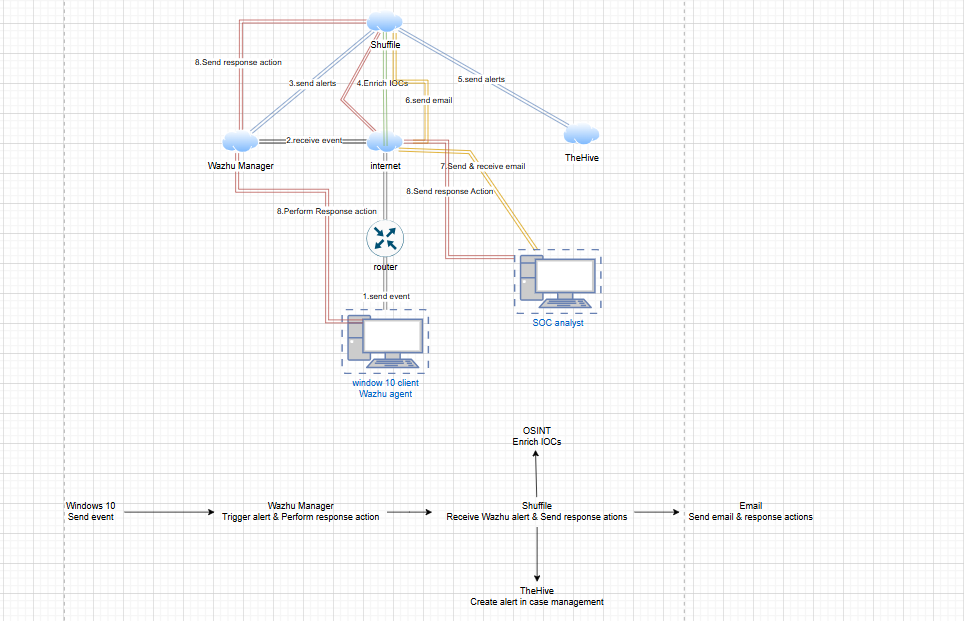
**SOC Automation Project**

1. Cài đặt và cấu hình máy khách Windows 10 với Sysmon để tạo sự kiện chi tiết.
2. Thiết lập Wazuh làm nền tảng quản lý sự kiện và cảnh báo trung tâm.
3. Cài đặt và cấu hình TheHive để quản lý trường hợp và phối hợp hành động ứng phó.
4. Tạo dữ liệu đo từ xa Mimikatz và tạo cảnh báo tùy chỉnh trong Wazuh.
5. Tích hợp Shuffle làm nền tảng SOAR để tự động hóa quy trình làm việc.
6. Xây dựng quy trình làm việc tự động để trích xuất mã băm tệp, kiểm tra điểm uy tín với VirusTotal, tạo cảnh báo trong TheHive và thông báo cho các nhà phân tích SOC qua email.



1. Cảnh báo Mimikatz đã được gửi đến Shuffle
2. Shuffle nhận được cảnh báo Mimikatz / trích xuất băm SHA256 từ tệp
3. Kiểm tra điểm uy tín với VirusTotal
4. Gửi thông tin chi tiết đến TheHive để tạo cảnh báo
5. Gửi email cho nhà phân tích SOC để bắt đầu cuộc điều tra

**Mimikatz là công cụ hậu tấn công sử dụng mục đích rà quét thông tin người dùng ngang hàng trong tổ chức hay thông tin trên AD để trích xuất thông tin phục vụ cho quá trình đăng nhập trái phép hoặc giả mạo ticket, cert**

Trong VMWare:

-1 máy window 10 đã cài đặt sysmon

-1 wazhu server dùng ubuntu 20.04

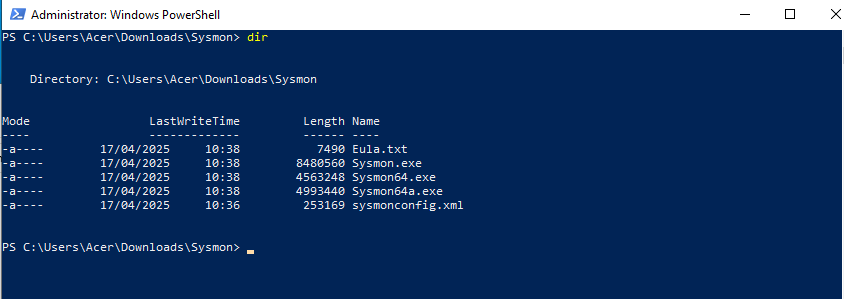
-1 TheHive server dùng ubuntu 20.04

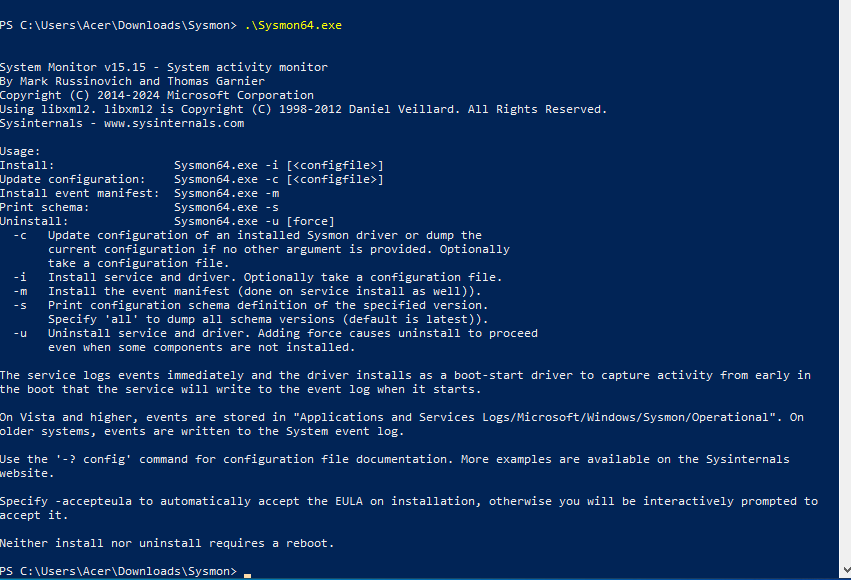
Tải sysmon và tệp sysmonconfig.xml trên <https://github.com/olafhartong/sysmon-modular>

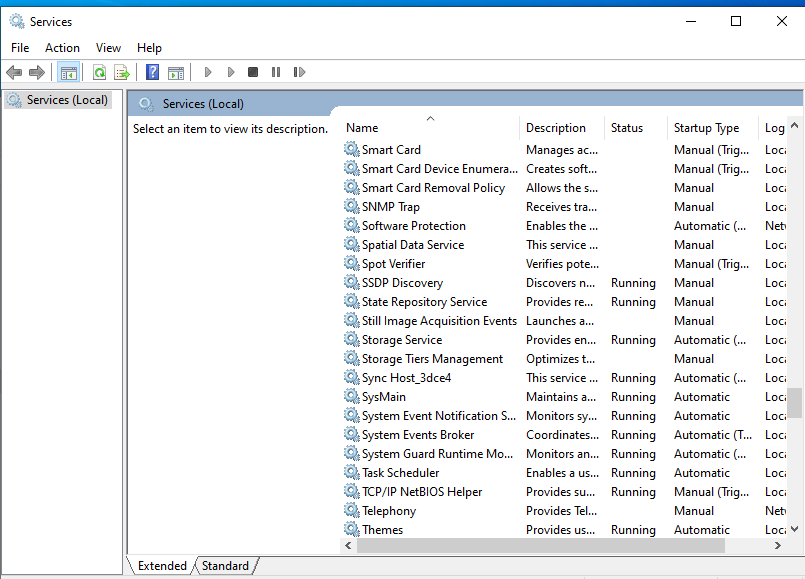
Mở powershel chạy với quyền admin

Chuyển đến thư mục có tệp sysmon

Đảm bảo rằng tệp sysconfig nằm trong thư mục sysmon đã được giải nén.

