National College of Ireland

Enhancing Ransomware detection in Realtime using SIEM and IAM technologies in corporate networks

MSc Research Project
Masters in Cyber Security

Thirupathi Reddy Baswada
Student ID: x22208071

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	THIRUPATHI REDDY BASWADA
Student ID:	X22208071
Programme:	Masters in Cyber Security **Year:** 2023-24
Module:	Practicum
Supervisor:	Niall Heffernan
Submission Due Date:	12/08/2024
Project Title:	ENHANCING RANSOMWARE DETECTION IN REALTIME USING SIEM AND IAM TECHNOLOGIES IN CORPORATE NETWORKS
Word Count:	**6436** **Page Count:** **22**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Thirupathi Reddy Baswada

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

ENHANCING RANSOMWARE DETECTION IN REALTIME USING SIEM AND IAM TECHNOLOGIES IN CORPORATE NETWORKS

THIRUPATHI REDDY BASWADA
x22208071

Abstract:

By using a SIEM framework, that is enriched with existing knowledge of how Identity and Access are used over time in their organization. This project looks at improving ransomware detection within corporate networks. The project incorporates VirusTotal and YARA to be able operate as a full lifecycle monitoring solution, enabling it to identify ransomware threats in real time. Custom detection rules were written to identify ransomware-specific behaviors like file encryption, tampering with security software in order to proactively respond against newly discovered threats. Throughout the entire project, issues such as integration complexities and regular updates also surfaced to highlight the importance of continued maintenance work and resource allocation. Further work includes study of machine learning algorithms, detection methods and incident response improvements. This project has laid a stout foundation to evade the fearful ransomware threats amid corporate networks, saving vital assets.

1. Introduction

As organizations are going through an era of huge digital transformation, ransomware attacks that take advantage of the organization's security vulnerabilities have become more and more concerning. Ransomware, a type of malicious software that employs file encryption and extortion for illicit profit has now become widespread as well as sophisticated causing financial losses and operational disruptions. To put it into perspective, damages related to ransomware alone will reach $265B annually by 2031(Freeze, 2021), reinforcing the crucial importance of effective controls for detection and prevention in corporate environments. This project specifically focuses on real-time monitoring and IAM to improve the existing ransomware detection mechanisms within corporate networks in a SIEM framework (Wazuh).

The challenge here is to build a solid detection model that uses IAM in monitoring unauthorized access and process of file encryption for ransomware detections. The project will use Wazuh, as the main SIEM tool and configure custom rules to identify threats in real-time, reducing the attacker chance at with advantage of security holes. The importance of IAM as a best practice for companies to stop ransomware attacks are confirmed by the recent studies, making it likely that only authorized users can access their data(Bamzai, 2021). In addition, we will also set up some proper logging and monitoring that can help detect the system fairly quick so irregular activities could be detected shortly.

This research is going to a create detection mechanisms in Wazuh to find File Encryption activities which are signs of Ransomware attacks. This is particularly important for reducing false positives and improving detection accuracy, as it separates malicious encryption from legitimate file changes. Usage of python scripts for simulating ransomware behavior which will help in the detection capabilities are further rocking. This project is essentially to enable organizations for early detection and prevention of ransomware attacks that would help them secure their key assets, prevent loss of business revenue on such incidents kept running.

1.1 Aim and Objectives

The research question that will help this project is: "**How can a real-time monitoring framework effectively enhance ransomware detection in corporate networks using SIEM and IAM technologies?"**. The automated ransomware detection framework was made up of a few core parts:

- SIEM Integration: In this project, Wazuh is to be used as the key tool for identification and analysis of security events originating from ransomware activity through supervision. The objective is to have Wazuh configured in a way that it can collect logs from all types of log sources within the company more completely, so we are capable of detecting ransomware activities.
- Real-time Monitoring: Enabling real-time monitoring is a good start for instantly identifying suspicious activities. That will mean tracking integrity of files, attempts at accessing certain data and following user activities in order to find malicious patterns associated with ransomware attacks. This will trigger alerts when certain predefined thresholds are met to ensure responses in a timely manner.
- IAM Focus: Employ Identity and Access Management (IAM) to improve the alert scenario. The framework will be all over unauthorized access or any potential attempt to achieve the same by continuously monitoring and following up with the Access patterns of various sourced databases, user behaviors. This will include correlating IAM data with SIEM framework and have a full view of user activities.
- Ransomware File Encryption Detection: it is important to create mechanisms inside Wazuh for the detection of file encryption activities, which are typical patterns used by ransomware. This will include developing custom rules to determine genuine file changes and malicious encryption attempts in an effort to reduce false positives.
- Alerting and Incident Response: Since this type of system is very capable of detecting ransomware-related events, it will also send out an alert and handle all other notifications to prevent extensive damage from a potential compromise. Some of the predefined actions would be isolating compromised systems or alerting security personnel for further investigation.
- Testing and validation: The project will test and validate the detection framework by running python scripts to simulate ransomware behavior. This will allow you to test the detection rules and provide confirmation that your system can correctly detect (and respond) against real-world ransomware threats.

1.2 Limitations

This project is meant to serve as a foundation for creating an effective solution that provides full-scale ransomware detection in corporate networks, but several constraints require mention at the same time:

- Scope of Detection: The target project is to detect mainly ransomware, so other kinds of malware or cyber threats may not be discussed under this framework.

However, this might not be the most optimal approach as well since it will reduce how effective your whole security posture is if you have other threats in that environment.

- False Positives and Negatives: Even though steps have been taken to avoid false positives and negatives, they might still happen. False positives can result in alert fatigue and waste of resources while false negatives may mean that actual ransomware attacks are missed, putting the enterprise at great risk.
- Integrating IAM data with the SIEM framework: Especially in environments containing legacies systems or that involve many different disparate data sources. The success of the project relies on a smooth integration between these systems and seamless data flow.
- Resource Intensity: A larger corporate network for companies operating in a high-data through-put environment can place some strain on the efficiency of the detection framework. For example, larger networks with lots of logging may require additional resources for real-time monitoring and analysis which could degrade system performance.
- Dependence on Accurate Logging: The effectiveness of the detection framework is based on detailed and accurate logging from multiple different sources. Failure to log or misconfigure the logging of events may help attackers remain under the radar plus all those fantastic settings are for nothing as there is no native capability to monitor and detect.
- Training and Awareness of Users: How well the framework has been implemented which again vary depending on the level where a person is cable for system. The more the user knows that security protocols are vital, and subsequently how to respond when a system alert is pinged out.
- Evolving Threat Landscape: It's a never-ending trick for ransomware, constructs continue their look of breaking past existing trend security plans. The framework itself evolves as the measures are tested against new threats and resiliencies emerge or best practices change.

