IBM Innovation Centre for Education

PHEMESOFT
Software That Matters

YENEPOYA
(DEEMED TO BE UNIVERSITY)

YENEPOYA INSTITUTE OF ARTS, SCIENCE, COMMERCE AND MANAGEMENT
(A constituent unit of Yenepoya Deemed to be University)

SECURATRIX

PROJECT REPORT

Security Operations Center (SOC)

Implementing SIEM for small Businesses

BACHELOR OF COMPUTER APPLICATION
(IoT, Ethical Hacking, Cyber Security and Digital Forensics)

SUBMITTED BY: Team-040: Securatrix

Name	**REG NO.**	**Email ID**
Kiran Singh	**22BCIECS048**	**21071@yenepoya.edu.in**
Mohammed Fairooz S	22BCIECS088	21114@yenepoya.edu.in
Sabareesh M S	22BCIECS109	21108@yenepoya.edu.in
Sayanth V P	22BCIECS112	22690@yenepoya.edu.in
Muhammed Ansar T	22BCIECS081	21062@yenepoya.edu.in

GUIDED BY: Mr. Shashank – IBM SME

TABLE OF CONTENTS

INTRODUCTION **1**
CHAPTER 1: TOPIC OVERVIEW **2**
1.1 WHAT IS INFORMATION SECURITY? 2
1.2 CHALLENGES IN INFORMATION SECURITY 3
1.3 THE IMPORTANCE OF INFORMATION SECURITY IN BUSINESS 4
1.4 WAZUH'S ROLE IN CYBERSECURITY MANAGEMENT AND MONITORING 5
CHAPTER 2: WAZUH SECURITY PLATFORM **7**
2.1 WHAT IS WAZUH? 7
2.1.1 Development history 7
2.1.2 Key Features of WAZUH 8
2.2 WAZUH ARCHITECTURE 10
2.2.1 Main Ingredients 10
2.2.2 Operating model 13
2.3 WAZUH SECURITY FEATURES 14
2.3.1 Log file monitoring 14
2.3.2 Intrusion Detection 15
2.3.3 Security Configuration Management 16
2.3.4 Event Management and Analysis 17
2.4 ADVANTAGES AND DISADVANTAGES OF WAZUH 18
2.4.1 Advantage 18
2.4.2 Limit 18
2.5 WAZUH AND OTHER SECURITY TOOLS 19
2.5.1 WAZUH vs Splunk 19
2.5.2 WAZUH vs OSSEC 20
2.5.3 WAZUH vs AlienVault OSSIM 20
2.6 WHAT IS ELK? 20
2.7 KEY COMPONENTS OF THE ELK STACK 21
2.8 ELK’S FUNCTIONALITY AND BENEFITS 22
2.9 What is Elasticsearch? 23

2.10 What is Logstash? 24
2.11 How LogStash work? 25
2.12 What is Kibana? 26
2.13 What Is Kibana Used For? 26
2.14 What is Suricata? 27
2.15 Benefits and Features of Suricata 28
CHAPTER 3: DEPLOYMENT OF TEST MODEL 29
3.1 PREPARE THE ENVIRONMENT 29
3.1.1 WAZUH Server 29
3.1.2 Suricata IDS/IPS 29
3.2 INSTALL WAZUH SERVER 31
3.3 INSTALL SURICATA 34
3.4 MONITOR FOLDERS AND FILES ON AGENT MACHINES AND INTEGRATE WITH VIRUSTOTAL API 37
3.5 COMBINE WITH SURICATA TO WARN OF CERTAIN ATTACK METHODS 40
3.6 WARNING ABOUT MITRE ATTACK-BASED ATTACK TECHNIQUES 43
3.7 IMPLEMENT CONTROL ACCORDING TO INTERNATIONAL STANDARDS (PCI DSS, GDPR, HIPAA, …) 46
CONCLUSION 48

LIST OF IMAGES

Figure 2. 1: What is WAZUH? 7

Figure 2. 2: WAZUH operating model 13

Figure 2. 3: What is Elasticsearch 23

Figure 2. 4: What is Logstash? 24

Figure 2. 5: What is Kibana? 26

Figure 2. 6: What is Suricata? 27

Figure 3. 1: Test model 30

Figure 3. 2: Add repository and public key to Elasticsearch 31

Figure 3. 3: Add source for Elastic to APT file 31

Figure 3. 4: Update package list 31

Figure 3. 5: Modify file elasticsearch.yml according to the IP address 32

Figure 3. 6: Starting and activating Elastic 32

Figure 3. 7: Kibana Installation 33

Figure 3. 8: Kibana file configuration 33

Figure 3. 9: Starting the Kibana service 33

Figure 3. 10: Installing WAZUH Manager 34

Figure 3. 11: Install WAZUH plugin 34

Figure 3. 12: Access to WAZUH Dashboard 34

Figure 3. 13: Suricata Installation 35

Figure 3. 14: Modifying Suricata configuration file 36

Figure 3. 15: Configuring Suricata to send logs to WAZUH Manager 36

Figure 3. 16: WAZUH Agent Configuration 37

Figure 3. 17: Access WAZUH Agent on WAZUH Dashboard 37

Figure 3. 18: Configuring directory monitoring on WAZUH Agent 38

Figure 3. 19: WAZUH Dashboard has received the log file from WAZUH Agent 38

Figure 3. 20: Integrating VirusTotal API into Wauzh Manager 39

Figure 3. 21: File containing malicious code downloaded from WAZUH Agent 40

Figure 3. 22: WAZUH Manager receives log when detecting malicious file from WAZUH Agent 40

Figure 3. 23: From Kali machine, use nmap to scan to Windows endpoint machine 41

Figure 3. 24: Warning from Suricata sent to WAZUH when detecting an nmap scanner 41

Figure 3. 25: Kali machine Brute force attack to Windows endpoint................................ 42
Figure 3. 26: WAZUH Manager has received logs when detecting brute force attack....... 42
Figure 3. 27: Sysmon logs events at Windows Endpoint 44
Figure 3. 28: Using AtomicRedTeam to attack based on Mitre Attack framework............ 45
Figure 3. 29: Warning from Sysmon on Windows sent to WAZUH Manager................... 46
Figure 3. 30: PCI DSS standard... 47
Figure 3. 31: GDPR standards 47

LIST OF ABBREVIATIONS

STT	Abbreviation	Phrase
1	SIEM	Security information and event management
2	OSSEC	Open-source HIDS SECurity
3	OSSIM	Open-source Security Information Management
4	AES	Advanced Encryption Standard
5	RSA	Rivest-Shamir-Adleman
6	SHA	Secure Hash Algorithm
7	IDS	Intrusion Detection System
8	IPS	Intrusion Prevention Systems
9	DDOS	Distributed Denial of Service
10	GDPR	General Data Protection Regulation
11	HIPAA	Health Insurance Portability and Accountability Act
12	ISO	International Organization for Standardization
13	ELK	Elasticsearch, Logstash, and Kibana
14	PCI DSS	Payment Card Industry Data Security Standard

15	JSON	JavaScript Object Notation
16	NSM	Network Security Monitoring
17	OISF	Open Information Security Foundation
18	MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge

INTRODUCTION

In the context of increasingly complex network security and increasingly sophisticated threats, deploying effective and flexible security solutions has become a top priority for organizations and businesses. The topic " Implementing SIEM for small Businesses" aims to exploit the potential of WAZUH, an outstanding open-source tool in the field of network security management and monitoring.

WAZUH, an open-source solution, provides a powerful set of tools for monitoring and analyzing network activities, including intrusion detection, system log analysis, and security event management. Built on the foundation of OSSEC, WAZUH extends the capabilities of traditional security tools by integrating advanced features such as in-depth analysis of security events, cross-platform support, and flexible scalability.

The goal of this project is to develop and customize WAZUH to meet the security needs of modern IT environments. This includes building custom configurations and rules to optimize threat detection, improve analysis and response, and integrate with other security systems and tools.

CHAPTER 1: TOPIC OVERVIEW

1.1 WHAT IS INFORMATION SECURITY?

Information security is a critical area of data management and protection that focuses on protecting information from potential threats such as unauthorized access, misuse, disclosure, disruption, modification, or destruction. It is a continuous process to ensure that an organization's information is comprehensively and securely protected. The goal of information security is to maintain and ensure three basic principles: confidentiality, integrity, and availability.

Confidentiality is the assurance that information can only be accessed by authorized people or systems. This is typically accomplished through measures such as encryption, user authentication, and access control. Encryption is the process of converting information into an encrypted form to prevent unauthorized access, with common algorithms such as AES, RSA, and SHA. Authentication is the process of confirming the identity of the user or system accessing information, using methods such as passwords, smart cards, biometrics (e.g. fingerprints, facial recognition). Access control manages access to information resources, with systems such as ACLs (Access Control Lists) and RBAC (Role-Based Access Control) to ensure that only authorized people can access important information.

Integrity ensures that information has not been altered or destroyed in an unauthorized manner. Measures such as digital signatures, hash functions, and data integrity checks are used to protect information from unauthorized changes. A digital signature is a method of confirming the integrity and authenticity of information through the use of cryptographic algorithms and public keys. A hash function generates a unique value from data, which helps detect any changes to the original data.

Availability ensures that information and information processing systems are accessible and usable when needed. Measures such as data backup, disaster recovery systems, and denial of service protection help maintain information availability. Regular data backup is an important measure to ensure that information can be recovered in the event of loss or damage. Disaster recovery systems include plans and measures to ensure the ability of systems to recover and continue operations after incidents or disasters, ensuring that the business can continue operating without major disruption.

Other information security elements and measures include authorization to grant access and permissions to resources to authenticated users or systems, and intrusion detection and monitoring. Intrusion detection and monitoring systems such as IDS (Intrusion Detection Systems) and SIEM (Security Information and Event Management) help detect and respond to threats. IDS monitor and analyze network traffic to detect unusual or unauthorized behavior, while SIEM integrates and analyzes security events from multiple sources to provide a comprehensive view of the security posture.

Finally, a disaster recovery plan includes routine data backups and establishing a backup facility to ensure the system's ability to recover and continue operations after an incident or disaster. Planning and implementing information security measures not only protects an organization's critical data and resources, but also helps maintain the trust and credibility of the business with customers and partners.

In general, information security plays an indispensable role in every organization, especially in the context of information technology and the internet growing strongly. Effective information security measures not only help prevent attacks and intrusions but also ensure the stability and continuity of business operations, thereby contributing to improving the efficiency of operations and competitiveness of enterprises in the market.

1.2 CHALLENGES IN INFORMATION SECURITY

As information technology continues to evolve, protecting information systems from threats and risks is becoming increasingly complex and challenging. One of the biggest challenges organizations face is the ever-increasing number of Cyber Attacks. Attacks such as ransomware, phishing, Distributed Denial of Service (DDoS) attacks, and exploits are becoming increasingly sophisticated and difficult to detect. This places an urgent need for security systems to be able to quickly detect and respond to suspicious behavior.

Another challenge comes from managing the large amount of log data and alerts generated by systems and devices within an organization. Organizations often use a variety of security tools, from firewalls, intrusion detection systems (IDS/IPS), to network monitoring software. However, aggregating, analyzing, and filtering out the truly important events from millions of log records is a task that requires a lot of time, resources, and specialized skills. Many organizations struggle to deploy a centralized solution to manage and optimize log data, leading to potential threats being overlooked.

In addition, the lack of highly skilled security personnel is also a major barrier. Training personnel to understand and operate complex security systems requires significant time and cost. At the same time, current security tools often lack compatibility and integration with each other, leading to complexity in system management and increasing the risk of missing security vulnerabilities.

1.3 THE IMPORTANCE OF INFORMATION SECURITY IN BUSINESS

The importance of enterprise security cannot be underestimated, as it plays an essential role in protecting the organization's important information and assets. In the increasingly digital context, external and internal threats are increasingly sophisticated and diverse, maintaining a solid security system becomes a top priority. Information security helps protect sensitive customer data and financial information from Cyber Attacks, thereby preventing information leaks that damage the company's reputation and finances. In addition, the security of internal data such as business plans, research and development documents, and partner information also needs to be strictly ensured to avoid theft or sabotage. A strong security platform also helps businesses build disaster recovery plans, ensuring that systems and data can be quickly restored after incidents such as data loss, Cyber Attacks or natural disasters, thereby minimizing downtime and ensuring business operations continue smoothly without significant disruption.

At the same time, a security platform also helps businesses comply with strict legal regulations on information security, such as GDPR (General Data Protection Regulation) in the EU, HIPAA (Health Insurance Portability and Accountability Act) in the US, or similar regulations in other countries. Compliance with these requirements helps businesses avoid fines and maintain customer trust, while improving transparency and compliance in the handling of personal and financial data. Preventing security incidents helps protect a business's reputation, as major data breaches can severely damage a business's reputation, causing customers to lose confidence and switch to competitors. When customers know that a business has strong security measures in place, they feel more secure sharing personal information and transacting with the company, thereby increasing brand loyalty and trust. Furthermore, investing in security helps reduce the costs of security breaches, including incident response costs, damages, and legal fees, while optimizing resource utilization and improving the operational efficiency of IT systems.

A modern security platform also helps businesses easily adapt to changes in the technological and legal environment, thereby improving their competitiveness in the global market. Businesses with strong security systems will have an advantage over their competitors, because customers and partners often prioritize cooperation with businesses that have good data protection capabilities. In short, a security platform is not only an important part of a business's risk management strategy, but also a key factor in maintaining sustainable development and protecting the company's valuable assets. Investing in information security not only helps businesses minimize risks and costs, but also contributes to improving reputation, customer trust and competitiveness in the global market.

1.4 WAZUH'S ROLE IN CYBERSECURITY MANAGEMENT AND MONITORING

WAZUH plays an important role in improving the ability of organizations to manage and monitor cybersecurity, especially in the context of increasingly complex and diverse threats. As an open-source security platform, WAZUH provides a comprehensive solution to detect, analyze and respond to security incidents in real time. One of the main roles of WAZUH is to centralize and analyze logs from various sources, including servers, network devices, applications and other security systems. This helps organizations have a more comprehensive and holistic view of the security status of the system, thereby providing timely prevention and remediation measures. In addition, WAZUH acts as a powerful intrusion detection system (HIDS). It is capable of monitoring unusual changes in files and systems, detecting suspicious behavior, and issuing alerts for administrators to handle. Additionally, file integrity monitoring (FIM) helps ensure that no unauthorized changes are made to important files, minimizing the risk from internal or external attacks.

Another important role of WAZUH is to support security compliance management. With the ability to test systems against popular cybersecurity standards such as PCI DSS, GDPR, HIPAA, or ISO/IEC 27001, WAZUH helps organizations meet legal and security regulatory requirements, while simplifying compliance testing and reporting. In particular, WAZUH can easily integrate with other tools and systems such as Elastic Stack, Kibana, and VirusTotal to expand monitoring and analysis capabilities. This integration allows organizations to take full advantage of WAZUH's power to combine data from multiple sources, thereby improving the effectiveness of detecting and preventing threats. As a comprehensive security monitoring and management platform, WAZUH not only helps minimize security risks but also optimizes deployment costs thanks to its open-source model. With its outstanding features and roles, WAZUH is increasingly becoming a top choice in protecting organizations' information systems against increasing challenges and risks.

CHAPTER 2: WAZUH SECURITY PLATFORM

2.1 WHAT IS WAZUH?

2.1.1 Development history

WAZUH started its journey in 2009 as OSSEC (Open-source Security), an open-source intrusion detection and monitoring tool developed by Daniel Cid, founder of One World Security. OSSEC quickly became a popular tool thanks to its powerful features such as log monitoring, intrusion detection, log analysis, and security incident alerting. By 2014, the OSSEC project underwent a major restructuring and was renamed to WAZUH. This transformation was not just a name change but also a significant expansion and upgrade in functionality and architecture, enabling WAZUH to meet increasingly complex security requirements.

Figure 2. 1: What is WAZUH?

During the period from 2017 to 2020, WAZUH has made significant progress thanks to close cooperation with the open-source security community. Contributions from the community and cybersecurity experts have helped WAZUH develop strongly and expand new features such as cloud resource monitoring, integration with Elasticsearch, Kibana, and Logstash (ELK Stack), thereby enhancing the ability to analyze and visualize security data.

WAZUH has become an indispensable tool for organizations in need of a comprehensive and effective security solution.

Since 2021, WAZUH has continued to modernize and develop new versions, adding many advanced features such as source code analysis, container monitoring, and integrating artificial intelligence (AI) and machine learning to improve the ability to detect and respond to security incidents. The WAZUH project has also continuously expanded its user and developer community, organizing meetings, workshops, and hackathons to promote continuous development and improvement. With a commitment to openness and collaboration, WAZUH has continued to affirm its position as a leading open-source security solution, meeting the diverse and complex security needs of organizations around the world.

2.1.2 Key Features of WAZUH

- Log Monitoring and Analytics:

- Log Collection and Storage: WAZUH is capable of collecting and storing logs from a variety of sources, including operating systems, applications, network devices, and cloud services. It uses components like Filebeat and Logstash to send log data to Elasticsearch, where it is stored and analyzed.
- Data Analytics: WAZUH uses powerful analytics tools to process and analyze logs, helping to identify unusual activity patterns and potential threats.

- Intrusion Detection System (IDS):

- Rules and Signatures: WAZUH uses a set of rules and signatures to detect suspicious or attack activities. These rules are updated regularly to reflect the latest threats.
- Behavioral Analytics: In addition to using static rules, WAZUH also applies machine learning models to analyze behavior and detect threats based on abnormal behavior.

- Vulnerability Management and Compliance Testing:

- Vulnerability Scanning: WAZUH is capable of scanning security vulnerabilities in the system, detecting weaknesses based on databases such as CVE (Common Vulnerabilities and Exposures).
- Compliance Testing: WAZUH supports compliance testing with security standards such as PCI-DSS, HIPAA, and GDPR, helping to ensure that an organization's systems comply with legal and industry regulations.

