

# **Log-Based End Point Security Solution**

**Submitted by**

- 1. Name: Md. Asgor Ali  
ID: ECSE 190101016**
- 2. Name: Md. Abdul Kader  
ID: ECSE 190301213**
- 3. Name: Abdullah Al Mamun  
ID: ECSE 190101044**
- 4. Name: Sajib Chandra Adhikari  
ID: ECSE 190301198**

**A Project Report Submitted in Partial Fulfillment of the Requirements for the  
Degree of Bachelor of Science in Computer Science & Engineering**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
NORTHERN UNIVERSITY BANGLADESH**

**July 2023**

# APPROVAL

The Project Report “**Log-Based End Point Security Solution**” submitted by Mr. **Md. Asgor Ali** (ID:ECSE190101016), Mr. **Md. Abdul Kader** (ID:ECSE190301213), Mr. **Abdullah Al Mamun** (ID:ECSE190101044) and Mr. **Sajib Chandra Adhikari** (ID:ECSE 190301198) to the Department of Computer Science and Engineering, Northern University Bangladesh, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents.

## Board of Examiners

- |  |              |
|--|--------------|
| 1. <b>Sumya Akter</b><br>(Lecturer)          | (Supervisor) |
| 2. <b>Rumman Ahmed Prodhan</b><br>(Lecturer) | (Examiner)   |
| 3. <b>Simon Bin Akter</b><br>(Lecturer)      | (Examiner)   |

-----  
**Md. Raihan Ul Masood**  
**Associate Professor and Head**  
**Department of Computer Science and Engineering**  
**Northern University Bangladesh**

# DECLARATION

We, here by, declare that the work presented in this Project report is the outcome of the investigation performed by us under the supervision of **Sumya Akter** (Lecturer) Department of Computer Science and Engineering at Northern University Bangladesh. We also declare that no part of this Project has been or is being submitted elsewhere for the award of any degree.

## Signature

.....  
**Name: Md. Asgor Ali**  
**ID: ECSE 190101016**

.....  
**Name: Md. Abdul Kader**  
**ID: ECSE 190301213**

.....  
**Name: Abdullah Al Mamun**  
**ID: ECSE 190101044**

.....  
**Name: Sajib Chandra Adhikari**  
**ID: ECSE 190301198**

# ACKNOWLEDGEMENTS

First of all, we would like to thank the Almighty ALLAH. Today we are successful in completing our work with such ease because He gave us the ability, chance, and a cooperating supervisor.

We are indebted to a number of individuals in academic circles as well as in university faculties who have contributed to prepare the book. Their contributions are important in so many different ways that we find it difficult to acknowledge them in any other manner but alphabetically. In particular, we wish to extend our appreciation to our respected supervisor **Sumya Akter (Lecturer)** Department of Computer Science & Engineering, **Northern University Bangladesh**, our honorable Coordinator, Faculty of Science and other respected faculties of Science Faculty **Northern University Bangladesh**, for their valuable suggestions on preparing and improving the presentation and the book. Again we would like to give thanks to our honorable supervisor **Sumya Akter** for his commitment to excellence in all aspects of the production of this book and completion of the work.

Last, of all, we are grateful to our family members; who are, always with us in over step of life.

# **Abstract**

Endpoint Solution, It's an integrated security solution that capable to collecting and monitoring real-time log data from registered agent and provide automated response different type of security event. A log is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system. Basically it's taking the decision according to the system log file that's why it's called log based Endpoint security solution. Log based End Point system collect log data of every event which has been generated by host machines and gather comprehensive amount log of data across enter endpoint or host infrastructure to make them accessible from the security operation team. In the modern era, thousands of malicious activities participate in daily networking tasks. A traditional firewall is unable to detect these kinds of activities because they work on their integrated certificate. On the other hand, End Point security system monitors users' activity and generates different-level alerts. If any user uses their credential for successful login around hundred times and suddenly there are few failed attempts, then Endpoint security detects it as abnormal behavior and sends an alert with a self-defined threat level. Generally, the End Point security solution is expensive. Where a paid version is cost minimum approximately \$2595 to \$4585 per month. On the other hand, in this study, few open-source tools were employed to design this End Point security system which makes it available at free of cost. Besides, it is capable to detect and mitigate malicious activities like attempt of brute force attack, malware attack, shellshock and ransomware attack by collecting event data, log, detecting vulnerability, file integrity and configuration assessment, provide system inventory that collect summary of ruing system.

# LIST OF ABBREVIATIONS

**EDR**- Endpoint Detection & Response

**SOC**- Security Operation Center

**IT**- Information Technology

**ATT&CK**- MITRE Adversarial Tactics Techniques and Common Knowledge

**MTTD**- Mean Time to Detect or Discover

**MTTR**- Mean Time to Recovery or Mean Time to Restore

**AR**- Active Response

**GUI**- Graphical User Interface

**CLI**- Command Line Interface

**IOC**- Indicator of Compromise

**IDS**- Intrusion Detection System

**IPS**- Intrusion Prevention System

**API**- Application Programming Interface

**CVE**- Common Vulnerabilities and Exposures

**FIM**- File Integrity Monitoring

**NVD**- National Vulnerability Database

**SCA**- Security Configuration Assessment 23

**PCI DSS**- Payment Card Industry Data Security Standard

**GDPR**- General Data Protection Regulation.

**NIST**- National Institute of Standards and Technology

**GPG13**- Good Practice Guide 13

**TSC SOC2**- Trust Services Criteria SOC2

**HIPAA**- Health Insurance Portability and Accountability Act

**SIEM**- Security Information and Event Management

# **TABLE OF CONTENTS**

<b>CONTENTS</b>	<b>PAGE</b>
Approval	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
List of Abbreviations	vi

## **CHAPTER**

<b>Chapter I</b>	<b>1-3</b>
<b>1 Introduction</b>	<b>1</b>
<b>1.1 Problem Statement</b>	<b>1</b>
<b>1.2 Motivation</b>	<b>1</b>
<b>1.3 Objective</b>	<b>2</b>
<b>1.4 Assumptions and Limitations</b>	<b>2</b>
<b>1.5 Project Outline</b>	<b>3</b>
<b>Chapter II</b>	<b>4-4</b>
<b>2 Literature Review</b>	<b>4</b>
<b>Chapter III</b>	<b>5-10</b>
<b>3 Proposed Architecture</b>	<b>5</b>
<b>3.1 Data Flow</b>	<b>6</b>
<b>3.2 OSSEC</b>	<b>6</b>
<b>3.3 Elasticsearch</b>	<b>7</b>

<b>3.4 Kibana</b>	<b>7</b>
<b>3.5 File Beate</b>	<b>7</b>
<b>3.6 Wazuh Server</b>	<b>7</b>
<b>3.7 Wazuh Agent</b>	<b>8</b>
<b>3.8 Cost and Time Estimation</b>	<b>9</b>
<b>3.9 Simple Comparison</b>	<b>10</b>
 <b>Chapter IV</b>	 <b>11-20</b>
<b>4. Implementation Methodology</b>	<b>11</b>
<b>4.1 Making Virtual Platform</b>	<b>11</b>
<b>4.2 Wazuh Installation</b>	<b>12</b>
<b>4.3 Elastic Search Installation</b>	<b>13</b>
<b>4.4 Kibana Installation</b>	<b>15</b>
<b>4.5 Filebate Installation</b>	<b>15</b>
<b>4.6 Agent Installation</b>	<b>17</b>
<b>4.7 Installing SI feed Integrations</b>	<b>19</b>
 <b>Chapter V</b>	 <b>21-40</b>
<b>5. Chapter Overview</b>	<b>21</b>
<b>5.1 Log Data Analysis</b>	<b>21</b>
<b>5.2 Security Analytic</b>	<b>22</b>
<b>5.3 File Interiority Monitoring</b>	<b>22</b>
<b>5.4 Vulnerability Detection</b>	<b>23</b>
<b>5.5 Security Configuration Assessments</b>	<b>24</b>
<b>5.6 System Inventory</b>	<b>25</b>
<b>5.7 MITRE ATT&amp;CK</b>	<b>26</b>



<b>5.8 Regulatory Compliance</b>	<b>27</b>
<b>5.9 Mitigate of Ransomware</b>	<b>27</b>
<b>5.10 Mitigate Shellshock</b>	<b>30</b>
<b>5.11 Active Response (AR) Against shellshock</b>	<b>32</b>
<b>5.12 Packet Analysis during Shellshock</b>	<b>33</b>
<b>5.13 Mitigate of Brut Force Attack</b>	<b>34</b>
<b>5.14 Active Response (AR) Against Brut Force Attack</b>	<b>36</b>
<b>5.15 Packet Analysis during Brut Force Attack</b>	<b>37</b>
<b>5.16 Malware Detection</b>	<b>37</b>
<b>5.17 Remove Malware with Active Response</b>	<b>40</b>
 <b>Chapter Vi</b>	 <b>41-41</b>
<b>Conclusion</b>	<b>41</b>
<b>Future Work</b>	<b>41</b>
 <b>Reference</b>	 <b>42-43</b>
 <b>Appendix - Complex Engineering</b>	 <b>44-45</b>
<b>Complex Engineering Problem (Ps):</b>	<b>44</b>

# Chapter I

## 1. Introduction:

End Point security system is a set of capabilities that allow for continuous monitoring and analysis of endpoint activity to identify and respond to advanced threats in real time. A central database that stores information on suspicious activities and events that occurs at the endpoint is used to extract valuable insights for threat response. End Point security solutions use forensic tools and analytic to use forensic tools and analytics to further investigate suspicious activities stored in the database including web processes and unrecognized connections. The volume of activity and more. End point security tools use this information to; Identify Threat patterns, create alerts, and generate reports IT security professionals can also use analytics and report from End Point security software to investigate past breeches and gain a better understanding of how malware and other exploits reach their network and centralized platform. End-point security tools go beyond detecting suspicious activity and automatically respond to threats as they arise.

### 1.1 Problem Statement:

Every enterprise regardless of size has what we call digital parameters compromised of all the devices or endpoints, which connect to our enterprise IT network and their cyber security protections. Laptop and desktop computers and as well as mobile and IoT devices all are included under the endpoint device. According to Global digital population as of April 2022 [1], A total of 5 billion people around the world use the internet today – equivalent to 63% of the world's total population [2] According to Techjury report 2022 regular in an average Globally, 30,000 websites are hacked daily. 64% of companies worldwide have experienced at least one form of cyber-attack. There were 20M breached records in March 2021. An average of around 24,000 malicious mobile apps are blocked daily on the internet. [3] According to 51% of cyber-attack Occur by compromising the endpoint or end user. To solve this many well-known tech giant companies like Cisco, Palo Alto, Fortinet, Sophos, TrendMicro, Symantec etc. are providing different types of EDR with attractive features. But many enterprise companies are not adopting that due to their budget shortage. In this paper, we are trying to implement an open-source endpoint detection and response system to mitigate uncovered cyber threats.

### 1.2 Motivation:

As we all know, cybersecurity is a critical issue in today's digital world. With the increasing reliance on technology, it is imperative that we have strong security measures in place to protect our sensitive information and prevent cyber-attacks. This is what motivated me to undertake this project. We were driven by our passion for cybersecurity and our desire to make a difference in the world by helping to protect it from the growing threat of cybercrime. We believed that through this project, we could contribute to the larger goal of creating a safer and more secure digital environment. During the project, we faced numerous challenges and obstacles, but we were determined to succeed. We put in countless hours of hard work and dedicated ourselves fully to the project. And we are proud to say that we were able to deliver a successful endpoint detection and response solution. Through this project, we learned invaluable lessons about the importance of persistence, teamwork, and dedication. We also gained a deeper

understanding of the complexities of cybersecurity and the critical role it plays in our lives. In conclusion, we are grateful for the opportunity to undertake this project and for the support of my team and mentor. We hope that my work will inspire others to pursue their passions and make a positive impact in the world.

### 1.3 Objective:

Regularly thousands of malicious activities are occurring along with the IT infrastructure. A major portion of those malicious actions remains uncovered. Due to the rising of cybercriminals, most organizations are going for End Point security protection solutions like EDR. Different type of End Point security solution available is market McAfee Symantec endpoint security CrowdStrike falcon sentinel 1 f-secure Cisco secure AMP and Palo Alto networks and many more. They have different type of interactive feature but there is some common feature that exists in all the EDR solution like different type of attack [brute force, DDoS, shellshock, MITM etc] and they can protect the system from different type of malware ransomware, virus, blacklisted IP address. End point security solution will depend on your company's size and existing security infrastructure. In this paper, we address the problem to protect the Endpoint of the enterprise network, unauthorized access from the bad guy a preventing different types of cyber-attack. The main contributions of this paper are as follows:

- Deployment of an open source **Endpoint Security Solution**. The proposed system adopts the **Wazuh** engine that is capable of Security Analytics, Intrusion Detection, Log Data Analysis, File Integrity Monitoring, Vulnerability Detection, Incident Response and figuration Assessment etc.
- Collecting feed from different security intelligence sources and integration with Wazuh the engine system and configuring proper rules to collect actual security analytic output.
- Comply with the endpoint to assessment configuration with a different regulatory commission like HIPPA, GDPR, NIST etc.

### 1.4 Assumptions and Limitations:

A centralized and efficient methodology for detecting malicious activity on the entire infrastructure has been developing, it has Assumptions and Limitations that should be investigated further. For instance –

- The new next-generation Endpoint security system has an interactive feature in terms of compatibility storage, virtualization and performance, as well as the ability to modernize the response process by selecting and deploying remedial action current response systems, are severely limited, and migration strategies and selected and implemented without a thorough impact analysis of attack and response circumstance.
- Furthermore, most Endpoint security system allow for the installation of a few new connectors to gather security events and log data, as well as the use of API to obtain events at a later time. Future Endpoint security system mast me take advantage of this feature to improve the quality of event logs delivered to the system. And provide fresh graphical representation by collecting logs from the Endpoint security system data repository via connectors.

- All of the procedures and performance analyses were completed in the lab environment, nevertheless, there may be issues when executing in a practical setting.

## 1.5 Project Outline:

The remainder of the report is organized as follows: In **Chapter II** a literature study on related work is given including definitions and explanations for the most impotent terms used in the paper basic concept and architecture of Endpoint Security System, Essentials Capability, Research Gap on Enterprise and Open Source Endpoint Security system has been discussed through this chapter. **Chapter III** introduces system models including the system architecture of OSSEC, Wazuh Server, Agent, Elastic Stack and the Working procedure of the entire Solution, Time and cost estimation. **Chapter IV** explains the details of the Virtual Platform setup with the details installation process of OSSEC, Wazuh Engine, Agent, and Elastic Stack. **Chapter V** discusses the performance and capabilities of components like Log Data Analysis, Security Analytics, File interiority Monitoring (FIM), Vulnerability Detection, Security Configuration assessment (SCA), System inventory., MITRE ATT&CK, and Regularity Commission. In **Chapter VI** the migration approach for different types of attacks such as shellshock, brute force, and Malware attacks are discussed Finally, future work and conclusion. In the **Appendix-** we will explain the CEP mapping of this project.

## Chapter II

### 2. Literature Review:

In the field of Endpoint security systems, a significant amount of work has been done. An overview of recent contributions is presented here, with an emphasis on detecting vulnerabilities, data logs, security events, Security configuration assessments, and devices' ability to check and meet IT compliance requirements. Endpoint security system technology is a complete tool that components that operate independently must work together. Endpoint security system systems include a variety of components. Most academic and security special side that vendors or manufacturers should agree on the structure and syntax of security event records to make the correlation process easier and to provide a trustworthy automated event analysis.

For example, in reaction to illegal activity, the authors of (Lakbbi et al 2014) recommend using the standard protocol IF-MAP to transmit real-time security events between the server and security device. [4] For the most common use cases, enterprise Endpoint security system systems include better administration of configuration deployment and correlation configuration filter and prebuilt visualization. They allow businesses to keep track of larger-scale data centre activity and administrate and configure security-related apps from a central location. [5] Perhaps most crucially, only enterprise Endpoint security system products now offer next-generation Endpoint security system features. Next-generation enterprise Endpoint security system include two new technologies which can save time, and enhance incident detection capability and response significantly. [6] The log format has a challenge in the Endpoint security system business because each program (or source device) does have its own log file format, which impacts the integrity of the analysis and resilience of the correlation engine. [7] When it comes to open-source solutions, rest confident that both LEM and Threat.

The monitor is built to go much beyond these essential functions while providing actionable insights and an intuitive, easy-to-use interface. [8] Organized ions can utilize open source Endpoint security system technologies to save money on software licenses and to test particular capabilities before investing in new products.