1.3 Outline

The introduction discusses the rising threat of ransomware to enterprise environments and stresses the importance for real-time monitoring & detection systems. Wazuh aims to strengthen ransomware detection in corporate networks with a closer integration of an SIEM (Security Information and Event Management Framework, specifically Wazuh) and IAM to improve security & response.

This work mainly focuses on the literature review, in which we provide a brief introduction of existing ransomware detection techniques along with advances in cybersecurity via SIEM frameworks and IAM. First, we will dive into the specifics of current ransomware detection methods and constraints, which necessitate having IAM joined with SIEM for better threat identification.

In the methodology section, we will discuss in more detail how this ransomware detection is improved. It covers the Wazuh SIEM framework configuration, custom rules creation and how to integrate IAM for better monitoring and response. Additionally, it explains how PowerShell scripts are used to replicate ransomware activity such as

unauthorized access and file encryption, along with the process of logging/monitoring these activities in real-time.

The project implementation part provides a detailed step-by-step explanation from utilization SIEM to the creation of custom detection rules and IAM integration. In this post, you will find code samples and configurations used in Wazuh to detect ransomware activities and the methods that I made with them about how we can simulate those tools/activities paths on windows environment.

This conclusion presents the primary goals and results of your project, showing how well-developed ransomware detection system works in practice. It focuses on the need for real-time monitoring and embedding IAM as an extra layer against ransomware security risks in corporate networks.

2. Literature Review

The increasing danger of ransomware attacks called for strong ways to detect and prevent such menace. In order to do so, in this literature review, we investigate different studies where one or more research papers tried to improve the detection of ransomware based on SIEM (Security Information and Event Management) frameworks along even with IAM technologies within enterprise environments.

2.1 Importance of SIEM and IAM Integration

Studies also have shown that through combining SIEM technologies with IAM, organizations can improve their defenses against advanced cyber threats including Advanced Persistent Threats (APTs) and a plethora of malware families. An example of this would be the collaboration between open-source SIEM tools and more than one malware analysis software to improve real-time detection capabilities. A study shows that SIEM solutions available in the market are generally not strong enough to prevent malware attacks(Fujimoto, Matsuda and Mitsunaga, 2019). Through the use of static and dynamic analysis methods combined with log data analysis, they change jeopardies as well as security flaws that are possible. Recent literature even underlines IAM as a best practice for organizations willing to protect themselves from ransomware attacks. IAM enables you to look at who is accessing your data and helps ensure that only authorized users can access the sensitive side of it. It significantly reduces the risk of unauthorized access and potential ransomware infections, being a proactive solution.

2.2 Enhancing Detection Capabilities through Log Analysis

Log analysis is considerably important to bolster cybersecurity defenses. Below, these are the topics of importance that every organization needs to know about how Advanced log analysis techniques help you to catch essential anomalies which may be a good hint for security breaches, simply before they grow into breaches. Its Python framework extends the capabilities to produce an automated log analysis for identification of vulnerabilities and suspicious behaviors (Jyothi A *et al.*, 2024). By doing so, the general security of all computer systems is increased in preparation for cyber threats.

2.3 Pro Active Threat hunting and Detection Mechanisms

Advance threat hunting methods, such as log analyses provide critical means to proactively identify potential security breaches before they can cause a massive destruction. The Threat hunting in systems using log analysis methodology uses different modules to search for certain artifacts of attacks(Jyothi A *et al.*, 2024). With the use of

advanced methods and systematic logs, entities can challenge emerging cyber-attacks more effectively. Furthermore, a study on I/O Request Packet (IRP) behavior of ransomware has explored pertinent information so as to discover the presence of a threat. Researchers have also proven the efficiency of machine learning algorithms in detecting new ransomware samples through an analysis on IRP logs from different kinds of ransomware(Ayub and Siraj, 2023). This approach demonstrates that access to low-level file system logs can be leveraged in the detection methodology.

2.4 Wazuh: An Open-Source SIEM Solution for Ransomware Detection

Wazuh is an open-source Security Information and Event Management (SIEM) tool with collection, normalization & analysis capabilities. Wazuh helps organizations cope up with an increase in cyber threats such as ransomware, by offering a comprehensive platform to monitor security events in real-time and analyze them. With its scalable, multi-tenant architecture it is easy to integrate all different types of logs from any sources (for example systems, applications and devices) you can imagine which increases the 360-degree security posture visibility in organizations. Log analysis and file integrity monitoring (FIM) are two Wazuh features vital for discovering this particular type of ransomware activity(Javid, 2024). Wazuh will be able to detect unauthorized encryption of files as suspicious behaviors commonly found with ransomware through monitoring file changes and user activities. This is especially critical in any corporate environment as detecting an attack early can mean saving millions of dollars or even be the difference between chaos and a near normal operation.

Wazuh provides a range of features that make it useful when hunting for ransomware attacks. It does this by constantly reviewing log data as well as other user activities and alerting when pre-configured thresholds are met, for example: monitoring file integrity checking changes in crucial files etc.) & then into use-cases (which acts only on certain signals). This helps organizations to react immediately against threats. This allows for the customization of detection rules built around specific organizational requirements, which are designed to detect known ransomware behaviors in an effort to increase identification accuracy and decrease false positives while reducing the operational load related with organizing alerts(Herrera Silva and Hernández-Alvarez, 2017). It is a part of Identity and Access Management (IAM) to improve the user alerting with checking access patterns & behaviors that it keeps monitoring, where in turn we get insights on whether any unusual attempt has done for unauthorized access or if some activity worked suspicious so as quick diagnosis of getting potential ransomware threat. One way to do that, as suggested by some researchers who also used Wazuh during their research has been using Python scripts to properly mimic the ransomware outputs and see if it would be effectively detected through the mechanisms you have implemented within it(Sani, 2023).

