Building Security Operations Center (SOC) using Open Source Technologies SIEM for Industries

by

Zahidul Haque Rabby
19101660

A project submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering
Brac University
September 2022

Declaration

It is hereby declared that

1. The project submitted is my own original work while completing a degree at Brac University.
2. The project does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The project does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Zahidul

Zahidul Haque Rabby
19101660

Approval

The project titled “Building Security Operations Center (SOC) Using Open Source Technologies SIEM for Industries” submitted by

1. Zahidul Haque Rabby (19101660)

Of Summer, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on September 20, 2022.

Examining Committee:

Supervisor:
(Member)

Annajiat Alim Rasel

Digitally signed by Annajiat Alim Rasel
DN: cn=Annajiat Alim Rasel, o=Brac University, ou=CSE Department, email=annajiat@bracu.ac.bd, c=BD
Date: 2023.01.14 23:04:00 +06'00'

Annajiat Alim Rasel
Senior Lecturer
Department of Computer Science and Engineering
Brac University

Secondary Supervisor:
(Member)

Muhammad Abdur Rahman Adnan
Lecturer
Department of Computer Science and Engineering
Brac University

Project Coordinator:
(Member)

Md. Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

____

Sadia Hamid Kazi
Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

In this day of rapidly expanding technology, large industries, enterprises, and startups must safeguard sensitive information about their clients, employees, internal processes, and more. However, with the growth of hackers and developed hacking tools and software, maintaining this level of security has become a difficult undertaking. In recent years, the odds of encountering a security breach by large industries have been on the rise. As a result, businesses are concerned about data security and are looking for innovative ways to safeguard themselves from cyber-attacks. For businesses looking to protect themselves from cyber-attacks, a Cybersecurity Operation Centre (SOC) might be an excellent solution. The Cybersecurity Operation Center (SOC) is a prevention and response center for network activities. Security Operation Centers (SOC) are essential for establishing industry cybersecurity strategy since it has the ability to identify, evaluate, and give detail information of a wide range of hostile unlawful conduct. However, the security operations center (SOC) is more of an afterthought in most industries or firms than the major section of the corporation in the IT sphere. The aim of our project is to give an overview of open-source SOC applications for industries and develop security operations utilizing open-source technology SIEM.

Keywords: SIEM; Cybersecurity; Wazuh; ELK; Security Operations Center; SOC; Security; Security Information; Open Source Technology.

Acknowledgement

Firstly, I am grateful to Almighty ALLAH. It would have been impossible for me to complete this project without His heavenly favor.
Secondly, I would like to thank Annajiat Alim Rasel, Senior Lecturer, and Muhammad Abdur Rahman Adnan, Lecturer, Department of Computer Science, Brac University, for their continuous support and encouragement throughout the thesis. They were incredibly kind and supportive of my efforts at all times. Without the help of all of my respected teachers, I would not have been able to achieve this academic goal. Additionally, they made an effort to push me outside my comfort zones, which helped me produce effective outcomes.
Lastly, I want to give a big thanks from my heart to all my family members for their support and motivation whenever I needed it.

Table of Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

1.1 Introduction

A security operations center (SOC) serves as the hub for an organization's information security department. The SOC refers to both the physical facility and the security team that identifies, analyses and responds to security threats. SOC teams frequently include management, security analysts, and engineers. Companies can now benefit from streamlined security operations that need less time and resources, thanks to next-generation security platforms and solutions.

Following the current statistics, the maximum number of security breaches that companies report increased from 130 in 2017 to 145 in 2018, an increase of 11% [3]. However, these figures only reflect incidences that have been recognized and recorded; the number of cases that have gone unreported is very certainly far higher. The annual cost of any cyber-attack is steadily increasing. It's sad that many attacks go largely unnoticed for a long time. In 2018, it took a median of 196 days to find a vulnerability, while preventing it required an average of 69 days [5]. The incident highlights how poorly corporations recognize and respond to cyber-attacks. Organizations without a security operations center (SOC) and who do not undertake periodic security assessments are unaware of the premier threats of security. For this reason, they are unaware of their system and when their systems have been compromised. In this thesis paper, an unethical approach is defined as a breach in cybersecurity. Security Operations Centers (SOC) can take efforts to identify information and respond to cybersecurity threats. They utilize a combination of people, procedures, and technology to successfully identify, mitigate dangers, ideally before they cause harm. There is no regular system for defining who is responsible for what task, how difficulties are addressed, or how they are documented. SIEM software is the backbone of a Security Operation Center. SIEM stands for "Security Information and Event Management." Many SIEM software are available in the market. Some are commercial while others are open source. Splunk, IBM, and McAfee are the most well-known paid SIEM providers. There are also some open source SIEM solutions available.

1.2 Research Objectives

The aim of this project is to build security operations using open-source technology SIEM for industries. So, the objectives of this project are:

1) To learn more about SOC and open source SIEM solutions.

2) To obtain complete data security in an affordable manner and gain reliability for open source technology.

3) Gathering network device log events (Computers, Routers, Switches, printers, etc).

4) Detect harmful activity by analyzing logs and events.

1.3 Explanation of Open Source SIEM

Security Information and Event Management, or SIEM, provides enterprises with next-generation capabilities for detection, analytics, and response. SIEM is basically the combination of SIM (security information management) and SEM (security event management). They analyze security alerts generated by network hardware and apps in real time. SIEM tools that are open source are freely available, they can be used by anyone who wants to use this tool. As it is public, anyone can change the code and modify it on their own and it is free of cost. The open source SIEM technologies are a public utility, anybody can use them. It is also free of charge. Paid SIEM technologies are widely accessible on the market. There are also several SEIM solutions that are free and open source. These are not expensive, and they help to cut costs, which may assist anybody in providing this service and taking the essential measures for businesses. In today's world, everyone wants to keep their data protected, and they're becoming more aware of cybersecurity. As a result, these open source SIEM products can assist businesses in avoiding unaffordable costs.

There are lots of open-source technologies available. Such as,

1. Apache Metron.
2. AlienVault OSSIM.
3. MozDef.
4. OSSEC 13.
5. Wazuh.
6. Prelude OSS.
7. Snort.
8. Sagan.
9. ELK Stack.
10. SEIMonste.

1.4 Techniques

Security Operation Center (SOC) is a group of experts working to preventing data leakage and other cybersecurity risks. A SOC's role is to monitor, identify, investigate, and respond to all types of cyber threats [1]. In this paper, SOC is divided into two functions. First, fixing out security monitoring tools, and second, open-source tools. In these two situations, we find indemnity and safety through it. Also, we trace the ambiguous and distressed activity. In this paper, some necessary tools have been adapted to proceed with research. - VirtualBox/VMWare tools have been used here for software virtualization, which ensures that any virtual machine can be run with this [2].

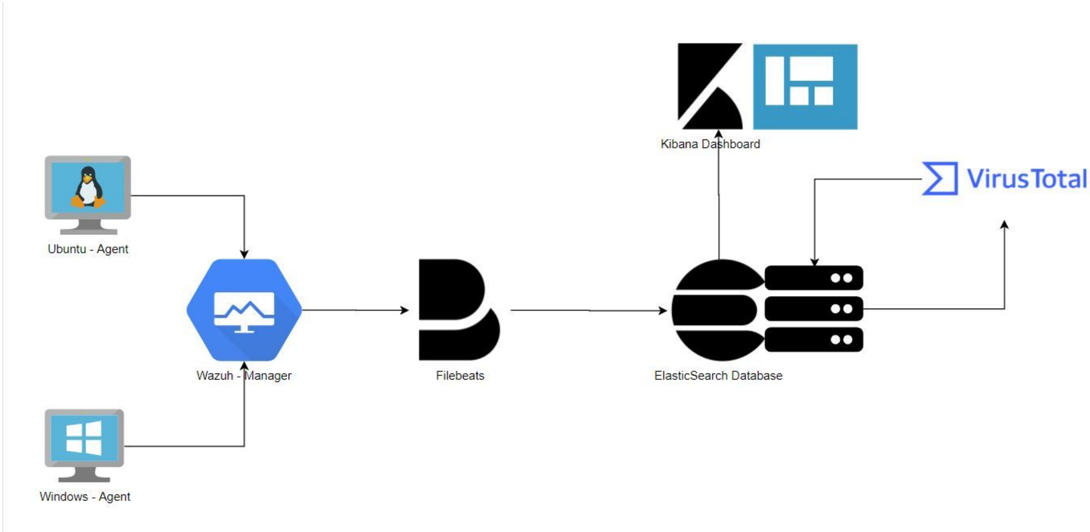


Figure 1.1: Network Infrastructure

Another one is Wazuh whose goal is to collect system logs from all of the agents belonging to the system. The best part of Wazuh is, that it can instruct the devices. Wazuh API is an open-source RESTful API that allows users to communicate with the Wazuh management via a web browser, a command-line tool such as cURL, or any script or program that can perform web calls [2]. Kibana Query Language (KQL) is a simple phrase for querying Elasticsearch data using either free text or field-based search. KQL is only used to filter data. It has no role for organizing or collecting it. As you type, KQL will suggest field names, values, and operators [4]. Elasticsearch, Logstash, and Kibana make up the ELK stack, which is an acronym for a stack made up of three major open-source projects. ELK Stack helps customers by providing a better basis that receives and processes data from several data sources, maintains it in a centralized data store that can scale as data evolves, and offers a variety of data analysis techniques [4]. The most widely used Open Source Intrusion Prevention System in the world is Snort (IPS). In order to detect dangerous network behavior, Snort IPS uses a collection of rules. It then applies those rules to find packets that match those requirements, issuing alerts for clients. [4].

1.5 Target Audience

On the market, plenty of paid SIEM software is available. However, they are very costly. For businesses, the expense might be very massive at times. The other difficulty is that businesses are not convinced enough of the benefits of open-source SIEM technology. Therefore, we mainly focused on mid-level industries as they do not often use any SIEM solutions for their company and for this reason they are mostly at risk at the current time. In such a situation, we came up with our solution which is providing free services to the companies as an alternative and our solutions can be customized as well which will create a huge impact on the industries.

1.6 Project Outline

There are 5 chapters in this project work. I presented the SOC in the first chapter using free source software. I covered the literature review for this study in chapter 2. The topics of simulation and analysis have been covered in chapter 3. The table of comparisons between largely relevant thesis works is included in Chapter 4. Finally, I came up with the conclusion and mentioned the future work scope in chapter 5.

Chapter 2

LITERATURE REVIEW

Nowadays, most industries need security to make sure their reliability, stability, and awareness. The more data is processed, the more risk it bears. As a result, to make the best implementation of an organization the safest way is prevention. Building security operations using open-source technology helps to get the solution of it.

