

# Final Year Project

**2nd year engineering student**

# Telecommunications and Networks Engineering



## Security Information and Event Management:

## ELK, Suricata, Logstash/Filebeat, Kibana

**Submitted By :**

FATHI ISMAIL

MAJID MOHAMMED

## Project Guide :

MR. BALBOUL YOUNES

## ACKNOWLEDGMENTS

We thank **Allah** Almighty for giving us the strength and courage to accomplish this work.

Our sincere thanks, accompanied by our gratitude, go to Professor **Balboul Younes**, who as a supervisor, has always been attentive and for their assistance and advice regarding the tasks mentioned in this report. we will always remember their kindness and availability. Please find in this work the expression of our deep respect.

## RESUME

In a global context where businesses are facing information security challenges, cyberattack attempts continue to rise. Beyond the increasing number and evolving threat posed by attackers who exploit organizational uncertainties, it has become crucial for companies to implement robust security measures. One prominent tool in the field of cybersecurity is SIEM (Security Information and Event Management).

By utilizing SIEM, organizations can gain valuable insights into their security posture. It allows for real-time monitoring and analysis of security logs, network traffic, and system events, aiding in the detection and prevention of potential cyber threats. SIEM's comprehensive capabilities and scalability make it suitable for both small and large enterprises.

SIEM provides a comprehensive security solution, offering various functionalities to enhance an organization's security. It combines log management, real-time monitoring, event correlation, and incident response capabilities. By integrating various data sources, SIEM enables organizations to have a centralized view of security events, alerts, and network traffic data, facilitating efficient incident response and threat hunting activities.

In summary, SIEM plays a vital role in addressing the increasing cybersecurity challenges faced by businesses. By leveraging its capabilities, organizations can proactively monitor their security landscape, detect potential threats, and respond effectively to security incidents. The integration of SIEM into their cybersecurity framework strengthens their defenses and helps safeguard critical assets against evolving cyber threats.

**Key words:** SIEM ,ELK stack, Elasticsearch, Logstash, Kibana,Data analysis,Data visualization Real-time monitoring Security logs, Network traffic analysis, System events, Cyber threats, Incident response, Threat hunting, Scalability, Flexible architecture, Intrusion Detection and Prevention System (IDPS), Open-source, Network traffic analysis, Real-time monitoring, Signature-based detection, Behavioral analysis, Anomaly-based detection, Malware infections, Network scans, Intrusion attempts, Security events, Alerts, Incident response, Threat mitigation

## Abstract

Dans un contexte mondial où les entreprises font face à des défis de sécurité de l'information, les tentatives de cyberattaques ne cessent d'augmenter. Au-delà du nombre croissant et de la menace en constante évolution posée par les attaquants qui exploitent les incertitudes organisationnelles, il est devenu crucial pour les entreprises de mettre en place des mesures de sécurité robustes. Un outil de premier plan dans le domaine de la cybersécurité est SIEM (Security Information and Event Management, Gestion des informations et des événements de sécurité).

En utilisant SIEM, les organisations peuvent obtenir des informations précieuses sur leur posture de sécurité. Il permet une surveillance et une analyse en temps réel des journaux de sécurité, du trafic réseau et des événements système, aidant ainsi à la détection et à la prévention des cybermenaces potentielles. Les capacités complètes et la scalabilité de SIEM le rendent adapté aux petites et grandes entreprises.

SIEM offre une solution de sécurité complète, regroupant différentes fonctionnalités pour renforcer la sécurité d'une organisation. Il combine la gestion des journaux, la surveillance en temps réel, la corrélation des événements et les capacités de réponse aux incidents. En intégrant diverses sources de données, SIEM permet aux organisations d'avoir une vue centralisée des événements de sécurité, des alertes et des données de trafic réseau, facilitant ainsi une réponse efficace aux incidents et des activités de recherche de menaces.

En résumé, SIEM joue un rôle essentiel dans la résolution des défis croissants en matière de cybersécurité auxquels sont confrontées les entreprises. En exploitant ses capacités, les organisations peuvent surveiller proactivement leur paysage de sécurité, détecter les menaces potentielles et y répondre efficacement. L'intégration de SIEM dans leur infrastructure de cybersécurité renforce leurs défenses et contribue à la protection des actifs critiques contre les menaces cybernétiques en constante évolution.

**Mots-clés :** ELK stack, Elasticsearch, Logstash, Kibana, Analyse des données, Visualisation des données, Surveillance en temps réel, Journaux de sécurité, Analyse du trafic réseau, Événements système, Menaces cybernétiques, Réponse aux incidents, Recherche de menaces, Scalabilité, Architecture flexible, Système de Détection et de Prévention d'Intrusion (IDPS), Open-source, Analyse du trafic réseau, Surveillance en temps réel, Détection basée sur des signatures, Analyse comportementale, Détection basée sur des anomalies, Infections par des logiciels malveillants, Scans réseau, Tentatives d'intrusion, Événements de sécurité, Alertes, Réponse aux incidents, Atténuation des menaces.

## Table of Contents

ACKNOWLEDGMENTS .....	2
RESUME .....	3
Abstract.....	4
LIST OF FIGURES .....	7
General Introduction .....	9
1st Chapter: Definition and Literature review .....	10
1- Introduction:.....	10
2- Definition: .....	10
How it works:.....	10
Why do we need it .....	12
3- Comparison between popular SIEM solutions.....	13
Splunk .....	13
QRadar .....	13
Exabeam.....	14
Elastic Stack.....	14
4- Rationale for Employing Elastic Stack .....	15
5- Comprehensive Overview of Elastic Stack Tools.....	16
Elasticsearch: .....	16
Logstash .....	16
Kibana.....	16
Beats.....	17
Elasticsearch Machine Learning .....	17
Elasticsearch Security .....	17
6- Overview of Suricata .....	18
Definition: .....	18
Features:.....	18
7- Illustration of Log Flow Diagram .....	19
8- Conclusion .....	20
2nd Chapter: Implementation and Test.....	21
1- Introduction.....	21
The goal of the implementation. ....	21
The setup environment: one server hosting all the tools and an Ubuntu client as an Apache client. .	21

1- Suricata Configuration .....	23
Installing Suricata .....	23
Configuring Suricata .....	24
Understand the Suricata rules format .....	25
Rule example: .....	26
2- ELK Stack, Kibana, Logstash/Filebeat Installation and Configuration .....	26
installing Elasticsearch.....	26
Configuring ELK .....	27
Installing Logstash (if applicable).....	29
Configuring Logstash.....	29
Installing Kibana.....	31
Configuring Kibana. ....	31
Installing Filebeat.....	32
Configuring Filebeat. ....	32
Configuration steps for integrating Suricata logs with the ELK.....	33
Additional settings or modifications made to optimize the SIEM environment.....	33
3- Client Configuration .....	34
Apache Installation. ....	34
Filebeat installation and configuration.....	35
Why we used Filebeat instead of Logstash .....	37
4- Test Scenario Setup.....	37
The test scenario and objectives.....	37
Test results .....	37
5- Conclusion .....	43
Conclusion .....	44
Webography.....	45

## LIST OF FIGURES

Figure 1: SIEM solution.....	10
Figure 2: SIEM process .....	11
Figure 3: SIEM Functionalities.....	12
Figure 4: Splunk's LOGO.....	13
Figure 5: QRadar LOGO .....	13
Figure 6: EXABEAM's LOGO .....	14
Figure 7: Elastic Stack's LOGO .....	14
Figure 8: Elasticsearch's logo .....	16
Figure 9: Logstash's LOGO .....	16
Figure 10: Kibana's LOGO.....	16
Figure 11: Beats's LOGO.....	17
Figure 12: Elasticsearch Security's LOGO.....	17
Figure 13: Elastic Stack Home .....	17
Figure 14: Suricata's LOGO .....	18
Figure 15: Suricata Event Overview.....	19
Figure 16: Log Flow Diagram .....	19
Figure 17: Setup Environment .....	21
Figure 18 : Steps to setup environment.....	22
Figure 19 : VMware configuration for SIEM SERVER.....	22
Figure 20 : VMware configuration: CLIENT .....	23
Figure 21 : Add the Open Information Security Foundation's (OISF) software repository information ...	23
Figure 22 : install the suricata package.....	23
Figure 23 : start suricata.....	24
Figure 24 : Stop suricata .....	24
Figure 25 : Identify the Network interface's name.....	24
Figure 26 : Editing suricata's configuration file.....	24
Figure 27 : Suricata configuration .....	25
Figure 28 : Update Suricata's rulesets.....	25
Figure 29 : Suricata's Rule example .....	26
Figure 30 : Start Suricata .....	26
Figure 31 : Adding the elastic GPG key .....	26
Figure 32 : adding the Elastic source list to the sources.list.d directory .....	26
Figure 33 : update the server's package index.....	26
Figure 34 : installing Elasticsearch and kibana.....	26
Figure 35 : Configuring Elasticsearch Networking .....	27
Figure 36 : single node and security features.....	27
Figure 37 : allow incoming traffic on the network interface.....	27
Figure 38 : allow the outgoing traffic on the network interface.....	28
Figure 39 : Generate users's passwords .....	28
Figure 40 : Elasticsearch users's credentials .....	28
Figure 41 : Generate xpack security secrets for Kibana.....	31
Figure 42 : Kibana's secrets.....	31
Figure 43 : add secrets to kibana's configuration file .....	31
Figure 44 : Configuring Kibana Networking .....	31

Figure 45 : Configuring Kibana Credentials.....	32
Figure 46 : start kibana .....	32
Figure 47 : Installing Filebeat .....	32
Figure 48 : filebeat configuration file.....	32
Figure 49 : adding network configuration & credentials to filebeat configuration file .....	32
Figure 50 : Enable Filebeat's built-in suricata module .....	33
Figure 51 : Load the SIEM dashboards and pipelines into Elasticsearch .....	33
Figure 52 : start filebeat.....	33
Figure 53 : Jvm options file for ELK.....	33
Figure 54 : Activating IPS mode in suricata.....	34
Figure 55 : Installing apache .....	34
Figure 56 : Kibana section modification.....	35
Figure 57 : Elasticsearch output modification .....	35
Figure 58 : modify filebeat's predefined module for apache .....	36
Figure 59 : Adding the paths to apache Logs.....	36
Figure 60 : Load modules to Elasticsearch server.....	36
Figure 61 : output of Filebeat setup command .....	36
Figure 62 : Suricata Rule for test.....	37
Figure 63 : visite the test domain .....	37
Figure 64 : access to Kibana .....	38
Figure 65 : Kibana Home page .....	38
Figure 66 : Search in Kibana Modules.....	39
Figure 67 : Suricata dashboard .....	39
Figure 68 : Suricata's Event section .....	40
Figure 69 : Suricata's alerts section .....	40
Figure 70 : Test Event.....	41
Figure 71 : Test Alert in diagram.....	41
Figure 72 : Test Alert.....	42
Figure 73 : Test Alert information.....	42
Figure 74 : Discover Section in Kibana .....	43
Figure 75 : Apache Logs .....	43



## **General Introduction**

In today's rapidly evolving digital landscape, organizations face an ever-increasing number of sophisticated cyber threats. Protecting sensitive information, preserving operational continuity, and safeguarding against malicious activities have become critical imperatives for businesses of all sizes. To address these challenges, organizations are turning to Security Information and Event Management (SIEM) solutions. This report provides a comprehensive analysis of SIEM, its significance in cybersecurity, and its ability to enhance an organization's overall security posture. The introduction of SIEM marks a paradigm shift in the way organizations approach security. SIEM represents a holistic solution that combines Security Information Management (SIM) and Security Event Management (SEM) capabilities, offering a centralized platform for collecting, analyzing, and correlating security event logs and information from diverse sources within an organization's IT infrastructure. The importance of SIEM lies in its ability to enhance an organization's overall security posture. By implementing a SIEM solution, organizations can proactively monitor their IT infrastructure, identify security incidents in real-time, and respond swiftly and effectively. SIEM enables early threat detection, reduces incident response times, enhances incident investigation capabilities, and supports compliance efforts.

In conclusion, SIEM represents a crucial component of a robust cybersecurity strategy. Its ability to collect, analyze, and correlate security events from diverse sources enables organizations to gain comprehensive visibility, detect anomalies, and respond swiftly to potential threats. By leveraging the features and capabilities of SIEM, organizations can significantly enhance their security posture, minimize vulnerabilities, and ensure the protection of critical assets in the face of evolving cyber threats.

# 1st Chapter: Definition and Literature review

## 1- Introduction:

Security Information and Event Management (SIEM) has emerged as a crucial component in modern cybersecurity strategies. In an era where businesses face an ever-evolving landscape of cyber threats, organizations need robust tools to protect their sensitive information, detect anomalies, and respond swiftly to potential security incidents.