- Cloud Resource Monitoring:

  - Cloud Integration: WAZUH integrates with popular cloud services like AWS, Azure, and Google Cloud to monitor and protect cloud resources.
  - Configuration Change Monitoring: This tool is capable of monitoring configuration changes and detecting unusual activities in the cloud environment, ensuring that cloud resources are comprehensively protected.

- User and Terminal Behavior Analytics:

  - User Behavior Monitoring: WAZUH provides user behavior monitoring and analysis, helping to detect suspicious activities such as failed logins or unauthorized configuration changes.
  - Endpoint Monitoring: This tool also monitors endpoints to detect unusual behavior and protect the system from internal threats.

- Diverse Reports and Dashboards:

  - Custom Reports: WAZUH provides custom reports, helping administrators monitor and analyze the security status of the system.
  - Visual Dashboards: Visual dashboards display key metrics and events, allowing users to easily monitor and manage cybersecurity.

- Integration and Expansion:

  - Integration Support: WAZUH supports integration with many other tools and systems such as Elasticsearch, Kibana, Logstash (ELK Stack), SIEM, and other security solutions.
  - Extensibility: The tool is extensible and customizable to suit the specific security needs of each organization, allowing for the integration of custom modules and plugins.

- Incident Alerting and Response:

  - Configure Alert Rules: WAZUH allows configuring alert rules based on specific conditions, helping to detect and respond to security incidents quickly.
  - Automated Response: This tool has the ability to perform automated response actions when an incident is detected, such as sending alerts via email, Slack, or triggering emergency response scenarios to mitigate risk.

These features make WAZUH a powerful and flexible tool for cybersecurity protection and management, meeting the needs of many organizations and businesses with diverse and complex security requirements.

2.2 WAZUH ARCHITECTURE

2.2.1 Main Ingredients

- WAZUH Manager:

- Role: WAZUH Manager is the control and management center of the WAZUH system. It is responsible for receiving, processing, and storing all security events from agents. It is the core component of the system, ensuring that data is collected, analyzed, and managed effectively.
- Function:
    - Detection Rules Management: WAZUH Manager manages detection rules, allowing users to configure and update intrusion detection, configuration change detection, and vulnerability scanning rules.
    - Alert and Event Processing: This tool processes and analyzes security events, generating alerts based on configured rules. It is also capable of analyzing patterns and unusual behavior to detect potential threats.
    - Data Storage: WAZUH Manager stores log data and security events in an Elasticsearch database, ensuring that data can be quickly queried and analyzed.

- WAZUH Agent:

- Role: WAZUH Agents are components installed on servers or endpoints. They are responsible for collecting security data and sending it to WAZUH Manager for analysis and storage.
- Function:
    - Log Collection: Agents collect system, application, and security logs from servers and endpoints. They can also monitor file and system configuration changes.
    - Send Data to Manager: Agents send events and log data to WAZUH Manager via secure protocols, ensuring that data is transmitted safely and securely.

    - Vulnerability Management and Alerting: Agents can perform vulnerability scans on systems and send alerts about security issues to WAZUH Manager.

- WAZUH API:

  - Role: WAZUH API provides an application programming interface (API) for external applications and tools to interact with WAZUH. This API allows users to access and manage WAZUH security data, alerts, and configurations.
  - Function:
    - Configuration and Data Management: Users can use the API to manage rules, configure agents, and query security data.
    - Integration With Other Tools: API supports integration with other monitoring, reporting, and incident management tools, extending security system management and interoperability.

- WAZUH Dashboard:

  - Role: WAZUH Dashboard is a graphical user interface (GUI) that provides an intuitive view of security events and system status. It helps users easily monitor, analyze, and manage security incidents.
  - Function:
    - Display Reports and Statistics: Dashboard provides visual reports, charts, and statistics on security events, helping administrators quickly identify security issues and trends.
    - Customize and Configure: Users can customize dashboards and reports as needed, adding widgets and key metrics to track.

- Elasticsearch

  - Role: Elasticsearch is a powerful search and analytics database system, commonly used to store and analyze WAZUH log data.
  - Function:
    - Data Storage: Elasticsearch stores events and security logs from WAZUH Manager, enabling high-performance querying and data analysis.
    - Search and Analytics: Elasticsearch supports complex search queries and big data analytics, helping users quickly detect threats and incidents.

- Kibana

- Role: Kibana is a data visualization tool, often used in conjunction with Elasticsearch to create dashboards and reports.
- Function:
    - Data Visualization: Kibana provides data visualization tools such as charts, tables, and maps, making it easy for users to analyze and understand security events.
    - Create Dashboards and Reports: Users can create and customize dashboards and reports, displaying key metrics and events as needed.

- Logstash

- Role: Logstash is a data processing engine, used to collect, process, and transform log data before sending it to Elasticsearch.
- Function:
    - Data Collection and Processing: Logstash collects data from various sources, processes and transforms the data into a suitable format for storage in Elasticsearch.
    - Data Normalization: This tool helps normalize and clean log data, ensuring that data is stored and analyzed accurately and efficiently.

- Filebeat:

- Role: Filebeat is a lightweight log shipper, used to collect and ship log data to Logstash or Elasticsearch.
- Function:
    - Log Collection: Filebeat collects log data from servers and endpoints, reducing system load by forwarding data efficiently.
    - Send Data to Elasticsearch or Logstash: Filebeat sends processed log data to Elasticsearch or Logstash, ensuring that data can be analyzed and stored quickly.

- WAZUH Rule Set:

- Role: WAZUH's security ruleset, used to identify suspicious patterns and behaviors.
- Function:
    - Intrusion Detection Rules: Provides intrusion detection rules, vulnerability monitoring, and security alerts, helping WAZUH detect and respond to threats.

- Update and Customize: Users can update and customize rules to suit their organization's specific environment and security requirements.

2.2.2 Operating model

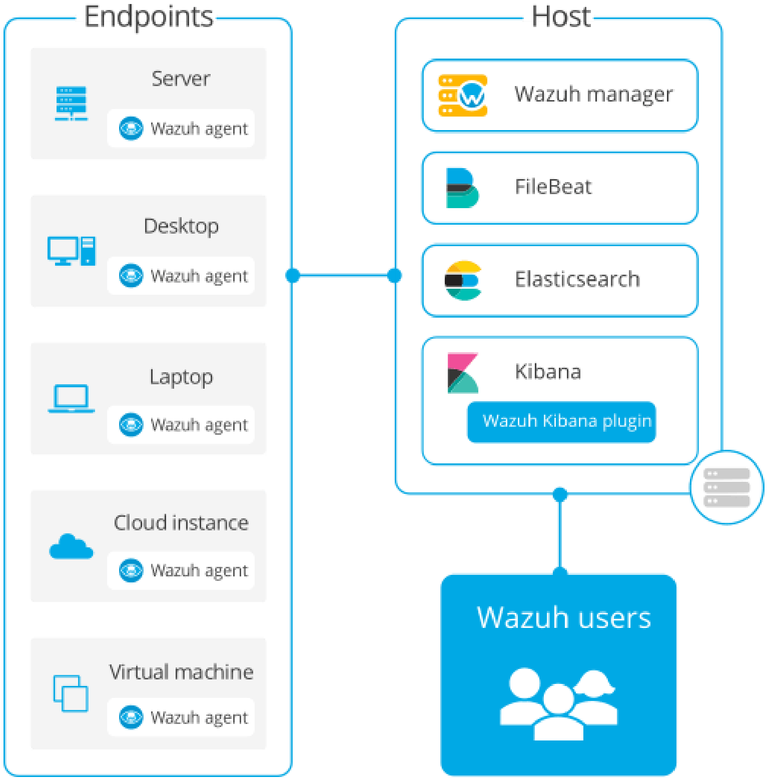


Figure 2. 2: WAZUH operating model

WAZUH operates based on a model consisting of three main components: WAZUH Agent, WAZUH Server (or WAZUH Manager), and WAZUH Dashboard (management interface). WAZUH Agent is a component installed directly on the devices that need to be monitored, including servers, personal computers, or other network devices. The Agent is responsible for collecting security information from the operating system, log files, and applications on the device, and detecting configuration changes or unusual activities. This data is then sent to WAZUH Server for further processing and analysis.

WAZUH Server is the central component that receives and analyzes security data from Agents. Based on pre-configured security rules, WAZUH Server can detect security-related events, such as intrusions, security vulnerabilities, or unwanted changes in system configuration. WAZUH Server can also integrate with other security tools, such as VirusTotal, to expand the scope and accuracy of threat detection. When security events are detected, the Server will generate alerts and send them to the WAZUH Dashboard.

WAZUH Dashboard is a web-based user interface that allows administrators to monitor and manage the entire security system. The Dashboard provides detailed reports, real-time alerts, and visual charts that help users easily grasp the security situation of the system. In addition, the Dashboard also supports configuration management for both WAZUH Agent and Server, facilitating system adjustment and optimization. The overall operation process of WAZUH starts with WAZUH Agent collecting information from devices, sending data to WAZUH Server for analysis and processing, generating alerts when detecting security events, and finally monitoring through WAZUH Dashboard. Thanks to the combination of these components, WAZUH provides a powerful security monitoring system that helps protect the network system from potential threats in an effective and comprehensive manner.

2.3 WAZUH SECURITY FEATURES

2.3.1 Log file monitoring

WAZUH provides a range of security and log monitoring functions to ensure comprehensive and effective system management and protection. First, the WAZUH Agent, a software installed on the devices to be monitored, collects log files from various sources, including operating systems, applications, and services. The Agent can be flexibly configured to monitor specific log files, such as operating system files and critical application log files. These log files are then sent to the WAZUH Server, where the data is aggregated and analyzed to detect security events, system errors, and suspicious activities.

WAZUH Server plays a central role in the system, processing and analyzing collected log data. Based on pre-configured security rules, the Server is able to identify abnormal behavior patterns or signs of attacks, such as intrusion attempts, malware, or unwanted changes in the system. When detecting suspicious events or security risks, the Server will generate alerts, immediately notifying the WAZUH Dashboard so that administrators can monitor and react quickly.

Another important feature of WAZUH is its ability to check the integrity of important system files. This helps detect unwanted changes in system configuration files or other important files, thereby identifying suspicious activities or attacks on the system. WAZUH also provides in-depth analysis of logs and generates detailed reports, providing a clear view of the security status of the system. These reports include information about security events, detected alerts, and system activity trends over time.

Finally, WAZUH supports the storage and management of logs, allowing users to easily access and search historical log files when needed. This not only helps in further investigation and analysis when incidents occur, but also assists in performing periodic security assessments and reports. Thanks to these functions, WAZUH not only helps in monitoring and analyzing system logs effectively, but also enhances the ability to detect and respond to security threats, ensuring that the system is always protected and operating stably.

2.3.2 Intrusion Detection

WAZUH provides powerful and comprehensive intrusion detection capabilities through a variety of security methods and features to ensure effective protection of the network. First, WAZUH Agent collects and sends log files from systems, applications, and services to WAZUH Server. The server then analyzes these logs based on pre-configured security rules. These rules are designed to recognize suspicious behavior patterns or signs of attacks, such as intrusion attempts, malware, or invalid activities. When a suspicious event is detected, WAZUH Server generates alerts, helping administrators quickly identify and respond to potential threats.

Another important function of WAZUH is its ability to monitor the integrity of important system and configuration files. WAZUH performs checks on these files to detect unwanted changes, which is important for identifying attacks such as rootkits or malware, which often hide in system changes. By monitoring these changes, WAZUH helps protect the system from potential threats, ensuring that important files are not tampered with.

The WAZUH system also uses a rich set of security rules to detect security threats. These rules can identify signs of common attacks, such as denial of service (DoS) attacks, exploits, or other invalid behavior. WAZUH not only relies on internal rules, but also has the ability to integrate with external threat databases and security intelligence services, thereby enhancing its ability to detect and respond to threats.

Additionally, WAZUH can integrate with other network monitoring systems and intrusion detection tools, such as Suricata, to provide network behavior-based intrusion detection. This integration allows WAZUH to analyze alerts and events from other security tools, enhancing its ability to detect network threats and intrusion behavior.

WAZUH also provides security event management and analysis tools, which help users investigate and analyze detected incidents and alerts. Detailed reports and event analysis help identify the source of attacks, assess the impact, and provide effective remediation measures. Additionally, WAZUH supports integration with other security tools, such as vulnerability management systems and threat intelligence services, to extend intrusion detection capabilities and provide a comprehensive view of the system's security posture. Thanks to these functions, WAZUH provides a powerful and comprehensive intrusion detection solution that protects the system from security threats and ensures the safety of data and system resources.

2.3.3 Security Configuration Management

Managing WAZUH security configuration is an essential part of maintaining and optimizing the effectiveness of a security monitoring system. First, configuring the WAZUH Agent, the software installed on the devices to be monitored, involves setting options for collecting data from the operating system, applications, and services. Users can configure the Agent to monitor specific log files, check the integrity of important files, and configure parameters related to sending data to the WAZUH Server. The main Agent configuration file is typically located in the /var/ossec/etc/ossec.conf directory, where these settings can be customized according to specific security needs.

Next, the WAZUH Server, also known as the WAZUH Manager, plays a central role in processing and analyzing security data. Server configuration includes setting up security rules, configuring how data is received and processed from Agents, and managing alerting and reporting options. The main configuration file for the Server is ossec.conf, where users can configure elements such as data sources, alert conditions, and event handling policies. The Server also supports integration with other security tools, such as network monitoring systems and threat intelligence services, to enhance threat detection capabilities.

Managing security rules and alert policies is an important part of security configuration in WAZUH. The system provides a basic set of security rules, but users can create and customize rules according to their needs to detect suspicious behavior and events. This includes setting alert conditions, severity levels, and actions to take when events are detected. WAZUH also provides tools for alert management and reporting, allowing users to track and analyze security events, receive alerts via email or other notification channels, and generate detailed reports on the security status of the system.

2.3.4 Event Management and Analysis

WAZUH event management and analysis are essential activities to maintain the effectiveness of the security system. This process begins with the WAZUH Agent collecting data from system log files, applications, and services on the devices to be monitored, then sending the data to the WAZUH Server. The server aggregates and processes this large volume of data, performing analysis based on configured security rules. These rules help identify suspicious behavior patterns, signs of attacks, and important security events, thereby detecting and classifying events to generate corresponding alerts. Alert management includes setting alert conditions, severity levels, and actions to take when alerts are received, with the ability to send notifications via multiple channels such as email or SMS.

In addition, WAZUH provides in-depth event analysis and incident investigation tools, allowing users to drill down into security events, track event chains, and identify root causes of issues. Detailed reports on events, alerts, and security trends help administrators monitor the security posture of their systems over time, evaluate the effectiveness of security measures, and take necessary remedial actions. The reporting system can be customized to meet the specific requirements of the organization, providing important information for decision making. Additionally, WAZUH supports integration with other security tools, such as vulnerability management systems and threat intelligence services, to extend event analysis capabilities and provide a comprehensive view of the security posture of the system. Thanks to these functions, WAZUH ensures that all security events are detected, analyzed and handled promptly, contributing to maintaining the safety and stability of the system.

2.4 ADVANTAGES AND DISADVANTAGES OF WAZUH

WAZUH is a powerful security information and event management (SIEM) solution that offers a wide range of security and monitoring features. Here are some of the pros and cons of WAZUH:

2.4.1 Advantage:

- Free and Open-source: WAZUH is open-source software, which means it is free and users can customize the source code according to their needs. This also reduces the initial investment cost and allows the community to contribute to the development of the software.

- High Compatibility: WAZUH supports multiple platforms and operating systems, including popular ones like Windows, Linux, and macOS. It also integrates with other security tools like Suricata and vulnerability management systems, extending its monitoring and analysis capabilities.

- Powerful Intrusion Detection: WAZUH provides powerful intrusion detection capabilities through analyzing system and application logs, checking file integrity, and using rich security rules. This helps detect suspicious behavior and security attacks.

- Alert Management and Detailed Reporting: The system provides tools to manage alerts and generate detailed reports on the security status of the system. These reports help track security events, analyze trends, and evaluate the effectiveness of security measures.

- Highly Customizable: WAZUH allows users to customize many aspects of the system, from configuring security rules to setting up alert and reporting policies. This makes it suitable for a wide range of security needs of organizations.

2.4.2 Limit:

- Configuration Complexity: WAZUH configuration can be quite complex, especially for beginners. Setting up and configuring security rules, alert policies, and integrating with other tools can require time and deep technical knowledge.

- System Resources: WAZUH can be resource intensive, especially when processing large amounts of log and alert data. This can result in high hardware requirements and should be considered in resource-constrained environments.

- Support and Documentation: While WAZUH has a large support community and extensive documentation, official developer support can be more limited than commercial SIEM solutions. This can be difficult for organizations that need in-depth and timely technical support.

- Integration and Extensibility: Although WAZUH supports many integrations and extensibility, integration with external tools and systems may require additional configuration and customization. This may increase the complexity of deploying and maintaining the system.

- Processing Speed: In environments with large volumes of data or many security events, WAZUH's processing speed may be affected. This may result in delays in detecting and responding to security events.

Overall, WAZUH is a powerful and flexible tool for security event monitoring and management, but users need to carefully consider the advantages and limitations to optimize system deployment and usage.

2.5 WAZUH AND OTHER SECURITY TOOLS

WAZUH is a comprehensive open-source security platform that offers threat detection, integrity monitoring, compliance management, and more. When comparing WAZUH with other security tools, it is essential to consider factors such as feature set, ease of use, extensibility, and community support. Here is how WAZUH compares to some popular security tools:

2.5.1 WAZUH vs Splunk

- Functionality: Splunk is a powerful platform for searching, monitoring, and analyzing machine-generated big data through a web interface. While WAZUH focuses on security information and event management (SIEM), intrusion detection (IDS), and compliance management, Splunk offers broader data analytics capabilities and has powerful log management features.