Open source Endpoint security system systems offer basic capabilities that might meet the demands of smaller businesses that are just getting started with logging and analyzing security event data. [9] Recent regulatory changes, such as PC-DSS and the European Union's GDPR, have made it critical to extract device and application log events from individual servers or virtual machines and securely store them for analysis and action. Organizations might 6 be investigating and comparing open source Endpoint security system technologies like Nagios Core or Alienvanlt OSSIM if they're not sacking an enterprise-level Endpoint security system. These solutions are ideal for testing finding out what is truly needed to monitor and track, and taking action when questionable behavior is detected. Also due to the huge amounts of data, open-source Endpoint security system often do not offer or manage storage, which is a sensitive problem. [9] Endpoint security system solutions were designed to assist administrators by creating security policies and managing events tromp a variety of sources. A simple EDR is made from dis-tact paces (e.g. source device, log collect ions, parsing normalization, rule engine log storage, and real-time tracking) that can work individually, but the Endpoint security system will not operate effectively if they don't all work together. [10] Endpoint security system platforms analyze security events generated by network devices and applications in real-time. Furthermore, current response systems identify and deploy protective measures without performing a comprehensive impact analysis of attacks and response contexts, although the fact that the new generation of Endpoint security system provides response capabilities to automate the selection process and deploy mitigation strategies. [11]

## Chapter III

### 3. Proposed Architecture:

In Basic terms, Open Source refers to the whole source code of any application that is licensed under an open-source license. That is useful in learning the application and making changes based on the organization. Besides, an Open Source Endpoint Solution indicates that the entire Endpoint security solution's source code is open to the public. These technologies are free to use and business may avoid the high costs associated with most commercial EDR systems though they still gain almost the same accessibility to their infrastructure. While free EDR products don't have the same degree of capabilities as enterprise-level solutions. Open Source EDR does provide solid capabilities at a low cost. Significantly the content that these free EDR tools use and preserve is unrestricted. Small and Medium size organizations find it enticing because of this.

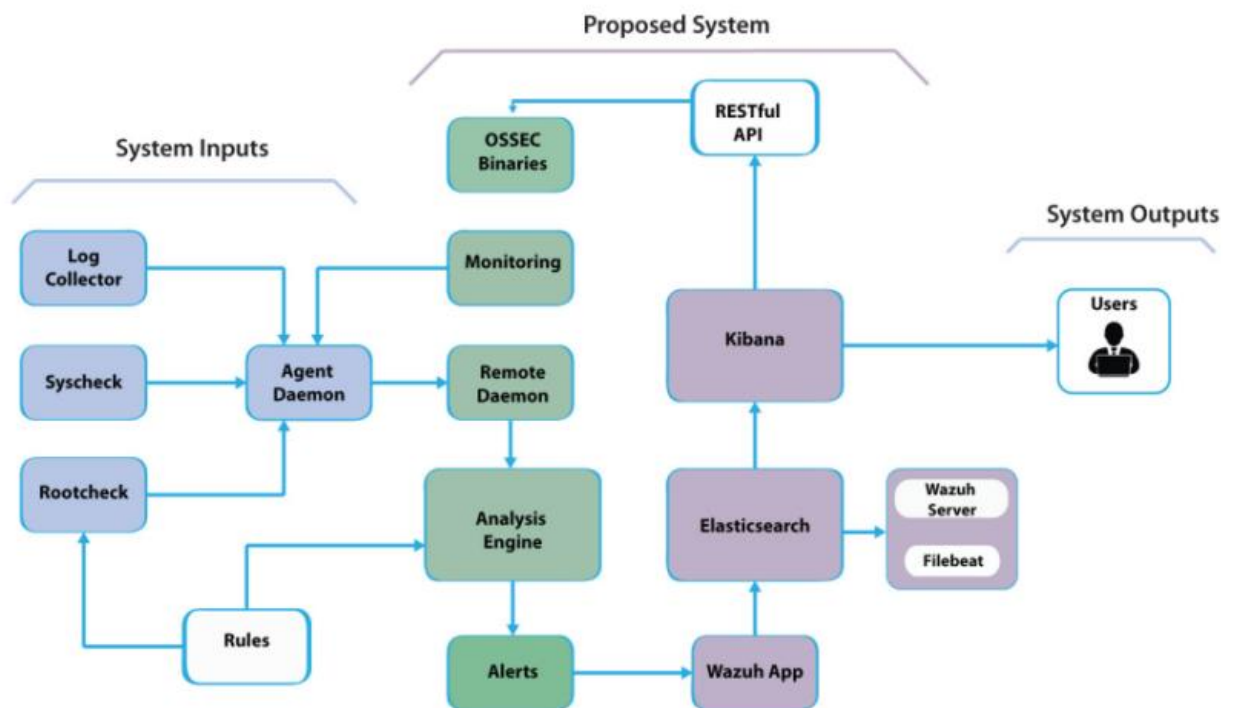


Figure 3.1: Proposed Architectural Diagram

(EDR), OSSEC HIDS with Wazuh manager server and Elastic stack which is a collection of Open Source log management technologies that includes Elasticsearch, Kibana, Filebeat and others.

### 3.1 Data Flow:

Figure 3.2 shows the data flow diagram of this EDR.

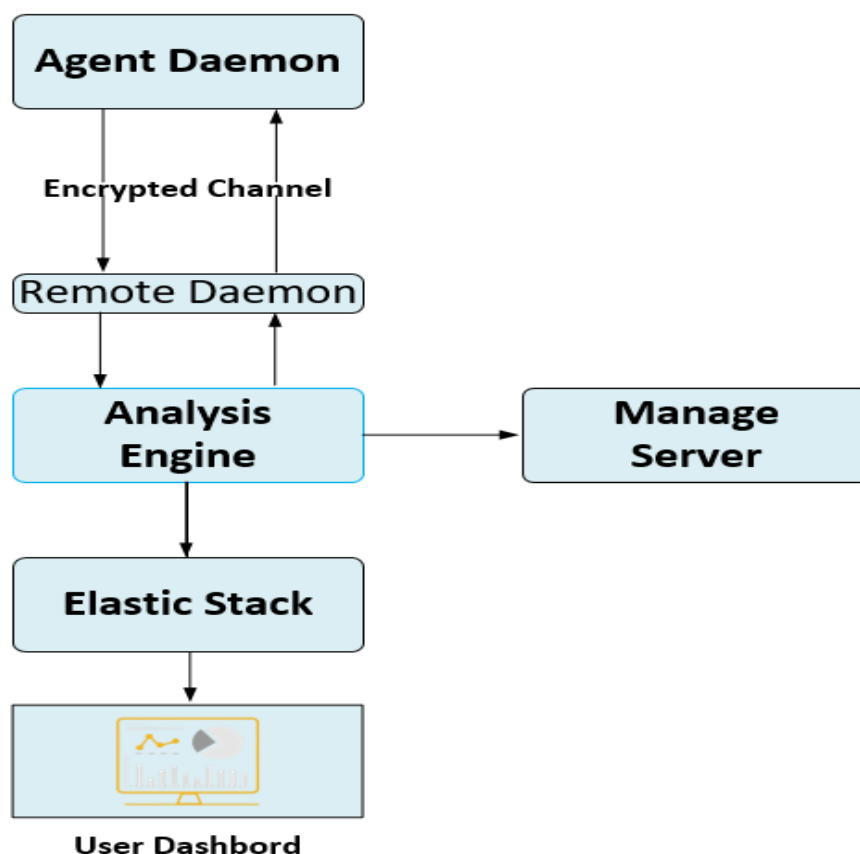


Figure 3.2: Data Flow Diagram

### 3.2 OSSEC:

OSSEC is among the most widely used host-based intrusion detection system (IDS) for Linux, windows, MACOS, Solaris, OpenBSD and FreeBSD. The host agent (which collects logs) and the primary OSSEC program (which evaluates all log details) are the major components of **OSSEC**. It also has a deprecated GUI but other Open Source solutions perform a better job at data visualization. the organization should utilize other solutions instead. Examples of such tools include **Kibana** and **Grafana**. The amount of characteristics on the host is directly monitored and logged by OSSEC. Log files, file integrity, malware detection and windows registry monitoring are an example. Other services that OSSEC may analyze logs from including the most prominent Open Source FTP, mail, DNS, Database, WEB, firewall and network-based IDS solutions. logs from a variety of enterprise services and security solutions can also be analyzed by OSSEC. It's questionable if OSSEC can be considered an "all-in-one" EDR system. OSSEC does the heavy work of setting up an EDR system .it collects data and analyses it. But it lacks some of the essential log management and analysis features. Other HIDS systems (e.g. Wazuh) have forked the OSSEC project, expanding its capabilities and making it a fuller EDR choice.

Wazuh started as a derivative of OSSEC, one of the most widely used Open Source EDRs. With additional features bug patches and more streamlined architecture, it has evolved into its distinct solution. Wazuh is based on the Elastic stack (Elastic-search, Filebeat and kibana) and can handle both agent-based and Syslog consumption. This makes it useful for monitoring devices like network devices and printers that create logs but don't support a full agent. Wazuh supports current OSSEC

agents and even offers a transition guide for moving from OSSEC to Wazuh because the two share a common code base. Wazuh is seen as an advancement of OSSEC due to the integration of a new web UI, REST API, more complete rule set and many other advancements.

### **3.3 Elasticsearch:**

It is a lightweight log forwarder that sends logs across a network to Elasticsearch. It is used to send events and alerts to Elasticsearch from the server. It reads the Wazuh analyzing engine's output and sends it in real time via an encrypted tunnel. When connected to a multi-node Elasticsearch cluster. It also enables load balancing.

### **3.4 Kibana:**

Kibana is a flexible and user-friendly online interface for data mining, analysis and visualization. It is built on top of an Elasticsearch cluster that indexes content. Wazuh's web UI has been fully integrated into Kibana as a plugin. It comes with dashboards for security events, regulatory compliance (e.g, PCI DSS, GDPR, CIS, HIPAA and NIST 800-53), discovered vulnerable applications, FIM data, SCA findings, cloud infrastructure monitoring events and more. Wazuh interfaces with Elastic Stack to provide a real-time web console for alarm and log data analysis, as well as a feed of already decoded log messages to be indexed by Elasticsearch. In addition, the Wazuh GUI running on top of kibana can be used for the management and monitoring of your Wazuh infrastructure. An Elasticsearch index is a set of documents that are comparable in some way (like certain common fields and shared data retention requirements. Wazuh stores distinct event kinds in up to three different indices, which are created daily. **wazuh-alerts:** The Wazuh server generates notifications, which are stored in this index. These are formed each time an event triggers a high priority rule (this threshold is configurable). **wazuh events:** All events (archive data) generated from the agents are indexes, regardless of whether they trip a rule. **wazuh-monitoring:** Data about the Wazuh agent's status over time is indexed in this. The web interface uses it to show whether or not particular agents are active. Disconnected, or Never connected. A document index is made of documents. Individual alerts, archived events and status events are examples of documents in the index value above. Elasticsearch indexes are split into one or more shards, with each shard having one or more replicas. Each Lucene index is unique for each primary and replica shard. As a result, an Elasticsearch index consists of several Lucene indexes. when users search the Elasticsearch index, it runs in parallel on shards and the results are blends. In multiple-node Elasticsearch clusters, dividing Elasticsearch indexes into several shards and replicas is used to scale out searches and ensure high availability. Elastic-search single-node clusters typically contain only one shard per index and no replication.

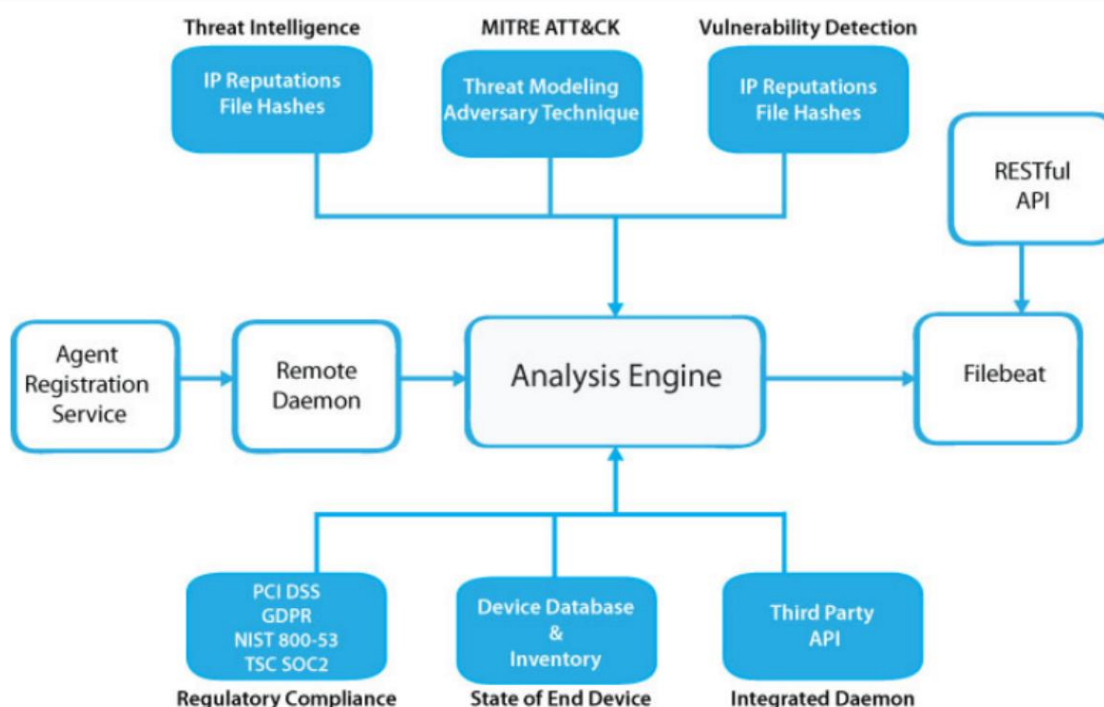
### **3.5 File Beate:**

It is a lightweight log forwarder that sends logs across a network to Elasticsearch. It is used to send events and alerts to Elasticsearch from the server. It reads the Wazuh analyzing engine's output and sends events in real-time via an encrypted tunnel. When connected to a multi-node Elasticsearch cluster, it also enables load balancing [14]

### **3.6 Wazuh Server:**

The Wazuh server is separated into three pieces. The Wazuh manager manages the Wazuh server where all the Endpoint security action takes place. When an event satisfies a rule (e.g. intrusion detected, file modified, a configuration not complying with policy, probable rootkit, etc.), the server component analyzes the collected data from the agents and triggers alarms. The server, which is commonly a stand-alone physical. system, virtual machine, or cloud instance, executes agent components to monitor itself. [15]





**Figure 3.3: Component of Manager Service**

Here following are the list of the most fundamental server components

**Registration service:** This service generates and distributes pre-shared keys that are unique to each agent in order to register new agents. This program operates as a communication network and uses TLS/SSL for authentication, as well as a fixed password.

**Remote daemon service:** The service that receives data from the agents is known as the remote daemon service. The pre-shared keys are used to verify each agent's identification and encrypt communications between the agent and the management.