## 2- Definition:

SIEM, which stands for Security Information and Event Management, is a crucial technology in the field of cybersecurity. It serves as a comprehensive software solution that combines the functionalities of Security Information Management (SIM) and Security Event Management (SEM). The primary purpose of SIEM is to provide organizations with a centralized platform for collecting, storing, analyzing, and correlating security event logs and information from various sources within their IT infrastructure.



Figure 1: SIEM solution

### How it works:

-SIEM enables organizations to achieve comprehensive visibility into their security landscape. By aggregating logs and events from diverse sources such as network devices, servers, applications, and security tools, SIEM empowers security teams to monitor, analyze, and respond to security incidents in real-time. This centralized approach allows for efficient monitoring, analysis, and correlation of security events, providing crucial insights into potential threats and vulnerabilities.

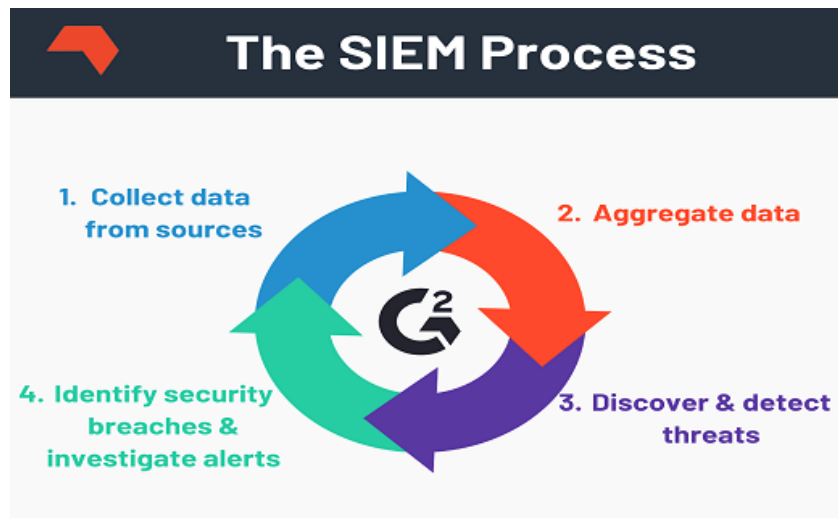


Figure 2: SIEM process

-One of the key features of SIEM is log collection and storage. SIEM systems gather security logs and events from multiple sources and store them in a centralized repository. This enables easy access and retrieval of critical security data for analysis and investigation purposes. Real-time monitoring and analysis are also essential aspects of SIEM. It continuously monitors security events, leveraging advanced analytics, correlation rules, and behavioral analysis techniques to identify patterns and anomalies that may indicate security incidents or potential threats.

-SIEM's event correlation and alerting capabilities are crucial for effective threat detection. It correlates and analyzes security events across multiple data sources, enabling the identification of complex relationships and the generation of timely alerts. These alerts notify security teams about potential threats, facilitating rapid response and mitigation.

-SIEM also offers incident response and workflow automation, streamlining incident response workflows by providing automated response actions, predefined workflows, and playbooks. This ensures that security incidents are promptly identified, analyzed, and mitigated, minimizing the potential impact. Compliance and reporting features are also integral to SIEM systems, assisting organizations in meeting regulatory requirements by generating comprehensive reports, audit trails, and evidence of security controls.

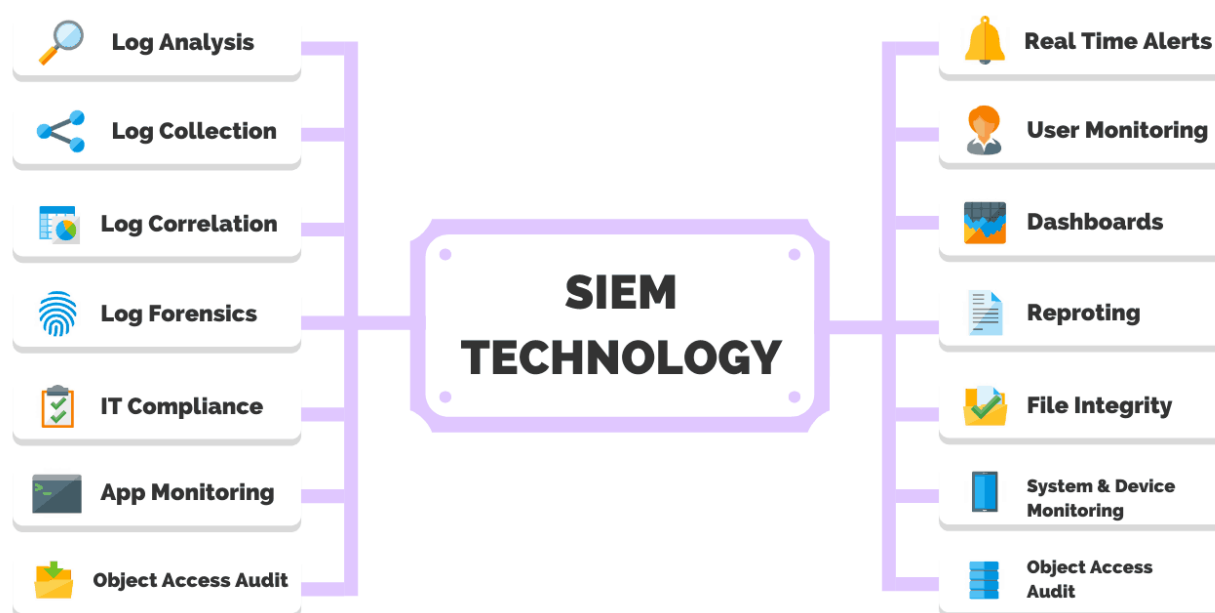


Figure 3: SIEM Functionalities

### Why do we need it

SIEM is essential because it provides organizations with comprehensive visibility into their security landscape. With the increasing complexity and frequency of cyber threats, organizations need a centralized platform to monitor, analyze, and respond to security incidents in real-time. SIEM enables efficient log collection, storage, and correlation, allowing for the detection of potential threats and vulnerabilities. It offers real-time monitoring, event correlation, and automated response actions, streamlining incident response workflows. SIEM also supports compliance efforts by generating reports and audit trails. In today's threat landscape, SIEM is crucial for organizations to proactively protect their critical assets and mitigate risks effectively.

### 3- Comparison between popular SIEM solutions

Having gained an understanding of the concept and functionality of SIEM, as well as its significance in enhancing an organization's security posture, it is now imperative to explore renowned SIEM solutions in the market.

**Splunk, QRadar, Exabeam, and ELK (Elasticsearch, Logstash, and Kibana)** are all popular SIEM solutions that provide organizations with comprehensive security information and event management capabilities. However, there are some differences among them in terms of features, architecture, and deployment options.

#### **Splunk**

Splunk is known for its powerful search and analytics capabilities. It offers a user-friendly interface and supports various data sources, allowing organizations to collect, analyze, and visualize data from multiple systems. Splunk's strength lies in its ability to handle large volumes of data and perform real-time monitoring and analysis. It also offers a wide range of pre-built apps and integrations, making it highly customizable and adaptable to different use cases.



Figure 4: Splunk's LOGO

#### **QRadar**

QRadar, developed by IBM, is recognized for its advanced threat detection and analytics capabilities. It utilizes AI and machine learning techniques to detect anomalies and potential threats. QRadar offers extensive log correlation, event aggregation, and provides real-time visibility into security incidents. It also integrates well with other IBM security products, allowing for a comprehensive security ecosystem.



Figure 5: QRadar LOGO

### **Exabeam**

Exabeam is known for its user and entity behavior analytics (UEBA) capabilities. It focuses on detecting insider threats and anomalies in user behavior. Exabeam combines data from multiple sources, including logs, endpoints, and cloud services, to identify suspicious activities and potential threats. It utilizes machine learning algorithms to establish a baseline of normal behavior and identify deviations that may indicate malicious intent.



**Figure 6: EXABEAM's LOGO**

### **Elastic Stack**

ELK, or the Elastic Stack, is an open-source SIEM solution consisting of Elasticsearch, Logstash, and Kibana. It offers flexibility and scalability, allowing organizations to collect, process, store, and visualize large amounts of data. ELK provides powerful search capabilities, log parsing, and real-time analytics. It can be customized and extended based on specific requirements and is suitable for organizations that prefer open-source solutions.



**Figure 7: Elastic Stack's LOGO**

#### **4- Rationale for Employing Elastic Stack**

Now that we gained a comprehensive understanding of the distinguishing features among various SIEM solutions, it is now imperative to elucidate the rationale behind our selection of Elastic Stack.

we choose the Elastic Stack, consisting of Elasticsearch, Logstash, and Kibana, over other SIEM solutions such as Splunk, QRadar, and Exabeam for several reasons:

1. Cost-effectiveness: Elastic Stack is an open-source solution, which means it offers a more cost-effective option compared to proprietary solutions like Splunk and QRadar. The availability of community support and a vast library of plugins and integrations further adds to its cost-saving advantage.
2. Flexibility and scalability: Elastic Stack provides high flexibility, allowing organizations to customize and adapt the solution to their specific needs. It offers a scalable architecture that can handle large volumes of data, making it suitable for organizations with diverse and evolving security requirements.
3. Powerful search capabilities: Elastic Stack excels in its search functionality, offering robust search capabilities across vast amounts of data. Elasticsearch, the primary component of the stack, provides fast and efficient search and indexing capabilities, enabling organizations to quickly retrieve and analyze security information.
4. Data processing and analysis: With Logstash, Elastic Stack enables efficient data processing and parsing. It supports a wide range of data formats, allowing organizations to easily collect, transform, and enrich data from various sources. This flexibility in data handling contributes to effective security event analysis.
5. Visualization and analytics: Kibana, the visualization component of Elastic Stack, offers rich visualizations, dashboards, and reporting features. It allows security teams to gain actionable insights from security data, facilitating threat detection, incident response, and compliance reporting.
6. Community and ecosystem: Elastic Stack benefits from a large and active community of users, developers, and contributors. The community-driven nature of the solution ensures continuous improvement, regular updates, and extensive support. Additionally, Elastic Stack integrates well with other tools and technologies, making it easy to integrate into existing IT environments.

## 5- Comprehensive Overview of Elastic Stack Tools

Elastic Stack comprises several powerful tools that collectively provide a comprehensive solution for data collection, processing, storage, search, analysis, visualization, and reporting. The core components of Elastic Stack are as follows:

### Elasticsearch:



elasticsearch

Elasticsearch serves as the heart of the Elastic Stack. It is a highly scalable and distributed search and analytics engine that allows for real-time exploration and analysis of structured and unstructured data. Elasticsearch provides fast indexing, robust search capabilities, and supports complex queries for retrieving and analyzing data efficiently.

Figure 8: Elasticsearch's logo

### Logstash



Logstash is a versatile data processing pipeline tool that facilitates the ingestion, transformation, and enrichment of data from various sources. It supports a wide range of data inputs, including logs, metrics, and event streams, and enables users to apply filters, parse data, and normalize it for indexing into Elasticsearch.

Figure 9: Logstash's LOGO

### Kibana



Kibana is a powerful visualization and exploration platform that works seamlessly with Elasticsearch. It provides a user-friendly interface for creating dynamic dashboards, visualizing data through charts, graphs, and maps, and conducting ad-hoc data exploration. Kibana enables users to gain valuable insights from the data stored in Elasticsearch and effectively communicate findings.

Figure 10: Kibana's LOGO





Beats are lightweight data shippers that collect and send data from various sources to Elasticsearch or Logstash. There are different types of Beats available, including Filebeat for log files, Metricbeat for system and application metrics, Packetbeat for network traffic analysis, and more. Beats simplify the process of data collection and enhance the scalability and efficiency of data ingestion.

### Elasticsearch Machine Learning

Elasticsearch Machine Learning (ML) is an advanced feature that leverages machine learning algorithms to automatically detect anomalies and patterns in data. It helps identify unusual behaviors, detect security threats, and uncover valuable insights from large datasets, enabling proactive monitoring and efficient threat detection.

### Elasticsearch Security



Elasticsearch Security provides robust access control and authentication mechanisms to ensure secure data access and protect sensitive information. It allows fine-grained control over user roles and permissions, supports integration with external authentication systems, and enables encryption of data in transit.