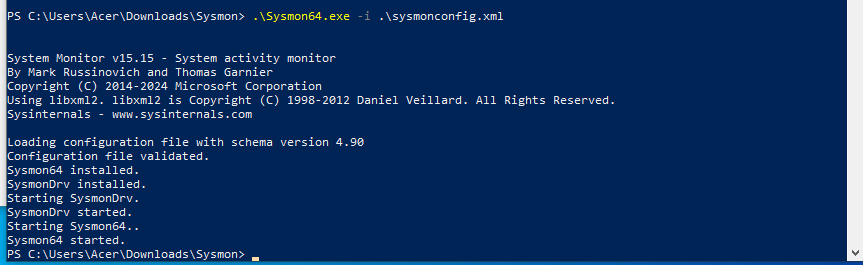




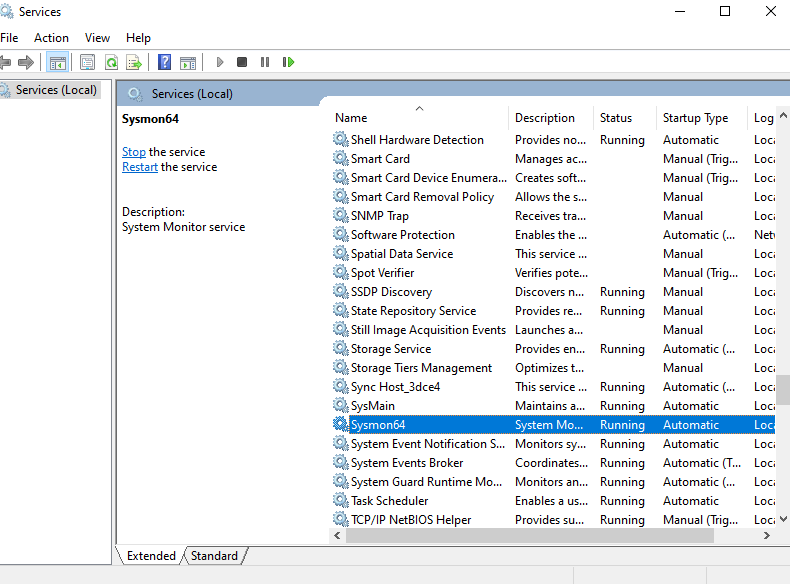
Kiểm tra lại xem đã cài đặt sysmon hay chưa mở menu nhập *services* 

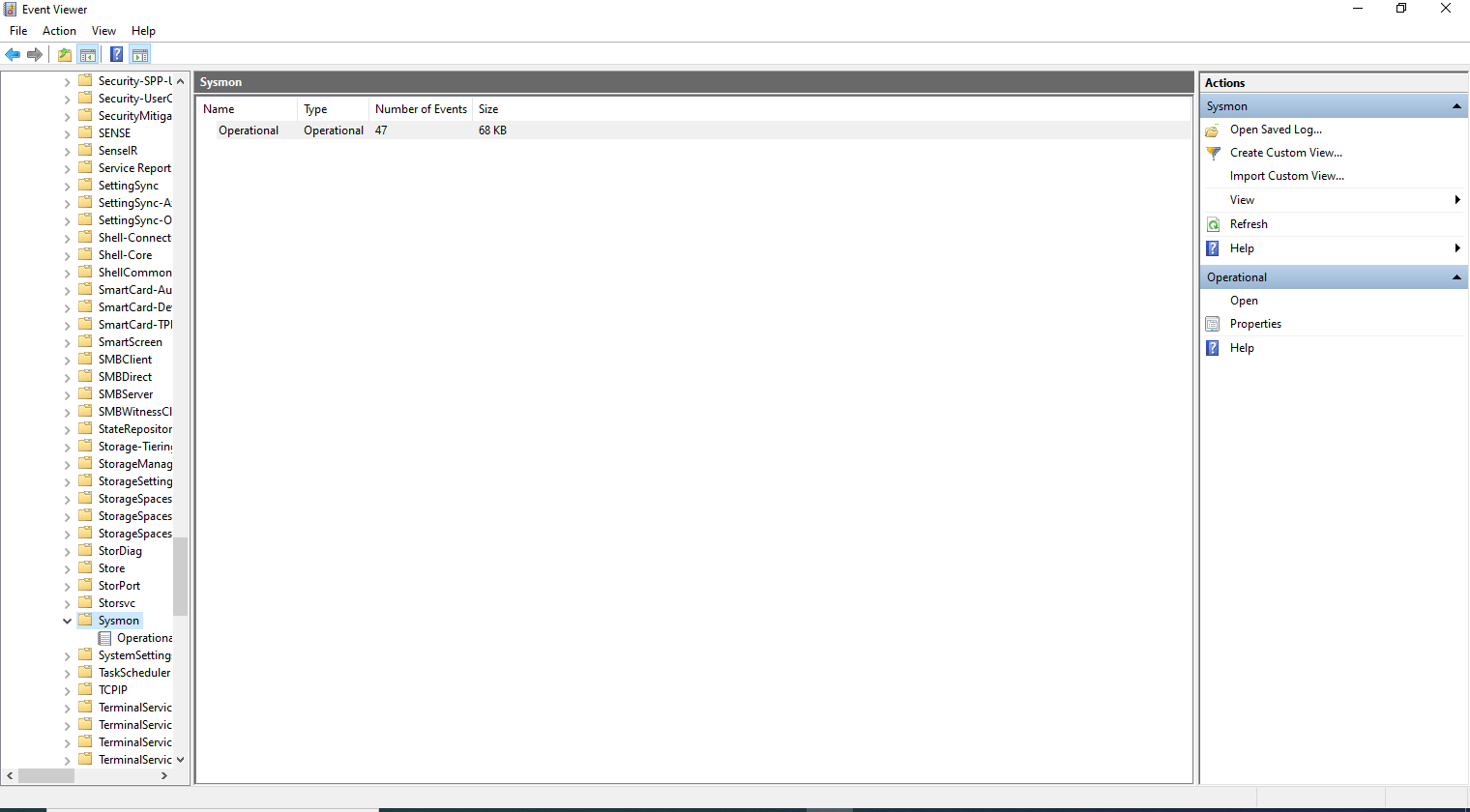
Hoặc có thể mở nhật ký sự kiện (event viewer). Chọn application and services > microsoft > window và tìm sysmon