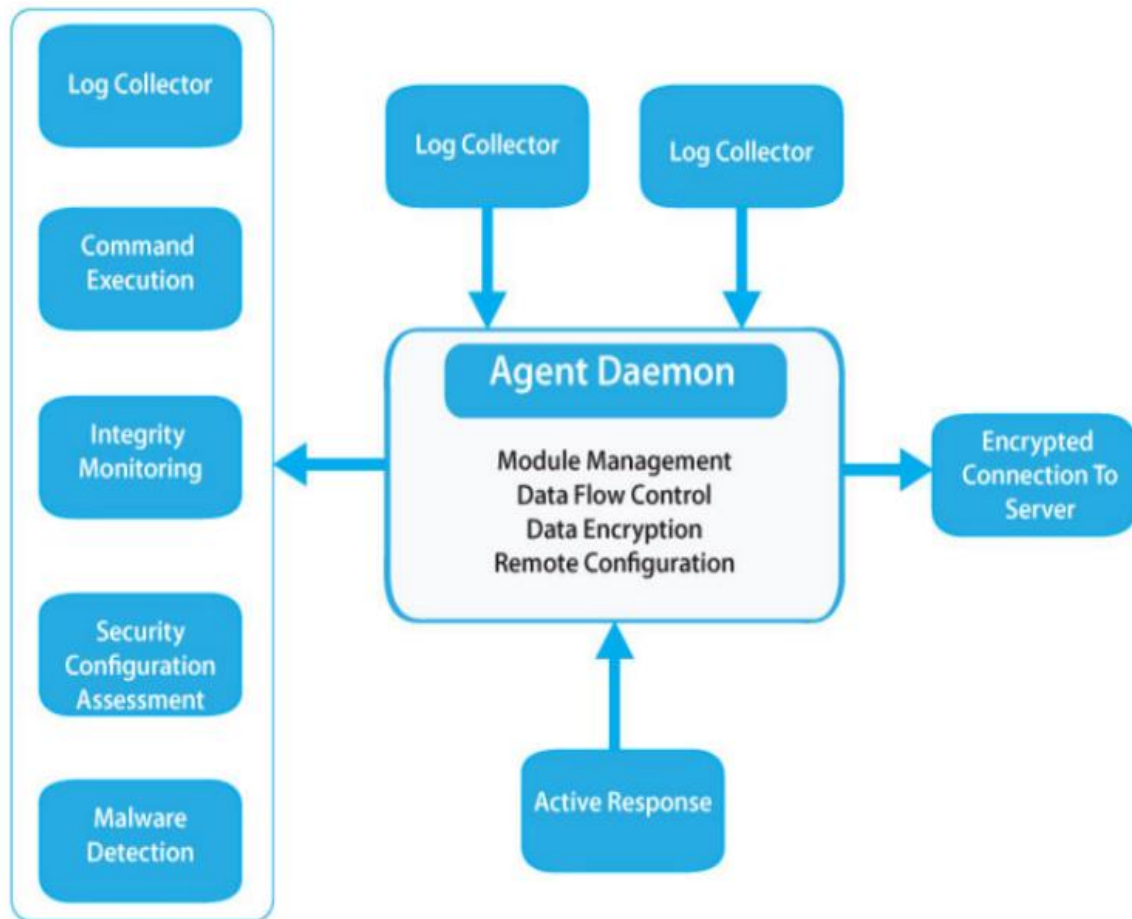
**Analysis daemon:** The process that does data analysis is known as the analysis daemon. It employs decoders to determine the type of data being processed (for example, Windows events, SSHD logs, web server logs, and so on) and then extracts appropriate data items from the log messages (e.g. source IP, event id, user, etc.). Then, using rules, it may spot specific patterns in decoded log records, triggering alert and possibly even triggering automated responses such as a firewall IP ban.

**RESTful API:** This interface helps to manage and track the status of agents' configuration and deployment. The Wazuh web interface, which is a Kibana app, also uses it. All log analyses are performed on the Wazuh manager server, after which they are sorted into the various attack and log fields, and then filtered and segregated logs are then saved in Elastic search indexes. [16] [17]

### 3.7 Wazuh Agent:

The Wazuh agent is built on a modular design, with separate components handling diverse duties such as file system monitoring, log message, reading, inventory data collection, system configuration scanning, malware detection, and so on. Configuration settings allow users to enable or disable agent's modules, allowing them to tailor the solution to their own needs.

The architecture and components of the agent are depicted in the diagram below:



**Figure 3.4: Wazuh Agent diagram**

### 3.8 Cost and Time Estimation:

Initially, we choose a Linux server to deploy our real-time system. Thus, we have to rent a Virtual private server for a faster processor and memory. which will cost 3,995/- BDT per month, we have rented it for 4 months so the total rent will be  $3,995 * 4 = 15,980$ /- BDT.

On the other hand, we need some client machines for that purpose and have rented another VPS that was 2,630 BDT we have rented it for 4 months so the total rent will be  $2,630 * 4 = 10,520$  /-BDT.

So, the total cost of our system development will be  $15,980 + 10,520 = 26,500$ /- BDT  
BDT Overview of time estimation for our proposed system is given in figure 7.1

Attribute	May-June (2022)	July-August (2022)	September-October (2022)	November-December (2022)	January-February (2023)
Literature Review					
Requirement Analysis & Tools Selection					
Server Environment Ready & Deployment					
Configuration & Performance Tuning					
Report Writing					

Figure 3.5: Overview of Time Estimation

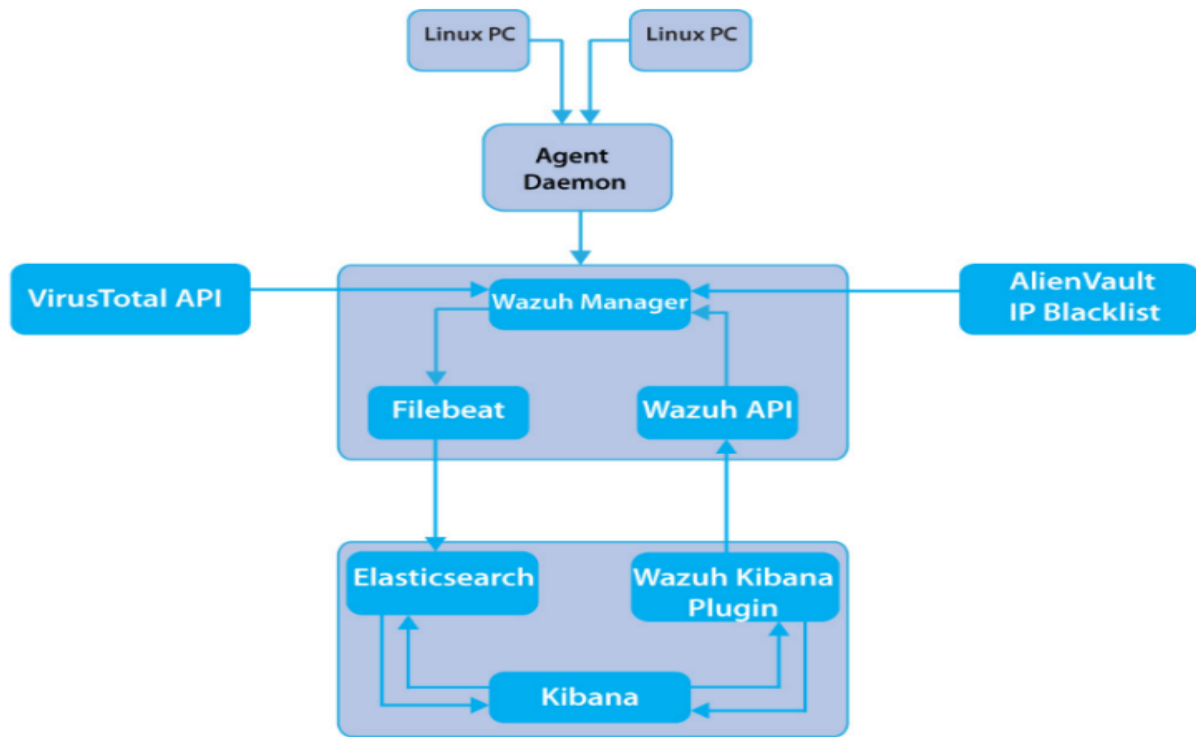
### 3.9 Simple Comparison:

Features	Cisco AMP	Sophos Intercept X	Symantec Endpoint Protection	Open source (Wazuh)
FIM	Yes	Yes	Yes	Yes
Vulnerability Scanning	Yes	Yes	Yes	Yes
Log data analysis	Yes	Yes	Yes	Yes
Compliance Check	NO	Yes	NO	Yes
Configuration Assessment	Yes	NO	Yes	Yes
System Inventory	Yes	Yes	Yes	Yes
Security intelligent Cloud	Yes	Yes	Yes	Yes
Malicious IP blocking	Yes	Yes	Yes	Yes
Unpatched program detection	Yes	Yes	Yes	Yes
RND support	Yes	Yes	Yes	NO
Source Code available	NO	NO	NO	Yes

## Chapter IV

### 4. Implementation Methodology:

This EDR architecture is built around agents that run on monitoring end devices and send security logs to a dedicated single server.



**Figure 4.1: Diagram Of Methodology**

Agentless devices (firewalls, switches, routers, access points and so on) are also supported and they can actively transmit log data via Syslog, SSH or their API. The information is decoded and analyzed by the central server, which then sends the results to an Elasticsearch cluster for indexing and storage. Figure 4.1 shows the diagram of the total methodology. In this section, the Elasticsearch basic license option from the Open Distro Project has been used, which contains everything in the Open-Source version under the Apache 2.0 license. In addition, some extra enterprise-grade features like Elastic stack security, Kibana alerting and more.

#### 4.1 Making Virtual Platform:

First of all, have to make the virtual platform ready. For virtualization VMware Workstation 16 pro and Ubuntu-20.04.4 live-server, amd64 as Wazuh manager server has been used. Ubuntu server 20.04 LTS (long-term support) provides enterprise-level stability, robustness and security. Canonical will support it as an LTS release until 2025. This is due to the UA-I subscriptions up to a ten-year security guarantee. Ubuntu server 20.4 comes with a five-year support period by default because it is an LTS release. The ESM service extends security updates for another five years, as a result, a very robust platform for both infrastructure and application deployment is created that is tailored to the demands of businesses. To use Ubuntu as the Manage server 4 core processors, 6 GB of Ram and 40 GB of storage have been used. Two network adapters are also used one with bridge mode to get IP from the router with DHCP which will allow the machine to go internet. And other custom V.M adapters to get a static IP of 10.1.1.x/24.

10.1.1.150 that has been used as manager server IP. The EDR manager server collects and analyzes data from the end devices that have been installed. The manager Wazuh API and Filebeat are all located there. Add the repository to the server to begin setting up Wazuh.

## 4.2 Wazuh Installation:

Now have to install the necessary packages, and then have to add the GPG key and the repository for installation.

```
root@manager:/home/user5# apt install curl apt-transport-http unzip wget  
libcap 2-bin software-properties-common lsb-release gnupg -y
```

```
root@manager:/home/user5# curl -s  
https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
```

```
root@manager:/home/user5# echo "deb  
https://packages.wazuh.com/4.x/apt/stable main" | tee-a  
/etc/apt/sources.list.d/wazuh.list deb  
https://packages.wazuh.com/4.x/apt/stable main
```

And then get the package information updated

```
root@manager:/home/user5# apt-get update -y
```

Now it's time to install Wazuh Manager

```
root@manager:/home/user5# apt-get install wazuh-manager -y  
root@manager:/home/user5# systemctl daemon-reload  
root@manager:/home/user5# systemctl enable wazuh-manager  
root@manager:/home/user5# systemctl start wazuh-manager
```

After that have to verify the status and the active status will appear

```
asgon@asgor:~$ systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-04 06:47:38 UTC; 4 months 27 days ago
     Tasks: 133 (limit: 9448)
    Memory: 4.0G
    CGroup: /system.slice/wazuh-manager.service
            └─879184 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
            └─879205 /var/ossec/bin/wazuh-integrator
            └─879227 /var/ossec/bin/wazuh-authd
            └─879242 /var/ossec/bin/wazuh-db
            └─879265 /var/ossec/bin/wazuh-execd
            └─879279 /var/ossec/bin/wazuh-analysisd
            └─879297 /var/ossec/bin/wazuh-syscheckd
            └─879314 /var/ossec/bin/wazuh-remoted
            └─879345 /var/ossec/bin/wazuh-logcollector
            └─879430 /var/ossec/bin/wazuh-monitord
            └─879479 /var/ossec/bin/wazuh-modulesd

Warning: journal has been rotated since unit was started, output may be incomplete.
asgon@asgor:~$
```

Figure 4.2: Status of Manager Service.

### 4.3 ElasticSearch Installation:

Wazuh manager installation is successfully done, now have to install Open Distro for Elasticsearch

```
root@manager:/home/user5# apt install elasticsearch-oss  
opendistroforelasticsearch -y
```

Then need to download the Elasticsearch configuration file of “elasticsearch.yml”. In order to use Wazuh kibana successfully need to create users and roles

```
root@manager:/home/user5# curl -so /etc/elasticsearch/elasticsearch.yml  
https://packages.wazuh.com/resource/4.2/open-distro/  
elasticsearch/7.x/elasticsearch.yml
```

```
root@manager:/home/user5# curl -so -  
/usr/share/elasticsearch/plugins/opendistro-  
security/securityconfig/roles.yml  
https://packages.wazuh.com/resource/4.2/open-  
distro/elasticsearch/role/roles.yml
```

```
root@manager:/home/user5# curl -so -  
/usr/share/elasticsearch/plugins/opendistro-  
security/securityconfig/roles-mapping.yml  
https://  
packages.wazuh.com/resources/4.2/open-distro/elasticsearch/role/roles-  
mapping.yml
```

```
root@manager:/home/user5# curl -so -  
/usr/share/elasticsearch/plugins/opendistro-  
security/securityconfig/internal-user.yml  
https://packages.wazuh.com/resources/4.2/open-  
distro/elasticsearch/role/internal-users.yml
```

These users and roles are intended to work in conjunction with the kibana plugin, however, they are password-protected and cannot be changed using the kibana interface. The “securityadmin” script must be run to change them or add new users or roles.

Now run the bash for wazuh-cert-tool.sh certificates –

```
root@manager:/home/user5# bash /wazuh-cert-tool.sh
```

and move the certificate to resemble directories-

```
root@manager:/home/user5# mkdir /etc/elasticsearch/certs/  
root@manager:/home/user5# mv ~/certs/elasticsearch*  
/etc/elasticsearch/certs/  
root@manager:/home/user5# mv ~/certs/admin* /etc/elasticsearch/certs/  
root@manager:/home/user5# cp ~/certs/root-ca* /etc/elasticsearch/certs
```

After enabling the Elasticsearch service active status appeared in the figure below

```
root@edrmanager: /home/asgor
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-03-21 17:34:36 UTC; 5 months 24 days ago
     Docs: https://www.elastic.co
    Main PID: 90443 (java)
      Tasks: 153 (limit: 9448)
     Memory: 1.8G
    CGroup: /system.slice/elasticsearch.service
           └─90443 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.t...

Warning: journal has been rotated since unit was started, output may be incomplete.
~
~
~
~
~
~
~
~
lines 1-11/11 (END)
```

**Figure 4.3: Elasticsearch Status**

To load the updated certificate information and activate the cluster, need to run the Elasticsearch “security admin” script. If goes well, the successful output will generate with the below command

```
root@manager:/home/user5#curl -XGET https://localhost:9200 -u admin:admin -k
```

```
root@edrmanager: /home/asgor
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor# curl -XGET https://localhost:9200 -u admin:admin -k
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "phQKimmNR6CrN_-f07M-wg",
  "version" : {
    "number" : "7.10.2",
    "build_flavor" : "oss",
    "build_type" : "deb",
    "build_hash" : "747e1cc71def077253878a59143c1f785afa92b9",
    "build_date" : "2021-01-13T00:42:12.435326Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@edrmanager:/home/asgor#
```

**Figure 4.4: Elasticsearch certificate Status**



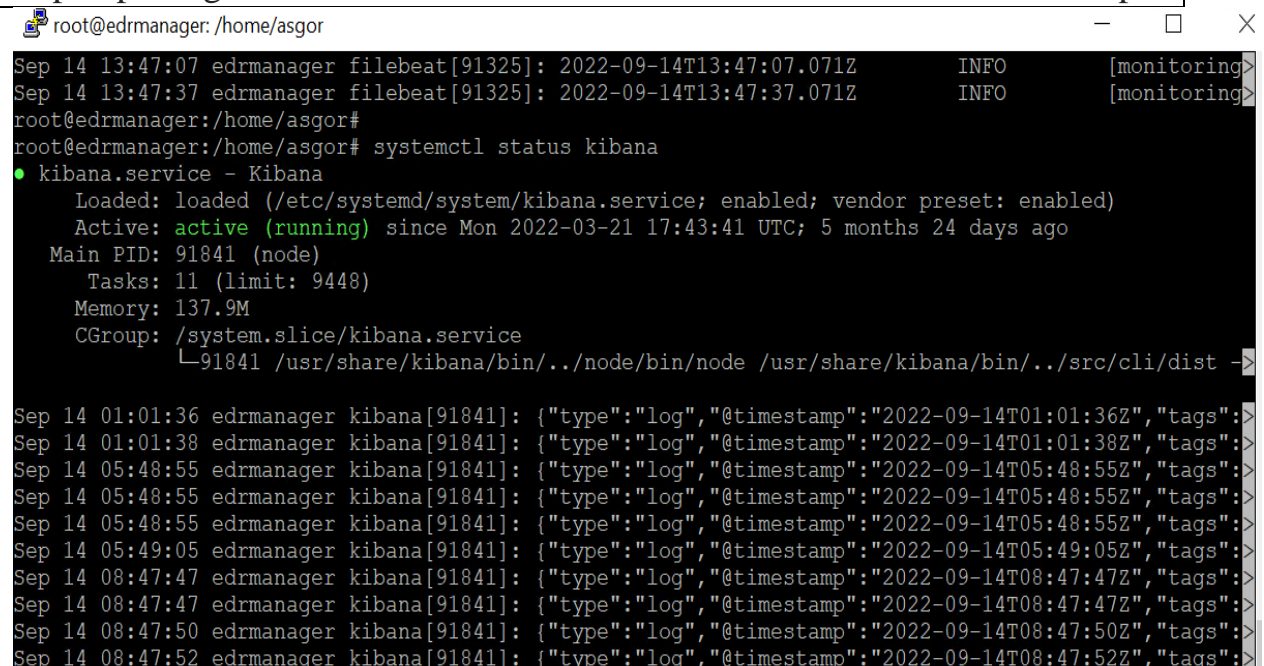
## 4.4 Kibana Installation:

kibana is a configurable and user-friendly web UI for mining, Visualizing Elastic-search events and archives. Now need to install the kibana package and download the kibana configuration file-

```
root@manager:/home/user5#apt-get install opendistroforelasticsearch-kibana
-y
root@manager:/home/user5#mkdir /usr/share/kibana/data
root@manager:/home/user5#chown -R kibana:kibana /usr/share/data
```