Figure 12: Elasticsearch Security's LOGO

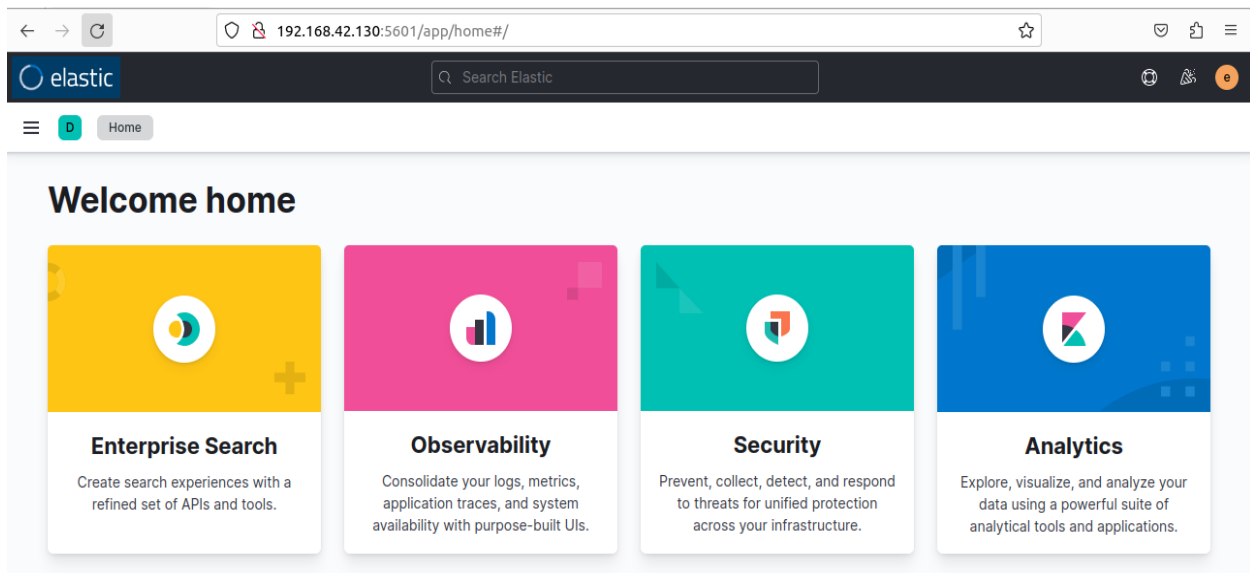


Figure 13: Elastic Stack Home

## 6- Overview of Suricata

### Definition:



Figure 14: Suricata's LOGO

Suricata is a high-performance open-source Intrusion Detection and Prevention System (IDPS) that provides network security monitoring and threat detection capabilities. It is designed to analyze network traffic in real-time and detect suspicious or malicious activities. Suricata is known for its ability to inspect network packets at high speed and perform deep packet inspection (DPI) to identify various types of network-based threats.

### Features:

Suricata is equipped with a powerful rule-based detection engine that allows security analysts to define custom rules to detect specific network-based attacks, such as malware infections, network scans, intrusion attempts, and more. It supports signature-based detection, where predefined patterns or signatures of known threats are matched against the network traffic, as well as behavioral and anomaly-based detection to identify unusual or abnormal network behavior.

In addition to its detection capabilities, Suricata also offers a range of features for network security monitoring and analysis. It can generate detailed alerts and logs, providing valuable information about detected threats and their associated network activities. Suricata integrates with various security tools and SIEM systems, allowing for centralized management and correlation of security events and alerts.

Suricata's open-source nature makes it highly customizable and extensible. It has an active community of developers and users who contribute to its ongoing development and provide support. Suricata is widely used in both enterprise and community environments, offering a flexible and effective solution for network security monitoring, threat detection, and incident response.

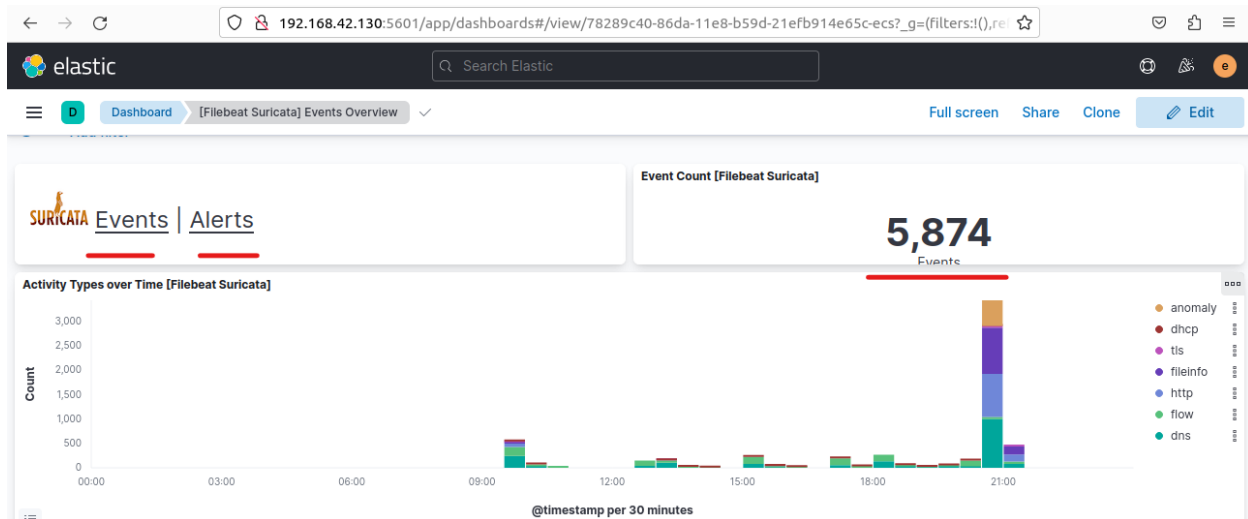


Figure 15: Suricata Event Overview

## 7- Illustration of Log Flow Diagram

In an intricate network environment, log flow plays a crucial role in capturing and analyzing valuable information from various sources. Servers, applications, and endpoints generate copious amounts of log data, serving as a vital source of insights for security and operational purposes. However, to effectively harness this data, a well-defined log flow process is essential.

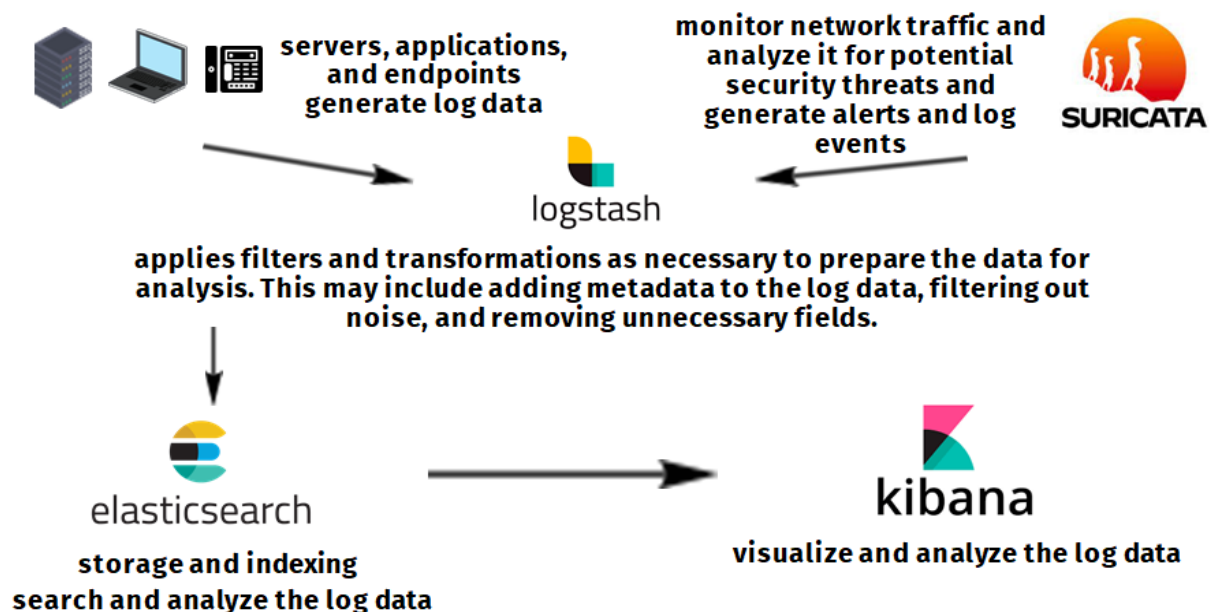


Figure 16: Log Flow Diagram

To begin, log data originating from servers, applications, and endpoints undergoes collection and analysis by Suricata, a powerful Intrusion Detection and Prevention System (IDPS). Suricata scrutinizes network traffic, identifying potential threats and generating relevant security alerts and logs.

The next phase involves the ingestion and processing of log data using Logstash, a versatile data processing pipeline tool. Logstash facilitates the extraction, transformation, and enrichment of log data, ensuring compatibility and uniformity before transmission.

Once processed, the log data is seamlessly forwarded to Elasticsearch, a highly scalable and distributed search and analytics engine. Elasticsearch acts as a centralized repository, storing the log data in a structured manner, facilitating efficient indexing and retrieval.

Finally, the log data is visualized and analyzed in Kibana, a powerful visualization and exploration platform. Kibana empowers users to create dynamic dashboards, generate insightful visualizations, and perform ad-hoc data exploration. Through Kibana's intuitive interface, security analysts and stakeholders gain valuable insights, enabling them to identify trends, detect anomalies, and derive actionable intelligence from the log data.

## **8- Conclusion**

In this chapter, we have explored the definitions and concepts related to SIEM (Security Information and Event Management) systems. We conducted a literature review to establish a solid foundation for understanding the importance of SIEM in monitoring and securing network infrastructure. Through our research, we gained insights into the key components and functionalities of SIEM solutions. Considering the available options, we made the decision to work with the ELK Stack (Elasticsearch, Logstash/Filebeat, and Kibana) due to its robust capabilities in log analysis, visualization, and scalability. This choice will enable us to leverage the advanced features of ELK Stack to enhance our security monitoring capabilities and gain valuable insights from log data. The knowledge acquired from the literature review will serve as a valuable reference throughout the subsequent chapters, where we will delve into the implementation and testing of our chosen SIEM solution.

## 2nd Chapter: Implementation and Test

### 1- Introduction

#### The goal of the implementation.

The goal of the implementation phase is to successfully configure and integrate the SIEM components, including Suricata, ELK Stack (Elasticsearch, Logstash/Filebeat, Kibana), and the Apache client, to establish a comprehensive security monitoring system. This implementation aims to demonstrate the effective detection, analysis, and visualization events using Suricata rules, ELK Stack, and Filebeat. Through this implementation, we aim to showcase the practical application and functionality of the SIEM solution, highlighting its ability to enhance network security and provide actionable insights for incident response and threat mitigation.

#### The setup environment: one server hosting all the tools and an Ubuntu client as an Apache client.

We used two Virtual machines to implement our system, one for the SIEM and one for the client: Vmware workstation as a virtualization environment .

Vm1: SIEM SERVER (ubuntu-22.04.1-live-server)

Vm2: Client (ubuntu-22.04-desktop)

We will install all tools in the SIEM server because of our limited recourses.

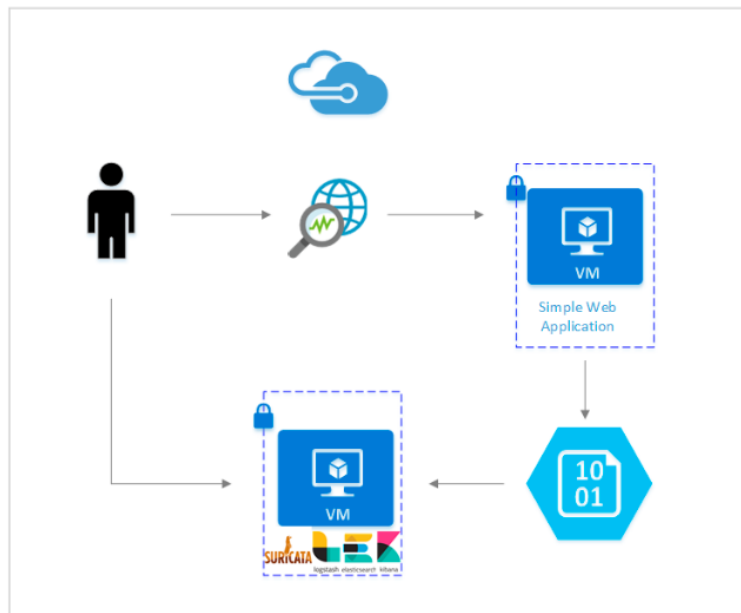


Figure 17: Setup Environment

Steps:

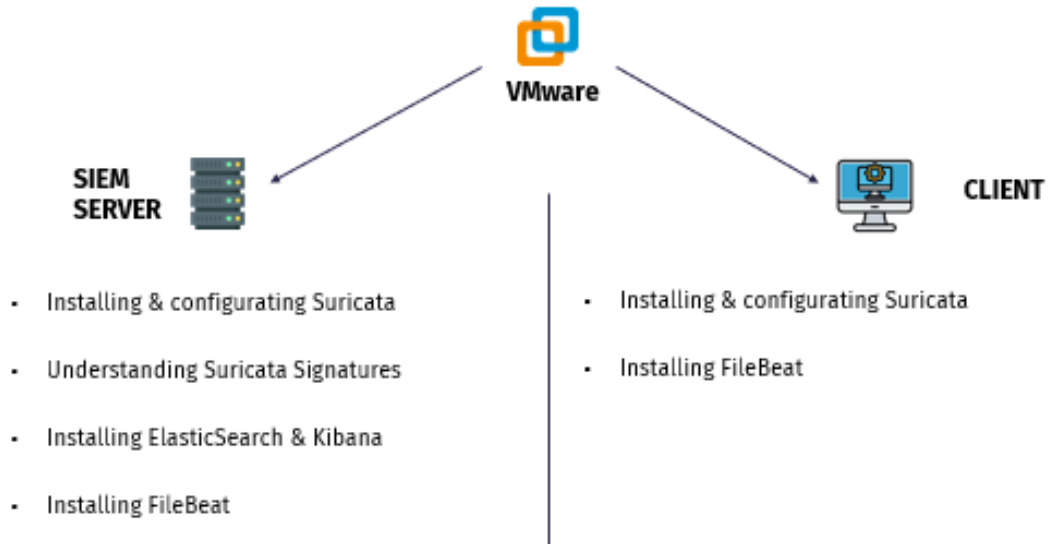


Figure 18 : Steps to setup environment

VMware Configuration :

SIEM SERVER :

RAM : 8GB

CPU : 2

Storage : 30GB

Network configuration : NAT

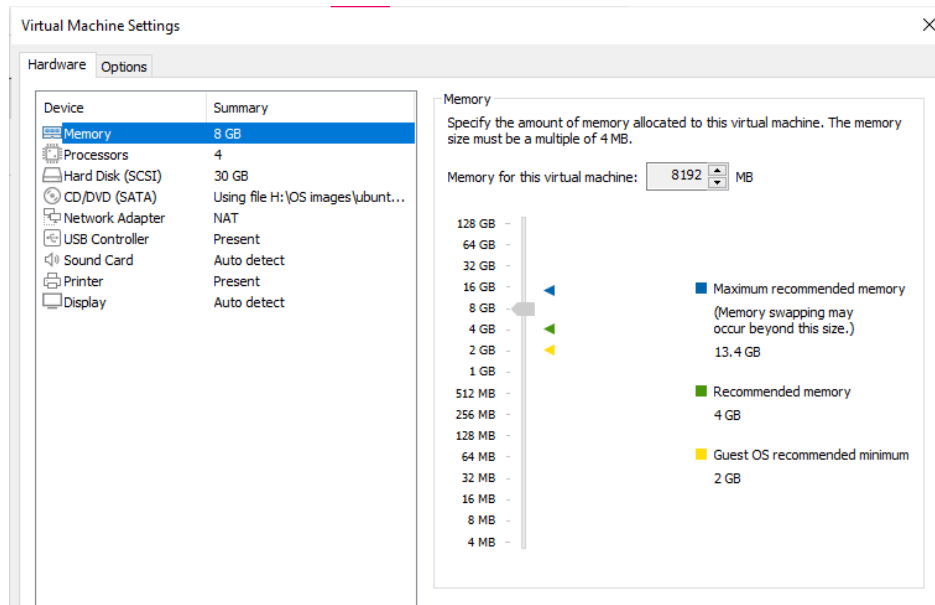


Figure 19 : VMware configuration for SIEM SERVER

CLIENT:

RAM: 2.5 GB

CPU: 2

Storage : 20GB

Network configuration : NAT

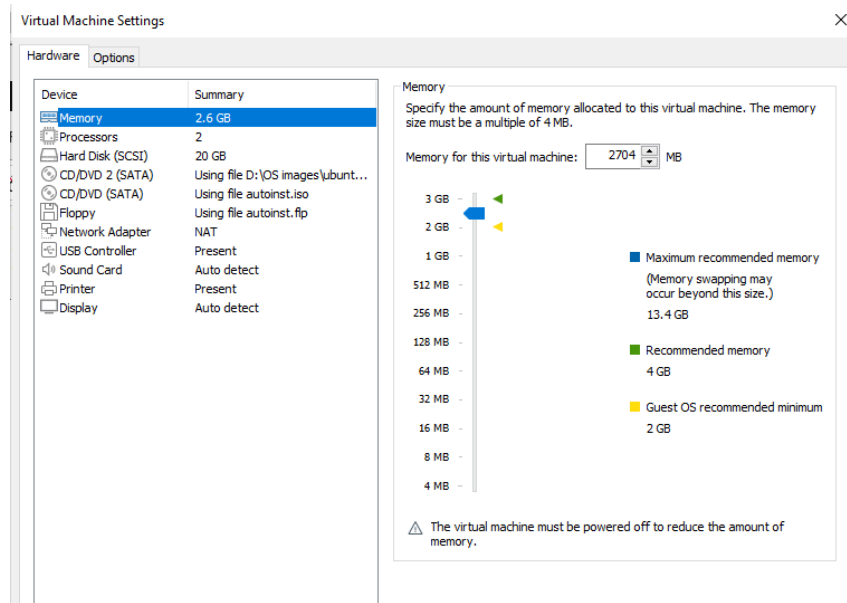


Figure 20 : VMware configuration: CLIENT

After finishing this part, we will start with configuring Suricata in the SIEM server.

## 1- Suricata Configuration

### Installing Suricata

1. Add the Open Information Security Foundation's (OISF) software repository information to your Ubuntu system. We can use the `add-apt-repository` command to do this.

```
siemadmin@siemadmin:~$ sudo add-apt-repository ppa:oiscf/suricata-satble
```

Figure 21 : Add the Open Information Security Foundation's (OISF) software repository information

2. install the Suricata package using the `apt` command:

```
siemadmin@siemadmin:~$ sudo apt install suricata
```

Figure 22 : install the suricata package

### 3. Start and Stop Suricata using the systemctl command:

```
siemadmin@siemadmin:~$ sudo systemctl start suricata
```

Figure 23 : start suricata

```
siemadmin@siemadmin:~$ sudo systemctl stop suricata
```

Figure 24 : Stop suricata

Stopping Suricata ensures that any changes made to the configuration file are validated and loaded when Suricata starts up again after the modification and testing process.

We will keep it stopped until editing and testing the configuration file.

#### Configuring Suricata

To customize the network interface(s) for Suricata to inspect traffic on, you may need to override the default settings. By default, the configuration file provided with the OISF Suricata package assumes the inspection of traffic on a device named eth0. However, if your system utilizes a different default network interface or you want to inspect traffic on multiple interfaces, you will have to modify this setting.

To identify the device name of your default network interface, you can employ the ip command in the following manner:

```
siemadmin@siemadmin:~$ ip -p -j route show default
[ {
  "dst": "default",
  "gateway": "192.168.42.2",
  "dev": "ens33",
  "protocol": "dhcp",
  "prefsrc": "192.168.42.130",
  "metric": 100,
  "flags": [ ]
} ]
```

Figure 25 : Identify the Network interface's name

Add the interfaces that you would like Suricata to inspect traffic on (by default is eth0) , we will add our interface .

We used nano command to modify our configuration file:

```
siemadmin@siemadmin:~$ sudo nano /etc/suricata/suricata.yaml
```

Figure 26 : Editing suricata's configuration file



```
GNU nano 6.2 /etc/suricata/suricata.yaml
##
# Linux high speed capture support
af-packet:
- interface: ens33
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per packet
  # This is only supported for Linux kernel > 3.1
```

Figure 27 : Suricata configuration

If you were to start Suricata, you would receive a warning message say there are no loaded rules.

By default, the Suricata package includes a limited set of detection rules (in the /etc/suricata/rules directory), so turning Suricata on at this point would only detect a limited amount of bad traffic. Suricata includes a tool called suricata-update that can fetch rulesets from external providers.

We will run it as follows to download an up-to-date ruleset for your Suricata server:

```
siemadmin@siemadmin:~$ sudo suricata-update
```

Figure 28 : Update Suricata's rulesets

suricata-update will fetch the free Emerging Threats ET Open Rules, and saved them to Suricata's /var/lib/suricata/rules/suricata.rules file.

## Understand the Suricata rules format

```
[alert][ip any any -> any any](msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|")
```

Action	Header	Options
--------	--------	---------

**Action:** An Action to take when traffic matches the rule:

**Pass:** passing packets without alerts

**Drop:** stop processing the packet and generate an alert

**Reject:** drop the matching packet.

**Alert:** Suricata will generate an alert and log it for further analysis.

**Header:** header section that describes the network protocol, source and destination IP addresses, ports, and direction of traffic.

<PROTOCOL> <SOURCE IP> <SOURCE PORT> -> <DESTINATION IP> <DESTINATION PORT>

**Options:** which specify things like the Signature ID (sid), log message, regular expressions that match the contents of packets, classification type, and other modifiers that can help narrow identify legitimate and suspicious traffic.

### Rule example:

```
alert https any any -> 192.168.42.130 any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown)
```

Figure 29 : Suricata's Rule example

If a packet from any address and any port to our server in any port contain the content : uid=0(Root) , suricata will generate an alert and we will see the results in the test part .

Run Suricata:

```
siemadmin@siemadmin:~$ sudo systemctl start suricata.service
```

Figure 30 : Start Suricata

## 2- ELK Stack, Kibana, Logstash/Filebeat Installation and Configuration

### installing Elasticsearch

```
siemadmin@siemadmin:~$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

Figure 31 : Adding the elastic GPG key

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

Figure 32 : adding the Elastic source list to the sources.list.d directory

```
siemadmin@siemadmin:~$ sudo apt update
```

Figure 33 : update the server's package index

```
siemadmin@siemadmin:~$ sudo apt install elasticsearch kibana
```

Figure 34 : installing Elasticsearch and kibana

The configuration file: **/etc/elasticsearch/elasticsearch.yml**

## Configuring Elasticsearch Networking :

We uncomment the indicated line and we add our privet IP : in all next sections our Privet IP is 192.168.42.130

```
GNU nano 6.2 /etc/elasticsearch/elasticsearch.yml
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 192.168.0.1
#network.host: localhost
network.bind_host: ["127.0.0.1", "192.168.42.130"]
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
```

### Figure 35 : Configuring Elasticsearch Networking

```
discovery.type: single-node
xpack.security.enabled: true
```

**Figure 36 : single node and security features**

The `discovery.type` setting allows Elasticsearch to run as a single node, as opposed to in a cluster of other Elasticsearch servers.

The `xpack.security.enabled` setting turns on some of the security features that are included with Elasticsearch.

## Firewall rules:

Finally, we add firewall rules to ensure our Elasticsearch server is reachable on its private network interface :

```
siemadmin@siemadmin:~$ sudo ufw allow in on ens33
```

**Figure 37 : allow incomming traffic on the network interface**

```
siemadmin@siemadmin:~$ sudo ufw allow out on ens33
```

Figure 38 : allow the outgoing traffic on the network interface

### Configuring Elasticsearch Passwords:

Now that we have enabled the `xpack.security.enabled` setting, we need to generate passwords for the default Elasticsearch users. Elasticsearch includes a utility in the `/usr/share/elasticsearch/bin` directory that can automatically generate random passwords for these users.

Those users are for authentication purpose for Kibana and Filebeats , we can use the utility one time for that , we saved the result in a separate file to save it .

