UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

Cybersecurity Incident Response in eHealth

A Master's Thesis

Submitted to the Faculty of the

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Diogo Donadoni Santos

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

telecos BCN

In partial fulfillment
of the requirements for the degree of
MASTER IN CYBERSECURITY

Advisor: Eva Rodriguez Luna

Barcelona, May 2023

Title of the thesis: Cybersecurity Incident Response in eHealth

Author: Diogo Donadoni Santos

Advisor: Eva Rodriguez Luna

Abstract

The thesis highlights the concept of Cybersecurity Incident Response, which involves preparing for and responding to cybersecurity breaches or attacks. It emphasizes the importance of timely and effective response to security incidents, with the goals of minimizing damage and preventing future incidents.

The main objective of the thesis, which is to design a system specifically for responding to cyber attacks in a specific eHealth use case. The system will have the capability to identify potential cyber attacks in the critical assets, evaluate the impact of such attacks, and create mitigation strategies (automated response) focused on maintaining business continuity.

Overall, the thesis aims to enhance the incident response capabilities of organizations operating in the eHealth sector, providing them with a systematic approach to handle cyber threats and ensure the smooth functioning of their infrastructures.

Acknowledgements

I want to acknowledge Eva Rodriguez Luna (TFM Supervisor and Master Coordinator) for her support, guidance and feedback on this project but also for being the tutor for the Master in Cybersecurity.

I want to acknowledge the Consortium for Continuing Education of Catalonia and the SEPE (Public State Employment Service) for subsidizing the cost of the Cybersecurity Incident Response training (86 hours). I also want to acknowledge Genís Margarit (Teacher and Cybersecurity consultant) and Tomàs Roy Català (Teacher and Director Cybersecurity Agency of Catalonia) for their knowledge sharing and support during the training where we discussed real cyber attacks that help me better understand this topic and conclude this thesis.

Finally, I want to also give thanks to my family for their comprehension during these tough months that I could not give them all the attention that they deserve.

Revision history and approval record

Revision	Date	Purpose
0	18/02/2023	Document creation
1	Weekly	Document revision with Eva Rodriguez Luna
2	22/05/2023	Final Document revision with Eva Rodriguez Luna

Written by:		Reviewed and approved by:	
Date	15/05/2023	Date	22/05/2023
Name	Diogo Donadoni Santos	Name	Eva Rodriguez Luna
Position	Project Author	Position	Project Supervisor

Table of contents

List of Figures

List of Tables

Glossary

CIS	Center for Internet Security
DOS	Denial of Service
DDoS	Distributed Denial of Service
EDR	Endpoint detection and response
GDPR	General Data Protection Regulation
HIDS	Host Intrusion Detection System
IDS	Intrusion Detection System
IPS	Intrusion Protection System
IOCs	Indicators of Compromise
JSON	JavaScript Object Notation
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
OSSEC	Open Source Host-based Intrusion Detection System
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management
SOAR	Security Orchestration, Automation and Response
XDR	Extended detection and response

1. Introduction

Cybersecurity Incident Response entails the process of preparing and responding to cybersecurity breaches or attacks. It involves a set of activities that help organizations respond to security incidents in a timely and effective manner, minimize the damage caused by the incident, and prevent similar incidents from happening in the future.

The purpose of this thesis is to create a system for responding to and adapting to cyber attacks in eHealth infrastructures. This system will identify critical assets and potential cyber attacks, assess the impact of the attack, and develop mitigation strategies aimed at ensuring business continuity.

1.1. Objectives

- Identification of critical assets in eHealth systems
- Identification cyberattacks in eHealth systems
- Impact evaluation of cyberattacks in eHealth systems
- Definition of mitigation strategies for the use case
- Evaluation Incident response automation and business continuity

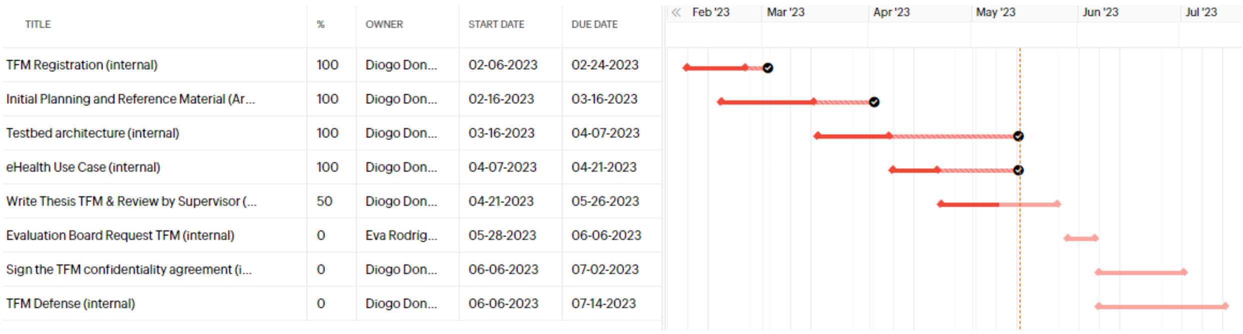
1.2. Methodology

This is the methodology that we will follow on this thesis :

1. A realistic work plan will be established and adjusted to the pre-established planning for the subject.
2. The different SIEM/IDS/XDR existing in the market will be analyzed and the one that best suits our needs will be chosen.
3. The implementation method, configuration and most appropriate architecture will be designed.
4. The system will be installed and configured with specific rules for the defined use cases to automatically respond to Cybersecurity Incidents.
5. Review the results and benefits obtained with this implementation
6. Conclusions and possible improvements that we will be provided in the final report

1.3. Planning: phases and tasks

Figure 01 shows the key milestones of this project, as well as their duration and start and end dates.



TITLE	%	OWNER	START DATE	DUE DATE
TFM Registration (internal)	100	Diogo Don...	02-06-2023	02-24-2023
Initial Planning and Reference Material (Ar...	100	Diogo Don...	02-16-2023	03-16-2023
Testbed architecture (internal)	100	Diogo Don...	03-16-2023	04-07-2023
eHealth Use Case (internal)	100	Diogo Don...	04-07-2023	04-21-2023
Write Thesis TFM & Review by Supervisor (...	50	Diogo Don...	04-21-2023	05-26-2023
Evaluation Board Request TFM (internal)	0	Eva Rodrig...	05-28-2023	06-06-2023
Sign the TFM confidentiality agreement (i...	0	Diogo Don...	06-06-2023	07-02-2023
TFM Defense (internal)	0	Diogo Don...	06-06-2023	07-14-2023

Figure 01 - Gantt Chart: Project Milestones

1.4. Thesis Structure

The remainder of this thesis is organized as follows:

Chapter 2: introduces the topics and concepts used throughout this dissertation and gives an overview of some related research works, together with state of the art in the field;

Chapter 3: introduces the critical assets and problem of this thesis work;

Chapter 4: briefly discusses how the solution was designed;

Chapter 5: covers the use case and details regarding the implementation of the architecture proposed in the previous chapter;

Chapter 6: discusses the results of some simulations performed targeting the implementation presented in the previous chapter;

Chapter 7: concludes the thesis and briefly mentions some future work.

2. State of the art of the technology applied in this thesis

This chapter provides an overview on what are the current established and emerging security technologies and related tools. Moreover, relevant concepts related to incident response automation are presented, so as to give a background knowledge useful throughout the rest of this thesis.

2.1. SIEM

Security information and event management (SIEM) is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

SIEM combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements.With the incorporation of artificial intelligence, SIEM has become more efficient, allowing for faster and more intelligent threat detection and incident response.

SIEM solutions gather and consolidate large amounts of data from an organization's applications, devices, servers, and users in real-time, allowing security teams to detect and prevent attacks. To identify potential threats and issue alerts, SIEM tools employ predefined or customized rules that aid security teams in defining and categorizing potential dangers.

SIEM systems typically offer several essential functions, including log management, event correlation, and incident monitoring and response. By collecting and organizing vast amounts of data, SIEM solutions can quickly identify potential threats, attacks, or breaches. Through event correlation, the system can recognize patterns and relationships between data to facilitate fast threat detection and response. Additionally, SIEM technology monitors network security incidents and generates alerts and audits related to incidents. Overall, SIEM systems can reduce cyber risk through use cases such as detecting suspicious user activity, monitoring user behavior, limiting access attempts, and generating compliance reports.

2.1.1. SIEM alternatives and selection

If we look at the Gartner Magic Quadrant for 2022 in figure 02, the leaders in SIEM systems are: Microsoft, Splunk, IBM, Exabeam and Securonix

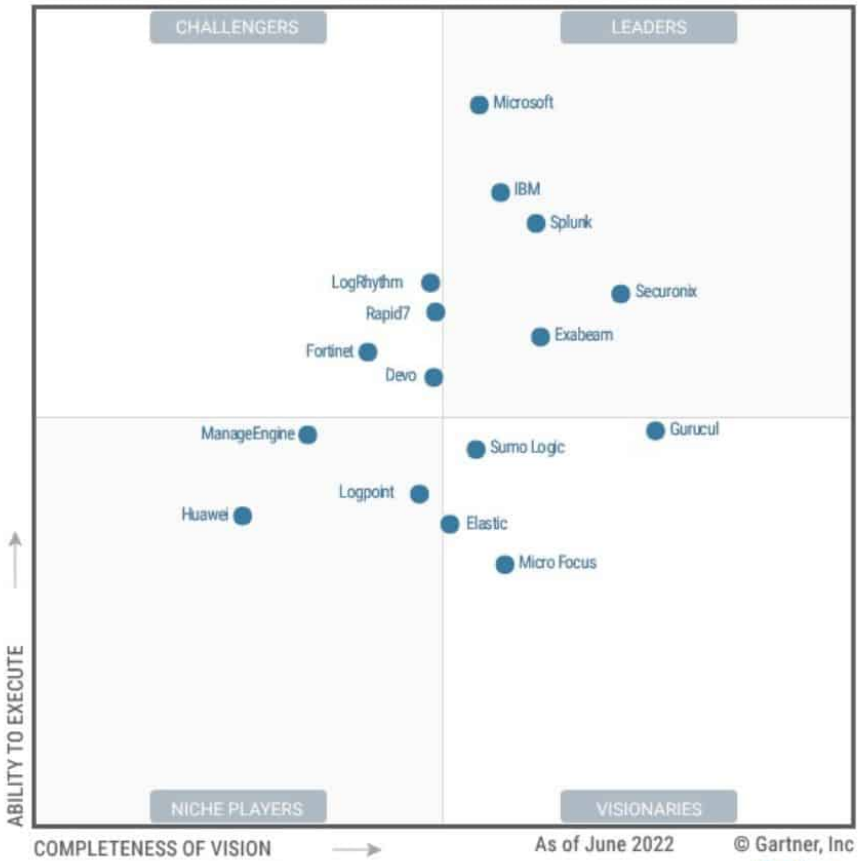


Figure 02 - Gartner Magic Quadrant for Intrusion Detection and Prevention Systems

These SIEMs do not meet the two fundamental requirements that are free software (open source) and that have no associated cost, so they are rejected.

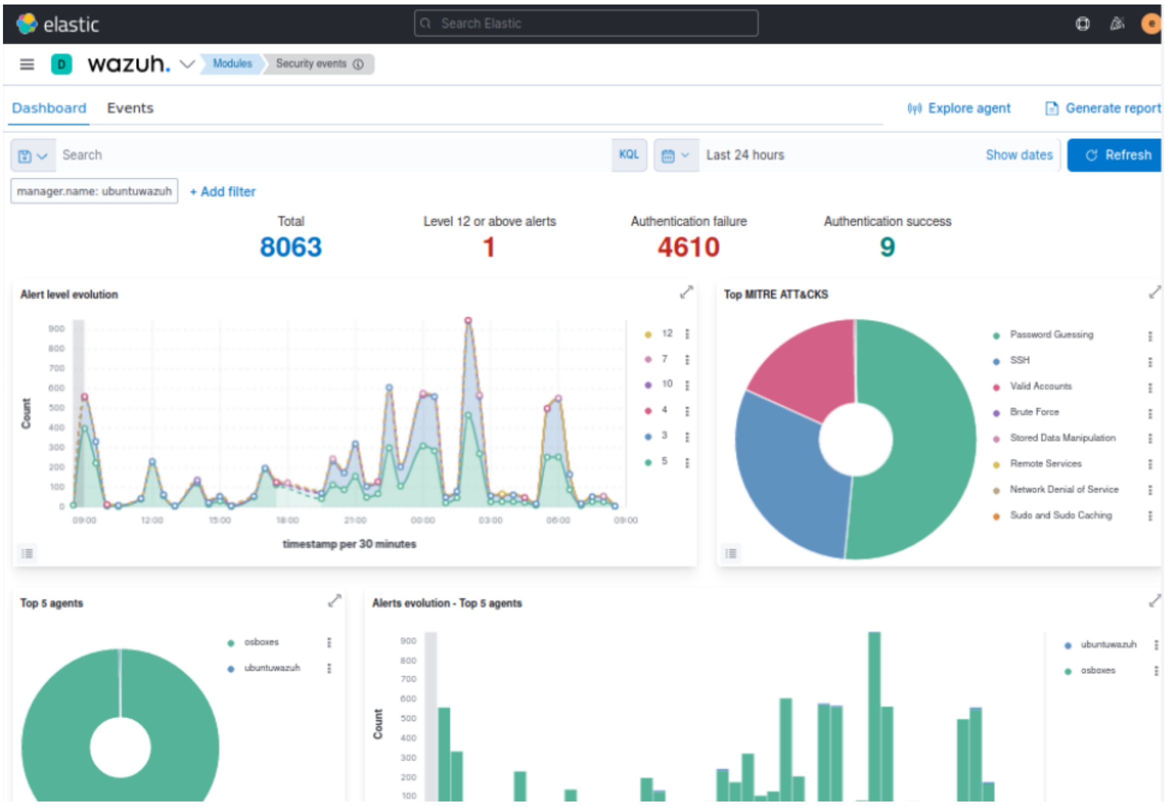
I have considered the following open source SIEMs:

- AlienVault OSSIM
- Apache Metron
- MozDef
- Wazuh

I selected Wazuh because of the following reasons:

- Centralized or distributed architecture
- A set of rules that detects many types of common attacks
- Vulnerability detection
- PCI DSS v3.1 and CIS compliance
- OSSEC based and compliant
- Excellent updated online documentation
- Supports Docker, Puppet, Chef and Ansible deployments
- Supports cloud infrastructure monitoring (AWS and Azure)

The Wazuh SIEM is a comprehensive solution that provides monitoring, detection, and alerting of security events and incidents.



Last 24 hours

manager.name: ubuntuwazuh

Total 8063

Level 12 or above alerts 1

Authentication failure 4610

Authentication success 9

Figure 03 - Wazu Security Events Module

2.2. IDS

Intrusion detection refers to the process of identifying events that are deemed inappropriate or unwelcome to a system. This can be done manually by examining network traffic and logs for each resource or automatically through the use of tools.

An Intrusion Detection System (IDS) is a tool that automates the processing of related information associated with intrusions. IDSs are categorized into two types:

2.2.1. Host Intrusion Detection Systems (HIDS)

HIDS is an intrusion detection system at the equipment level and detects events on a server or workstation. It can generate alerts similar to a NIDS, but it is also capable of inspecting the communication flow comprehensively. Unlike NIDS, it is not vulnerable to evasion techniques such as fragmentation attacks. Furthermore, encrypted communications can be monitored because HIDS inspects traffic before encryption.

A HIDS should perform the following checks:

- File integrity check
- System log monitoring
- Rootkit detection
- Active response

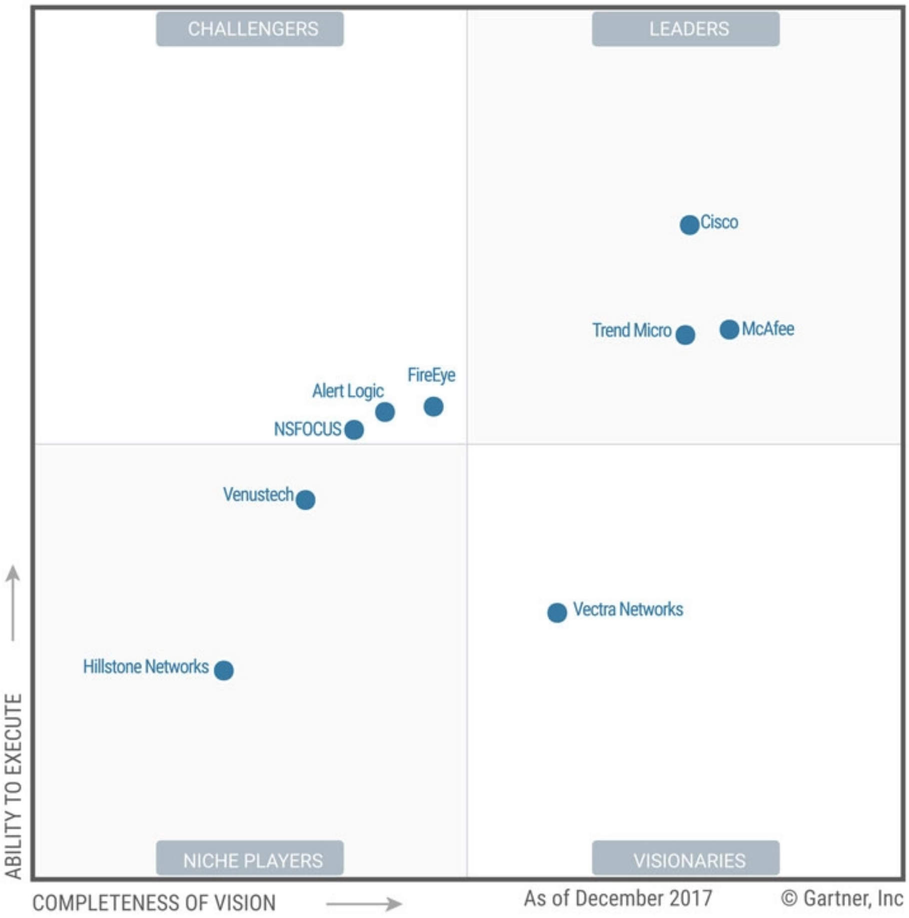
2.2.2. Network Intrusion Detection Systems (NIDS)

NIDS is a network-level intrusion detection system that monitors network traffic and detects anomalies. Unlike HIDS, it cannot inspect encrypted traffic. However, some NIDSs can take action as a result of generating an alert, which is a feature that distinguishes them from Network Intrusion Prevention Systems (NIPS).

2.2.3. IDS/IPS alternatives and selection

If we look at the Gartner Magic Quadrant for 2018 in figure 04, the leaders in IDS/IPS systems are: Cisco, TrendMicro and McAfee

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems



Source: Gartner (January 2018)

Figure 04 - Gartner Magic Quadrant for Intrusion Detection and Prevention Systems

These IDS/IPS do not meet the two fundamental requirements that are free software (open source) and that have no associated cost, so they are rejected.

I have considered the following open source IDS/IPS:

- Snort
- Suricata

At present, there are no major significant differences between the two technologies. There are small differences pertaining to rulesets, new releases.