- Cost: WAZUH is open-source and free, with paid support options, while Splunk can be very expensive, especially when deployed at scale.

- Ease of Use: Splunk has a more polished interface and a more mature ecosystem, but that comes with a higher learning curve. WAZUH's interface is simpler and focused on security use cases.

- Community & Support: WAZUH has a growing community and good documentation, but Splunk has a larger user base and more extensive professional support.

2.5.2 WAZUH vs OSSEC

- Functionality: WAZUH is actually built on top of OSSEC, expanding its functionality significantly. WAZUH adds a more modern and user-friendly interface, real-time alerting, and advanced monitoring capabilities, including cloud and container security.

- Scalability: WAZUH scales better than OSSEC, especially in large or complex environments.

- Integration: WAZUH offers better integration with other tools like Elasticsearch and Kibana, making it a more versatile choice.

2.5.3 WAZUH vs AlienVault OSSIM

- Functionality: Both WAZUH and AlienVault OSSIM are open-source SIEM solutions. WAZUH is more flexible, allows integration with many external tools like the ELK stack, and offers a more modern interface. AlienVault OSSIM offers integrated threat intelligence and a more extensive security feature set.

- Community & Support: AlienVault OSSIM has been around longer, so it has a larger community. However, WAZUH's community is growing rapidly and it offers more frequent updates along with a more flexible development process.

- Ease of Use: WAZUH is generally more intuitive and easier to set up than OSSIM.

2.6 WHAT IS ELK?

ELK is an acronym that stands for Elasticsearch, Logstash, and Kibana. Together, these three components provide a powerful, integrated solution for managing large volumes of data, offering real-time insights and a comprehensive analytics suite.

- Elasticsearch is at the core of the stack. It acts as a highly efficient search and analytics engine, capable of handling vast amounts of data with speed and accuracy.

- Logstash is the data processing component of the stack. It specializes in collecting, enriching, and transporting data, making it ready for analysis.

- Kibana is the user interface of the stack. It allows users to create and manage dashboards and visualizations, turning data into easily understandable formats.

ELK's emergence as a key tool in the Big Data era is a reflection of its ability to address the complex challenges of data management and analysis. It has become a go-to solution for organizations looking to harness the power of their data. The synergy between Elasticsearch, Logstash, and Kibana is the cornerstone of ELK's effectiveness, truly transforming the whole into something greater than its parts. Each component complements the others, creating a powerful toolkit that enables businesses to transform their raw data into meaningful insights. This synergy provides sophisticated search capabilities, efficient data processing, and dynamic visualizations, all within a single, integrated platform.

2.7 KEY COMPONENTS OF THE ELK STACK

Elasticsearch: At its heart, Elasticsearch is a distributed search and analytics engine. It excels in managing and analyzing large volumes of data. Its main features include:

- Advanced full-text search capabilities.

- Efficient indexing for quick data retrieval.

- Powerful data querying functions.

Elasticsearch is renowned for its scalability and reliability, especially when dealing with massive datasets. It is designed to scale horizontally, ensuring that as an organization's data requirements grow, its data analysis capabilities can grow correspondingly.

Logstash plays a pivotal role in the ELK stack as the data collection, transformation, and enrichment tool. It is versatile in handling a wide range of data sources and formats, including both structured and unstructured logs. The plugin ecosystem is a significant feature of Logstash, allowing users to extend its functionality with custom plugins tailored to specific needs.

Kibana acts as the window into the ELK stack, providing a powerful platform for data visualization and exploration. It enables users to create various visual representations of data, such as dynamic, real-time dashboards and detailed charts and graphs for in-depth data analysis. Kibana is designed with user experience in mind, offering an intuitive interface that allows for easy navigation and extensive customization options.

2.8 ELK'S FUNCTIONALITY AND BENEFITS

- Log management and analysis: ELK excels in centralizing log storage and facilitating comprehensive log analysis. It supports real-time log processing and efficient indexing, enabling quick data retrieval and analysis.

- Data visualization and dashboards: Kibana is a powerful tool for creating interactive visualizations and dashboards. These visualizations help in extracting actionable insights from log data, making complex data sets understandable and useful.

- Monitoring and analytics: ELK is highly effective for performance monitoring and system analytics. Its capabilities extend to detecting anomalies, aiding in troubleshooting issues, and optimizing overall IT infrastructure. Advanced applications of the ELK stack include predictive analytics and machine learning, demonstrating its versatility and adaptability to various use cases.

ELK is indispensable for log management, analytics, and system monitoring. Its importance in the realm of IT cannot be overstated, with applications ranging from straightforward log aggregation to complex data analytics and predictive modeling.

Anyone can delve deeper into the ELK stack. A wealth of resources is available for those seeking to further their knowledge and skills, including comprehensive guides, active forums, and professional networks. The ELK stack represents not just a set of tools but a gateway to unlocking the vast potential of data in driving forward business and technological innovation.

2.9 What is Elasticsearch?

Figure 2. 3: What is Elasticsearch

Elasticsearch is an open-source and distributed search and analytics engine built based on the Apache Lucene. It is designed to handle large volumes of data and provide near real-time search capabilities across various types of structured and unstructured data.

Elasticsearch is part of the Elastic Stack, which includes other tools like Kibana for data visualization, Beats for data shipping, and Logstash for data processing. Elasticsearch stores data in JSON format and making it easy to index and search structured and unstructured data. Elasticsearch supports the concept of multi-tenancy, allowing us to index and search data for multiple applications or users within a single cluster. Elasticsearch is developed and supported by Elastic NV, a company that provides commercial products and services around the Elastic Stack.

Key Features of Elasticsearch:

- Distributed and Scalable: Elasticsearch is distributed by nature, allowing it to scale horizontally across multiple nodes to handle large datasets and high query volumes.

- Full-Text Search: It provides powerful full-text search capabilities, enabling users to search for documents based on their content and relevance.

- Real-Time Data Analysis: Elasticsearch supports real-time indexing and querying, making it suitable for use cases that require up-to-date insights from continuously changing data.

- RESTful API: Elasticsearch exposes a RESTful API, making it easy to interact with the system using simple HTTP requests.

- Schemaless: Elasticsearch is schemaless, meaning we can index and search data without having to define a rigid schema already.

2.10 What is Logstash?

Figure 2. 4: What is Logstash?

Logstash is an open-source data processing pipeline tool that ingests, transforms, and ships data from various sources to various destinations. Part of the Elastic Stack, it supports real-time data collection and transformation using a pluggable architecture with input, filter, and output plugins. Commonly used for centralized logging, data transformation, and real-time analytics, Logstash enables workflows and immediate insights by feeding data into systems like Elasticsearch or PubNub Iluminate for analysis.

Primary functions:

- Ingestion: Logstash can collect and aggregate data from multiple sources in real-time. It supports a wide range of input sources including log files, databases, message queues, and various cloud services.

- Transformation: Once the data is ingested, Logstash allows you to parse and transform it using a variety of filters. You can use these filters to clean, enrich, and modify the data before it is sent to the final destination. Common transformations include parsing unstructured log data, adding geographic information, or anonymizing sensitive information.

- Output: After processing, Logstash can ship the data to various destinations such as Elasticsearch (for storage and search), various databases, or other systems and services.

2.11 How LogStash work?

Logstash works by utilizing a pipeline architecture that processes data through three main stages: input, filter, and output. Here's a step-by-step explanation of how it operates:

Input Stage:

- Logstash collects data from various sources using input plugins. These sources can include log files, databases, message queues, cloud services, and more.

- Each input plugin is configured to capture data from a specific source. For example, the file input plugin reads data from log files, while the jdbc input plugin reads from databases.

Filter Stage:

- Once data is ingested, it passes through a series of filters for processing. Filters allow you to parse, clean, enrich, and transform the data.

- Common filter plugins include:

- grok for parsing unstructured log data.
- mutate for modifying fields (e.g., renaming, removing).
- date for parsing timestamps.
- geoip for adding geographic information based on IP addresses.

- Filters can be chained together to perform complex transformations.\

Output Stage:

- After filtering, the processed data is sent to one or more destinations using output plugins.

- Destinations can include Elasticsearch (for storage and search), databases, messaging systems, and other services.

- For example, the elasticsearch output plugin sends data to an Elasticsearch cluster, while the stdout plugin outputs data to the console for debugging.

2.12 What is Kibana?

Figure 2. 5: What is Kibana?

Kibana is the formerly open-source visualisation user interface that allows users to produce visualisations, reports and dashboards from a variety of data sources. Kibana was initially developed in 2013 by Rashid Khan, who in addition to Kibana is also the creator of the tools, Timelion and Canvas. Kibana makes up the data visualisation arm of the ELK stack (whose two remaining components include Logstash and Elasticsearch).

2.13 What Is Kibana Used For?

Due to its support for unstructured and semi-structured data, one of the leading use cases for Kibana is log and metrics analysis. Some of the most popular additional use cases for Kibana include the following, which have been listed alongside visual examples in our guide to Kibana dashboard examples:

- Centralised analytics dashboard for microservices
- Understanding user behaviour
- Jenkins application monitoring
- Measuring sales performance
- Resource allocation reporting
- Data streaming dashboard
- Monitoring website uptime
- Automated test tracking
- Global data monitoring

- Vulnerability scanning

- SIEM as a Service

- Firewall monitoring

- Tracking sign ups

- Linux monitoring

Some other more underutilised use cases for Kibana include its data visualisation capabilities for compliance auditing, IT operations monitoring and application performance monitoring.

2.14 What is Suricata?

Figure 2. 6: What is Suricata?

Suricata is an open-source detection engine that can act as an intrusion detection system (IDS) and an intrusion prevention system (IPS). It was developed by the Open Information Security Foundation (OSIF) and is a free tool used by enterprises, small and large. The system uses a rule set and signature language to detect and prevent threats. Suricata can run on Windows, Mac, Unix and Linux.

Intrusion detection "detects" and "alerts" a threat. In contrast, an intrusion prevention system also takes action on the event and attempts to block the traffic. Suricata can do both and also does well with deep packet inspection. Making it perfect for pretty much any kind of standard security monitoring initiatives your company might have.

2.15 Benefits and Features of Suricata:

Suricata comes with a comprehensive set of features, including:

- Support for a wide range of protocols
- Ability to detect a wide range of threats
- High performance
- Easy to install and configure
- Comprehensive set of tools

Suricata Benefits:

- Suricata offers a number of benefits, including:
- High performance: Suricata is a high-performance engine that can be used to monitor both wired and wireless networks.
- Wide range of detections: Suricata can detect a wide range of threats, including malware, network intrusions, denial-of-service attacks, and data breaches.
- Easy to use: Suricata is easy to install and configure, and it comes with a comprehensive user guide.
- Open source: Suricata is an open-source tool, which means that it is free to use and can be easily customized.

Suricata is a powerful IDS/IPS tool that can be used to protect networks from a wide range of threats. Suricata is easy to install and configure, and it comes with a comprehensive set of features. Suricata is a good choice for organizations of all sizes.

CHAPTER 3: DEPLOYMENT OF TEST MODEL

3.1 PREPARE THE ENVIRONMENT

To deploy the WAZUH open-source security system with Suricata integration, the environment preparation part is quite important. This is the foundation step to ensure that the system operates stably, effectively and has the ability to detect and respond to security threats in an optimal way.

3.1.1 WAZUH Server:

Operating System: WAZUH requires a stable and well-supported operating system. Ubuntu is a popular choice, especially an LTS (Long Term Support) version like Ubuntu 20.04 or 22.04. These versions ensure that the system will be updated and supported for a long time, minimizing the risk of software vulnerabilities.

RAM: For WAZUH to run smoothly, it is recommended to equip the system with at least 4GB of RAM. However, for larger systems or when monitoring multiple servers and large data, it is recommended to use at least 8GB of RAM or even more. This helps ensure that WAZUH has enough resources to handle large data streams and analyze them efficiently.

ROM: Hard drive capacity is an important factor, especially when WAZUH has to store a lot of logs from different systems. It is recommended to reserve at least 20GB for the system and an additional space of 50GB to 100GB or more for log storage. Using an SSD will also improve data retrieval speed, making the system more responsive during event analysis.

3.1.2 Suricata IDS/IPS:

Operating System: Like WAZUH, Suricata also requires a stable and secure environment. Ubuntu, especially the LTS versions, is the ideal choice to ensure stability and receive timely security updates. Using the same operating system for both WAZUH and Suricata also simplifies system management and configuration.

RAM: Suricata is a powerful intrusion detection tool that can analyze network traffic in real time. To function effectively, Suricata requires a minimum of 4GB of RAM. However, if you plan to monitor a large network with high traffic, you should prepare at least 8GB or more. Large memory helps Suricata process and analyze data packets quickly, minimizing latency and improving threat detection.

ROM: Suricata requires sufficient storage space to record logs and events detected from the network. Similar to WAZUH, it is recommended to prepare at least 20GB for the operating system and at least 50GB to 100GB of storage space for logs. If Suricata operates in a complex and high-traffic network environment, larger storage provisioning is necessary. Using SSDs also speeds up log data writing and retrieval, improving overall system performance.

Properly preparing the environment with the right hardware and software configuration is crucial to the success of the WAZUH open-source security system integrated with Suricata. When both tools are deployed on a robust platform and properly configured, the system will be able to comprehensively monitor and protect the network, from detecting threats to managing events and meeting security compliance requirements.

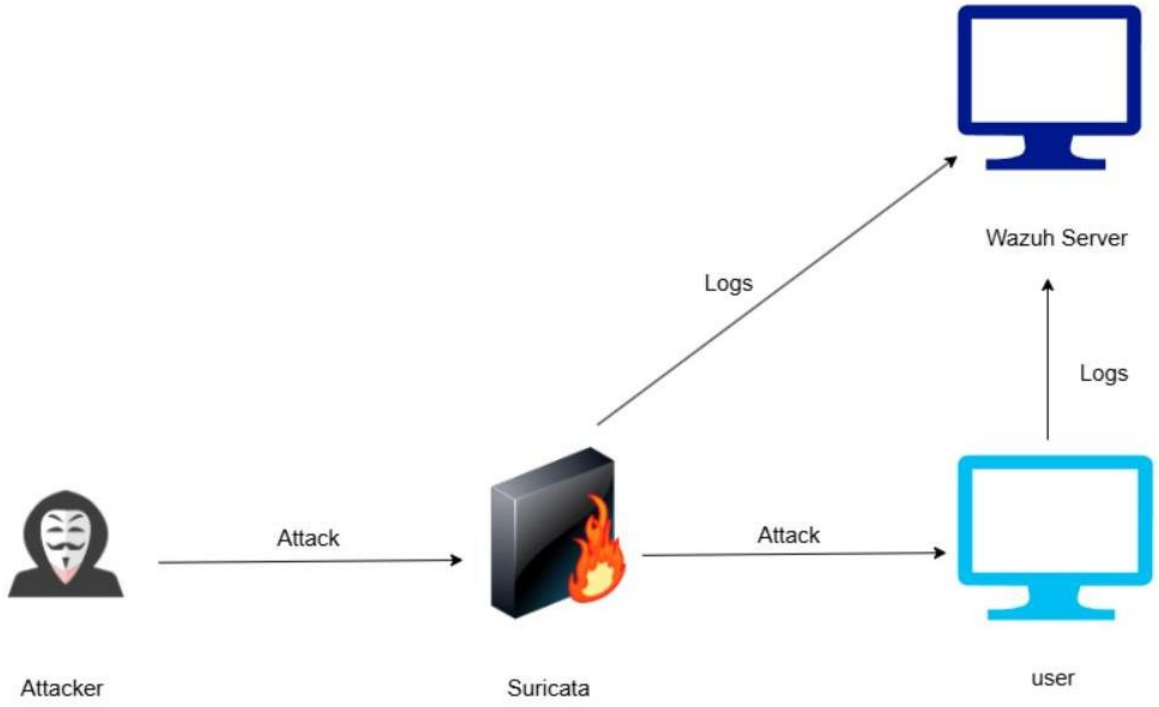
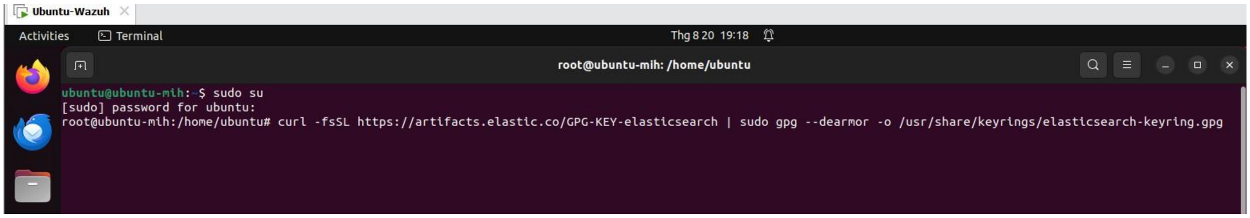


Figure 3. 1: Test model

3.2 INSTALL WAZUH SERVER

In order for WAZUH to be able to store and search data, integrating Elasticsearch will help WAZUH search data and execute faster.