Cài đặt sysmon bằng lệnh *.\Sysmon64.exe -i .\sysmonconfig.xml*

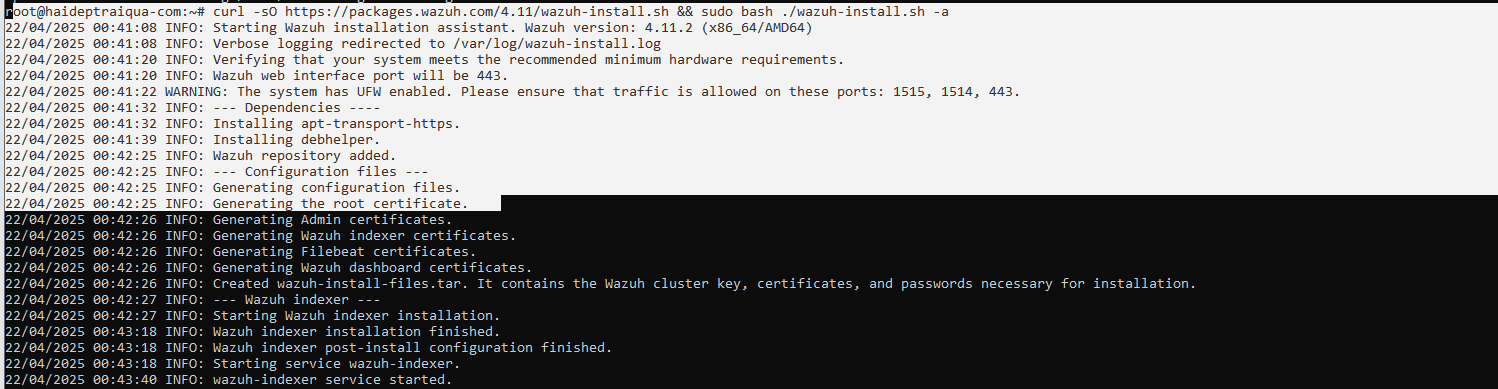


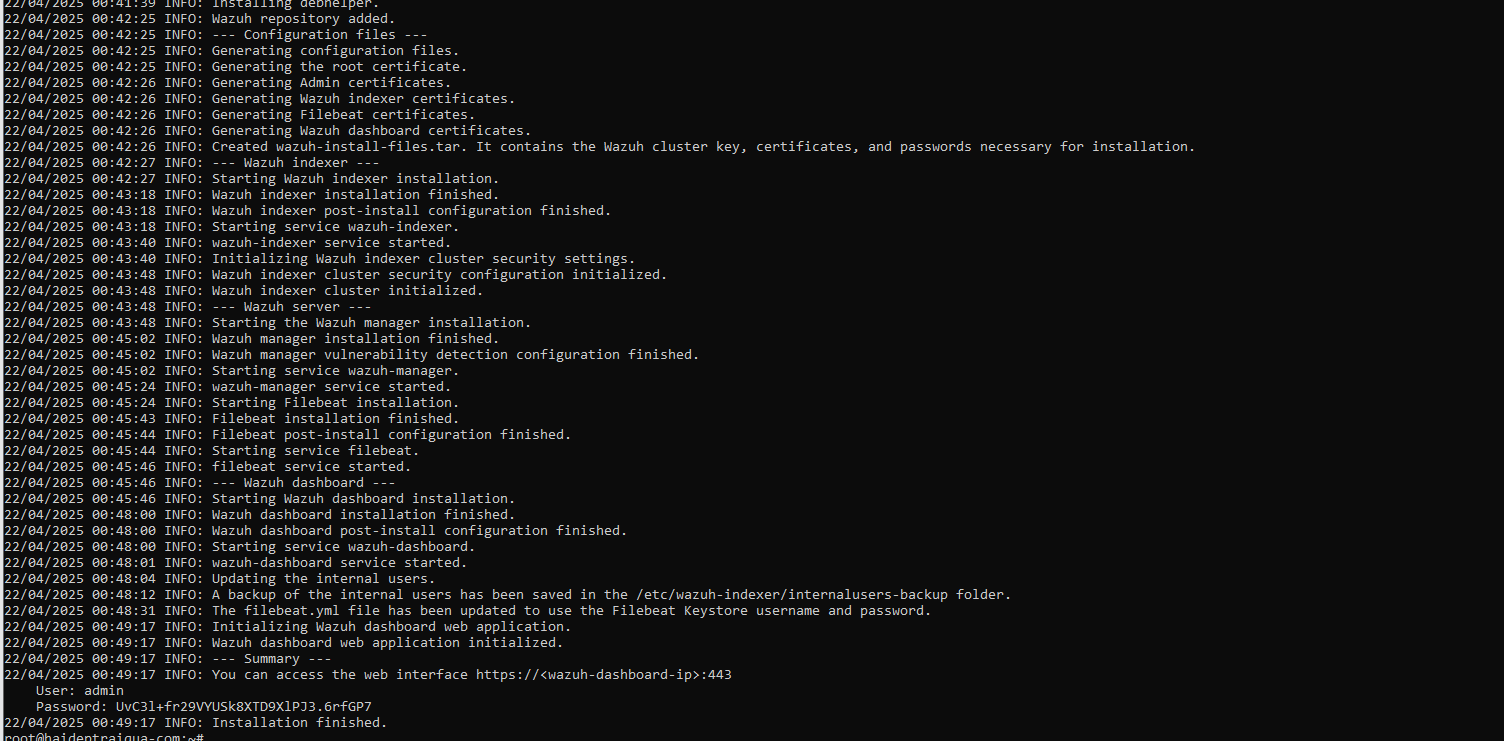
Ktra lại xem đã có sysmon chưa





curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a





**User: admin**

**Password: UvC3l+fr29VYUSk8XTD9XlPJ3.6rfGP7**

**A computer screen shot of a program

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**User: admin**

**Password: NxZ8hXkVUu\*aUC2fGkFeyr.wZeE0WQq2**

Cassandra đóng vái trò là cơ sở dữ liệu

Vào tệp cấu hình cassandra. Thay đổi tên cụm thành “hai’

A screenshot of a computer

AI-generated content may be incorrect.

TÌm địa chỉ lắng nghe ta sẽ thấy đang để ở máy chủ cục bộ. Xóa đi và sửa thành địa chỉ máy chủ theHive.

A screenshot of a computer screen

AI-generated content may be incorrect.

Tìm địa chỉ RPC. Và sửa như trên

A screenshot of a computer

AI-generated content may be incorrect.

Tìm và thay đổi địa chỉ seed

A screenshot of a computer screen

AI-generated content may be incorrect.

Sau đo ta dừng dịch vụ lại: *systemctl stop cassandra.service*

Xóa các tệp cũ*: rm -rf /var/lib/cassandra/\**

Mở lại dịch vụ: *systemctl start cassandra.service*

TheHive sử dụng Elasticsearch để tìm kiếm và truy xuất dữ liệu một cách nhanh chóng và hiệu quả.

Cấu hình elasticsearch: *sudo nano /etc/elasticsearch/elasticsearch.yml*

A screenshot of a computer

AI-generated content may be incorrect.

Đổi network\_host thành địa chỉ của máy chủ theHive

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó khởi động elasticsearch:

*systemctl start elasticsearch*

*systemctl enable elasticsearch*

Kiểm tra xem root có quyền truy cập vào thehive không. ta thấy là có

A screenshot of a computer

AI-generated content may be incorrect.

Thay đổi chủ sở hưu thành người dùng thehive

*chown -R thehive:thehive /opt/thp*

A screenshot of a computer

AI-generated content may be incorrect.

Cấu hình thehive

*nano /etc/thehive/application.conf*

A screenshot of a computer screen

AI-generated content may be incorrect.

ở hostname đổi thành địa chỉ ip thehive

tên cụm đổi thành tên cụm cassandra đã thay đổi ở trên là “hai”

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Khởi động thehive

A screenshot of a computer code

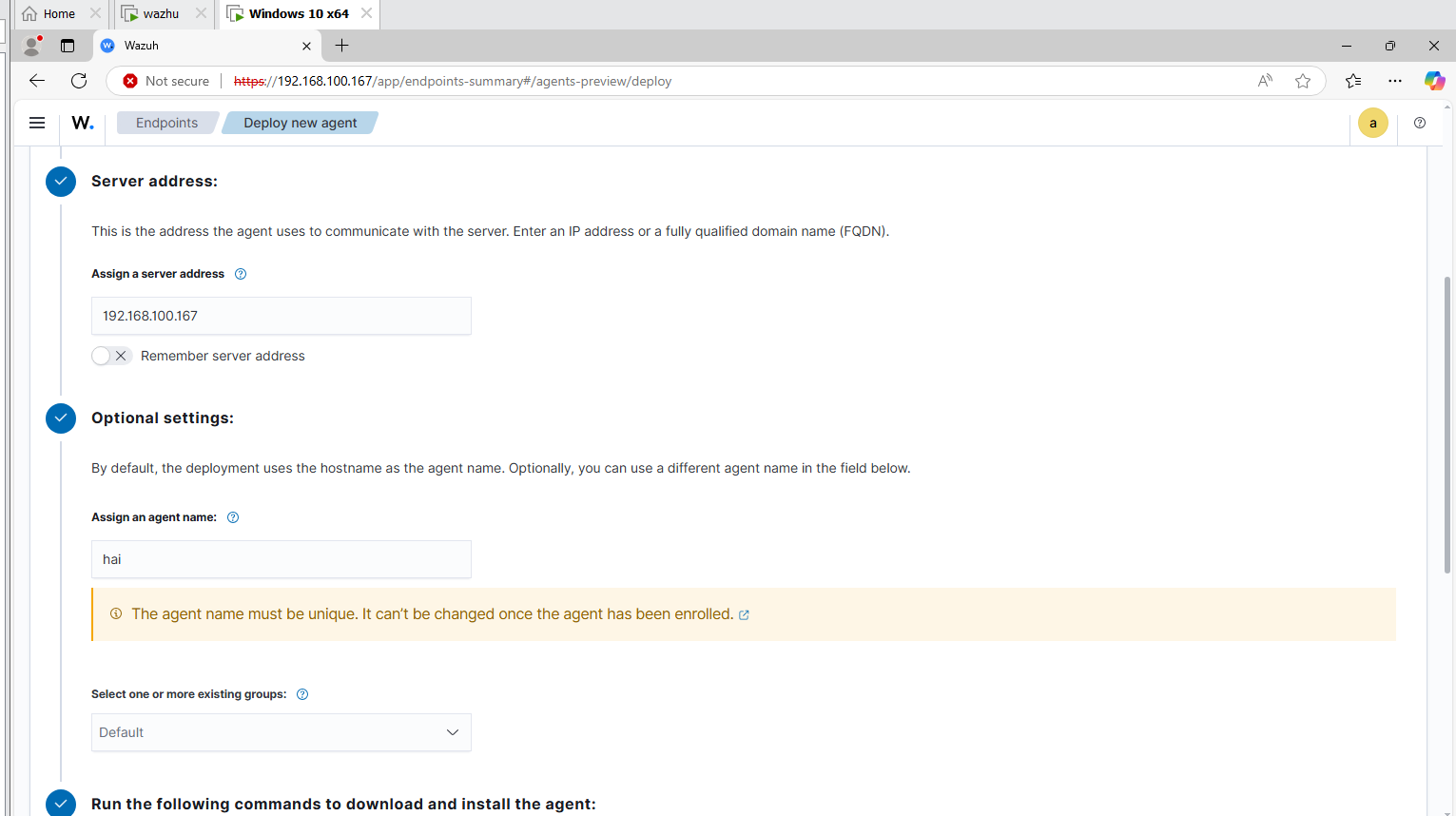
AI-generated content may be incorrect.