The selected tool was Suricata due to the feature of being multi-threaded, able to take advantage of all available CPUs. It also has built-in hardware acceleration technology that can leverage the power of graphic cards to inspect network traffic and there are more documents on how to integrate it with Wazuh (SIEM).

2.3. EDR/XDR

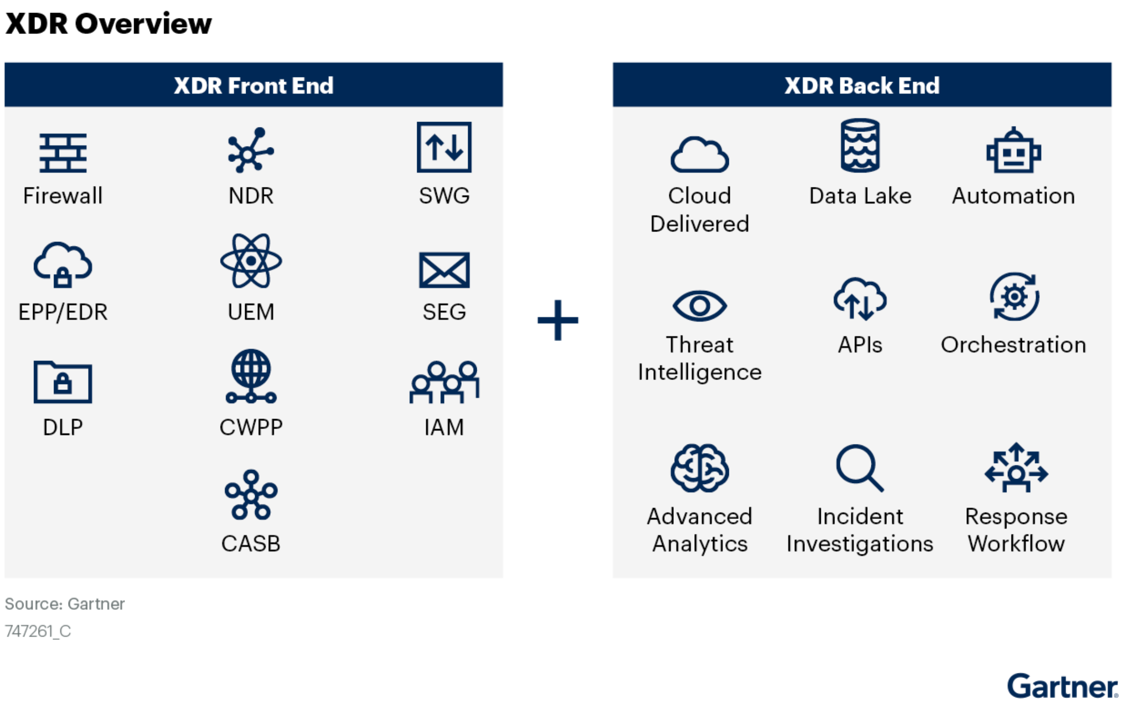
Endpoint Detection and Response (EDR) is a cybersecurity solution that collects and analyzes data from various endpoints to detect behavioral deviations and identify potential threats to the endpoint and connected information systems. EDR helps teams respond quickly by neutralizing threats and sorting alerts that could indicate a threat.

According to Anton Chuvakin of Gartner [23] , EDR is "a category of tools and solutions that focus on detecting suspicious activity directly on the hosts of the information system." In other words, EDR is a new generation of anti-malware that doesn't rely solely on signature-based detection systems. Instead, EDR incorporates behavioral process analysis capabilities to identify deviations from normal behavior.

According to Gartner [24]: ‘XDR is cloud-delivered technology that includes multipoint solutions and advanced analytics to correlate alerts from multiple sources into incidents from individual weaker signals to create more accurate detections. It aims to reduce product sprawl, alert fatigue, integration challenges and operational expenses, and will especially appeal to security operations teams that struggle to manage a portfolio of best-of-breed solutions or leverage a SIEM or SOAR solution.”

Unlike EDR, which focuses on detecting suspicious activity at the endpoint level, XDR (Extended Detection and Response) goes beyond that by collecting and detecting potentially malicious activity across a wide range of sources such as servers, cloud, and networks.

In addition to a wider range of sources, XDR also offers advanced functionalities such as increased contextualization by connecting to Cyber Threat Intelligence (CTI), greater anticipation capacity by cross-referencing detected technical information with external content, and more refined possibilities for response automation by providing even finer granularity to intervention.



Source: Gartner
747261_C

Figure 05 - XDR Overview

A credible XDR needs to have two primary components and they need to be able to be identified and evaluated by security leaders. These are described as XDR front end and XDR back end in Figure 05.

2.3.1. XDR Front-End Components

To create a comprehensive XDR solution, the front-end should include at least three different components or sensors that focus on threat detection and response. These components may include but are not limited to:

- Endpoint Detection and Response (EDR): An endpoint security solution that collects and analyzes data from endpoints to identify potential security threats.
- Endpoint Protection Platforms (EPP): Security software that is deployed on endpoint devices to prevent malware infections, detect and block malicious activity, and provide threat intelligence.
- Network-based security solutions: Firewalls, Intrusion Detection and Prevention Systems (IDPS), Network Detection and Response (NDR), and other security tools that monitor network traffic for suspicious behavior and detect potential threats.
- Identity-based security: Solutions that manage user identities, authenticate users, and enforce access control policies to prevent unauthorized access.

- Email security: Solutions that protect email systems from phishing attacks, malware, and other email-based threats.
- Mobile threat detection: Solutions that protect mobile devices from malicious applications and other mobile-based threats.
- Security Services Edge (SSE): A security solution that provides secure access to cloud applications and services.
- Cloud workload protection: Solutions that protect cloud-based workloads from unauthorized access, malware, and other cloud-based threats.
- Deception: Solutions that create decoys or traps that can lure attackers away from critical assets, enabling organizations to detect and respond to attacks more effectively.

These front-end components work together to provide a comprehensive XDR solution that can detect and respond to threats across a wide range of sources.

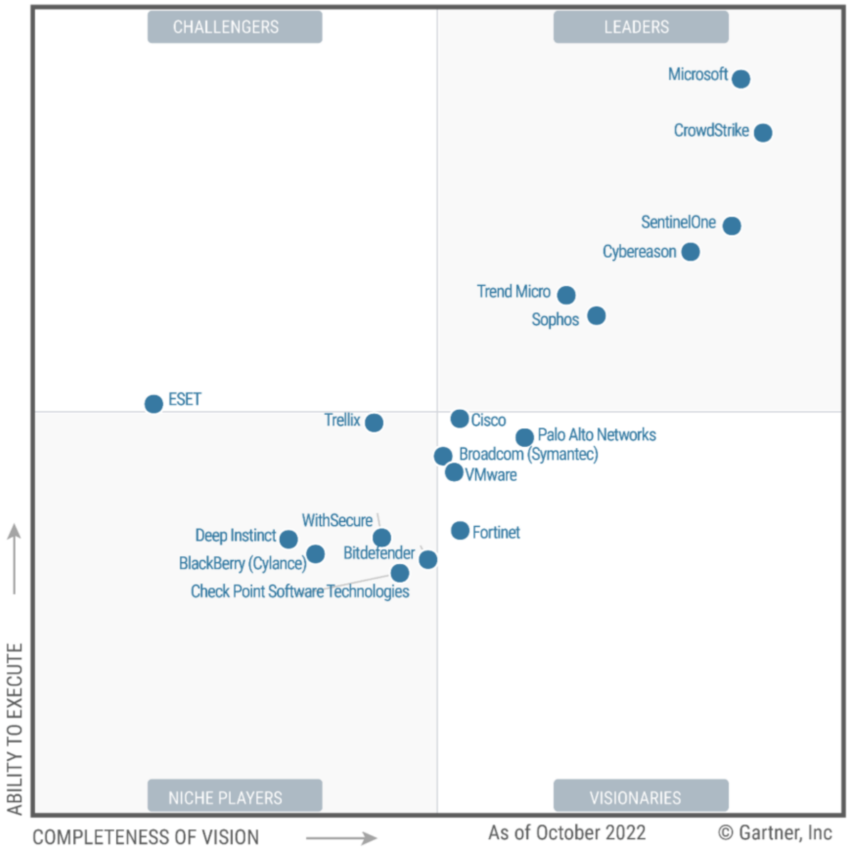
2.3.2. XDR Back-End Components

The back-end of an XDR system should include features such as:

- Predominantly cloud-delivered solutions, reducing the need for on-premises components to a minimum.
- Machine learning and artificial intelligence algorithms to analyze and correlate large amounts of data in real-time and identify potential threats before they escalate.
- Threat intelligence feeds and integrations with third-party security tools to enrich the data and improve threat detection.
- Dashboards and reporting tools provide to security teams the visibility into the security posture of the organization, including threat trends, incidents, and response times.
- Integration with ticketing systems, allowing security incidents to be automatically opened and assigned to the appropriate team member for resolution.
- Compliance and regulatory reporting capabilities to assist with audits and compliance requirements.
- Continuous monitoring and auditing of system configurations and changes to identify potential vulnerabilities or unauthorized access.
- Role-based access controls to ensure that only authorized users have access to sensitive data and security controls.
- Scalability and flexibility to accommodate growth and changing security requirements.

2.3.3. EDR/XDR alternatives and selection

If we look at the Gartner Magic Quadrant for 2022 in figure 06, the leaders in EDR/XDR systems are: Microsoft, CrowdStrike, SentinelOne, Cybereason, Trend Micro and Sophos



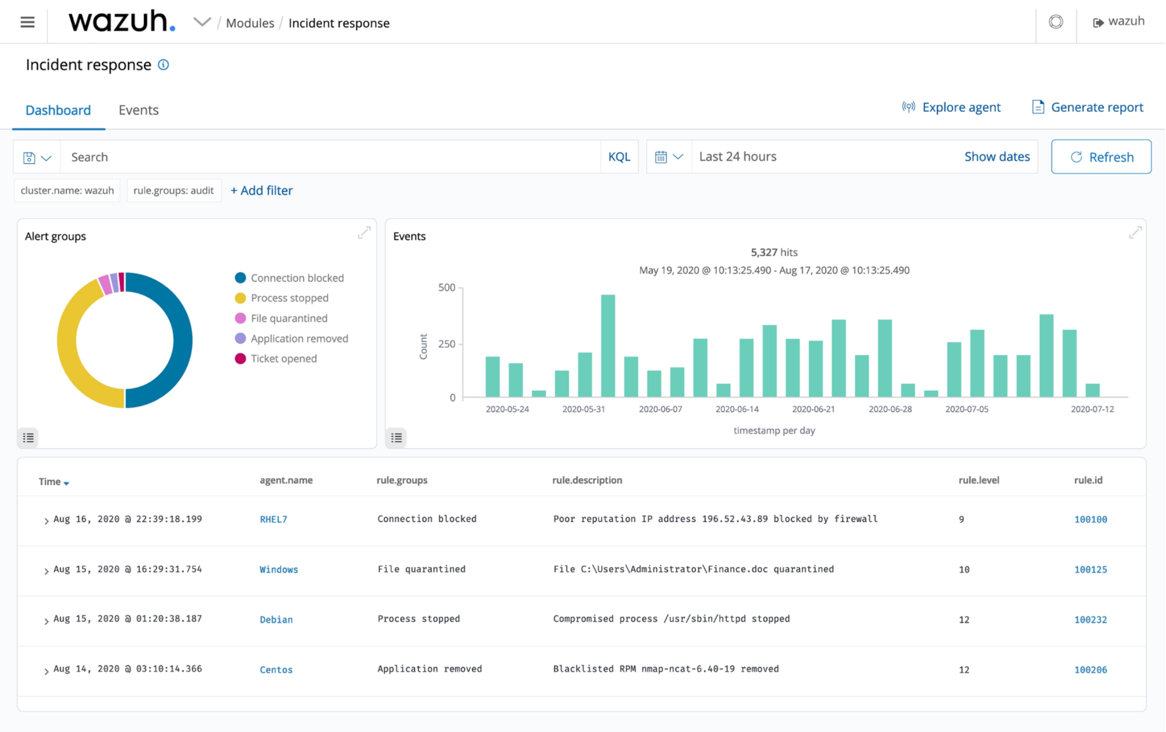
Source: Gartner (December 2022)

Figure 06 - Gartner - Magic Quadrant for Endpoint Protection Platforms

These EDR/XDR do not meet the two fundamental requirements that are free software (open source) and that have no associated cost, so they are rejected.

I selected Wazuh as the SIEM solution and this tool also provides the XDR capability so I will also take advantage of SIEM integration.

Wazuh provides analysts real-time correlation and context. Active responses are granular, encompassing on-device remediation so endpoints are kept clean and operational.



Time	agent.name	rule.groups	rule.description	rule.level	rule.id
Aug 16, 2020 @ 22:39:18.199	RHEL7	Connection blocked	Poor reputation IP address 196.52.43.89 blocked by firewall	9	100100
Aug 15, 2020 @ 16:29:31.754	Windows	File quarantined	File C:\Users\Administrator\Finance.doc quarantined	10	100125
Aug 15, 2020 @ 01:20:38.187	Debian	Process stopped	Compromised process /usr/sbin/httpd stopped	12	100232
Aug 14, 2020 @ 03:10:14.366	Centos	Application removed	Blacklisted RPM nmap-ncat-6.40-19 removed	12	100206

Figure 07 - Wazuh Incident Response Module

2.4. Incident Response

The security landscape has witnessed significant transformations due to the rise in the complexity of threats and the exploration of new security management techniques. The prime objective in all security-related discussions is to avoid incidents that may harm crucial assets or lead to unfavorable outcomes.

According to the National Institute of Standards and Technology (NIST), a security incident can be described as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." In other words, a security incident refers to any activity or event that violates or poses a threat to an organization's security policies, practices, or infrastructure.

While threats may ultimately result in incidents that impact resources, services, and other assets, it is important to note that the steps and methodologies involved in handling these incidents should not be limited to incident response. Effective incident management requires a series of actions to be taken both before and after the incident has occurred, which can be grouped into different stages.

Structured operations are essential for incident handling tasks at all stages. It is imperative to establish protocols well in advance of any malicious events. Organizations should structure themselves to create appropriate teams and facilities that can handle all stages of incident response, from prevention to post-incident activities, in a seamless manner.

The NIST [25] defines incident response as a continuous cycle of operations that occur before, during, and after an incident. These operations are grouped into four stages, each targeting different tasks, with the moment of detection and containment as a central reference point. Different teams may be responsible for each stage, with specialized skills and appropriate tools provided. The stages are summarized with brief descriptions of their activities and recommendations for handling them well. Using this methodology allows for timely incident response through predefined playbooks and reduces costs and service disruption. It also facilitates compliance by requiring extensive incident documentation and continuous improvement of procedures. Figure 08 represents the incident response life cycle stages.

2.4.1. Incident response life cycle

The incident response life cycle consists of four stages:

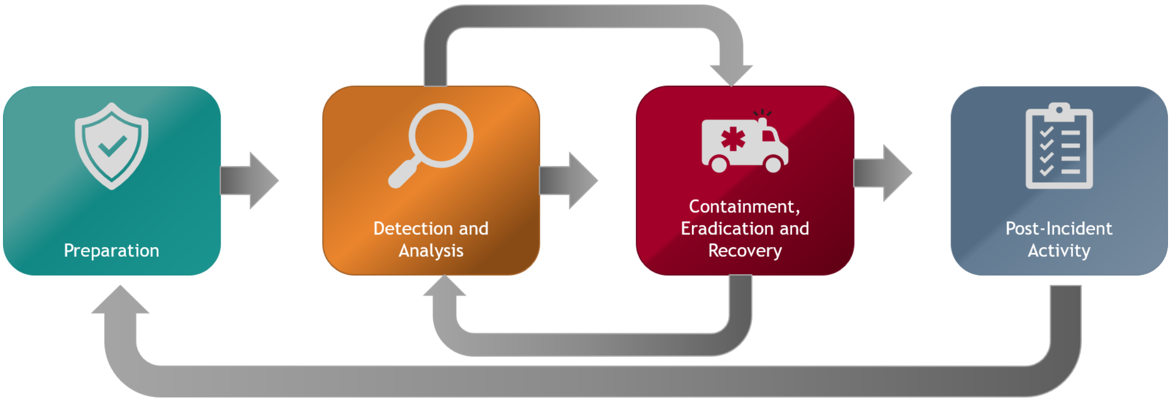


Figure 08 - Incident response life cycle

- Preparation: In this stage, the organization prepares for potential incidents by creating an incident response plan, establishing incident response teams, and providing training to personnel. This stage also includes conducting risk assessments and implementing appropriate security controls.
- Detection and Analysis: In this stage, incidents are detected and analyzed to determine the scope and nature of the incident. This includes identifying the affected assets, evaluating the severity of the incident, and determining the root cause.

- Containment, Eradication, and Recovery: In this stage, the incident is contained to prevent further damage, eradicated to remove the threat, and the affected systems are recovered to normal operations. This stage also includes implementing corrective actions to prevent similar incidents from occurring in the future.
- Post-Incident Activity: In this stage, a thorough review of the incident response process is conducted to identify areas for improvement. This includes analyzing the effectiveness of the incident response plan, evaluating the performance of incident response teams, and updating policies and procedures based on lessons learned.

It is important for organizations to have a structured approach to incident handling and to regularly review and update the incident response plan and procedures. This helps to ensure a timely and effective response to incidents, minimize the impact of incidents on business operations, and improve overall security posture.

2.5. Incident Response automation

There is a growing belief that security teams are inundated with alerts, and while some of them may be inaccurate, they may miss legitimate alerts. If these alerts accumulate and are not addressed promptly or at all, critical problems may go unnoticed and worsen, resulting in a significant security breach. Detecting and responding to security incidents should occur as quickly as possible to minimize the window in which an attacker can execute an attack.

Automating incident response processes using a Security Information and Event Management (SIEM) solution involves four key steps that can be highly effective. By automating repetitive tasks, security teams can free up their time to focus on more complex issues. These four steps include identifying the incident types to automate, defining response workflows and actions, integrating and testing the automation, and finally, monitoring and updating the automation to ensure its effectiveness over time.

- **Creating a correlation rule :** a mechanism in a SIEM solution that enables the detection of patterns and the triggering of alerts on any unusual or abnormal activity.

- **Creating a custom workflow:** designing a set of predefined actions and procedures to be executed when an alert is triggered. These workflows can include a sequence of automated actions, such as isolating the affected system, collecting relevant information, notifying the appropriate personnel, and initiating a targeted response to contain the attack. The goal is to automate the incident response process and reduce the time it takes to detect and respond to an incident. By creating a custom workflow, security teams can ensure that the right steps are taken promptly to minimize the impact of the attack.

- **Configuring an incident rule:** setting up rules for incident categorization, prioritization, and assignment. Once the rule is established, incidents are automatically generated for the alerts that meet the rule's criteria, and they are assigned to the relevant security administrator for timely resolution. This ensures that security incidents are tracked, monitored, and addressed promptly, reducing the risk of a security breach.

- **Managing tickets effectively:** is an important step in incident response automation. By creating tickets for further investigation, security teams can prioritize and track incidents, assign them to the appropriate personnel, and ensure that they are resolved in a timely manner. This can be achieved by integrating the SIEM solution with third-party ticketing or help desk tools, which can automate the ticket creation process and ensure that all necessary information is included. This helps reduce the time it takes to resolve incidents and ensures that nothing falls through the cracks.