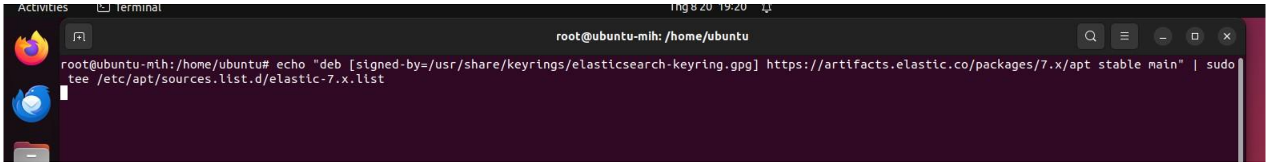
- Add repository and public key to Elasticsearch



```
ubuntu@ubuntu-mih:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-mih:/home/ubuntu# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

Figure 3. 2: Add repository and public key to Elasticsearch

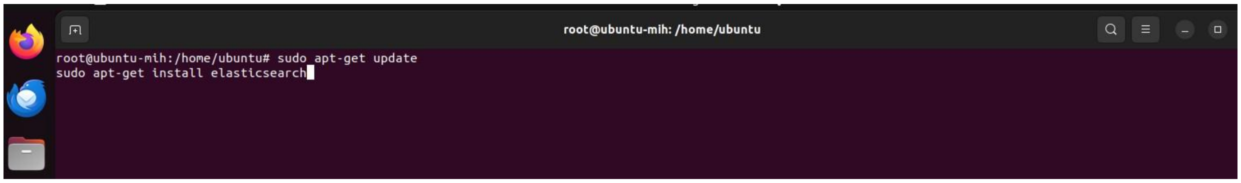
- Add the source for Elasticsearch to the APT source file:



```
root@ubuntu-mih:/home/ubuntu# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo
 tee /etc/apt/sources.list.d/elastic-7.x.list
```

Figure 3. 3: Add source for Elastic to APT file

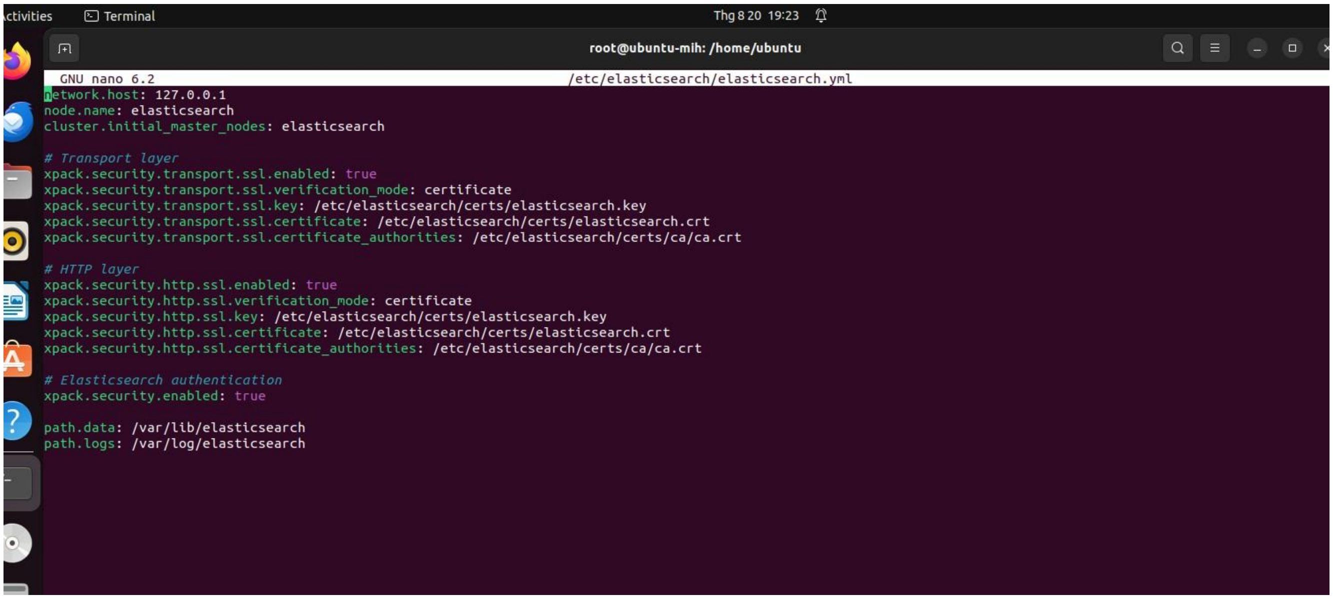
- Update package list and install Elasticsearch:



```
root@ubuntu-mih:/home/ubuntu# sudo apt-get update
sudo apt-get install elasticsearch
```

Figure 3. 4: Update package list

- Modify the configuration file /etc/elasticsearch/elasticsearch.yml according to the machine's IP address or localhost.

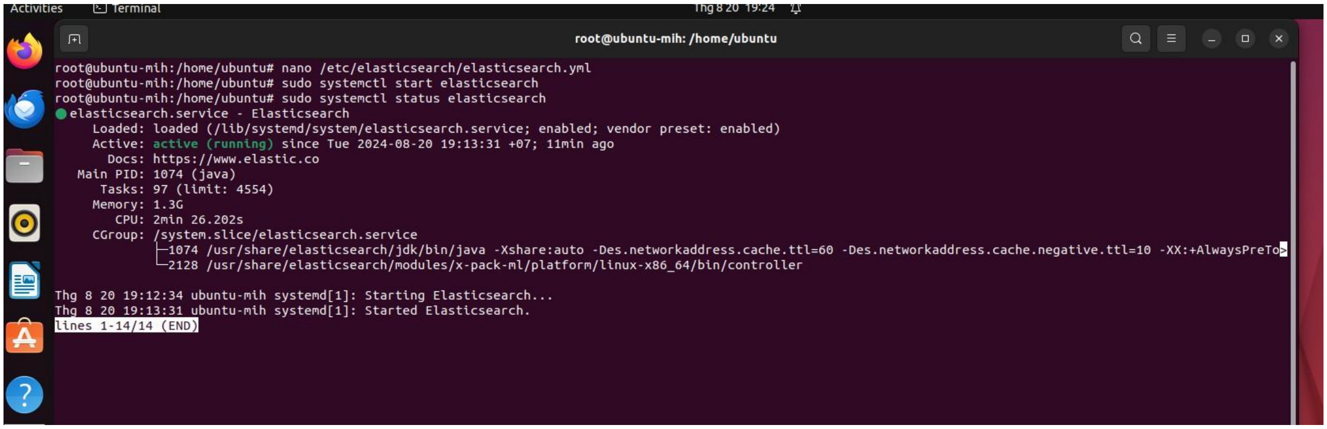


Activities
Terminal
Thg 8 20 19:23
root@ubuntu-mih: /home/ubuntu
GNU nano 6.2
/etc/elasticsearch/elasticsearch.yml

```
network.host: 127.0.0.1
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/elasticsearch.crt
xpack.security.transport.ssl.certificate_authorities: /etc/elasticsearch/certs/ca/ca.crt

# 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.crt

# Elasticsearch authentication
xpack.security.enabled: true

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

Figure 3. 5: Modify file elasticsearch.yml according to the IP address

- Start and enable Elasticsearch:

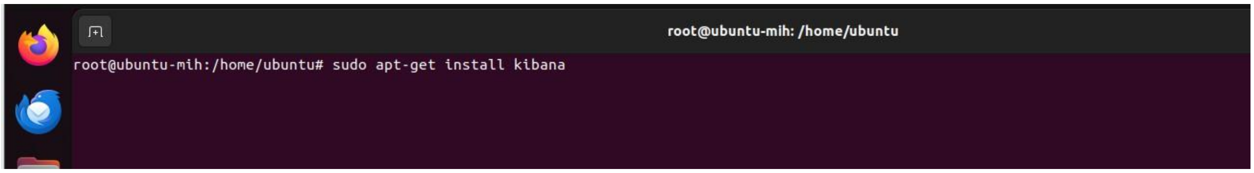


```
root@ubuntu-mih:/home/ubuntu# nano /etc/elasticsearch/elasticsearch.yml
root@ubuntu-mih:/home/ubuntu# sudo systemctl start elasticsearch
root@ubuntu-mih:/home/ubuntu# sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-08-20 19:13:31 +07; 11min ago
       Docs: https://www.elastic.co
   Main PID: 1074 (java)
      Tasks: 97 (limit: 4554)
     Memory: 1.3G
        CPU: 2min 26.202s
     CGroup: /system.slice/elasticsearch.service
             ├─1074 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTo>
             └─2128 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Thg 8 20 19:12:34 ubuntu-mih systemd[1]: Starting Elasticsearch...
Thg 8 20 19:13:31 ubuntu-mih systemd[1]: Started Elasticsearch.
lines 1-14/14 (END)
```

Figure 3. 6: Starting and activating Elastic

To visualize the data that Elasticsearch receives, Kibana is a support tool for Elasticsearch that helps users read charts more intuitively.

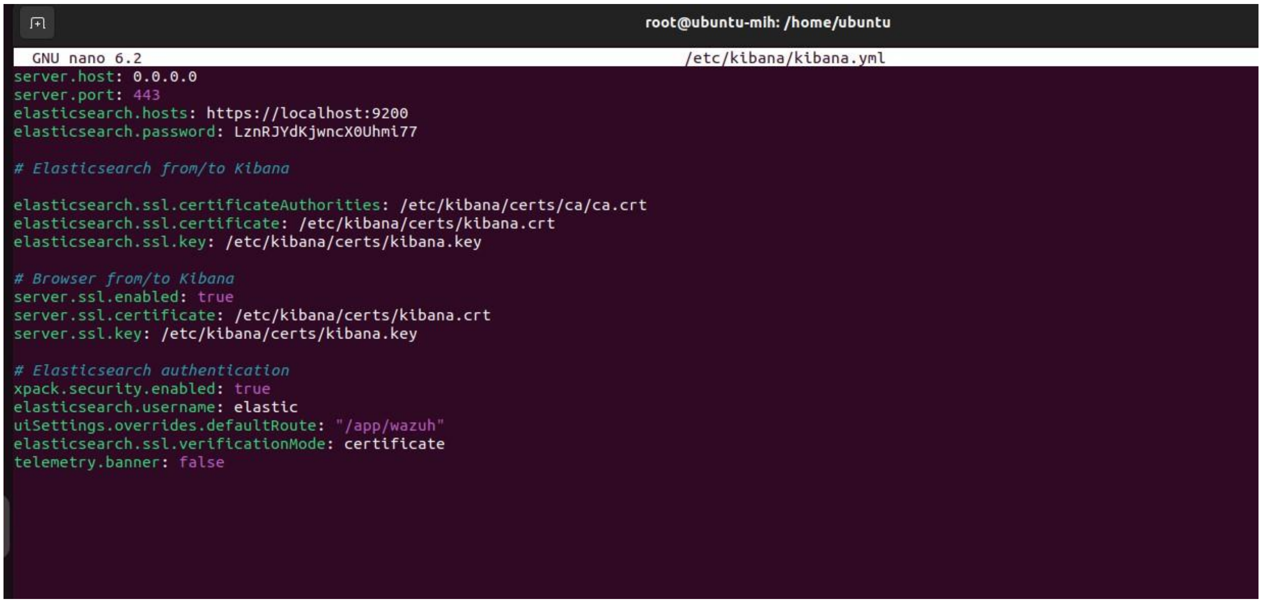
- Install Kibana on Elasticsearch



```
root@ubuntu-mih:/home/ubuntu# sudo apt-get install kibana
```

Figure 3. 7: Kibana Installation

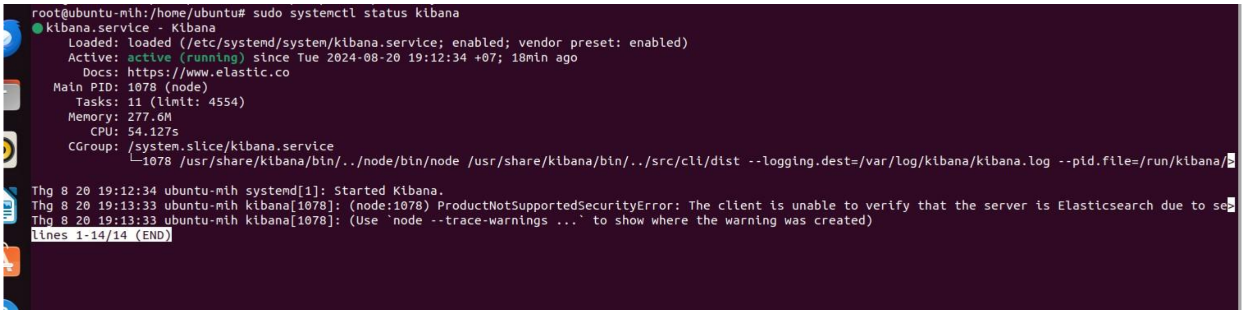
- Kibana Configuration: Modify the /etc/kibana/kibana.yml file to connect to Elasticsearch.



```
  GNU nano 6.2                                             /etc/kibana/kibana.yml
server.host: 0.0.0.0
server.port: 443
elasticsearch.hosts: https://localhost:9200
elasticsearch.password: LznRJYdKjwncX0Uhmi77

# Elasticsearch from/to Kibana

elasticsearch.ssl.certificateAuthorities: /etc/kibana/certs/ca/ca.crt
elasticsearch.ssl.certificate: /etc/kibana/certs/kibana.crt
elasticsearch.ssl.key: /etc/kibana/certs/kibana.key

# Browser from/to Kibana
server.ssl.enabled: true
server.ssl.certificate: /etc/kibana/certs/kibana.crt
server.ssl.key: /etc/kibana/certs/kibana.key

# Elasticsearch authentication
xpack.security.enabled: true
elasticsearch.username: elastic
uiSettings.overrides.defaultRoute: "/app/wazuh"
elasticsearch.ssl.verificationMode: certificate
telemetry.banner: false
```

Figure 3. 8: Kibana file configuration

- Start Kibana

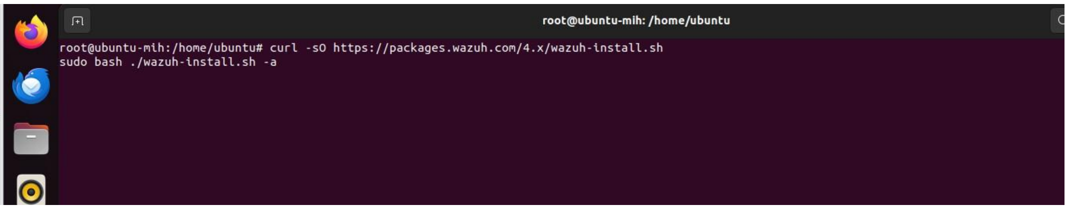


```
root@ubuntu-mih:/home/ubuntu# sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-08-20 19:12:34 +07; 18min ago
       Docs: https://www.elastic.co
   Main PID: 1078 (node)
      Tasks: 11 (limit: 4554)
     Memory: 277.6M
        CPU: 54.127s
     CGroup: /system.slice/kibana.service
             └─1078 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest=/var/log/kibana/kibana.log --pid.file=/run/kibana/>

Thg 8 20 19:12:34 ubuntu-mih systemd[1]: Started Kibana.
Thg 8 20 19:13:33 ubuntu-mih kibana[1078]: (node:1078) ProductNotSupportedSecurityError: The client is unable to verify that the server is Elasticsearch due to se>
Thg 8 20 19:13:33 ubuntu-mih kibana[1078]: (Use `node --trace-warnings ...` to show where the warning was created)
lines 1-14/14 (END)
```

Figure 3. 9: Starting the Kibana service

After installing Elasticsearch and Kibana, I will proceed to install WAZUH Server on the same Ubuntu machine.

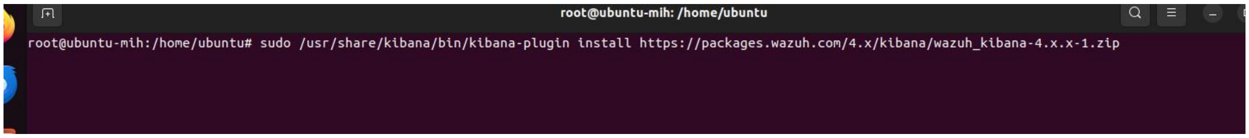
- Install WAZUH Manager:



```
root@ubuntu-mih:/home/ubuntu# curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh
sudo bash ./wazuh-install.sh -a
```

Figure 3. 10: Installing WAZUH Manager

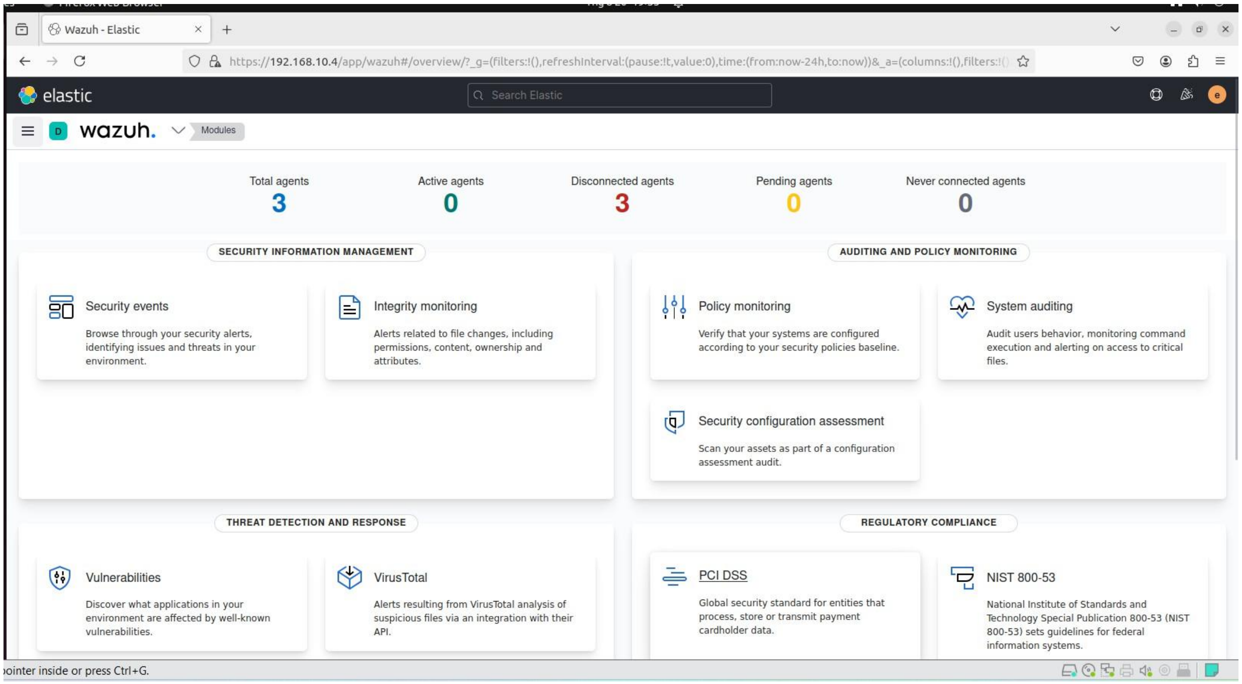
- Install WAZUH plugin on Kibana:



```
root@ubuntu-mih:/home/ubuntu# sudo /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/kibana/wazuh_kibana-4.x.x-1.zip
```

Figure 3. 11: Install WAZUH plugin

- Once installed, go to your browser and log in to your account.