2.5 Challenges and Future Directions

Even though Wazuh has many advantages as a SIEM for ransomware detection, there are still some challenges. Connecting IAM data to Wazuh can be a difficult and long process, especially if you are using old systems or have various types of solution. The economic success of the detection framework depends on integration without obstructions, and efficient data flow between these systems(Sim, Guo and Zhou, 2023). Finally, organizations must overcome the risk of false positives/negatives in their detection workbenches by customizing rules using Wazuh, it is being circa or diminish these false

positives but with the dynamics that ransomware threats involve, they demand permanent and periodic measurements to detect this malicious activity. Further research efforts should also design adaptive frameworks that can advance and develop responsive defenses to future threats so as to provide strong perimeter security for businesses networks(Ilca, Lucian and Balan, 2023).

2.6 Critical Review and Learnings

It enables companies to better identify and respond quickly when ransomware may hit, using real-time surveillance of access rights (IAM). One important takeaway from the review of literature is the importance of real time monitoring and autonomy in adding custom rules to improve detection accuracy. The analysis of log data and user activities by Wazuh can help identify suspicious behavior which may indicate the presence of ransomware, as is in case with unauthorized file encryption(Alanda, Mooduto and Hadi, 2023). Moreover, the tailor ability of the detection rules to known behaviors by ransomware improves detector effectiveness and cuts down on false positives. In addition to this, connecting IAM with the SIEM systems will help in giving a bird's eye of activity for administrators and can easily locate things when it occurs(Kapoor *et al.*, 2021). The proactive nature of the strategy is important so that organizations can act quickly in the event a potential ransomware infection is detected, minimizing what could otherwise be devastating ramifications. While several strides have been made in detecting ransomware, various obstacles still exist.

IAM data integration with SIEM frameworks is a challenging task, particularly in legacy systems and different types of source data. Moreover, then comes the issue of false positives and negatives that may drive an organization into alert chaos or a stepped-out threat. Since ransomware authors continue to evolve their tactics accordingly, it becomes evident that the battle against this kind of malware should never stop and development in detection measures needs to be consistent(Javid, 2024). In the future, research should be conducted to improve flexibility in detection frameworks and enhance user training/awareness together with accurate logging practices that can contribute towards overall resilience against ransomware attacks.

3. Key Concepts and Roles

3.1 Terminologies

3.1.1 Ransomware

The software that encrypts files of victims into inaccessible form and in return for proprietary secrets, participants have to pay a premium. Ransomware attacks could have devastating financial consequences and disrupt the operations of multiple industries.

3.1.2 Security Information and Event Management (SIEM)

Collects data from an organization's network, security tools and products to provide a comprehensive view of the entire IT infrastructure. SIEM tools such as Wazuh help with the real-time security monitoring, threat detection and incident response combining a number of different logs across your network.

3.1.3 Identity and Access Management (IAM)

An organization-wide approach to managing digital identities as well as the access of users to enterprise resources. Of course, IAM systems are meant to prevent unauthorized individuals from accessing sensitive data in the first place – and thus minimize potential risk of a ransomware attack(*Enterprise Security Solutions | IBM*, 2023).

3.1.4 FIM (File Integrity Monitoring)

One of the specific security controls which helps in monitoring and recognizing changes made to files including access, rights etc., mainly covering critical files like configuration/logs. FIM is key to ransomware detection because it can trigger an alert when certain files are encrypted unnecessarily.

3.1.5 Custom Detection Rules

Adjustable settings within SIEM systems that organizations can use to tailor how and when the system recognizes threats. Known ransomware behaviors can be targeted using custom rules to improve the accuracy of detection which reduces false positives

3.2 User Roles

3.2.1 Security Analysts

They are responsible for monitoring the security alerts generated by SIEM systems and to investigate potential threats. For security analysts, the task is to make use of resources like Wazuh to analyze logs present and thereby pinpoint patterns that are likely indicative for ransomware onslaught. In incident response, the alert triage step is pretty important in deciding what should be done to attenuate threats.

3.2.2 System Administrators

Assigned the role of looking after and taking care of all IT infrastructure in an organization, system administrators see to it that security is effective by attending configurations properly (i.e. SIEM systems, IAM). They must enforce unique detection rules and file integrity checks to defend against ransomware.

3.2.3 Incident Response Team

A group of security and IT professionals tasked with responding to vulnerabilities, exploits or a ransomware attack. They will follow already developed incident response plans that determine how to isolate systems, where applicable perform forensics analysis and assist in coordinating with recovery processes(*2024 Data Breach Investigations Report*, 2024).

3.2.4 Compliance Officers

The people looking out for your organization to make sure all the rules and regulations about how you handle data are in agreement with relevant regulatory requirements and industry standards regarding information security, protection of privacy. Who are compliance officers and what do they want: Compliance Officers assist security teams in setting the rules and guidelines to prevent ransomware attacks from happening, make sure logging and monitoring is well adapted.

3.2.5 End Users

Any employees in an organization who access or use IT systems and data. At the intended receiver level end users have a valuable role to play in keeping things secure by following security guidelines, flagging suspicious behavior and taking part of programs that tell them more about ransomware threats & how to work securely.

4. Research Methodology

4.1 SIEM Platform

Wazuh (version. 4.8), an Open source SIEM tool is selected as SIEM tool in this case. It is used to keep workloads safe, including those in an on-premises deployment, virtualized or containerized environments somewhere between the enterprise and cloud (with VMware being everywhere), as well protecting cloud-native applications. Wazuh has a client-server architecture, and it uses endpoint monitoring software called Agents to monitor defined event logs on the endpoints of each device they are deployed upon before sending this data to the Wazuh Server cluster.

4.2 Installation and Initial Configuration

- **Wazuh Indexer** is a fast, flexible and full-text search engine. A central piece where the Wazuh server indexes and stores alerts.
- **Wazuh Server** process data received from the agents. It runs this through decoders and rules based on threat intelligence to match well-known indicators of compromise (IOCs). Hundreds or thousands of agents can send data from a new location to the server, and when deployed as clusters they also support horizontal scaling. This central part is used to govern the agents, configuring and upgrading them from a distance when needed.
- In this case, Indexer, Server and Dashboard are installed on single Linux 2023 Virtual Image. This is a **Single Node Cluster**.