The parameter server host in the file is set to 0.0.0.0 it signifies that kibana is accessible from the outside and accepts all of the host's available IPs. If necessary, this value can be modified for a specific IP address. Wazuh kibana is a plugin for kibana. The plugin must be installed from the kibana home directory in the following manner:

```
root@manager:/usr/share/kibana#sudo -u kibana /usr/share/kibana/bin/kibana-plugin
install
https://package.rwazuh.com/4.x/ui/kibana/wazuh-kibana-4.2.5-7.10.2-1.zip
```



The screenshot shows a terminal window with the following content:

```
root@edrmanager:/home/asgor
Sep 14 13:47:07 edrmanager filebeat[91325]: 2022-09-14T13:47:07.071Z INFO [monitoring>
Sep 14 13:47:37 edrmanager filebeat[91325]: 2022-09-14T13:47:37.071Z INFO [monitoring>
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-03-21 17:43:41 UTC; 5 months 24 days ago
     Main PID: 91841 (node)
        Tasks: 11 (limit: 9448)
       Memory: 137.9M
      CGroup: /system.slice/kibana.service
              └─91841 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bin/./src/cli/dist ->
Sep 14 01:01:36 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T01:01:36Z","tags":>
Sep 14 01:01:38 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T01:01:38Z","tags":>
Sep 14 05:48:55 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T05:48:55Z","tags":>
Sep 14 05:48:55 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T05:48:55Z","tags":>
Sep 14 05:48:55 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T05:48:55Z","tags":>
Sep 14 05:49:05 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T05:49:05Z","tags":>
Sep 14 08:47:47 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T08:47:47Z","tags":>
Sep 14 08:47:47 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T08:47:47Z","tags":>
Sep 14 08:47:50 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T08:47:50Z","tags":>
Sep 14 08:47:52 edrmanager kibana[91841]: {"type":"log","@timestamp":"2022-09-14T08:47:52Z","tags":>
```

Figure 4.5: Kibana Status

## 4.5 Filebeat Installation:

Filebeat is a Wazuh server utility that sends alarms and archived events to Elasticsearch inside a secure manager.

```
root@manager:/home/user5# apt-get install filebeat -y
```

To forward Wazuh alerts to Elasticsearch, need to download the filebeat configuration file that comes pre-configured:

```
root@manager:/home/user5#curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/resource/4.2/open-distro/filebeat/7.x/filebeat-all-in-one.yml
```



Now have to download the Elasticsearch alerts template and the Wazuh module for Filebeat:

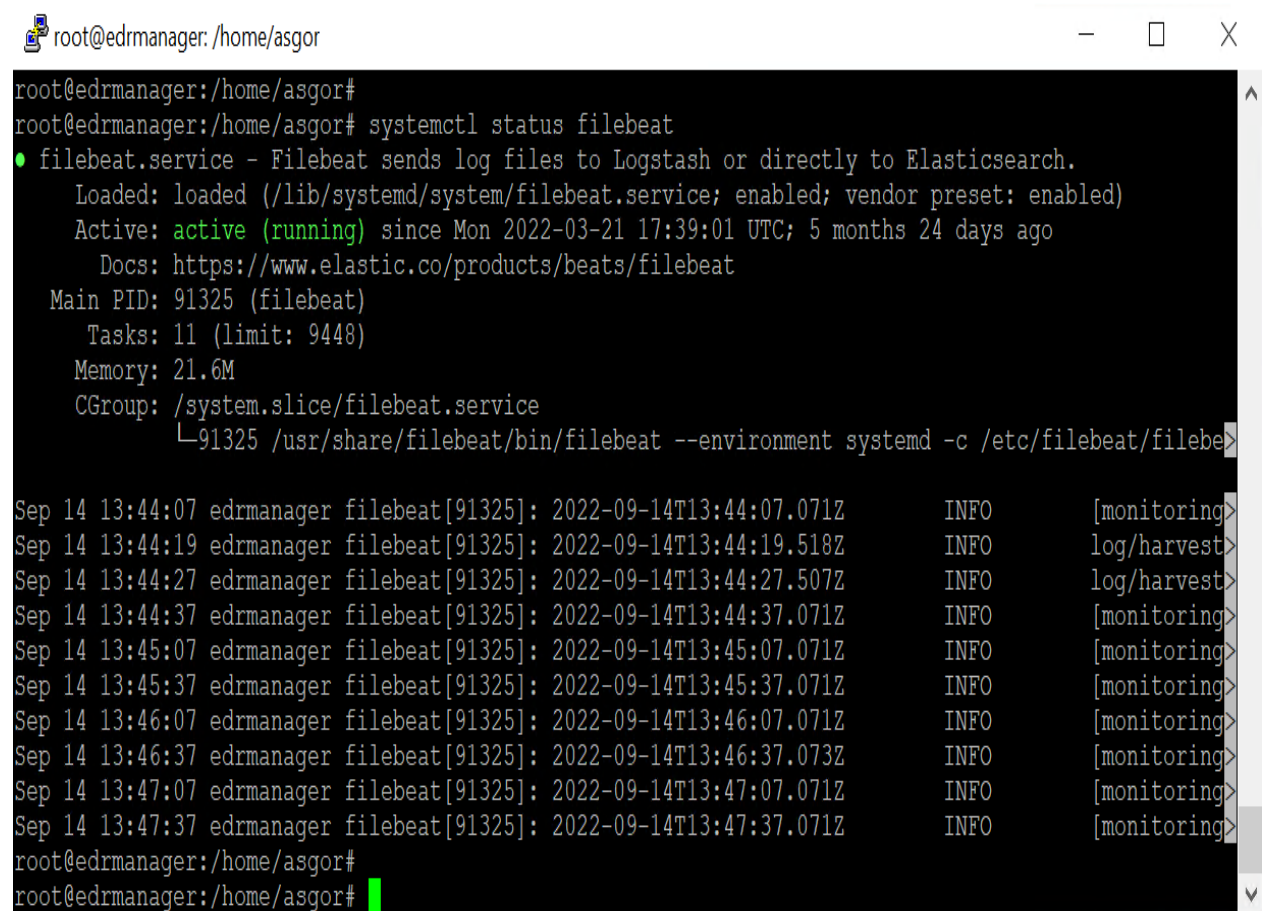
```
root@manager:/home/user5# curl -so /etc/filebeat/wazuh-template.json
http://raw.githubusercontent.com/wazuh/4.2/extension/elasticsearch/7.x/
wazuh-template.json
```

In /etc/filebeat/certs, copy the Elasticsearch certification .

```
root@manager:/home/user5# chmod go+ /etc/filebeat/wazuh-template.json
root@manager:/home/user5# curl -s
https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat -0.1.tar.gz | tar -
xuz-C /usr/share/filebeat/module
```

```
root@manager:/home/user5# mkdir /etc/filebeat/certs
root@manager:/home/user5# cp ~ certs/root-ca.pem /etc/filebeat/certs/
root@manager:/home/user5# mv ~ /certs/filebeat* /etc/filebeat/certs/
```

After enabling the service following active status appeared,



```
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor# systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-03-21 17:39:01 UTC; 5 months 24 days ago
     Docs: https://www.elastic.co/products/beats/filebeat
    Main PID: 91325 (filebeat)
      Tasks: 11 (limit: 9448)
     Memory: 21.6M
    CGroup: /system.slice/filebeat.service
            └─91325 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebe>

Sep 14 13:44:07 edrmanager filebeat[91325]: 2022-09-14T13:44:07.071Z      INFO      [monitoring>
Sep 14 13:44:19 edrmanager filebeat[91325]: 2022-09-14T13:44:19.518Z      INFO      log/harvest>
Sep 14 13:44:27 edrmanager filebeat[91325]: 2022-09-14T13:44:27.507Z      INFO      log/harvest>
Sep 14 13:44:37 edrmanager filebeat[91325]: 2022-09-14T13:44:37.071Z      INFO      [monitoring>
Sep 14 13:45:07 edrmanager filebeat[91325]: 2022-09-14T13:45:07.071Z      INFO      [monitoring>
Sep 14 13:45:37 edrmanager filebeat[91325]: 2022-09-14T13:45:37.071Z      INFO      [monitoring>
Sep 14 13:46:07 edrmanager filebeat[91325]: 2022-09-14T13:46:07.071Z      INFO      [monitoring>
Sep 14 13:46:37 edrmanager filebeat[91325]: 2022-09-14T13:46:37.073Z      INFO      [monitoring>
Sep 14 13:47:07 edrmanager filebeat[91325]: 2022-09-14T13:47:07.071Z      INFO      [monitoring>
Sep 14 13:47:37 edrmanager filebeat[91325]: 2022-09-14T13:47:37.071Z      INFO      [monitoring>
root@edrmanager:/home/asgor#
root@edrmanager:/home/asgor#
```

Figure 4.6: Filebeat Status

Also, successful test output appeared as shown in figure 4.6

```
root@edrmanager: /home/asgor
root@edrmanager:/home/asgor# filebeat test output
elasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.10.2
root@edrmanager:/home/asgor#
```

**Figure 4.7: Filebeat Output**

## 4.6 Agent Installation:

The server's IP address 192.168.102.210 will lead to the login page if it types and hits the browser. It is a multi-platform agent that operates on the hosts, and the user is requested to monitor it. it communicates with the Wazuh manager over an encrypted and authenticated channel, sending data in real-time. The agent is created with the goal of monitoring a wide range of endpoints without affecting their functionality. As a result, it works with the majority of operating systems and only takes roughly 0.1 GB of RAM. WINDOWS 10 AND Ubuntu 20.04.4-live-server-amd64 has been used in this paper as an agent. on a Linux system deployment parameters are used to make the task of installing registering and configuring an agent easier.

To get the official packages to have to Install the GPG key and add the Wazuh repository:

```
root@user2:/home/user2#curl -s https://package.rwazuh.com/key/GPG-KEY-WAZUH | apt-key add-
root@user2:/home/user2#echo "deb https:// package.rwazuh.com/4.x/apt /stable main" | tree /etc/apt /source.list /wazuh.list
root@user2:/home/user2#WAZUH-MANAGER="10.1.1.150" apt-get install wazuh-agent
```

and after enabling the service of wazuh agent active status appeared

```

asgor@ubuntuagent: ~
asgor@ubuntuagent:~$ systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor pr
   Active: active (running) since Fri 2022-05-27 16:06:53 UTC; 3 months 18 day
   Tasks: 31 (limit: 4617)
   Memory: 949.3M
   CGroup: /system.slice/wazuh-agent.service
           └─2781736 /var/ossec/bin/wazuh-execd
             └─2781747 /var/ossec/bin/wazuh-agentd
               └─2781761 /var/ossec/bin/wazuh-syscheckd
                 └─2781775 /var/ossec/bin/wazuh-logcollector
                   └─2781793 /var/ossec/bin/wazuh-modulesd

Warning: journal has been rotated since unit was started, output may be incomple
asgor@ubuntuagent:~$ █

```

**Figure 4.8: Linux Agent status**

```

C:-1>$source=https://packages.wazuh.com/4.x/windows/wazuh-agent-4.2.5-1.msi
C:-1>$destination = 'c:-agent-4.2.5-1.msi'
C:-1>invoke-WebRequest-Uri $source -OutFile $destination
C:-1>agent-4.2.5-1.msi /q WAZUH-MANAGER="10.1.1.150" WAZUH
REGISTRATION -SERVER="10.1.1.150"

```

Now the running status appeared using "Get-service -Displayname"\*wazuh\*"

For Windows first, need to download the installer file to start installation-

```

C:-1>$source https://packages.wazuh.com/4.1/windows/wazuh-agent-4.2.5-1.msi
C:-1 $destination = c:-agent-4.2.5-1.msi'
C:-1>Invoke-WebRequest - Uri $source -Out File $destination
C:-1-agent-4.2.5-1.msi /q WAZUH-MANAGER="10.1.1.150" WAZUH
REGISTRATION-SERVER-"10.1.1.150"

```

Now the running status appeared using "Get-Service -displayname "\*wazuh\*"

```

Administrator: Windows PowerShell
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-Service -displayname "*Wazuh*"

Status      Name                DisplayName
-----
Running     WazuhSvc            Wazuh

PS C:\WINDOWS\system32> █

```

**Figure 4.9: Windows Agent Service Status**

## 4.7 Installing SI feed Integrations:

AlienVault collects dynamic data from global organizations via their Tap devices, uploads it to their EDR and analyzes it to generate an IP reputation. AlienVault has an IP Blacklist vault with tens of thousands of IP addresses. Here a Blacklist of IPs would be downloaded from Github with the following command.

```
root@manager:/home/user5#wget /usr/bin/curl https://raw.githubusercontent.com/firehole/blocklist-ipsets/master/alienvault-reputation.ipset | grep -v '#' | sed 's/'s/$/:/g' > /var/ossec/etc/lists/blacklist-alienvault
```

Now a rule needs to be made at /var/ossec/etc/ossec.conf so the EDR can be accepted this list



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

**Figure 4.10: Alient Vault Rule Set Configuration**

Then the permission needs to be taken to OSSEC with the below command. Normally default permission is taken by root. `root@manager:/home/user5/# ossec:ossec blacklist-alienvault`  
Now a cronjob will update that list daily from Github. With the below command, then will synchronize the list every 24hrs by automatically.

```
0 1 * * * /usr/bin/curl https://raw.githubusercontent.com/firehole/blocklist-ipsets/master/alienvault-reputation.ipset | grep -v '^#' | sed 's/'s/$/:/g' > /var/ossec/etc/lists/blacklist-alienvault.
```

A CDB list was added with the name of AlienVault. Now one can add their own choices IP by themselves

















Search...		
Key	Value	Actions
1.34.58.110		 
1.34.226.50		 
1.161.219.86		 
1.171.103.192		 
1.173.242.161		 
1.246.222.20		 
1.246.222.134		 
1.246.222.234		 
1.246.222.101		 

Figure 4.11: Alient Vault IP List

## Chapter V

### 5. Chapter Overview :

When EDR Manager Server and End Devices are ready. All these essential features become available. Here has more information about the components in detail. After a successful installation procedure, the proposed system is ready to use and has gained all of the essential EDR capabilities.

File Integrity has the capacity to identify even a single change of a file of the directory in real-time. Its security analysis ability allows organizations to discover intrusion, threats and behavioural abnormalities by collecting aggregating, indexing and analyzing security data. Ans it's log data management with a specific time stamp detects multi-line formats and supports XPath filters for Windows events (e.g. Linux Audit logs). It can also add additional metadata to JSON format events. It also has the capacity to discover vulnerabilities and generate reports by comparing data with the National Vulnerability Database (NVD) and information from other OS vendors. Also, SCA performs continuous configuration assessments using out-of-the-box checks based on CIS standards. Users can also use SCA measures to monitor assets as 36 their security policies. System inventory aids in the identification of assets as well as the evaluation of patch management effectiveness. Information like memory consumption, disk space, CPU specifications, network interface, open ports, running processes, and a list of installed apps are all included in this report.

MITRE ATT&CK framework represents many stages of the adversary's attack lifecycle as well as the platforms that are known to target. The regulatory Compliance feature is frequently utilized to meet regulatory compliance standards' technological requirements. All regulatory compliance standards like PCL DSS, GDPR, NIST 800-53, GPG13, TSC SOC2, and HIPAA are available.

This proposed system can evaluate behaviour and risk. As well as an Active Response feature that allows it to respond to an alert promptly and correctly on attacks like Brute Force, Shellshock, Ransomware and Malware attacks and also those attacks were successfully mitigated.