Wazuh - Elastic
https://192.168.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(),filters:!()
elastic
Search Elastic
wazuh.
Modules
ointer inside or press Ctrl+G.

Total agents 3

Active agents 0

Disconnected agents 3

Pending agents 0

Never connected agents 0

SECURITY INFORMATION MANAGEMENT

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

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

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE

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

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

REGULATORY COMPLIANCE

PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.

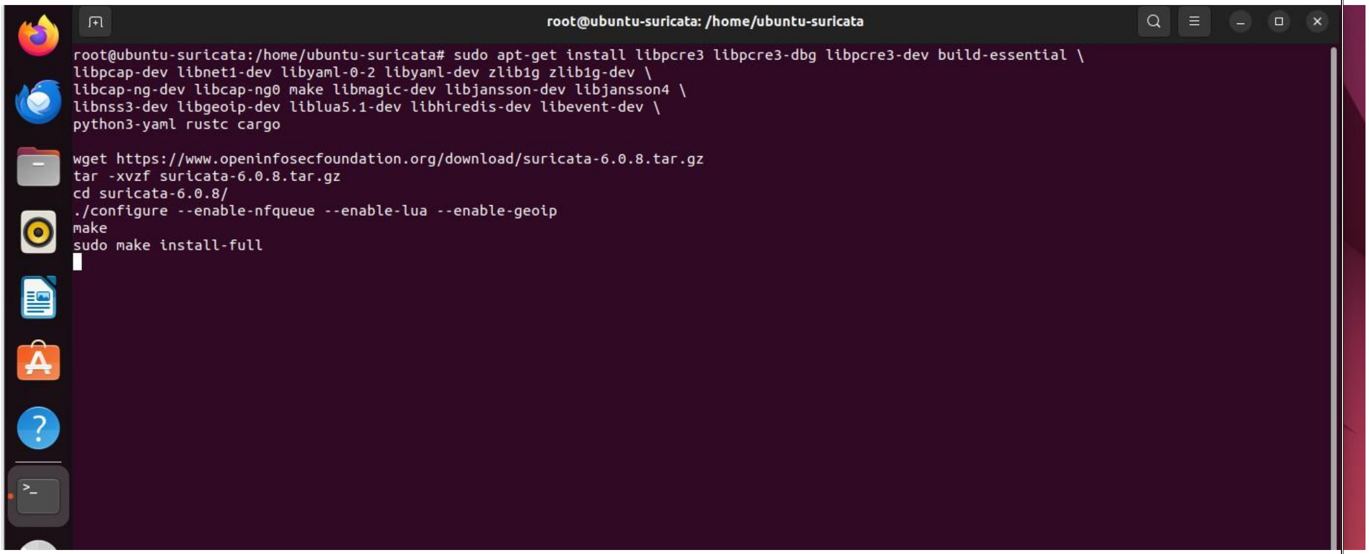
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

Figure 3. 12: Access to WAZUH Dashboard

3.3 INSTALL SURICATA

To ensure the ability to respond and effectively prevent security vulnerabilities for the system, I will integrate the Suricata IDS/IPS tool. Suricata not only provides the ability to detect and prevent Cyber Attacks in real time, but also helps monitor network traffic in detail and accurately. With Suricata, my system will be better protected against potential threats, thereby improving safety and minimizing risks from security vulnerabilities. The combination of Suricata and existing security solutions will create a comprehensive defense layer, helping the system maintain stability and security against increasingly sophisticated attacks.

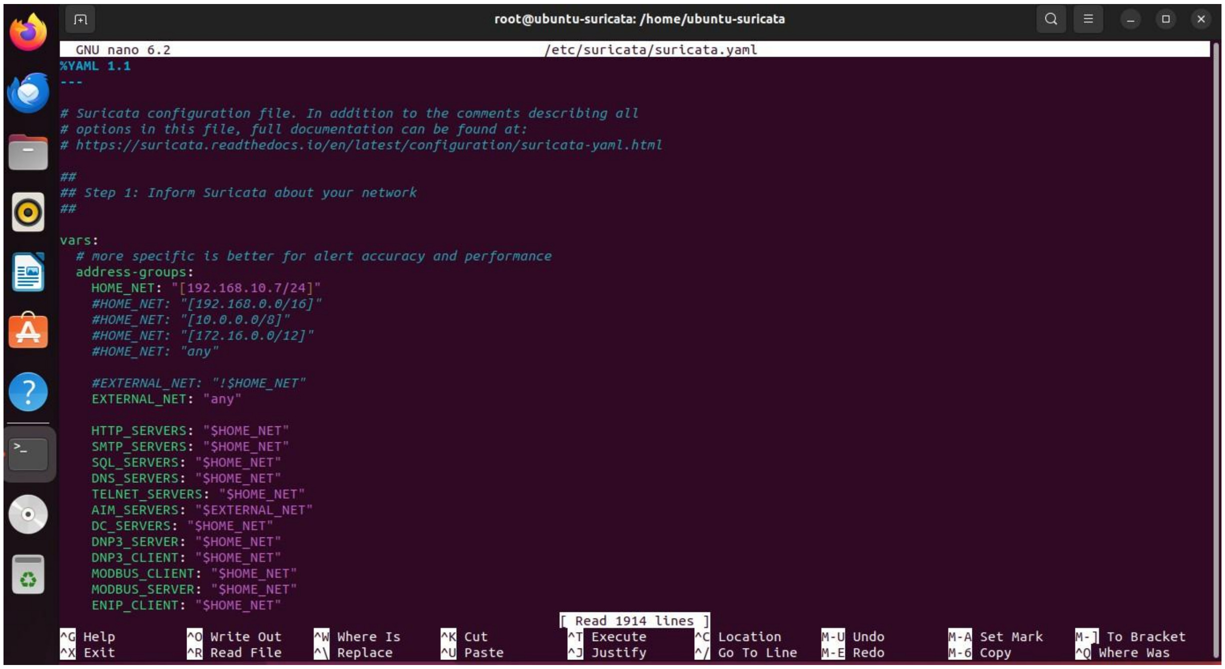
- Install Suricata. To install the latest version, I will install Suricata from Source.



```
root@ubuntu-suricata:/home/ubuntu-suricata# sudo apt-get install libpcre3 libpcre3-dbg libpcre3-dev build-essential \
libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev \
libcap-ng-dev libcap-ng0 make libmagic-dev libjansson-dev libjansson4 \
libnss3-dev libgeoip-dev liblua5.1-dev libhiredis-dev libevent-dev \
python3-yaml rustc cargo

wget https://www.openinfosecfoundation.org/download/suricata-6.0.8.tar.gz
tar -xvzf suricata-6.0.8.tar.gz
cd suricata-6.0.8/
./configure --enable-nfqueue --enable-lua --enable-geoip
make
sudo make install-full
```

Figure 3. 13: Suricata Installation

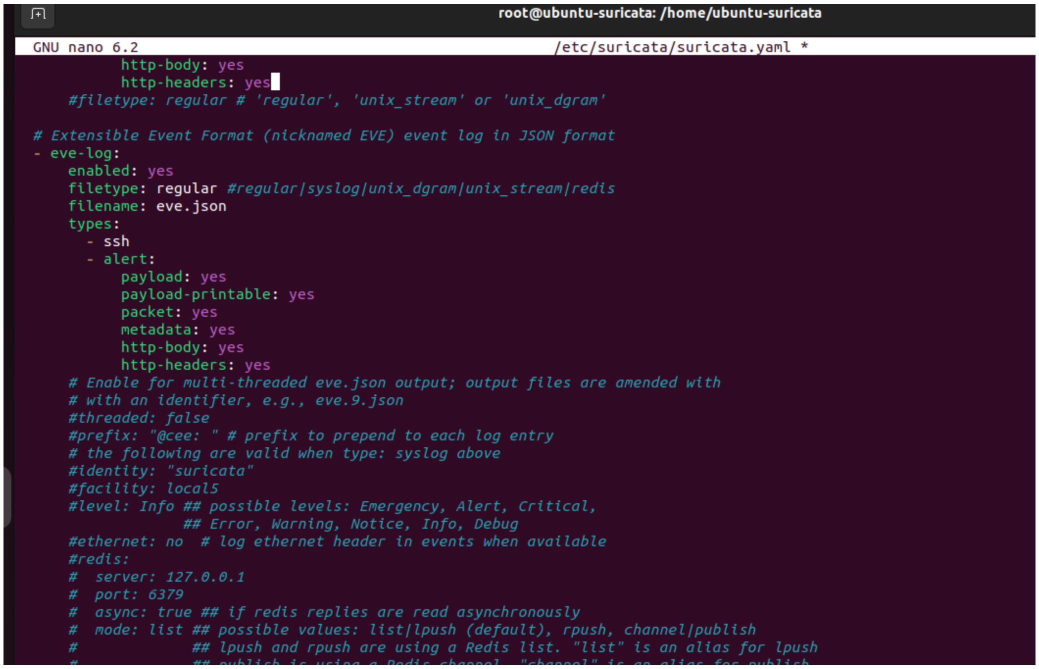
- Suricata Configuration: Modify the Suricata configuration file (/etc/suricata/suricata.yaml) to suit your network environment.



```
root@ubuntu-suricata: /home/ubuntu-suricata
  GNU nano 6.2                          /etc/suricata/suricata.yaml
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.10.7/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    #EXTERNAL_NET: "!$HOME_NET"
    EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
                                              [ Read 1914 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark    M-] To Bracket
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo        M-6 Copy        ^Q Where Was
```

Figure 3. 14: Modifying Suricata configuration file

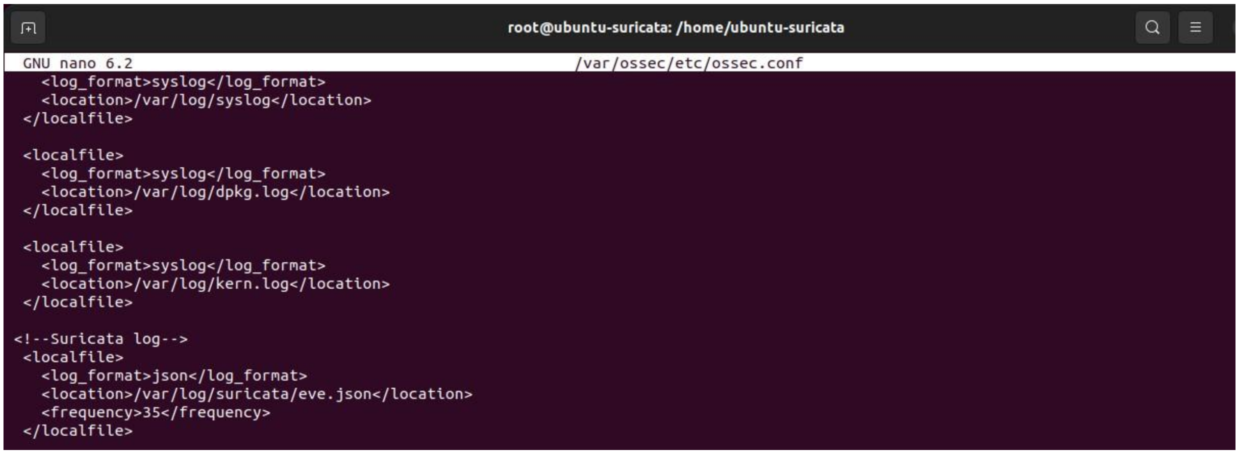
- Configure Suricata to send logs to WAZUH: Edit Suricata's configuration to export data to a JSON file (eve.json). Set the path so that WAZUH Agent can collect these logs.



```
root@ubuntu-suricata: /home/ubuntu-suricata
  GNU nano 6.2                          /etc/suricata/suricata.yaml *
            http-body: yes
            http-headers: yes
      #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

  # Extensible Event Format (nicknamed EVE) event log in JSON format
  - eve-log:
      enabled: yes
      filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
      filename: eve.json
      types:
        - ssh
        - alert:
            payload: yes
            payload-printable: yes
            packet: yes
            metadata: yes
            http-body: yes
            http-headers: yes
      # Enable for multi-threaded eve.json output; output files are amended with
      # with an identifier, e.g., eve.9.json
      #threaded: false
      #prefix: "@cee: " # prefix to prepend to each log entry
      # the following are valid when type: syslog above
      #identity: "suricata"
      #facility: local5
      #level: Info ## possible levels: Emergency, Alert, Critical,
                   ## Error, Warning, Notice, Info, Debug
      #ethernet: no  # log ethernet header in events when available
      #redis:
      #  server: 127.0.0.1
      #  port: 6379
      #  async: true ## if redis replies are read asynchronously
      #  mode: list ## possible values: list|lpush (default), rpush, channel|publish
      #             ## lpush and rpush are using a Redis list. "list" is an alias for lpush
      #             ## publish is using a Redis channel. "channel" is an alias for publish
```

Figure 3. 15: Configuring Suricata to send logs to WAZUH Manager

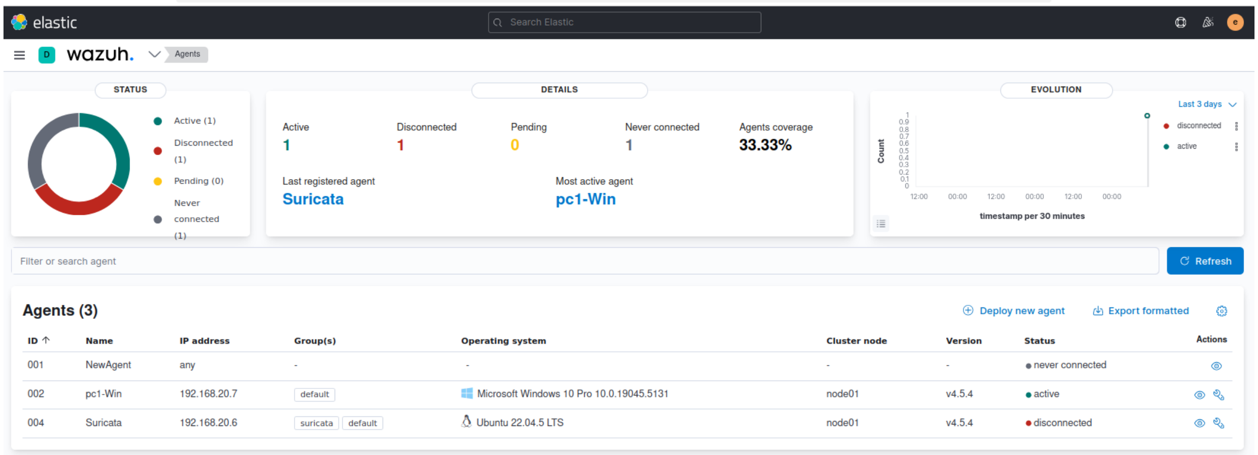
- WAZUH Agent Configuration: Configure WAZUH Agent to collect logs from Suricata.



```
 GNU nano 6.2                                              /var/ossec/etc/ossec.conf
    <log_format>syslog</log_format>
    <location>/var/log/syslog</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

<!--Suricata log-->
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
    <frequency>35</frequency>
  </localfile>
```

Figure 3. 16: WAZUH Agent Configuration

- To know if WAZUH Server has received Suricata, access WAZUH Dashboard on WAZUH server and select WAZUH Agent



Active	Disconnected	Pending	Never connected	Agents coverage
1	1	0	1	33.33%

Last registered agent: Suricata

Most active agent: pc1-Win

Agents (3)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	NewAgent	any	-	-	-	-	● never connected	
002	pc1-Win	192.168.20.7	default	Microsoft Windows 10 Pro 10.0.19045.5131	node01	v4.5.4	● active	
004	Suricata	192.168.20.6	suricata default	Ubuntu 22.04.5 LTS	node01	v4.5.4	● disconnected	

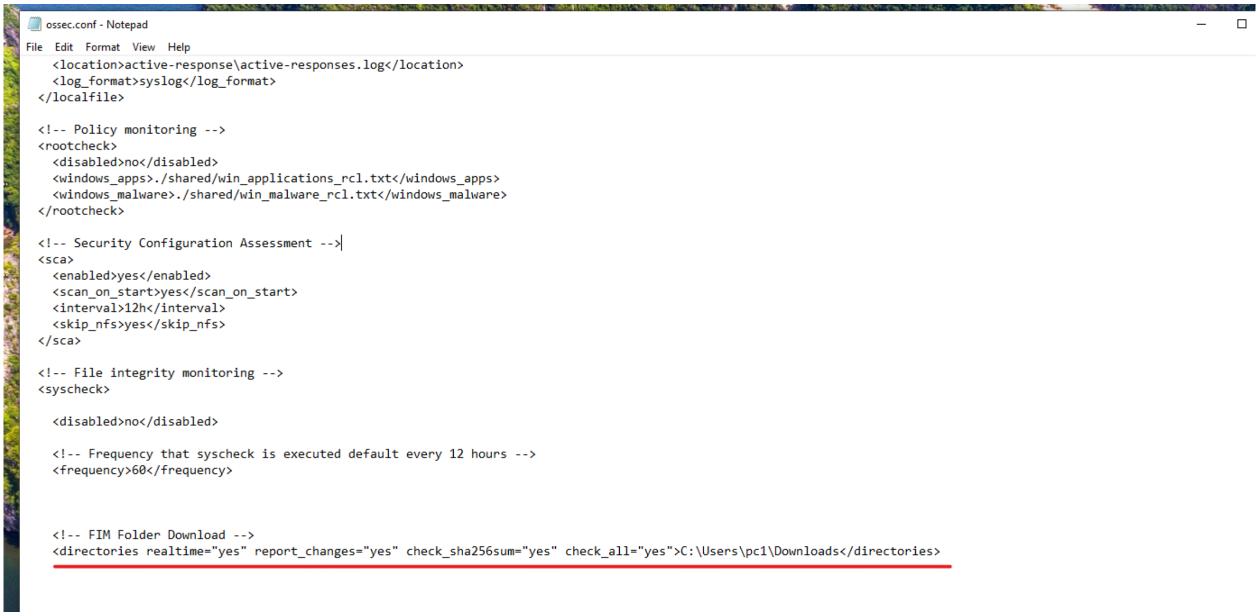
Figure 3. 17: Access WAZUH Agent on WAZUH Dashboard

3.4 MONITOR FOLDERS AND FILES ON AGENT MACHINES AND INTEGRATE WITH VIRUSTOTAL API

Directory monitoring on WAZUH Agent is an important part of system protection, especially in early detection of unwanted changes, network attacks, or malicious activities.