Automated incident response capabilities can significantly enhance the effectiveness of Security Operations Centers (SOCs). By automating incident response, SOCs can detect patterns and correlate suspicious events, prioritize alerts based on severity, and trigger immediate actions through automated response workflows. This allows the first line of defense to respond to incidents quickly and effectively, reducing the time it takes to detect and respond to security incidents. Additionally, automated incident response allows SOCs to manage incidents centrally, ensuring that they are tracked and resolved efficiently.

2.5.1. Wazuh Active Response

Security teams can face several challenges in incident response, including responding to high-severity incidents promptly and implementing complete mitigation actions. Gathering relevant information in real-time can also be a challenge, making it harder to understand the full extent of an incident. These issues can ultimately lead to difficulty in containing and mitigating the impact of a cyberattack.

Wazuh SIEM and XDR platform improves incident response by:

- Providing real-time visibility into security events.
- Reducing alert fatigue.
- Automating response actions to threats.
- Providing out-of-the-box response scripts.

The active response module of Wazuh provides security teams with the capability to automate response actions triggered by specific events, thus allowing them to efficiently handle security incidents.

Automating response actions ensures that high-priority incidents are addressed and remediated in a timely and consistent manner. This is especially valuable in environments where security teams are resource constrained and need to prioritize their response efforts.

The active response module in Wazuh offers pre-built response scripts that can be used to quickly respond to and mitigate threats. These scripts include blocking malicious network access and deleting malicious files on monitored endpoints. This helps alleviate the workload on security teams and allows them to efficiently manage security incidents

The Wazuh active response module triggers scripts on monitored endpoints based on the alert level, rule ID, or rule group. Security teams can configure multiple scripts to respond to specific triggers, but caution must be exercised to avoid vulnerabilities resulting from poorly implemented rules and responses.

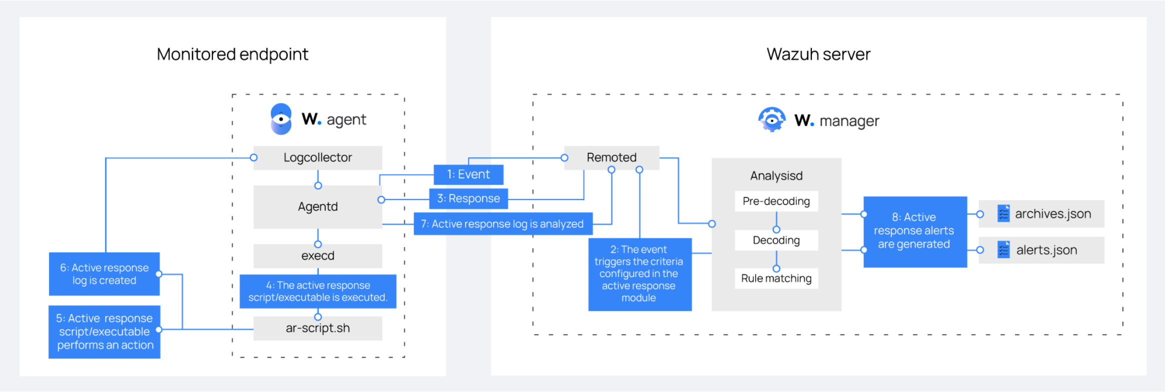

Monitored endpoint
W. agent
Logcollector
Agentd
execd
4: The active response script/executable is executed.
ar-script.sh
6: Active response log is created
5: Active response script/executable performs an action
1: Event
3: Response
7: Active response log is analyzed
Wazuh server
W. manager
Remoted
2: The event triggers the criteria configured in the active response module
Analysisd
Pre-decoding
Decoding
Rule matching
8: Active response alerts are generated
archives.json
alerts.json

Figure 09 - Wazuh active response workflow

https://documentation.wazuh.com/current/_images/active-response-workflow1.png

Active response can be divided into two types: stateless and stateful.

- **Stateless active response** refers to a one-time action that doesn't have an event definition to revert or stop it. For instance, blocking an IP address in response to a security alert is a stateless response because the IP remains blocked indefinitely, even after the alert has been resolved.
- **Stateful active response,** on the other hand, refers to actions that are reversible or stoppable after a certain period of time. For example, quarantining a compromised endpoint in response to an alert is a stateful response because the endpoint can be released from quarantine after a period of time or after the threat has been neutralized.

Wazuh comes with a set of default scripts used in active response. These scripts are located in the /var/ossec/active-response/bin/ directory on Linux/Unix endpoints. The firewall-drop active response script works with Linux/Unix operating systems. It uses iptables to block malicious IP addresses.

```
<command>

  <name>firewall-drop</name>

  <executable>firewall-drop</executable>

  <timeout_allowed>yes</timeout_allowed>

</command>
```

The **<command>** block contains information about the action to be executed on the Wazuh agent:

<name>: Sets a name for the command. In this case, firewall-drop.

<executable>: Specifies the active response script or executable that must run upon a trigger. In this case, it’s the firewall-drop executable.

<timeout_allowed>: Allows a timeout after a period of time. This tag is set to yes here, which represents a stateful active response.

3. Problem statement

The healthcare industry has undergone a significant transformation in recent years due to the increasing use of electronic health records and the rapid development of technology. The integration of technology in healthcare has made it easier to provide quality care and services to patients, but it has also led to an increase in the number of cyber attacks. Cybersecurity breaches in eHealth infrastructures can have severe consequences, such as loss of sensitive data, financial loss, and reputational damage. Therefore, it is essential to have a system in place to respond to and adapt to these attacks promptly and efficiently.

3.1. Critical Assets

The key step in responding to cyber attacks in eHealth infrastructures is to identify critical assets and potential vulnerabilities. This includes identifying all the hardware, software, and data that are essential for the smooth functioning of the eHealth infrastructure. Critical assets include patient information, medical records, and financial data. Once these assets have been identified, it is necessary to assess the potential risks and vulnerabilities that could compromise their security. This includes conducting regular vulnerability assessments, penetration testing, and risk analysis to identify potential weaknesses that could be exploited by cybercriminals.

We described in table 01 the critical assets, potential cyber-attacks, impact, response and mitigations for the eHealth sector.

Critical Asset	Potential Cyber Attacks	Impact	MITRE ATT&CK	Response or Mitigation
Services and Network [1]	DoS Attack	1. Disrupt the services and overwhelm the networks as well as slowing and shutting down the significant networks. 2. Financial losses also prevent the providers from accessing or transforming essential information [2].	T1499.004 Endpoint Denial of Service: Application or System Exploitation	Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.
Healthcare System web portal [18]	DDoS	1. Turn down the online healthcare website. 2. Make the website or App unavailable for legitimate users. 3. It also overwhelms the server, which leads to the crash or slow response of the server. 4. It can halt the network service instantly and prevent the accessing of sensitive data [19].	T1498.001 Network Denial of Service: Direct Network Flood T1595 Active Scanning	Blocking source addresses, sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport As immediate response may require rapid engagement of 3rd parties, analyze the risk associated with critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.

Critical Asset	Potential Cyber Attacks	Impact	MITRE ATT&CK	Response or Mitigation
Computer's information (Patient's account Records, tamper the information in the computer) [3]	Malicious software viruses: 1. Trojans or Malware 2. Rootkits 3. Network packet detection [11] 4. IP spoofing [11] 5. Password assaults [11]	1. The data is hacked or altered, through an external drive or software. 2. losing some sensitive information from the user account 3. tamper the information of the database 4. got some false statistics injected by the hackers for wrong communication signal 5. lose the control over the account, password	1. T1587.001 Malware 2. T0851 Rootkit 3. T0842 Network Sniffing 4. T1499 Endpoint Denial of Service 5. T1110.001 Brute Force: Password Guessing	1. This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Isolate infected device or network. 2. Audit the integrity of the system and DLLs. Isolate infected device. 4. Response with block rule for newly executed processes that can aid in sniffing network traffic to capture information about an environment. 5. Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted 6. Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guess
Information(Patient's financial information)[4]	1. Phishing: using of emails 2. Spam attack: install malware through email 3. Injection attack: malicious code through browser [5] 4. Cryptographic Attack [5]	1. a huge business and financial loss 2. steal personal information 3. significant information of the victims are stolen 4. misuse the data for financial gain	1. T1566 Phishing 2. T1587.001 Malware 3. T1055 Process Injection 4. T1600 Weaken Encryption	1. Network intrusion prevention systems scan and remove malicious email attachments or links that can be used to block activity. 2. Isolate infected device or network. 3. endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process 4. Ensure that the cryptographic system is implemented correctly
Data Breaches (Patient's health and medical insurance data)	1. Formjacking [6] 2. Browser Extension [7] 3. Malware [8] 4. Man in the Middle (MITM) or Eavesdropping [5] 5. Ransomware [5] [22]	1. loss of data confidentiality, accessibility of websites 2. huge loss of financial and personal data 3. data originality is lost or partially data is changed 4. It leads to fatal or impact on a patient's health.	1. T1055 Process Injection 2. T1176 Browser Extensions 3. T1587.001 Malware 4. T1638 Adversary-in-the-Middle 5. T1486 Data Encrypted for Impact	1. endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process 2. Set a browser extension allow or deny list as appropriate for your security policy 3. Isolate infected device or network. 4. Applications that properly encrypt network traffic may evade some forms of AiTM behavior. 5. Enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware

Table 01 - Critical assets and potential cyber-attacks of eHealth sector

As part of the research samples of real attacks from the last 10 years will be listed below.

1. In 2014, a Dos attack had shut down the administration of Boston's children hospital, causing a lot of loss to the hospital. [12]

2. In 2017, Kaleida Health, New York's largest provider, was attacked twice by phishing, compromising the health records of more than 3000 patients at a time [3].

3. Hackers insinuated by the WHO websites and created an email such as, coronavirusfund@who.org for data breaches using this email. Where the official website of WHO is www.WHO.int. The hackers altered the website and misused it [4].

4. Very recently a cyber-threat was posed on public health by a vulnerability known as the Wannacry software virus, commonly known as Ransomware [6].

5. In 2015, the USA experienced the most highly publicized cyber-attacks, in the healthcare sector, in which the hackers stole around 80 million records from Anthem, a US-based health Insurance Company [9].

6. In 2019, 16,819 cancer patients' records were revealed by targeting the addresses, from $I to $1000 [11].

7. In May 2019, the American Medical Collection Agency was hacked for almost eight months, stealing patient's personal information including their credit and debit card details and compromising it [11].

8. The scale of the 2017 WannaCry attack was unprecedented. WannaCry infected more than 300,000 computers across the world demanding that users pay bitcoin ransoms [13].

9. Mansfield-Devine reports that between 2015 and 2016, half of UK NHS trusts were hit by some form of ransomware [14].

10. In 2016, US media highlighted the case of the Hollywood Presbyterian Medical Centre shut down for 10 days until it paid a $17,000 ransom; in an attack thought to have originated from a phishing email [15].

11. In 2017 ,UK healthcare trust suffered an unspecified cyberattack which led to the shutdown of its IT systems and cancellation of almost all planned operations and outpatient appointments for multiple days [16].

12. In 2017 ,An attack known as Medjack ("Medical Device Hijack") is an exploit that injects malware into unprotected medical devices to move laterally across the hospital network [17].

13. In 2017, The United States HHS (Department of Human Health) faced DDoS attacks from an unknown source, hospitals in France, and the Czech Republic, which were working on the development of the COVID-19 vaccine were hit by DDoS attacks [18].

14. In 2020, A DDoS attack targeted the website of the Department of Health and Human Services (DHoS) in the U.S. by flooding millions of users at a time [20].

15. In 2022, The Ransomexx gang claimed responsibility for the cyberattack against Catalan hospitals and leaks patient data [21].

16. In 2023, The Hospital Clínic in Barcelona, Spain, recently suffered a "sophisticated and complex" cyberattack that targeted the hospital's IT systems. The attack is said to have compromised the hospital's data, causing significant disruptions to its operations. As result of the attack several surgeries and medical appointments were postponed [22].

4. Design Overview

This chapter is organized as follows. In the first place, a high-level perspective of the proposed solution system architecture is presented, making use of a component subdivision. After that, an overview of each component, be it a software module or abstract component of the solution is covered.

4.1. High level design

The proposed architecture consists of designing a system to protect a critical infrastructure utilizing open source tools. The system has several components, each with its own set of functions. These components are organized into different layers, with each layer representing a specific set of functionalities. Figure 10 illustrates a schematic representation of this architecture.

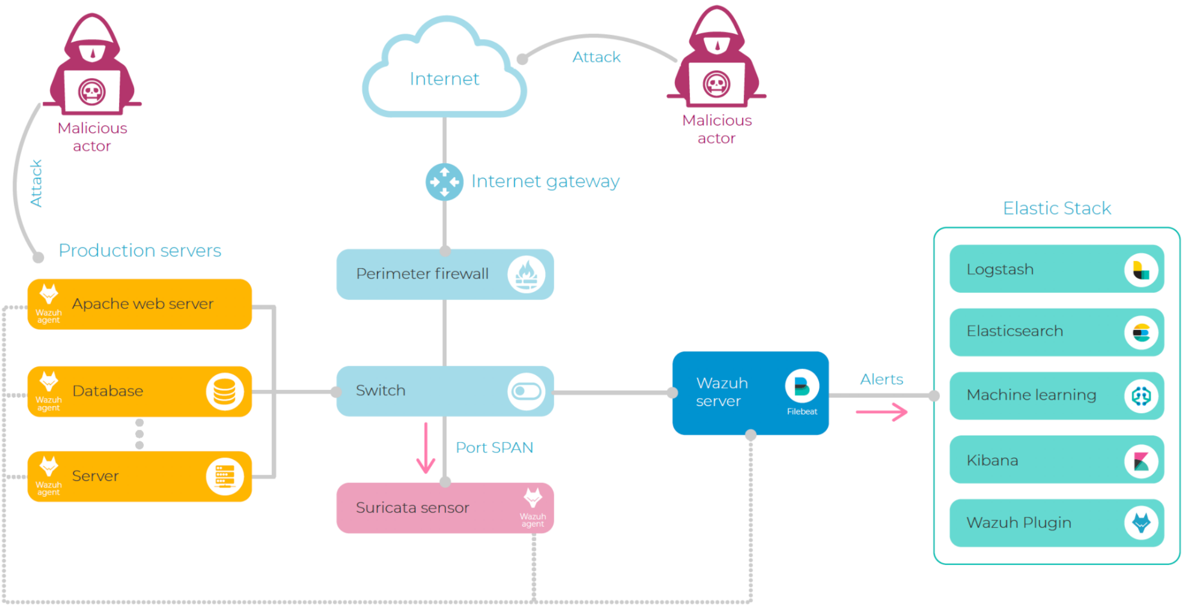


Figure 10 - System High Level Design

The solution is based on Wazuh Platform that provides XDR and SIEM features to protect your cloud, container, and server workloads. These include log data analysis, intrusion and malware detection, file integrity monitoring, configuration assessment, vulnerability detection, and support for regulatory compliance.

Wazuh solution is based on the Wazuh agent, which is deployed on the monitored endpoints, and on three central components: the Wazuh server, the Wazuh indexer, and the Wazuh dashboard as illustrated in the figure 11.

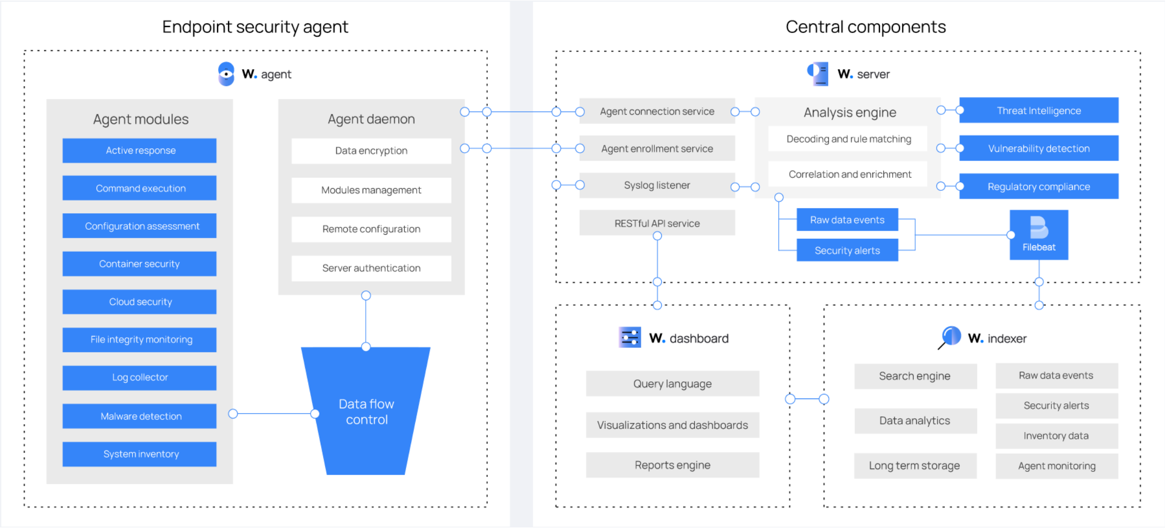


Figure 11 - Wazuh Solution (Agent and Components)

https://documentation.wazuh.com/current/_images/wazuh-components-and-data-flow1.png

The Wazuh **server** is responsible for analyzing data that is received from its agents. This involves processing the data through decoders and rules, which use threat intelligence to detect well-known indicators of compromise (IOCs). The server is designed to handle data from hundreds or thousands of agents, and can scale horizontally when configured as a cluster. In addition to data analysis, the Wazuh server serves as a central management point for its agents, allowing for remote configuration and upgrades when necessary.

The Wazuh **indexer** is a component that serves as a highly scalable engine for full-text search and analytics. Its primary function is to index and store alerts that are created by the Wazuh Server. As part of this work we will be utilizing **Elasticsearch** for this functionality.

The Wazuh **dashboard** is a web-based user interface that facilitates data visualization and analysis. It provides a range of pre-configured dashboards for various security events, regulatory compliance frameworks such as PCI DSS, GDPR, CIS, HIPAA, NIST 800-53, and other features like detected vulnerable applications, file integrity monitoring data, configuration assessment results, and cloud infrastructure monitoring events. Additionally, the dashboard is utilized for managing Wazuh configuration and monitoring its status. As part of this work we will be utilizing **Kibana** for this functionality.

Wazuh **agents** are deployed on various endpoints such as laptops, desktops, servers, virtual machines, and cloud instances. Their main purpose is to provide capabilities for threat prevention, detection, and response. These agents can be installed on multiple operating systems, including Linux, Windows, macOS, Solaris, AIX, and HP-UX.

In addition to agent-based monitoring capabilities, the Wazuh platform can monitor agent-less devices such as firewalls, switches, routers, or network IDS, among others. For example, a system log data can be collected via Syslog, and its configuration can be monitored through periodic probing of its data, via SSH or through an API

4.2. Low level design

It is feasible to run the Wazuh process in an environment with root or with an unprivileged user depending on the situation.

The service in linux is executed either with systemctl, service or initctl, in the case of windows C:\Program Files (x86)\ossec-agent\win32ui.exe is used.

