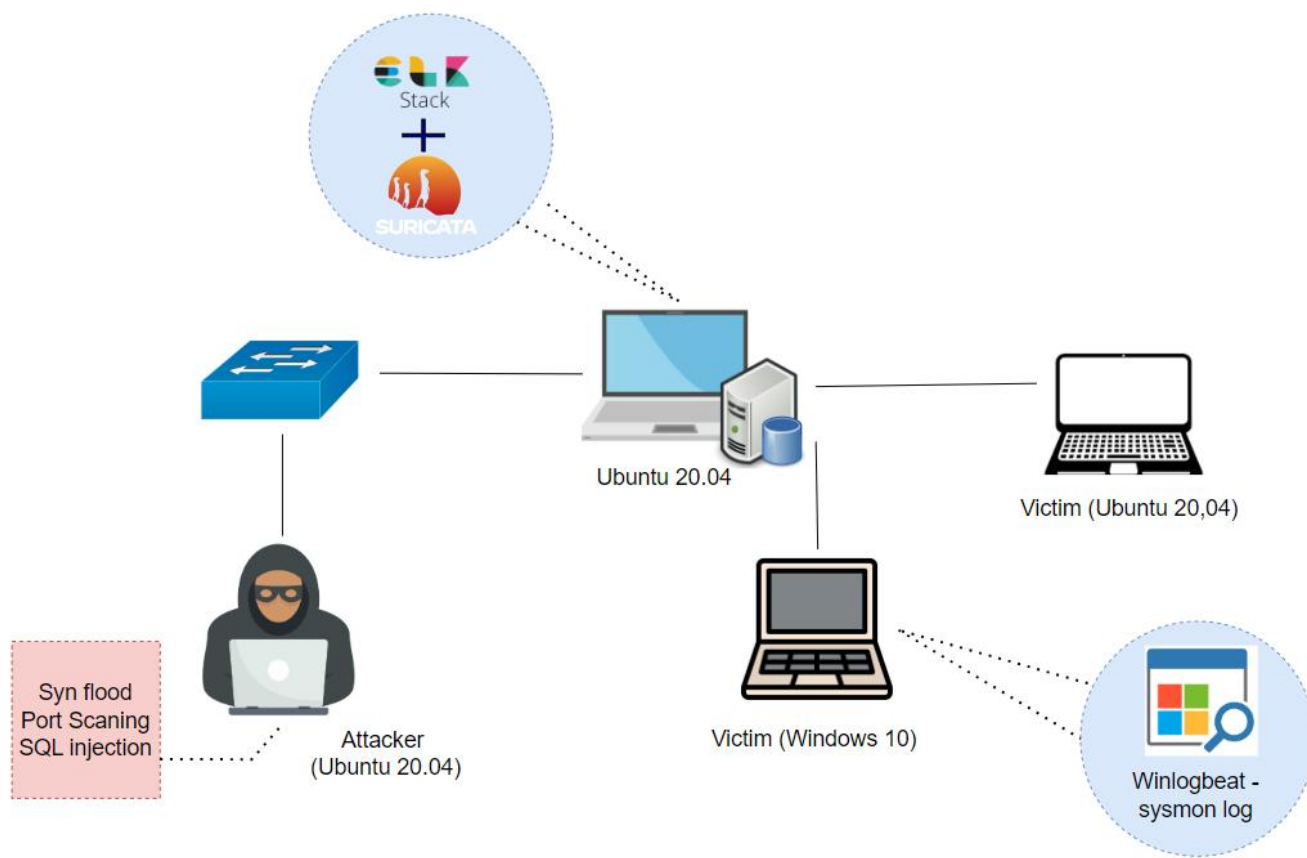
+ Quản lý sự cố: TheHive cho phép đội ngũ SOC tạo ra một hồ sơ cho mỗi sự cố bảo mật, bao gồm thông tin về sự cố, thời gian, mức độ nghiêm trọng, và những người chịu trách nhiệm.

+ Tích hợp và tự động hóa: TheHive tích hợp với nhiều công cụ và nguồn thông tin khác, cho phép tự động hóa quy trình phân tích và ứng phó với sự cố bảo mật. Nó có khả năng gửi thông tin đến các công cụ phân tích và tạo tác vụ tự động dựa trên quy tắc.

+ Quản lý công việc: TheHive cho phép gán các công việc cụ thể cho từng sự cố và theo dõi tiến trình thực hiện công việc đó. Điều này giúp đảm bảo rằng mọi người trong đội SOC đều biết mình đang làm gì và cần làm gì tiếp theo.

+ Báo cáo và thống kê: TheHive cung cấp khả năng tạo báo cáo và thống kê về tình trạng và tiến độ của các sự cố bảo mật, giúp đội SOC đánh giá hiệu suất và hiệu quả của họ.

### 3.2. Triển khai thực nghiệm



Hình 3: Mô hình tổng quan

Tên máy	Dịch vụ/ công cụ	IP
Attacker	Hping3	192.168.40.129
Suricata-ELK	ElasticSearch, Logstash, Kibana, Filebeat, Suricata, TheHive, n8n	192.168.40.128
Windows 10	Winlogbeat, Sysmon Log	192.168.40.131
Ubuntu 20.04	User	192.168.40.132

### 3.2.1. Triển khai Suricata

Sử dụng máy Ubuntu 20.04 với RAM 6GB

+ Bước 1: Cài đặt Suricata

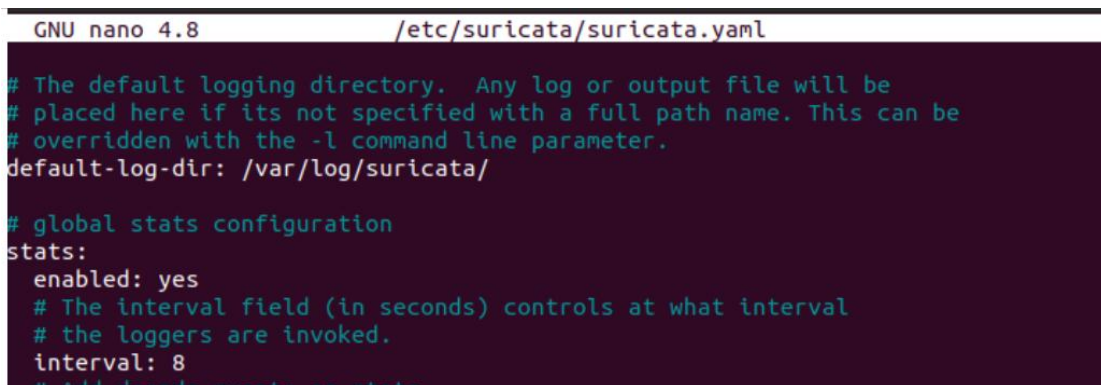
```
# sudo add-apt-repository ppa:oisf/suricata-stable
```

```
# sudo apt install suricata
```

```
# sudo systemctl stop suricata.service
```

## + Bước 2: Cấu hình Suricata

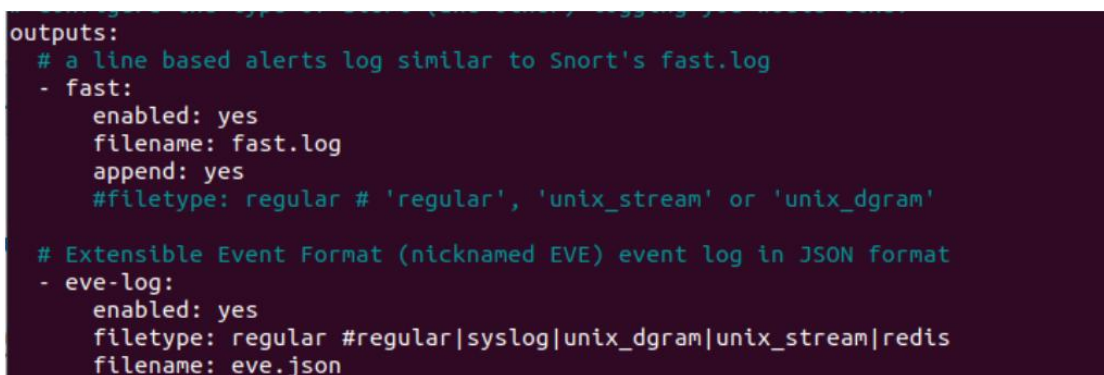
# sudo nano /etc/suricata/suricata.yaml



```
GNU nano 4.8 /etc/suricata/suricata.yaml
# The default logging directory. Any log or output file will be
# placed here if its not specified with a full path name. This can be
# overridden with the -l command line parameter.
default-log-dir: /var/log/suricata/

# global stats configuration
stats:
  enabled: yes
  # The interval field (in seconds) controls at what interval
  # the loggers are invoked.
  interval: 8
# Add decode events as state
```

Hình 4: Cấu hình file yaml cho Suricata



```
outputs:
# a line based alerts log similar to Snort's fast.log
- fast:
  enabled: yes
  filename: fast.log
  append: yes
  #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

# Extensible Event Format (nicknamed EVE) event log in JSON format
- eve-log:
  enabled: yes
  filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
  filename: eve.json
```

Hình 5: Chuyển enabled thành yes, chọn filename có thể là fast.log hoặc eve.json....