The WAZUH Agent syscheck module is responsible for monitoring the integrity of files and directories. It uses techniques such as hashing, checking file modification times, and other attributes to identify changes. These changes include: Creating new files/directories, modifying files/directories, deleting files/directories, renaming files/directories.

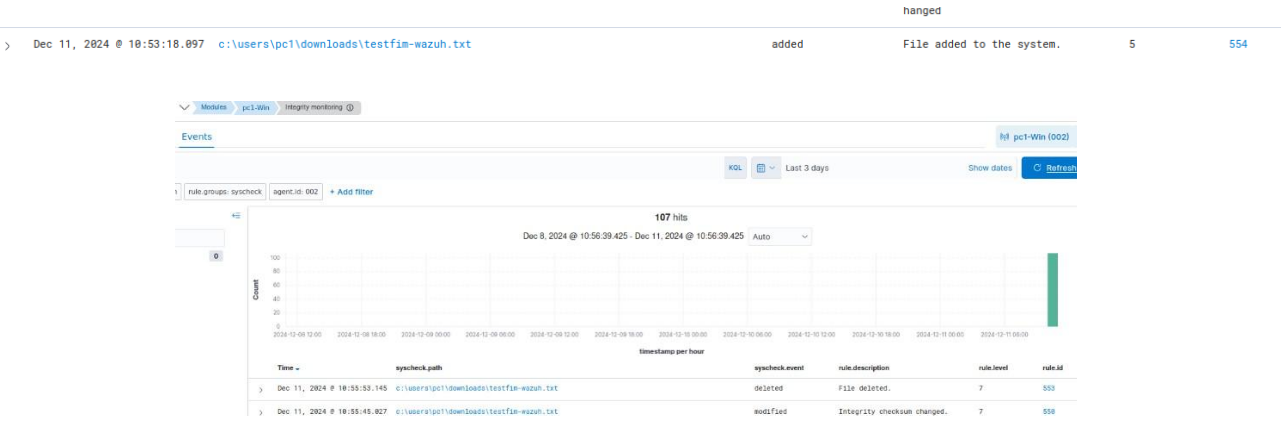
- Configure to monitor folders on WAZUH Agent, access the ossec.conf file to change the value in <syscheck>, here I will open file/folder monitoring mode and monitor the “Downloads” folder.



```
    <location>active-response\active-responses.log</location>
    <log_format>syslog</log_format>
  </localfile>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
    <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
  </rootcheck>

  <!-- Security Configuration Assessment -->
  <sca>
    <enabled>yes</enabled>
    <scan_on_start>yes</scan_on_start>
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
  </sca>

  <!-- File integrity monitoring -->
  <syscheck>

    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>60</frequency>


    <!-- FIM Folder Download -->
    <directories realtime="yes" report_changes="yes" check_sha256sum="yes" check_all="yes">C:\Users\pc1\Downloads</directories>
```

Figure 3. 18: Configuring directory monitoring on WAZUH Agent

- After adding the folder to monitor, I will restart the WAZUH Agent service. Next, I will add, edit and delete folders/files in the “Downloads” folder. After that, the WAZUH Server will notify the changes that have been made to the “Downloads” folder.

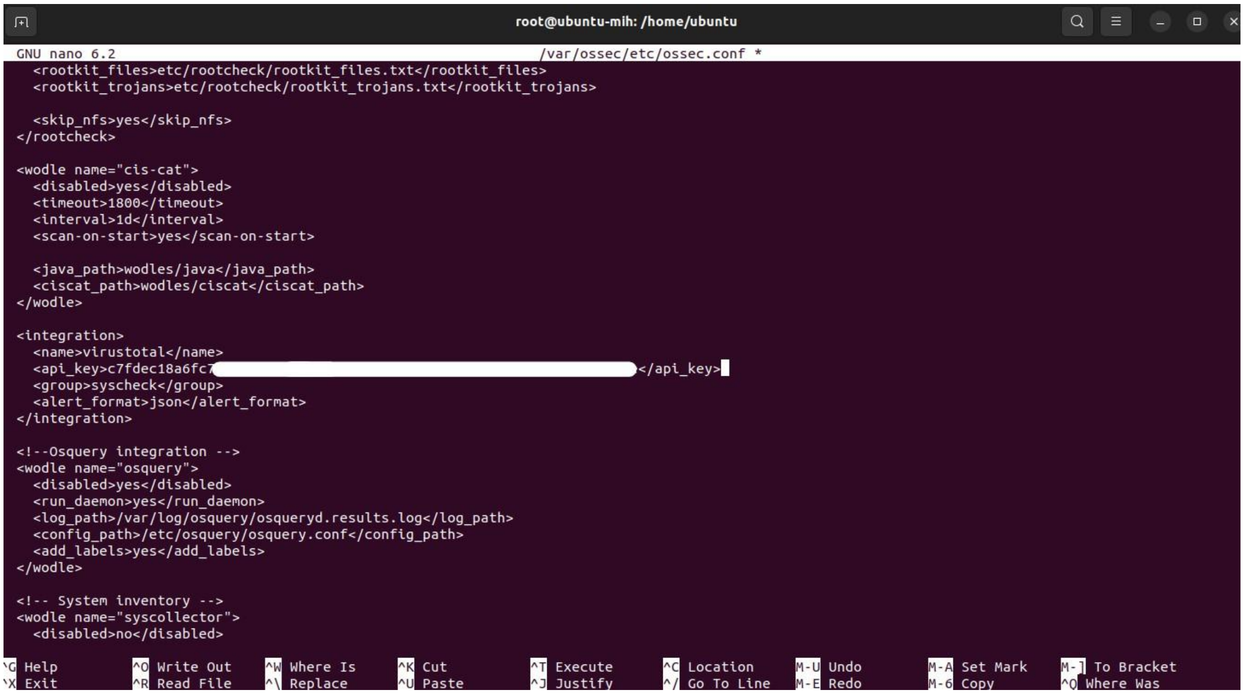


```
                                                                                              hanged
Dec 11, 2024 @ 10:53:18.097  c:\users\pc1\downloads\testfim-wazuh.txt      added              File added to the system.      5    554

Time                          syscheck.path                                 syscheck.event     rule.description               rule.level  rule.id
Dec 11, 2024 @ 10:55:53.145  c:\users\pc1\downloads\testfim-wazuh.txt      deleted            File deleted.                  7    553
Dec 11, 2024 @ 10:55:45.027  c:\users\pc1\downloads\testfim-wazuh.txt      modified           Integrity checksum changed.    7    550
```

Figure 3. 19: WAZUH Dashboard has received the log file from WAZUH Agent

Integrating VirusTotal API on WAZUH Server enhances the ability to detect and respond to malicious files and URLs using VirusTotal's powerful analysis service. VirusTotal allows submitting files and URLs for checking through various security tools, providing detailed information about their potential threat level. Functions when integrating APT VirusTotal on WAZUH Manager: File/URL analysis, threat detection, alert generation for supervisors.

- To get the VirusTotal API, I will register on the VirusTotal homepage. After registering and getting the API, I will add the VirusTotal API to the /var/ossec/etc/ossec.conf file on the WAZUH Server.

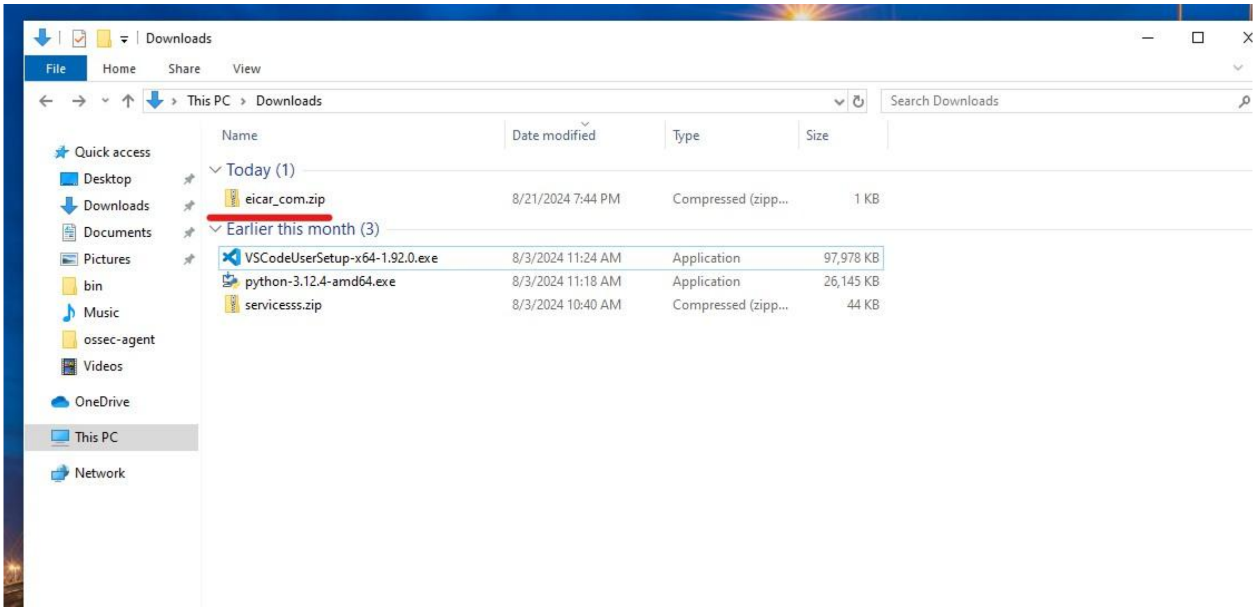


```
root@ubuntu-mih: /home/ubuntu
GNU nano 6.2                                    /var/ossec/etc/ossec.conf *
  <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>

  <skip_nfs>yes</skip_nfs>
</rootcheck>

<wodle name="cis-cat">
  <disabled>yes</disabled>
  <timeout>1800</timeout>
  <interval>1d</interval>
  <scan-on-start>yes</scan-on-start>

  <java_path>wodles/java</java_path>
  <ciscat_path>wodles/ciscat</ciscat_path>
</wodle>

<integration>
  <name>virustotal</name>
  <api_key>c7fdec18a6fc7[redacted]</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>

<!--Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

Figure 3. 20: Integrating VirusTotal API into Wauzh Manager

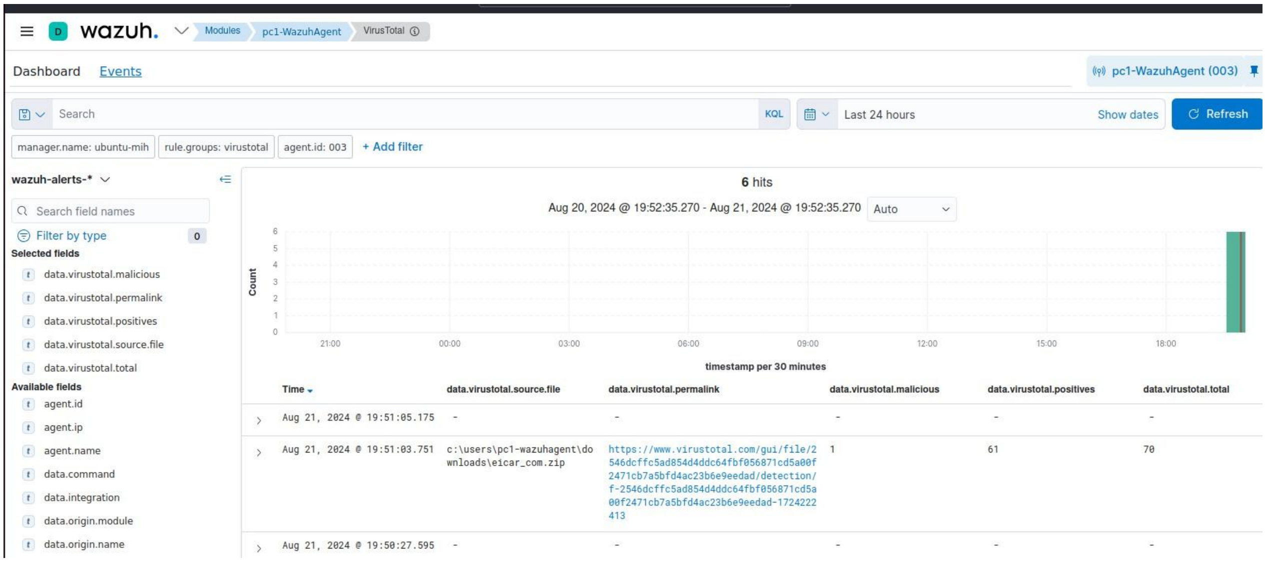
- After making changes to the configuration file, restart the WAZUH Manager service to apply the new configuration.

- Next, I will download a test file containing malicious code on WAZUH Agent so that WAZUH Server can scan it and display a notification to the network supervisor about dangerous files.



Name	Date modified	Type	Size
Today (1)			
eicar_com.zip	8/21/2024 7:44 PM	Compressed (zipp...	1 KB
Earlier this month (3)			
VSCodeUserSetup-x64-1.92.0.exe	8/3/2024 11:24 AM	Application	97,978 KB
python-3.12.4-amd64.exe	8/3/2024 11:18 AM	Application	26,145 KB
servicesss.zip	8/3/2024 10:40 AM	Compressed (zipp...	44 KB

Figure 3. 21: File containing malicious code downloaded from WAZUH Agent



Time	data.virustotal.source.file	data.virustotal.permalink	data.virustotal.malicious	data.virustotal.positives	data.virustotal.total
Aug 21, 2024 @ 19:51:05.175	-	-	-	-	-
Aug 21, 2024 @ 19:51:03.751	c:\users\pc1-wazuhagent\downloads\eicar_com.zip	https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad-1724222413	1	61	70
Aug 21, 2024 @ 19:50:27.595	-	-	-	-	-

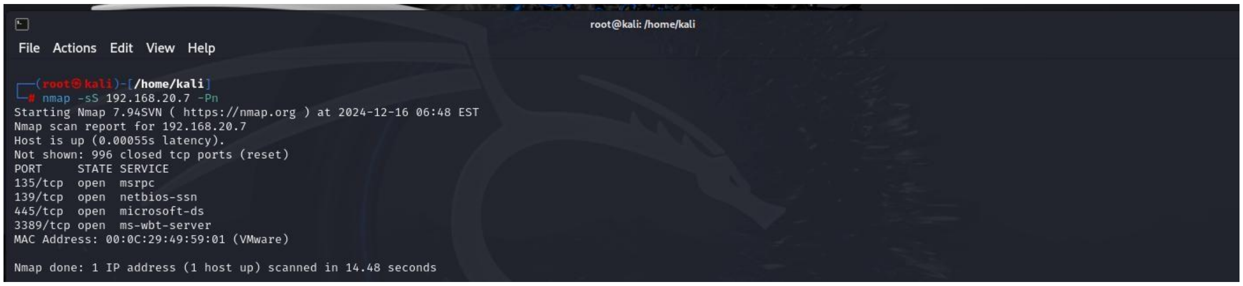
Figure 3. 22: WAZUH Manager receives log when detecting malicious file from WAZUH Agent

3.5 COMBINE WITH SURICATATO WARN OF CERTAIN ATTACK METHODS

Suricata is an open-source intrusion detection system (IDS), intrusion prevention system (IPS), and network security monitoring (NSM). Developed by the Open Information Security Foundation (OISF), Suricata monitors network traffic and analyzes packets in real time to detect suspicious behavior or attacks.

- Use Suricata to alert when the network uses NMAP to scan:

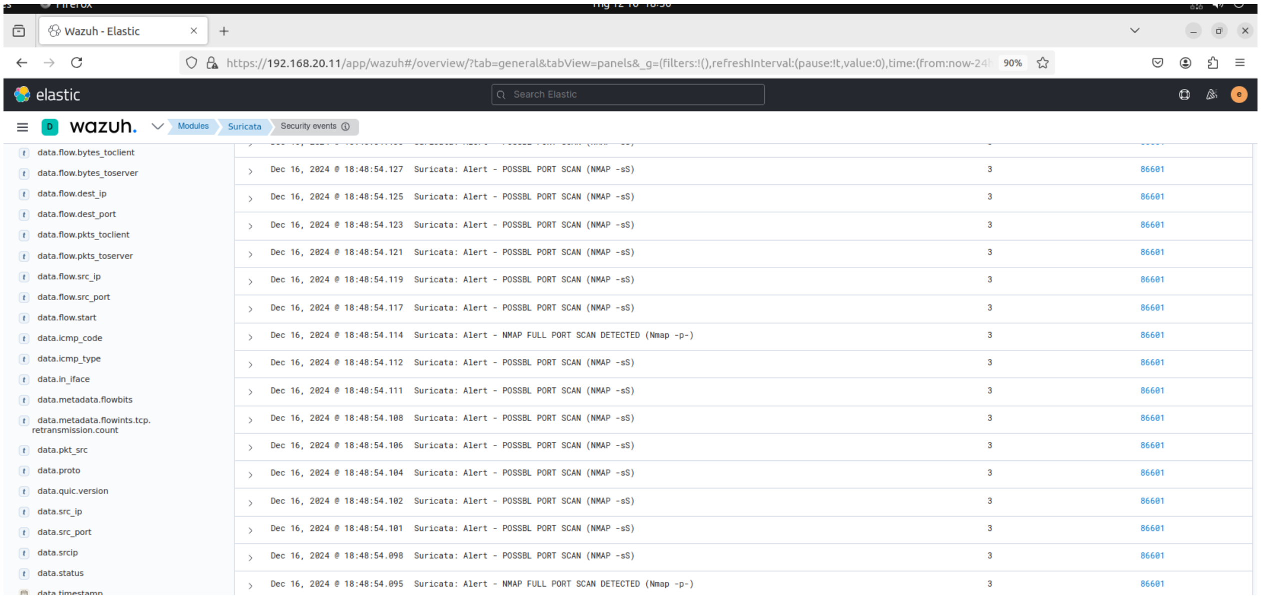
- On Kali Linux perform an NMAP scan to a Windows Endpoint machine with WAZUH Agent installed.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.20.7 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 06:48 EST
Nmap scan report for 192.168.20.7
Host is up (0.00055s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:49:59:01 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
```