A diagram of the network communications flow is shown in figure 12.

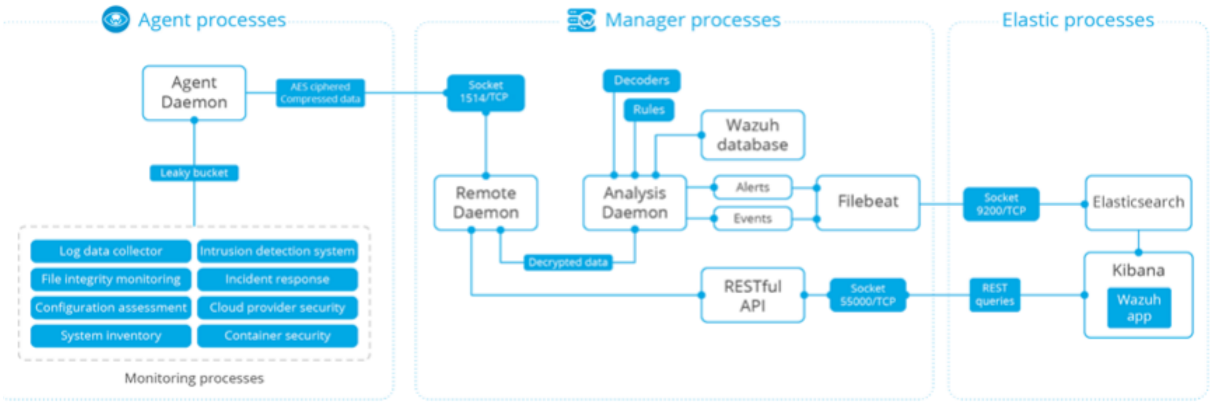


Figure 12 - Wazuh Low level design

https://lh4.googleusercontent.com/qQeVUQWREoQfmpO9RECaITM3w9moy636M5aA4x7Z8bRf_3GWed4wgBSEmrtZLhqUGcpgQj4LJeYp5HAtxU6_YWW4VnK9mOcP2KkMFd7aUKfN6TMZChkbkusfn73ySeW28RH32yp5

Connections between agents and managers in Wazuh are secured using pre-shared keys (AES) and encrypted using compression. This occurs via TCP or UDP 1514. Additionally, Wazuh's Remote Daemon is capable of accepting TCP and/or UDP port 514 messages directly from syslog-sending devices. For more robust centralized syslog collection, syslog servers can be installed on agents.

Wazuh employs authentication and encryption to ensure secure communication. All communications between Wazuh components are encrypted using either AES or TLS encryption. The Wazuh manager worker nodes utilize TLS to synchronize configuration and status data with the manager master node. Each agent is assigned a unique cryptographic key, which is used to report to the manager securely. Despite the significant privilege separation and isolation implemented in the Wazuh server, it is still recommended to implement additional security measures, particularly if remote commands are enabled, as other systems may depend on and be affected by it.

5. Implementation

In this chapter, we will cover the eHealth use case and details regarding the implementation of the architecture proposed in the previous chapter

The framework architecture is based on the one discussed in the previous chapter and will be focused on the automated response to incidents by means of mitigation or remediation strategies packaged into correlation, incident rules and custom workflow.

5.1. eHealth Use Case

We will consider a generic scenario where we have a public hospital with local infrastructure. In this use case, we have identified the Healthcare System web portal as a critical asset that requires protection using incident response automation. The primary objective is to quickly respond to DDos attacks to ensure that the portal remains functional and operational, thereby ensuring business continuity.

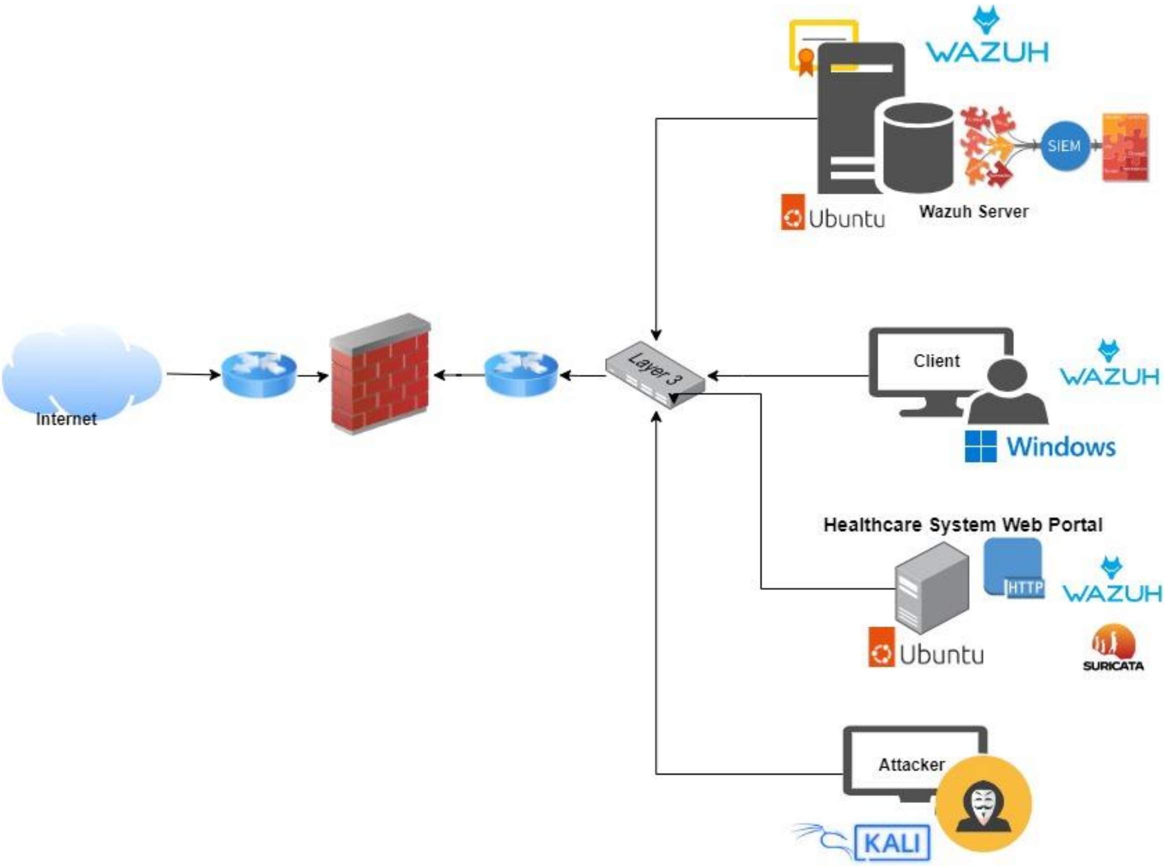


Figure 13 - eHealth Use Case

5.2. Use case Implementation

The installation of Wazuh, ElasticSearch, Filebeat, Kibana, Suricata, Apache Server (Health Care System web portal) and attacker machine was done in my personal computer, which has the following characteristics:

• Windows 11 Pro 64-bit

• Lenovo X1 Yoga 3rd Generation, i7-8650U CPU 1.90GHz with 8 GB of RAM

• 256 GB SSD hard drive

These virtual machines have been created in Oracle VM Virtualbox and the software was installed following the instructions in Appendix.

5.2.1. VM information and software versions installed

Wazuh/ElasticSearch/Filebeat/Kibana Server

- hostname : ubuntuwazuh
- IP : 10.0.12.4
- Operating System: Ubuntu 22.04 LTS
- Kernel: Linux 5.19.0-38-generic
- Wazuh Server version 4.3.10
- Wazuh Server revision 40323
- ElasticSearch version 7.17.9
- Filebeat version 7.17.9
- Kibana version 7.17.9

Suricata/Apache Server (Health Care System web portal)

- hostname : osboxes
- IP : 10.0.12.6
- Operating System: Ubuntu 22.04 LTS
- Kernel: Linux 5.19.0-38-generic
- Suricata version 6.0.10
- Apache Server version 2.4.41
- Wazuh client version 4.3.10
- Wazuh client revision 40323

Attacker Machine

- hostname : ca
- IP : 10.0.12.20
- Operating System: Kali GNU/Linux Rolling
- Kernel: Linux 5.18.0-kali7-amd64

5.2.2. Wazuh Server - Suricata

In order to centrally manage the configuration of all endpoints with Suricata installed, create a new agent group called Suricata and add the Ubuntu agent where suricata is installed.

Creating an agent group and adding an agent

1. Create an agent group called Suricata:

```
sudo /var/ossec/bin/agent_groups -a -g Suricata -q
```

2. Get the ID of all agents you want to add to this category:

```
sudo /var/ossec/bin/manage_agents -l
```

3. Include the agent ID using the command below:

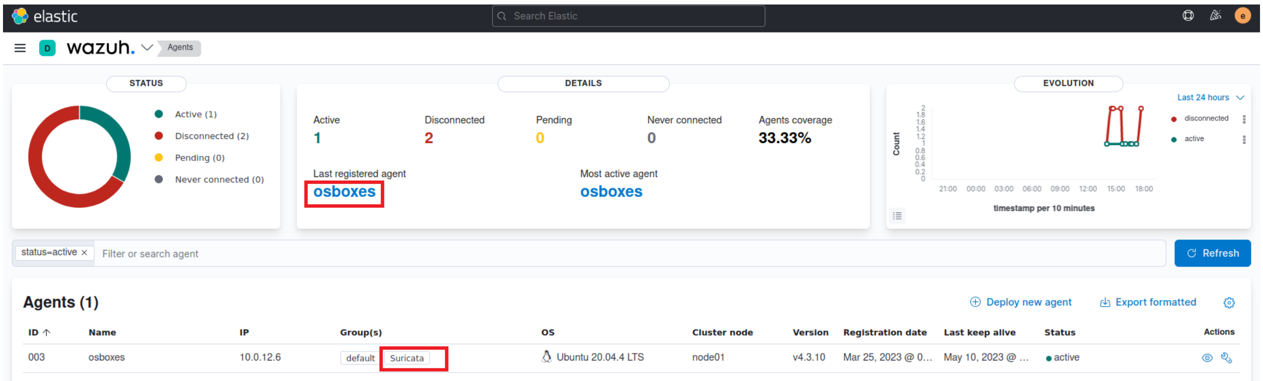
```
sudo /var/ossec/bin/agent_groups -a -i <AGENT_ID> -g Suricata -q
```

Where:

AGENT_ID is the ID of the agent you want to add to the Suricata group.

4. Add the following configuration to the Suricata group shared agent configuration file **/var/ossec/etc/shared/Suricata/agent.conf**:

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



Active	Disconnected	Pending	Never connected	Agents coverage
1	2	0	0	33.33%

Last registered agent
osboxes

Most active agent
osboxes

Agents (1)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
003	osboxes	10.0.12.6	default Suricata	Ubuntu 20.04.4 LTS	node01	v4.3.10	Mar 25, 2023 @ 0…	May 10, 2023 @ …	● active	

Figure 14 - Wazuh Suricata Group

5.2.3. Extending the JSON decoder for Suricata

In Suricata logs, the **src_ip** field holds the IP address of the malicious actor. The Wazuh **firewall-drop** active response script expects the field **srcip** in the alert that triggers the active response. To ensure that the field **src_ip** is processed by the active response scripts, we configure a custom decoder to map the **src_ip** field to **srcip**.

To do this, perform the following steps:

1. Add the decoders below to the local decoders file **/var/ossec/etc/decoders/local_decoder.xml:**

```
<decoder name="json">

  <prematch>^{\s*"</prematch>

</decoder>

<decoder name="json_child">

  <parent>json</parent>

  <regex type="pcre2">"src_ip":"([^"]+)"</regex>

  <order>srcip</order>

</decoder>

<decoder name="json_child">

  <parent>json</parent>

  <plugin_decoder>JSON_Decoder</plugin_decoder>

</decoder>
```

2. Restart the Wazuh manager for the changes to apply:

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

5.2.4. Creating custom correlation rules from Suricata alerts

On the Wazuh server, we added custom rules to detect the use of the GoldenEye DoS attack and Nmap scripting engine from Suricata alerts. These rules will be used by the active response module to trigger the firewall-drop script on the Ubuntu agent where Health Care System web portal is installed

1. Add the following rules to the **/var/ossec/etc/rules/local_rules.xml** file:

```
<group name="custom_active_response_rules,">
  <rule id="100200" level="12">
    <if_sid>86601</if_sid>
    <field name="event_type">^alert$</field>
    <match>ET DOS Inbound GoldenEye DoS attack</match>
    <description>GoldenEye DoS attack has been detected. </description>
    <mitre>
      <id>T1498</id>
    </mitre>
  </rule>

  <rule id="100201" level="12">
    <if_sid>86601</if_sid>
    <field name="event_type">^alert$</field>
    <match>ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)</match>
    <description>Nmap scripting engine detected. </description>
    <mitre>
      <id>T1595</id>
    </mitre>
  </rule>
</group>
```

5.2.5. Active response configuration

Wazuh includes an out-of-box firewall-drop script that adds the IP address extracted from an alert to the monitored endpoints firewall block list. Configure the firewall-drop active response on the Wazuh server using the following step

1. Open the Wazuh server configuration file **/var/ossec/etc/ossec.conf** and confirm the command section for **firewall-drop** exists. Add the configuration block below if it does not:

```
<ossec_config>
  <command>
    <name>firewall-drop</name>
    <executable>firewall-drop</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>
</ossec_config>
```

2. Edit the Wazuh server configuration file /var/ossec/etc/ossec.conf and add the following section:

```
<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100200, 100201</rules_id>
    <timeout>180</timeout>
  </active-response>
</ossec_config>
```

The firewall-drop script adds the malicious IP address to the firewall block list on the monitored agent.

location: This specifies where the active response command is executed. To execute the script on the Wazuh agent, we use local.

rules_id: This limits the execution of the active response script to when rules 100200 and 100201 fire. Rules can be separated with the use of a comma.

timeout: This specifies the time in seconds, taken before the active response command is reversed.

3. Restart the Wazuh manager for the configuration changes to apply:

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

6. Evaluation and testing

In order to evaluate the performance on the proof of concept of the proposed use case a series of tests have been conducted. These aim at testing various aspects, or components, of the proposed architecture implementation, along the whole workflow, from the reception of alert to the automated response through the deployment of custom workflow.

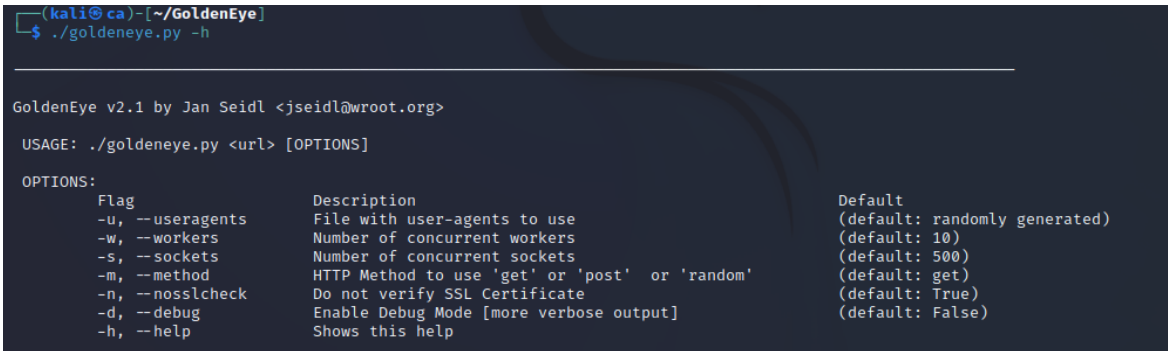
6.1. Attack emulation 1: DDoS attack at Healthcare System web portal

Denial of service attacks aims to render system resources unavailable to users. In this scenario, we used the GoldenEye tool installed on the Kali Linux endpoint to perform a DDoS attack against the web server (Healthcare System web portal) on the Ubuntu endpoint.

GoldenEye is a HTTP DoS Test Tool. This tool can be used to test if a site is susceptible to Distributed Denial of Service (DDoS) attacks. It is possible to open several parallel connections against a URL to check if the web server can be compromised.

The program tests the security in networks and uses ‘HTTP Keep Alive

- NoCache’ as attack vector.

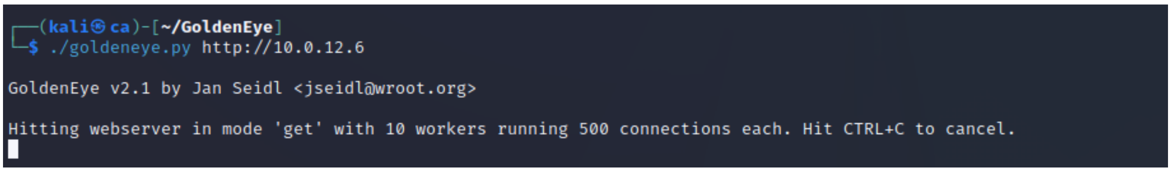


```
┌──(kali㉿ca)-[~/GoldenEye]
└─$ ./goldeneye.py -h

────────────────────────────────────────────────────────────────────────────────────────────────────────────

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

 USAGE: ./goldeneye.py <url> [OPTIONS]

 OPTIONS:
        Flag                    Description                                             Default
        -u, --useragents        File with user-agents to use                            (default: randomly generated)
        -w, --workers           Number of concurrent workers                            (default: 10)
        -s, --sockets           Number of concurrent sockets                            (default: 500)
        -m, --method            HTTP Method to use 'get' or 'post'  or 'random'         (default: get)
        -n, --nosslcheck        Do not verify SSL Certificate                           (default: True)
        -d, --debug             Enable Debug Mode [more verbose output]                 (default: False)
        -h, --help              Shows this help
```

Figure 15 - Wazuh DDoS - GoldenEye command options

Navigate to the folder where the GoldenEye repository was cloned. Run the following command to launch the attack:

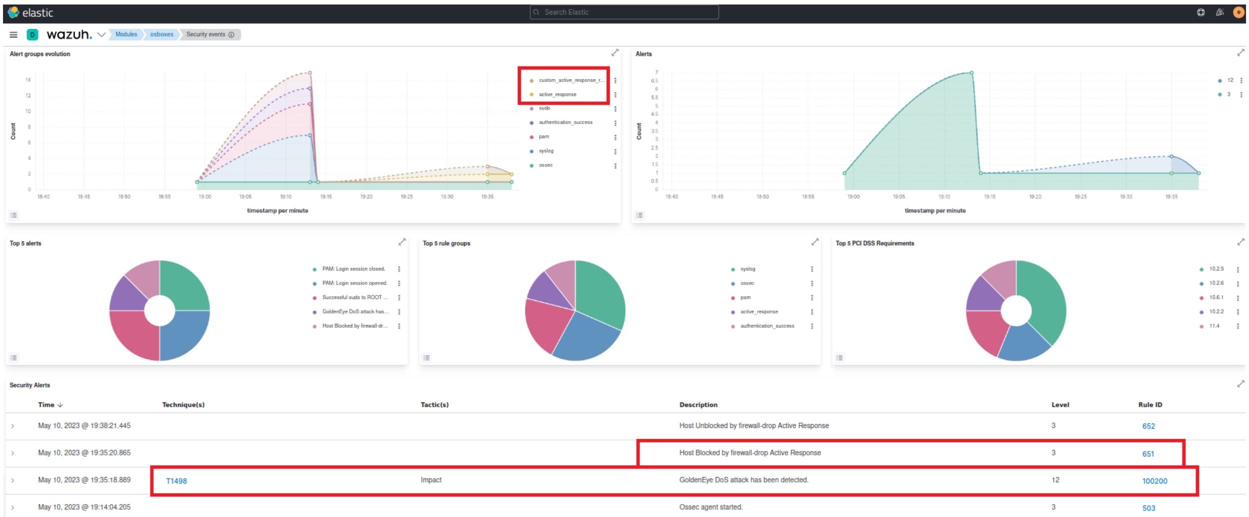
./goldeneye.py http://<Ubuntu_IP>



```
┌──(kali㉿ca)-[~/GoldenEye]
└─$ ./goldeneye.py http://10.0.12.6

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
█
```

Figure 16 - Wazuh DDoS - GoldenEye command to attack at Healthcare System web portal

We can see in the figure 17 the Wazuh active response alert that blocked the DDoS attack.