Đảm bảo cả 3 cassandra, elasticsearch và thehive đều đang hoạt động. Truy cập vào thehive bằng địa chỉ ip và cổng 9000

A screenshot of a computer

AI-generated content may be incorrect.

Vào wazhu thêm agent



Copy

A close-up of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Tải mimikatz: [*https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20220919*](https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20220919)  
Vô hiệu hóa windows defender hoặc loại trừ thư mục tải xuống mimikatz vì windows defender chắc chắn sẽ phát hiện ra mimikatz

* Loại trừ đường dẫn tải xuống. Vào windows security -> virut & threat protection -> virut & threat protection setting -> add or remove exclusions -> add thư mục dowloads

A screenshot of a computer

AI-generated content may be incorrect.

Bỏ chặn tải mimikatz ở edge:

Mở setting -> Privacy, search, and services -> security -> tắt Microsoft Defender SmartScreen

A screenshot of a computer

AI-generated content may be incorrect.

Giở tải xuống mimikatz và giải nén

Mở powershell và chạy với quyền quản trị và chạy mimikatz

A computer screen shot of a blue screen

AI-generated content may be incorrect.

ở wazhu vào nano /var/ossec/etc/ossec.conf sửa phần logall và logall\_json thành yes

A computer screen shot of white text

AI-generated content may be incorrect.

Thay đổi cấu hình để wazhu bắt đầu thu thập nhật ký. Thay đổi trong filebeat

nano /etc/filebeat/filebeat.yml

A screenshot of a computer screen

AI-generated content may be incorrect.

Kiểm tra xem sysmon cosghi lại mimikatz hay không. Vào event viewer

A screenshot of a computer

AI-generated content may be incorrect.

Check lại ở cat archives.json | grep -i mimikatz

A screenshot of a computer screen

AI-generated content may be incorrect.

Trong wazuh tìm kiếm mimikatz

A screenshot of a computer

AI-generated content may be incorrect.

Ta thấy có 4 sự kiện

Thiết lập rule

Vào server management và chọn rule ấn vào custom rules ta sẽ thấy 1 tệp quy tắc cụ bộ và chúng ta có thể chỉnh sửa tệp đó

Các quy tắc tùy chỉnh luôn bắt đầu từ 100000 nên ta sẽ sửa id thành 100002 và thứ 2 là level mức độ cao nhất chúng ta có thể tùy chỉnh là 15. Ta sẽ đặt level là 15

Tên trường chúng ta sẽ để là win.eventdata. originalFileName thay vì win.eventdata.parentImage (tên trường có phân biệt chữ hoa chữ thường)

Sử dụng originalfilename trường này đảm bảo cảnh báo sẽ được kích hoạt ngay cả khi kẻ tấn công thay đổi tên thực thi Mimikatz.

Giá trị trường đổi thành (?i)mimikatz\.exe

Description để Mimikatz Usage Detected

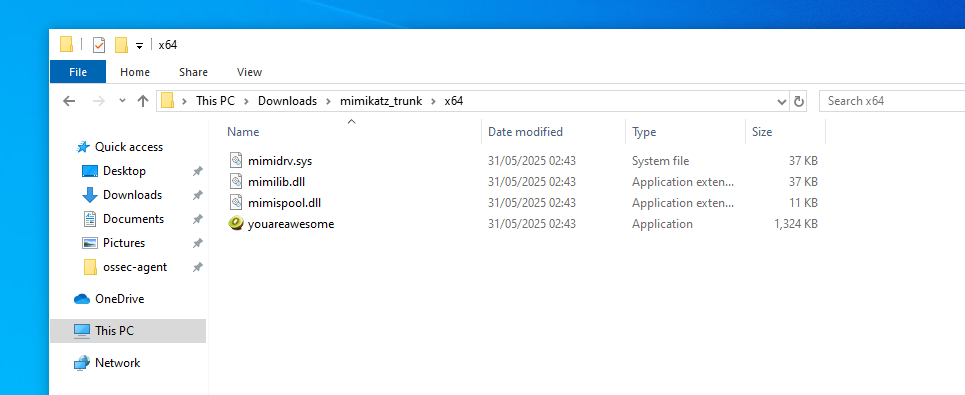
id Mitre để là T1003 vì đó là credential dumping

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó lưu và khởi động lại

ở máy windows đổi tên mimikatz thành youareawesome



Mở powershell và chạy youareawesome.exe

Vào Threat Hunting chọn event sẽ thấy cảnh báo mimikatz. Cảnh báo vẫn được kích hoạt ngay cả khi chúng ta đổi tên tệp vì chúng ta xem originalFileName thay vì chúng ta xem image

A screenshot of a computer

AI-generated content may be incorrect.

Mở shuffle. Vào workflows chon create workflows

Kéo thả 1 webhook đổi tên thành Wazuh-alerts

Vào chang me bấn vào dấu + ở mục call. Mở wazuh để kết nối với shuffle

Dán vào /var/ossec/etc/ossec.conf

<integration>

<name>shuffle</name>

<hook\_url>http**://<YOUR\_SHUFFLE\_URL**>/api/v1/hooks/<HOOK\_ID></hook\_url>

<rule\_id>100002</rule\_id>

<alert\_format>json</alert\_format>

</integration>

Thay vì cảnh báo bằng level chúng ta sẽ đổi thành rule\_id mà ta đã tạo trước đó cho mimikatz

A screenshot of a computer

AI-generated content may be incorrect.

Lưu và khởi động lại dịch vụ: systemctl restart wazuh-manager.service

Mở powershell và chạy lại mimikatz

A computer screen shot of a blue screen

AI-generated content may be incorrect.

Mở shuffle chạy wazuh-alerts

A screenshot of a computer

AI-generated content may be incorrect.

Bấm vào biểu tượng người A black box with white text

AI-generated content may be incorrect.

Và bấn test workflows kiểm tra quy trình làm việc

Ta thấy cảnh báo

A screenshot of a computer

AI-generated content may be incorrect.

**Trích xuất băm SHA256**

Nhấn vào nút **"Change Me"** và chọn **"Regex capture group"** thay cho **"Repeat back to me"**.  
Trong phần **"Input data"**, chọn tùy chọn **"hashes"**.  
Trong tab **"Regex"**, nhập mẫu regex để phân tích giá trị hash SHA256:

SHA256=([0-9A-Fa-f]{64})

Lưu lại workflow.

A screenshot of a computer

AI-generated content may be incorrect.

**Kết nối với virut total**

ở mục change me phàn find action chọn regex capture group

input date chọn hashes

A screenshot of a computer

AI-generated content may be incorrect.