### 5.1 Log Data Analysis:

When EDR Manager Server and End Devices are ready, all these essential features become available, here has information about the components with details. Wazuh agents scan and securely transfer OS and application logs to a central manager for rule base analysis and storage. It can also add additional metadata to JSON format events. Rules alert the SOC team about the application of system problems, configuration issues, attempted or successful harmful operations, policy violations, and other security and suspicious activities.

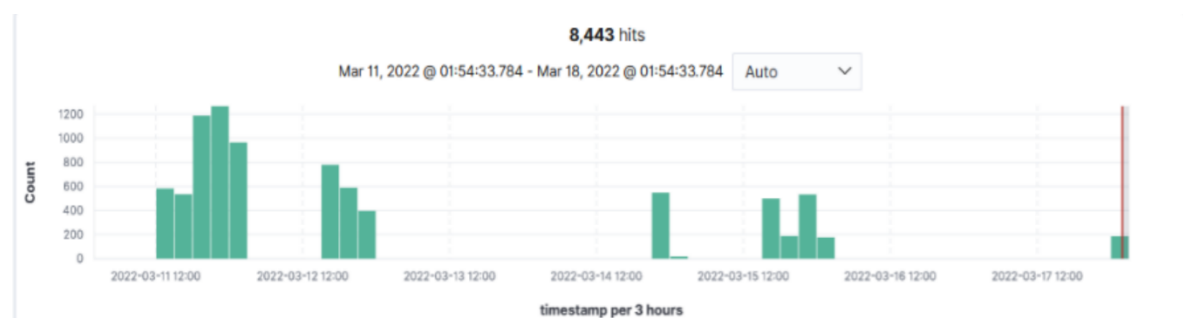


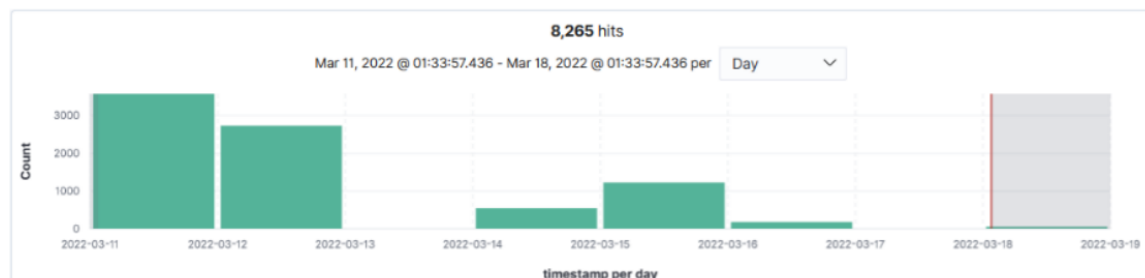
Figure 5.1: Log Analysis



The graphs here show the analysis of log data for the last seven days, from March 11 to March 18. The chart displays each 3-hour time stamp. Where the X-Axis shows the number of days in these 7 days with 3 hours' time stamp, and the Y-axis shows the number of logs received per 3 hours. IT received 1267 logs between 2022-03-11 21:00 to 2022-03-12 00:00

## 5.2 Security Analytic:

Wazuh allows organizations to discover intrusions threats, and behavioural abnormalities by collecting aggregating, indexing and analyzing security data. Real-time monitoring and security analysis are required to detect and remediate agent conduct monitoring and response functions, while the server component delivers security intelligence and data

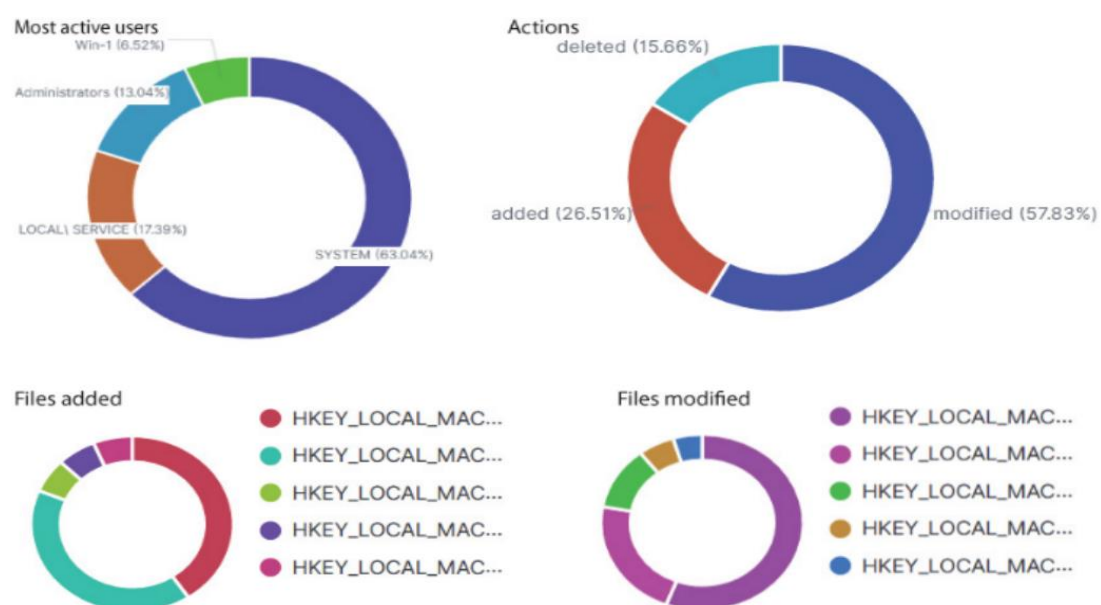


**Figure 5.2: Security Event Analysis**

The graphs here represent the security analysis for the last seven days, from March 11 to March 18. Where the X- axis shows the number of days in these 7 days, and the Y-axis show the number of security alerts identified per day. It identified 3573 security alerts between the dates of 2022-03-11 and 2022-03-12.

## 5.3 File Interiority Monitoring:

It is a module that keeps track of the file system and alerts the SOC team when the file is generated, erased, or modified. File properties, permissions, ownership, and data are all tracked. It collects who, what, and when details in real-time when an event occurs. Even a Single change of character can be tracked.



**Figure 5.3: FIM Dashboard**

Flowing figure 5.3 shows Four categories have been shown here for the last 7 days. The firestone is Showing the most active users, the third and fourth one shows the list of file which has been added and deleted by those users in the last 7 days. Even after creating a text file and writing something into it, an alert would be available within a second. The figure below shows the logs which have been generated for the text file. The changes are also available here, which have been written in the text file.

```

t rule.tsc          PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3

t syscheck.attrs_after  ARCHIVE

t syscheck.changed_attributes  size, mtime, md5, sha1, sha256

t syscheck.diff        < check kors1
                      ---
                      > For my pmit project

t syscheck.event        modified

t syscheck.md5_after    4e1a7658d4b0c37027902a0ada6d04f2

t syscheck.md5_before  4beba54f03220ad3f7a4894b834bc494

t syscheck.mode        realtime

t syscheck.mtime_after  Mar 14, 2022 @ 22:42:20.000

t syscheck.mtime_before Feb 25, 2022 @ 21:35:40.000

t syscheck.path        c:\integritycheck\texti.txt

t syscheck.sha1_after   062bd359d52ce924b0a90677b760bae9429a9a3a

t syscheck.sha1_before  21452a6807b5d301544723601382a4d703924fc0

t syscheck.sha256_after acc0753f81576964eed1c2589a2a9b047b1866b28ce3674821ed2765be0940e1

t syscheck.sha256_before f7742bc019a8188e3d81a31d7a9475a8474f996db4bf4682448636afe63879f6

```

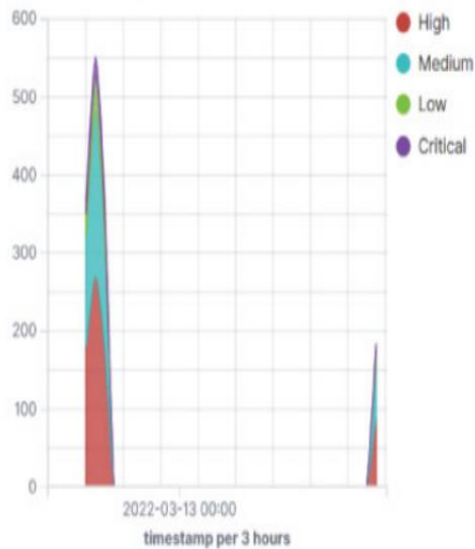
**Figure 5.4: File Integrity Monitoring (FIM) After File Change**

## 5.4 Vulnerability Detection:

Hackers frequently target vulnerable software applications in order to compromise devices and establish a lasting presence on targeted networks. Using software inventory capabilities, the EDR platform keeps track of all apps installed on end devices. It's able to detect insecure apps and risk reports by correlating this data with the National Vulnerability Database (NVD) and information collected from other OS suppliers. It employs a CVE database developed automatically using data from the following sources to detect Vulnerable software.



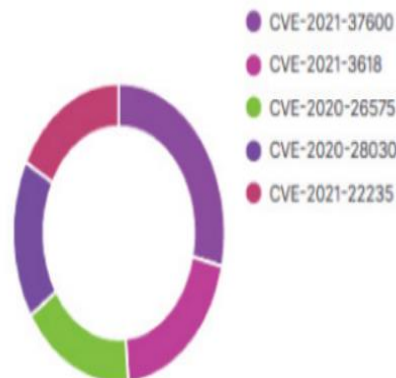
Alerts severity over time



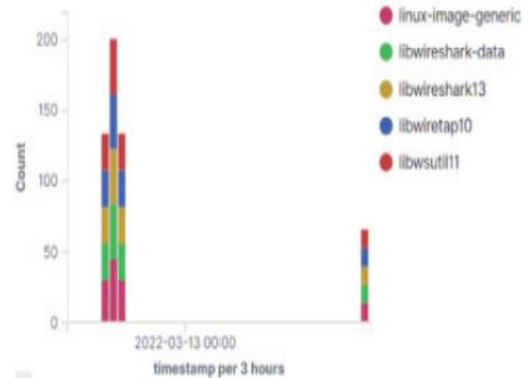
Most common rules

Rule ID	Description	Count
23505	CVE-2020-25862 affects libwiretap10	8
23505	CVE-2020-25863 affects libwireshark-data	8
23505	CVE-2020-25863 affects libwsutil11	8
23505	CVE-2020-25863 affects tshark	8
23505	CVE-2020-28030 affects wireshark-common	8
23505	CVE-2020-6096 affects libc6	8

Most common CVEs



Alerts evolution: Commonly affected packages



**Figure 5.5: Vulnerability Detection Alert & Dashboard**

Flowing figure 5.5 shows Vulnerability Detection Alert and its Dashboard Four categories have been shown here for the last 7 days. The first one is showing the alert severity for the last 7 days with 3 hours' time stamp, during the time period of 2022-03-11 21:00 to 2022-03-12 00:00 it has detected the highest 27 alerts with the highest severity. The second one show the id of the most common rule which detected CVE, the third one shows the most detected CVEs and the fourth one shows the commonly affected packages in the last 7 days. According to the graph, libwsutil11 is the Vulnerable and top-affected package.

## 5.5 Security Configuration Assessments:

SCA performs continuous configuration assessment using out-of-the-box checks based on CIS standards, Users can also use SCA measures to monitor and enforce. Their security policies.

Figure 5.6 shows the Security configuration assessment audit via Benchmark.

Benchmark for Windows audit ⓘ

Export formatted

Refresh

Pass

23

Fail

10

Not applicable

38

Score

69%

End scan

Mar 14, 2022

@

ID ↑	Title	Target	Result	
14500	Ensure 'Accounts: Limit local a...	<b>Registry:</b> HKEY_LOCAL_MACHINE\System \\CurrentControlSet\\Control\\Lsa	● Passed	▼
14501	Ensure 'Audit: Shut down syste...	<b>Registry:</b> HKEY_LOCAL_MACHINE\System \\CurrentControlSet\\Control\\Lsa	● Passed	▼
14503	Ensure 'Devices: Prevent users...	<b>Registry:</b> HKEY_LOCAL_MACHINE\System \\CurrentControlSet\\Control\\Print \\Providers\\LanMan Print Services\\Servers	● Failed	▼

Figure 5.6 : Security Configuration Assessment (SCA) Alert

## 5.6 System Inventory:

The hardware and software information from the monitored devices is collected by the system inventory module. This feature aids in the identification of assets as well as the evaluation of patch management effectiveness. Information like memory consumption, disk space, CPU specifications, network interfaces, open ports, running processes, and a list of installed apps are all included in this report.

Cores: 2	Memory: 2047.49 MB	Arch: x86_64	OS: Microsoft Windows 10 Enterprise 10.0.19042	CPU: Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz	Last scan: Mar 14, 2022 @ 23:19:05.000
----------	--------------------	--------------	--	--	--

Network interfaces					Network ports				
Name	MAC	State	MTU	Type	Process	Local IP	Local port	State	Protocol
Bluetooth Network Connection	78:2b:46:c0:ba:6f	down	1500	ethernet	System	0.0.0.0	445	listening	tcp
					System	10.1.1.128	139	listening	tcp
					System	::	445	listening	tcp6
Loopback Pseudo-Interface 1	00:00:00:00:00:00	up			System	10.1.1.128	137		udp
					System	10.1.1.128	138		udp
Ethernet1	00:0c:29:94:8e:ff	up	1500	ethernet	svchost.exe	0.0.0.0	49667	listening	tcp

Fig 5.7 System Inventory

## 5.7 MITRE ATT&CK:

MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior. It represents many stages of an adversary's attack lifecycle and the platform known to target. [18]

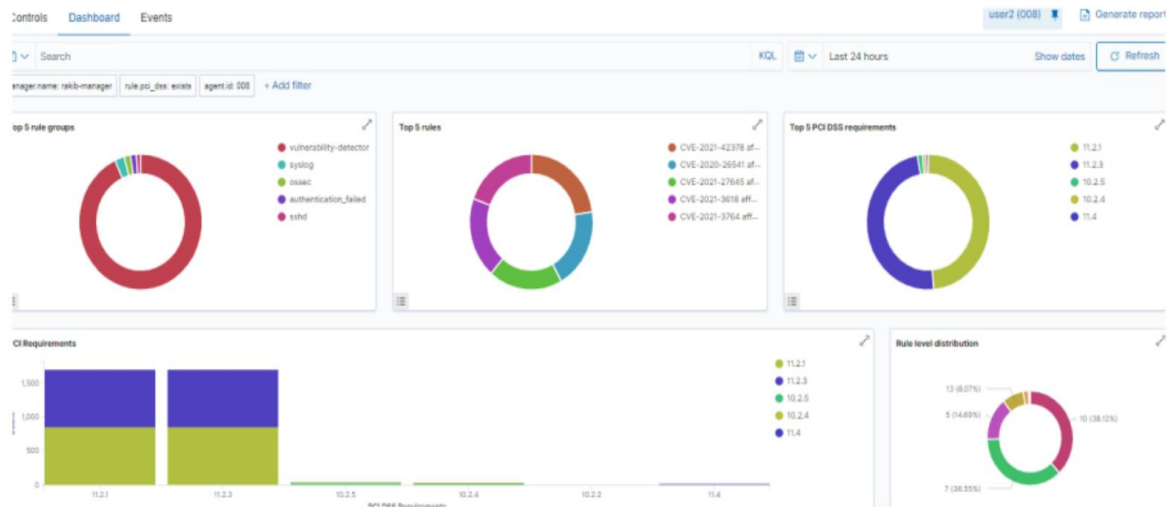


**Figure 5.8: MITRE ATT&CK Dashboard**

Flowing figure 5.8 shows MITRE ATT&CK report. Five categories have been shown here for the last 3 days. Alerts evolution over time showing the different types of attacks with 3 hours' time stamp. Here the top-level attack type is Stored Data Manipulation, which has been tried a total of 34 times during the time period of **Mar 12, 2022, 15:00 to Mar 12, 2022, 18:00**. And the lowest type of attack is Exploitation for Client Execution, tried only single time at Mar 12, 2022, 15:00 to Mar 12, 2022, 18:00. The Second category showing the Top tactics of attack. The third category shows the types of attacks by rule level. Where the maximum attack is identified by rule 5. The fourth one represents the MITRE attacks by tactics. Where File Deletion Impact is the top tactic. The fifth category is also showing rule-level tactics of attack where the impact of file deletion is top.