## 3.2.2. Triển khai ELK

### a. Cài đặt Elasticsearch

#### + Bước 1: Cài đặt các chương trình hỗ trợ ELK stack:

# sudo apt-get install openjdk-8-jdk -y

#### + Bước 2: Cài đặt Elasticsearch và Kibana

# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

# sudo apt update

#### + Bước 3: Cấu hình Elasticsearch

```
# sudo nano /etc/elasticsearch/elasticsearch.yml
```

Đổi `network.bind_host` thành địa chỉ ip của máy, thêm `discovery.type: single-node` và `xpack.security.enabled: true` và cuối file `yml`

+ Bước 4: Cấu hình lại Firewall

```
# sudo ufw allow in on eth1
```

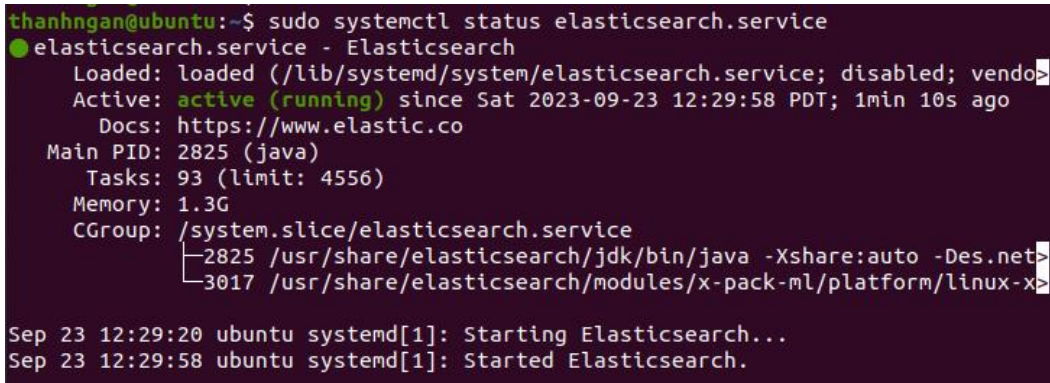
```
# sudo ufw allow out on eth1
```

+ Bước 5: Cấu hình Elastic password

```
# cd /usr/share/elasticsearch/bin
```

```
# sudo ./elasticsearch-setup-passwords auto
```

+ Bước 6: Start ElasticSearch



```
thanhngan@ubuntu:~$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; disabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-09-23 12:29:58 PDT; 1min 10s ago
     Docs: https://www.elastic.co
   Main PID: 2825 (java)
    Tasks: 93 (limit: 4556)
   Memory: 1.3G
   CGroup: /system.slice/elasticsearch.service
           └─2825 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net
           └─3017 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/java

Sep 23 12:29:20 ubuntu systemd[1]: Starting Elasticsearch...
Sep 23 12:29:58 ubuntu systemd[1]: Started Elasticsearch.
```

Hình 6: Khởi động Elasticsearch service

## b. Cài đặt Kibana

+ Bước 1: Cài đặt Kibana

```
#sudo apt install elasticsearch kibana
```

+ Bước 2: Cấu hình Kibana

```
#cd /usr/share/kibana/bin/
```

```
#sudo ./kibana-encryption-keys generate -q
```

Copy lại 3 dòng bỏ vào file `/etc/kibana/kibana.yml`:

```
xpack.encryptedSavedObjects.encryptionKey:
```

```
3418ae4b3bcd7d416829b7ad521583bb
```

```
xpack.reporting.encryptionKey: 9fe876934ac0db590ffb4ca314902f03
```

```
xpack.security.encryptionKey: ac0e536c87418925b32f080fd86aafc0
```

Set server.host: "your\_private\_ip" trong file kibana.yml thành địa chỉ ip của máy

+ Bước 3: Định cấu hình thông tin xác thực Kibana

#sudo ./kibana-keystore thêm elasticsearch.username

#sudo ./kibana-keystore thêm elasticsearch.password

+ Bước 4: Start Kibana

```
thanhngan@ubuntu:~$ sudo systemctl status kibana.service
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; disabled; vendor prese
   Active: active (running) since Sat 2023-09-23 12:30:30 PDT; 1min 3s ago
     Docs: https://www.elastic.co
   Main PID: 3113 (node)
    Tasks: 11 (limit: 4556)
   Memory: 615.5M
    CGroup: /system.slice/kibana.service
           └─3113 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bi

Sep 23 12:30:30 ubuntu systemd[1]: Started Kibana.
Sep 23 12:30:31 ubuntu kibana[3113]: Kibana is currently running with legacy Op
```

Hình 7: Khởi động kibana service

### c. Cài đặt Filebeat

+ Bước 1: Cài đặt Filebeat

#curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

#echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a  
/etc/apt/sources.list.d/elastic-7.x.list

#sudo apt update

#sudo apt install filebeat

+ Bước 2: Cấu hình Filebeat

#sudo nano /etc/filebeat/filebeat.yml

Thay đổi host: "your\_private\_ip:5601" thành ip của máy và ở phần Elasticsearch Output trong filebeat ta cấu hình lại host, username và password cho giống với bên ElasticSearch



```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.40.128:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "71m1cbexx442qCR3U54"

# ----- Logstash Output -----
```

Hình 8: Chính sửa cấu hình của filebeat

+ Bước 3: Start Filebeat

```
#sudo filebeat modules enable suricata
```

```
#sudo filebeat setup
```

```
thanhngan@ubuntu:~$ sudo systemctl status filebeat.service
● filebeat.service - Filebeat sends log files to Logstash or directly to Elastic
   Loaded: loaded (/lib/systemd/system/filebeat.service; disabled; vendor pre
   Active: active (running) since Sat 2023-09-23 12:30:38 PDT; 5s ago
     Docs: https://www.elastic.co/beats/filebeat
    Main PID: 3130 (filebeat)
      Tasks: 11 (limit: 4556)
     Memory: 116.3M
    CGroup: /system.slice/filebeat.service
            └─3130 /usr/share/filebeat/bin/filebeat --environment systemd -c />

Sep 23 12:30:38 ubuntu systemd[1]: Started Filebeat sends log files to Logstash>
Sep 23 12:30:41 ubuntu filebeat[3130]: 2023-09-23T12:30:41.084-0700      INFO>
Sep 23 12:30:41 ubuntu filebeat[3130]: 2023-09-23T12:30:41.090-0700      INFO>
```

Hình 9: Khởi động filebeat

### 3.2.3. Cài đặt Sysmon log và Winlogbeat trên Windows

#### a. Cài đặt Sysmon log trên Windows 10

+ Bước 1: Tải file sysmon từ <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>,

sau đó tạo một file sysmon-config.xml với nội dung như trong đường dẫn

<https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>

Eula.txt	6/27/2023 4:54 PM	Text Document	8 KB
Sysmon.exe	6/27/2023 4:55 PM	Application	8,246 KB
Sysmon64.exe	6/27/2023 4:55 PM	Application	4,443 KB
Sysmon64a.exe	6/27/2023 4:55 PM	Application	4,873 KB
sysmon-config.xml	9/12/2023 3:46 PM	XML Document	122 KB

Hình 10: Tạo file sysmon-config.xml như trong hình ở thư mục cùng với cái file sysmon.exe

+ Bước 2: Chạy lệnh Sysmon64.exe -accepteula -i sysmon-config.xml

```
C:\Users\windows10\Desktop\Sysmon>Sysmon64.exe -accepteula -i sysmon-config.xml

System Monitor v15.0 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Hình 11: Sysmon log đã cài đặt thành công trên Windows 10

#### b. Cài đặt Winlogbeat trên Windows 10

+ Bước 1: Tải file Winlogbeat ở <https://www.elastic.co/downloads/beats/winlogbeat> và chạy các lệnh sau để cài đặt Winlogbeat làm dịch vụ Windows:

```
C:\Windows\system32>cd C:\Program Files\Winlogbeat
C:\Program Files\Winlogbeat>.\install-service-winlogbeat.ps1
```

Hình 12: Cài đặt winlogbeat

+ Bước 2: Cấu hình winlogbeat bằng cách mở file winlogbeat.yml



```

# The supported keys are name (required), tags, fields, fields_under_root,
# forwarded, ignore_older, level, event_id, provider, and include_xml. Please
# visit the documentation for the complete details of each option.
# https://go.es.io/WinlogbeatConfig
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

)
  - name: Security
    processors:
      - script:
        lang: javascript
        id: security
        file: ${path.home}/module/security/config/winlogbeat-security.js

  - name: Microsoft-Windows-Sysmon/Operational
    processors:
      - script:
        lang: javascript
        id: sysmon
        file: ${path.home}/module/sysmon/config/winlogbeat-sysmon.js

#===== Elasticsearch template settings =====

```

Hình 13: Cấu hình các thông số liên quan cho winlogbeat trong file yml

### + Bước 3: Kết nối tới ELK

```

#===== Kibana =====

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.40.128:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

```

Hình 14: Sửa đổi phần setup Kibana, thêm địa chỉ ip của máy và port Kibana

```
#===== Outputs =====

# Configure what output to use when sending the data collected by the beat.

#----- Elasticsearch output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.40.128:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  username: "elastic"
  password: "71m1cbehxx442qCR3U54"

#----- Logstash output -----
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]
```

Hình 15: Sửa đổi phần setup Kibana, thêm địa chỉ ip của máy và port Elasticsearch

+ Bước 4: Kiểm tra xem tệp cấu hình có đúng về mặt cú pháp không và khởi động winlogbeat với start-Service winlogbeat