ở phần regex viết regex có thể vào chatgpt viết hộ:  
create regex to parse the sha256 value SHA1=E3B6EA8C46FA831CEC6F235A5CF48B38A4AE8D69,MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5,SHA256=61C0810A23580CF492A6BA4F7654566108331E7A4134C968C2D6A05261B2D8A1,IMPHASH=55EE500BB4BDFC49F27A98AE456D8EDF  
lưu ý hash lấy ở phần hash mimikatz ta vừa test ở trước

ta sẽ được regex: SHA256=([A-F0-9]{64})

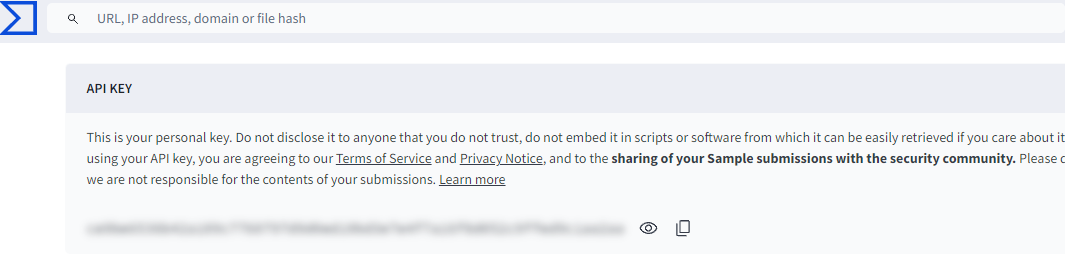
dán vào phần regex ở shuffle và lưu lại

A screenshot of a computer

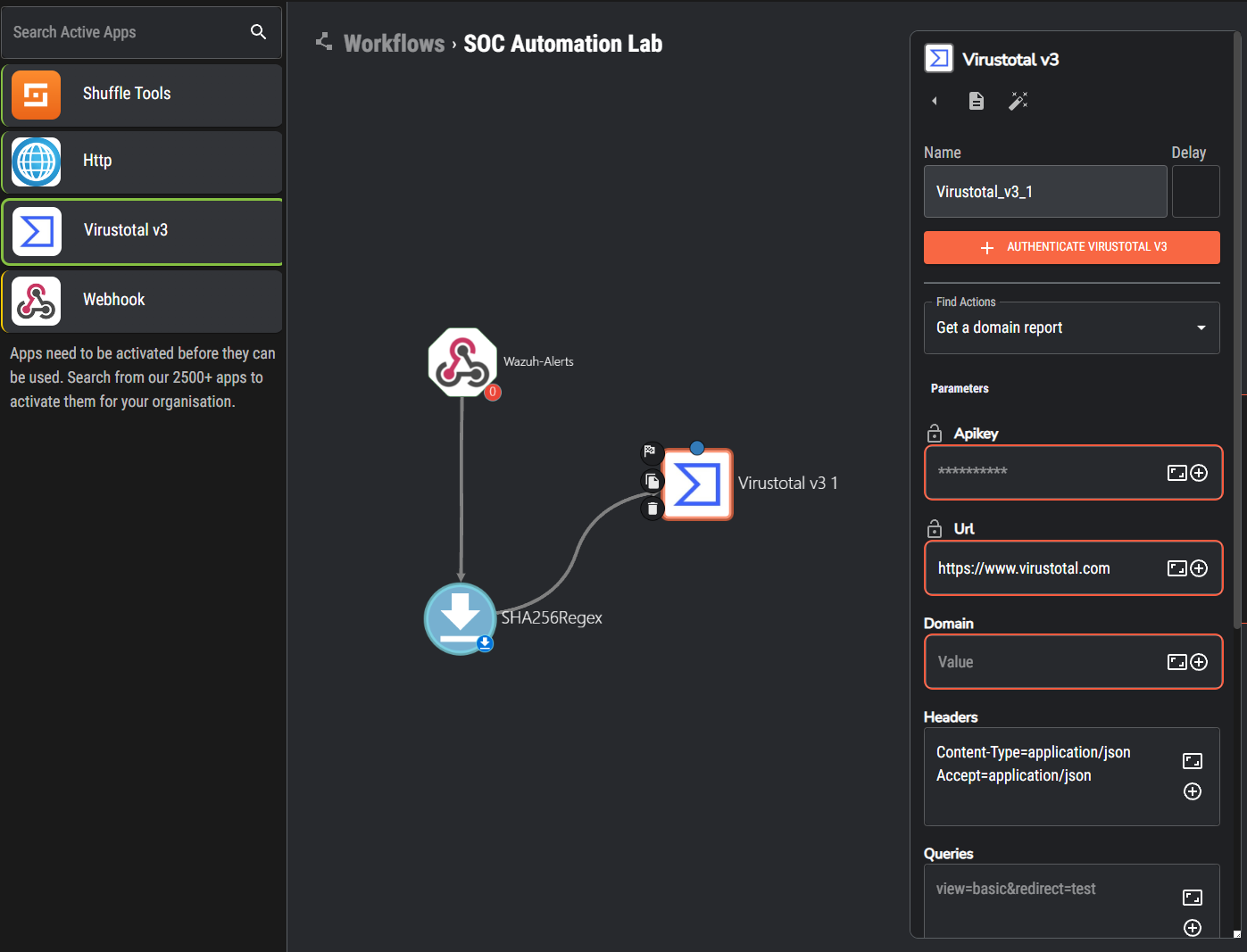
AI-generated content may be incorrect.

Bấm vào biểu tượng hình người và chọn rerun workflow ta tháy nó đã phân tích cú pháp băm sha256

Tạo tài khoản VirusTotal để truy cập API



Sao chép **API key** và quay lại **Shuffle**.  
Trong Shuffle, nhấp vào tab **"Apps"** và tìm **"VirusTotal"**.  
Kéo ứng dụng **VirusTotal** vào workflow, và nó sẽ tự động kết nối.



Nhập **API key** ở phía bên phải hoặc nhấp vào **"Authenticate VirusTotal v3"** để xác thực.

A screenshot of a black box

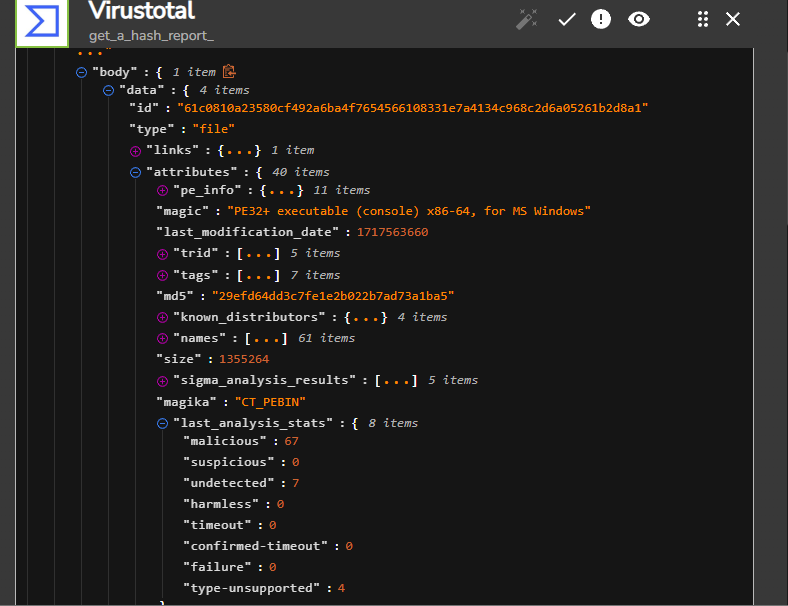
AI-generated content may be incorrect.

Thay đổi trường "ID" thành giá trị "SHA256Regex" đã tạo trước đó.



Lưu quy trình làm việc và chạy lại.

Mở rộng kết quả để xem thông tin chi tiết về quá trình quét VirusTotal, bao gồm số lần phát hiện.



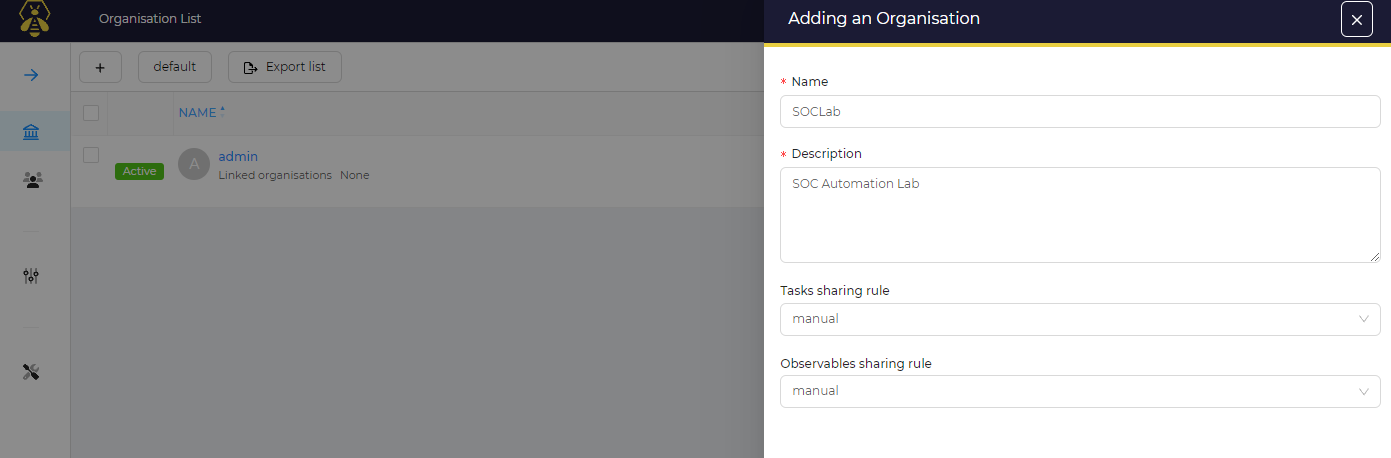
**Tích hợp TheHive:** Trong Shuffle, hãy tìm "TheHive" trong mục "Apps" và kéo nó vào quy trình làm việc.