This study analyses the possibilities of converting unfavorable Central Authentication Service (CAS) logs into useful data points by detecting anomalies using Elastic Stack (Filebeat, Logstash, Elasticsearch, and Kibana). Filebeat collects AS logs and forwards them to Logstash. In this paper, a pilot project utilizing Elastic Stack to process, convert, and analyze unused CAS data was presented in order to identify digital risks and strengthen cybersecurity. The paper described several forms of cyber threats that exist today, as well as the dangers they may create.
The paper also explained why and how the solution's bespoke Grok pattern was developed. The efficacy of the Kibana visualization tool was recorded in order to demonstrate how simple it was to consume CAS data after it had been structured. Furthermore, the efficiency of the Elasticsearch component was analyzed
[4].

Implementing a SOC for a company in our country is an expensive process. However, most companies fail to acknowledge the obstacles to implementing a SOC in their industries according to the individuals, methods, and expertise.

The research [3] came up with a solution for the integration problems that occur with introducing a SOC into a company. The obstacles of embedding a freshly constructed SOC through an association's data IT environment, including which workstations, processors, connection endpoints, software, and programs are hosted and web servers are employed, were covered in this study. Furthermore, the article also describes how to connect the SOC SIEM to the organization's system developed. Eventually, the paper highlights how to generate value for significant investments made in creating, building, and running a SOC.

Cybersecurity has been considered a vital issue for all industries as a result of cyberattacks. Due to limited funds, a lack of knowledge, and a lack of awareness of the risks that they will encounter, small to medium-sized organizations (SMEs) struggle to exercise appropriate network protection.

The research work [1] proposes SOC to improve industries' security with the techniques that are mentioned with triad PPT (Person, Process, and Technology). They have also implemented three SIEM tools (OSSIM, ELK, LogPoint) and showed differences among them. Moreover, the ideas that are mentioned here will help to know the usage of the tool for specific situations.

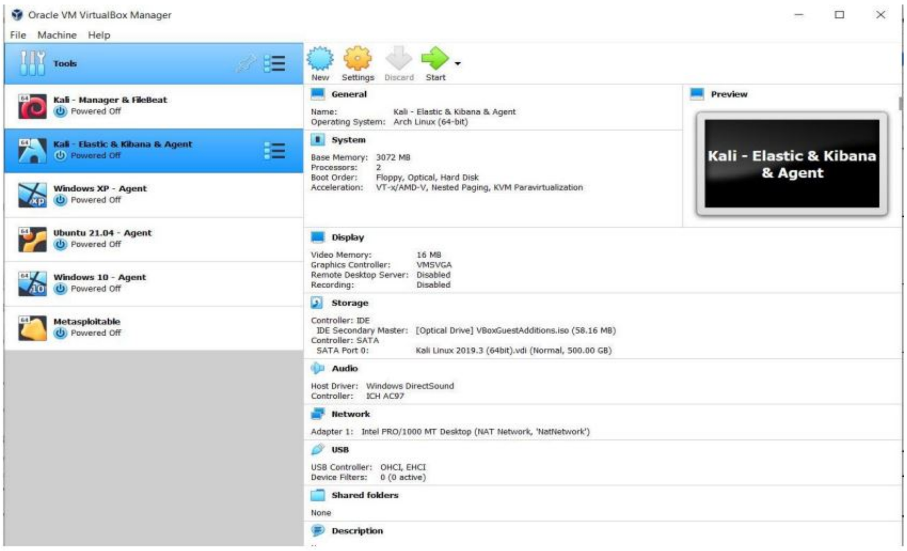
Security event correlation is fundamental to any SIEM system. The paper [6] talks about the current status of research in the security event correlation literature by conducting a comprehensive review of the literature over the past decade including publication year, knowledge extraction techniques, utilized data sources, architectural solutions, and quality assessment of correlation techniques. The datasets and metrics utilized here are quite rational and perfectly linked with security event correlation. In this paper, they explored and assessed the obstacles and improvements of techniques to building security event correlation in depth, although it might have been more explicit. Moreover, the research focuses on the possibilities of detecting unknown attacks, architectural solutions, and the usage of event-starting data which is quite interesting.

Chapter 3

SIMULATION AND ANALYSIS

3.1 Environment Setup

Ubuntu and Windows XP have been deployed as agents in the virtual box for network infrastructure. The Wazuh Manager collects the log data from the agents. The log data from the agents will be collected by it. Elasticsearch will get data from Filebeats. For passing data to Elasticsearch, there are several established rules. Elasticsearch is used to quickly and simultaneously store, search, and analyze vast amounts of data, with results arriving in milliseconds. Finally, data will be visualized using statistical features, graphs, scatter plots, graphical representations and established global capabilities in Kibana.



```
Kali - Manager & FileBeat
Powered Off
Kali - Elastic & Kibana & Agent
Powered Off
Windows XP - Agent
Powered Off
Ubuntu 21.04 - Agent
Powered Off
Windows 10 - Agent
Powered Off
Metasploitable
Powered Off
```

```
General
Name:              Kali - Elastic & Kibana & Agent
Operating System:  Arch Linux (64-bit)

System
Base Memory:   3072 MB
Processors:    2
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: IDE
  IDE Secondary Master:  [Optical Drive] VBoxGuestAdditions.iso (58.16 MB)
Controller: SATA
  SATA Port 0:           Kali Linux 2019.3 (64bit).vdi (Normal, 500.00 GB)

Audio
Host Driver:  Windows DirectSound
Controller:   ICH AC97

Network
Adapter 1:  Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

USB
USB Controller:  OHCI, EHCI
Device Filters:  0 (0 active)

Shared folders
None

Description
```

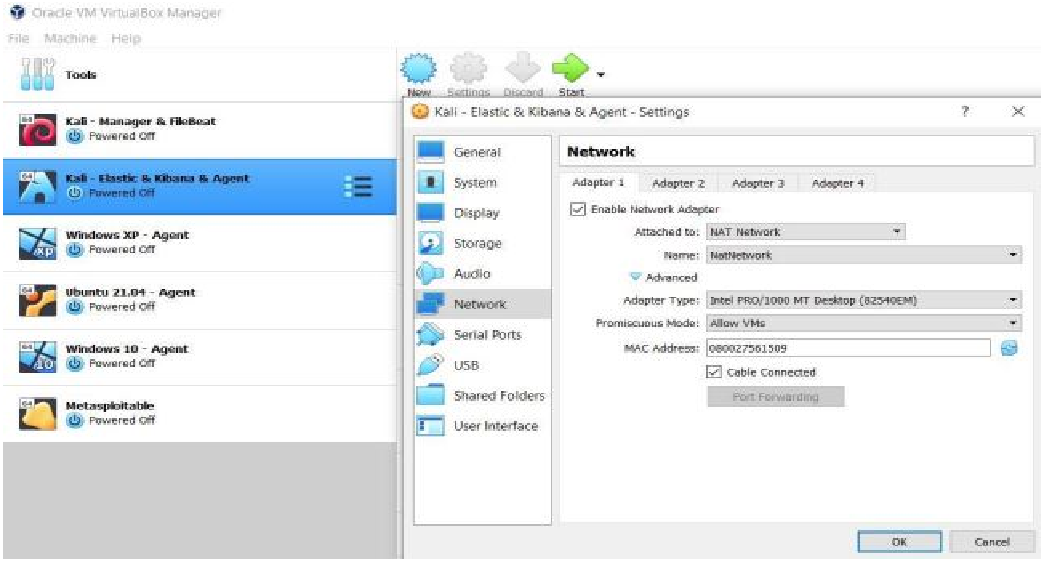
Figure 3.1: Oracle Virtual Box setup

We must consider the capabilities of our host system, since we are executing this lab setting on our own local platform. Our system, for example, has four cores and eight gigabytes of RAM. We'll install Wazuh manager and File Beats on one system (Kali) for improved RAM management, and ElasticSearch and Kibana on another Kali machine. There are two agents in total. The first is Windows 10, while the second is Ubuntu.

Machine	OS	RAM	CPU	IP
Agent-3	Kali Rolling x64, 2020.4	2GB	1	10.0.2.10
Elasticsearch and Kibana	Kali Linux x64, 2019.3	3GB	2	10.0.2.15
Agent-2	Ubuntu 21.04	1GB	1	10.0.2.15
Agent-1	Windows XP	1GB	1	10.0.2.9

Table 3.1: Machine Details

3.2 Machine Details



Kali - Elastic & Kibana & Agent - Settings

Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow VMs

MAC Address: 080027561509

☑ Cable Connected

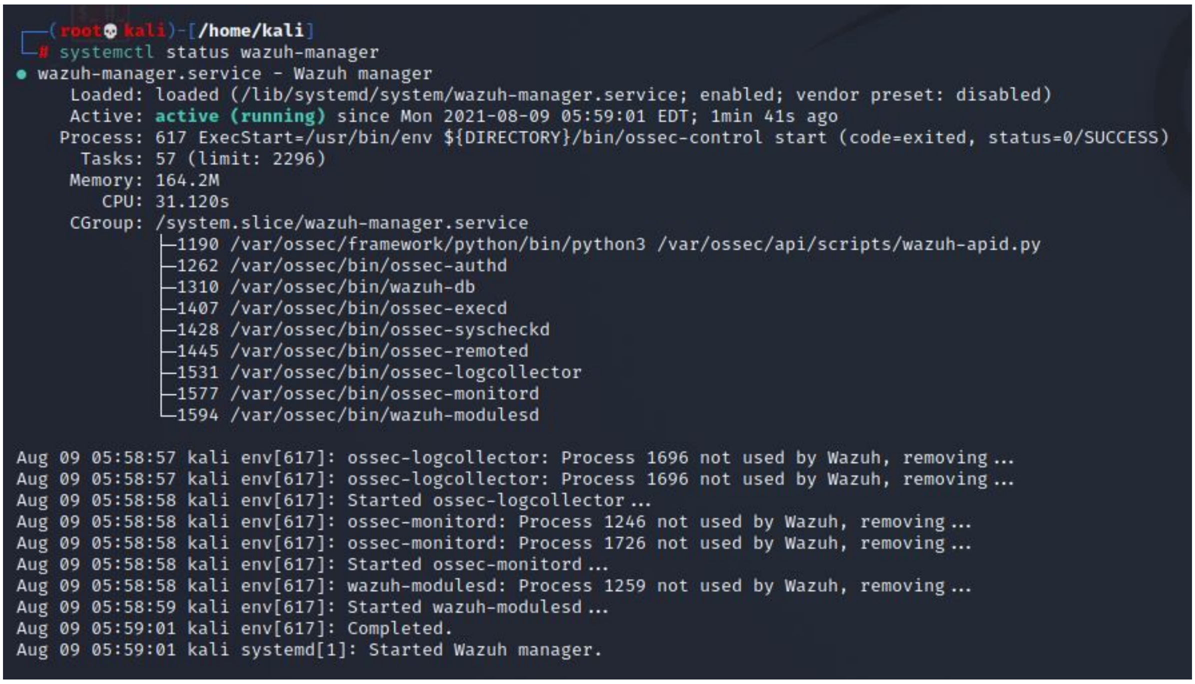
Figure 3.2: Elasticsearch, Kibana & Agent machine configuration

In below, it is showing the configuration of a Kali Machine which contains Wazuh-manager and Filebeat. The given RAM of this machine is 2GB, and it's taking 2 processors.