```
C:\Program Files\Winlogbeat>.winlogbeat.exe test config -c .\winlogbeat.yml -e
2023-09-23T21:48:52.614+0700 INFO instance/beat.go:610 Home path: [C:\Program Files\Winlogbeat] Config path: [C:\Program Files\Winlogbeat] Data path: [C:\Program Files\Winlogbeat\data] Logs path: [C:\Program Files\Winlogbeat\logs]
2023-09-23T21:48:52.636+0700 INFO instance/beat.go:618 Beat ID: 0fe0b5af-22cd-4876-85f4-dc18fba47de2
2023-09-23T21:48:52.734+0700 INFO [beat] instance/beat.go:941 Beat info {"system_info": {"beat": {"path": {"config": "C:\\Program Files\\Winlogbeat", "data": "C:\\Program Files\\Winlogbeat\\data", "home": "C:\\Program Files\\Winlogbeat", "logs": "C:\\Program Files\\Winlogbeat\\logs"}, "type": "winlogbeat", "uuid": "0fe0b5af-22cd-4876-85f4-dc18fba47de2"}}}
2023-09-23T21:48:52.749+0700 INFO [beat] instance/beat.go:950 Build info {"system_info": {"build": {"commit": "60dd883ca29e1fdd5b8b075bd5f3698948b1d44d", "libbeat": "7.5.1", "time": "2019-12-16T22:05:28.000Z", "version": "7.5.1"}}}
2023-09-23T21:48:52.764+0700 INFO [beat] instance/beat.go:953 Go runtime info {"system_info": {"go": {"os": "windows", "arch": "amd64", "max_procs": 2, "version": "go1.12.12"}}}
2023-09-23T21:48:52.806+0700 INFO [beat] instance/beat.go:957 Host info {"system_info": {"host": {"architecture": "x86_64", "boot_time": "2023-09-23T16:30:19.19+07:00", "name": "DESKTOP-V627V56", "ip": ["fe80::91af:bec9:4e4e:8f6d/64", "192.168.40.131/24", "fe80::b521:1279:fa30:f0bf/64", "169.254.240.191/16", "::1/128", "127.0.0.1/8"], "kernel_version": "10.0.17763.316 (WinBuild.160101.0800)", "mac": ["00:0c:29:6c:ad:3c", "c8:b2:9b:6e:11:6b"], "os": {"family": "windows", "platform": "windows", "name": "Windows 10 Enterprise LTSC 2019", "version": "10.0", "major": 10, "minor": 0, "patch": 0, "build": "17763.316"}, "timezone": "+07", "timezone_offset_sec": 25200, "id": "6bed6f84-dc19-4a45-9bc6-2c81bb78b257"}}}
2023-09-23T21:48:52.853+0700 INFO [beat] instance/beat.go:986 Process info {"system_info": {"process": {"cwd": "C:\\Program Files\\Winlogbeat", "exe": "C:\\Program Files\\Winlogbeat\\winlogbeat.exe", "name": "winlogbeat.exe", "pid": 2196, "ppid": 3060, "start_time": "2023-09-23T21:48:52.413+0700"}}}
2023-09-23T21:48:52.862+0700 INFO instance/beat.go:297 Setup Beat: winlogbeat; Version: 7.5.1
2023-09-23T21:48:52.864+0700 INFO [index-management] idxmemt/std.go:182 Set output.elasticsearch.index t
```

Hình 16: Kiểm tra winlogbeat đã hoạt động hay chưa với câu lệnh test config -c

### 3.2.4. Đặt rules trên Suricata

+ Bước 1: Vào đường dẫn dưới đây tạo hai file rules là Portscaning và DoS

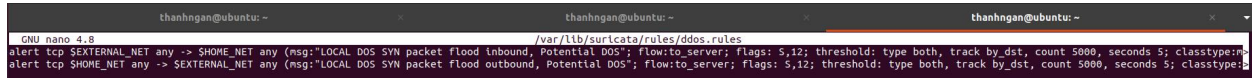
```

thanhngan@ubuntu:~$ sudo ls /var/lib/suricata/rules
[sudo] password for thanhngan:
classification.config  portscaning.rules      suricata.rules
ddos.rules             portscaning.rules.save
thanhngan@ubuntu:~$

```

Hình 17: Đường dẫn chứa các rules của Suricata

+ Bước 2: Tạo các rules cho Suricata



Hình 18: Rule DoS cho Suricata

```

thanhngan@ubuntu:/var/lib/suricata$ sudo cat rules/portscaning.rules
alert ip any any -> 192.168.40.131 any ( \
  (msg:"Allow incoming traffic to ports 20-100 and 1000-10000 on Victim"; \
  ip_proto:tcp; \
  flow:to_server,established; \
  dport:20:100,1000:10000; \
  sid:10000001; \
  rev:1;))
thanhngan@ubuntu:/var/lib/suricata$

```

Hình 19: Rule nmap cho Suricata

### 3.2.5. Thu thập log từ máy Ubuntu và Windows, gửi log lên ELK

#### a. Thu thập log từ máy Ubuntu

+ Bước 1: Sử dụng 1 máy attacker (ubuntu 192.168.40.129) khác thực hiện tấn công hping3 và nmap lên máy victim (ubuntu 192.168.40.131) để Suricata thu log

```

[thanhngan@ubuntu:~$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 22 --flood --rand-source 192.168.40.131
HPING 192.168.40.131 (ens33 192.168.40.131): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.40.131 hping statistic ---
19348 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

```

Hình 20: Sử dụng công cụ hping tấn công tới máy victim



```
tinayoung@ubuntu:~$ nmap -p- 192.168.40.131
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-25 00:20 PDT
Nmap scan report for 192.168.40.131
Host is up (0.0027s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
7680/tcp   open  pando-pub
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49672/tcp  open  unknown
49674/tcp  open  unknown
49675/tcp  open  unknown
```

Hình 21: Sử dụng công cụ nmap tấn công tới máy victim

+ Bước 2: Mở đường dẫn sau để đọc log thu được trên Suricata

```
thanhngan@ubuntu:~$ cd /var/log/suricata/
thanhngan@ubuntu:/var/log/suricata$ ls
certs  eve.json  fast.log  files  stats.log  suricata.log
thanhngan@ubuntu:/var/log/suricata$
```

Hình 22: Đường dẫn chứa log của Suricata

09/23/2023	11:13:27.468747	**	1:5:0	LOCAL	DOS SYN packet flood	Inbound	Potential	DOS	**	Classification: Misc activity	Priority: 3	[TCP] 11.213.147.155:8042 -> 192.168.40.131:22
09/23/2023	11:13:32.331393	**	1:5:0	LOCAL	DOS SYN packet flood	Inbound	Potential	DOS	**	Classification: Misc activity	Priority: 3	[TCP] 170.76.11.213:8042 -> 192.168.40.131:22
09/23/2023	11:13:37.333993	**	1:5:0	LOCAL	DOS SYN packet flood	Inbound	Potential	DOS	**	Classification: Misc activity	Priority: 3	[TCP] 108.8.25.146:43167 -> 192.168.40.131:22
09/23/2023	11:13:42.391961	**	1:5:0	LOCAL	DOS SYN packet flood	Inbound	Potential	DOS	**	Classification: Misc activity	Priority: 3	[TCP] 208.28.117.104:61186 -> 192.168.40.131:22
09/23/2023	11:13:47.917885	**	1:5:0	LOCAL	DOS SYN packet flood	Inbound	Potential	DOS	**	Classification: Misc activity	Priority: 3	[TCP] 63.71.207.18:19039 -> 192.168.40.131:22
09/23/2023	11:13:51.279102	**	1:5:0	LOCAL	DOS SYN packet flood	Inbound	Potential	DOS	**	Classification: Misc activity	Priority: 3	[TCP] 10.16.16.12:28234 -> 192.168.40.131:22

Hình 23: Log của tấn công DoS trong file fast.log

10/04/2023-21:35:02.032785	[**]	[1:1000010:4]	POSSBL SCAN NMAP KNOWN TCP (type -sT) [**] [Classificat
ion: Attempted Information Leak	[Priority: 2]	{TCP}	192.168.40.131:49775 -> 45.122.232.8:80
10/04/2023-21:36:05.258619	[**]	[1:1000010:4]	POSSBL SCAN NMAP KNOWN TCP (type -sT) [**] [Classificat
ion: Attempted Information Leak	[Priority: 2]	{TCP}	192.168.40.131:49792 -> 8.255.194.126:80
10/04/2023-21:36:12.947064	[**]	[1:1000010:4]	POSSBL SCAN NMAP KNOWN TCP (type -sT) [**] [Classificat
ion: Attempted Information Leak	[Priority: 2]	{TCP}	192.168.40.131:49807 -> 20.42.65.84:443

Hình 24: Log của tần công nmap trong file fast.log

+ Bước 3: Cấu hình filebeat lấy đường dẫn chứa log của của Suricata

```
thanhngan@ubuntu: /etc/filebeat
GNU nano 4.8 filebeat.yml

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: log

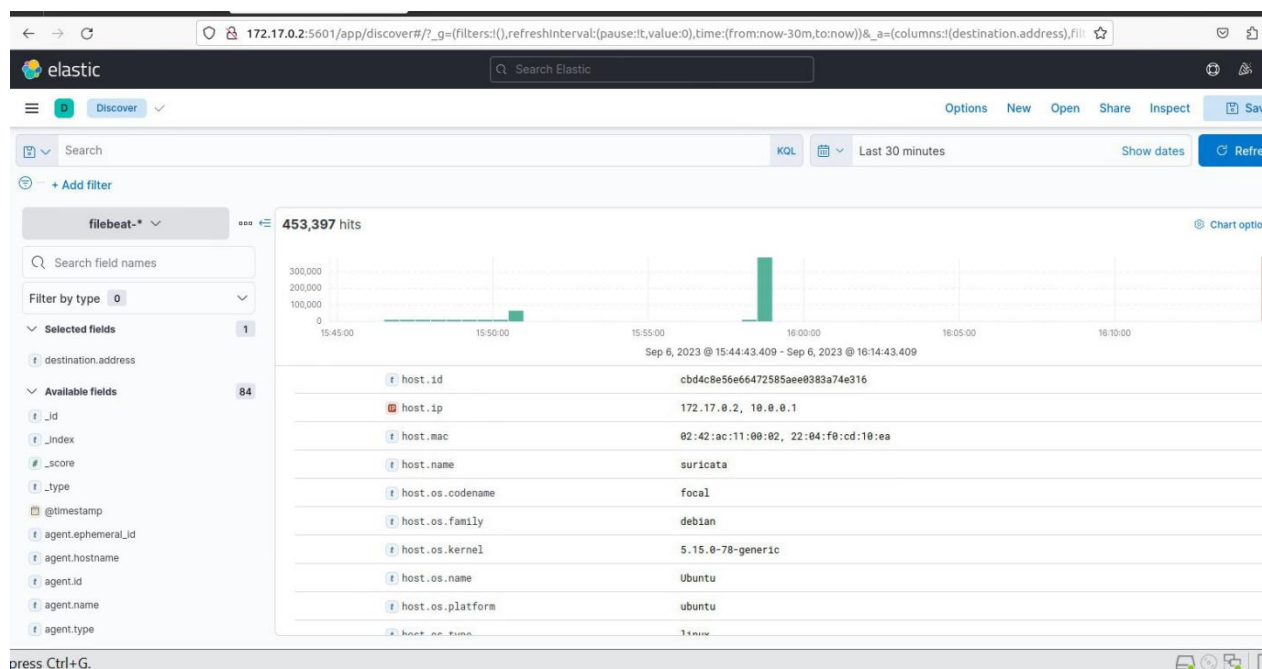
# Unique ID among all inputs, an ID is required.
# id: my-filestream-id