Figure 3. 23: From Kali machine, use nmap to scan to Windows endpoint machine

- Go to WAZUH Manager to check the log from Suricata transferred to WAZUH

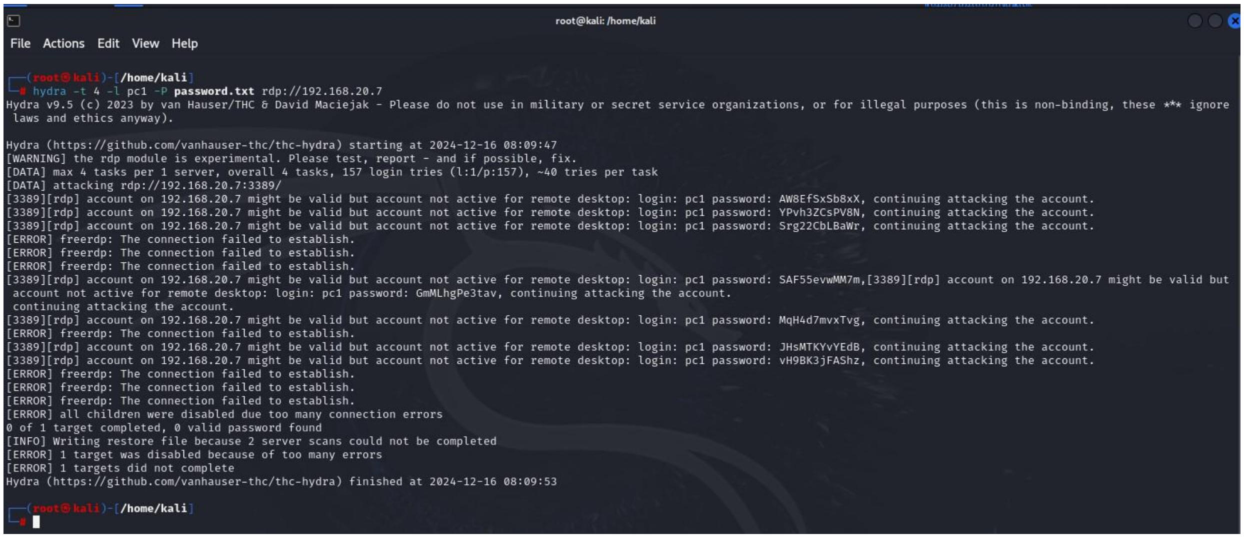


```
Dec 16, 2024 @ 18:48:54.127  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.125  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.123  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.121  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.119  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.117  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.114  Suricata: Alert - NMAP FULL PORT SCAN DETECTED (Nmap -p-)  3  86601
Dec 16, 2024 @ 18:48:54.112  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.111  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.108  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.106  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.104  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.102  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.101  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.098  Suricata: Alert - POSSBL PORT SCAN (NMAP -sS)  3  86601
Dec 16, 2024 @ 18:48:54.095  Suricata: Alert - NMAP FULL PORT SCAN DETECTED (Nmap -p-)  3  86601
```

Figure 3. 24: Warning from Suricata sent to WAZUH when detecting an nmap scanner

- Use Suricata to detect brute force attacks and alert on WAZUH Manager:

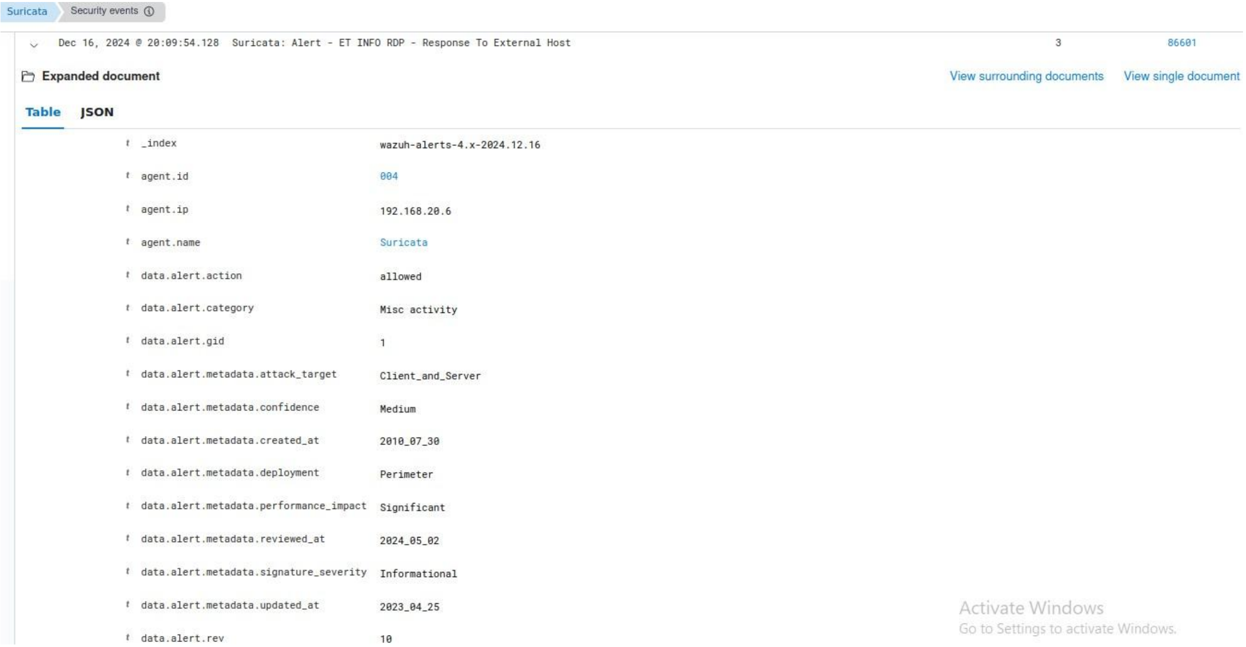
- On the Kali attack machine, use hydra to brute force attack to the windows endpoint that has installed WAZUH agent.



```
┌──(root㉿kali)-[/home/kali]
└─# hydra -t 4 -l pc1 -P password.txt rdp://192.168.20.7
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
 laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-16 08:09:47
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 157 login tries (l:1/p:157), ~40 tries per task
[DATA] attacking rdp://192.168.20.7:3389/
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: AW8EfSxSb8xX, continuing attacking the account.
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: YPvh3ZCsPV8N, continuing attacking the account.
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: Srg22CbLBaWr, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: SAF55evwMM7m,[3389][rdp] account on 192.168.20.7 might be valid but
 account not active for remote desktop: login: pc1 password: GmMLhgPe3tav, continuing attacking the account.
 continuing attacking the account.
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: MqH4d7mvxTvg, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: JHsMTKYvYEdB, continuing attacking the account.
[3389][rdp] account on 192.168.20.7 might be valid but account not active for remote desktop: login: pc1 password: vH9BK3jFAShz, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 08:09:53

┌──(root㉿kali)-[/home/kali]
└─#
```

Figure 3. 25: Kali machine Brute force attack to Windows endpoint

- WAZUH Manager immediately receives a warning when Suricata detects a Brute force attack and sends a warning to WAZUH Manager.



Dec 16, 2024 @ 20:09:54.128 Suricata: Alert - ET INFO RDP - Response To External Host 3 86601

```
_index                                      wazuh-alerts-4.x-2024.12.16
agent.id                                    004
agent.ip                                    192.168.20.6
agent.name                                  Suricata
data.alert.action                           allowed
data.alert.category                         Misc activity
data.alert.gid                              1
data.alert.metadata.attack_target           Client_and_Server
data.alert.metadata.confidence              Medium
data.alert.metadata.created_at              2010_07_30
data.alert.metadata.deployment              Perimeter
data.alert.metadata.performance_impact      Significant
data.alert.metadata.reviewed_at             2024_05_02
data.alert.metadata.signature_severity      Informational
data.alert.metadata.updated_at              2023_04_25
data.alert.rev                              10
```

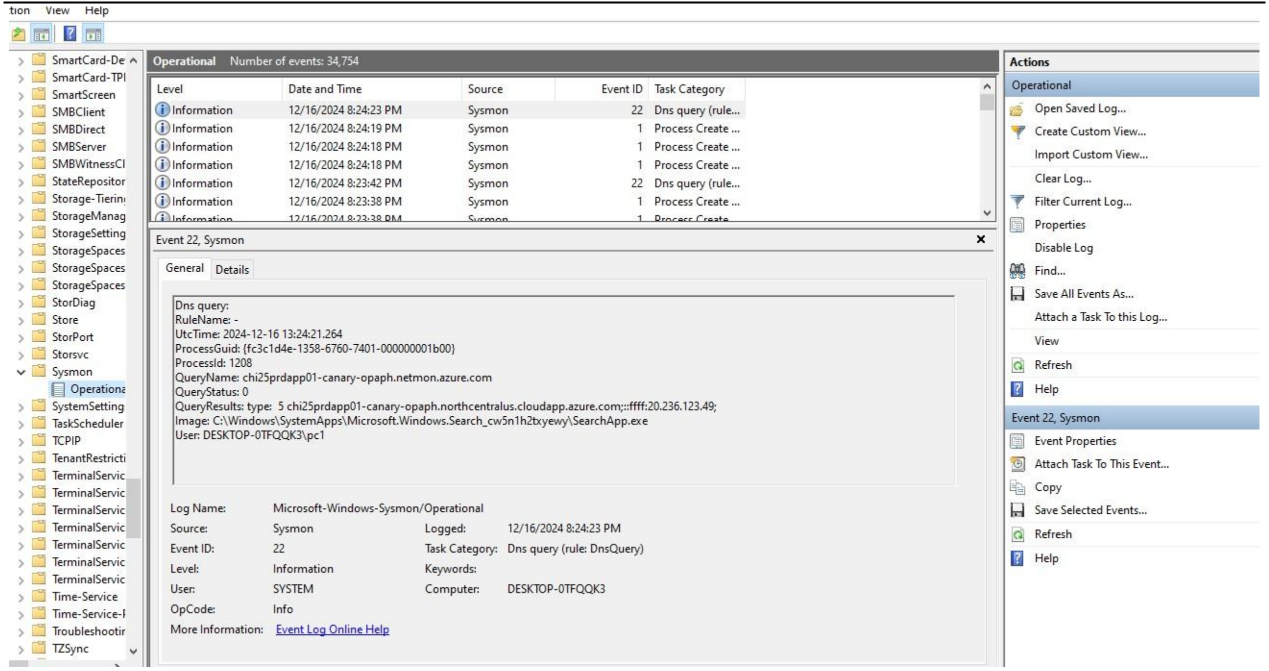
Figure 3. 26: WAZUH Manager has received logs when detecting brute force attack

3.6 WARNING ABOUT MITRE ATTACK-BASED ATTACK TECHNIQUES

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a framework developed by MITRE to provide a knowledge base of tactics, techniques, and attack methods commonly used by real-world attackers. The framework helps organizations better understand cyber security threats and improve their defenses and responses to attacks. MITRE ATT&CK focuses on describing attacker behaviors, from Initial Access to Privilege Escalation to Collection.

When WAZUH is integrated with MITRE ATT&CK, it acts as a monitoring and analysis tool that detects suspicious behavior based on the techniques defined in the ATT&CK framework. WAZUH uses log data from systems, devices, and applications and compares it with the techniques in MITRE ATT&CK to identify signs of attack behavior. This allows security administrators to quickly identify the techniques that attackers are using and take appropriate countermeasures. Additionally, the WAZUH dashboard provides a visual view of compliance and activities related to the ATT&CK framework, helping to improve threat detection and response.

- On Windows machine download and install Sysmon, to monitor windows endpoint system through sysmon tool. After installation, Sysmon will record detailed events such as running processes, network connections and file changes, which is very useful in detecting suspicious activities.



Operational Number of events: 34,754

Level	Date and Time	Source	Event ID	Task Category
Information	12/16/2024 8:24:23 PM	Sysmon	22	Dns query (rule...
Information	12/16/2024 8:24:19 PM	Sysmon	1	Process Create ...
Information	12/16/2024 8:24:18 PM	Sysmon	1	Process Create ...
Information	12/16/2024 8:24:18 PM	Sysmon	1	Process Create ...
Information	12/16/2024 8:23:42 PM	Sysmon	22	Dns query (rule...
Information	12/16/2024 8:23:38 PM	Sysmon	1	Process Create ...
Information	12/16/2024 8:23:38 PM	Sysmon	1	Process Create