3.3 Setting Up Wazuh Manager

The framework known as the Wazuh manager monitors the data obtained from every single identified expert and notifies users when an incident exceeds an user to check. For instance, disruption discovered, document updated, layout not as specified, prospective malware and so on. The supervisor also serves as an expert on the neighborhood machine, which means it has all of the components that a specialist has. Furthermore, the director may advance the warnings that it generates through Syslog, messaging, or coordinated external APIs.

The Wazuh manager will use this network to gather log data from the agents, and wash manager will be the major store. Logs generated by agents will be saved at the wazuh manager. The Wazuh manager is run on a Kali Linux computer. The manager's IP address is 10.0.2.10.

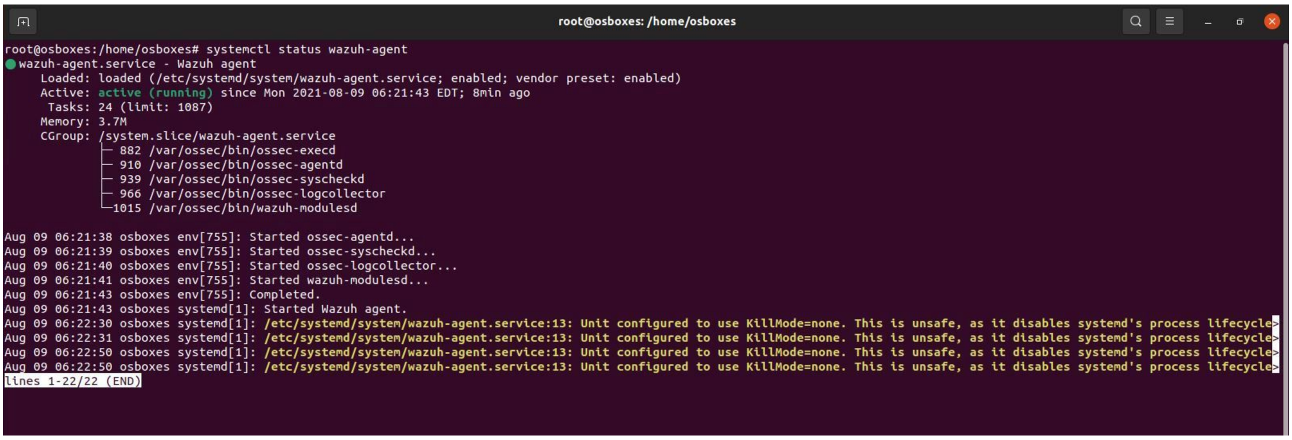


```
┌──(root💀kali)-[/home/kali]
└─# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: disabled)
     Active: active (running) since Mon 2021-08-09 05:59:01 EDT; 1min 41s ago
    Process: 617 ExecStart=/usr/bin/env ${DIRECTORY}/bin/ossec-control start (code=exited, status=0/SUCCESS)
      Tasks: 57 (limit: 2296)
     Memory: 164.2M
        CPU: 31.120s
     CGroup: /system.slice/wazuh-manager.service
             ├─1190 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1262 /var/ossec/bin/ossec-authd
             ├─1310 /var/ossec/bin/wazuh-db
             ├─1407 /var/ossec/bin/ossec-execd
             ├─1428 /var/ossec/bin/ossec-syscheckd
             ├─1445 /var/ossec/bin/ossec-remoted
             ├─1531 /var/ossec/bin/ossec-logcollector
             ├─1577 /var/ossec/bin/ossec-monitord
             └─1594 /var/ossec/bin/wazuh-modulesd

Aug 09 05:58:57 kali env[617]: ossec-logcollector: Process 1696 not used by Wazuh, removing ...
Aug 09 05:58:57 kali env[617]: ossec-logcollector: Process 1696 not used by Wazuh, removing ...
Aug 09 05:58:58 kali env[617]: Started ossec-logcollector ...
Aug 09 05:58:58 kali env[617]: ossec-monitord: Process 1246 not used by Wazuh, removing ...
Aug 09 05:58:58 kali env[617]: ossec-monitord: Process 1726 not used by Wazuh, removing ...
Aug 09 05:58:58 kali env[617]: Started ossec-monitord ...
Aug 09 05:58:58 kali env[617]: wazuh-modulesd: Process 1259 not used by Wazuh, removing ...
Aug 09 05:58:59 kali env[617]: Started wazuh-modulesd ...
Aug 09 05:59:01 kali env[617]: Completed.
Aug 09 05:59:01 kali systemd[1]: Started Wazuh manager.
```

Figure 3.3: Wazuh-manager active status

3.4 Ubuntu Agent

This Ubuntu machine serves as an agent for our system, as seen in Figure 6.

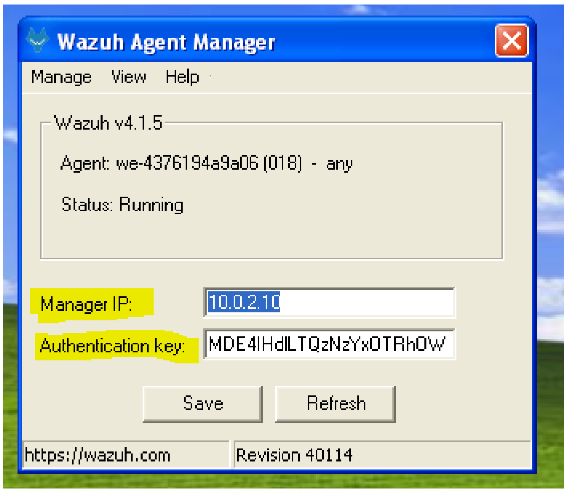


```
root@osboxes:/home/osboxes# systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/etc/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-08-09 06:21:43 EDT; 8min ago
      Tasks: 24 (limit: 1087)
     Memory: 3.7M
     CGroup: /system.slice/wazuh-agent.service
             ├─ 882 /var/ossec/bin/ossec-execd
             ├─ 910 /var/ossec/bin/ossec-agentd
             ├─ 939 /var/ossec/bin/ossec-syscheckd
             ├─ 966 /var/ossec/bin/ossec-logcollector
             └─1015 /var/ossec/bin/wazuh-modulesd

Aug 09 06:21:38 osboxes env[755]: Started ossec-agentd...
Aug 09 06:21:39 osboxes env[755]: Started ossec-syscheckd...
Aug 09 06:21:40 osboxes env[755]: Started ossec-logcollector...
Aug 09 06:21:41 osboxes env[755]: Started wazuh-modulesd...
Aug 09 06:21:43 osboxes env[755]: Completed.
Aug 09 06:21:43 osboxes systemd[1]: Started Wazuh agent.
Aug 09 06:22:30 osboxes systemd[1]: /etc/systemd/system/wazuh-agent.service:13: Unit configured to use KillMode=none. This is unsafe, as it disables systemd's process lifecycle>
Aug 09 06:22:31 osboxes systemd[1]: /etc/systemd/system/wazuh-agent.service:13: Unit configured to use KillMode=none. This is unsafe, as it disables systemd's process lifecycle>
Aug 09 06:22:50 osboxes systemd[1]: /etc/systemd/system/wazuh-agent.service:13: Unit configured to use KillMode=none. This is unsafe, as it disables systemd's process lifecycle>
Aug 09 06:22:50 osboxes systemd[1]: /etc/systemd/system/wazuh-agent.service:13: Unit configured to use KillMode=none. This is unsafe, as it disables systemd's process lifecycle>
lines 1-22/22 (END)
```

Figure 3.4: Ubuntu agent active status

3.5 Windows Agent

This Windows XP machine serves as a system agent, controlling all of the virtual machines in the system's 8 GB RAM. It might also be any Windows operating system.



Wazuh v4.1.5

Agent: we-4376194a9a06 (018) - any

Status: Running

Manager IP: 10.0.2.10

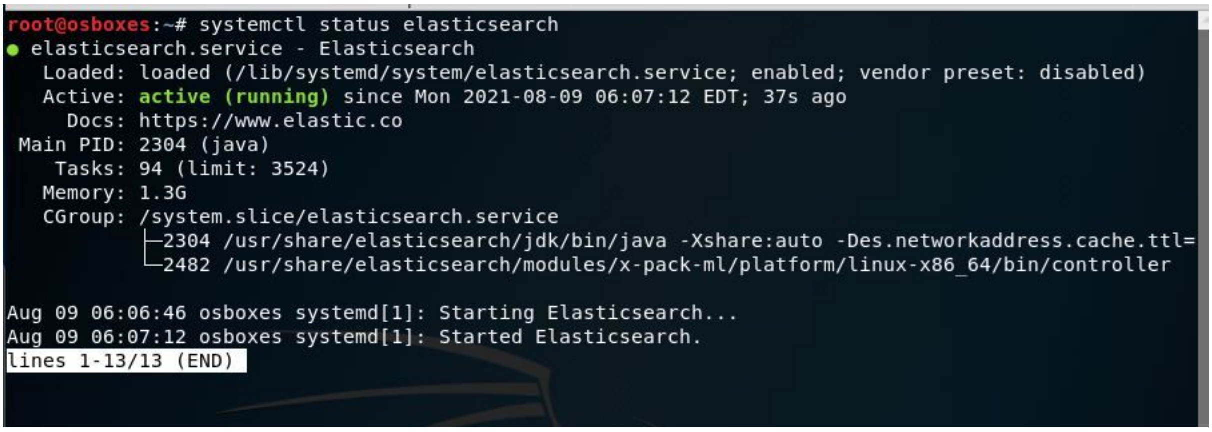
Authentication key: MDE4lHdLTQzNzYxOTRhOW

https://wazuh.com Revision 40114

Figure 3.5: Windows XP agent

3.6 Elasticsearch

Wazuh provides security visibility into your Docker hosts and compartments, monitoring their behavior and identifying hazards, flaws, and anomalies. Clients can see images, volumes, network settings, and operating compartments, thanks to the Wazuh agent's local coordination with the Docker motor.