# Change to true to enable this input configuration.
enabled: false

# Paths that should be crawled and fetched. Glob based paths.
paths:
  - /var/log/suricata/fast.log
  #- c:\programdata\elasticsearch\logs\*
```

Hình 25: Cấu hình filebeat

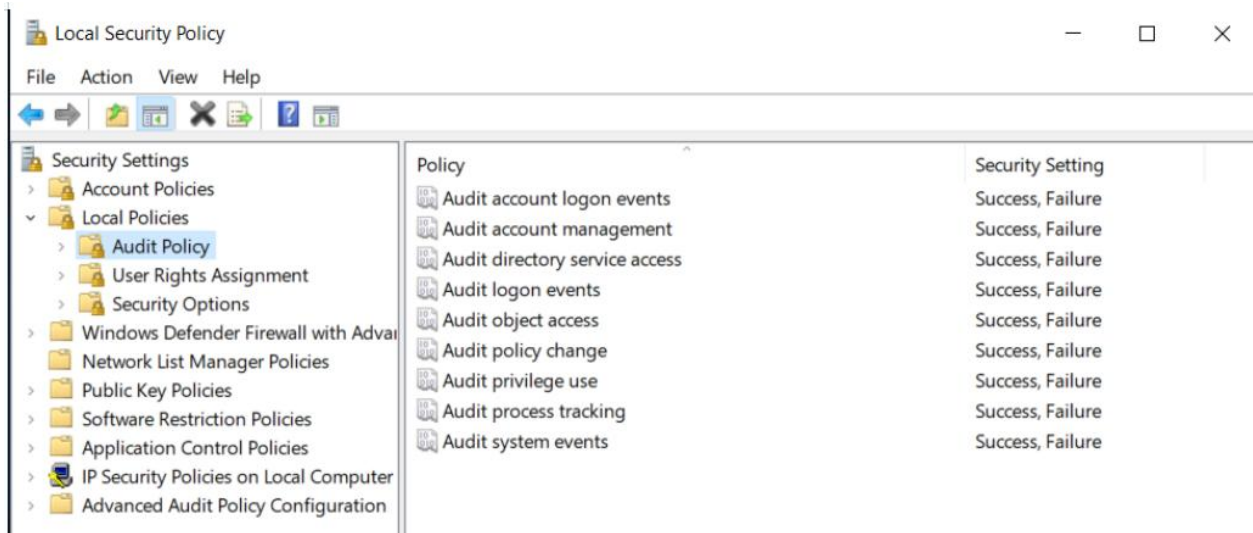
+ Bước 4: Hiển thị log từ Suricata đẩy lên với index filebeat ở Discosvery



Hình 26: Log của Suricata được hiển thị trên elk với index filebeat

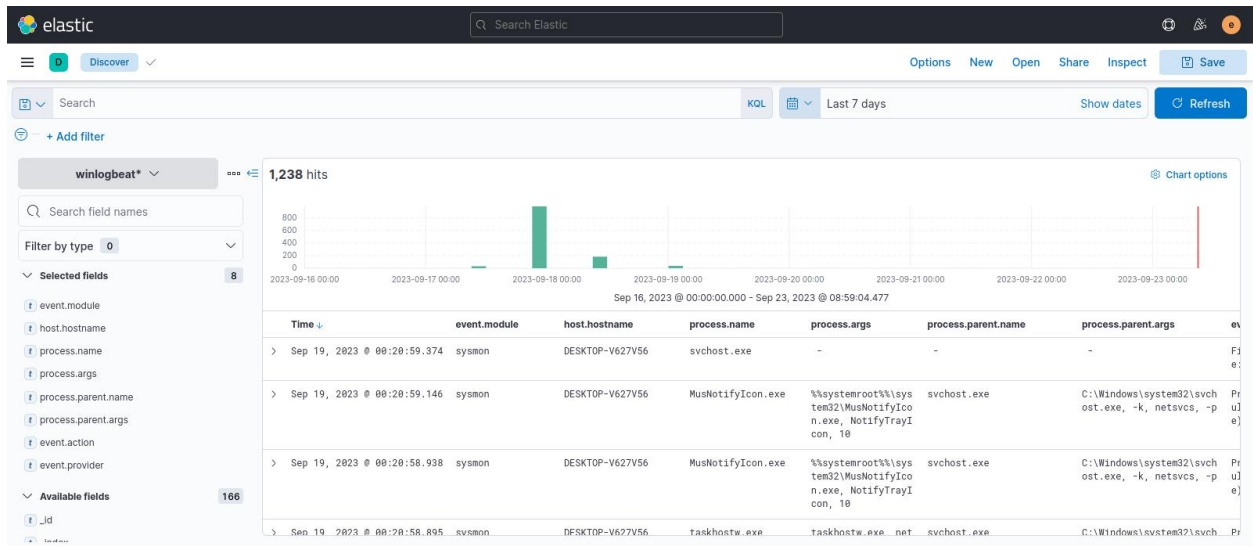
## b. Thu thập log trên Windows 10

+ Bước 1: Để có thể thu log một cách đầy đủ cần bật audit log trên Windows 10



Hình 27: Bật audit log trên máy Windows 10

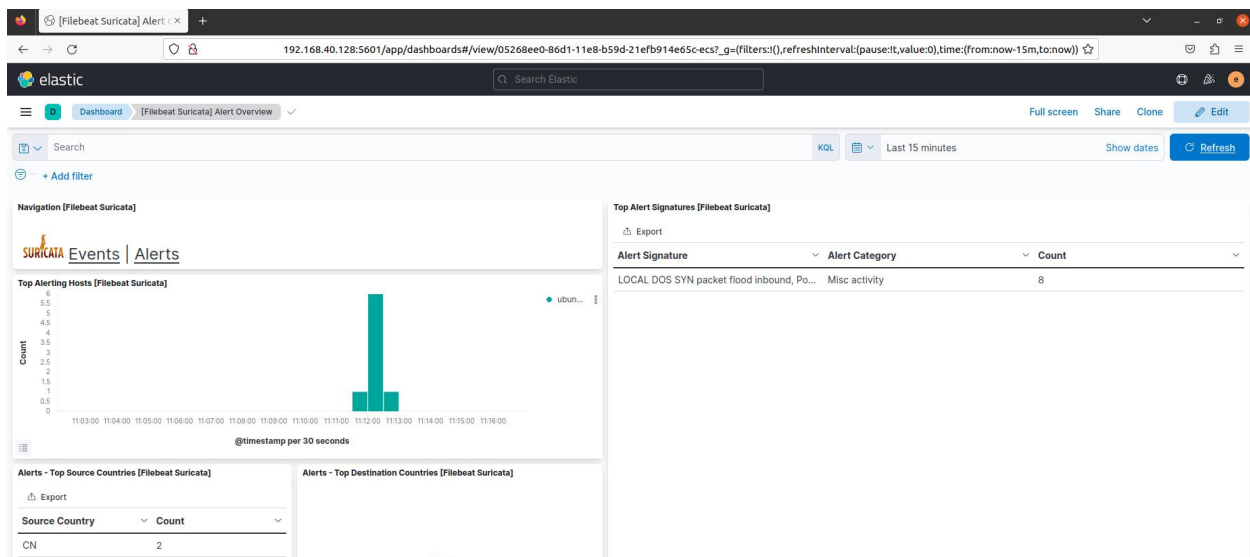
+ Bước 2: Log Windows được đưa lên trên ELK thông qua logstash với index Winlogbeat



Hình 28: Log được thu từ máy Windows, bao gồm cả audit log hiện thị trên elk với index winlogbeat

### 3.2.6. Trực quan hoá dữ liệu, tạo Dashbroad và rules trên ELK

Ta có thể sử dụng các dashboard có sẵn trên ELK để xem các alert từ Suricata gửi lên



Hình 29a: Sử dụng Dashboard có sẵn xem alert là Suricata alert overview để trực quan hoá dữ liệu

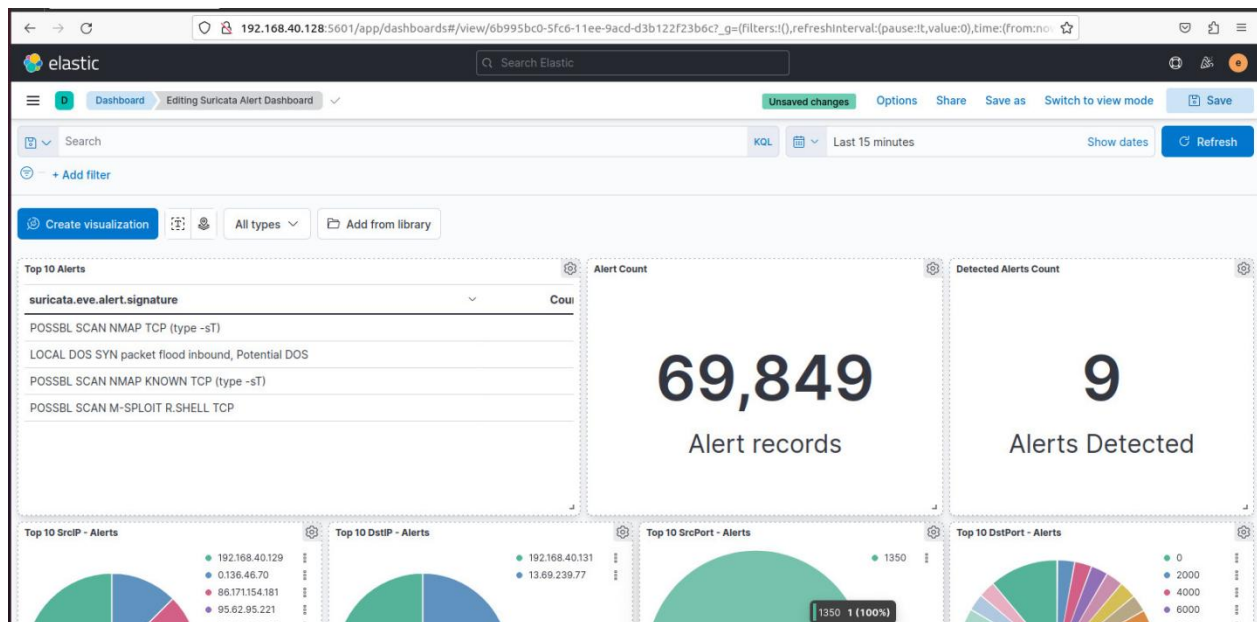
The screenshot shows the Elastic Kibana dashboard for '[Filebeat Suricata] Alert Overview'. The dashboard displays a table of alerts with the following columns: Time, host.name, suricata.event\_id, source.ip, source.port, destination.ip, destination.port, source.geo.country\_iso\_code, and destination.geo.country\_iso\_code. The table shows 9 documents.

Time	host.name	suricata.event_id	source.ip	source.port	destination.ip	destination.port	source.geo.country_iso_code	destination.geo.country_iso_code
Sep 23, 2023 @ 11:13:07.814	ubuntu	2151266883106483	198.79.111.20	6883	192.168.40.131	22	US	-