## 5.8 Regulatory Compliance:

EDR platform is frequently utilized to meet regulatory compliance standards' technological requirements. All regulatory compliance standards like PCI DSS, and GDPR. NIST 800-53, GPG13, TSC SOC2, and HIPAA are available. [19]

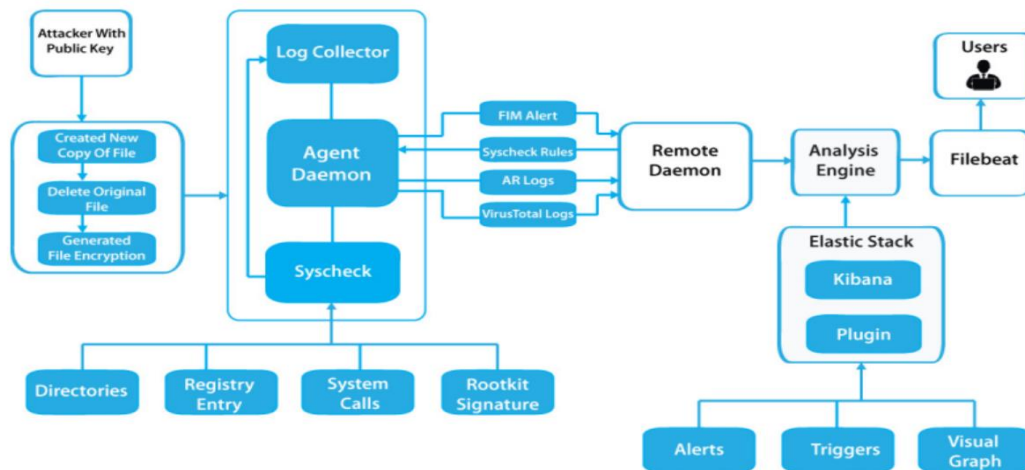


**Figure 5.9: Regulatory Compliance of PCI DSS**

Figure 5.9 shows the MITRE ATT&CK report. Five categories have been shown here for the last 24 hours. First from the left is the Top 5 rule group used to detect the vulnerability and malicious activity for comparison of PCI DSS. Where vulnerability detector rules are used to identify the most vulnerable here. The second one shows the id of the most common rule which detected CVE, where CVE-2021-42378 is the top vulnerability. third and fourth one shows the top 5 PCI DSS needs to meet regulatory compliance. And the final one is the comparison of the top 5 rule distributions. Where the top distribution rule is 10 which used 38.12%.

## 5.9 Mitigate of Ransomware:

To keep the system safe, EDR must take steps to prevent and identify ransomware attacks. To test, a ransomware attack was launched and then used the file integrity monitoring module to detect that. In recent years increasing waves of ransomware attacks have been recorded that target many economic sectors. This sort of malware works by encrypting a computer system or data and preventing access until a ransom is paid. Typically, ransomware spreads by phishing scams and spam. Furthermore, certain ransomware families, such as WannaCry, use exploits to infect other systems in the network, implying that they do not require human assistance to spread. It is advised that organizations keep their systems updated and adequately secured, backup data regularly, and educate end-users on security to avoid ransomware. [11]



**Figure: 5.10: Ransomware Attack Procedure and Mitigation Diagram**

The following components aid in the prevention and detection of ransomware: Vulnerability identification without scanning - Correlates inventory data with well-known CVEs to identify susceptible systems and applications. Security configuration assessment (SCA) -This tool is used to identify systems that aren't properly set up. It performs configuration checks on a regular basis, enforcing best practices by adhering to standards such as CIS (Center of Internet Security). File integrity monitoring (FIM) This feature keeps track of changes to the file system and can be used to locate malicious files. During an attack, the ransomware does the following actions:

- >Read the contents of the file.
- >Write the content into a new file after encrypting it.
- >Get rid of the original file.

It can readily be discovered that new files are being generated while encrypted, and the original ones are destroyed since Wazuh FIM can monitor the addition, modifications, and deletion of files in directories. It could be dealing with a ransomware attack if an unusually high number of file creation and deletion warnings are raised. Using FIM detecting ransomware - first and foremost, on the end device, python3 as well as the cryptography package, need to be installed. Then a ransomware attack was launched by using a Python script. There are hundreds of free scripts available on GitHub.

Also, a test directory was used to test the environment –

```
root@user2: #mkdir -p /home/vagrant/test
root@user2: #cd /home/vagrant/test
```

Then need to download the ransomware python script –

```
root@user2:/home/vagrant/test#weget“https://github.com/ncorbuk/Python-
Ransomware/blob/master/Ransom Ware.py”
root@user2:/home/vagrant/test#python3 Ransom Ware.py prepare
```

After running the prepare command, the script could create ten to twenty directories. The new files which were added are shown in the alert:



Time	agent.name	full_log	rule.description
> Mar 5, 2022 @ 22:53:11.031	agent01	File '/home/vagrant/test/Directory_09/File_19.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.028	agent01	File '/home/vagrant/test/Directory_09/File_18.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.025	agent01	File '/home/vagrant/test/Directory_09/File_12.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.022	agent01	File '/home/vagrant/test/Directory_09/File_15.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.019	agent01	File '/home/vagrant/test/Directory_09/File_14.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.016	agent01	File '/home/vagrant/test/Directory_09/File_13.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.013	agent01	File '/home/vagrant/test/Directory_09/File_06.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.010	agent01	File '/home/vagrant/test/Directory_09/File_09.txt' was added.	File added to the system
> Mar 5, 2022 @ 22:53:11.007	agent01	File '/home/vagrant/test/Directory_09/File_10.txt' was added.	File added to the system

**Figure 5.11: Ransomware File Added Log**

An attack was launched by the following command. Then each file would be encrypted, and the original would be deleted –

**root@user2:/home/vagrant/test#python3 Ransom Ware.py attack**

> Mar 5, 2022 @ 22:53:09.982	/home/vagrant/test/Directory_09/File_19.txt.encrypted	added	File added to the system.	5
> Mar 5, 2022 @ 22:53:09.979	/home/vagrant/test/Directory_09/File_01.txt	deleted	File deleted.	7
> Mar 5, 2022 @ 22:53:09.976	/home/vagrant/test/Directory_09/File_17.txt.encrypted	added	File added to the system.	5
> Mar 5, 2022 @ 22:53:09.973	/home/vagrant/test/Directory_09/File_03.txt	deleted	File deleted.	7
> Mar 5, 2022 @ 22:53:09.970	/home/vagrant/test/Directory_09/Directory_08/File_09.txt.encrypted	added	File added to the system.	5

**Figure 5.12: Ransomware Encryption Lags**

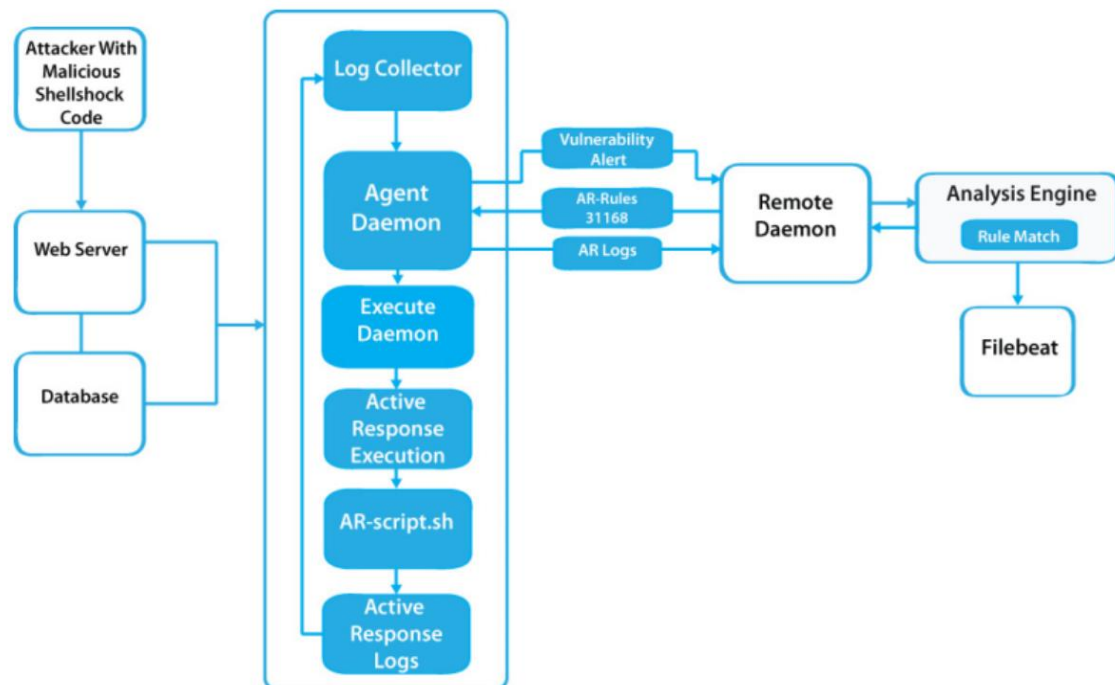
Two sorts of file integrity monitoring notifications were noticed in the Wazuh UI: added and deleted. Alerts monitor and triggers set up It can still be difficult to tell when an attack is taking place. As a result, it aids in the immediate triggering of alarms when this condition is observed. Here Open Distro's Alerting tool is used for this reason. To begin, a monitor is built for the newly added file alerts. That has to establish a trigger for the previously defined monitor with a condition of 100 hits. Then need to create another monitor for newly deleted file alerts, and finally, a separate monitor is constructed for file deletion warnings. When Wazuh identifies assault behaviour in the future, both monitors will be engaged at the same time. It is now possible to respond fast to an ongoing ransomware attack. Which is critical for the protection of systems.

Monitors						
<input type="text" value="Search"/>			All states <span>▼</span>		< 1 >	
<input type="checkbox"/> Monitor name <span>▼</span>	Last updated by	Latest alert	State	Last notification time	Active	Acknowl
<input type="checkbox"/> File Deleted Alert of ...	admin	--	Enabled	-	0	0
<input type="checkbox"/> File Added Alert of R...	admin	FIM-Huge-Add-Trig...	Enabled	03/10/22 4:11 pm	0	0

**Figure 5.13: Ransomware Monitor Dashboard**

## 5.10 Mitigate Shellshock:

Shellshock refers to a set of vulnerabilities that can affect Linux Bash shell, and it was discovered in late 2014. [21] These flaws allowed shell commands to be injected into Linux web servers via maliciously crafted web requests. Any instances of servers being probed with Shellshock requests are fairly strong evidence of malicious probing worthy of automated countermeasures. [22]



**Figure 5.14: Shellshock attack procedure and mitigation Diagram**

In response to this attack, numerous active reaction scenarios are built up and tested in this case, the offender will be instantly blocked from accessing Linux computers and directed through the Windows system.

A web server is needed to install on Linux agent pc. Figure 5.16 shows the NGINX status

```

root@user2:/home/user2# apt-get install nginx -y
root@user2:/home/user2# systemctl start nginx
  
```

```
root@user2:/home/user2# systemctl status nginx
```

```
root@user2:/home/user2# systemctl start nginx
root@user2:/home/user2# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-03-06 06:38:53 UTC; 5min ago
     Docs: man:nginx(8)
  Main PID: 3229 (nginx)
    Tasks: 3 (limit: 2289)
   Memory: 5.5M
    CGroup: /system.slice/nginx.service
            └─3229 nginx: master process /usr/sbin/nginx -g daemon on; master
               └─3230 nginx: worker process
                  └─3231 nginx: worker process

Mar 06 06:38:53 user2 systemd[1]: Starting A high performance web server and a
Mar 06 06:38:53 user2 systemd[1]: Started A high performance web server and a
root@user2:/home/user2#
```

**Figure 5.15: NGNIX Active Status**

It needs to be sure that the server collects the Nginx access and error logs by including these `localfile` sections in the agent's `/var/ossec/etc/ossec.conf` file:

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/nginx/access.log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/log/nginx/error.log</location>
</localfile>

</ossec_config>

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit          ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell
```

**Figure 5.16: OSSEC rule Change for NGNIX**

A Shellshock probe is sent to the webserver and looks at the alert that comes back. Figure 5.17 shows the alert due to Shellshock attack.



```
root@user3:/home/user3#hellshock Target="10.1.1.100"
```

```
root@user3:/home/user3# curl -insecure $Shellshock Target -H "User-Agent :();  
/bin/cat /etc/passwd"
```

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Mar 6, 2022 @ 13:32:18 .557	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack detected	15	31168

**Figure 5.17: Shellshock Alert**

### 5.11 Active Response (AR) Against shellshock:

Now countermeasures against Shellshock probes using Active Response (AR) are set up. Wazuh Active Response (AR) allows scripted actions to be performed in response to certain Wazuh rule requirements being met. All agents have AR enabled by default, and all standard AR commands are defined in `ossec.conf` on the Wazuh management. However, there are no actual requirements for calling the AR commands. No AR commands are executed until the manager is configured further.

In Linux, using the IP tables firewall, and in Windows, using null routing/ blackholing, respectively, is a widely popular command for automatic blocking:

Then a new firewall-drop command is added in active response, using the rule ID 31168, which detects the attack. Hence, by using iptables, the victim could block the attacker.

```
<active-response>  
  <disabled>no</disabled>  
  <command>firewall-drop</command>  
  <location>local</location>  
  <rules_id>31168</rules_id>  
  <timeout>300</timeout>  
</active-response>
```

**Figure 5.18: Shellshock Alert Rule**

To test the AR, another attack is launched and then monitor the alerts.

```
root@user3:/home/user3#hellshock Target="10.1.1.100"
root@user3:/home/user3#rl -insecure $ShellshockTarget -H "User-Agent
:(): ;;/bin/cat /etc/passwd"
```

After having alert, AR drops the ip which is used to attack. Figure 5.19 shows, after detecting attack AR immediately blocked the IP by firewall drop rules.

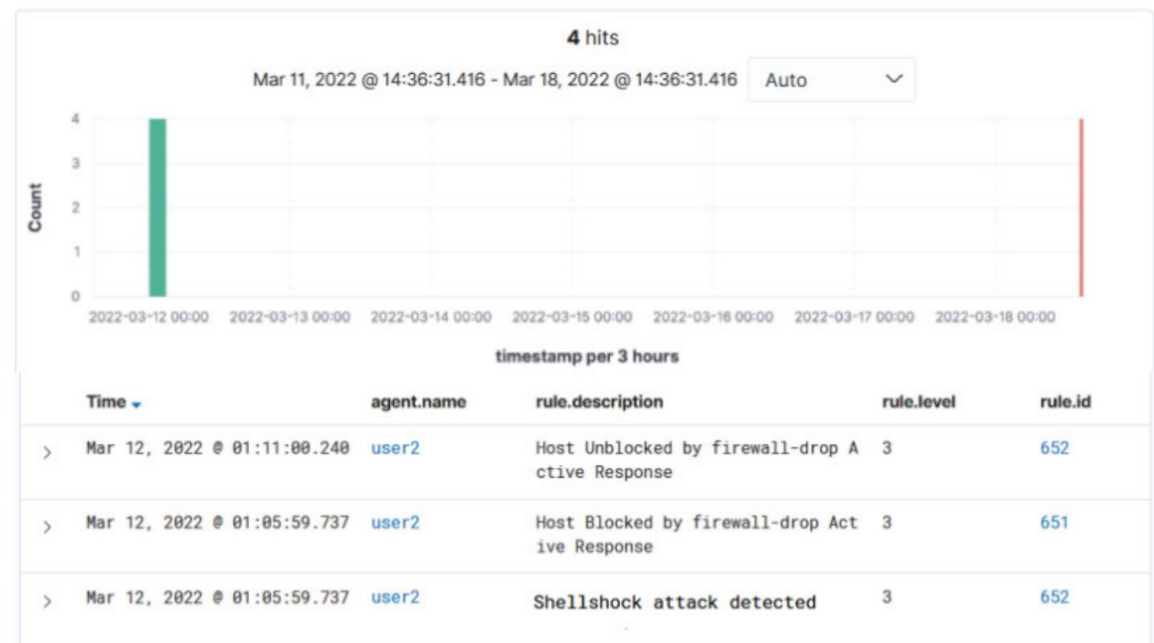


Figure 5.19: Shellshock Prevention Log

## 5.12 Packet Analysis during Shellshock:

Figure 5.20 and 5.21 shows the captured packet during shellshock attack.