A screenshot of a computer

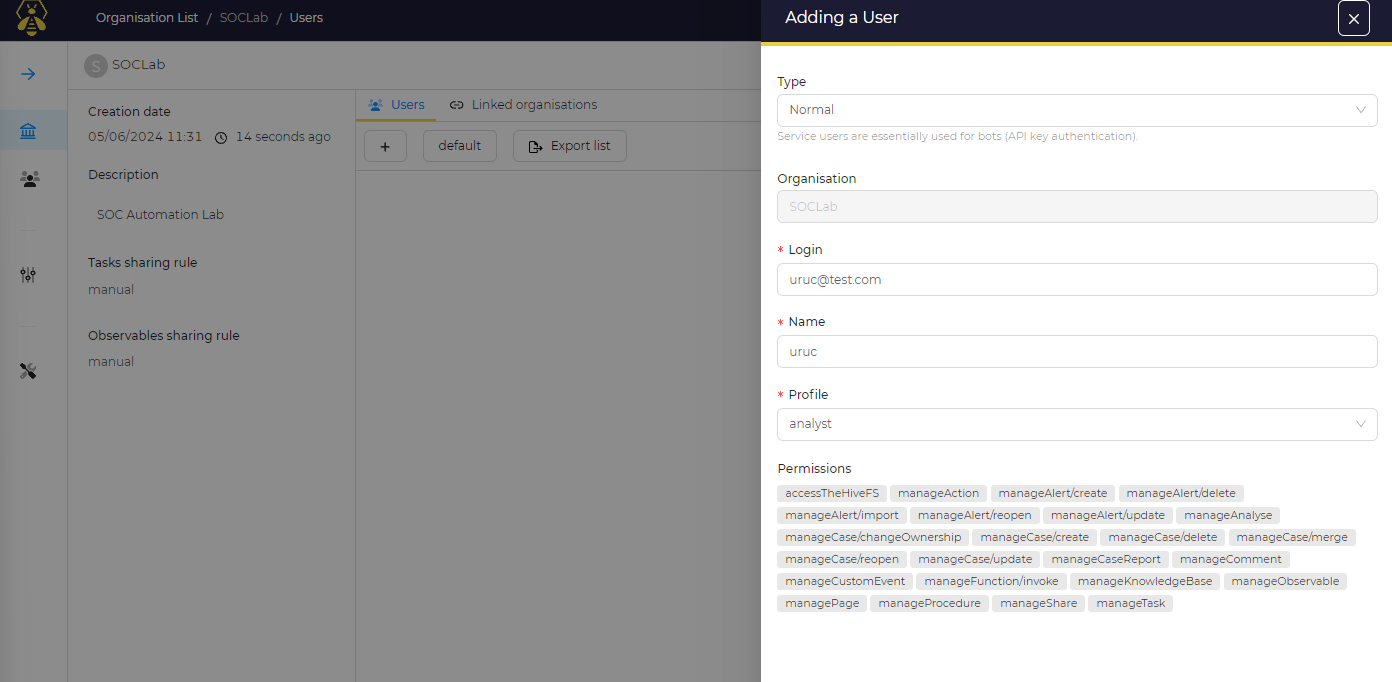
AI-generated content may be incorrect.

Đăng nhập vào TheHive bằng thông tin đăng nhập mặc định: Tên người dùng: admin@thehive.local Mật khẩu:secret

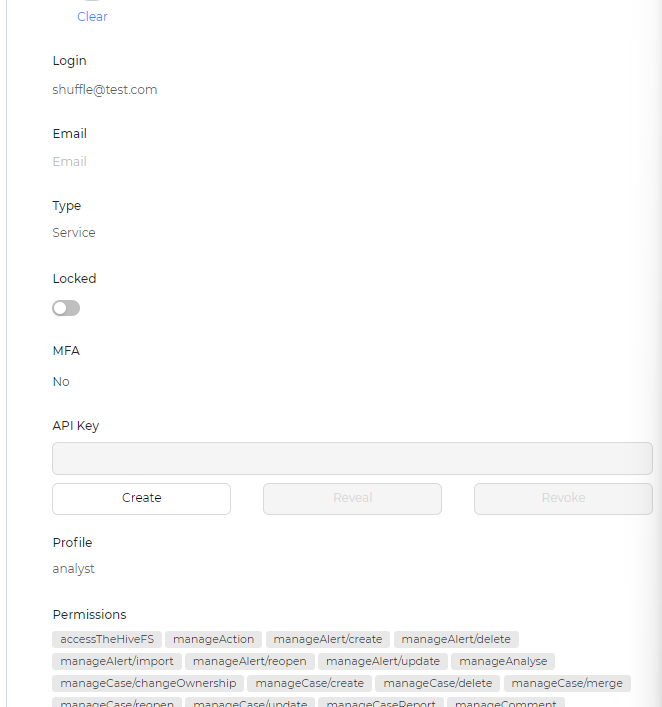
**Cấu hình TheHive:** Tạo tổ chức và người dùng mới cho tổ chức trong TheHive.



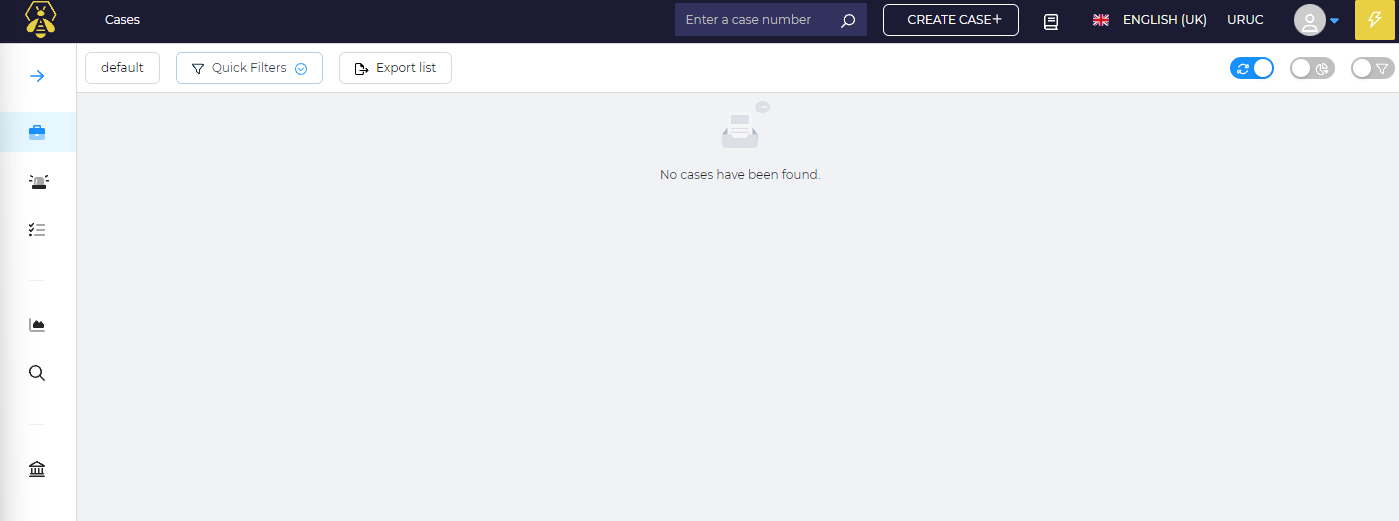
Thêm người dùng mới với các hồ sơ khác nhau khi cần thiết.