Sep 23, 2023 @ 11:12:32.906	ubuntu	855128112834829	221.225.126.188	36660	192.168.40.128	22	CN	-
Sep 23, 2023 @ 11:12:27.746	ubuntu	2087899868740646	51.115.215.68	22187	192.168.40.128	22	GB	-
Sep 23, 2023 @ 11:12:22.361	ubuntu	1842857363538570	45.126.146.161	1474	192.168.40.128	22	IN	-
Sep 23, 2023 @ 11:12:16.933	ubuntu	1744957878582931	232.94.11.196	45868	192.168.40.128	22	-	-
Sep 23, 2023 @ 11:12:12.029	ubuntu	1532412831757216	66.148.51.240	28399	192.168.40.128	22	US	-
Sep 23, 2023 @ 11:12:06.917	ubuntu	994109547886583	60.20.127.211	58873	192.168.40.128	22	CN	-
Sep 23, 2023 @ 11:12:01.905	ubuntu	8605961941803858	30.92.180.127	31563	192.168.40.128	22	US	-
Sep 23, 2023 @ 11:11:57.322	ubuntu	787983329258515	240.66.135.235	7778	192.168.40.128	22	-	-

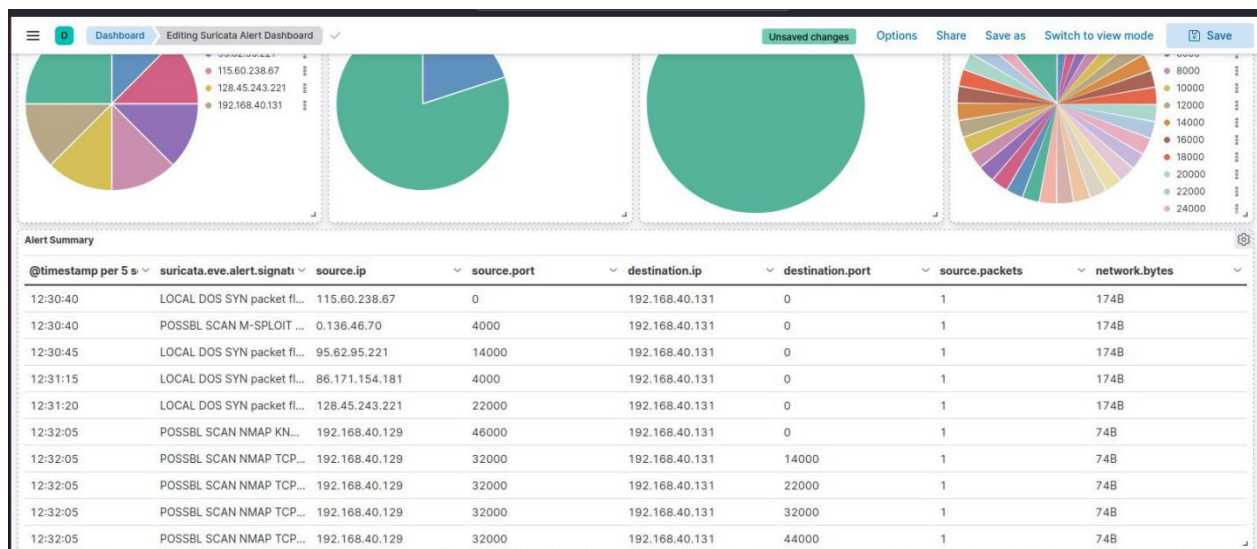
Hình 29b

Ngoài việc sử dụng các dashboard có sẵn ta có thể trực quan hoá dữ liệu và tạo dashboard theo ý muốn theo chỉ dẫn <https://www.elastic.co/guide/en/kibana/current/create-a-dashboard-of-panels-with-web-server-data.html>, bạn chọn vào Create visualization và lấy ra cái trường theo mong muốn của bản thân.





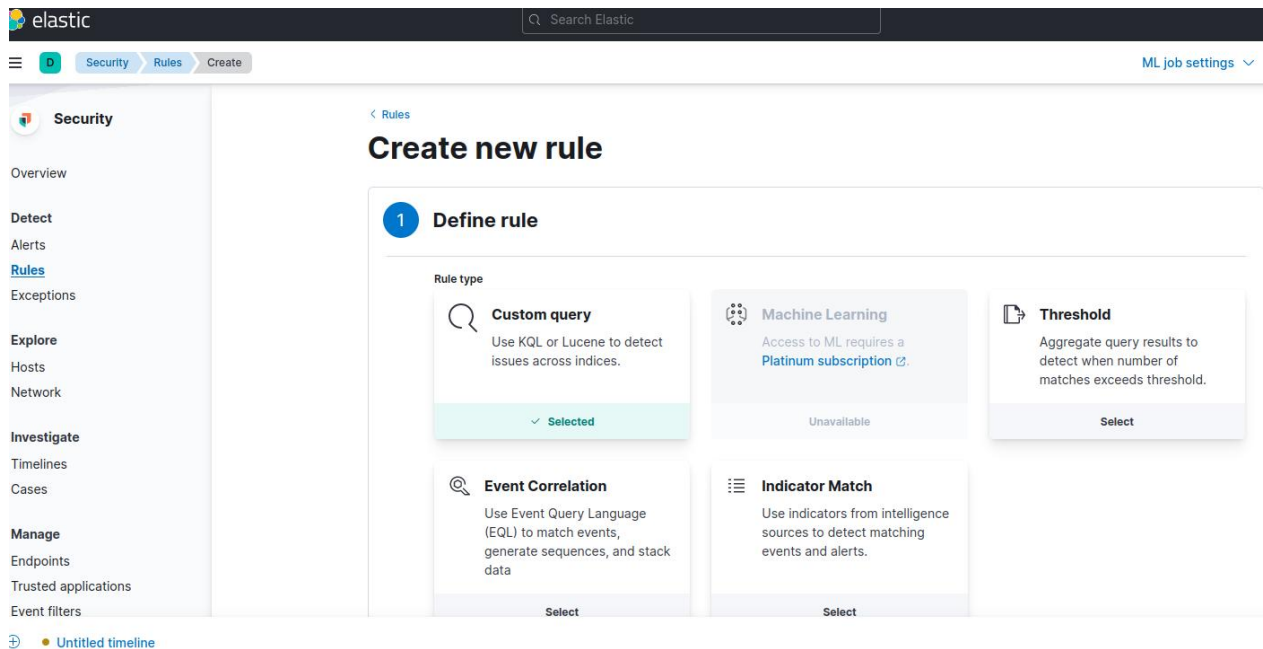
Hình 30a: Dashboard tự tạo



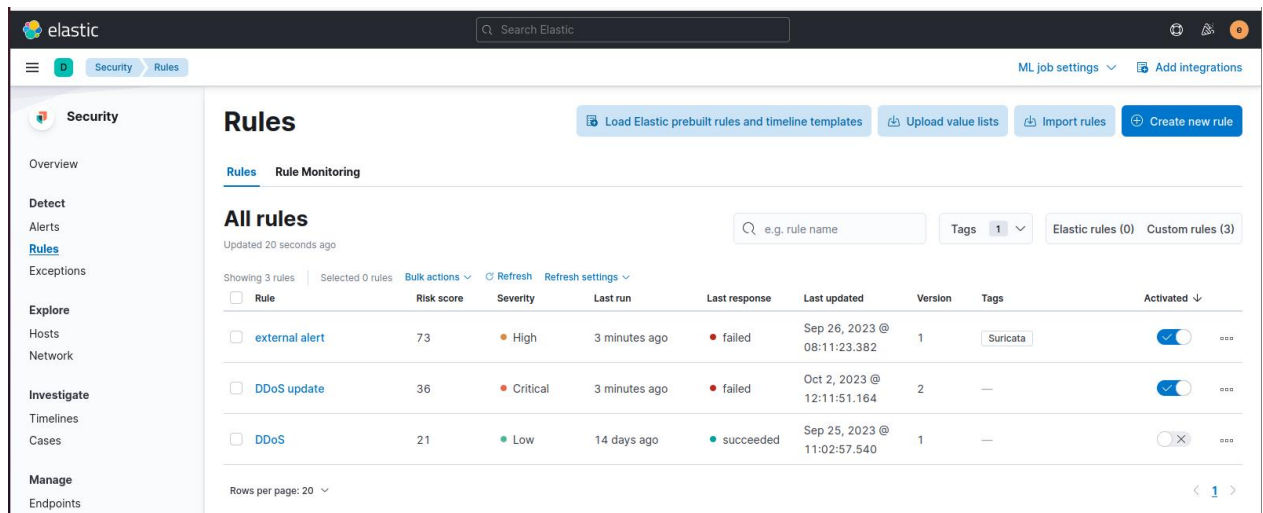
Hình 30b: Bao gồm 10 vị trí dẫn đầu các Source port, Destination port, Source IP, ....

Trên ELK dựa trên những query tới logs thu được, ELK hỗ trợ nhiều loại rule:

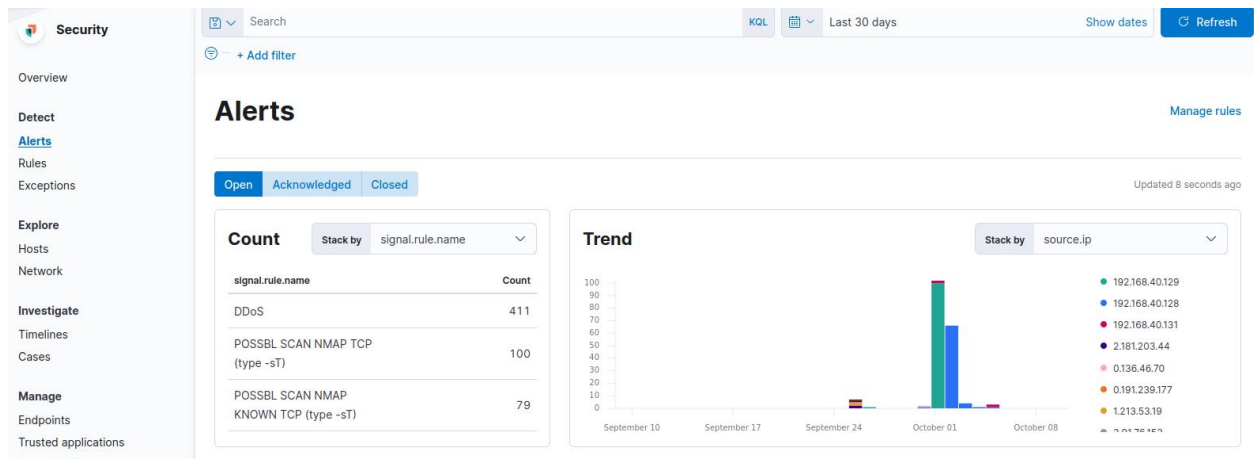




Hình 31: Một số loại rules mà ELK hỗ trợ



Hình 32: Các rules đã tạo

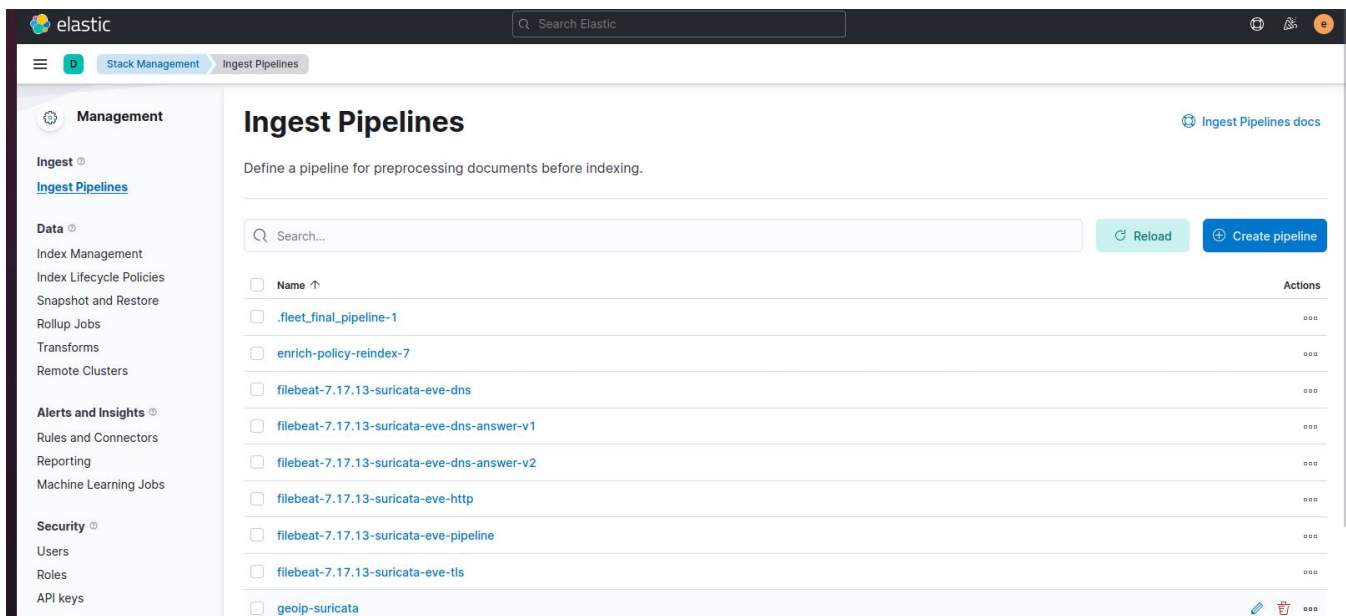


Hình 33: Alert security thu được sau khi chạy các rules trên

### 3.2.7. Ingest Pipelines trên ELK

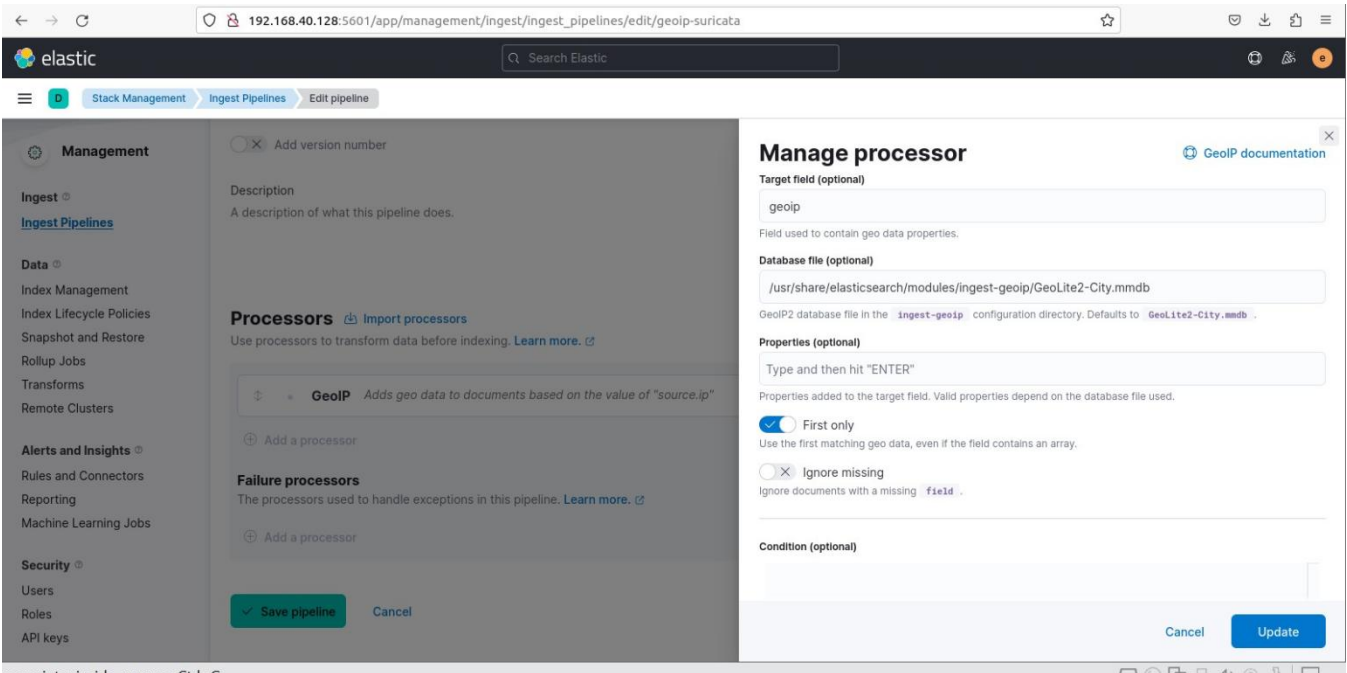