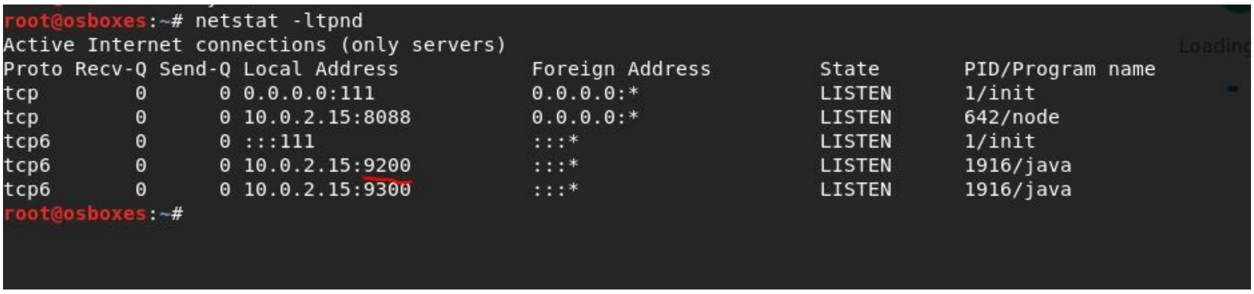
```
root@osboxes:~# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-08-09 06:07:12 EDT; 37s ago
     Docs: https://www.elastic.co
 Main PID: 2304 (java)
    Tasks: 94 (limit: 3524)
   Memory: 1.3G
   CGroup: /system.slice/elasticsearch.service
           ├─2304 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=
           └─2482 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Aug 09 06:06:46 osboxes systemd[1]: Starting Elasticsearch...
Aug 09 06:07:12 osboxes systemd[1]: Started Elasticsearch.
lines 1-13/13 (END)
```

Figure 3.6: Elasticsearch active status

Elasticsearch is working on the default port 9200.
The service is offered through 9200 ports, and the port is accessible.

3.7 Kibana

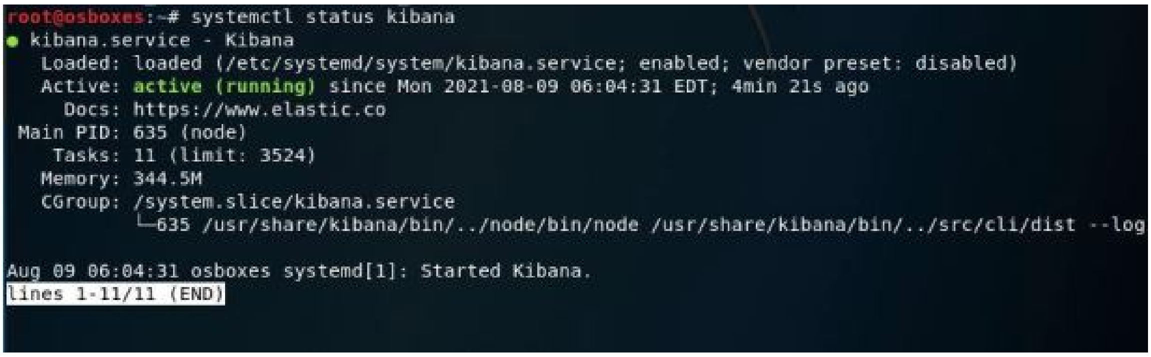
Kibana is just a software tool for data analysis and visualization that is commonly used for operational foresight use case scenarios, statistical models, and log evaluation. It has outstanding and user-friendly features including implicit geographic support, bar graphs, arc charts, graph patterns, and graphical representations. Using the Elastic Stack as its foundation, the free and open-source desktop implementation Kibana offers search functionality. Moreover, it shows data visualization



```
root@osboxes:~# netstat -ltpnd
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1/init
tcp        0      0 10.0.2.15:8088          0.0.0.0:*               LISTEN      642/node
tcp6       0      0 :::111                  :::*                    LISTEN      1/init
tcp6       0      0 10.0.2.15:9200          :::*                    LISTEN      1916/java
tcp6       0      0 10.0.2.15:9300          :::*                    LISTEN      1916/java
root@osboxes:~#
```

Figure 3.7: Netstat port scanning outcome

features for Elasticsearch-indexed data.



```
root@osboxes:~# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-08-09 06:04:31 EDT; 4min 21s ago
     Docs: https://www.elastic.co
 Main PID: 635 (node)
    Tasks: 11 (limit: 3524)
   Memory: 344.5M
   CGroup: /system.slice/kibana.service
           └─635 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --log

Aug 09 06:04:31 osboxes systemd[1]: Started Kibana.
lines 1-11/11 (END)
```

Figure 3.8: Kibana active status

3.8 SSL Certification

An SSL authentication is a data record made possible by a site's beginning point worker. SSL enables SSL/TLS encryption and include the site's public key and character, as well as associated data.

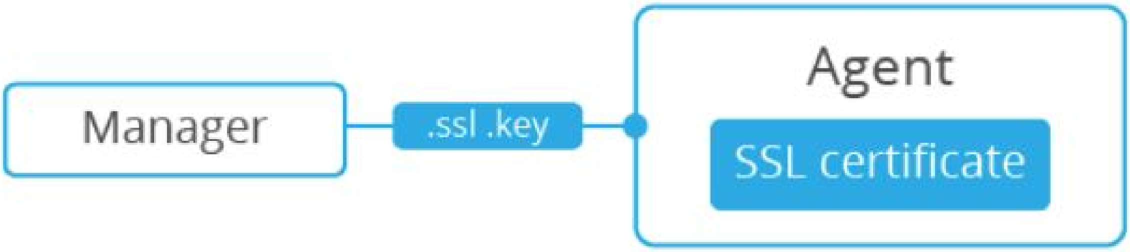


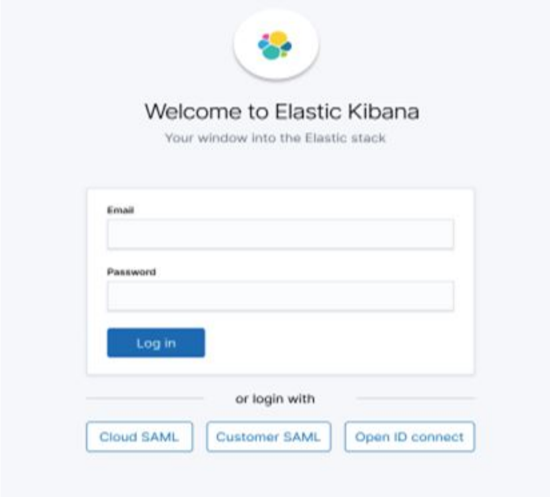
Figure 3.9: Infrastructure for Secure Sockets Layer (SSL)

3.9 File Integrity Monitoring

A file integrity monitoring tool is one of the most fundamental PCI-DSS consistency requirements for the viability of a security program. As complex systems and organizations evolve, it is possible to become resistant to PCI principles in a surprising amount of time. Your firm's organization is dynamic, which is why organizations nowadays want arrangements that operate continually to assess and eliminate security risks. However, before you invest in consistency and security, you should first understand what document uprightness checking is and how it works.

3.10 Secure Sockets Layer

A technical assertion known as an SSL certificate ensures the integrity of a website and facilitates a data communication. Secure Sockets Layer, or SSL, is a security protocol which creates a secure connection between a web server and a desktop.



Welcome to Elastic Kibana

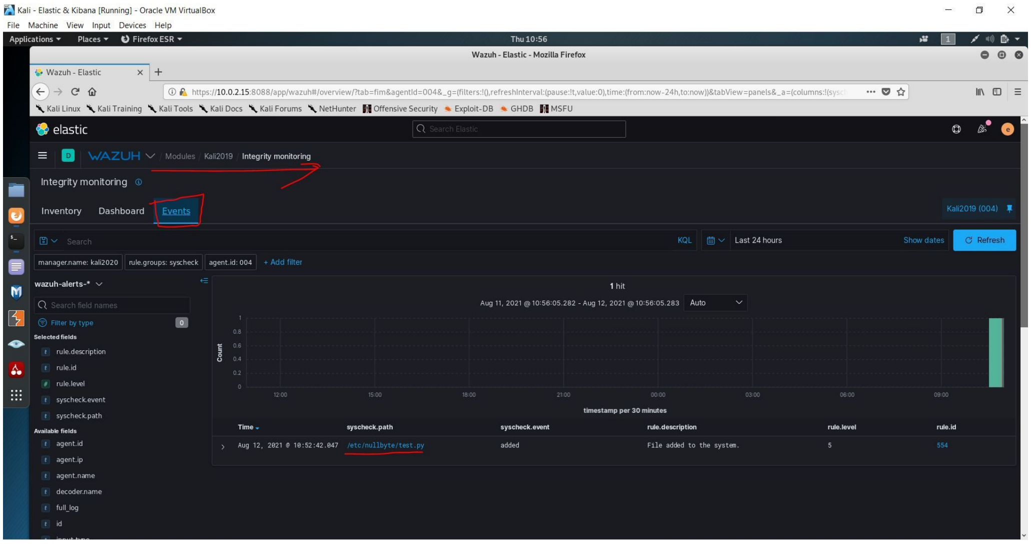
Your window into the Elastic stack

Figure 3.10: Login to the dashboard of Elastic Kibana

After successfully setting everything, the Kibana dashboard is ready to go. Login credentials must be needed to access the site.

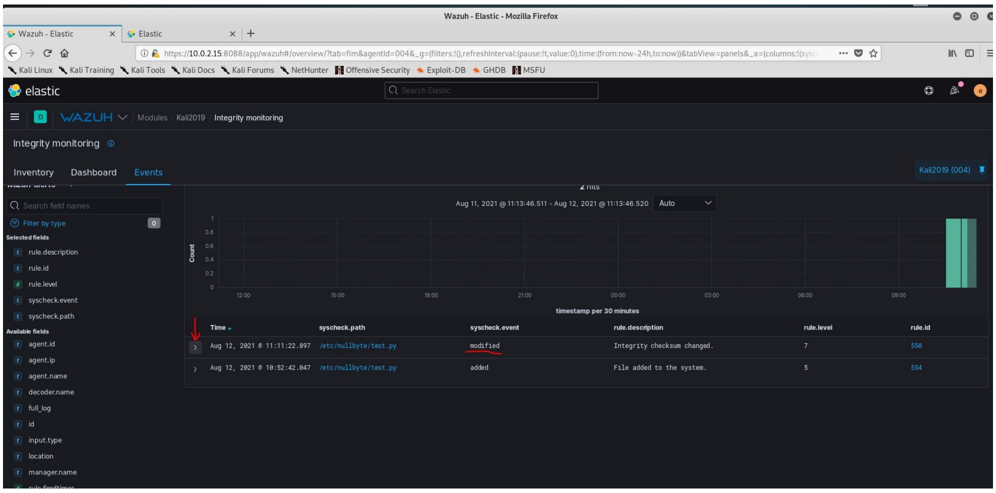
3.11 Events check from the dashboard

Kibana dashboard will notify us in the event that we make a contribution to our repository. The software has visuals in a number of different areas. The data are first organized into distinct categories using a filter to provide information for the signals, and then they are displayed as figures, scatter plots, statistics, and so on. You can use the majority of the app's visualizations, which are interactive, to narrow down your search to more specific alert fields or to a specific time frame by clicking and dragging to select a time period. The fact that the majority of the visualizations in the program are interactive allows for this.



Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Aug 12, 2021 @ 10:52:42.047	/etc/nullbyte/test.py	added	File added to the system.	5	554

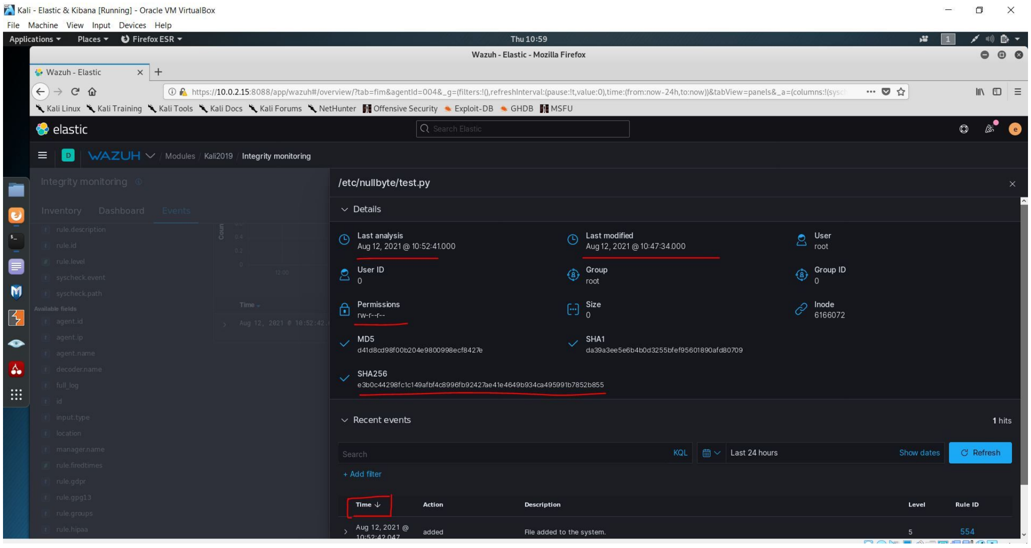
Figure 3.11: Event logs from a dashboard



Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Aug 12, 2021 @ 11:11:22.897	/etc/nullbyte/test.py	modified	Integrity checksum changed.	7	550
Aug 12, 2021 @ 10:52:42.047	/etc/nullbyte/test.py	added	File added to the system.	5	554

Figure 3.12: Modified event logs from dashboard

If we make a change or modification anything in our repository, it will also be reflected in the corresponding section of our Kibana dashboard.



/etc/nullbyte/test.py

Details

Last analysis Aug 12, 2021 @ 10:52:41.000	Last modified Aug 12, 2021 @ 10:47:34.000	User root
User ID 0	Group root	Group ID 0
Permissions rw-r--r--	Size 0	Inode 6166072
MD5 d41d8cd98f00b204e9800998ecf8427e	SHA1 da39a3ee5e6b4b0d3255bfef95601890afd80709	
SHA256 e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855		

Recent events

1 hits

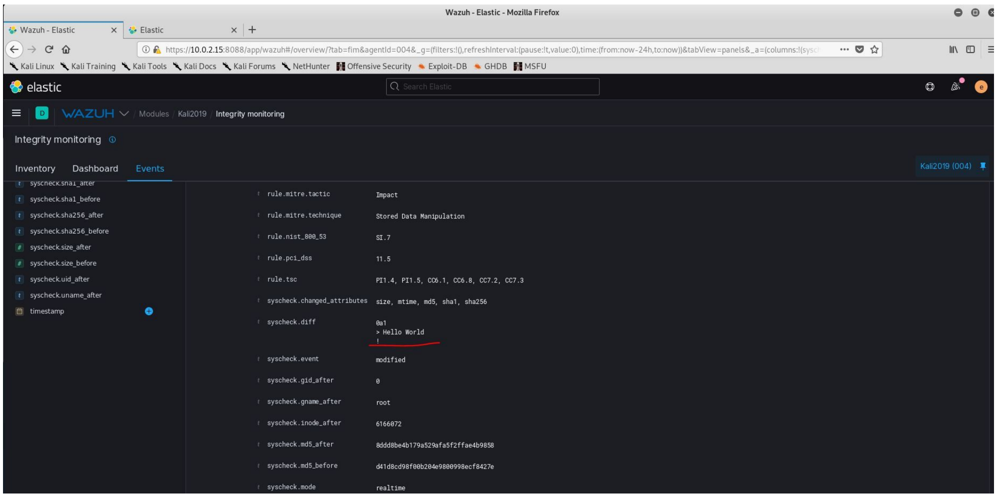
Last 24 hours

Time	Action	Description	Level	Rule ID
Aug 12, 2021 @ 10:52:42.047	added	File added to the system.	5	554

Figure 3.13: Details of event logs from dashboard

A change was made in the repository, and the dashboard is now displaying the event as a notification of the change.

Details about file modifications, such as the date and time of the most recent change, the identity of the person making the change, and the file's hash value, are included here.



```
rule.mitre.tactic              Impact
rule.mitre.technique           Stored Data Manipulation
rule.nist_800_53               SI.7
rule.pci_dss                   11.5
rule.tsc                       PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3
syscheck.changed_attributes    size, mtime, md5, sha1, sha256
syscheck.diff                  0a1
                               > Hello World
                               !
syscheck.event                 modified
syscheck.gid_after             0
syscheck.gname_after           root
syscheck.inode_after           6166072
syscheck.md5_after             8ddd8be4b179a529afa5f2ffae4b9858
syscheck.md5_before            d41d8cd98f00b204e9800998ecf8427e
syscheck.mode                  realtime
```

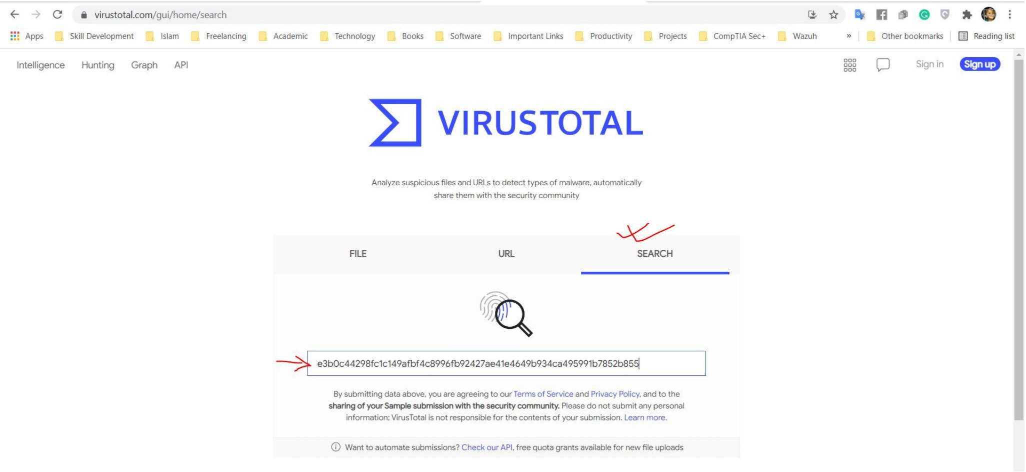
Figure 3.14: Event logs modification-specific data from the dashboard

Modification: What exactly was the change that is able to be illustrated? The alteration that was made for that specific event was a string that said ”Hello World.”

3.12 Integrity Check with Virustotal

Our data integrity can be manually verified using the virustotal website or equivalent programs.

VirusTotal integrates several antivirus products and web sweep engines to look for viruses that the client's own antivirus may have missed, as well as to validate against any false positives. Documents up to 650MB in size can be transferred to the site or delivered through email (maximum 32MB). Antivirus software providers can receive copies of files detected by other sweeps but cleared by their own engine in order to improve the functioning of both their own product and VirusTotal. Customers may also examine rumored URLs and search the VirusTotal database. For dynamic malware analysis, VirusTotal makes use of the Cuckoo Sandbox.



virustotal.com/gui/home/search

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

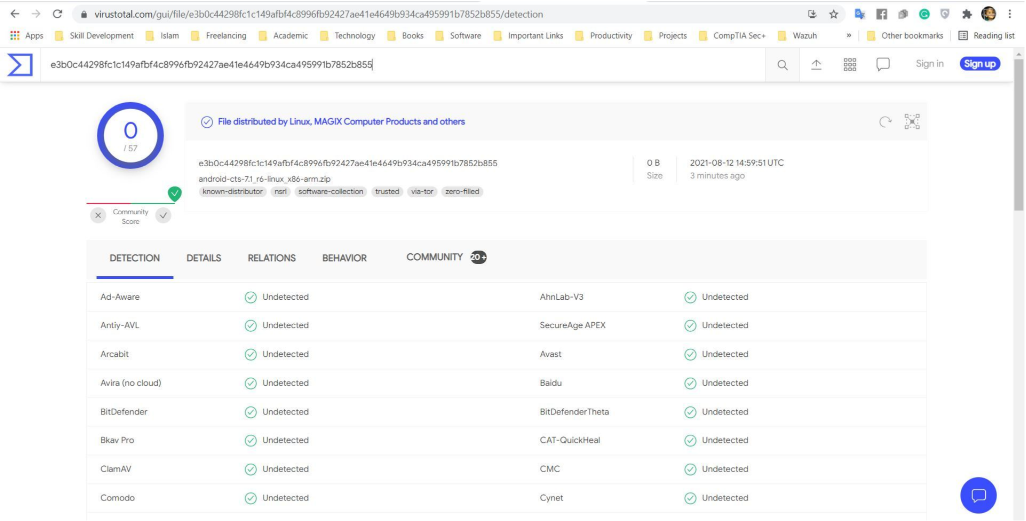
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads

Figure 3.15: VirusTotal interface

Pasting the SHA256 value in the VIRUSTOTAL SEARCH box.



virustotal.com/gui/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/detection

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

0
/ 57

File distributed by Linux, MAGIX Computer Products and others

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
android-cts-7.1_r6-linux_x86-arm.zip
known-distributor nsrl software-collection trusted via-tor zero-filled

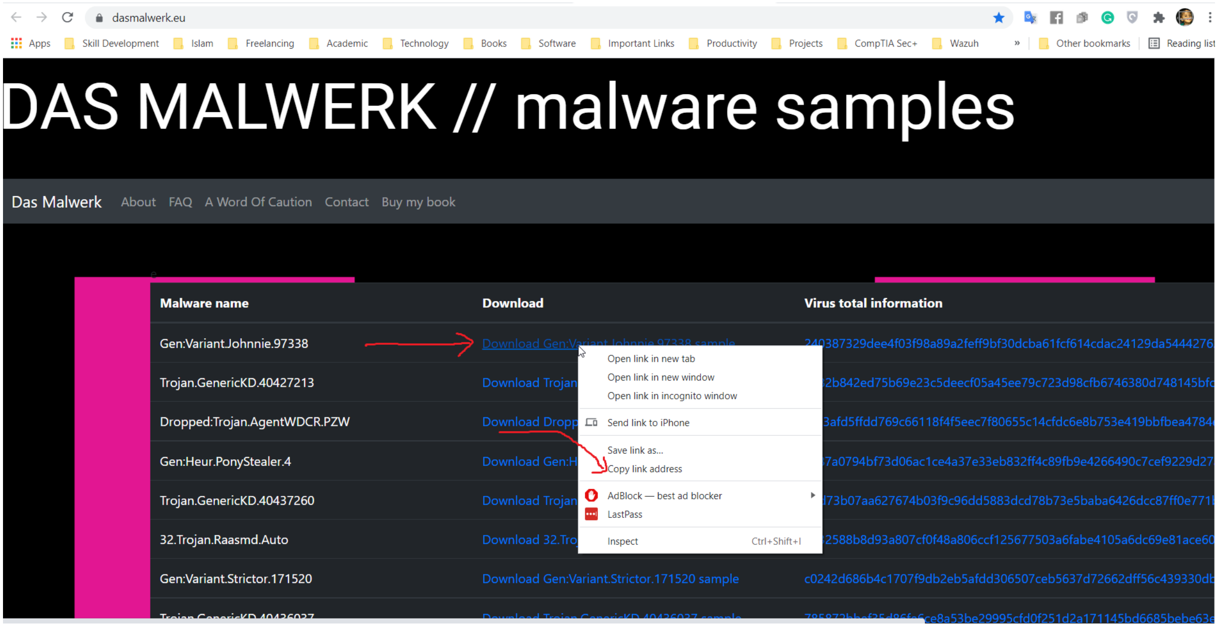
0 B
Size

2021-08-12 14:59:51 UTC
3 minutes ago

Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected
Antiy-AVL	✓ Undetected	SecureAge APEX	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	Cynet	✓ Undetected

Figure 3.16: VirusTotal result

The result shows the integrity status of this file. For that case, it's showing that the searched file was not malware.

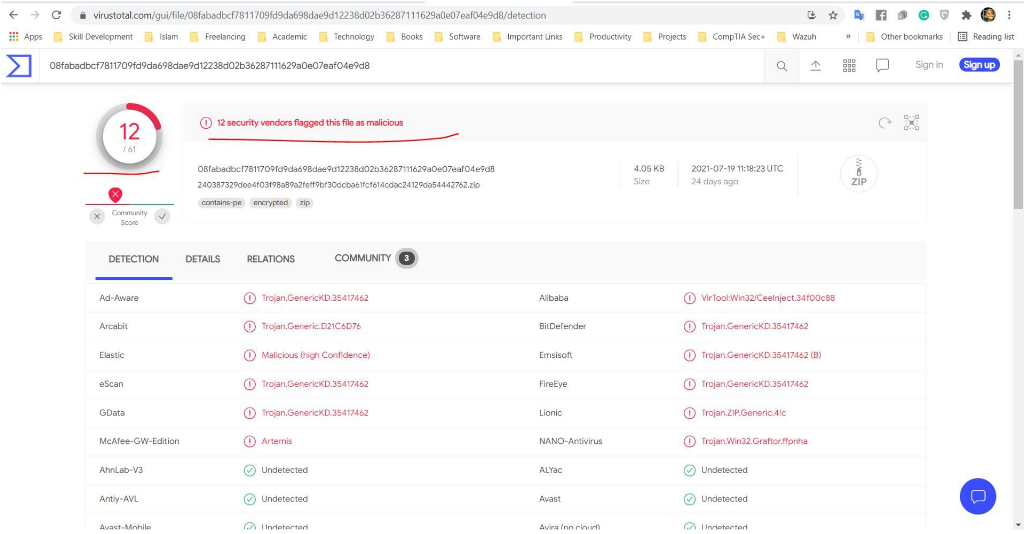


DAS MALWERK // malware samples

Malware name	Download	Virus total information
Gen:Variant.Johnnie.97338	Download Gen:Variant.Johnnie.97338 sample	240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da5444276
Trojan.GenericKD.40427213	Download Trojan	2b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc
Dropped:Trojan.AgentWDCR.PZW	Download Dropp	3afd5ffdd769c66118f4f5eec7f80655c14cfdc6e8b753e419bbfbea4784
Gen:Heur.PonyStealer.4	Download Gen:H	7a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27
Trojan.GenericKD.40437260	Download Trojan	l73b07aa627674b03f9c96dd5883dcd78b73e5baba6426dcc87ff0e771
32.Trojan.Raasmd.Auto	Download 32.Tro	2588b8d93a807cf0f48a806ccf125677503a6fabe4105a6dc69e81ace60
Gen:Variant.Strictor.171520	Download Gen:Variant.Strictor.171520 sample	c0242d686b4c1707f9db2eb5afdd306507ceb5637d72662dff56c439330db
Trojan.GenericKD.40436037	Download Trojan.GenericKD.40436037 sample	785872bbaf35d86fa6ce8a53be29995cfd0f251d2a171145bd6685bebe63e

Figure 3.17: Das Malwerk malware website

For real-life intrusion detection, a malware file has been downloaded from this site. Das Malware is a renowned website where already exposed malware is available.



08fabadbcf7811709fd9da698dae9d12238d02b36287111629a0e07eaf04e9d8

12 security vendors flagged this file as malicious

08fabadbcf7811709fd9da698dae9d12238d02b36287111629a0e07eaf04e9d8
240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762.zip
contains-pe encrypted zip

4.05 KB
Size

2021-07-19 11:18:23 UTC
24 days ago

DETECTION DETAILS RELATIONS COMMUNITY 3

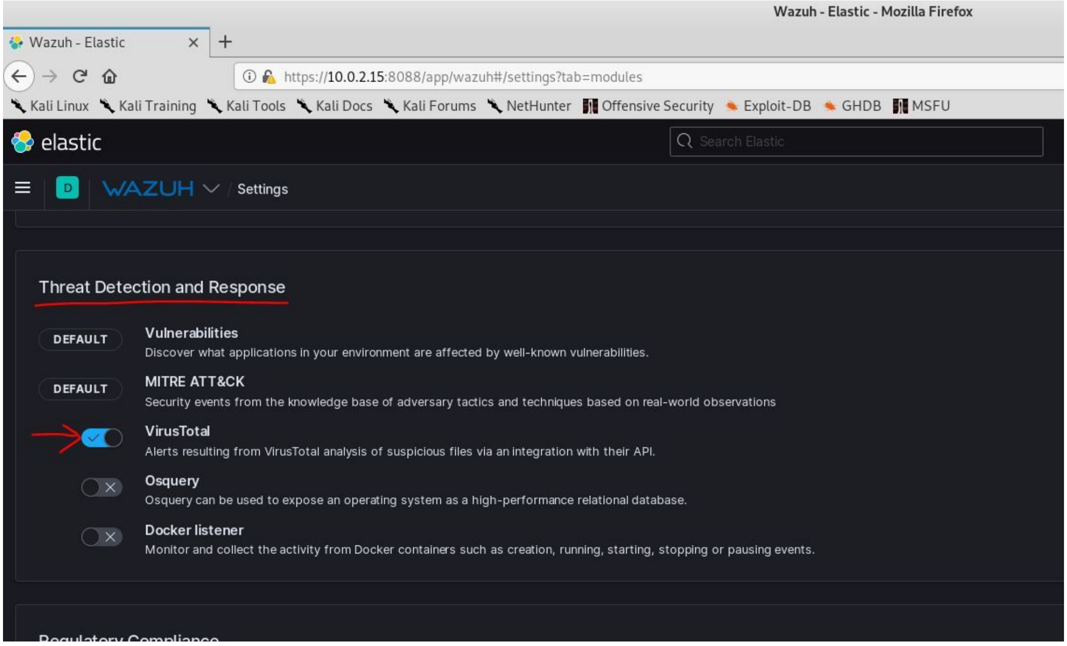
Ad-Aware	Trojan.GenericKD.35417462	Alibaba	VirTool:Win32/CeeInject.34f00c88
Arcabit	Trojan.Generic.D21C6D76	BitDefender	Trojan.GenericKD.35417462
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.GenericKD.35417462 (B)
eScan	Trojan.GenericKD.35417462	FireEye	Trojan.GenericKD.35417462
GData	Trojan.GenericKD.35417462	Lionic	Trojan.ZIP.Generic.4!c
McAfee-GW-Edition	Artemis	NANO-Antivirus	Trojan.Win32.Graftor.ffpnha
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Avast	✓ Undetected
Avast-Mobile	✓ Undetected	Avira (no cloud)	✓ Undetected

Figure 3.18: Virustotal infected files result

The virus has been downloaded in a directory. Wazuh generates an alarm, which is shown on the dashboard. This is the hash value of this specific alteration as tested by virustotal. The outcome indicates that this file is malware.