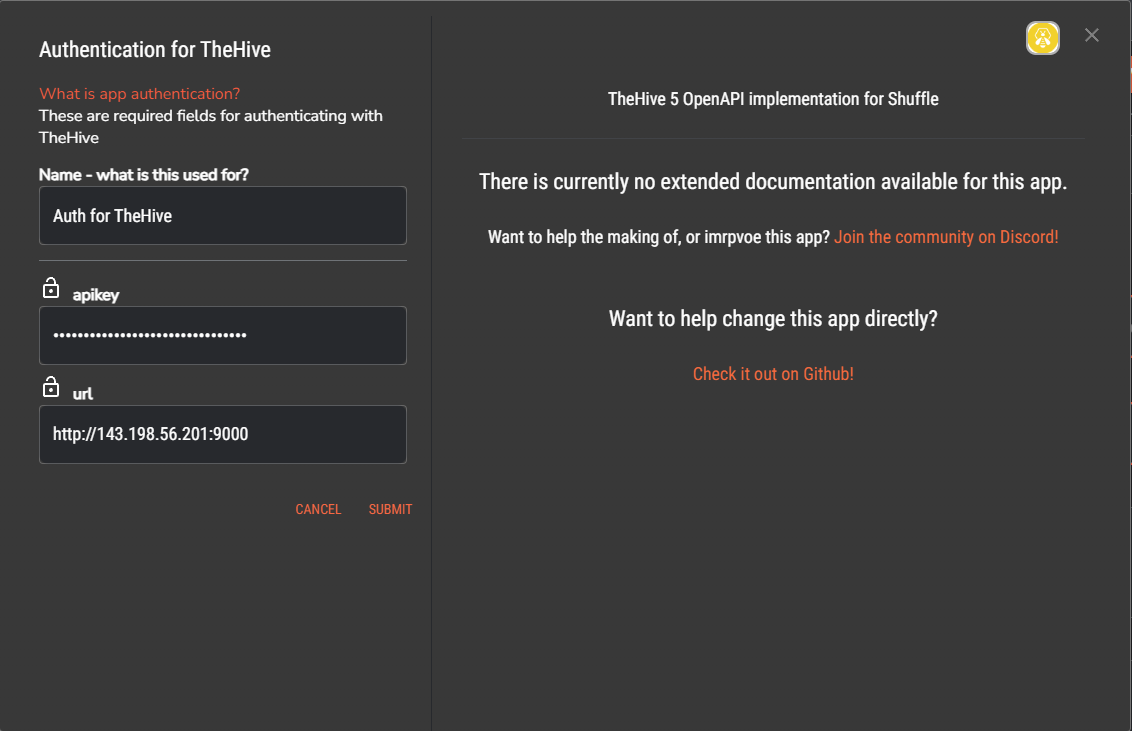
Đặt mật khẩu mới cho người dùng. Đối với người dùng được tạo để tích hợp Shuffle, hãy tạo khóa API.



Tạo khóa API và lưu trữ an toàn. Khóa này sẽ được sử dụng để xác thực Shuffle. Đăng xuất khỏi tài khoản quản trị viên và đăng nhập bằng một trong các tài khoản người dùng.



**Cấu hình Shuffle để hoạt động với TheHive:** Trong Shuffle, nhấp vào nút màu cam "Authenticate TheHive" và nhập khóa API đã tạo trước đó. Đối với URL, hãy nhập địa chỉ IP công khai của TheHive cùng với số cổng



Trong mục **"Find actions"**, nhấp vào **"TheHive"** và chọn **"Create alerts"**.  
Thiết lập **JSON payload** để TheHive nhận cảnh báo.  
Ví dụ payload cho tình huống **Mimikatz** như sau:

{

"description": "Mimikatz Detected on host: DESKTOP-HS8N3J7",

"externallink": "",

"flag": false,

"pap": 2,

"severity": "2",

"source": "Wazuh",

"sourceRef": "Rule:100002",

"status": "New",

"summary": "Details about the Mimikatz detection",

"tags": [

"T1003"

],

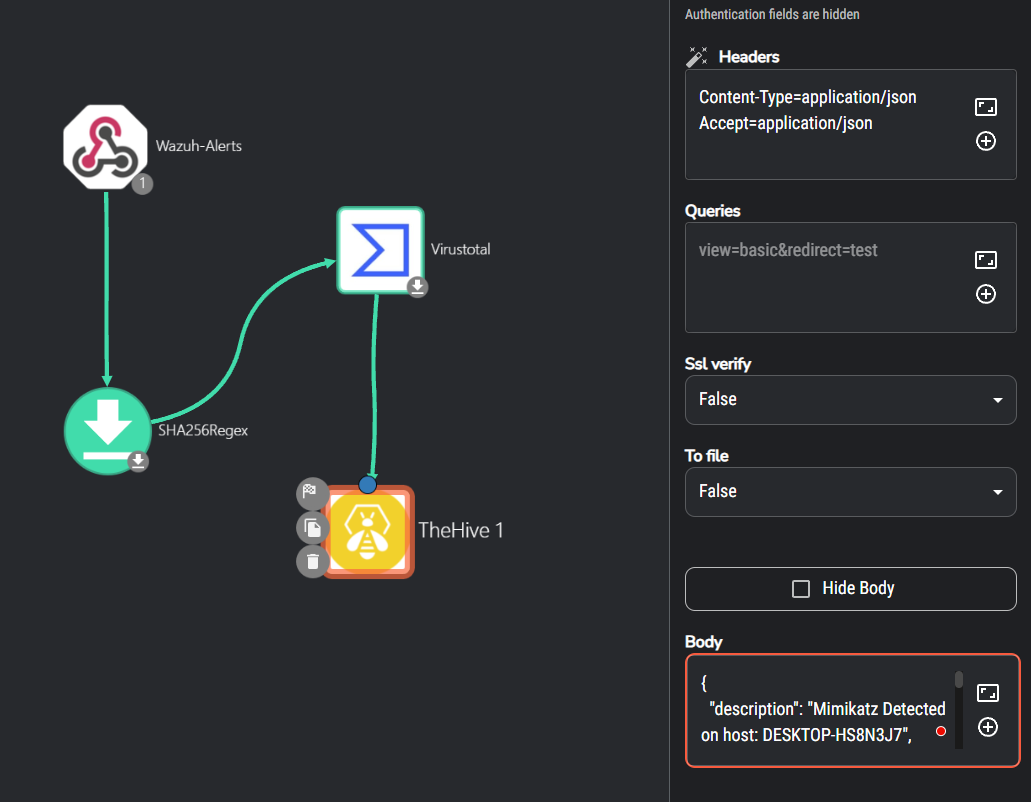
"title": "Mimikatz Detection Alert",

"tlp": 2,

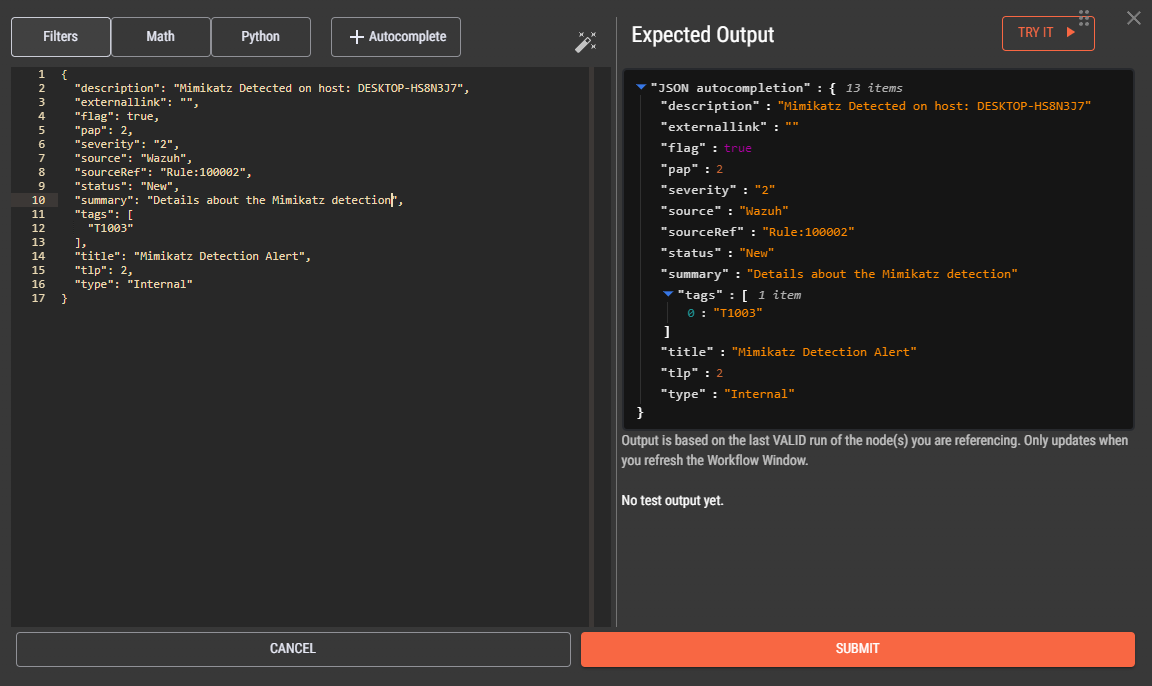
"type": "Internal"

}

Mở rộng phần **"Body"** để thiết lập **payload**.