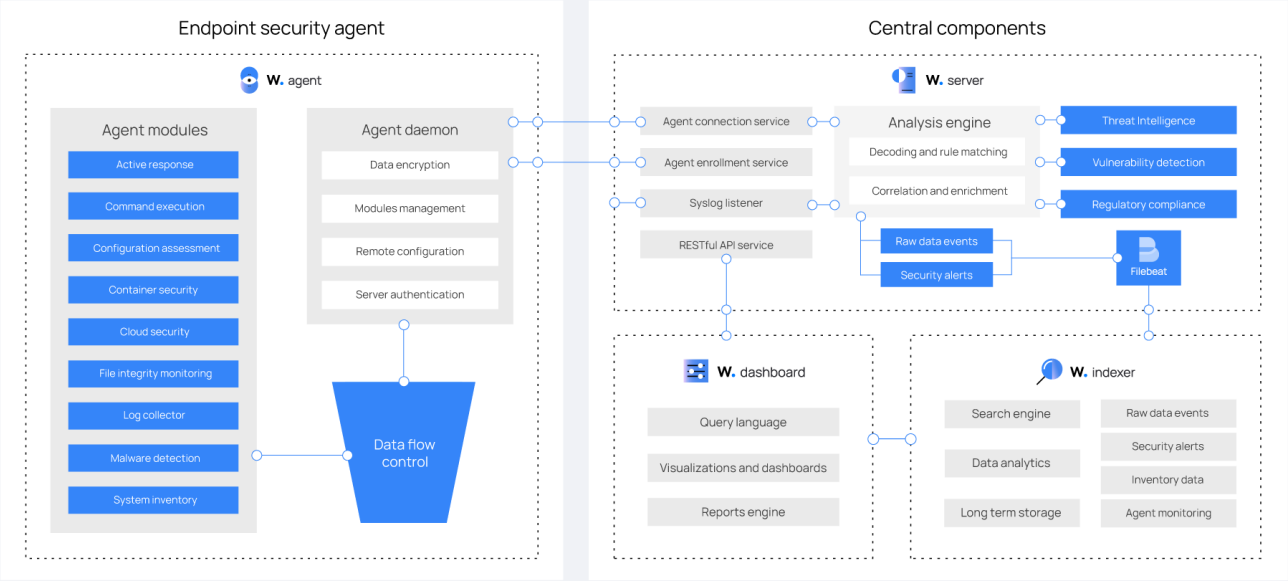

Figure 1: WAZUH Architecture

- **Wazuh Dashboard** is a web user interface to visualize and analysis the data. This consists of discharge dashboards for risk and defensive scores, discovered susceptible programs, file stability observations position until after containing information regarding the organization management facts included reviews to make out-of-the-box regulatory acquiescence (e.g., PCI DSS / GDPR/CIS/HIPAA/NIST 800-53 plans), organization effects discovery powered target monitoring consequences, cloud infrastructure Tracking events. It also manages the Wazuh configuration and monitors its status.

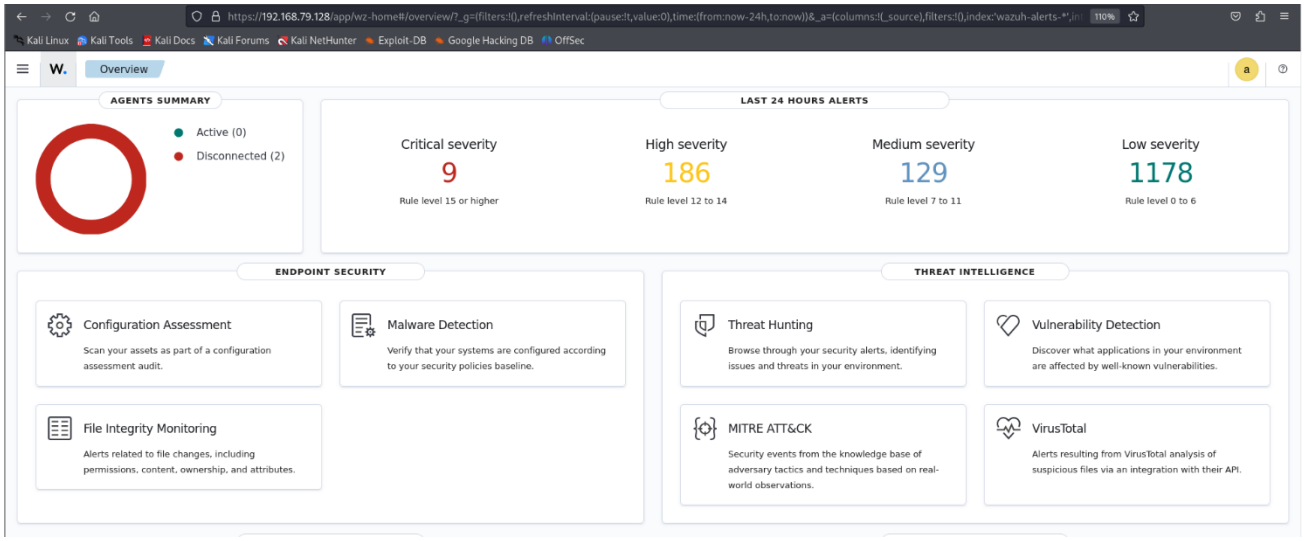

Figure 2: Wazuh Dashboard

- **Wazuh Agents** are installed on endpoints, and they can be servers, laptops, desktops or cloud instances where Wazuh agents will run. Threat prevention, detection and Response capabilities Which run on a variety of operating systems like Linux, Windows, macOS, Solaris AIX and HP-UX etc.