```
siemadmin@siemadmin:~$ cd /usr/share/elasticsearch/bin
```

```
siemadmin@siemadmin:/usr/share/elasticsearch/bin$ sudo ./elasticsearch-setup-passwords auto
```

Figure 39 : Generate users's passwords

These are our credentials:

```
siemadmin@siemadmin:~$ cat passwords.txt
Changed password for user apm_system
PASSWORD apm_system = yNTBzVONjtOGZToXJg5v

Changed password for user kibana_system
PASSWORD kibana_system = 86xHaovILpmRjFpaCYm2

Changed password for user kibana
PASSWORD kibana = 86xHaovILpmRjFpaCYm2

Changed password for user logstash_system
PASSWORD logstash_system = M07NTULq8cwIKefjyliw

Changed password for user beats_system
PASSWORD beats_system = mZdZjkLzdWfPAXwajXL7

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = y8rl5TgZ9WW77xYEYJDc

Changed password for user elastic
PASSWORD elastic = xaNu2vZPtH7LQIywE74N
siemadmin@siemadmin:~$
```

Figure 40 : Elasticsearch users's credentials

### Installing Logstash (if applicable)

in our environment we did not use Logstash to reduce consumption of server resources, but if you want to use it these are the configurations required:

run the following command to install it :

```
curl -L -O https://artifacts.elastic.co/downloads/logstash/logstash-5.2.0.deb
```

```
sudo dpkg -i logstash-5.2.0.deb
```

### Configuring Logstash

we need to configure Logstash to read from the file output of eve.json of suricata

Create a logstash.conf file using:

```
sudo touch /etc/logstash/conf.d/logstash.conf
```

Add the following content to the file (make sure the path to the eve.json file is correct):

```
input {
  file {
    path => ["/var/log/suricata/eve.json"]
    codec => "json"
    type => "SuricataIDPS"
  }
}

filter {
  if [type] == "SuricataIDPS" {
    date {
      match => [ "timestamp", "ISO8601" ]
    }
    ruby {
      code => "
        if event.get('[event_type]') == 'fileinfo'
          event.set('[fileinfo][type]',
event.get('[fileinfo][magic]').to_s.split(',')[0])
        end
      "
    }
  }

  ruby{
    code => "
      if event.get('[event_type]') == 'alert'
        sp = event.get('[alert][signature]').to_s.split(' group ')
        if (sp.length == 2) and /\A\d+\z/.match(sp[1])
          event.set('[alert][signature]', sp[0])
        end
      end
    "
  }
}
```

```

        end
        "
    }
}

if [src_ip] {
    geoip {
        source => "src_ip"
        target => "geoip"
        #database => "/opt/logstash/vendor/geoip/GeoLiteCity.dat"
        add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
        add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]
    }
    mutate {
        convert => [ "[geoip][coordinates]", "float" ]
    }
    if ![geoip.ip] {
        if [dest_ip] {
            geoip {
                source => "dest_ip"
                target => "geoip"
                #database => "/opt/logstash/vendor/geoip/GeoLiteCity.dat"
                add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
            ]
            add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]
        ]
    }
    mutate {
        convert => [ "[geoip][coordinates]", "float" ]
    }
}
}

output {
    elasticsearch {
        hosts => "localhost"
    }
}

```

Make sure to grant the correct permissions for the eve.json file so that Logstash can ingest the file ;

```
sudo chmod 775 /var/log/suricata/eve.json
```

To start Logstash, run the command:

```
sudo /etc/init.d/logstash start
```

### Installing Kibana.

We already install it with elasticsearch see the figure 34 .

### Configuring Kibana.

We configured Elasticsearch to listen for connections on our Elasticsearch server's private IP address. we will need to do the same for Kibana;

First, we will enable Kibana's xpack security functionality by generating some secrets that Kibana will use to store data in Elasticsearch. Then we will configure Kibana's network setting and authentication details to connect to Elasticsearch.

```
siemadmin@siemadmin:~$ cd /usr/share/kibana/bin/
```

```
siemadmin@siemadmin:~$ sudo ./kibana-encryption-keys generate -q
```

Figure 41 : Generate xpack security secrets for Kibana

```
siemadmin@siemadmin:~$ cat kibana_keys
xpack.encryptedSavedObjects.encryptionKey: 41afbf231ec790aa3d6e085343c010d9
xpack.reporting.encryptionKey: 702c4b1665c74f679a3012e1d8eef222
xpack.security.encryptionKey: e1cf4fa79f70aff14af4a77747cdc0ae
siemadmin@siemadmin:~$
```

Figure 42 : Kibana's secrets

- Add the xpack keys at the end of the configuration file : `/etc/kibana/kibana.yml`

```
xpack.encryptedSavedObjects.encryptionKey: b44611edc3f00e7acc3e9eef5c1e8f5c
xpack.reporting.encryptionKey: c446454a949bd67c30712347fcbe38af
xpack.security.encryptionKey: ed22083dafcd3d6a13380ab7f528f168
```

Figure 43 : add secrets to kibana's configuration file

- Configuring Kibana Networking

```
#server.host: "localhost"
server.host: "192.168.42.130"
# Enables you to specify a path to
# Use the `server.configBasePath`
```

Figure 44 : Configuring Kibana Networking

- Configuring Kibana Credentials

```
# is proxied through the Kibana server.  
elasticsearch.username: "kibana_system"  
elasticsearch.password: "86xHaovILpmRjFpaCYm2"
```

Figure 45 : Configuring Kibana Credentials

Start Kibana:

```
siemadmin@siemadmin:~$ sudo systemctl start kibana.service
```

Figure 46 : start kibana

### Installing Filebeat.

Install filebeat with the following command :

```
siemadmin@siemadmin:~$ sudo apt install filebeat
```

Figure 47 : Installing Filebeat

### Configuring Filebeat.

Filebeat configuration file : /etc/filebeat/filebeat.yml

```
siemadmin@siemadmin:~$ sudo nano /etc/filebeat/filebeat.yml
```

Figure 48 : filebeat configuration file

```
# This requires a Kibana endpoint configuration.  
setup.kibana:  
  
# Kibana Host  
# Scheme and port can be left out and will be set to the default (http and 5601)  
# In case you specify an additional path, the scheme is required: http://localhost:5601/path  
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601  
#host: "localhost:5601"  
host: "192.168.42.130:5601"  
# Kibana Space ID  
# ID of the Kibana Space into which the dashboards should be loaded. By default,  
# the Default Space will be used.  
#space.id:
```

Figure 49 : adding network configuration & credentials to filebeat configuration file



## Configuration steps for integrating Suricata logs with the ELK

Now we must enable Filebeat's built-in Suricata module with the following command:

```
siemadmin@siemadmin:~$ sudo filebeat modules enable suricata
```

Figure 50 : Enable Filebeat's built-in suricata module

Now that Filebeat is configured to connect to Elasticsearch and Kibana, with the Suricata module enabled, the next step is to load the SIEM dashboards and pipelines into Elasticsearch.

Run the filebeat setup command. It may take a few minutes to load everything:

```
siemadmin@siemadmin:~$ sudo filebeat setup
```

Figure 51 : Load the SIEM dashboards and pipelines into Elasticsearch

Start filebeat :

```
sudo systemctl start filebeat.service
```

Figure 52 : start filebeat

## Additional settings or modifications made to optimize the SIEM environment.

*How to make ELK use less of resources.*

We must modify the jvm options of Elasticsearch :

Change to the root user by running : `sudo su`

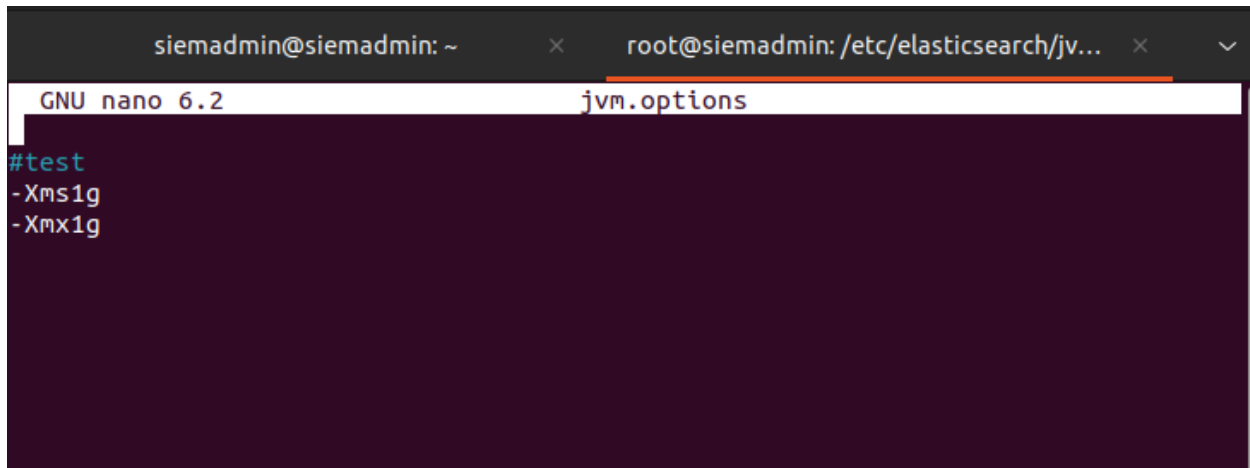
Place in the following directory : `/etc/elasticsearch/jvm.options.d/`

Run the following command to modify or add this file : `nano jvm.options`

```
siemadmin@siemadmin: ~ x root@siemadmin: /etc/elasticsearch/jv... x v
siemadmin@siemadmin:~$ sudo su
root@siemadmin:/home/siemadmin# cd /etc/elasticsearch/jvm.options.d/
root@siemadmin:/etc/elasticsearch/jvm.options.d# nano jvm.options
root@siemadmin:/etc/elasticsearch/jvm.options.d#
```

Figure 53 : Jvm options file for ELK

Add these lines , they mean that ELK must use 1GB as a minimum and maximum value for the usage of memory , be sure that you have write the same value for the both , you can use 512m as a value if you want .

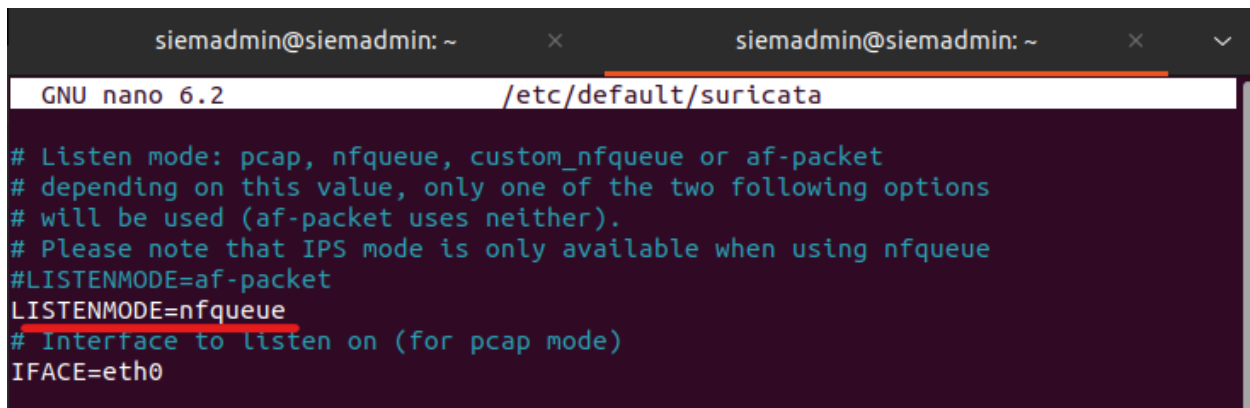


```
siemadmin@siemadmin: ~ x root@siemadmin: /etc/elasticsearch/jv... x v
GNU nano 6.2 jvm.options
#test
-Xms1g
-Xmx1g
```

### *Activating Suricata IPS mode*

Suricata runs in IDS mode by default, which means it will not actively block network traffic. To switch to IPS mode, you'll need to edit Suricata's /etc/default/suricata configuration file.

Find the LISTENMODE=af-packet line and comment it out by adding a # to the beginning of the line. Then add a new line LISTENMODE=nfqueue line that tells Suricata to run in IPS mode.



```
siemadmin@siemadmin: ~ x siemadmin@siemadmin: ~ x v
GNU nano 6.2 /etc/default/suricata
# Listen mode: pcap, nfqueue, custom_nfqueue or af-packet
# depending on this value, only one of the two following options
# will be used (af-packet uses neither).
# Please note that IPS mode is only available when using nfqueue
#LISTENMODE=af-packet
LISTENMODE=nfqueue
# Interface to listen on (for pcap mode)
IFACE=eth0
```

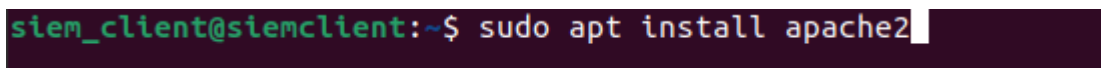
Figure 54 : Activating IPS mode in suricata

Then restart suricata .

## **3- Client Configuration**

### **Apache Installation.**

Installing Apache:



```
siem_client@siemclient:~$ sudo apt install apache2
```

Figure 55 : Installing apache

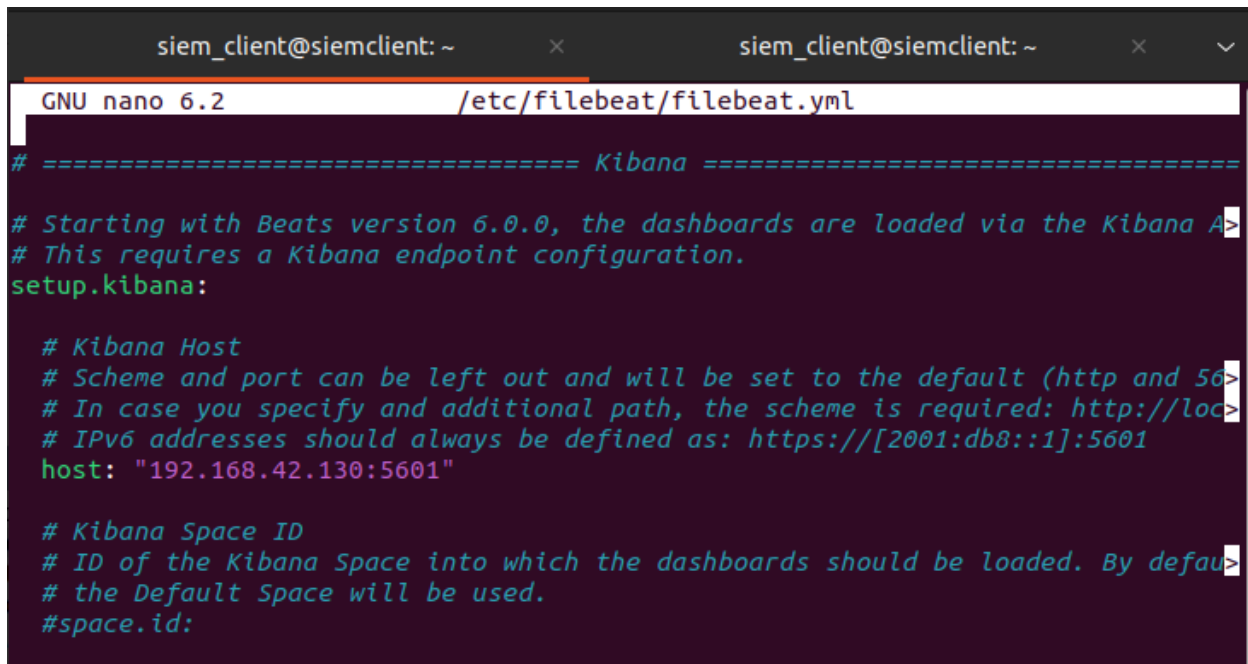
## Filebeat installation and configuration.

Run the two command in figure 31 and 32 .

Update the client package with : `sudo apt update`

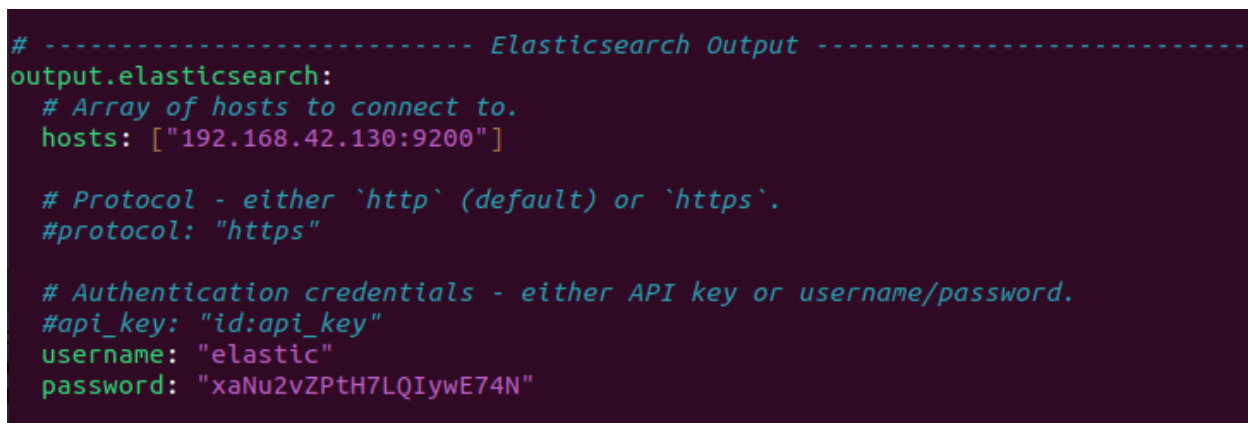
Install filebeat with : `sudo apt install filebeat` .

Network configuration : add the IP adresse of the server with the 5601 port in the kibana section and add it also in the elasticsearch output section , if you are using Logstash keep the elasticsearch output commented and modify the Logstash output with the IP adresse of the server and his credentials , in our case we work with elasticsearch output .



```
siem_client@siemclient: ~  
GNU nano 6.2 /etc/filebeat/filebeat.yml  
# ===== Kibana =====  
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.  
# This requires a Kibana endpoint configuration.  
setup.kibana:  
  
# Kibana Host  
# Scheme and port can be left out and will be set to the default (http and 5601).  
# In case you specify an additional path, the scheme is required: http://localhost:5601/path  
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601  
host: "192.168.42.130:5601"  
  
# Kibana Space ID  
# ID of the Kibana Space into which the dashboards should be loaded. By default, the  
# the Default Space will be used.  
#space.id:
```

Figure 56 : Kibana section modification



```
# ----- Elasticsearch Output -----  
output.elasticsearch:  
# Array of hosts to connect to.  
hosts: ["192.168.42.130:9200"]  
  
# Protocol - either `http` (default) or `https`.  
#protocol: "https"  
  
# Authentication credentials - either API key or username/password.  
#api_key: "id:api_key"  
username: "elastic"  
password: "xANu2vZPtH7LQIywE74N"
```

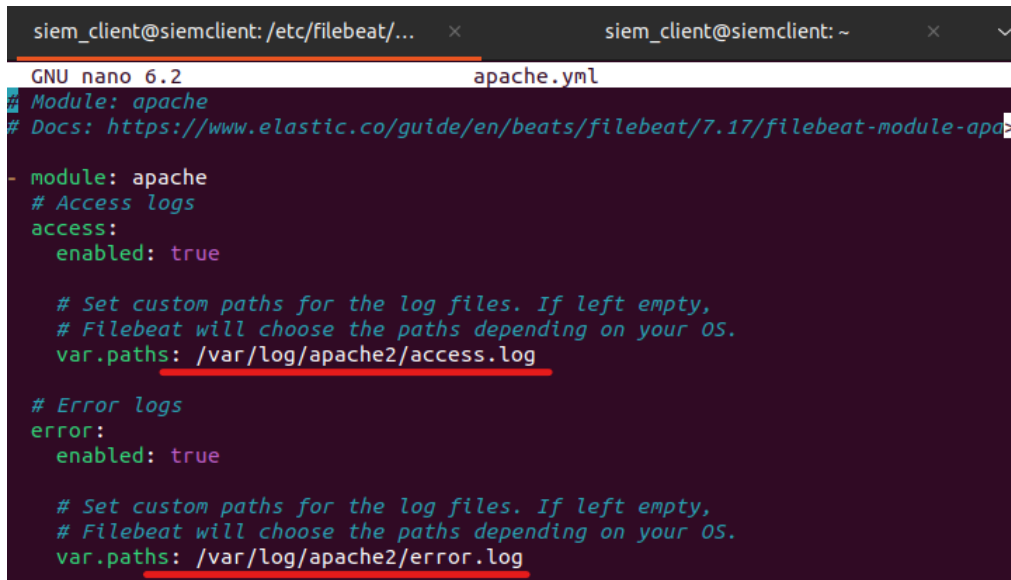
Figure 57 : Elasticsearch output modification

We must modify the predefined module in filebeat configuration to collect logs from the apache's Logs

Modify or creat the apache.yml in this directory : /etc/filebeat/modules.d

```
siem_client@siemclient:/etc/filebeat/modules.d$ sudo nano apache.yml
```

Figure 58 : modify filebeat's predefined module for apache



```
siem_client@siemclient:/etc/filebeat/... x siem_client@siemclient: ~ x v
GNU nano 6.2 apache.yml
# Module: apache
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-apache.html

- module: apache
  # Access logs
  access:
    enabled: true

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  var.paths: /var/log/apache2/access.log

  # Error logs
  error:
    enabled: true

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  var.paths: /var/log/apache2/error.log
```

Figure 59 : Adding the paths to apache Logs

```
siem_client@siemclient:/usr/share/filebeat/bin$ sudo filebeat setup
```

Figure 60 : Load modules to Elasticsearch server

Output must be like the following :

```
siem_client@siemclient:/usr/share/filebeat/bin$ sudo filebeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling
.
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.
See more: https://www.elastic.co/guide/en/machine-learning/current/index.html
It is not possible to load ML jobs into an Elasticsearch 8.0.0 or newer using the Beat.
Loaded machine learning job configurations
Loaded Ingest pipelines
siem_client@siemclient:/usr/share/filebeat/bin$
```

Figure 61 : output of Filebeat setup command

## Why we used Filebeat instead of Logstash .

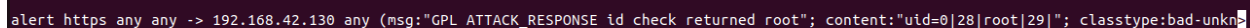
The decision to use Filebeat instead of Logstash was motivated by the goal of optimizing resource usage. Filebeat's lightweight nature and reduced memory footprint make it a favorable choice in environments where resource constraints are a concern. By eliminating the need for an additional component, Logstash, Filebeat simplifies the architecture and improves overall efficiency. Its streamlined log forwarding mechanism ensures minimal overhead and faster delivery of logs to Elasticsearch for analysis. This choice enables scalability, as Filebeat can be easily deployed across multiple servers without significant resource strain. Overall, Filebeat strikes a balance between resource efficiency and effective log collection, enhancing the performance and responsiveness of the SIEM solution.

## 4- Test Scenario Setup

### The test scenario and objectives.

We will test the Suricata alerts with the following rules and see the alert in Kibana dashboard after connecting with it with the elastic user credential, and we will discover the Logs collected from the Apache client.

### Test results