Đặt tải trọng ở phía bên trái và kiểm tra đầu ra ở phía bên phải.



Lưu quy trình làm việc và chạy lại. Một cảnh báo sẽ xuất hiện trên bảng điều khiển TheHive.

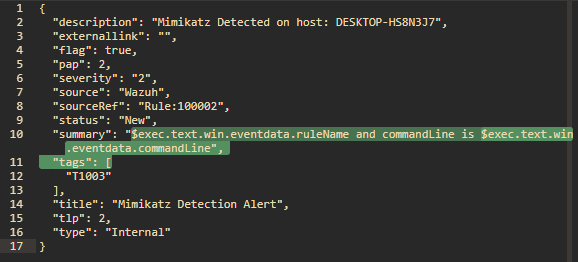
A screenshot of a computer

AI-generated content may be incorrect.

**Lưu ý: Nếu cảnh báo không xuất hiện, hãy đảm bảo rằng tường lửa của TheHive trong nhà cung cấp dịch vụ đám mây của bạn cho phép lưu lượng truy cập đến trên cổng 9000 từ bất kỳ nguồn nào.**

Để thêm thông tin vào cảnh báo, hãy tùy chỉnh các trường trong dữ liệu JSON của TheHive. Ví dụ: hãy tạo một bản tóm tắt chi tiết hơn. Trong Shuffle, hãy nhấp vào nút "Show Body" để xem các trường dữ liệu JSON khả dụng.

Trong trường tóm tắt, bạn có thể bao gồm các chi tiết bổ sung như kỹ thuật và dòng lệnh liên quan đến cảnh báo.



Tham khảo phần nội dung của TheHive trong Shuffle để xác định những gì cần đưa vào các trường này.

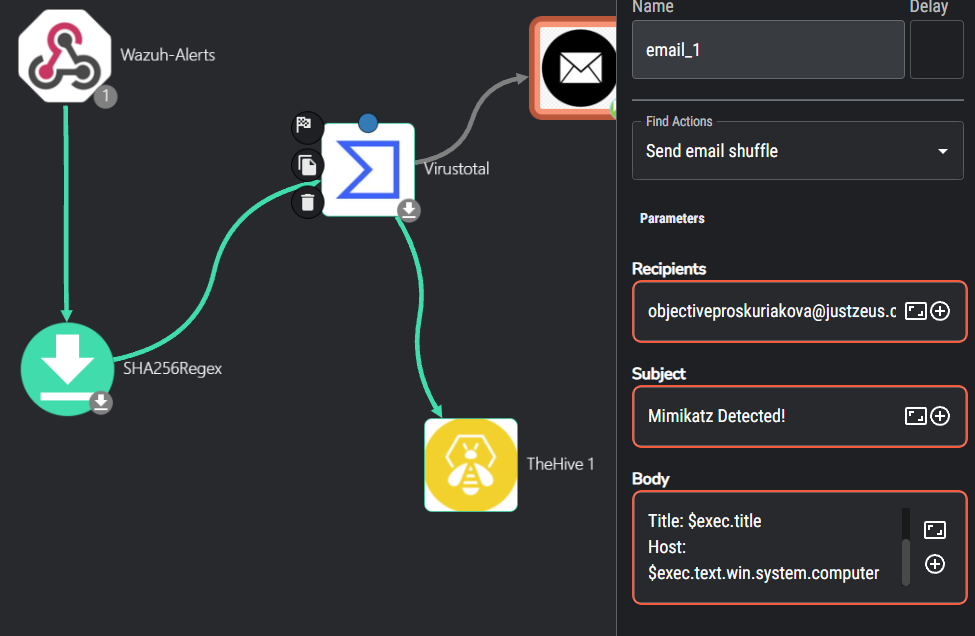


Lưu và chạy lại quy trình làm việc để xem cảnh báo đã cập nhật với nhiều thông tin hơn.

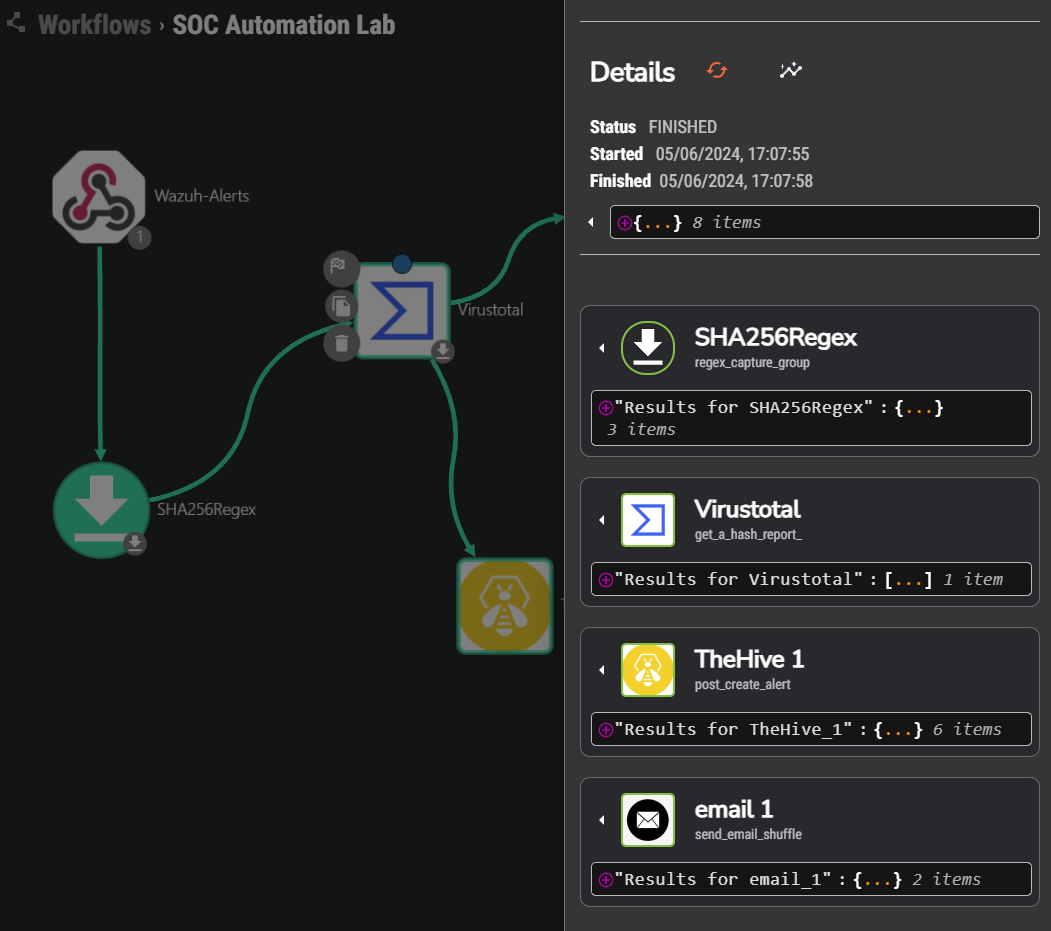
**Gửi thông báo qua email:** Trong Shuffle, tìm "Email" trong "Ứng dụng" và kết nối VirusTotal với nút email. A screenshot of a computer

AI-generated content may be incorrect.

Cấu hình cài đặt email, bao gồm người nhận, chủ đề và nội dung, để gửi cảnh báo kèm theo thông tin sự kiện có liên quan.



Lưu quy trình làm việc và chạy lại.



Xác minh rằng email đã nhận được có chứa thông tin chi tiết cảnh báo mong đợi.