Ingest Pipelines trong ELK (Elasticsearch, Logstash, Kibana) có mục đích chính là xử lý và biến đổi dữ liệu trước khi nó được lưu trữ trong Elasticsearch. Một số mục đích chính của Ingest Pipelines: Tiền xử lý dữ liệu, phân tích và trích xuất thông tin, enrichment (bổ sung thông tin), kiểm tra và xử lý lỗi, giảm kích thước lưu trữ, áp dụng quy tắc an ninh, chuyển đổi dữ liệu không đồng nhất.

+ Bước 1: Vào Ingest Pipelines trong management, ở đây chọn Create Pipelines



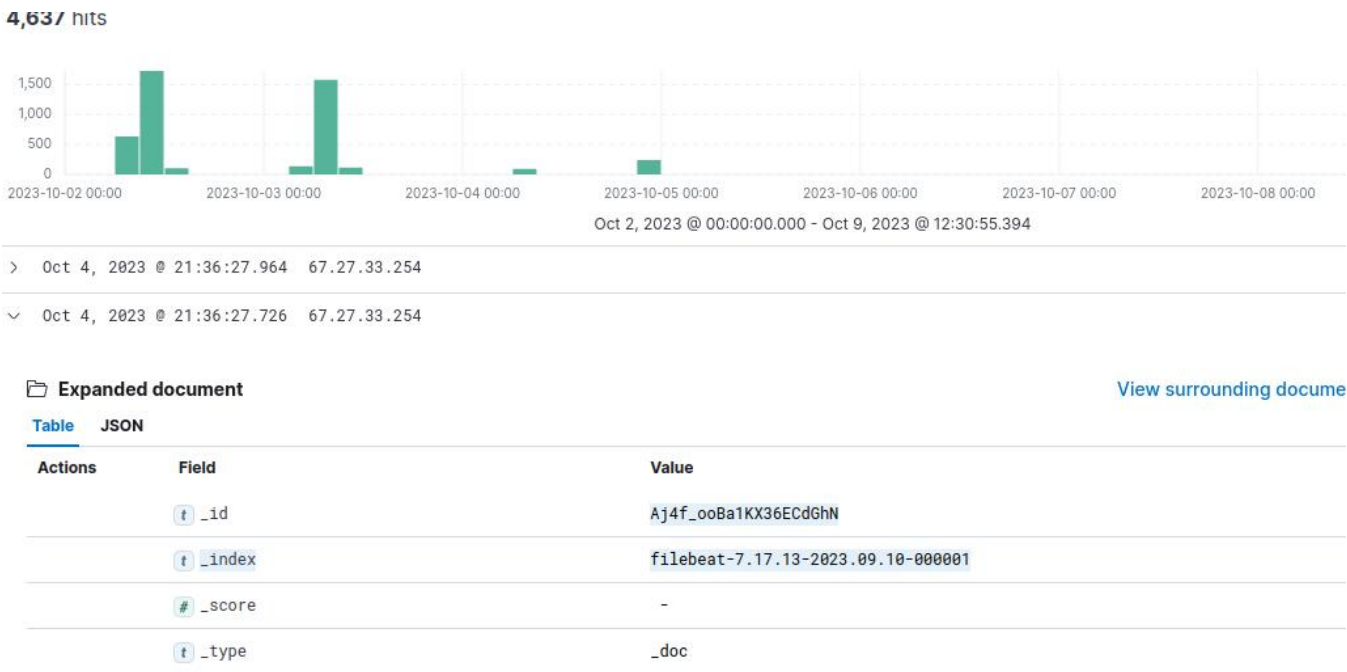
Hình 34: Pipelines có sẵn và create Pipelines

+ Bước 2: Tạo xong Pipeline thì chọn save Pipeline sau đó add document để kiểm tra Pipeline vừa tạo (ở đây chọn Pipeline GeoiP)



Hình 35: Giao diện sau khi tạo Pipeline, có thể update Pipeline

+ Bước 4: Lấy trường index và id của một log bất kì bỏ vào để kiểm tra Pipeline



Hình 36a: Index và id của một log trong phần discovery

The screenshot shows the 'Documents' tab in the Elasticsearch UI. It features a form to add a test document from an index. The form includes two input fields: 'Index' with the value 'filebeat-7.17.13-2023.09.10-000001' and 'Document ID' with the value 'Aj4f\_ooBa1KX36ECdGhN'. Below these fields is a blue 'Add document' button. At the bottom, there is a 'Documents' table with a 'Clear all' link. The table is currently empty, showing only the opening and closing brackets of an array.

**Documents** [Clear all](#)

[
]

Hình 36b: Thả index và id bên trên vào Pipeline

+ Bước 5: Run Pipeline nhận được kết quả như sau, có thể thấy được quốc gia, lục địa, địa chỉ đích....



Hình 37: Test Pipelines

### 3.2.7. Triển khai n8n

+ Bước 1: update và cài đặt các phần cần thiết