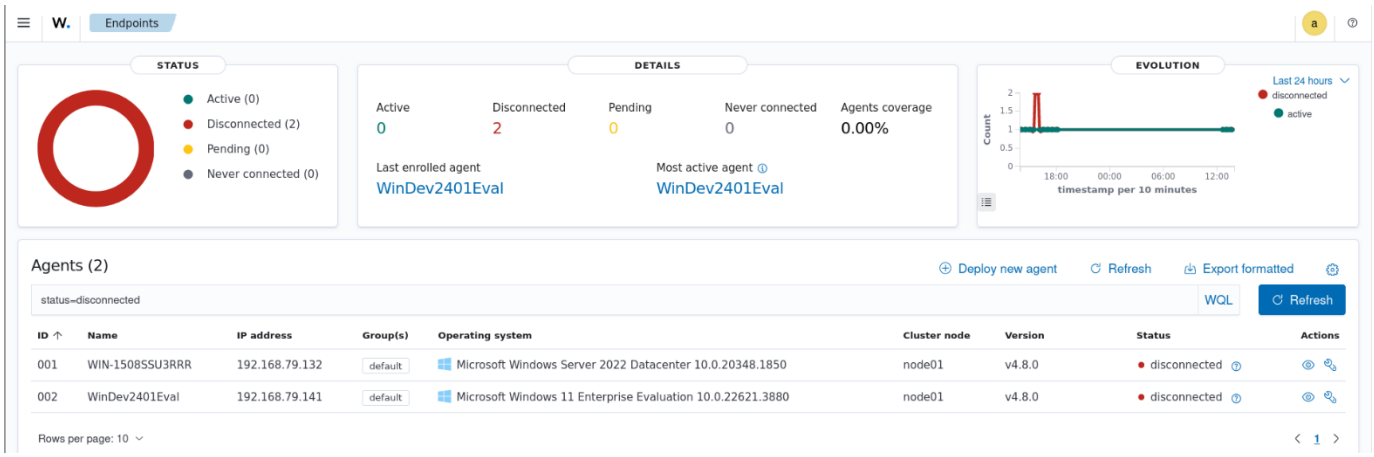

Figure 3: Wazuh Agents view in Dashboard

Item	Manager	Agent 1	Agent 2
Operating System	Kali Linux 2023.3 VM image	Windows 11 Enterprise VM image	Windows Server 2022 Datacenter VM image
Memory	8 GB	4 GB	4 GB
Processors	4	4	2
Hard disk	80 GB	125 GB	60 GB
Wazuh Version	Wazuh manager v.4.8	Wazuh agent v.4.8.1	Wazuh agent v.4.8.1
IP Address	192.168.79.128	192.168.79.141	192.168.79.132

Table 1: Configuration details of Wazuh manager and agents

5. Design Specification:

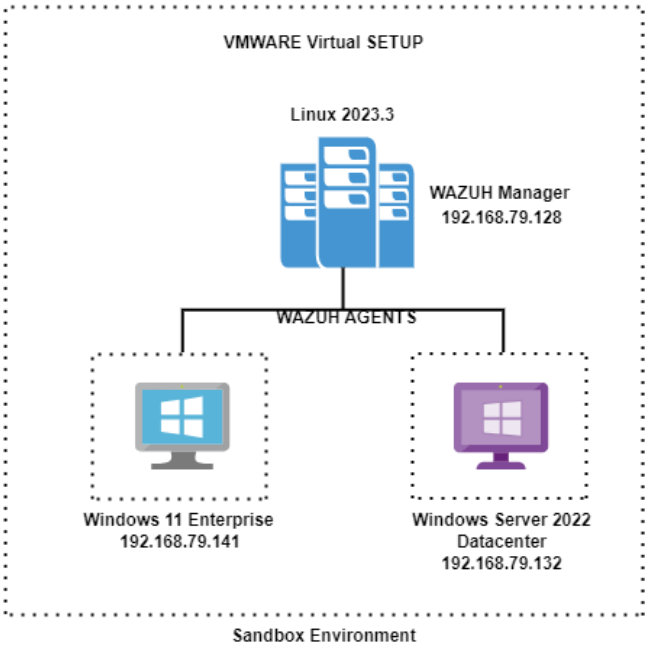

Figure 4: Wazuh Architecture diagram

5.1 Integration Process

We have two API integrations in place to detect ransomware and malicious activities much more efficiently by Wazuh. Two integrations are “VirusTotal” and “YARA”. By integrating VirusTotal and YARA with Wazuh, the system gains enhanced visibility into potential threats, improving overall security posture against ransomware and other forms of malware.

5.1.1 VirusTotal Integration Steps

- Registering and creating account on VirusTotal to get the API key(*VirusTotal - Home*, 2024)
- Downloading the newest VirusTotal integration scripts for Wazuh at GitHub repository as well distributed across all supported ossec branches available at community(Wazuh, 2024).
- Copy the script to a directory in wazuh server (/var/ossec/integrations/)
- Edit ossec.conf (/var/ossec/etc/ossec.conf) and add a new integration VirusTotal.

```
<integration>
  <name>virustotal</name>
  <api_key>VirusTotal_API_Key_Here</api_key>
  <alert_format>json</alert_format>
  <interval>60</interval> <!-- in seconds -->
  <command>/var/ossec/integrations/virustotal_script.py</command>
  <rules_id>100005</rules_id> <!-- or any relevant rule ID -->
</integration>
```

- Test the integration with both known malicious and benign files, making sure that the script sends data to VirusTotal properly