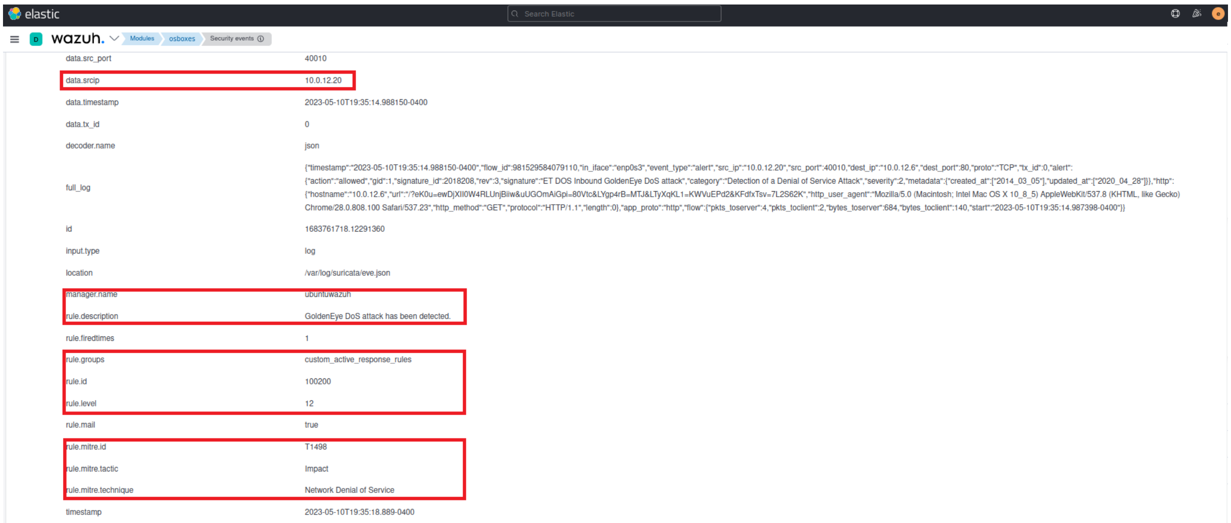


Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 10, 2023 @ 19:38:21.445			Host Unblocked by firewall-drop Active Response	3	652
May 10, 2023 @ 19:35:20.865			Host Blocked by firewall-drop Active Response	3	651
May 10, 2023 @ 19:35:18.889	T1498	Impact	GoldenEye DoS attack has been detected.	12	100200
May 10, 2023 @ 19:14:04.205			Ossec agent started.	3	503

Figure 17 -Wazuh DDoS - Active response alert that blocked the DDoS attack

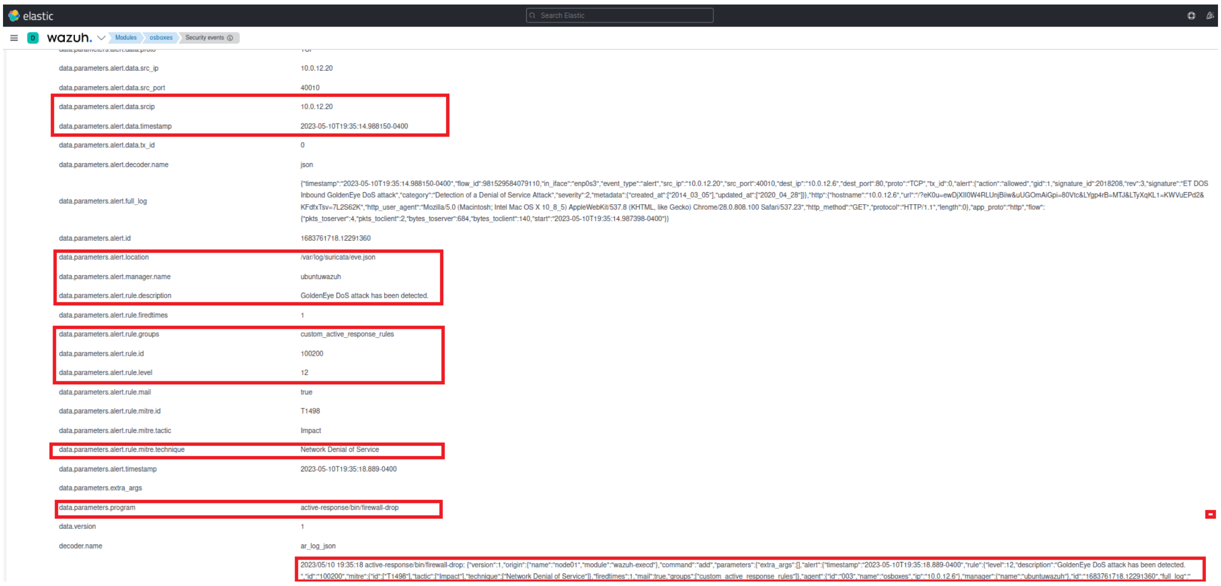
We can see in the figure 18 the event log of the Wazuh active response alert that blocked the DDoS attack.



data.src_port	40010
data.srcip	10.0.12.20
data.timestamp	2023-05-10T19:35:14.988150-0400
data.tx_id	0
decoder.name	json
full_log	{"timestamp":"2023-05-10T19:35:14.988150-0400","flow_id":981529584079110,"in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.12.20","src_port":40010,"dest_ip":"10.0.12.6","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2018208,"rev":3,"signature":"ET DOS Inbound GoldenEye DoS attack","category":"Detection of a Denial of Service Attack","severity":2,"metadata":{"created_at":["2014_03_05"],"updated_at":["2020_04_28"]}},"http":{"hostname":"10.0.12.6","url":"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K","http_user_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 Safari/537.23","http_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":2,"bytes_toserver":684,"bytes_toclient":140,"start":"2023-05-10T19:35:14.987398-0400"}}
id	1683761718.12291360
input.type	log
location	/var/log/suricata/eve.json
manager.name	ubuntuwazuh
rule.description	GoldenEye DoS attack has been detected.
rule.firedtimes	1
rule.groups	custom_active_response_rules
rule.id	100200
rule.level	12
rule.mail	true
rule.mitre.id	T1498
rule.mitre.tactic	Impact
rule.mitre.technique	Network Denial of Service
timestamp	2023-05-10T19:35:18.889-0400

Figure 18 - Wazuh DDoS - GoldenEye DDoS attack event log

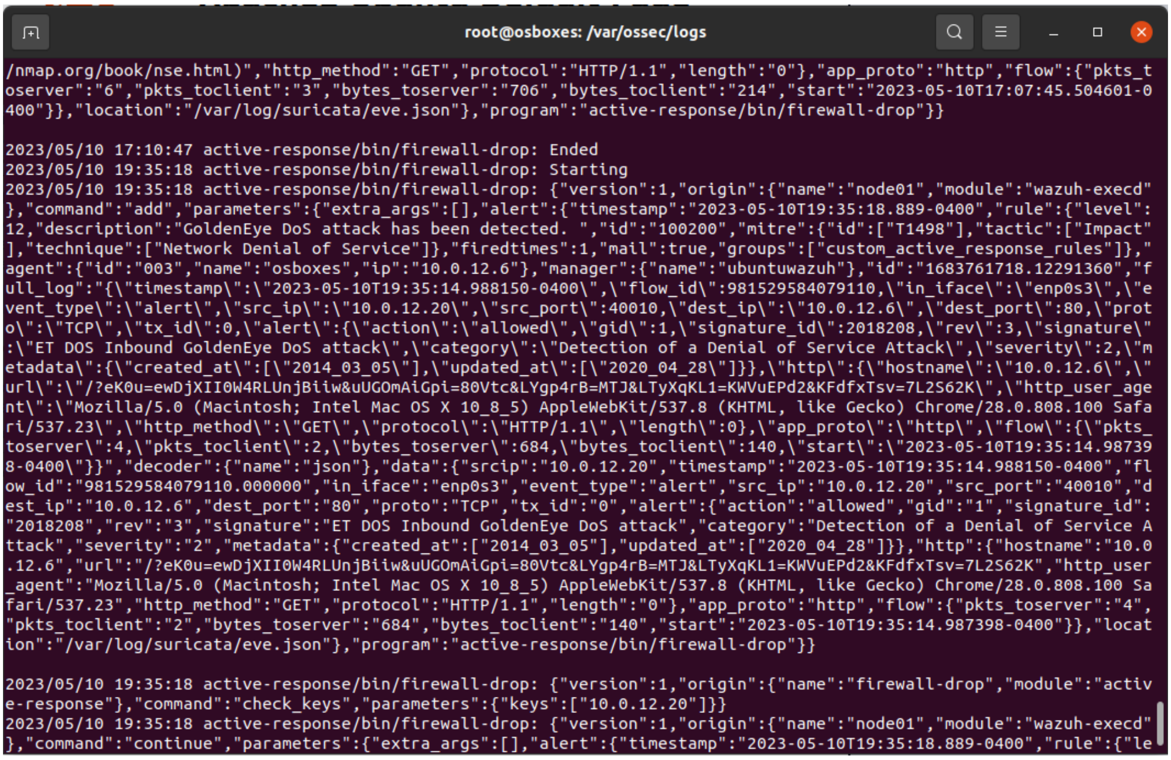
We can see in the figure 19 the Wazuh active response alert that blocked in the Wazuh agent the DDoS attack.



data.parameters.alert.data.proto	TCP
data.parameters.alert.data.src_ip	10.0.12.20
data.parameters.alert.data.src_port	40010
data.parameters.alert.data.srcip	10.0.12.20
data.parameters.alert.data.timestamp	2023-05-10T19:35:14.988150-0400
data.parameters.alert.data.tx_id	0
data.parameters.alert.decoder.name	json
data.parameters.alert.full_log	{"timestamp":"2023-05-10T19:35:14.988150-0400","flow_id":981529584079110,"in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.12.20","src_port":40010,"dest_ip":"10.0.12.6","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2018208,"rev":3,"signature":"ET DOS Inbound GoldenEye DoS attack","category":"Detection of a Denial of Service Attack","severity":2,"metadata":{"created_at":["2014_03_05"],"updated_at":["2020_04_28"]}},"http":{"hostname":"10.0.12.6","url":"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K","http_user_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 Safari/537.23","http_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":2,"bytes_toserver":684,"bytes_toclient":140,"start":"2023-05-10T19:35:14.987398-0400"}}
data.parameters.alert.id	1683761718.12291360
data.parameters.alert.location	/var/log/suricata/eve.json
data.parameters.alert.manager.name	ubuntuwazuh
data.parameters.alert.rule.description	GoldenEye DoS attack has been detected.
data.parameters.alert.rule.firedtimes	1
data.parameters.alert.rule.groups	custom_active_response_rules
data.parameters.alert.rule.id	100200
data.parameters.alert.rule.level	12
data.parameters.alert.rule.mail	true
data.parameters.alert.rule.mitre.id	T1498
data.parameters.alert.rule.mitre.tactic	Impact
data.parameters.alert.rule.mitre.technique	Network Denial of Service
data.parameters.alert.timestamp	2023-05-10T19:35:18.889-0400
data.parameters.extra_args	
data.parameters.program	active-response/bin/firewall-drop
data.version	1
decoder.name	ar_log_json
	2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T19:35:18.889-0400","rule":{"level":12,"description":"GoldenEye DoS attack has been detected. ","id":"100200","mitre":{"id":["T1498"],"tactic":["Impact"],"technique":["Network Denial of Service"]},"firedtimes":1,"mail":true,"groups":["custom_active_response_rules"]},"agent":{"id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683761718.12291360","full_log":"

Figure 19 - Wazuh DDoS - Host Blocked by firewall-drop Active Response event log

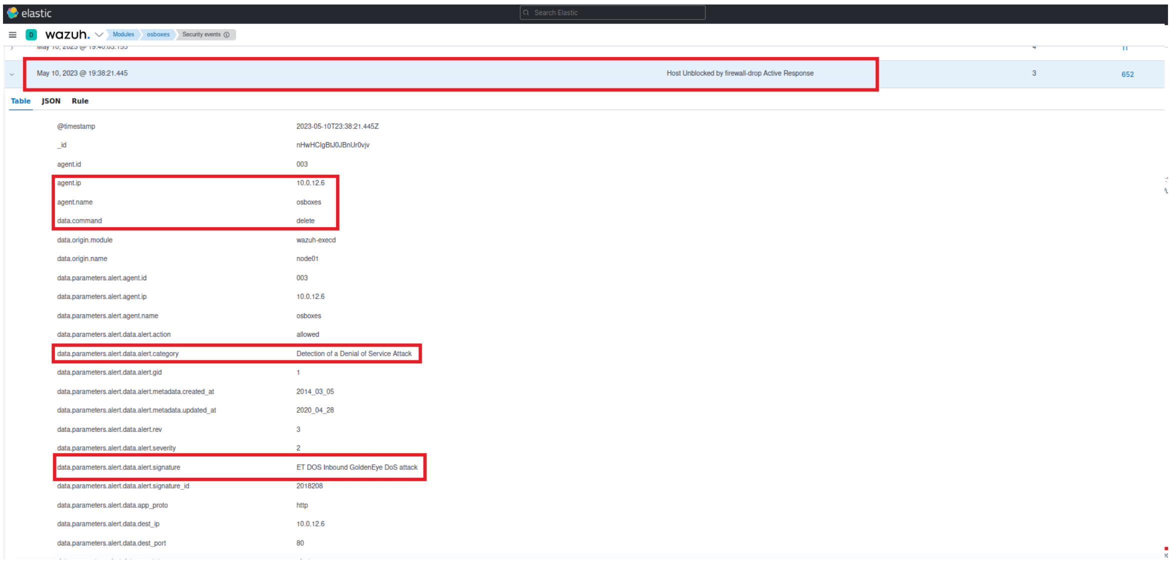
We can see in the figure 20 the agent active-response.log of the Wazuh client with the active response alert that blocked the DDoS attack.



```
/nmap.org/book/nse.html)","http_method":"GET","protocol":"HTTP/1.1","length":"0"},"app_proto":"http","flow":{"pkts_t
oserver":"6","pkts_toclient":"3","bytes_toserver":"706","bytes_toclient":"214","start":"2023-05-10T17:07:45.504601-0
400"}},"location":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 17:10:47 active-response/bin/firewall-drop: Ended
2023/05/10 19:35:18 active-response/bin/firewall-drop: Starting
2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T19:35:18.889-0400","rule":{"level":
12,"description":"GoldenEye DoS attack has been detected. ","id":"100200","mitre":{"id":["T1498"],"tactic":["Impact"
],"technique":["Network Denial of Service"]},"firedtimes":1,"mail":true,"groups":["custom_active_response_rules"]},"
agent":{"id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683761718.12291360","f
ull_log":"{\"timestamp\":\"2023-05-10T19:35:14.988150-0400\",\"flow_id\":981529584079110,\"in_iface\":\"enp0s3\",\"e
vent_type\":\"alert\",\"src_ip\":\"10.0.12.20\",\"src_port\":40010,\"dest_ip\":\"10.0.12.6\",\"dest_port\":80,\"prot
o\":\"TCP\",\"tx_id\":0,\"alert\":{\"action\":\"allowed\",\"gid\":1,\"signature_id\":2018208,\"rev\":3,\"signature\"
:\"ET DOS Inbound GoldenEye DoS attack\",\"category\":\"Detection of a Denial of Service Attack\",\"severity\":2,\"m
etadata\":{\"created_at\":[\"2014_03_05\"],\"updated_at\":[\"2020_04_28\"]}},\"http\":{\"hostname\":\"10.0.12.6\",\"
url\":\"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K\",\"http_user_age
nt\":\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 Safa
ri/537.23\",\"http_method\":\"GET\",\"protocol\":\"HTTP/1.1\",\"length\":0},\"app_proto\":\"http\",\"flow\":{\"pkts_
toserver\":4,\"pkts_toclient\":2,\"bytes_toserver\":684,\"bytes_toclient\":140,\"start\":\"2023-05-10T19:35:14.98739
8-0400\"}}","decoder":{"name":"json"},"data":{"srcip":"10.0.12.20","timestamp":"2023-05-10T19:35:14.988150-0400","fl
ow_id":"981529584079110.000000","in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.12.20","src_port":"40010","d
est_ip":"10.0.12.6","dest_port":"80","proto":"TCP","tx_id":"0","alert":{"action":"allowed","gid":"1","signature_id":
"2018208","rev":"3","signature":"ET DOS Inbound GoldenEye DoS attack","category":"Detection of a Denial of Service A
ttack","severity":"2","metadata":{"created_at":["2014_03_05"],"updated_at":["2020_04_28"]}},"http":{"hostname":"10.0
.12.6","url":"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K","http_user
_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 Sa
fari/537.23","http_method":"GET","protocol":"HTTP/1.1","length":"0"},"app_proto":"http","flow":{"pkts_toserver":"4",
"pkts_toclient":"2","bytes_toserver":"684","bytes_toclient":"140","start":"2023-05-10T19:35:14.987398-0400"}},"locat
ion":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"firewall-drop","module":"activ
e-response"},"command":"check_keys","parameters":{"keys":["10.0.12.20"]}}
2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"continue","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T19:35:18.889-0400","rule":{"le
```

Figure 20 - Wazuh DDoS - Host Blocked by firewall-drop Active Response event log (agent active-response.log)

We can see in the figure 21 the Wazuh active response alert that unblocked in the Wazuh agent the DDoS attack.