```
# sudo apt update
```

```
# sudo apt upgrade -y
```

```
# curl -sL https://deb.nodesource.com/setup_16.x | sudo bash -
```

```
# sudo apt install nodejs -y
```

+ Bước 2: cài đặt cơ sở dữ liệu

```
# sudo apt install mariadb-server mariadb-client -y
```

```
# sudo su
```

```
# mysql_secure_installation
```

```
# mysql -u root -p
```

+ Bước 3: tạo cơ sở dữ liệu n8n và người dùng cơ sở dữ liệu

```
CREATE DATABASE n8n;
```

```
GRANT ALL ON n8n.* to 'n8n_rw'@'localhost' IDENTIFIED BY 'n8n_N8N!';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

```
Exit
```

+ Bước 4: đặt biến môi trường

```
export DB_TYPE="mysqldb"
```

```
export DB_MYSQLDB_DATABASE="n8n"
```

```
export DB_MYSQLDB_HOST="localhost"
```

```
export DB_MYSQLDB_USER="n8n_rw"
```

```
export DB_MYSQLDB_PASSWORD="n8n_N8N!"
```

```
export GENERIC_TIMEZONE="America/New_York"
```

+ Bước 5: cài đặt n8n

```
# sudo npm install n8n --location=global
```

```
# sudo npm audit fix
```

+ Bước 6: SQLite3

```
# npm install sqlite3 --save
```



```

thanhngan@ubuntu:~$ npm install sqlite3 --save
npm WARN old lockfile
npm WARN old lockfile The package-lock.json file was created with an old version of n
pm,
npm WARN old lockfile so supplemental metadata must be fetched from the registry.
npm WARN old lockfile This is a one-time fix-up, please be patient...
npm WARN old lockfile string-width-cjs: No matching version found for string-width-cj
s@4.2.3.
npm WARN old lockfile   at module.exports (/home/thanhngan/.npm/versions/node/v18.1
8.0/lib/node_modules/npm/node_modules/npm-pick-manifest/lib/index.js:209:23)
npm WARN old lockfile   at RegistryFetcher.manifest (/home/thanhngan/.npm/versions/
node/v18.18.0/lib/node_modules/npm/node_modules/pacote/lib/registry.js:119:22)
npm WARN old lockfile   at async Array.<anonymous> (/home/thanhngan/.npm/versions/n
ode/v18.18.0/lib/node_modules/npm/node_modules/@npmcli/arborist/lib/arborist/build-id
eal-tree.js:727:24)
npm WARN old lockfile Could not fetch metadata for string-width-cjs@4.2.3 string-wid
th-cjs: No matching version found for string-width-cjs@4.2.3.
npm WARN old lockfile   at module.exports (/home/thanhngan/.npm/versions/node/v18.1
8.0/lib/node_modules/npm/node_modules/npm-pick-manifest/lib/index.js:209:23)
npm WARN old lockfile   at RegistryFetcher.manifest (/home/thanhngan/.npm/versions/
node/v18.18.0/lib/node_modules/npm/node_modules/pacote/lib/registry.js:119:22)
npm WARN old lockfile   at async Array.<anonymous> (/home/thanhngan/.npm/versions/n
ode/v18.18.0/lib/node_modules/npm/node_modules/@npmcli/arborist/lib/arborist/build-id
eal-tree.js:727:24) {

```

Hình 38: Cài đặt SQLite cho n8n

+ Bước 7: Run n8n

```

Stopping n8n...
thanhngan@ubuntu:~$ ./node_modules/n8n/bin/n8n
n8n ready on 0.0.0.0, port 5678
Initializing n8n process
Version: 1.8.2

Editor is now accessible via:
http://localhost:5678/

Press "o" to open in Browser.
Owner was set up successfully
User survey updated successfully

```

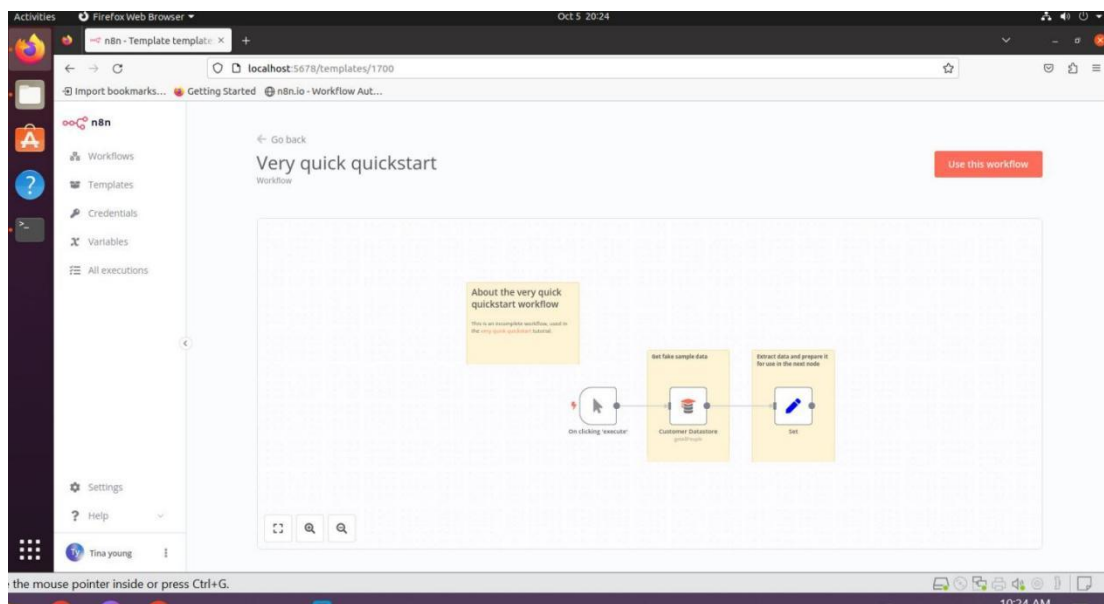
Hình 39: Hoàn thành cài đặt n8n

+ Bước 8: Đăng nhập vào n8n với port 5678

The screenshot shows a web browser window with the address bar displaying 'localhost:5678/setup'. The page title is 'Set up owner account'. The form contains the following fields and elements:

- Email \***: A text input field containing 'thanhngan1792002@gmail.com'.
- First Name \***: A text input field containing 'Tina'.
- Last Name \***: A text input field containing 'young'.
- Password \***: A password input field with masked characters '\*\*\*\*\*'. Below it, a note states: '8+ characters, at least 1 number and 1 capital letter'.
- ☒ **Inform me about security vulnerabilities if they arise**
- Next**: A red button at the bottom right of the form.