```
alert https any any -> 192.168.42.130 any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|root|29|"; classtype:bad-unkn
```

Figure 62 : Suricata Rule for test

We used this domain to test our rule: <https://testmynids.org/uid/index.html>

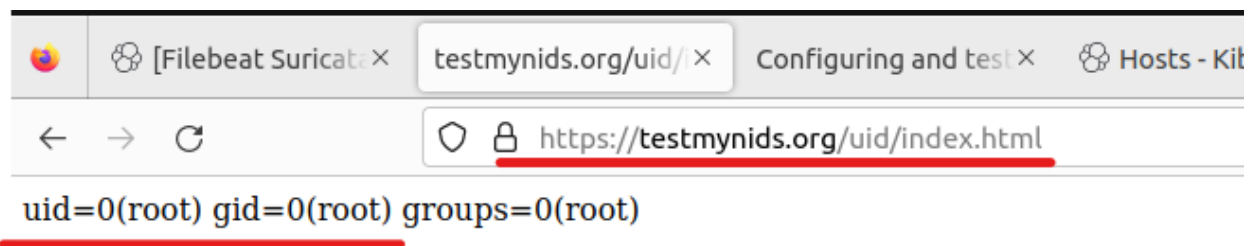


Figure 63 : visite the test domain

Any packet use https and his content contain uid=0(root) Suricata will alert us, and we will see the alert in kabana:

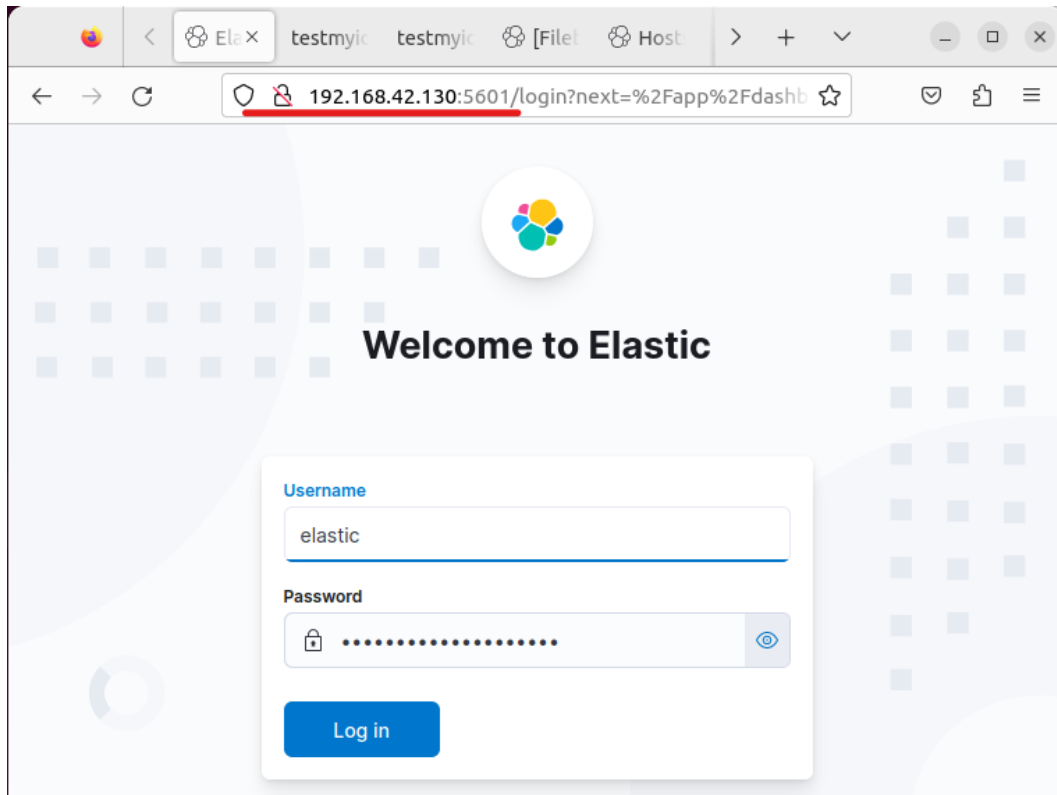


Figure 64 : access to Kibana

We use the server private IP with the port of Kibana to access it, and use the elastic user credential. This is the home page with different Kibana's functions

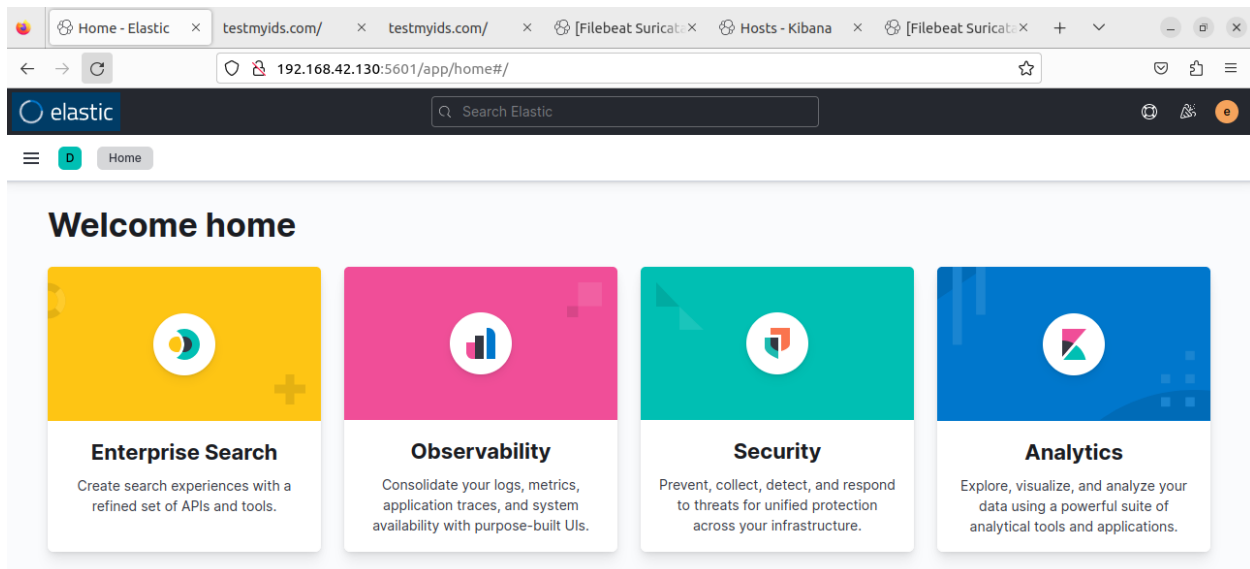


Figure 65 : Kibana Home page

Use the search input to search Suricata dashboard:

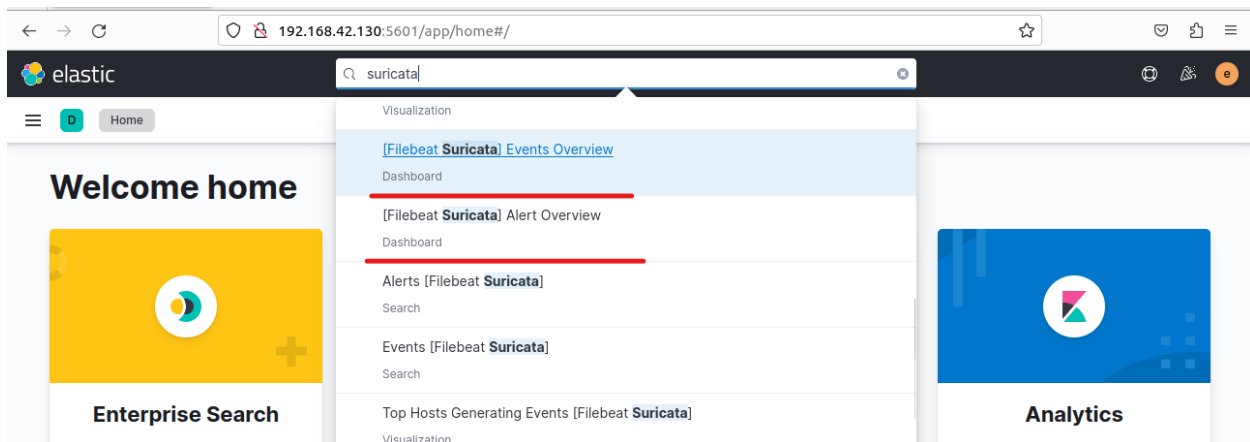


Figure 66 : Search in Kibana Modules

Suricata dashboard contain data about the events and alerts generated by Suricata with different presentations like diagrams, there is Event section that contain each event with different data like the source IP, destination IP, Port, content, meta data, with real time detection, in the Alert section we have the same information but this time for alerts.

We can see the full information about any event or alert with expanding button in the left of each one.

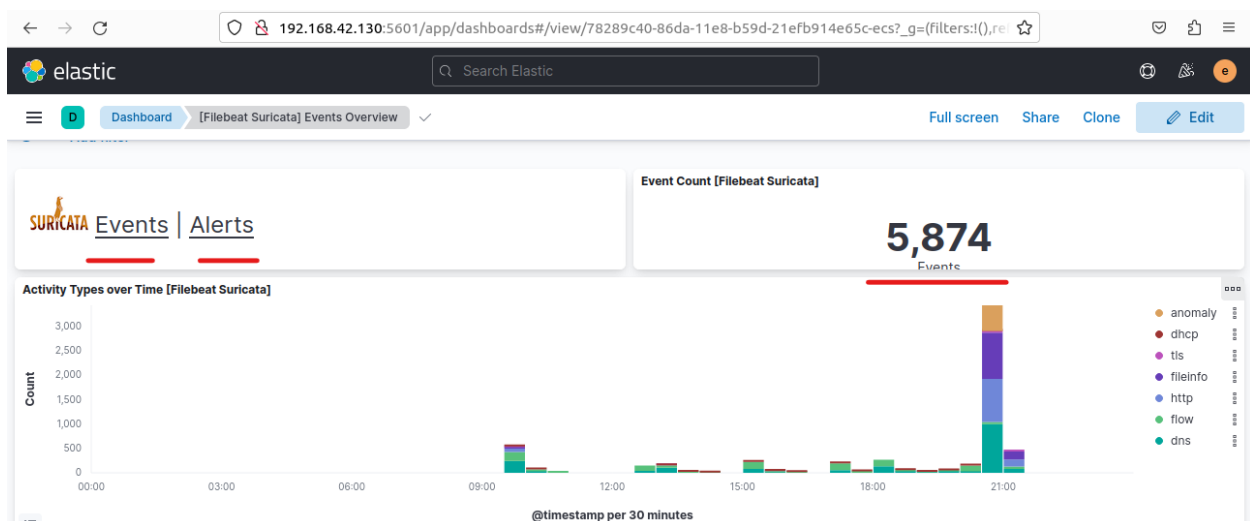


Figure 67 : Suricata dashboard

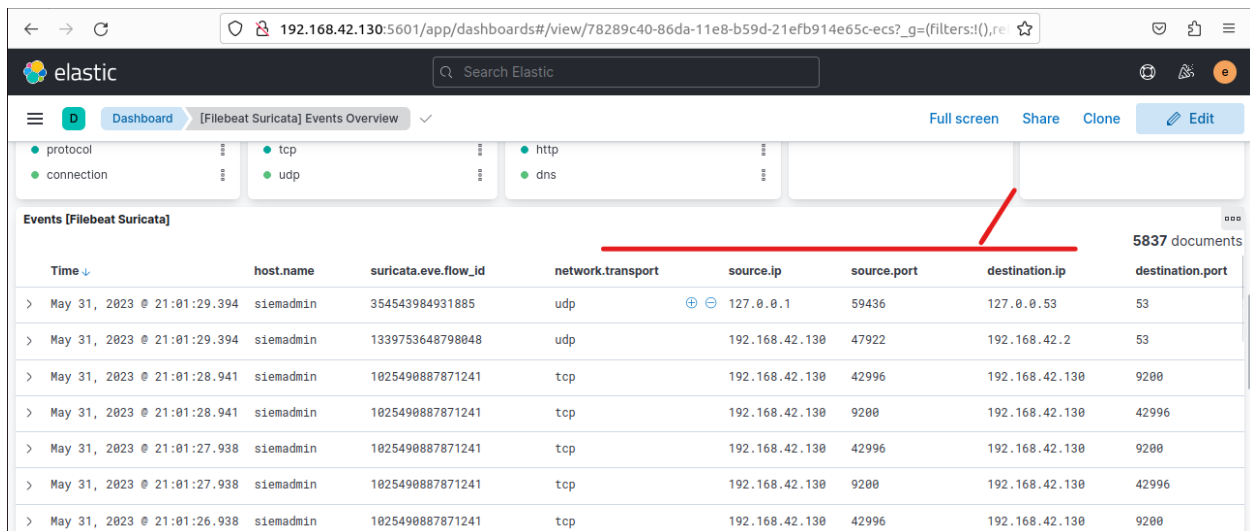


Figure 68 : Suricata's Event section

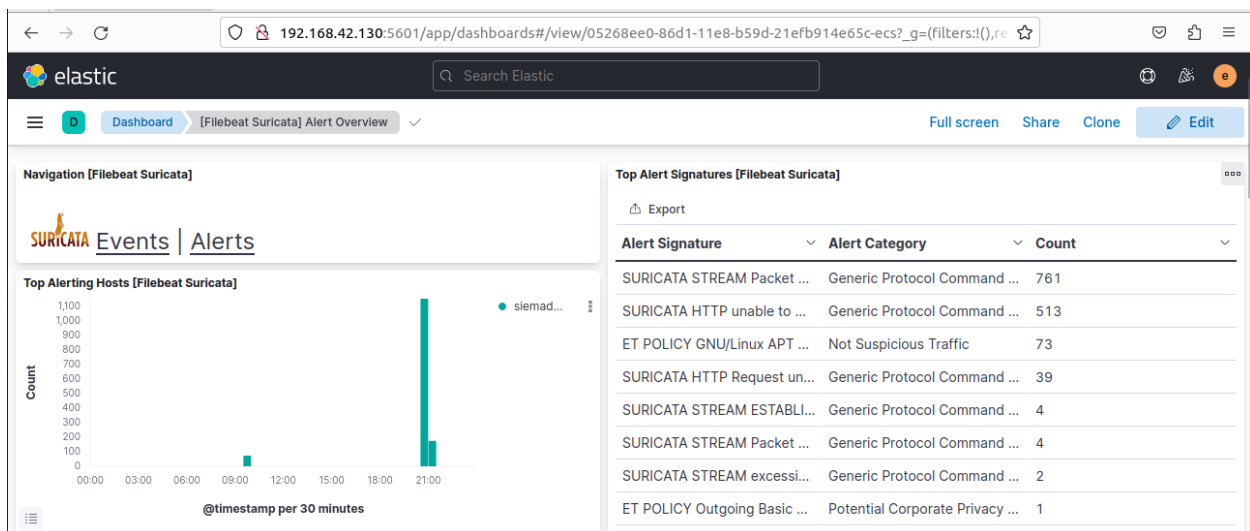


Figure 69 : Suricata's alerts section

We will find an event in our Event Overview, we expand the event and we will see more data about it.



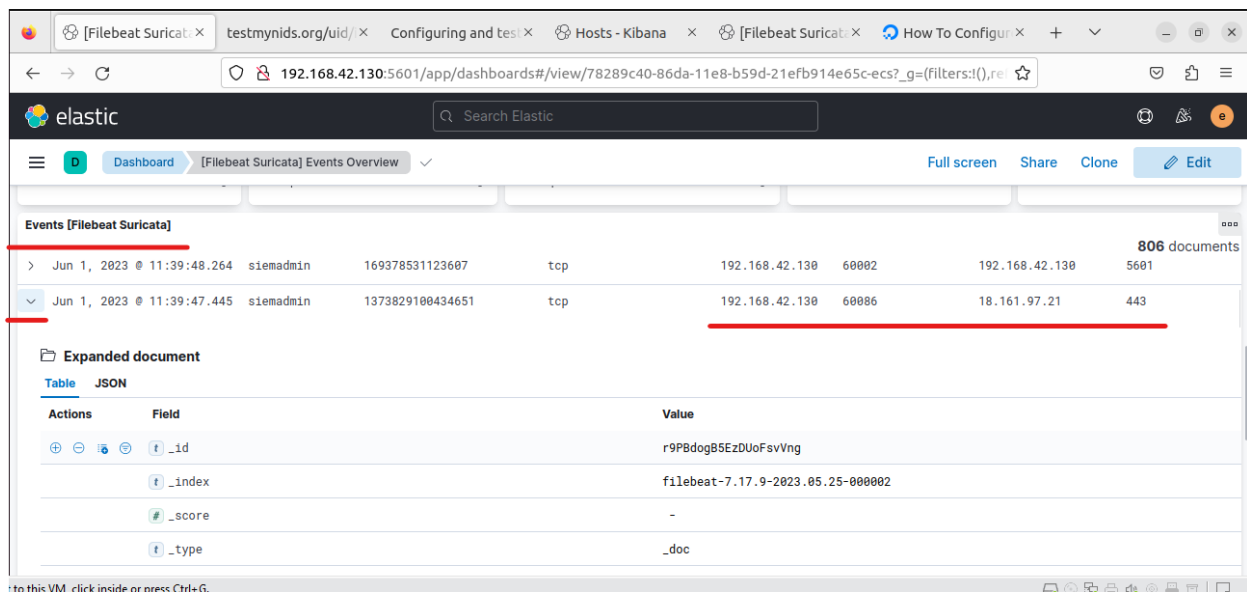


Figure 70 : Test Event

But we need an alert, let's see the alert section.

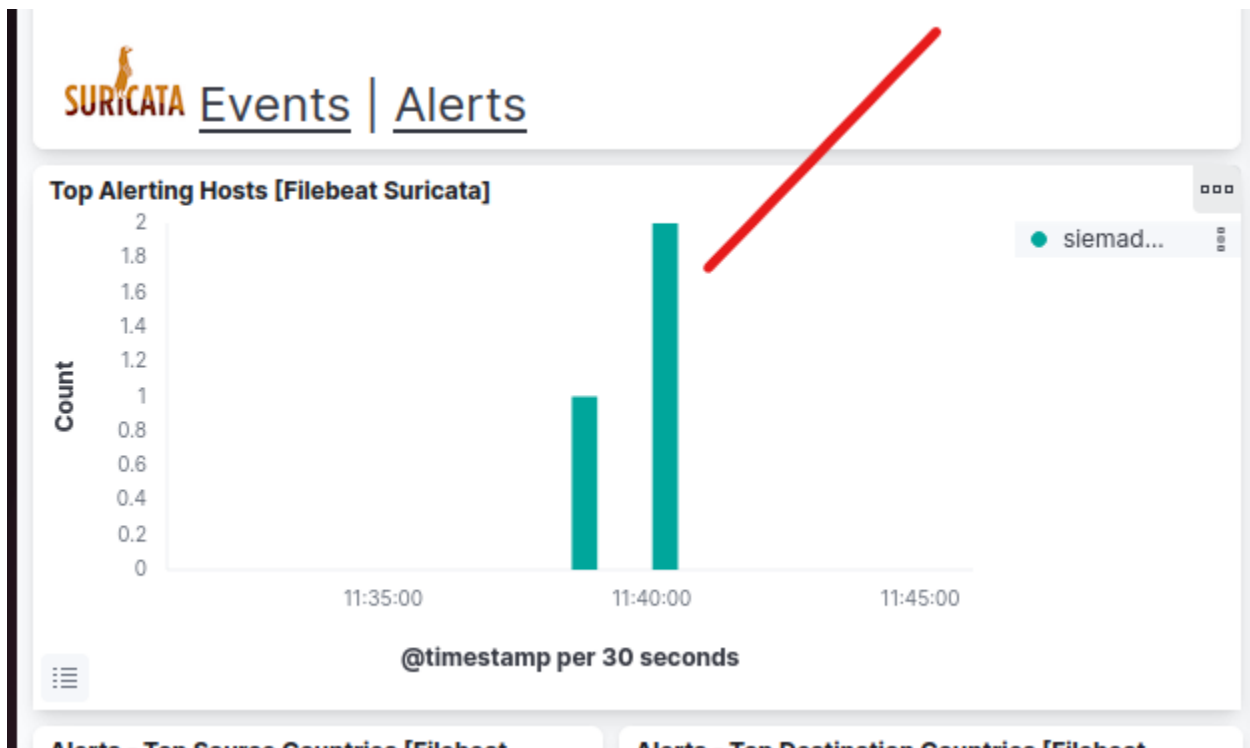


Figure 71 : Test Alert in diagram

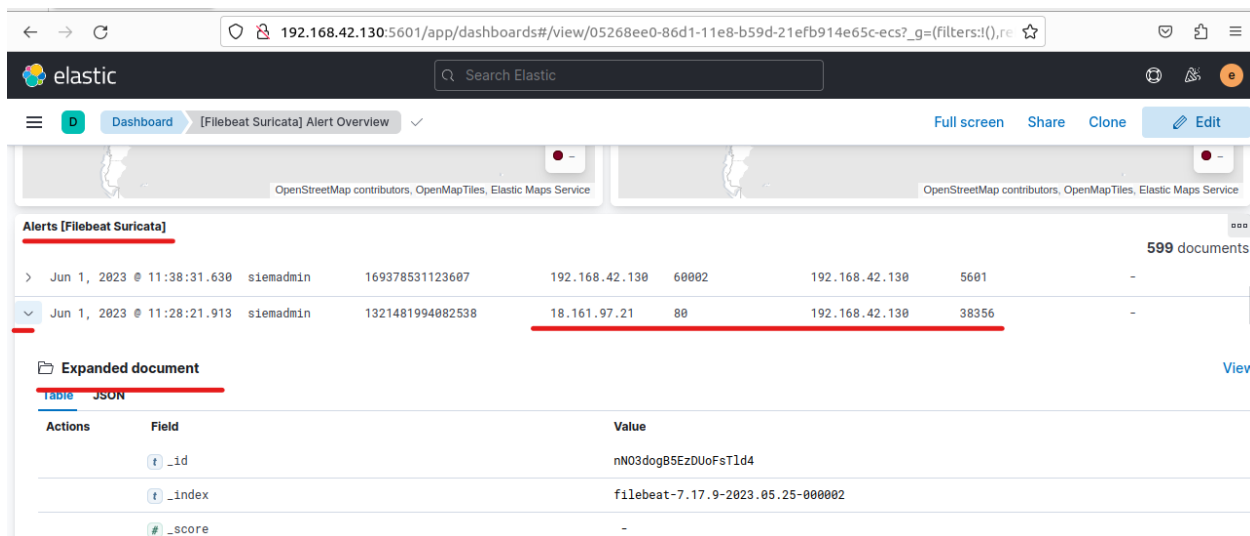


Figure 72 : Test Alert



Figure 73 : Test Alert information

These is an alert generated by Suricata rule that we defined before.

To see the Apache Logs in Kibana we will go to the discover section from the left Menu,

In the Discover Part we find the Filebeat index, where we will have all the Logs received from our client using Filebeat.

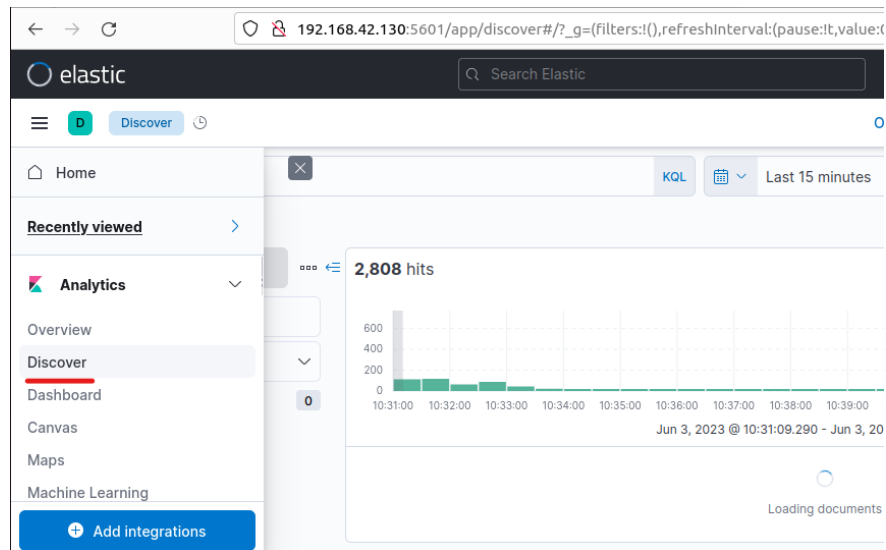


Figure 74 : Discover Section in Kibana

We can use the search input with the filter option to find our Logs, use the Client IP .

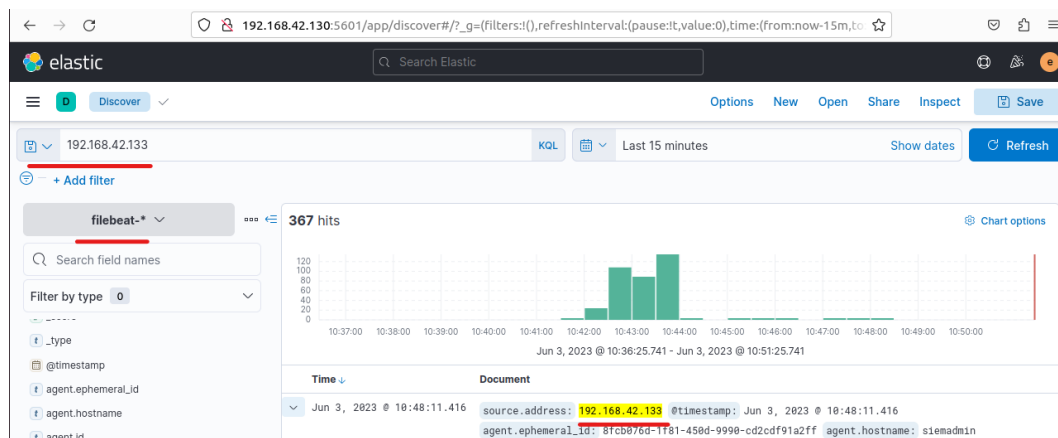


Figure 75 : Apache Logs

## 5- Conclusion

In this chapter, we have successfully implemented and tested a SIEM solution with Suricata, ELK Stack, and Filebeat. We have configured Suricata, an intrusion detection and prevention system, and integrated it with the ELK Stack, consisting of Elasticsearch, Logstash/Filebeat, and Kibana. The implementation involved setting up the necessary components, configuring the system, and conducting tests to validate the functionality of the solution. Through this implementation, we have demonstrated the effective detection, analysis, and visualization of security events using Suricata rules, ELK Stack, and Filebeat. This chapter highlights the practical application and functionality of the SIEM solution, showcasing its ability to enhance network security and provide actionable insights for incident response and threat mitigation.