3.13 Integrity Check Automation

First virustotal option should be turned ON from the setting



Threat Detection and Response

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

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

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

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

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

Regulatory Compliance

Figure 3.19: Turning on the VirusTotal option

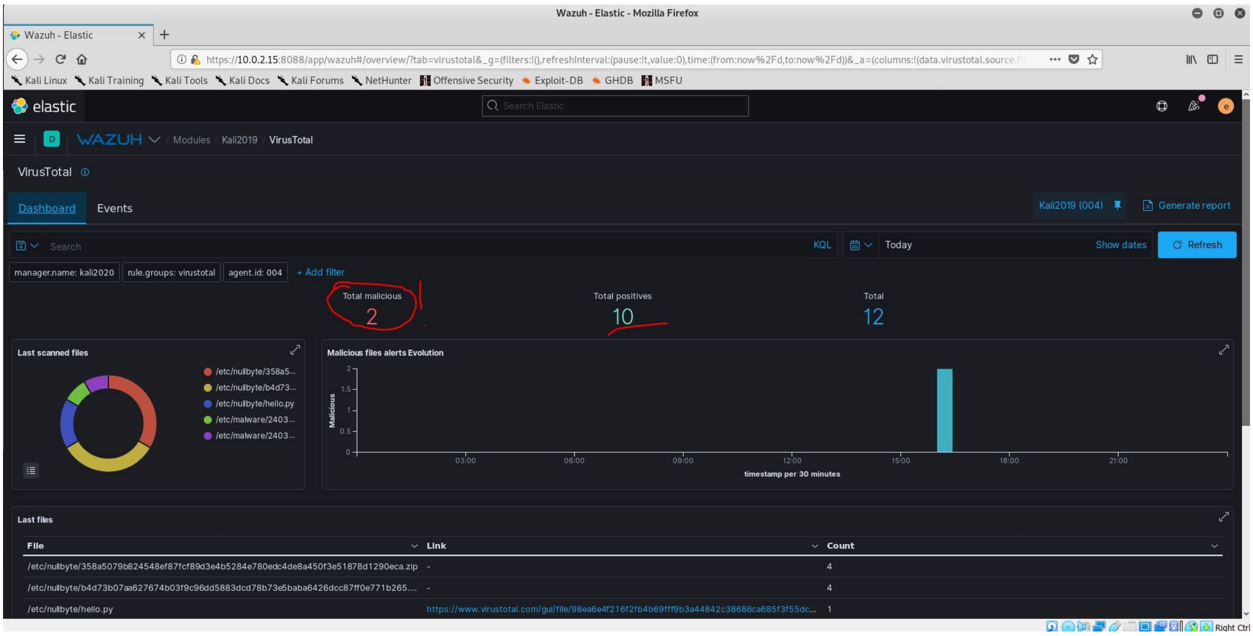
Virustotal option Turning on from the setting - Threat Detection and Response.

After finishing the automation process, this system may automatically recognize virus-affected/malware files. The outcome can be seen in the security events dashboard. The whole File Integrity result is shown in this figure.

3.14 Active Response

Active Response decreases the resources required to identify hazards from unidentified programs running on endpoints by supplying information about possibly malicious activities. Active Response enables you to respond to shared threat data with streamlined workflows by integrating file reputation. You can quickly address a danger and put preventative measures in place to thwart such attacks.

Active Response, Threat Intelligence Exchange, and Data Exchange Layer work in concert to reduce the time between an advanced targeted attack's initial contact and its eventual containment from days, weeks, or months to just a few seconds.



Total malicious 2

Total positives 10

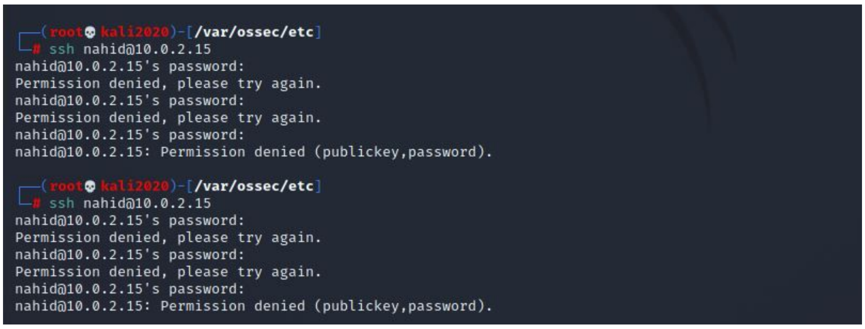
Total 12

File	Link	Count
/etc/nullbyte/358a5079b824548ef87fcf89d3e4b5284e780edc4de8a450f3e51878d1290eca.zip	-	4
/etc/nullbyte/b4d73b07aa627674b03f9c96dd5883dcd78b73e5baba6426dcc87ff0e771b265....	-	4
/etc/nullbyte/hello.py	https://www.virustotal.com/gui/file/98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc...	1

Figure 3.20: VirusTotal security dashboard

3.15 Case Scenario

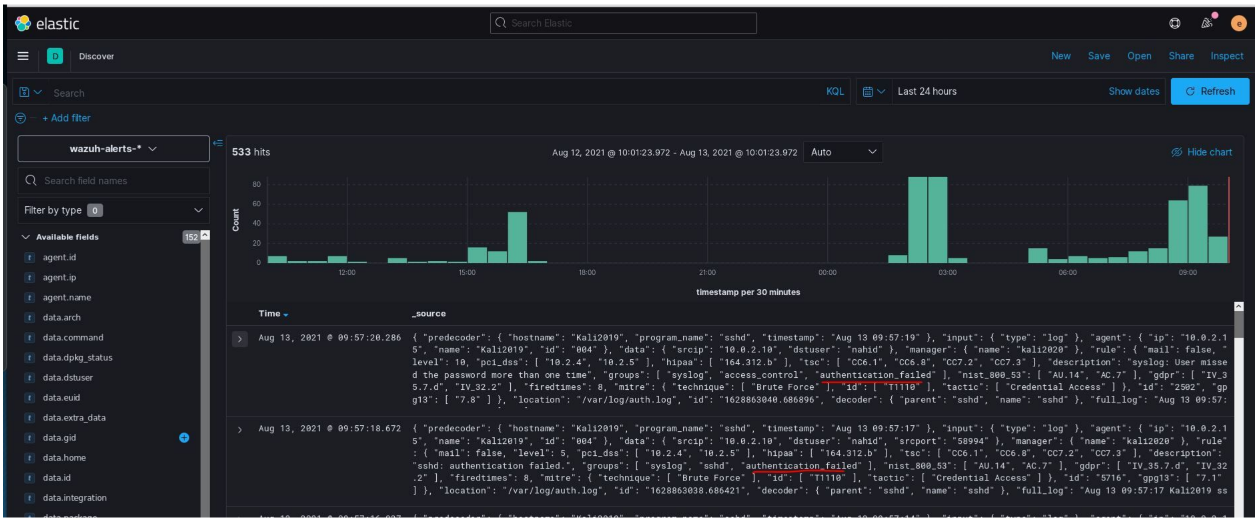
From another machine, if someone tries to access this particular machine with wrong privilege, the targeted machine is denied access first. Then, after several wrong attempts, the attacker machine will be banned/blocked for any duration of the time that can be defined by the admin.



```
┌──(root💀kali2020)-[/var/ossec/etc]
└─# ssh nahid@10.0.2.15
nahid@10.0.2.15's password:
Permission denied, please try again.
nahid@10.0.2.15's password:
Permission denied, please try again.
nahid@10.0.2.15's password:
nahid@10.0.2.15: Permission denied (publickey,password).

┌──(root💀kali2020)-[/var/ossec/etc]
└─# ssh nahid@10.0.2.15
nahid@10.0.2.15's password:
Permission denied, please try again.
nahid@10.0.2.15's password:
Permission denied, please try again.
nahid@10.0.2.15's password:
nahid@10.0.2.15: Permission denied (publickey,password).
```

Figure 3.21: Access a computer remotely

While attacking the targeted machine, permission was denied all the time. Authentication problem information is displayed in event logs. This data may be used to track down the attacker's IP address, location and machine. The server will first block the user for a few minutes before unblocking them again. This is because some legitimate users may have forgotten their authentication credentials. The system will unblock them for safety reasons. However, if they try again with the same incorrect credentials, the system will block them for a few more attempts. This time system, for example, may prohibit this user for 1 hour. That is how it works.



```
Aug 13, 2021 @ 09:57:20.286  { "predecoder": { "hostname": "Kali2019", "program_name": "sshd", "timestamp": "Aug 13 09:57:19" }, "input": { "type": "log" }, "agent": { "ip": "10.0.2.1
                             5", "name": "Kali2019", "id": "004" }, "data": { "srcip": "10.0.2.10", "dstuser": "nahid" }, "manager": { "name": "kali2020" }, "rule": { "mail": false, "
                             level": 10, "pci_dss": [ "10.2.4", "10.2.5" ], "hipaa": [ "164.312.b" ], "tsc": [ "CC6.1", "CC6.8", "CC7.2", "CC7.3" ], "description": "syslog: User misse
                             d the password more than one time", "groups": [ "syslog", "access_control", "authentication_failed" ], "nist_800_53": [ "AU.14", "AC.7" ], "gdpr": [ "IV_3
                             5.7.d", "IV_32.2" ], "firedtimes": 8, "mitre": { "technique": [ "Brute Force" ], "id": [ "T1110" ], "tactic": [ "Credential Access" ] }, "id": "2502", "gp
                             g13": [ "7.8" ] }, "location": "/var/log/auth.log", "id": "1628863040.686896", "decoder": { "parent": "sshd", "name": "sshd" }, "full_log": "Aug 13 09:57:

Aug 13, 2021 @ 09:57:18.672  { "predecoder": { "hostname": "Kali2019", "program_name": "sshd", "timestamp": "Aug 13 09:57:17" }, "input": { "type": "log" }, "agent": { "ip": "10.0.2.1
                             5", "name": "Kali2019", "id": "004" }, "data": { "srcip": "10.0.2.10", "dstuser": "nahid", "srcport": "58994" }, "manager": { "name": "kali2020" }, "rule"
                             : { "mail": false, "level": 5, "pci_dss": [ "10.2.4", "10.2.5" ], "hipaa": [ "164.312.b" ], "tsc": [ "CC6.1", "CC6.8", "CC7.2", "CC7.3" ], "description":
                             "sshd: authentication failed.", "groups": [ "syslog", "sshd", "authentication_failed" ], "nist_800_53": [ "AU.14", "AC.7" ], "gdpr": [ "IV_35.7.d", "IV_32
                             .2" ], "firedtimes": 8, "mitre": { "technique": [ "Brute Force" ], "id": [ "T1110" ], "tactic": [ "Credential Access" ] }, "id": "5716", "gpg13": [ "7.1"
                             ] }, "location": "/var/log/auth.log", "id": "1628863038.686421", "decoder": { "parent": "sshd", "name": "sshd" }, "full_log": "Aug 13 09:57:17 Kali2019 ss
```

Figure 3.22: Active Response events log

Chapter 4

AN EVALUATION AND COMPARISON OF SIEM INTELLIGENCE

4.1 SIEM INTELLIGENCE COMPARISON AND ANALYSIS

There is a work that is extremely comparable to the task that I do. We are going to evaluate them side by side and compare them. After that we will identify the most important difference between our two systems. The infrastructure that follows pertains to the job that they do.