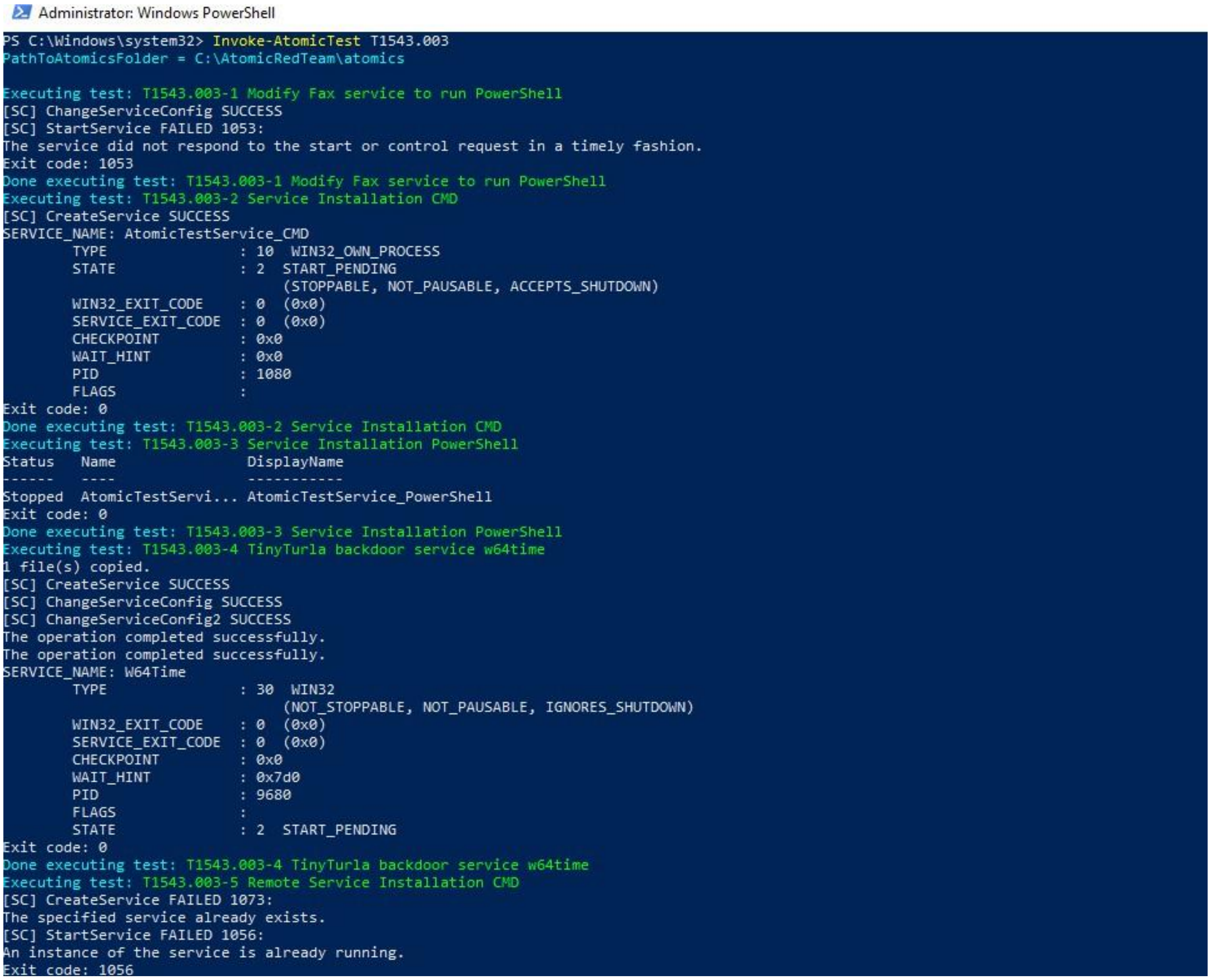
Event 22, Sysmon

```
Dns query:
RuleName: -
UtcTime: 2024-12-16 13:24:21.264
ProcessGuid: {fc3c1d4e-1358-6760-7401-000000001b00}
ProcessId: 1208
QueryName: chi25prdapp01-canary-opaph.netmon.azure.com
QueryStatus: 0
QueryResults: type:  5 chi25prdapp01-canary-opaph.northcentralus.cloudapp.azure.com;::ffff:20.236.123.49;
Image: C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
User: DESKTOP-0TFQQK3\pc1
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	12/16/2024 8:24:23 PM
Event ID:	22	Task Category:	Dns query (rule: DnsQuery)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-0TFQQK3
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 3. 27: Sysmon logs events at Windows Endpoint

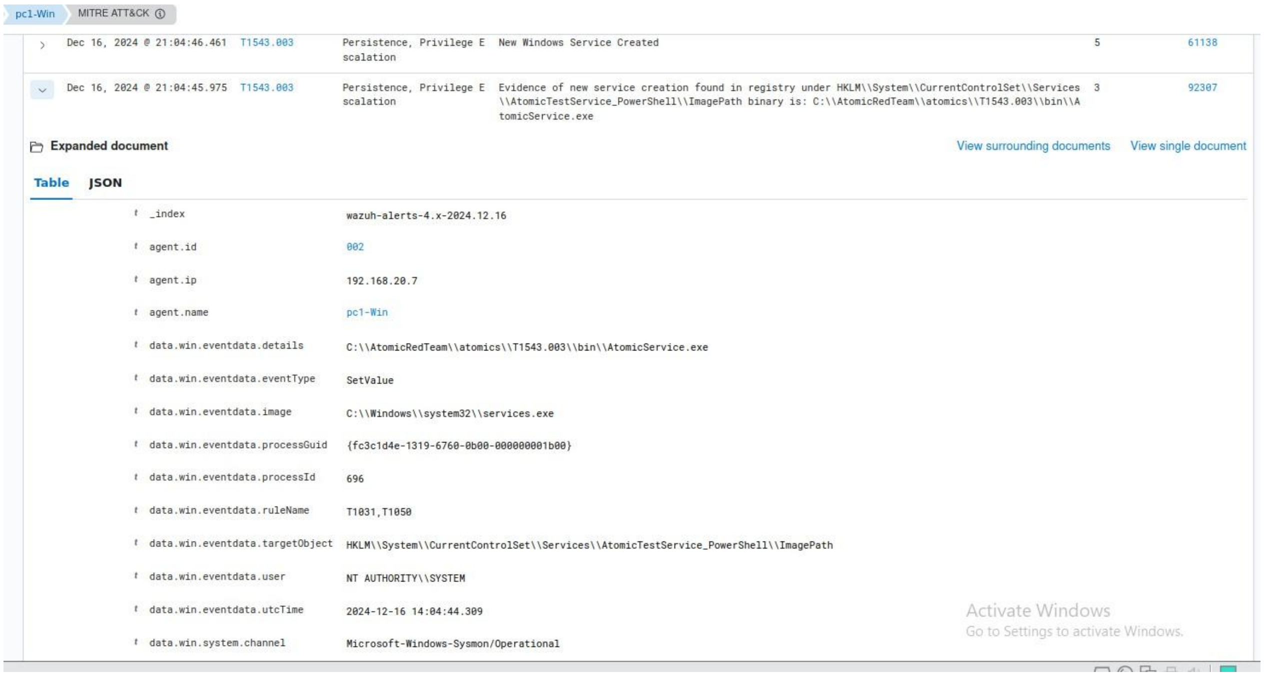
- On Windows Endpoint download and install AtomicRedTeam. Atomic Red Team is a powerful tool designed to simulate attack techniques according to the MITRE ATT&CK framework. Open PowerShell with Administrator privileges, then run some attack techniques that have been prepared in Atomic Red Team. In this example, I will use technique T1543.003 to create new or modify Windows Services to achieve some goals such as persistence, execution, or privilege escalation.



```
PS C:\Windows\system32> Invoke-AtomicTest T1543.003
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1543.003-1 Modify Fax service to run PowerShell
[SC] ChangeServiceConfig SUCCESS
[SC] StartService FAILED 1053:
The service did not respond to the start or control request in a timely fashion.
Exit code: 1053
Done executing test: T1543.003-1 Modify Fax service to run PowerShell
Executing test: T1543.003-2 Service Installation CMD
[SC] CreateService SUCCESS
SERVICE_NAME: AtomicTestService_CMD
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 1080
        FLAGS              :
Exit code: 0
Done executing test: T1543.003-2 Service Installation CMD
Executing test: T1543.003-3 Service Installation PowerShell
Status   Name               DisplayName
------   ----               -----------
Stopped  AtomicTestServi... AtomicTestService_PowerShell
Exit code: 0
Done executing test: T1543.003-3 Service Installation PowerShell
Executing test: T1543.003-4 TinyTurla backdoor service w64time
1 file(s) copied.
[SC] CreateService SUCCESS
[SC] ChangeServiceConfig SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
The operation completed successfully.
The operation completed successfully.
SERVICE_NAME: W64Time
        TYPE               : 30  WIN32
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 9680
        FLAGS              :
        STATE              : 2  START_PENDING
Exit code: 0
Done executing test: T1543.003-4 TinyTurla backdoor service w64time
Executing test: T1543.003-5 Remote Service Installation CMD
[SC] CreateService FAILED 1073:
The specified service already exists.
[SC] StartService FAILED 1056:
An instance of the service is already running.
Exit code: 1056
```

Figure 3. 28: Using AtomicRedTeam to attack based on Mitre Attack framework

- After Windows uses AtomicRedTeam to test against the Mitre Attack framework, Sysmon will record events and send them to WAZUH Manager, from which WAZUH Manager will analyze those events and notify the technical supervisor which Mitre Attack was used.



```
>  Dec 16, 2024 @ 21:04:46.461  T1543.003  Persistence, Privilege E  New Windows Service Created                                                          5   61138
                                           scalation
v  Dec 16, 2024 @ 21:04:45.975  T1543.003  Persistence, Privilege E  Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services  3   92307
                                           scalation                 \\AtomicTestService_PowerShell\\ImagePath binary is: C:\\AtomicRedTeam\\atomics\\T1543.003\\bin\\A
                                                                     tomicService.exe
```

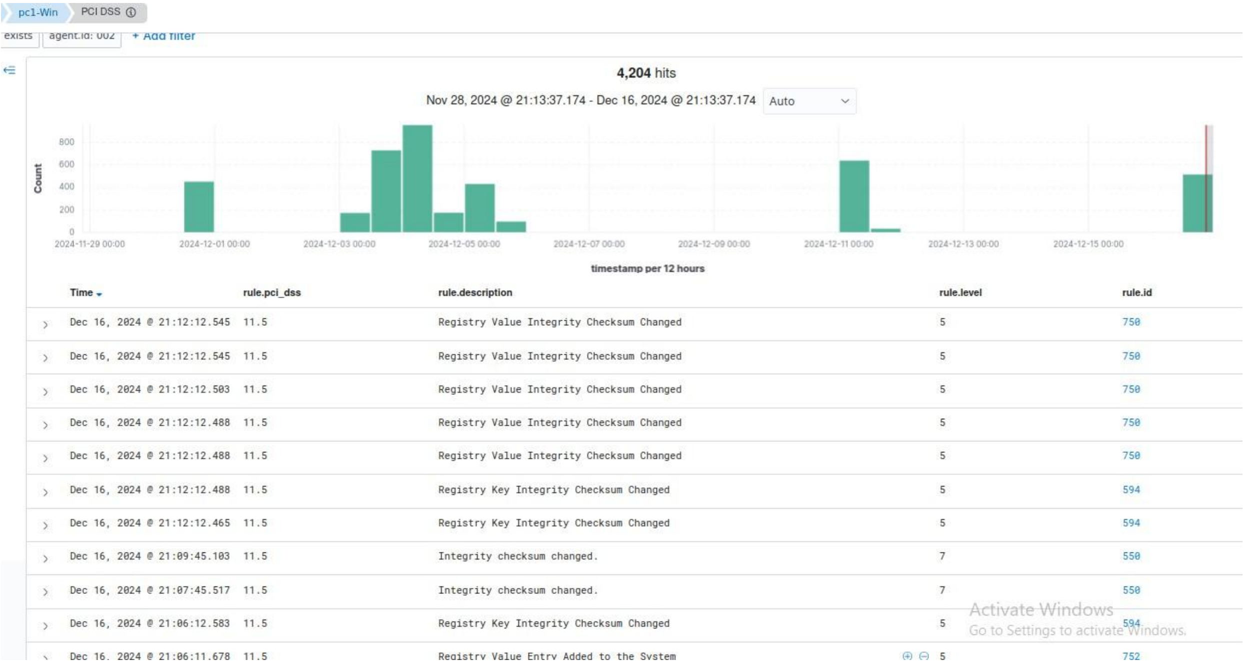
```
t  _index                          wazuh-alerts-4.x-2024.12.16
t  agent.id                        002
t  agent.ip                        192.168.20.7
t  agent.name                      pc1-Win
t  data.win.eventdata.details      C:\\AtomicRedTeam\\atomics\\T1543.003\\bin\\AtomicService.exe
t  data.win.eventdata.eventType    SetValue
t  data.win.eventdata.image        C:\\Windows\\system32\\services.exe
t  data.win.eventdata.processGuid  {fc3c1d4e-1319-6760-0b00-000000001b00}
t  data.win.eventdata.processId    696
t  data.win.eventdata.ruleName     T1031,T1050
t  data.win.eventdata.targetObject HKLM\\System\\CurrentControlSet\\Services\\AtomicTestService_PowerShell\\ImagePath
t  data.win.eventdata.user         NT AUTHORITY\\SYSTEM
t  data.win.eventdata.utcTime      2024-12-16 14:04:44.309
t  data.win.system.channel         Microsoft-Windows-Sysmon/Operational
```

Figure 3. 29: Warning from Sysmon on Windows sent to WAZUH Manager

3.7 IMPLEMENT CONTROLACCORDING TO INTERNATIONAL STANDARDS (PCI DSS, GDPR, HIPAA, …)

Security controls based on international standards such as PCI DSS, GDPR, and HIPAA are guiding frameworks to ensure that organizations handle data securely, comply with security regulations, and protect sensitive information. When integrated into the WAZUH system, these standards bring many outstanding benefits. WAZUH provides automated compliance monitoring, real-time breach detection, and centralized risk management through intuitive dashboards. The system also supports the generation of detailed reports for audits, making it easy for organizations to demonstrate compliance to regulatory agencies. At the same time, WAZUH enhances systemsecurity by continuously monitoring logs, network activity, and configuration changes, thereby quickly detecting and handling suspicious or non-compliant behavior. As a result, organizations not only reduce their risk of legal and financial violations, but also build trust with customers and partners, while optimizing resources and focusing on business goals.

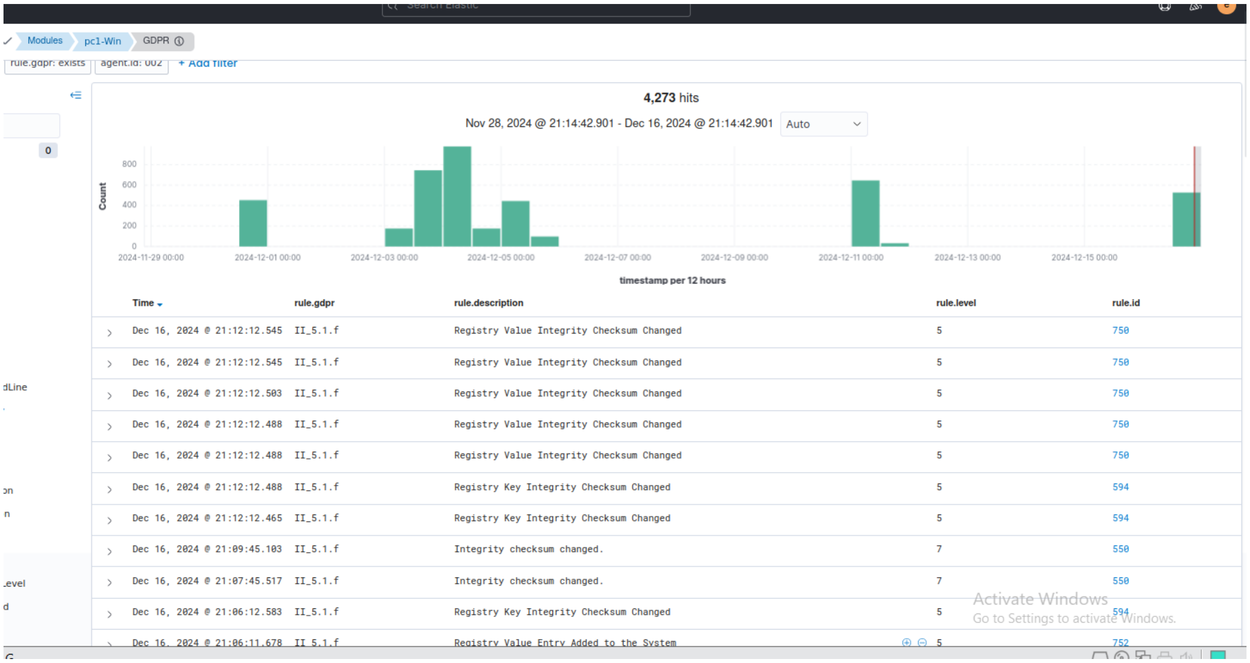
- PCI DSS Standards:



Time	rule.pci_dss	rule.description	rule.level	rule.id
Dec 16, 2024 @ 21:12:12.545	11.5	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.545	11.5	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.503	11.5	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.488	11.5	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.488	11.5	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.488	11.5	Registry Key Integrity Checksum Changed	5	594
Dec 16, 2024 @ 21:12:12.465	11.5	Registry Key Integrity Checksum Changed	5	594
Dec 16, 2024 @ 21:09:45.103	11.5	Integrity checksum changed.	7	550
Dec 16, 2024 @ 21:07:45.517	11.5	Integrity checksum changed.	7	550
Dec 16, 2024 @ 21:06:12.583	11.5	Registry Key Integrity Checksum Changed	5	594
Dec 16, 2024 @ 21:06:11.678	11.5	Registry Value Entry Added to the System	5	752

Figure 3. 30: PCI DSS standard

- GDPR Standards:



Time	rule.gdpr	rule.description	rule.level	rule.id
Dec 16, 2024 @ 21:12:12.545	II_5.1.f	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.545	II_5.1.f	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.503	II_5.1.f	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.488	II_5.1.f	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.488	II_5.1.f	Registry Value Integrity Checksum Changed	5	750
Dec 16, 2024 @ 21:12:12.488	II_5.1.f	Registry Key Integrity Checksum Changed	5	594
Dec 16, 2024 @ 21:12:12.465	II_5.1.f	Registry Key Integrity Checksum Changed	5	594
Dec 16, 2024 @ 21:09:45.103	II_5.1.f	Integrity checksum changed.	7	550
Dec 16, 2024 @ 21:07:45.517	II_5.1.f	Integrity checksum changed.	7	550
Dec 16, 2024 @ 21:06:12.583	II_5.1.f	Registry Key Integrity Checksum Changed	5	594
Dec 16, 2024 @ 21:06:11.678	II_5.1.f	Registry Value Entry Added to the System	5	752

Figure 3. 31: GDPR standards

CONCLUSION

IMPLEMENTATION RESULTS

The topic "Research and implementation of WAZUH open-source security platform" focuses on establishing and integrating these two powerful security tools WAZUH and Suricata to create an effective network attack monitoring and detection system. The results include installing and configuring WAZUH and Suricata, setting up Suricata to detect security events and send logs to WAZUH Manager for analysis. This system allows administrators to monitor network attacks such as port scanning and brute force, and generate detailed alerts and reports. The topic also evaluates the performance and accuracy of the system, and provides deployment and optimization instructions to improve security effectiveness and practical applicability in the enterprise environment.

DEVELOPMENT DIRECTION

The development direction of the topic "Research and implementation of WAZUH open-source security platform with Suricata integration" includes expanding integration with other security tools, optimizing system performance to save resources and improve scalability, developing custom rules and signatures to detect new threats, and improving the ability to automatically respond to security incidents. The topic can also apply AI and Machine Learning to analyze and predict threats more effectively, improve the user interface and reporting of WAZUH Dashboard, and study the possibility of deployment in multi-cloud environments to ensure comprehensive security in complex systems.

REFERENCES

[1] WAZUH Team (2023), WAZUH Documentation, Official Documentation.

[2] Cybertool Guardian (2024), Sending Suricata Logs to WAZUH, Medium.

[3] Aravind Raja (2024), VirusTotal Integration in WAZUH, LinkedIn Pulse.

[4] 17rjain (2024), File Integrity Monitoring (FIM) in WAZUH: A Step-by-Step Guide, Medium.

[5] Rajneesh Gupta (2023), Home Lab6: MITRE ATT&CK WAZUH Walkthrough, LinkedIn Pulse.

[6] WAZUH Team (2023), Compliance Module in WAZUH, Official Documentation.

[7] Yulaw1011 (2022), Elasticsearch, Kibana, Logstash: Overview, Installation and Usage, Viblo.

[8] Ifeanyi Onyia Odike (2022), Responding to Network Attacks with Suricata and WAZUH XDR, WAZUH Blog.

[9] WAZUH Team (2023), Detecting Web Attacks: Shellshock, Official Documentation.

[10] Red Canary Team (2023), Invoke-AtomicRedTeam Wiki, GitHub Wiki.

[11] Microsoft Team (2024), Sysmon v15.15 - Download and Documentation.

[12] WAZUH Team (2023), Detect and Remove Malware with VirusTotal Integration, Official Documentation.