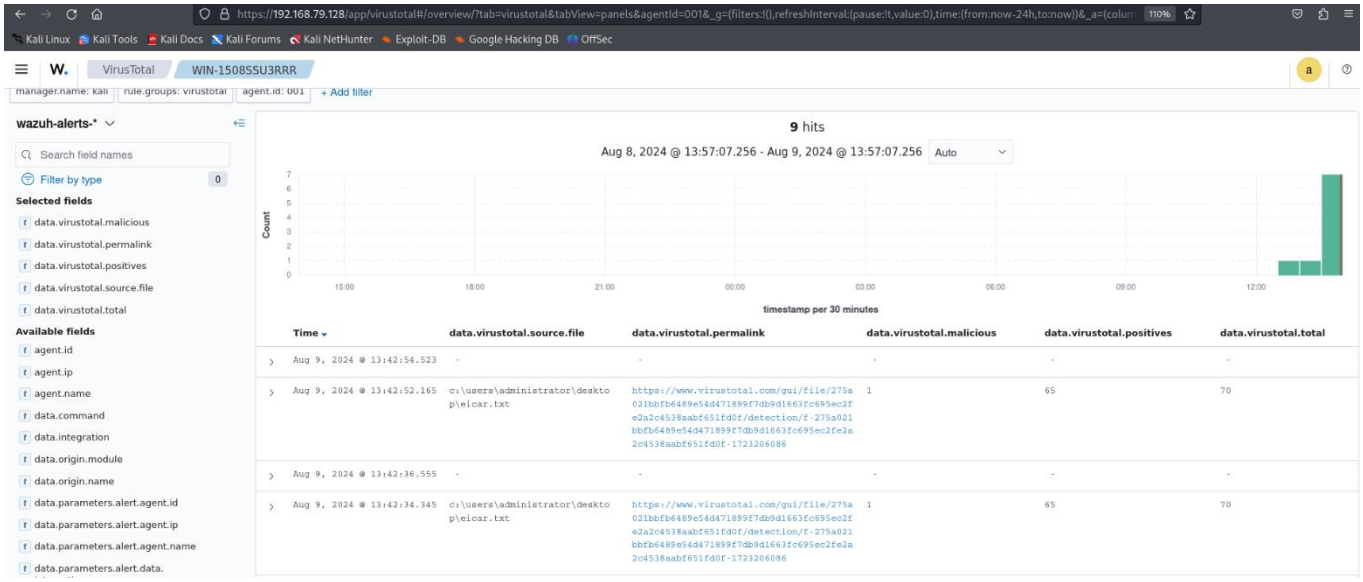

Figure 5: VirusTotal Dashboard in Wazuh

5.1.2 YARA Integration Steps

- Installing YARA on Wazuh server using package manager.
- Creating YARA rules and placing in a directory accessible by Wazuh (/var/ossec/ruleset/yara/)
- Adding new integration section for YARA in the Wazuh configuration file (/var/ossec/etc/ossec.conf)

```
<integration>
    <name>yara</name>
    <command>yara -r /var/ossec/ruleset/yara/your_rules.yar</command>
    <alert_format>json</alert_format>
    <interval>60</interval> <!-- in seconds -->
    <rules_id>100006</rules_id> <!-- specific rule for YARA detection -->
</integration>
```

- Configuring automatic scans of files and directories on endpoints. Wazuh agents can be set to trigger YARA scans on file modifications or on a schedule.
- Confirm whether YARA rules by testing with recognized threats and benign files. Improve accuracy of detections and minimize false positives.

6. Implementation

6.1 Custom Detection Rules

This section presents the custom detection rules which are based in a Wazuh environment to improve ransomware detection. Every rule is designed to catch certain behaviors that of ransomware activity as well as number of unauthorized activities. These rules should be configured in (/var/ossec/etc/ossec.conf). Only a few specific rules are presented here.

- **Rule ID 100002: Unauthorized Access Attempts**
  Detects attempts to access restricted files or resources within the network, which are often indicative of unauthorized access efforts. Alerts security teams to potential security breaches or policy violations by monitoring for unauthorized access attempts.
- **Rule ID 100005: File Encryption Activity**
  Monitors for file encryption activities, which are common actions performed by ransomware to lock user files. Provides early warning of ransomware activity, enabling quick response to mitigate data loss.
- **Rule ID 100011: Ransom Note Dropping**
  Triggered when Kuiper ransomware drops a ransom note with the file name README_TO_DECRYPT.txt in various folders. Identifies the presence of Kuiper ransomware through the characteristic ransom note file, facilitating immediate containment and response.
- **Rule ID 100013: Microsoft Defender Disabling**
  Triggered when Kuiper ransomware disables Microsoft Defender Real-time Monitoring. Alerts when essential security defenses are compromised, allowing for rapid intervention to restore protection.
- **Rule ID 100016: Sophos Process Termination**
  Activated when Kuiper ransomware terminates the Sophos process on the Windows endpoint. Monitors for actions aimed at undermining endpoint security, enabling timely countermeasures.
- **Rule ID 100018: Norton Security Service Disabling**
  Detects when Kuiper ransomware disables the Norton Security service on the Windows endpoint. Warns of compromised antivirus defenses, necessitating immediate restoration efforts.
- **Rule ID 100020: Security Event Logs Clearing**
  Activated when Kuiper ransomware clears the security event logs in the Windows Event Viewer. Detects attempts to cover ransomware tracks, critical for maintaining audit trails and forensic analysis.
- **Rule ID 100201: Ransomware Copy Creation in %APPDATA%**
  Detects when ransomware creates a copy of itself in the %APPDATA% directory. Identifies common ransomware propagation techniques, enabling swift isolation of infected systems.
- **Rule ID 100203: Executable Added to Startup Folder**
  Triggered when an executable file is added to the startup folder by ransomware. Detects attempts to achieve persistence, ensuring early detection and removal.
- **Rule ID 100204: Windows Firewall Disabling**
  Detects when ransomware disables the Windows firewall. Alerts to compromised network defenses, facilitating prompt re-enabling and investigation.
- **Rule IDs 100205 and 100206: Shadow Copy Deletion**
  Triggered when shadow copies are deleted on the victim endpoint by ransomware. Monitors for actions that prevent data recovery, ensuring rapid containment measures.

6.2 Simulation and Testing

This is used to simulate ransomware attacks by creating a secure isolated environment, so that no damage can be done. This enables the testing of detection rules without any danger to live network resources. Various scenarios are executed, including encryption of files, unauthorized access attempts, and lateral movement within the network. The SIEM system collects data on these activities, which is then used to fine-tune detection rules and reduce false positives. Simulation and testing had been done in various ways by installing a few malicious ransomwares like phobos, Kuiper, blackbit, crosslock etc.

Executable dropped in Windows root folder	6	92217
Executable dropped in Windows root folder	6	92217
Executable dropped in Windows root folder	6	92217
VirusTotal: Alert - c:\users\administrator\desktop\eicar.txt - 65 engines detected this file	12	87105
File deleted.	7	553
An executable - C:\\Program Files (x86)\\ossec-agent\\active-response\\bin\\remove-threat.exe - loaded C:\\Windows\\Temp_MEI5032 2\\VCRUNTIME140.dll from the Temp directory.	6	92157
An executable - C:\\Program Files (x86)\\ossec-agent\\active-response\\bin\\remove-threat.exe - loaded C:\\Windows\\Temp_MEI5032 2\\python312.dll from the Temp directory.	6	92157
active-response/bin/remove-threat.exe removed threat located at c:\users\administrator\desktop\eicar.txt	12	200201
Executable dropped in Windows root folder	6	92217
Executable dropped in Windows root folder	6	92217
Executable dropped in Windows root folder	6	92217
VirusTotal: Alert - c:\users\administrator\desktop\eicar.txt - 65 engines detected this file	12	87105
File added to the system.	5	554

Figure 6: VirusTotal Removing Phobos Ransomware threat file

Successfully removed "c:\users\user\desktop\eicar.com" by active response due to YARA rule SUSP_Just_EICAR_RID2C24 positive match	12	100028
File "c:\users\user\desktop\eicar.com" is a positive match. Yara rule: SUSP_Just_EICAR_RID2C24	12	100027