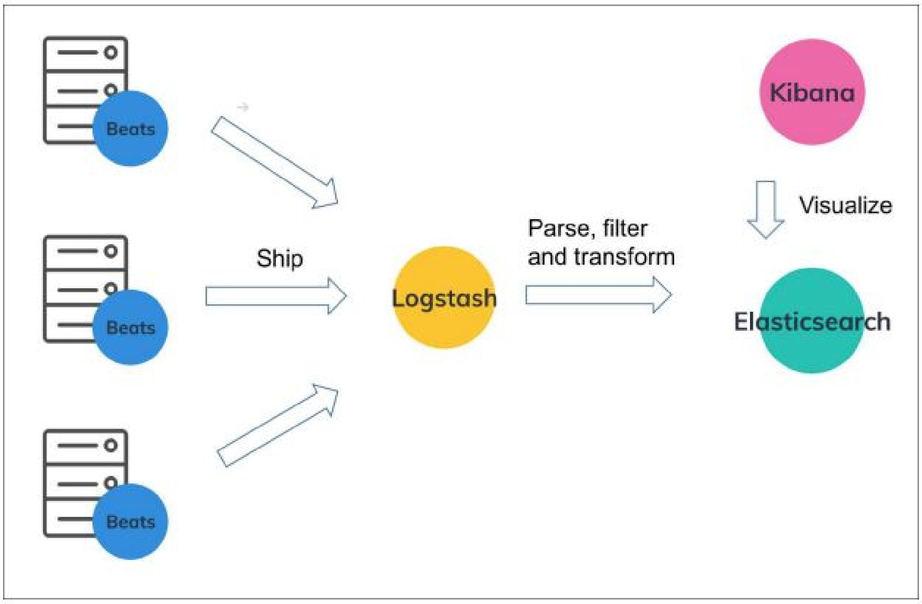


Figure 4.1: Threat identification using elastic stack workflow diagram

In this setup, Filebeats collects log data directly from the agents. After the collection is complete, Filebeats sends the information to Logstash.

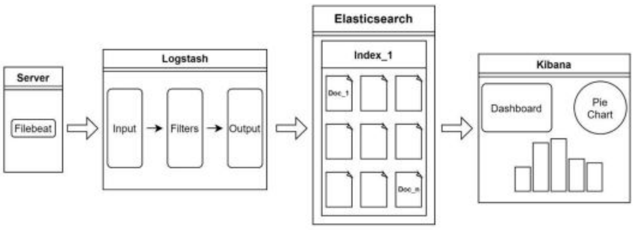


Figure 4.2: Elastic stack pipeline

Logstash receives the data as inputs, processes them by applying filters, and then transmits them to Elasticsearch. Elasticsearch was responsible for indexing the data, and then it sent them to Kibana so that the dashboard could be shown.

On the other hand, if we take a look at the diagram of our system, we can see that:

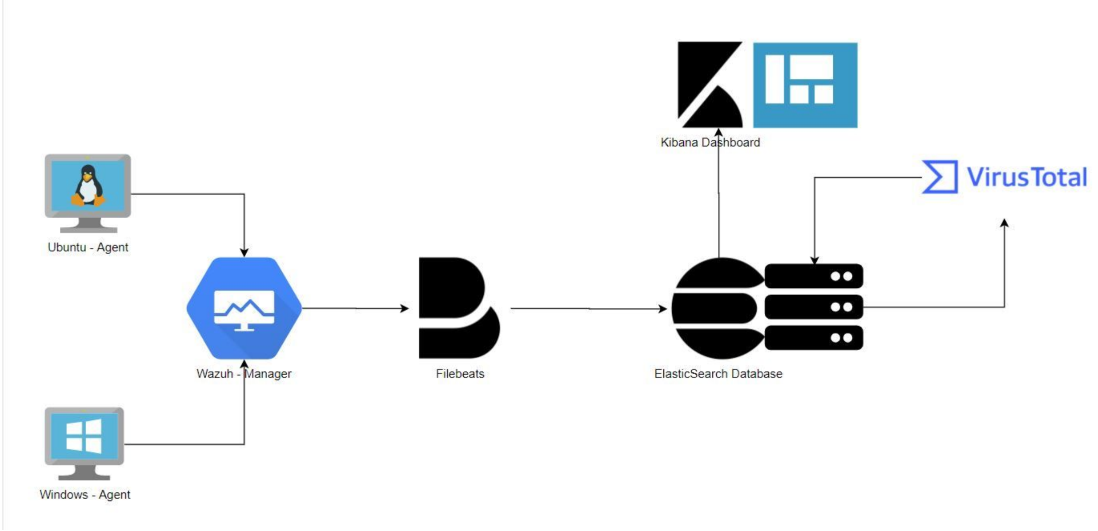


Figure 4.3: VirusTotal flowchart.

Wazuh management is currently gathering data from the agents. While sending events and alerts to Elasticsearch, Filebeat works in cooperation with Wazuh Manager to accomplish this task. Elasticsearch receives the results of the Virustotal file integrity check after receiving the events from Virustotal. After that, the data are sent from Elasticsearch to Kibana so that it may be seen.

The following is a list of the primary distinctions between our system and theirs:

- **Intelligence:** Their organizational structure is quite straightforward and simple. Taking the agent log and simply visualizing it on the dashboard. There is no sign of intellect there at all. To provide one example, what do the user's actions based on the log data really mean? On the other hand, our system is equipped with a Wazuh-manager that performs analyses of security data in order to identify intrusions, threats, and abnormalities in behavioral patterns.

- **Complete SIEM solution:** According to what we know, a good SIEM system should feature these which are given below

  - Safety Measures for Containers

  - Maintaining Compliance with Regulations

  - Incident Response.

  - Safety in Cloud.

  - Detection of Unauthorized Access.

  - Log Data Analysis.

  - Configuration Assessment.

  - Analytical Measures for Safety.

  - Monitoring of file's integrity.

  - Identification of Weaknesses and Exposures.

  The Wazuh manager meets all of the requirements for a SIEM solution. In our setup, the Wazuh manager is the one who is responsible for all of the tasks. For a SIEM solution to be considered optimum, the following feature absolutely need to be included in the system.

- **Alert:** A Wazuh manager determines whether or not alerts are necessary by doing analysis on the data included in the logs. The Wazuh manager is proficient of finding inspection information.

- **Malware Detection File Integrity:** The well-known malware detection technology Virustotal assists the system recognize harmful malware files, and there is a dedicated dashboard panel that highlights the files that have been contaminated by the virus. Now the whole of the process is mechanized. Virustotal's application programming interface (API) has been included into our system.

- **Authentication:** Our technology is able to recognize the DDOS assault. After three unsuccessful attempts to log in with the incorrect password, the system will temporarily block the IP address of the user who is suspected of being the intruder. We are not going to permanently restrict the user's IP address, since it is possible for legitimate users to forget their passwords.

- **Incident Response:** When there is a problem with the system, the wazuh manager will step up to the plate as quickly as possible to take responsibility for fixing it. It's almost like a one-stop shop for services. The problem will be discovered by the manager in a short amount of time, an alert will be sent, virustotal will scan this file, and appropriate action will be performed.

- **Filebeat vs Logstash:** Both Filebeat and Logstash are capable of transferring logs that originate from a file-based data source to an output destination that is supported. Filebeat, a logstash-integrated service, manages the system's data gathering and filtering operations. However, in our system, we have only ever utilized filebeat to send data to elasticsearch. The most significant distinction between them is that Filebeat is said to be "A lightweight shipper for transporting and centralizing log data." It provides a lightweight method to forward and consolidate logs and data, which allows you to keep the basic things simple, which is quite helpful. On the other hand, Logstash is described as having the ability to "Collect, Parse, and Enrich Data."

4.2 Comparison Table

This table shows the differences between our work and existing work.

Our Work	Existing Work
The Wazuh Manager collects data from the agent.	The Filebeats take data directly from the agent.
Filebeats is used in conjunction with Wazuh Manager.	Filebeats is used to collect the data.
No Logstash is used here.	Filebeats send the data to Logstash.
Wazuh Manager sends the data to Elasticsearch.	Logstash filters the data and sends the data to Elasticsearch.
Virustotal takes the data for integrity check and returns it to Elasticsearch.	Virustotal is not used here.
Our system applied Intelligence.	No Intelligence is used here.
After analyses and taking proper action the collected data are sent for visualization.	Only visualize the log data without taking any action.
Our system has the capability of locating audit files.	No capability of locating audit files.
Our technology can recognize the DDOS assault.	There is no user recognition functionality.
Quickly discover problems and has the ability to fix them.	There is no automatic recovery feature.

Table 4.1: SIEM Comparison Table

Chapter 5

FUTURE WORK AND CONCLUSION

5.1 Conclusion

In this paper, we showed a comprehensive SIEM solution built with Wazuh. As a result, our system can ensure network security, identify intrusions, threats, and behavioral anomalies, and take appropriate action as required. Though SIEM technology or data security technology is very much expensive for all sorts of industries, we came up with Open source SIEM tools as a solution. In conclusion, all industries can easily get the best solution with it as well as in an affordable way.

5.2 Future Work

In the first phase, we have given a SIEM solution that assures Incident Response, Security Analytics, Intrusion Detection, file integrity monitoring, Log Data Analysis, Configuration Assessment, Vulnerability Detection, across a network.

In the future, we have plans to add automated monitoring of lateral movement so that our SIEM may be able to connect such relevant events together. Incident Prioritization so that our SIEM can remove false positives and concentrating only on events with anomalous behaviors is vital for robust security, Cloud Security services, etc.

Bibliography

[1] M. Nabil, S. Soukainat, A. Lakbabi, and O. Ghizlane, “Siem selection criteria for an efficient contextual security,” in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, 2017, pp. 1–6.

[2] L. F. Bernardo, “Targeted attack detection by means of free and open source solutions,” 2018.

[3] M. Mutemwa, J. Mtsweni, and L. Zimba, “Integrating a security operations centre with an organization’s existing procedures, policies and information technology systems,” in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, IEEE, 2018, pp. 1–6.

[4] S. Vethanayagam, “Threat identification from access logs using elastic stack,” 2020.

[5] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, “Security operations center: A systematic study and open challenges,” *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020.

[6] I. Kotenko, D. Gaifulina, and I. Zelichenok, “Systematic literature review of security event correlation methods,” *IEEE Access*, 2022.