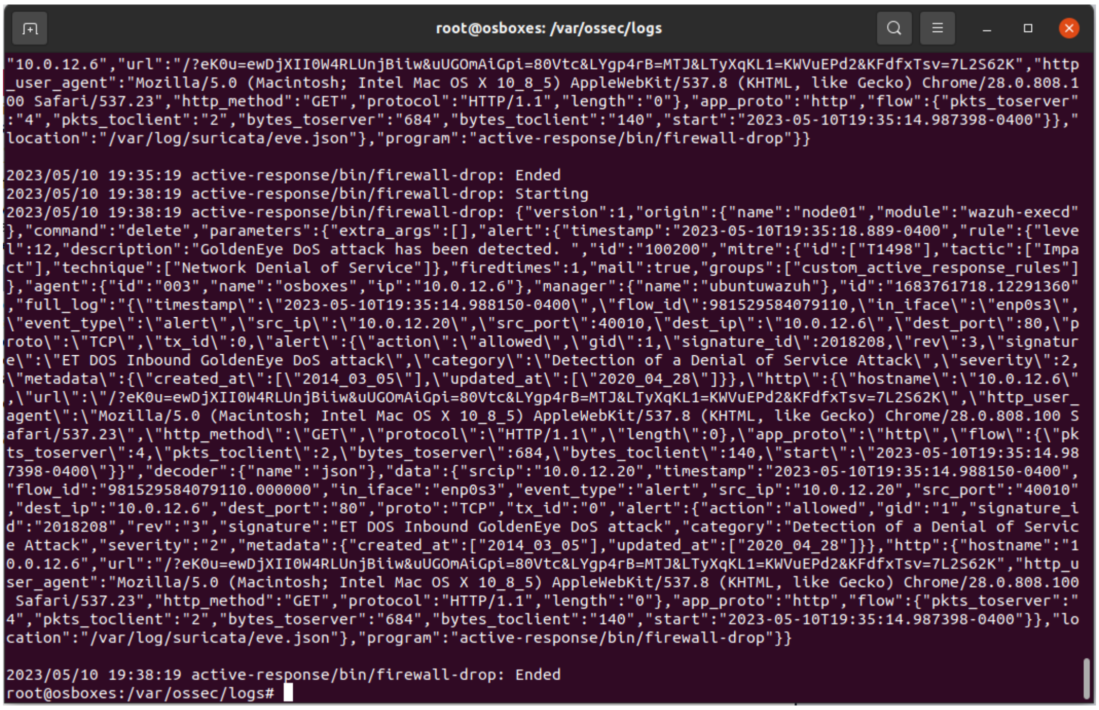


May 10, 2023 @ 19:38:21.445	Host Unblocked by firewall-drop Active Response	3	652

@timestamp	2023-05-10T23:38:21.445Z
_id	nHwHClgBtJ0JBnUr0vjv
agent.id	003
agent.ip	10.0.12.6
agent.name	osboxes
data.command	delete
data.origin.module	wazuh-execd
data.origin.name	node01
data.parameters.alert.agent.id	003
data.parameters.alert.agent.ip	10.0.12.6
data.parameters.alert.agent.name	osboxes
data.parameters.alert.data.alert.action	allowed
data.parameters.alert.data.alert.category	Detection of a Denial of Service Attack
data.parameters.alert.data.alert.gid	1
data.parameters.alert.data.alert.metadata.created_at	2014_03_05
data.parameters.alert.data.alert.metadata.updated_at	2020_04_28
data.parameters.alert.data.alert.rev	3
data.parameters.alert.data.alert.severity	2
data.parameters.alert.data.alert.signature	ET DOS Inbound GoldenEye DoS attack
data.parameters.alert.data.alert.signature_id	2018208
data.parameters.alert.data.app_proto	http
data.parameters.alert.data.dest_ip	10.0.12.6
data.parameters.alert.data.dest_port	80

Figure 21 - Wazuh DDoS - Host Unblocked by firewall-drop Active Response event log

We can see in the figure 22 the agent active-response.log of the Wazuh client with the active response alert that unblocked the DDoS attack.



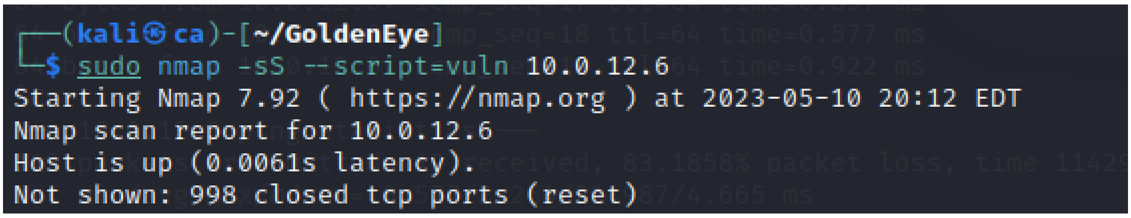
```
"10.0.12.6","url":"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K","http
_user_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.1
00 Safari/537.23","http_method":"GET","protocol":"HTTP/1.1","length":"0"},"app_proto":"http","flow":{"pkts_toserver"
:"4","pkts_toclient":"2","bytes_toserver":"684","bytes_toclient":"140","start":"2023-05-10T19:35:14.987398-0400"}},"
location":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 19:35:19 active-response/bin/firewall-drop: Ended
2023/05/10 19:38:19 active-response/bin/firewall-drop: Starting
2023/05/10 19:38:19 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"delete","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T19:35:18.889-0400","rule":{"leve
l":12,"description":"GoldenEye DoS attack has been detected. ","id":"100200","mitre":{"id":["T1498"],"tactic":["Impa
ct"],"technique":["Network Denial of Service"]},"firedtimes":1,"mail":true,"groups":["custom_active_response_rules"]
},"agent":{"id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683761718.12291360"
,"full_log":"{\"timestamp\":\"2023-05-10T19:35:14.988150-0400\",\"flow_id\":981529584079110,\"in_iface\":\"enp0s3\",
\"event_type\":\"alert\",\"src_ip\":\"10.0.12.20\",\"src_port\":40010,\"dest_ip\":\"10.0.12.6\",\"dest_port\":80,\"p
roto\":\"TCP\",\"tx_id\":0,\"alert\":{\"action\":\"allowed\",\"gid\":1,\"signature_id\":2018208,\"rev\":3,\"signatur
e\":\"ET DOS Inbound GoldenEye DoS attack\",\"category\":\"Detection of a Denial of Service Attack\",\"severity\":2,
\"metadata\":{\"created_at\":[\"2014_03_05\"],\"updated_at\":[\"2020_04_28\"]}},\"http\":{\"hostname\":\"10.0.12.6\"
,\"url\":\"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K\",\"http_user_
agent\":\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 S
afari/537.23\",\"http_method\":\"GET\",\"protocol\":\"HTTP/1.1\",\"length\":0},\"app_proto\":\"http\",\"flow\":{\"pk
ts_toserver\":4,\"pkts_toclient\":2,\"bytes_toserver\":684,\"bytes_toclient\":140,\"start\":\"2023-05-10T19:35:14.98
7398-0400\"}}","decoder":{"name":"json"},"data":{"srcip":"10.0.12.20","timestamp":"2023-05-10T19:35:14.988150-0400",
"flow_id":"981529584079110.000000","in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.12.20","src_port":"40010"
,"dest_ip":"10.0.12.6","dest_port":"80","proto":"TCP","tx_id":"0","alert":{"action":"allowed","gid":"1","signature_i
d":"2018208","rev":"3","signature":"ET DOS Inbound GoldenEye DoS attack","category":"Detection of a Denial of Servic
e Attack","severity":"2","metadata":{"created_at":["2014_03_05"],"updated_at":["2020_04_28"]}},"http":{"hostname":"1
0.0.12.6","url":"/?eK0u=ewDjXII0W4RLUnjBiiw&uUGOmAiGpi=80Vtc&LYgp4rB=MTJ&LTyXqKL1=KWVuEPd2&KFdfxTsv=7L2S62K","http_u
ser_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100
 Safari/537.23","http_method":"GET","protocol":"HTTP/1.1","length":"0"},"app_proto":"http","flow":{"pkts_toserver":"
4","pkts_toclient":"2","bytes_toserver":"684","bytes_toclient":"140","start":"2023-05-10T19:35:14.987398-0400"}},"lo
cation":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 19:38:19 active-response/bin/firewall-drop: Ended
root@osboxes:/var/ossec/logs#
```

Figure 22 - Wazuh DDoS - Host Unblocked by firewall-drop Active Response event log (agent active-response.log)

6.2. Attack emulation 2: NMAP at Healthcare System web portal

Nmap is an active reconnaissance tool used to gather information on infrastructure. From the Kali endpoint, we perform an Nmap scan against the web server (Healthcare System web portal) on the Ubuntu endpoint using the command below:

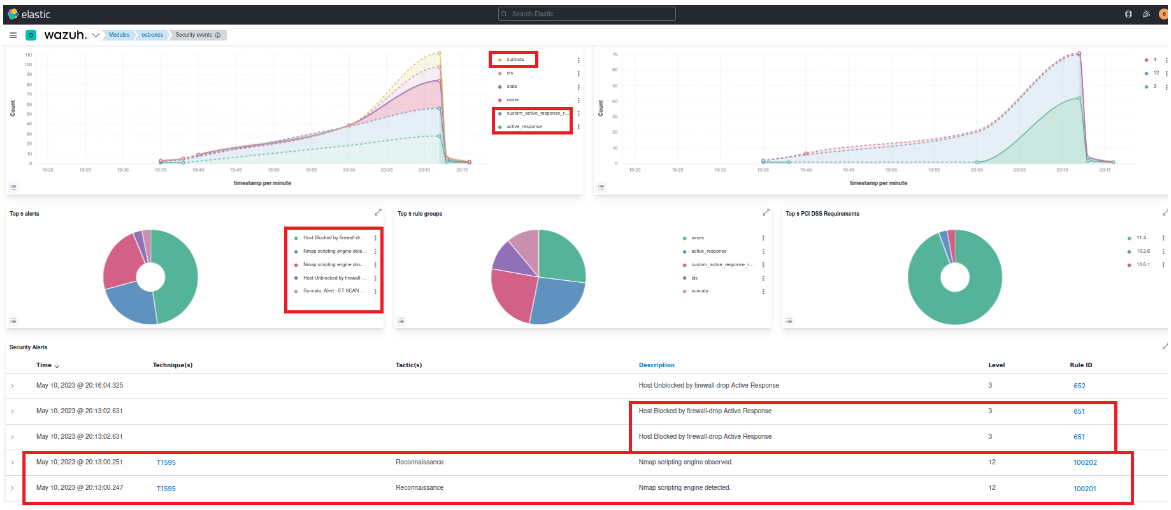
sudo nmap -sS --script=vuln <Ubuntu_IP>



```
┌──(kali㉿ca)-[~/GoldenEye]
└─$ sudo nmap -sS --script=vuln 10.0.12.6
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-10 20:12 EDT
Nmap scan report for 10.0.12.6
Host is up (0.0061s latency).
Not shown: 998 closed tcp ports (reset)
```

Figure 23 - Nmap command to scan the Healthcare System web portal

We can see in the figure 24 the Wazuh active response alert that blocked the NMAP scan.



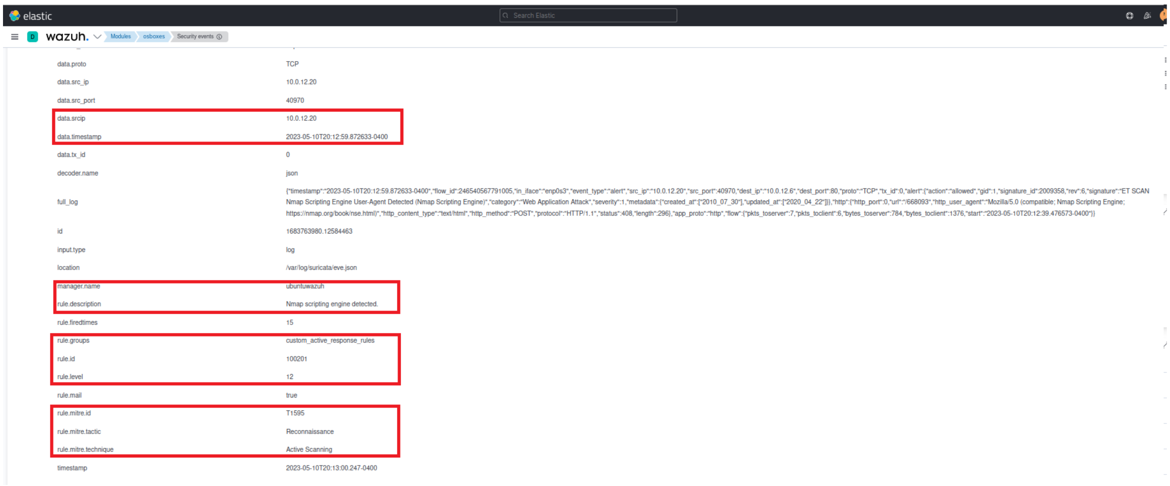
elastic
Search Elastic
wazuh.
Modules
ossbsses
Security events
Count
timestamp per minute
suricata
ids
stats
ossec
custom_active_response_r...
active_response
Top 5 alerts
Host Blocked by firewall-dr...
Nmap scripting engine dete...
Nmap scripting engine obs...
Host Unblocked by firewall-...
Suricata: Alert - ET SCAN ...
Top 5 rule groups
ossec
active_response
custom_active_response_r...
ids
suricata
Top 5 PCI DSS Requirements
11.4
10.2.6
10.6.1

Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 10, 2023 @ 20:16:04.325			Host Unblocked by firewall-drop Active Response	3	652
May 10, 2023 @ 20:13:02.631			Host Blocked by firewall-drop Active Response	3	651
May 10, 2023 @ 20:13:02.631			Host Blocked by firewall-drop Active Response	3	651
May 10, 2023 @ 20:13:00.251	T1595	Reconnaissance	Nmap scripting engine observed.	12	100202
May 10, 2023 @ 20:13:00.247	T1595	Reconnaissance	Nmap scripting engine detected.	12	100201

Figure 24 - Wazuh NMAP - Active response alert that blocked the NMAP

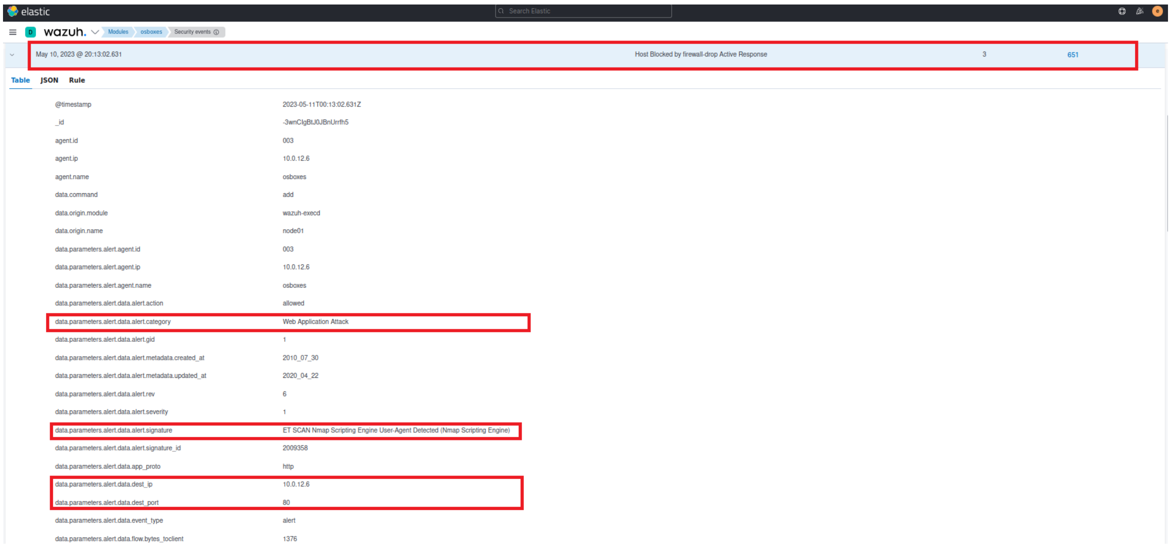
We can see in the figure 25 the event log of the Wazuh active response alert that blocked the NMAP scan.



data.proto	TCP
data.src_ip	10.0.12.20
data.src_port	40970
data.srcip	10.0.12.20
data.timestamp	2023-05-10T20:12:59.872633-0400
data.tx_id	0
decoder.name	json
full_log	{"timestamp":"2023-05-10T20:12:59.872633-0400","flow_id":246540567791005,"in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.12.20","src_port":40970,"dest_ip":"10.0.12.6","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009358,"rev":6,"signature":"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)","category":"Web Application Attack","severity":1,"metadata":{"created_at":["2010_07_30"],"updated_at":["2020_04_22"]}},"http":{"http_port":0,"url":"/668093","http_user_agent":"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)","http_content_type":"text/html","http_method":"POST","protocol":"HTTP/1.1","status":408,"length":296},"app_proto":"http","flow":{"pkts_toserver":7,"pkts_toclient":6,"bytes_toserver":784,"bytes_toclient":1376,"start":"2023-05-10T20:12:39.476573-0400"}}
id	1683763980.12584463
input.type	log
location	/var/log/suricata/eve.json
manager.name	ubuntuwazuh
rule.description	Nmap scripting engine detected.
rule.firedtimes	15
rule.groups	custom_active_response_rules
rule.id	100201
rule.level	12
rule.mail	true
rule.mitre.id	T1595
rule.mitre.tactic	Reconnaissance
rule.mitre.technique	Active Scanning
timestamp	2023-05-10T20:13:00.247-0400

Figure 25 - Wazuh NMAP attack event log

We can see in the figure 26 the Wazuh active response alert that blocked in the Wazuh agent the NMAP scan.