```
1 0.000000000 10.1.1.110 -> 10.1.1.100 TCP 74 36542 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
ERM=1 TSval=3174098354 TSecr=0 WS=128
2 0.000044345 10.1.1.100 -> 10.1.1.110 TCP 74 80 -> 36542 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
1460 SACK_PERM=1 TSval=512851521 TSecr=3174098354 WS=128
3 0.000623886 10.1.1.110 -> 10.1.1.100 TCP 66 36542 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=317
4098355 TSecr=512851521
4 0.000624079 10.1.1.110 -> 10.1.1.100 HTTP 160 GET / HTTP/1.1
5 0.000717025 10.1.1.100 -> 10.1.1.110 TCP 66 80 -> 36542 [ACK] Seq=1 Ack=95 Win=65152 Len=0 TSval=51
2851521 TSecr=3174098355
6 0.001731040 10.1.1.100 -> 10.1.1.110 HTTP 925 HTTP/1.1 200 OK (text/html)
7 0.002268867 10.1.1.110 -> 10.1.1.100 TCP 66 36542 -> 80 [ACK] Seq=95 Ack=860 Win=64128 Len=0 TSval=
3174098356 TSecr=512851522
8 0.002607367 10.1.1.110 -> 10.1.1.100 TCP 66 36542 -> 80 [FIN, ACK] Seq=95 Ack=860 Win=64128 Len=0 T
Sval=3174098357 TSecr=512851522
```

Figure 5.20: Shellshock Captured Packet-1.

```

25 4.562712946 10.1.1.110 → 10.1.1.100 TCP 74 [TCP Retransmission] 36544 → 80 [SYN] Seq=0 Win=64240
Len=0 MSS=1460 SACK_PERM=1 TSval=3174102916 TSecr=0 WS=128
26 5.104615129 VMware_00:8d:60 → VMware_ae:14:b0 ARP 42 Who has 10.1.1.110? Tell 10.1.1.100
27 5.105500814 VMware_ae:14:b0 → VMware_00:8d:60 ARP 60 10.1.1.110 is at 00:0c:29:ae:14:b0
28 5.233904320 VMware_ae:14:b0 → VMware_00:8d:60 ARP 60 Who has 10.1.1.100? Tell 10.1.1.110
29 5.233947320 VMware_00:8d:60 → VMware_ae:14:b0 ARP 42 10.1.1.100 is at 00:0c:29:00:8d:60
30 7.073649550 10.1.1.110 → 10.1.1.150 TCP 208 52460 → 1514 [PSH, ACK] Seq=919 Ack=90 Win=1523 Len=1
42 TSval=1024483068 TSecr=2810032644
31 7.074408016 10.1.1.150 → 10.1.1.110 TCP 66 1514 → 52460 [ACK] Seq=90 Ack=1061 Win=501 Len=0 TSval
=2810036640 TSecr=1024483068
32 7.074949542 10.1.1.110 → 10.1.1.150 TCP 224 52460 → 1514 [PSH, ACK] Seq=1061 Ack=90 Win=1523 Len=
158 TSval=1024483070 TSecr=2810036640
33 7.075501161 10.1.1.150 → 10.1.1.110 TCP 66 1514 → 52460 [ACK] Seq=90 Ack=1210 Win=501 Len=0 TSval

```

Figure 5.21: Shellshock Captured Packet-2.

### 5.13 Mitigate of Brut Force Attack:

Common attack vectors include brute-forcing SSH (on Linux) or RDP (on Windows). By correlating several authentication failure events, Wazuh EDR provides out-of-the-box rules capable of spotting brute-force assaults. Here a Brute Force attack is made. [23] [24]

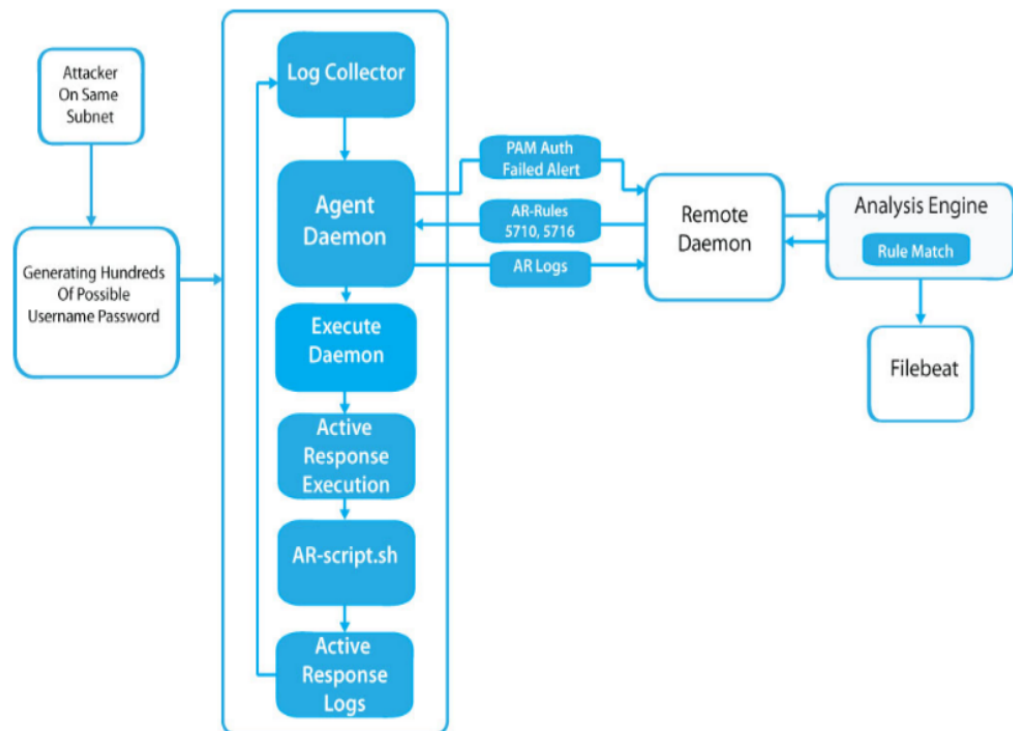


Figure 5.22: Brute Force Attack Procedure And Mitigation Diagram.

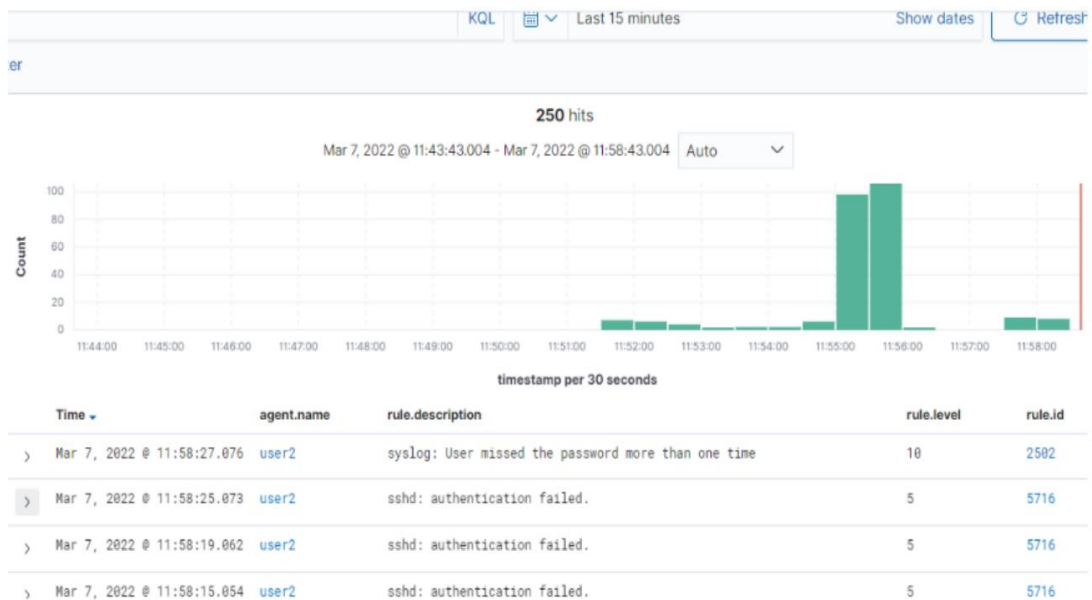


Figure 5.23: Brute Force Alert

```

"164.312.b"
],
"tsc": [
  "CC6.1",
  "CC6.8",
  "CC7.2",
  "CC7.3"
],
"description": "syslog: User missed the password more than one time"
"groups": [
  "syslog",
  "access_control",
  "authentication_failed"
],
"nist_800_53": [
  "AU.14",
  "AC.7"
],
"gdpr": [
  "IV_35.7.d",
  "IV_32.2"
],
"firedtimes": 2,
"mitre": {
  "technique": [
    "Brute Force"
  ],
  "id": [
    "T1110"
  ]
}

```

Figure 5.24: Brute Force Log

Figure 5.23 and 5.24 shows the multiple authentications failed alert and in the details log it has been identified as a Brute Force technique. After detecting and generating an alert it could block the IP with AR.

## 5.14 Active Response (AR) Against Brut Force Attack:

Now an Active Response rule is made to block the IP, which has been used to attack. In the following figure, a rule is made to block an IP under the 5712 rule ID for agent 008. Also, input a timeout of 60 sec. Thus, AR could unblock the IP within 60sec. For repeated offenders put a time value of 30min, 60min, and 120 to extend the duration block.

```

t ossec.conf of Manager
263 | <executable>netsh.exe</executable>
264 | <timeout_allowed>yes</timeout_allowed>
265 | </command>
266 |
267 | <active-response>
268 | | <command>firewall-drop</command>
269 | | <location>defined-agent</location>
270 | | <agent_id>008</agent_id>
271 | | <rules_id>5712</rules_id>
272 | | <timeout>60</timeout>
273 | | <repeated_offenders>30,60,120</repeated_offenders>
274 | </active-response>
275 |

```

Figure 5.25: Brute Force Prevention Rule

The following figure 5.26 depicts the alerts of blocking ip, and after 60 sec AR releases the IP to unblock.

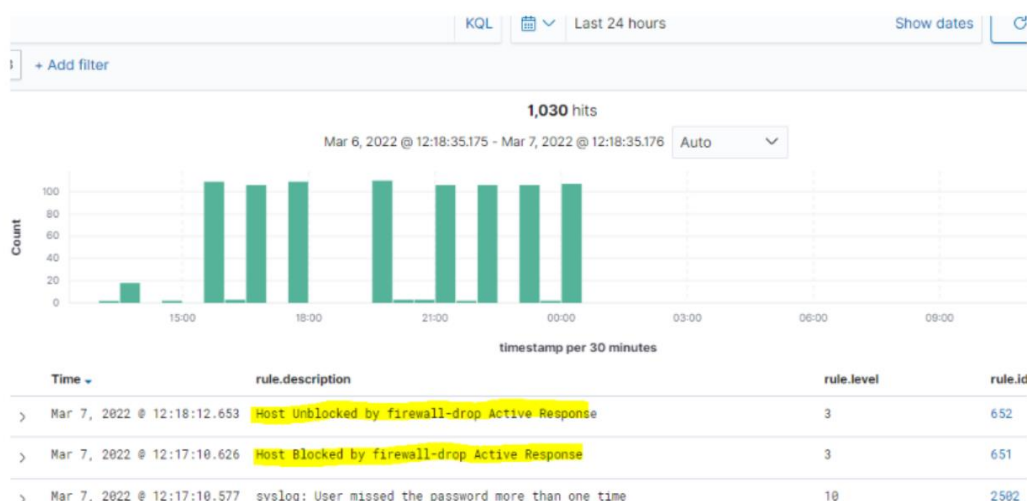


Figure 5.26: Brute Force Prevention Logs



## 5.15 Packet Analysis during Brut Force Attack:

Figure 5.27 and 5.28 show the capture packet of during brute force attack.

```
10 0.039853531 10.1.1.110 → 10.1.1.1 SSH 118 Server: Encrypted packet (len=64)
11 0.081029830 10.1.1.1 → 10.1.1.110 TCP 60 54236 → 22 [ACK] Seq=65 Ack=65 Win=509 Len=0
12 0.218877023 10.1.1.1 → 10.1.1.110 SSH 118 Client: Encrypted packet (len=64)
13 0.219287921 10.1.1.110 → 10.1.1.1 SSH 118 Server: Encrypted packet (len=64)
14 0.260174555 10.1.1.1 → 10.1.1.110 TCP 60 54236 → 22 [ACK] Seq=129 Ack=129 Win=509 Len=0
15 0.376692201 10.1.1.1 → 10.1.1.110 SSH 118 Client: Encrypted packet (len=64)
16 0.377116231 10.1.1.110 → 10.1.1.1 SSH 118 Server: Encrypted packet (len=64)
17 0.417924134 10.1.1.1 → 10.1.1.110 TCP 60 54236 → 22 [ACK] Seq=193 Ack=193 Win=509 Len=0
18 0.531780163 10.1.1.1 → 10.1.1.110 SSH 118 Client: Encrypted packet (len=64)
19 0.531780627 10.1.1.1 → 10.1.1.110 SSH 118 Client: Encrypted packet (len=64)
20 0.532137351 10.1.1.110 → 10.1.1.1 TCP 60 22 → 54236 [ACK] Seq=193 Ack=321 Win=501 Len=0
21 0.532365913 10.1.1.110 → 10.1.1.1 SSH 118 Server: Encrypted packet (len=64)
```

Figure 5.27: Brute Force Captured Packet-1

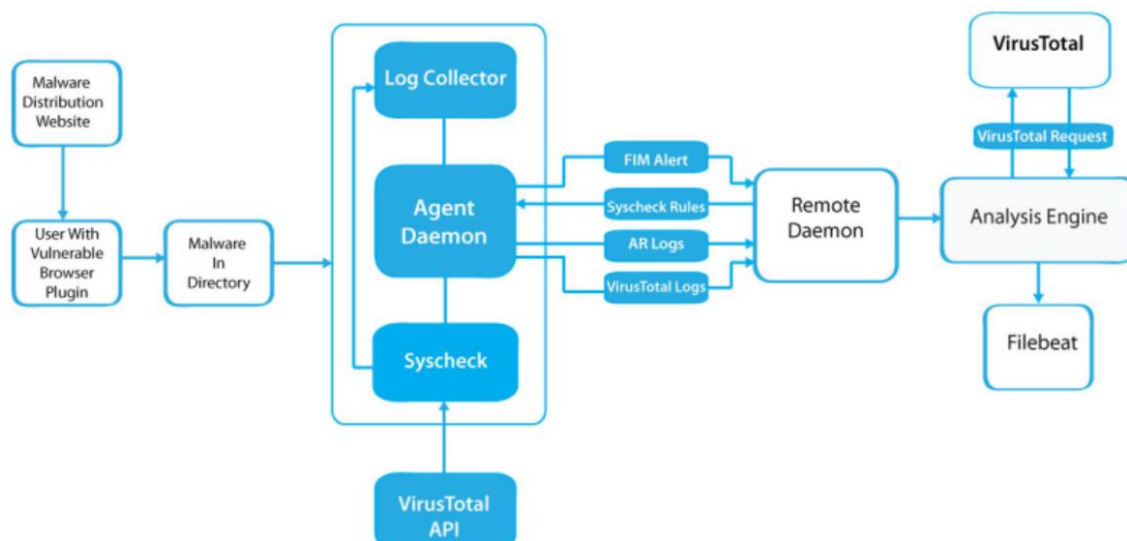
```
177 24.040734343 10.1.1.1 → 10.1.1.110 SSH 118 Client: Encrypted packet (len=64)
178 24.041238252 10.1.1.110 → 10.1.1.1 SSH 118 Server: Encrypted packet (len=64)
179 24.081079520 10.1.1.1 → 10.1.1.110 TCP 60 54236 → 22 [ACK] Seq=1793 Ack=2049 Win=507 Len=0
180 27.002568604 10.1.1.110 → 10.1.1.100 TCP 66 [TCP Retransmission] 34368 → 22 [FIN, ACK] Seq=317 Ack=157 Win=501 Len=0 TSval=3364021741 TSecr=2427832937
181 27.400651065 10.1.1.100 → 10.1.1.110 SSH 118 Server: [TCP Spurious Retransmission], Encrypted packet (len=52)
182 27.401614582 10.1.1.110 → 10.1.1.100 TCP 78 [TCP Dup ACK 112#7] 34368 → 22 [ACK] Seq=318 Ack=157 Win=501 Len=0 TSval=3364022140 TSecr=2427839848 SLE=105 SRE=157
183 28.212816331 VMware_c0:00:01 → VMware_ae:14:b0 ARP 60 Who has 10.1.1.110? Tell 10.1.1.1
184 28.213310904 VMware_ae:14:b0 → VMware_c0:00:01 ARP 60 10.1.1.110 is at 00:0c:29:ae:14:b0
184 packets captured
```

Figure 5.28: Brute Force Captured Packet-2

Figure 5.17 indicates several ssh requests sent from 10.1.1.110 to 10.1.1.100, as the gateway failed to connect due to incorrect credentials. As soon as it's detected that this is a brute force attack, Active Response block the IP. On figure 6.16, after this session ended 10.1.1.110 was unable to ssh again to 10.1.1.100.

## 5.16 Malware Detection:

Now an Active Response rule is made to block the IP, which has been used to attack. In the following figure, a rule is made to block an IP under the 5712 rule ID for agent 002. Also, input a timeout of 60 sec. Thus, AR could unblock the IP within 60sec. For repeated offenders put a time value of 30min, 60min, and 120 to extend the duration block.



**Figure 5.29: Malware Attack Procedure and Mitigation Diagram**

First, need to register on Virustotal.com and generate an API Key. [25] Then the OSSEC configuration file is edited in the manager. Where Virustotal API Key is integrated with Group and alert format.