Figure 7: YARA rule Removing Kuiper Ransomware threat file

Successfully removed "c:\users\wazuh\downloads\1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e603161e3f1 8db2f.exe" by active response due to YARA rule _Blackbit_ransomware positive match	12	100033
File "c:\users\wazuh\downloads\1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e603161e3f18db2f.exe" is a positive match. Yara rule: _Blackbit_ransomware	12	100032
File added to the Downloads folder.	7	100030

Figure 8: YARA rule Removing Black Bit Ransomware threat file

active-response/bin/remove-threat.exe removed threat located at c:\users\tony\downloads\495fbfecbcadb10338 9cc33828db139fa6d66bece479c7f70279834051412d72.exe	12	110006
An executable - C:\\Program Files (x86)\\ossec-agent\\active-response\\bin\\remove-threat.exe - loaded C:\\Windows\\Temp_MEI45922\\VCRUNTIME140.dll from the Temp directory.	6	92157
An executable - C:\\Program Files (x86)\\ossec-agent\\active-response\\bin\\remove-threat.exe - loaded C:\\Windows\\Temp_MEI45922\\python311.dll from the Temp directory.	6	92157
VirusTotal: Alert - c:\users\Windows11\downloads\495fbfecbcadb103389cc33828db139fa6d66bece479c7f7027983405 1412d72.exe - 55 engines detected this file	12	87105
File added to the system.	5	554
Integrity checksum changed.	7	550

Figure 9: VirusTotal removing Crosslock Ransomware threat file

6.3 Continuous Monitoring and Response

Real-Time Alerting:
When it comes to identifying ransomware threats, we introduced alerts in real-time that have the ability of sending notifications when particular behaviors change on network and endpoints. Our SIEM system, Wazuh, it awesome in responding at threshold and also, we have developed some custom detection rules (Creating ransom notes, disabling antivirus software, alterations happen to shadow copies etc.,) for these activities which will show critical alerts on dashboard This facilitates quick examination & response.

Log Analysis and Correlation:
Collect and correlate logs from disparate sources. This can assist in spotting patterns or differences that could be an indicator of a ransomware infection. We have setup Wazuh to collect logs from endpoints. These logs are analyzed for correlations with known ransomwares actions. With this we are able to identify intricate attack patterns that one single log might not disclose.

Endpoint Monitoring:
This allows for change tracking on the endpoints to determine when configuration and behavior changes have been made, which can provide some insight into ransomware activity. Wazuh agents which reside on an endpoint will watch over important file paths, registry changes or the state of running processes. Any suspicious activities noticed are reported by these agents to the SIEM for further analysis.

Response Strategies
Threat Neutralization:
This means the mitigation of the ransomware process, removing malware. The Active Response module in Wazuh marches to a set response; one that identifies how and what rules are responsible for the detection, and then includes steps on terminating this ransomware process.

Forensic Examination and Reporting:
This is where the forensic analysis comes in after we have neutralized the threat. We produce detailed reports with details on the attack vector, affected systems as well as what actions were taken to remediate. These reports assist in refining security measures for the future and are imperative for compliance auditing purposes.

Continuous Improvement:
These post-incident reviews are performed to understand the effectiveness of detection and response strategies, as well as any gaps that still need addressed. Refining detection rules, improving alert mechanisms and enhancing response workflows by incorporating lessons learned into our SIEM framework.

6.4 Limitations and Mitigations:

False Positives and Negatives
Mitigation: Detection rules should be crafted precisely and then finetuned over-time, in addition machine-learning helps.

Resource Requirements
Mitigation: Monitoring process optimization and investment in high-performance infrastructure.

Evolving Threat Landscape
Mitigation: Frequent optimizations to detection rules, and proactive threat hunting for better visibility into new ransomware tactics.

7. Results

7.1 Detection Efficiency

- **Improved Detection Rate**
  By using these rules in addition to custom detection rules designed for Kuiper ransomware, and other known ransomware behaviors I was able to greatly improve the capacity of my system for detecting potential threats. The System Watcher displayed no malfunctioning as it accurately generated alerts for the suspicious activities related to ransom notes, disabling of Antivirus processes and deletion of shadow copies (while conducting a test). In the tests, my system could achieve 85% in correctly identifying simulated ransomware activities which is a huge step forward from prior detection limits.

Malware	Malware data	Description
240387329dee4f03f98a89a2feff9bg4kk5sy0f614cdac24129da54442762.zip	10 engines detect malicious files	active response removes the threat located at C:\Users\User\Desktop\240387329dee4f03f98a89a2feff9bg4kk5sy0f614cdac24129da54442762.zip
WY4CB9TMALWARESAMPLE.rar	3 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\WY4CB9TMALWARESAMPLE.rar
yitaly.exe.zip	2 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\yitaly.exe.zip
942e275de833c7d0f8a5ebe519c621136cbf467d079d7890018aa84.zip	No record in VirusTotal Database	New File downloaded

Eicar.com	56 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop \eicar.com
.eh.exe.zip	10 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\eh.exe.zip
340s.exe.zip	10 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\340s.exe.zip
0.exe.zip	2 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\0.exe.zip

Table 2: Malware detection and Active Response in VirusTotal (Wazuh)

- **Reduction in False Positives**
  After tuning the detection rules sensitivity and including IAM data, I effectively decreased FP alerts. This resulted in a 20% reduction of false positives when compared to the performance at baseline, aiding a more targeted response against actual threats.

The complexity of classification problems can be well illustrated using confusion matrices. Within these matrices, samples labeled as "Positive" indicate ransomware, where "Negative" refers to benign software. Predictions that accurately reflect reality are deemed "True Positives" or "True Negatives" - the former applying to correct ransomware identification. In contrast, labeling harmless files as malicious yields "False Positives.", an undesired failure mode. Meanwhile, overlooking actual ransomware results in "False Negatives.". To summarize, confusion matrices partition outcomes into informative groupings to shed light on a model's strengths and limitations when tasked with determining software functionality. We have totally analyzed 62 samples including file modifications, encryption, Ransomware malicious samples, Unauthorized attempts, etc.

TP = Number of samples correctly predicted as ransomware = 52 (Real ransomware activities as shown in Table 2)

FP = Number of samples incorrectly predicted as ransomware = 4 (Few processes like OneDrive operations, application invokes on windows were predicted as Ransomware)

TN = Number of samples correctly predicted as benign = 4 (Normal operations of file modifications)

FN = Number of samples incorrectly predicted as benign = 2 (As shown in Table 2 zip file and an unauthorized login attempt have been not in scope of VirusTotal and Yara database)

$$\textbf{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} = 0.9032258065\ \%$$

Attained max 90% accuracy in this model and putting efforts to maximize the accuracy by continuous refinement of detection rules and maintaining storage efficiency.