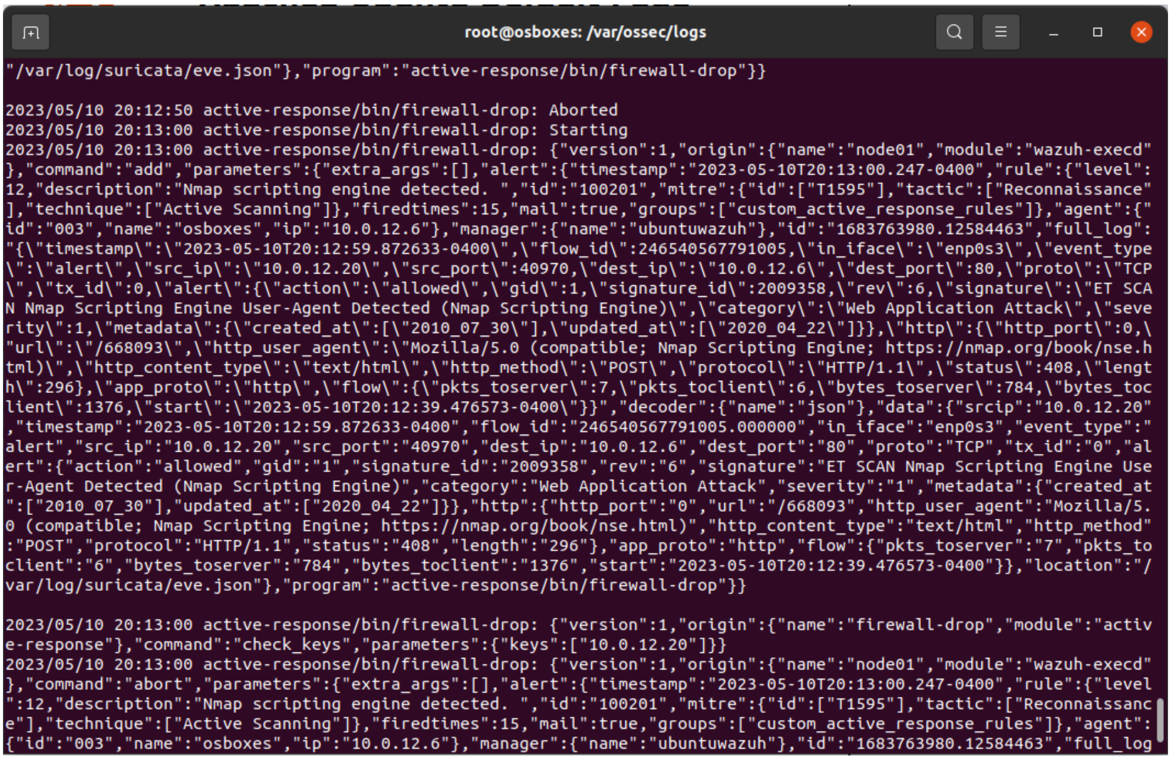


May 10, 2023 @ 20:13:02.631	Host Blocked by firewall-drop Active Response	3	651

@timestamp	2023-05-11T00:13:02.631Z
_id	-3wnCIgBtJ0JBnUrrfh5
agent.id	003
agent.ip	10.0.12.6
agent.name	osboxes
data.command	add
data.origin.module	wazuh-execd
data.origin.name	node01
data.parameters.alert.agent.id	003
data.parameters.alert.agent.ip	10.0.12.6
data.parameters.alert.agent.name	osboxes
data.parameters.alert.data.alert.action	allowed
data.parameters.alert.data.alert.category	Web Application Attack
data.parameters.alert.data.alert.gid	1
data.parameters.alert.data.alert.metadata.created_at	2010_07_30
data.parameters.alert.data.alert.metadata.updated_at	2020_04_22
data.parameters.alert.data.alert.rev	6
data.parameters.alert.data.alert.severity	1
data.parameters.alert.data.alert.signature	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
data.parameters.alert.data.alert.signature_id	2009358
data.parameters.alert.data.app_proto	http
data.parameters.alert.data.dest_ip	10.0.12.6
data.parameters.alert.data.dest_port	80
data.parameters.alert.data.event_type	alert
data.parameters.alert.data.flow.bytes_toclient	1376

Figure 26 - Wazuh NMAP - Host Blocked by firewall-drop Active Response event log

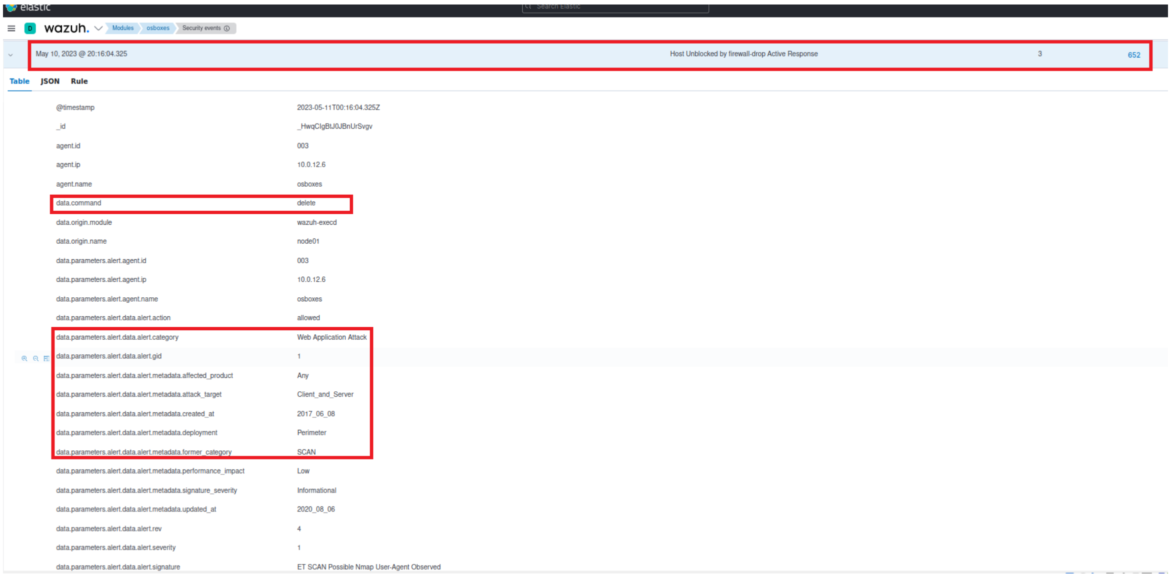
We can see in the figure 27 the agent active-response.log of the Wazuh client with the active response alert that blocked the NMAP scan.



```
"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 20:12:50 active-response/bin/firewall-drop: Aborted
2023/05/10 20:13:00 active-response/bin/firewall-drop: Starting
2023/05/10 20:13:00 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T20:13:00.247-0400","rule":{"level":
12,"description":"Nmap scripting engine detected. ","id":"100201","mitre":{"id":["T1595"],"tactic":["Reconnaissance"
],"technique":["Active Scanning"]},"firedtimes":15,"mail":true,"groups":["custom_active_response_rules"]},"agent":{"
id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683763980.12584463","full_log":
"{\"timestamp\":\"2023-05-10T20:12:59.872633-0400\",\"flow_id\":246540567791005,\"in_iface\":\"enp0s3\",\"event_type
\":\"alert\",\"src_ip\":\"10.0.12.20\",\"src_port\":40970,\"dest_ip\":\"10.0.12.6\",\"dest_port\":80,\"proto\":\"TCP
\",\"tx_id\":0,\"alert\":{\"action\":\"allowed\",\"gid\":1,\"signature_id\":2009358,\"rev\":6,\"signature\":\"ET SCA
N Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)\",\"category\":\"Web Application Attack\",\"seve
rity\":1,\"metadata\":{\"created_at\":[\"2010_07_30\"],\"updated_at\":[\"2020_04_22\"]}},\"http\":{\"http_port\":0,\
"url\":\"/668093\",\"http_user_agent\":\"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.h
tml)\",\"http_content_type\":\"text/html\",\"http_method\":\"POST\",\"protocol\":\"HTTP/1.1\",\"status\":408,\"lengt
h\":296},\"app_proto\":\"http\",\"flow\":{\"pkts_toserver\":7,\"pkts_toclient\":6,\"bytes_toserver\":784,\"bytes_toc
lient\":1376,\"start\":\"2023-05-10T20:12:39.476573-0400\"}}","decoder":{"name":"json"},"data":{"srcip":"10.0.12.20"
,"timestamp":"2023-05-10T20:12:59.872633-0400","flow_id":"246540567791005.000000","in_iface":"enp0s3","event_type":"
alert","src_ip":"10.0.12.20","src_port":"40970","dest_ip":"10.0.12.6","dest_port":"80","proto":"TCP","tx_id":"0","al
ert":{"action":"allowed","gid":"1","signature_id":"2009358","rev":"6","signature":"ET SCAN Nmap Scripting Engine Use
r-Agent Detected (Nmap Scripting Engine)","category":"Web Application Attack","severity":"1","metadata":{"created_at
":["2010_07_30"],"updated_at":["2020_04_22"]}},"http":{"http_port":"0","url":"/668093","http_user_agent":"Mozilla/5.
0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)","http_content_type":"text/html","http_method"
:"POST","protocol":"HTTP/1.1","status":"408","length":"296"},"app_proto":"http","flow":{"pkts_toserver":"7","pkts_to
client":"6","bytes_toserver":"784","bytes_toclient":"1376","start":"2023-05-10T20:12:39.476573-0400"}},"location":"/
var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 20:13:00 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"firewall-drop","module":"activ
e-response"},"command":"check_keys","parameters":{"keys":["10.0.12.20"]}}
2023/05/10 20:13:00 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"abort","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T20:13:00.247-0400","rule":{"level
":12,"description":"Nmap scripting engine detected. ","id":"100201","mitre":{"id":["T1595"],"tactic":["Reconnaissanc
e"],"technique":["Active Scanning"]},"firedtimes":15,"mail":true,"groups":["custom_active_response_rules"]},"agent":
{"id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683763980.12584463","full_log
```

Figure 27 - Wazuh NMAP - Host Blocked by firewall-drop Active Response event log (agent active-response.log)

We can see in the figure 28 the Wazuh active response alert that unblocked in the Wazuh agent the NMAP scan.

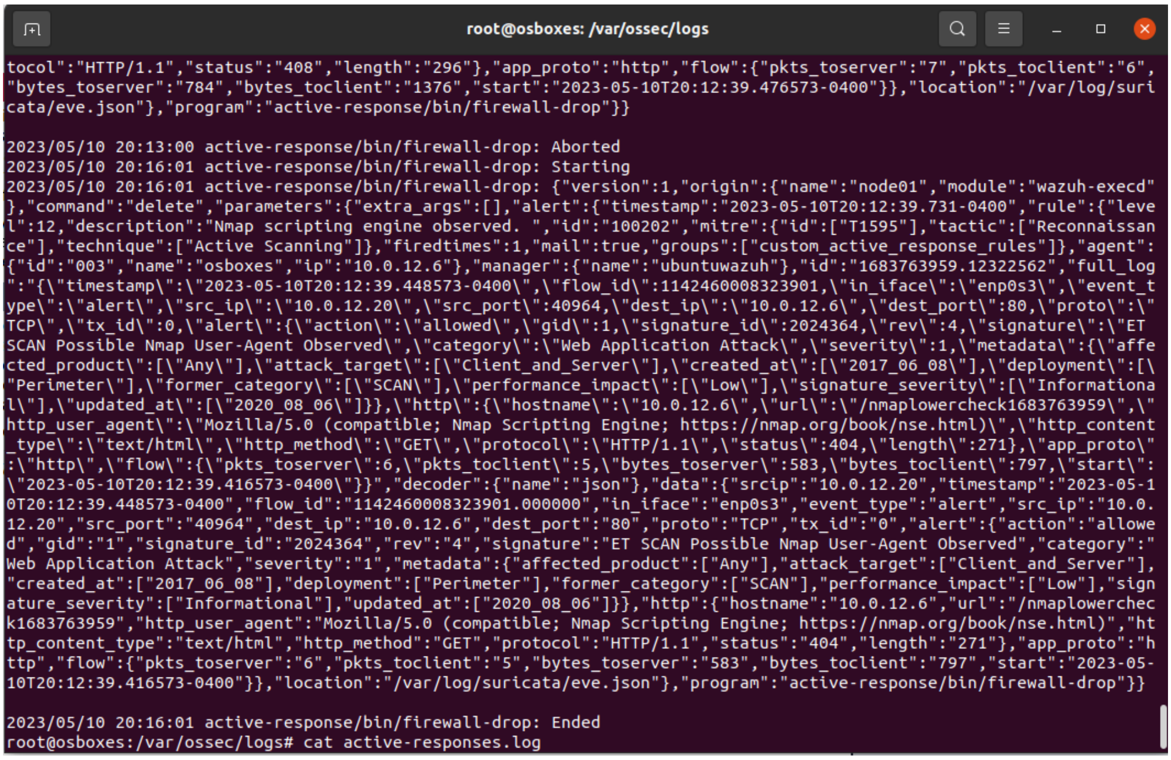


May 10, 2023 @ 20:16:04.325 Host Unblocked by firewall-drop Active Response 3 652

@timestamp	2023-05-11T00:16:04.325Z
_id	_HwqClgBtJ0JBnUrSvgv
agent.id	003
agent.ip	10.0.12.6
agent.name	osboxes
data.command	delete
data.origin.module	wazuh-execd
data.origin.name	node01
data.parameters.alert.agent.id	003
data.parameters.alert.agent.ip	10.0.12.6
data.parameters.alert.agent.name	osboxes
data.parameters.alert.data.alert.action	allowed
data.parameters.alert.data.alert.category	Web Application Attack
data.parameters.alert.data.alert.gid	1
data.parameters.alert.data.alert.metadata.affected_product	Any
data.parameters.alert.data.alert.metadata.attack_target	Client_and_Server
data.parameters.alert.data.alert.metadata.created_at	2017_06_08
data.parameters.alert.data.alert.metadata.deployment	Perimeter
data.parameters.alert.data.alert.metadata.former_category	SCAN
data.parameters.alert.data.alert.metadata.performance_impact	Low
data.parameters.alert.data.alert.metadata.signature_severity	Informational
data.parameters.alert.data.alert.metadata.updated_at	2020_08_06
data.parameters.alert.data.alert.rev	4
data.parameters.alert.data.alert.severity	1
data.parameters.alert.data.alert.signature	ET SCAN Possible Nmap User-Agent Observed

Figure 28 - Wazuh NMAP - Host Unblocked by firewall-drop Active Response event log

We can see in the figure 29 the agent active-response.log of the Wazuh client with the active response alert that unblocked the NMAP scan.



```
tocol":"HTTP/1.1","status":"408","length":"296"},"app_proto":"http","flow":{"pkts_toserver":"7","pkts_toclient":"6",
"bytes_toserver":"784","bytes_toclient":"1376","start":"2023-05-10T20:12:39.476573-0400"}},"location":"/var/log/suri
cata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 20:13:00 active-response/bin/firewall-drop: Aborted
2023/05/10 20:16:01 active-response/bin/firewall-drop: Starting
2023/05/10 20:16:01 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"delete","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T20:12:39.731-0400","rule":{"leve
l":12,"description":"Nmap scripting engine observed. ","id":"100202","mitre":{"id":["T1595"],"tactic":["Reconnaissan
ce"],"technique":["Active Scanning"]},"firedtimes":1,"mail":true,"groups":["custom_active_response_rules"]},"agent":
{"id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683763959.12322562","full_log
":"{\"timestamp\":\"2023-05-10T20:12:39.448573-0400\",\"flow_id\":1142460008323901,\"in_iface\":\"enp0s3\",\"event_t
ype\":\"alert\",\"src_ip\":\"10.0.12.20\",\"src_port\":40964,\"dest_ip\":\"10.0.12.6\",\"dest_port\":80,\"proto\":\"
TCP\",\"tx_id\":0,\"alert\":{\"action\":\"allowed\",\"gid\":1,\"signature_id\":2024364,\"rev\":4,\"signature\":\"ET
SCAN Possible Nmap User-Agent Observed\",\"category\":\"Web Application Attack\",\"severity\":1,\"metadata\":{\"affe
cted_product\":[\"Any\"],\"attack_target\":[\"Client_and_Server\"],\"created_at\":[\"2017_06_08\"],\"deployment\":[\
"Perimeter\"],\"former_category\":[\"SCAN\"],\"performance_impact\":[\"Low\"],\"signature_severity\":[\"Informationa
l\"],\"updated_at\":[\"2020_08_06\"]}},\"http\":{\"hostname\":\"10.0.12.6\",\"url\":\"/nmaplowercheck1683763959\",\"
http_user_agent\":\"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\",\"http_content
_type\":\"text/html\",\"http_method\":\"GET\",\"protocol\":\"HTTP/1.1\",\"status\":404,\"length\":271},\"app_proto\"
:\"http\",\"flow\":{\"pkts_toserver\":6,\"pkts_toclient\":5,\"bytes_toserver\":583,\"bytes_toclient\":797,\"start\":
\"2023-05-10T20:12:39.416573-0400\"}}","decoder":{"name":"json"},"data":{"srcip":"10.0.12.20","timestamp":"2023-05-1
0T20:12:39.448573-0400","flow_id":"1142460008323901.000000","in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.
12.20","src_port":"40964","dest_ip":"10.0.12.6","dest_port":"80","proto":"TCP","tx_id":"0","alert":{"action":"allowe
d","gid":"1","signature_id":"2024364","rev":"4","signature":"ET SCAN Possible Nmap User-Agent Observed","category":"
Web Application Attack","severity":"1","metadata":{"affected_product":["Any"],"attack_target":["Client_and_Server"],
"created_at":["2017_06_08"],"deployment":["Perimeter"],"former_category":["SCAN"],"performance_impact":["Low"],"sign
ature_severity":["Informational"],"updated_at":["2020_08_06"]}},"http":{"hostname":"10.0.12.6","url":"/nmaplowerchec
k1683763959","http_user_agent":"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)","ht
tp_content_type":"text/html","http_method":"GET","protocol":"HTTP/1.1","status":"404","length":"271"},"app_proto":"h
ttp","flow":{"pkts_toserver":"6","pkts_toclient":"5","bytes_toserver":"583","bytes_toclient":"797","start":"2023-05-
10T20:12:39.416573-0400"}},"location":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 20:16:01 active-response/bin/firewall-drop: Ended
root@osboxes:/var/ossec/logs# cat active-responses.log
```

Figure 29 - Wazuh NMAP- Host Unblocked by firewall-drop Active Response event log (agent active-response.log)

7. Conclusions and future development

This chapter concludes the thesis and briefly mentions some of the possible research direction that can be explored to expand and improve this work

This implementation demonstrated how the combination of Suricata for network event detection and Wazuh for analysis and automated response can effectively protect your organization from network-based attacks. It provides a practical example of Wazuh's active response module in action by illustrating its response to a Distributed denial-of-service (DDoS) attack and an Nmap scan in our eHealth use case.

As part of the research I also analyzed and discussed with professors during the Cybersecurity Incident Response training what could be taken as a lessons learned in a recent eHealth cyber attack at Hospital Clinic [22] and the key takeaways are :

- Have the proper tooling (EDR/XDR/SIEM/Firewall) installed and configured to detect and respond to cyber attacks. They had installed the tool **Sophos** that is recognized as one of the leaders in the EDR/XDR Magic Quadrant at Gartner but it was not properly configured to automatically respond to that attack.

- Have a good plan for incident response and review of these processes frequently. As part of the improvement the Cybersecurity Agency of Catalonia will integrate Hospital Clinic in their Health SOC service that will help with additional support to plan for incident response, vulnerability assessments, penetration testing, risk analysis and improve the communication plan.

- Have the people with the right skill and experience to respond to the cyber attack. As part of the improvement the Cybersecurity Agency of Catalonia will integrate Hospital Clinic in their Health SOC service that will help with further expert knowledge. Additionally it will be important to provide regular training to staff on cybersecurity best practices.

In conclusion, cyber attacks in eHealth infrastructures can have severe consequences, and it is essential to have a system in place to respond to and adapt to these attacks promptly and efficiently. The system should include a plan for incident response, regular vulnerability assessments, penetration testing, risk analysis, automated responses and a comprehensive communication plan. It is also crucial to involve all stakeholders in the evaluation process and to define mitigation strategies to ensure business continuity. By implementing these measures, healthcare providers can protect patient data and ensure the continuity of care in the event of a cyber attack.

7.1. Future Works

Some improvements can be made to the proposed system, with some regarding the usage of additional Wazuh modules or integration of external features.

One of the improvements would be including the additional Wazuh module called Malware detection, it uses a non-signature-based approach and is capable of detecting anomalies and the possible presence of rootkits. Also, it looks for hidden processes, hidden files, and hidden ports while monitoring system calls.

As part of the external features would be including the integration VirusTotal, as it aggregates many antivirus products and online scan engines, offering an API that can be queried by using either URLs, IPs, domains or file hashes.

The Wazuh integration can automatically perform a request to VirusTotal API with the hashes of files that are created or changed in any folder monitored with FIM.