Hình 40: Đăng nhập vào n8n thông qua port 5678



Hình 41: Workflow đơn giản trên n8n



### 3.2.8. TheHive

#### + Bước 1: Cài đặt Java Virtual Machine

```
apt-get install -y openjdk-8-jre-headless
echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" >> /etc/environment
export JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64"
```

#### + Bước 2: Cài đặt Cassandra database

```
curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt key add -
echo "deb http://www.apache.org/dist/cassandra/debian 311x main" | sudo tee -a
                                /etc/apt/sources.list.d/cassandra.sources.list

sudo apt update
sudo apt install cassandra
```

#### + Bước 3: Cấu hình

```
cqlsh localhost 9042
cqlsh> UPDATE system.local SET cluster_name = 'thp' where key='local';
```

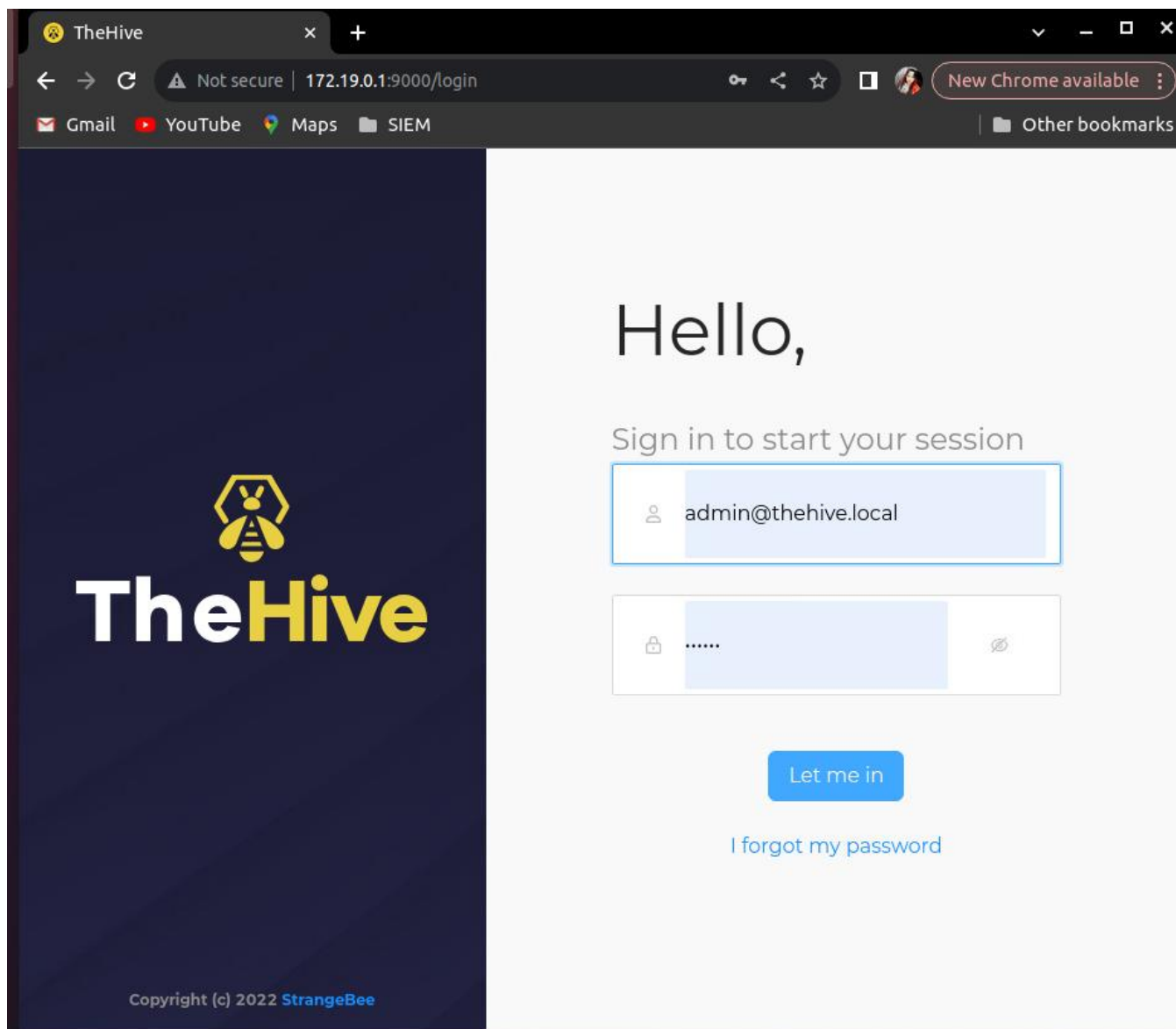
#### + Bước 4: Thoát ra chạy Nodetool và chỉnh file cấu hình yml

```
nodetool flush
service cassandra restart
```

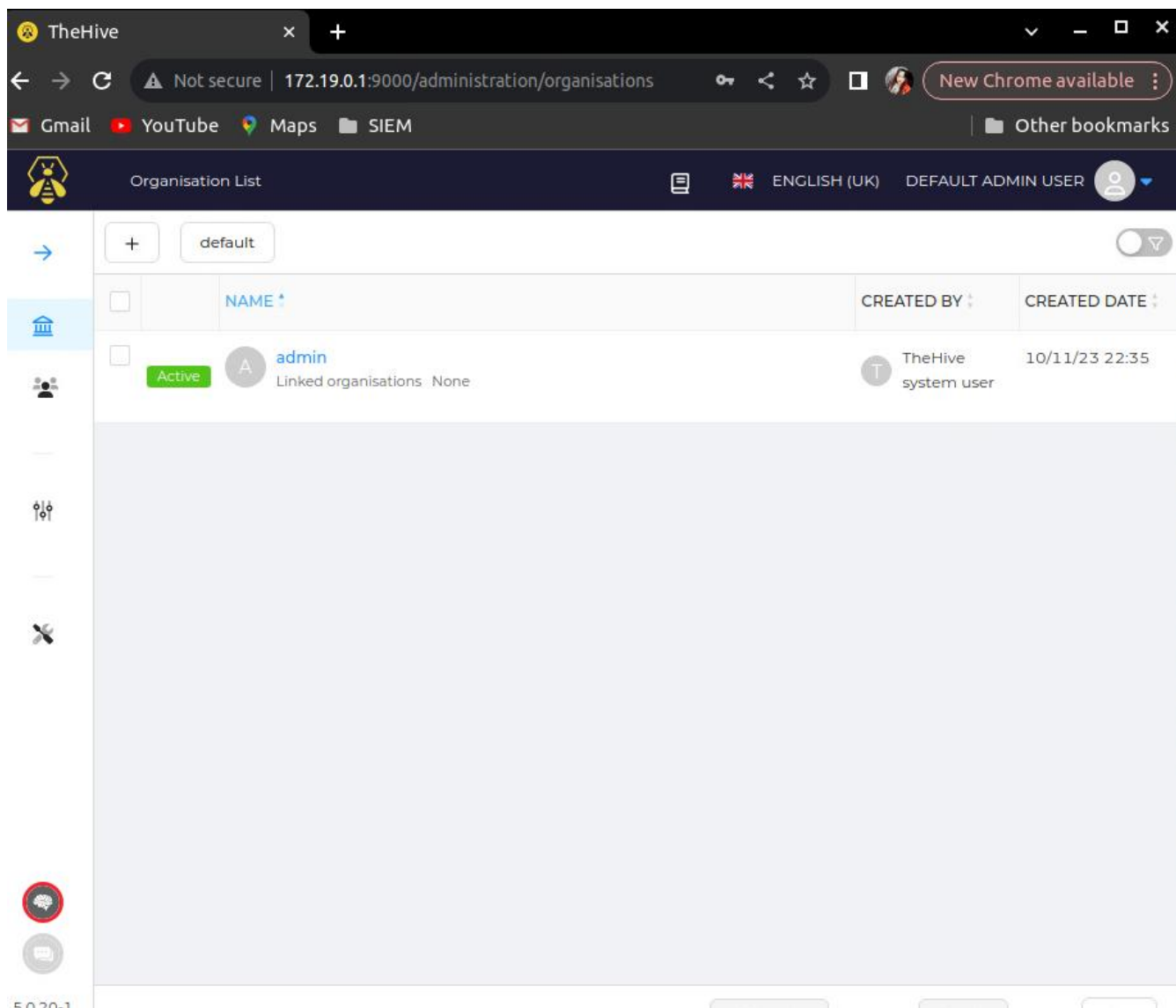
#### + Bước 5: Cài đặt TheHive

```
echo 'deb https://deb.thehive-project.org release main' | sudo tee -a
                                /etc/apt/sources.list.d/thehive-project.list

sudo apt-get update
sudo apt-get install thehive4
service thehive start
```



Hình 42: Đăng nhập vào TheHive



Hình 43: Giao diện TheHive

## **CHƯƠNG IV: KẾT QUẢ ĐẠT ĐƯỢC**

### **4.1. Kết quả đạt được**

Kì thực tập cho em một cơ hội để tiếp thu nhiều kiến thức mới và đạt được mục tiêu đề ra thi tham gia thực tập, đó là ứng dụng kiến thức về an toàn thông tin học tại trường vào các vấn đề thực tế, xây dựng mô hình ELK và các thành phần trong quy trình SOC. Đồng thời bản thân thông qua quá trình thực tập cũng đã rèn luyện được nhiều kỹ năng: quản lý và sắp xếp thời gian, đọc tài liệu, tìm kiếm thông tin, tương tác và trình bày vấn đề,...

### **4.2. Những khó khăn và hạn chế**

Sau 2 tháng thực tập và thực hiện đề tài được giao, bản thân em đã thu được những kết quả nhất định, cả về kiến thức. Bên cạnh đó được tìm hiểu những công nghệ mới, kiến thức mà trước đó bản thân chưa được tiếp xúc. Tuy nhiên, trong quá trình thực tập vẫn còn nhiều khó khăn trong việc ứng dụng các kiến thức về an toàn thông tin vào môi trường thực tế do chưa có nhiều kinh nghiệm. Bên cạnh đó, mô hình đề xuất gặp khó khăn khi triển khai trên nhiều máy ảo đòi hỏi về mặt tài nguyên máy.

## TÀI LIỆU THAM KHẢO

[1] "Elastic Documentation" [Online]. Available:

<https://www.elastic.co/guide/index.html/>

[2] "n8n Tutorials"

<https://i12bretro.github.io/tutorials/0784.html>

[3] "TheHive Documentation"

<https://docs.thehive-project.org/thehive/installation-and-configuration/installation/step-by-step-guide/>

[4] "Build a SIEM with Suricata"

<https://www.digitalocean.com/community/tutorials/how-to-build-a-siem-with-suricata-and-elastic-stack-on-ubuntu-20-04>