# Conclusion

This report has provided a comprehensive overview of the implementation and testing of a SIEM solution with Suricata, ELK Stack, and Filebeat.

In the first chapter, we explored the definitions and conducted a literature review to establish a solid foundation for understanding SIEM concepts and technologies. By reviewing relevant literature, we gained insights into the importance of SIEM in monitoring and securing network infrastructure.

The second chapter focused on the implementation and testing phase, where we successfully configured and integrated Suricata, ELK Stack, and Filebeat. Suricata, as an intrusion detection and prevention system, played a vital role in detecting and alerting on security events.

The ELK Stack, consisting of Elasticsearch, Logstash/Filebeat, and Kibana, facilitated log collection, analysis, and visualization, enabling effective security monitoring. The decision to utilize Filebeat over Logstash was driven by its advantages in terms of resource usage, including reduced memory footprint and streamlined log forwarding.

Through our implementation, we established a comprehensive security monitoring system. By simulating test scenarios and visualizing event and alert data in Kibana, we demonstrated the effectiveness of the SIEM solution. The integration of Suricata, ELK Stack, and Filebeat provided actionable insights for incident response and threat mitigation, showcasing the practical application of the SIEM solution in real-world environments.

Overall, this report highlights the importance of using SIEM solutions for monitoring and securing network infrastructure. The combination of Suricata, ELK Stack, and Filebeat enables proactive threat detection, centralized log analysis, and visualization of security events. By leveraging these technologies, organizations can enhance their network security posture, improve incident response capabilities, and gain valuable insights into potential threats and vulnerabilities.

In conclusion, the implementation and testing of the SIEM solution with Suricata, ELK Stack, and Filebeat exemplify the practical application of SIEM concepts discussed in the first chapter. By integrating these technologies, organizations can establish a robust security monitoring system, effectively monitor network infrastructure, and respond promptly to security incidents.

## Webography

[https://www.digitalocean.com/community/tutorial\\_series/securing-your-network-with-suricata](https://www.digitalocean.com/community/tutorial_series/securing-your-network-with-suricata)

visited: 9/04/2023

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

visited: 9/04/2023

<https://learn.microsoft.com/fr-fr/azure/network-watcher/network-watcher-intrusion-detection-open-source-tools>

visited: 22/04/2023

<https://akintola-lonlon.medium.com/elasticsearch-how-to-install-and-set-up-filebeat-on-ubuntu-20-04-66375c967798>

visited: 22/04/2023

<https://www.geeksforgeeks.org/how-to-install-gui-on-ubuntu-server/>

visited: 1/02/2023

<https://unicornsec.com/home/siem-home-lab-series-part-1>

visited: 22/05/2023