```

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

<integration>
  <name>virustotal</name>
  <api_key>956a2a99383b4b424011b560fda58904f2cfb7</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>

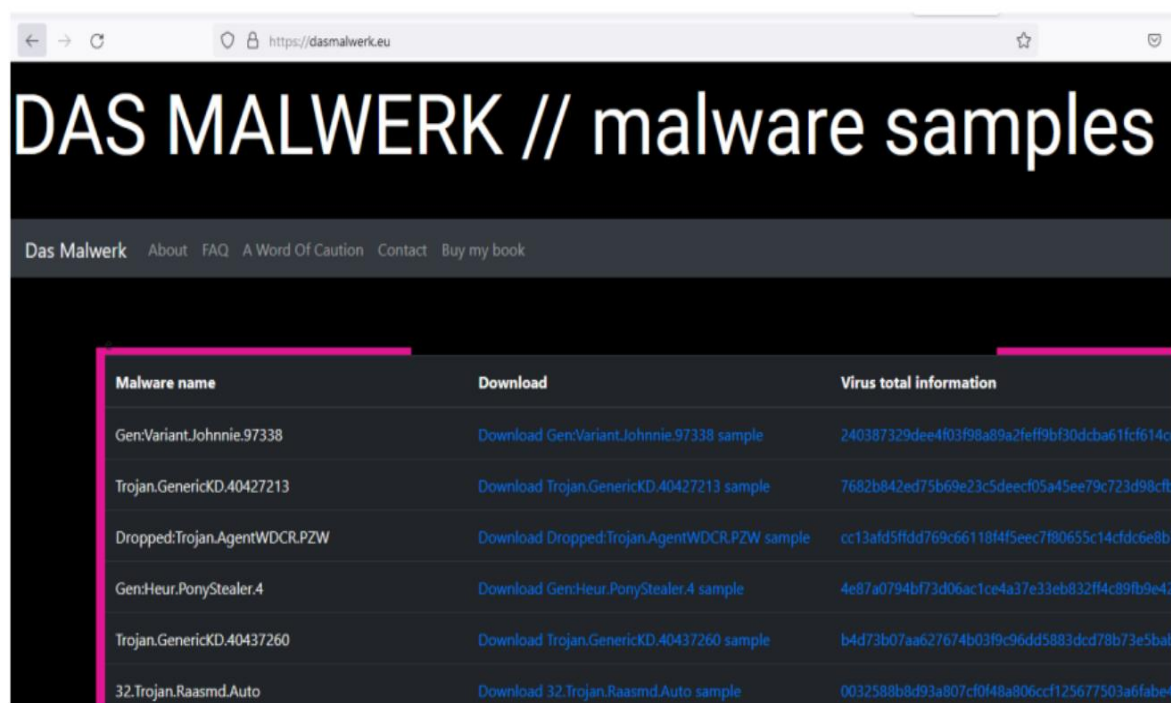
<!-- Osquery integration -->
<wodle name="osquery">

```

**Figure 5.30: Virus Total API Integrations**

As the FIM is already working through the "syscheck" group, it just needs to enable the "Virustotal" section in the Kibana GUI.

To test the Virustotal detection service, a malware file is needed to download on the end device from <https://dasmalwerk.eu/> and put that on any of the directories. Figure 5.31 shows the Malware downloading process from Dasmalwerk.



**Figure 5.31: Malware Downloading process from DAS Malwerk**

Then an alert may appear on the Virustotal dashboard with details. Figure 5.32 shows the log of VirusTotal malware detection with Virus Total permalink

```

index          wazuh-alerts-4.x-2022.03.06
timestamp      Mar 6, 2022 @ 14:07:53.318
agent.name     DESKTOP-DCM2F0M
data.integration virustotal
data.virustotal.perm alink https://www.virustotal.com/gui/file/b56601c1bfa1c8327c0d2573c9424aed6a67e74ea890e558f6c0b80d1c78410b/detection/f-b56601c1bfa1c8327c0d2573c9424aed6a67e74ea890e558f6c0b80d1c78410b-1643110491
data.virustotal.sha1 09d915a6e9cbfe02869cb035b9762eb0ee15b822
data.virustotal.source.file c:/integritycheck/7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af.zip
data.virustotal.source.md5 cfc331cbcb0d62f6b3dd31c4032109bd
data.virustotal.source.sha1 09d915a6e9cbfe02869cb035b9762eb0ee15b822
decoder.name    json
input.type      log
manager.name    rakib-manager
rule.description VirusTotal: Alert - c:/integritycheck/7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af.zip - 3 engines detected this file
rule.gdpr       IV-35.7.d
rule.groups     virustotal
rule.mitre.id   T1203
rule.mitre.tactic Execution
rule.mitre.technique Exploitation for Client Execution

```

**Figure 5.32: Virus Total Log got Malware detection**



## 5.17 Remove Malware with Active Response:

On malware detection alert, the rule id is 87105, which detected the malware. Then new firewall-drop command is added in active response, and add AR command in /var/osser/etc/ossee.conf.

Figure 5.33 shows the rules procedure of removing malware threat.

```
<ossec_config>
  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

^G Get Help    ^O Write Out    ^W Where Is    ^K Cut Text  
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text

Figure 5.33: AR Rule for Malware Remove

Rule 87105 is now activated. Active response will trigger as soon as VirusTotal designates a file as malicious. Figure 5.34 shows the logs of malware remove.

decoder.name	json
id	1646554073.511080
input.type	log
location	virustotal
manager.name	rakib-manager
rule.description	File deleted.
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.groups	virustotal
rule.id	87105
rule.level	12
rule.mail	true
rule.mitre.id	T1203
rule.mitre.tactic	Execution

Figure 5.34: Generate Log After Malware Remove

## Chapter Vi

### **Conclusion:**

In this study, a EDR was designed by using open-source resources rather than premium or enterprise-level solutions. The Open Distro for Elasticsearch, a highly scalable full-text search and analytics engine, is used. Filebeat is used to read the output of the analysis engine and communicate events in real time via an encrypted tunnel. Kibana, a web-based GUI analysis and visualization tool that is both versatile and user-friendly is also deployed. This EDR can evaluate behaviour and risk. As well as an Active Response feature that allows it to respond to an alert promptly and correctly.

Most enterprise EDR capabilities, including Security analysis, Log analysis, Vulnerability and Malware detection, SCA, FIM, Inventory, MITRE ATT&CK, and Regulatory compliance with effective Active Response, are presented in this EDR. Even a single character added or written to a file on a directory is tracked in real-time and displayed in an alert using FIM facilities.

In addition, a few Malware, Shellshock, Brute Force, and Ransomware attacks were successfully mitigated. Finally, it can be concluded that the EDR model used here is capable of successfully managing small organizations or companies operations.

### **Future Work:**

Security Information and Event Management or EDR is an established and modern technology in cyber security. Still, there is a vast area to contribute to research and make the technology more effective. Most reputed vendors are still working to make this technology more powerful, effective, and affordable.

The proposed model for this project has been made to work on a small enterprise that does not need all the next-generation features, but large enterprises or organizations may go for enterprise or paid versions. This proposed model has been tested in a lab environment. Also, different types of attacks have been mitigated. Thus the performance and output data can be tested in a practical environment. Also, EDR generates thousands of logs and events. It is hard to manage these logs without Artificial Intelligence. With AI EDR it will be more effective in the future. Besides, the Active Response can improve, as it's kind of complex on this EDR.

## Reference

- [1] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, p. 4759, Jan. 2021. Number: 14 Publisher: Multidisciplinary Digital Publishing Institute, Jan, 2021.
- [2] D. Howell, "Building better data protection with SIEM," *Computer Fraud & Security*, vol. 2015, pp. 19-20, Aug. 2015.
- [3] J. D. Linares, L. R. O'Neil, R. M. Leitch, C. S. Glantz, G. P. Landine, J. L. Bryant, J. Lewis, G. Mathers, R. Rodger, and C. Johnson, "How to implement security controls for an information security program at CBRN facilities," Tech. Rep. PNNL-25112. Pacific Northwest National Lab. (PNNL), Richland, WA (United States), Dec. 2015.
- [4] N. Moukafih, G. Orhanou, and S. Elhajji, "Mobile agent-based SIEM for event collection and normalization externalization," *Information & Computer Security*, vol. ahead-of-print, Aug. 2019.
- [5] "Top six SIEM use cases." <https://resources.infosecinstitute.com/topic/top-6-seim-use-cases>. Accessed March 10, 2022.
- [6] "7 Open Source SIEMS: Features vs. Limitations." <https://www.exabeam.com/explainers/siem/7-open-source-siems/>. Accessed March 6, 2022.
- [7] M. Yadav and D. Mishra, "Study of challenges faced by Enterprises using Security Information and Event Management (SIEM)," *Journal of University of Shanghai for Science and Technology*, vol. 23, pp. 511-522, Aug. 2021.
- [8] "SIEM Open Source Overview," Feb. 2019. <https://www.n-able.com/blog/ossim-open-source-siem-overview>. Accessed March 6, 2022.
- [9] A. Vazão, L. Santos, M. B. Piedade, and C. Rabadão, "SIEM Open Source Solutions: A Comparative Study," in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-5, June 2019. ISSN: 2166-0727.
- [10] C. B. Allen Harper, *Security Information and Event Management (SIEM) Implementation*. Noida, Uttar Pradesh, India: McGraw Hill Education, first edition ed., 2010.
- [11] "What is SIEM and how does it work?." <https://fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html>. Accessed March 10, 2022.
- [12] J. Andress and S. Winterfeld, "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition," pp. 1- 217, Jan. 2014.
- [13] "Must-Have Features of a Modern SIEM - What is Next-Gen SIEM - Logsign." <https://logsign.com/blog/must-have-features-of-a-modern-siem/>. Accessed March 5, 2022.

- [14] 2022 SIEM vs Log Management Detailed Comparison | Panther." <https://runpanther.io/cyber-explained/siem-vs-log-management-an-overview/> Accessed March 5, 2022.
- [15] A. Majeed, R. Rasool, F. Ahmad, M. Alam, and N. Javaid, "Near-miss situation based visual analysis of SIEM rules for real time network security monitoring." *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, Apr. 2019.
- [16] 9780128184271: Security Controls Evaluation, Testing, and Assessment Hand- book - AbeBooks - Johnson, Leighton: 0128184272." Publisher: Academic Press, 2019.
- [17] D. Stefanova, "SIEM for Regulatory Compliance: Importance, Best Practices, Use Cases," Feb, 2021.
- [18] L. Merel and J. Horalek, "SIEM Implementation for Small and Mid-Sized Business Environments," *Journal of Engineering and Applied Sciences*, vol. 14, pp. 10497-10501, Jan. 2020.
- [19] "Open Which Source SIEM VS You?."Is Right for Enterprise-Level SIEM: [helpsystems.com/blog/](https://helpsystems.com/blog/)
- [20] "Download the 2021 Gartner Magic Quadrant for SIEM." <https://logrhythm.com/gartner-magic-quadrant-siem-report-2021/>. Accessed March 5, 2022.
- [21] "What is open source?." [https://opensource.com/resources/ what-open-source](https://opensource.com/resources/what-open-source). Accessed March 7, 2022.
- [22] "OSSEC Atomic OSSEC Atomicorp." [https://atomicorp.com/ atomic-enterprise-ossec/](https://atomicorp.com/atomic-enterprise-ossec/). Accessed March 10, 2022.
- [23] S. B. Ambati and D. Vidyarthi, "A BRIEF STUDY AND COMPARISON OF OPEN SOURCE INTRUSION DETECTION SYSTEM TOOLS," undefined, 2013.
- [24] A. Hay, D. Cid, and R. Bray, *OSSEC Host-Based Intrusion Detection Guide*. Syngress Publishing, 2008.
- [25] D. Berman, "OSSEC Wazuh fork," May 2016. 18T08:03:192. original-date: 2016-05-
- [26] "Elasticsearch: The Official Distributed Search & Analytics Engine." <https://elastic.co/elasticsearch>. Accessed March 10, 2022.
- [27] "Filebeat overview | Filebeat Reference [8.1] Elastic." <https://elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html>. Accessed March 10, 2022.
- [28] "Elasticsearch, Kibana, Elastic Cloud 8.1: Faster indexing, less disk storage, and smarter analytics capabilities." [https://elastic.co/en-us/blog/ whats-new-elasticsearch-kibana-cloud-8-1-0](https://elastic.co/en-us/blog/whats-new-elasticsearch-kibana-cloud-8-1-0). Accessed March 10, 2022.
- [29] "Wazuh Kibana App." Mar, 2022. wazuh-kibana-app. Accessed March 02, 2022. <https://github.com/wazuh/>

## Appendix - Complex Engineering

### Complex Engineering Problem (Ps):

Ps	Attribute	How Ps are addressed through the project	CO	PO
<b>P1</b>	Depth of Knowledge Requirement	Study of Log-based endpoint security solutions (Security Analytics, Intrusion Detection, Log Data Analysis, File Integrity Monitoring, Vulnerability Detection, Incident Response, Regulatory Compliance, Vulnerability Detection.) and log data collected from different types of operating systems as our research literature (K8). Engineering design (resource allocation for multiple virtual machines) (K5) and configure that VM as per our requirement (K6). Knowledge of Linux, operating system, open-distro and other related software knowledge like elastic search, Kibana, Filebate, Wazuh, etc needed as our engineering fundamentals (K3). The specialist knowledge of Cybersecurity terminology, cryptography, and Windows and links file system is (K4) and proper documentation required.	<b>CO2</b>  <b>CO8</b>	<b>PO b</b> <b>PO c</b> <b>PO j</b>
<b>P2</b>	Range of Conflicting Requirement	We collected real-time log data from the user's machine or server system (e.g., Windows PC, Linux server) and created demo events on that system. The alarm will be triggered on the manager server dashboard. The manager server will categorize the alarm with some severity. also a conflicting requirement and Some time it's the Manger server provide some false alarm due to low resource issue.	<b>CO1</b>	<b>PO 1</b>
<b>P3</b>	Depth of Analysis Required	To malware analysis using dynamic feed from different source and collecting malaises IP address from different source also added domain and URL reputation using sandboxing. To improve the performance, analyzing the current systems, as well as the selection of the tools, are needed. With proper maintenance and tuning, these types of open source endpoint security systems can be used in small and medium corporate environments for a long time.	<b>CO2</b>  <b>CO4</b>	<b>PO b</b> <b>PO c</b> <b>PO g</b>
<b>P7</b>	Interdependence	The project involves high-level problems in Subsystems such as Data collection, Data normalization, Data parsing and data visualization with graph and chart format. All the data are log data that are system-generated data, we are collecting from different types of operating systems such as windows and Linux..	<b>CO3</b>  <b>CO6</b>	<b>PO k</b> <b>PO i</b>

<b>K</b>	<b>Short Name</b>
K1	Natural Sciences
K2	Mathematics
K3	Engineering Fundamentals
K4	Specialist Knowledge
K5	Engineering Design
K6	Engineering Practice
K7	Comprehension
K8	Research Literature

As	Attribute	How As are addressed through the project
A1	Range of resources	This project needs to engage diverse resources including Cybersecurity professional , money, endpoint, and log file of end-user and server system with predefined security polices information and technologies.
A2	Level of interaction	By using logs analysis of the agent machines and detecting malicious events from every system. A well-grounded interaction is required in collecting log files from end-user and server systems through agents, analyzing them, separating each good and bad event and verifying the cause of bad events and taking necessary action.
A3	Consequence for society and the environment	An Open Source Endpoint Protection System can have positive consequences for society and the environment. It can improve security and affordability, promote sustainability, democratize access to cybersecurity tools, and foster a sense of community among cybersecurity professionals. These benefits can lead to a more secure and equitable digital ecosystem, reduce negative environmental impacts, and promote knowledge-sharing and skill development
A4	Familiarity	The project deals with a relatively new area for us such as Security Information and Event Management.