If VirusTotal's response is positive Wazuh will generate an alert in the system:

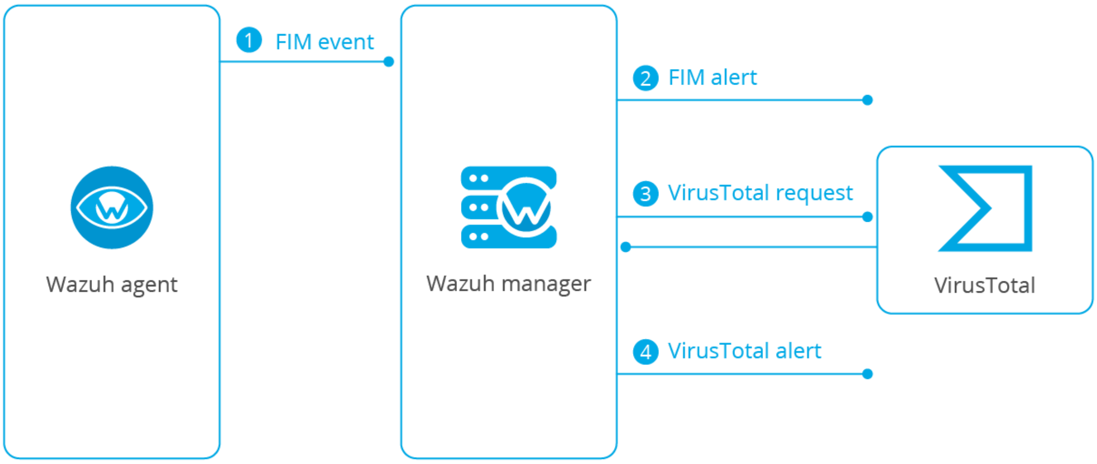


Figure 30 - Wazuh Virus Total Integration

https://wazuh.com/uploads/2020/07/virustotal-flow-diagram.png

(1)File monitoring. The FIM module detects a file change and triggers an alert (2).

(3) VirusTotal request. After FIM triggers an alert, the Wazuh manager queries VirusTotal with the hash of the file.

(4) Alerting. If positive matches are found, the Wazuh manager generates a VirusTotal alert.

Bibliography

[1] Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), pp. 618-623. IEEE, 2017.

[2] Deng, Zhiliang, Yongjun Ren, Yepeng Liu, Xiang Yin, Zixuan Shen, and Hye-Jin Kim. "Blockchain-based trusted electronic records preservation in cloud storage." Comput. Mater. Continua 58, no. 1 (2019): 135-151.

[3] Vankamamidi S, Naresh, Suryateja, S. Pericherla, Pilla Sita Rama, Murty, Sivaranjani Reddy, “Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions”, Comput Syst Sci & Eng (2020) 6: 411–421 © 2020 Tech Science Press

[4] Wang, J, Chen, W, Wang, L, Ren, Y, and Sherratt, R, “Blockchain-based data storage mechanism for the industrial internet of things”, Intelligent Automation and Soft Computing, 26 (5). pp. 1157-1172. ISSN 2326-005X

[5] Pranav Ratta, Amanpreet Kaur, Sparsh Sharma, Mohammad Shabaz, and Gaurav Dhiman, “Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives”, Hindawi Journal of Food Quality Volume 2021, Article ID 7608296, 20 pages

[6] Luis Fernandes, “Data security and privacy in times of pandemic”, Proceedings of the digital Privacy and security conference, 2021.

[7] Bhosale, Karuna S., Maria Nenova, and Georgi Iliev. "A study of cyber-attacks: In the healthcare sector." In 2021 Sixth Junior Conference on Lighting (Lighting), pp. 1-6. IEEE, 2021.

[8] Chen, Hao, Xueqin Jia, and Heng Li. "A brief introduction to IoT gateway." In IET international conference on communication technology and application (ICCTA 2011), pp. 610-613. IET, 2011.

[9] José Luis, Fernández-Alemán, Inmaculada Carrión Señor, Pedro Ángel Oliver Lozoya, Ambrosio Toval “Security and privacy in electronic health records: A systematic literature review”, Journal of Biomedical Informatics 46 (2013) 541–562

[10] Mohammad Zarour, Mamdouh Alenezi, Md Tarique Jamal Ansari, Abhishek Kumar Pandey, Masood Ahmad, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan, “Ensuring data integrity of healthcare information in the era of digital health”, Healthcare Technology Letters, 23 March 2021

[11] Delia Ioana Dogaru, I. D. (2017). Cyber Security in Healthcare Networks. International Conference on E-Health and Bioengineering (pp. 414-417). Sinaia,Romania: IEEE.

[12] Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In 2017 IEEE international congress on big data (BigData congress), pp. 557-564. Ieee, 2017.

[13] M. Scott, N. Wingfield, Hacking attack has security experts scrambling to contain fallout, New York Times, (2017) https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html .

[14] S. Mansfield-Devine, Ransomware: taking businesses hostage, Netw. Secur. 2016, (2016), pp. 8–17, http://dx.doi.org/10.1016/S1353-4858(16)30096-4.

[15] R. Winton, Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating, Los Angeles Times, (2016) https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html. (Accessed 19 February 2018).

[16] A. Morse - National Audit Office Investigation: WannaCry cyber attack and the NHS https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf . (Accessed 19 February 2018).

[17] D. Storm, MEDJACK, Hackers hijacking medical devices to create backdoors in hospital networks, Comput. World, (2015), p. 8 https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html . (Accessed 19 February 2018).

[18] Zhou, Zhili, Akshat Gaurav, B. B. Gupta, Hedi Hamdi, and Nadia Nedjah. "A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic." Neural Computing and Applications (2021): 1-14.

[19] Ray, Soumya, and Sandip Dutta. "DDoS Detection and Prevention of Attacks on M-Health Sensitive Data: A novel approach." (2022).

[20] [12] S. Stein and J. Jacobs, “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak,” 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response . [Accessed: 04-May-2020].

[21] A. Mercader / S. Cid, “The Ransomexx gang claims responsibility for the cyberattack against Catalan hospitals and leaks patient data,” 2022. [Online]. Available: https://cronicaglobal.elespanol.com/vida/ransomexx-ciberataque-hospitales-catalanes-filtra-datos-pacientes_728849_102.html. [Accessed: 17-Feb-2023].

[22] N. Portella, “The cyberattack that has paralysed Barcelona's Hospital Clínic: "No ransom will be paid"” 2023. [Online]. Available: https://www.elnacional.cat/en/news/cyberattack-paralysed-barcelona-hospital-clinic-no-ransom-paid_982914_102.html. [Accessed: 06-Mar-2023].

[23] A.Chuvakin, Gartner “Named Endpoint Threat Detection & Response-Anton Chuvakin” Gartner [Online] Available:

http://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/ [Accessed: 26 July 2013].

[24] C.Lawson, P. Firstbrook, P. WebberA.Chuvakin, Gartner “Market Guide for Extended Detection and Response” Gartner [Online] Available:

https://www.gartner.com/doc/reprints?id=1-283MGU5C&ct=211115&st=sb

[Accessed: 8 November 2021].

[25] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer security incident handling guide”, tech. rep., NIST, August 2012

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Appendix

In this chapter some information regarding how to run the proof of concept implementation discussed in chapter 5 is provided.

The commands provided were used to deploy it in an Ubuntu 22.04 environment.

Implementation prerequisites

Some extra packages are needed for the installation, such as curl or unzip, which will be used in further steps. However, this step can be skipped if curl and unzip are already installed on the server.

Install all the necessary packages:

```
 apt-get install apt-transport-https zip unzip lsb-release curl gnupg
```

Installing Elasticsearch

Elasticsearch is a highly scalable full-text search and analytics engine.

1 - Install the GPG key:

```
curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --no-default-keyring
--keyring gnupg-ring:/usr/share/keyrings/elasticsearch.gpg --import && chmod 644
/usr/share/keyrings/elasticsearch.gpg
```

2 - Add the repository

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

3 - Update the package information:

```
apt-get update
```

Elasticsearch installation and configuration

1 - Install the Elasticsearch package:

```
apt-get install elasticsearch=7.17.9
```

2- Download the configuration file /etc/elasticsearch/elasticsearch.yml as follows:

```
curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/4.4/tpl/elastic-basic/elasticsearch_all_in_one.yml
```

Certificates creation and deployment

1 - Download the configuration file for creating the certificates:

```
curl -so /usr/share/elasticsearch/instances.yml https://packages.wazuh.com/4.4/tpl/elastic-basic/instances_aio.yml
```

In the following steps, a file that contains a folder named after the instance defined here will be created. This folder will contain the certificates and the keys necessary to communicate with the Elasticsearch node using SSL.

2 - The certificates can be created using the elasticsearch-certutil tool:

```
/usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem --in instances.yml --keep-ca-key --out ~/certs.zip
```

3 - Extract the generated /usr/share/elasticsearch/certs.zip file from the previous step.

```
unzip ~/certs.zip -d ~/certs
```

4 - The next step is to create the directory /etc/elasticsearch/certs, and then copy the CA file, the certificate and the key there:

```
mkdir /etc/elasticsearch/certs/ca -p
cp -R ~/certs/ca/ ~/certs/elasticsearch/* /etc/elasticsearch/certs/
chown -R elasticsearch: /etc/elasticsearch/certs
chmod -R 500 /etc/elasticsearch/certs
chmod 400 /etc/elasticsearch/certs/ca/ca.* /etc/elasticsearch/certs/elasticsearch.*
rm -rf ~/certs/ ~/certs.zip
```

5 - Enable and start the Elasticsearch service:

```
systemctl daemon-reload
systemctl enable elasticsearch
systemctl start elasticsearch
```

6 - Generate credentials for all the Elastic Stack pre-built roles and users:

```
/usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
```

The command above will prompt an output like this. Save the password of the elastic user for further steps:

Output

```
Changed password for user elastic
PASSWORD elastic = AN4UeQGA7HGl5iHpMla7
```

To check that the installation was made successfully, run the following command replacing <elastic_password> with the password generated in the previous step for elastic user:

```
curl -XGET https://localhost:9200 -u elastic:<elastic_password> -k
```

Output

```
{
  "name" : "elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "CFw_rkxnR7avI7pBv9MvtQ",
  "version" : {
    "number" : "7.17.9",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "ef48222227ee6b9e70e502f0f0daa52435ee634d",
    "build_date" : "2023-01-31T05:34:43.305517834Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Installing Wazuh server

1 - Install the Wazuh manager package:

```
apt-get install wazuh-manager
```

2 - Enable and start the Wazuh manager service:

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

3 - Run the following command to check if the Wazuh manager is active:

```
systemctl status wazuh-manager
```

Installing Filebeat

Filebeat is the tool on the Wazuh server that securely forwards alerts and archived events to Elasticsearch.

Filebeat installation and configuration

1 - Install the Filebeat package:

```
apt-get install filebeat=7.17.9
```

2 - Download the pre-configured Filebeat config file used to forward Wazuh alerts to Elasticsearch:

```
curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.4/tpl/elastic-basic/filebeat_all_in_one.yml
```

3 - Download the alerts template for Elasticsearch:

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/4.4/extensions/elasticsearch/7.x/wazuh-template.json
```

```
chmod go+r /etc/filebeat/wazuh-template.json
```

4 - Download the Wazuh module for Filebeat:

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

5 - Edit the file /etc/filebeat/filebeat.yml and add the following line:

```
output.elasticsearch.password: <elasticsearch_password>
```

Values to be replaced:

<elasticsearch_password>: the password generated during the Elasticsearch installation and configuration for the elastic user.

Replace elasticsearch_password with the previously generated password for elastic user.

6 - Copy the certificates into /etc/filebeat/certs/

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

7 - Enable and start the Filebeat service:

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

To ensure that Filebeat has been successfully installed, run the following command:

```
filebeat test output
```

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: 7.17.9
```

Kibana installation and configuration

Kibana is a flexible and intuitive web interface for mining and visualizing the events and archives stored in Elasticsearch.

1 - Install the Kibana package:

```
apt-get install kibana=7.17.9
```

2 - Copy the Elasticsearch certificates into the Kibana configuration folder:

```
mkdir /etc/kibana/certs/ca -p
cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/
cp /etc/elasticsearch/certs/elasticsearch.key /etc/kibana/certs/kibana.key
cp /etc/elasticsearch/certs/elasticsearch.crt /etc/kibana/certs/kibana.crt
chown -R kibana:kibana /etc/kibana/
chmod -R 500 /etc/kibana/certs
chmod 440 /etc/kibana/certs/ca/ca.* /etc/kibana/certs/kibana.*
```

Edit the /etc/kibana/kibana.yml file:

elasticsearch.password: **<elasticsearch_password>**

Values to be replaced:

<elasticsearch_password>: the password generated during the Elasticsearch installation and configuration for the elastic user.

4 - Create the /usr/share/kibana/data directory:

```
mkdir /usr/share/kibana/data
chown -R kibana:kibana /usr/share/kibana
```

5 - Install the Wazuh Kibana plugin. The installation of the plugin must be done from the Kibana home directory as follows:

```
cd /usr/share/kibana

sudo -u kibana /usr/share/kibana/bin/kibana-plugin install
https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.4.1_7.17.9-1.zip
```

6 - Link Kibana's socket to privileged port 443:

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

7 - Enable and start the Kibana service:

```
systemctl daemon-reload

systemctl enable kibana

systemctl start kibana
```

8 - Access the web interface using the password generated during the Elasticsearch installation process:

URL: https://<wazuh_server_ip>

user: elastic

password: <PASSWORD_elastic>

Upon the first access to Kibana, the browser shows a warning message stating that the certificate was not issued by a trusted authority. An exception can be added in the advanced options of the web browser or, for increased security, the ca.crt file previously generated can be imported to the certificate manager of the browser. Alternatively, a certificate from a trusted authority can be configured.

Disabling repositories

This installation guide describes how to install and configure Wazuh and Elastic Stack by first configuring their repositories.

With each new release of Wazuh or Elastic Stack, the development team at Wazuh thoroughly tests the compatibility of each component and performs necessary adjustments before releasing a new Wazuh Kibana plugin.

We recommend disabling the repositories so that the individual packages will not be updated unintentionally, which could potentially lead to having a version of the Elastic Stack for which the Wazuh integration has not been released yet.

```
sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list

sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/elastic-7.x.list

apt-get update
```

Next steps - Agent Installation

Once the Wazuh environment is ready, a Wazuh agent can be installed on every endpoint to be monitored. The Wazuh agent installation guide is available for most operating systems.

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

Network IDS integration - Suricata

Wazuh integrates with a network-based intrusion detection system (NIDS) to enhance threat detection by monitoring network traffic.

In this use case, we demonstrate how to integrate Suricata with Wazuh. Suricata can provide additional insights into your network's security with its network traffic inspection capabilities.

Prerequisites

1- fresh Ubuntu 22.04 installation

2 - A root password is configured on your server

Configuration

Take the following steps to configure Suricata on the Ubuntu endpoint and send the generated logs to the Wazuh server.

1 - Install Suricata on the Ubuntu endpoint. We tested this process with version 6.0.10 and it can take some time:

```
sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

sudo apt-get install suricata -y
```

2 - Download and extract the Emerging Threats Suricata ruleset:

```
cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.10/emerging.rules.tar.gz

sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/

sudo chmod 640 /etc/suricata/rules/*.rules
```

3 - Modify Suricata settings in the /etc/suricata/suricata.yaml file and set the following variables:

```
HOME_NET: "<UBUNTU_IP>"
EXTERNAL_NET: "any"
default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules"
# Global stats configuration
stats:
enabled: no
# Linux high speed capture support
af-packet:
  - interface: enp0s3
```

interface represents the network interface you want to monitor. Replace the value with the interface name of the Ubuntu endpoint. For example, enp0s3.

```
Ifconfig
```

Output

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::9ba2:9de3:57ad:64e5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:14:65:bd  txqueuelen 1000  (Ethernet)
        RX packets 6704315  bytes 1268472541 (1.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4590192  bytes 569730548 (543.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4 - Restart the Suricata service:

```
sudo systemctl restart suricata
```

5 - Add the following configuration to the /var/ossec/etc/ossec.conf file of the Wazuh agent. This allows the Wazuh agent to read the Suricata logs file

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

6 - Restart the Wazuh agent to apply the changes:

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

Attack emulation

Wazuh automatically parses data from /var/log/suricata/eve.json and generates related alerts on the Wazuh dashboard.

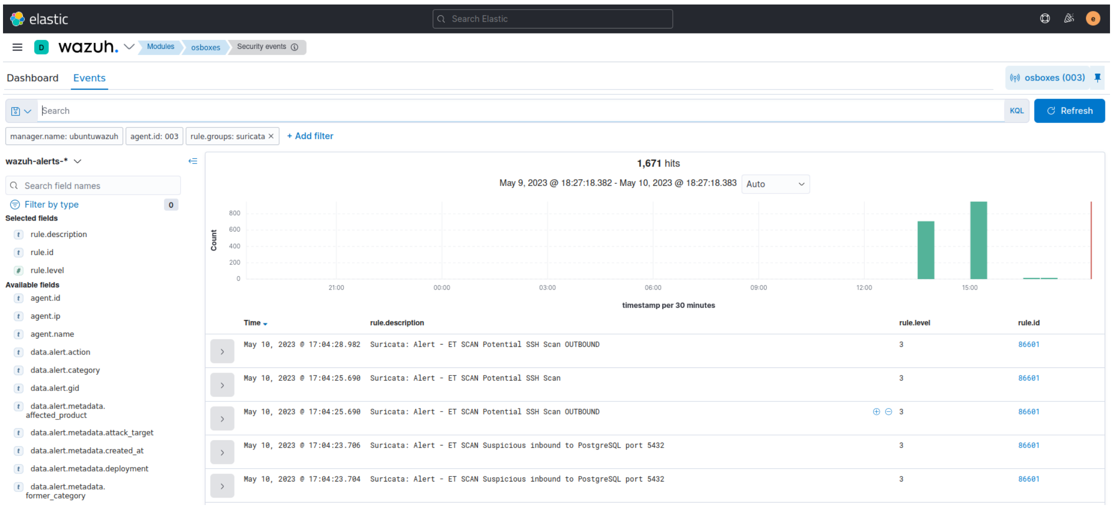
Ping the Ubuntu endpoint IP address from the Wazuh server:

```
ping -c 20 "<UBUNTU_IP>"
```

Visualize the alerts

You can visualize the alert data in the Wazuh dashboard. To do this, go to the Security events module and add the filters in the search bar to query the alerts

rule.groups:suricata



manager.name: ubuntuwazuh · agent.id: 003 · rule.groups: suricata

1,671 hits

May 9, 2023 @ 18:27:18.382 - May 10, 2023 @ 18:27:18.383

Time	rule.description	rule.level	rule.id
May 10, 2023 @ 17:04:28.982	Suricata: Alert - ET SCAN Potential SSH Scan OUTBOUND	3	86601
May 10, 2023 @ 17:04:25.690	Suricata: Alert - ET SCAN Potential SSH Scan	3	86601
May 10, 2023 @ 17:04:25.690	Suricata: Alert - ET SCAN Potential SSH Scan OUTBOUND	3	86601
May 10, 2023 @ 17:04:23.706	Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	3	86601
May 10, 2023 @ 17:04:23.704	Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	3	86601

Apache web server - (Health Care System web portal)

Apache is available within Ubuntu’s default software repositories, making it possible to install it using conventional package management tools.

1 - Installing Apache

```
sudo apt update

sudo apt install apache2

sudo systemctl start apache2
```