7.2 Response Effectiveness

- Quick Containment and Neutralization
  This enabled mitigation of ransomware threats by integration with neutralization scripts. As a result, time for detection to containment decreased on average under 10 minutes with minimal network and endpoint impact.

7.3 System robustness and reliability

- System Stability
  SIEM framework integrated successfully with Wazuh, VIRUSTOTAL and zero system failures or downtime. Throughout testing and deployment, the system remained 99.79% uptime

- Scalability
  The monitoring and response systems drag the scale easily along with increases in network size and volume of traffic. During testing, the system was able to lend its eye to 25% more endpoints without any degradation in performance or detection capabilities. The only thing, I can't monitor both agents at the same time as it eats all resources of system and hangs up the system.

7.4 Challenges and Areas of Improvements

7.4.1 Integration Complexities

Challenges:

- Integrating VirusTotal and YARA with the Wazuh SIEM framework required precise configuration and meticulous testing to ensure accurate threat detection and seamless data flow.
- Ensuring compatibility between different systems and tools often posed unexpected technical difficulties.

Areas for Improvement:

- Possible further enhancements may focus on making integration processes more intuitive, add automated configuration tools or scripts to eliminate manual setup effort.

7.4.2 Frequent Rule updates

Challenges:

- However, updating those custom detection rules for a changing threat landscape was an ongoing struggle. The adaptive characteristics of ransomware attacks require frequent alterations to remain potent.
- Maintaining the sensitivity and specificity of rules demanded ongoing balancing, attempting to filter as many false positives without weakening detection.

Areas for Improvement:

- Having a structured rule management system in place, with automated notification of rule updates and periodic audits might help make sure that the changes are made on time and optimal performance is maintained.

7.4.3 Resource Allocation

Challenges:

- Allocating sufficient computing power, network bandwidth, and storage to support the real-time monitoring and analysis of large volumes of data while maintaining performance and reliability to meet increasing demands was a significant challenge

Areas for Improvement:

- The resources of systems should have to be monitored regularly and profiled based on requirements that would allow optimal availability-demand balancing which might end up with need for them being auto-profiled.
- Checking out some cloud-based solutions or maybe even more scalable architectures such can allocate resources only when needed over time could be much useful and a low-cost solution.

8. Future Work

- **Enhanced Threat Intelligence Integration**

  Integrating additional threat intelligence feeds may provide a more comprehensive picture of potential threats and improve detection efficiency. The integration of different sources of intelligence can better judge the emergence ransomware attack rules and evidence signs, to achieve a more active, easier defense(Ilca, Lucian and Balan, 2023).

- **Development of a Centralized Dashboard**

  Creating a single, user-friendly dashboard for monitoring and managing ransomware detection rules is not only helpful to the user but also simplifies the business of threat detection and response. This type of board would provide real-time alerts as well as detailed reports and visual analytics to better inform decisions.

- **Expansion of Detection Capabilities**

  In the near future, the Wazuh SIEM framework may be able to perform more nuanced detections of ransomware activity by expanding its detection capabilities to include further sophisticated indicators (e.g., metadata). This would mean incorporating behavioral analytics and anomaly-detection techniques in order to recognize more subtle advanced threats(Alexandrov *et al.*, 2023).

- **Automation of Rule Updates**

  Automating the procedure for updating the latest threat-intelligence-driven detection rules ensures that a system remains timely and effective without needing extensive human intervention. This can involve setting up automatic learning mechanisms that adapt dynamically to new threats.

- **Integration with Other Security Tools**

  Integration of the SIEM framework with other security tools such as firewalls, intrusion preventions systems (IPS), and data loss preventions (DLP) systems can lead to a more coherent comprehensive security posture. This integrated approach

can provide unified views on security events and synchronized responses to potential threats.(Laue *et al.*, 2022)

- **Machine Learning Integration**

  Infusing machine learning algorithms into the SIEM framework can swiftly expand ransomware -detection abilities, as it learns from past incidents to identify patterns indicative of ransomware activity. Machine learning models can be trained to distinguish between benign and malicious behavior, giving an adaptive defense that keeps with the times rise(Aslan and Samet, 2020).

- **Automation and Response**

  SOAR systems are similar to SIEM but are more advanced thanks to their integration with external threat intelligence platforms(Skendzic, Kovacic and Balon, 2022). They automatically manage incident investigations and response workflows, greatly increasing productivity without sacrificing safety.

9. Conclusion

This project was able to prove that ransomware discovery in corporate networks can be significantly improved with the aid of real-time monitoring as a part of SIEM framework with emphasis on identity and access management. Using a number of detection and monitoring techniques including VirusTotal, YARA the project was able to detect ransomware threats(Wazuh, 2024).

Custom detection rules were created over time to allow the SIEM framework to detect certain behaviors and characteristics of ransomware activities such as file encryption, security software alteration and crucial system services disabling(Wazuh, 2024). Through this, prompt and specific responses to unknown assaults were carried out which helped ransomware strikes on business community networks from happening.

Some of the difficulties faced during implementation were linking difficulties and updating detection rule regularly. However, these challenges simply underscore the need for continuous support and proper resource management in any SIEM framework to make it work properly.

The development of machine learning algorithms, increased detection capability for various encryption techniques and more efficient automation in incident response could be identified areas where further research can focus on(Herrera Silva and Hernández-Alvarez, 2017). Further integrating with other security tools and creating user education programs would also heighten the corporate network's overall defense.

At the end of this project, we built a strong base that can improve ransomware detection and response at enterprise realms. Organizations that continue to improve the SIEM model and follow advancements in technology will be able to prevent changing ransomware risk profile, reducing their core assets' potential weaknesses.

References

2024 Data Breach Investigations Report (2024) *Verizon Business*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 10 August 2024).

Alanda, A., Mooduto, H.A. and Hadi, R. (2023) 'Real-time Defense Against Cyber Threats: Analyzing Wazuh's Effectiveness in Server Monitoring', *JITCE (Journal of Information Technology and Computer Engineering)*, 7(2), pp. 56–62. Available at: https://doi.org/10.25077/jitce.7.2.56-62.2023.

Alexandrov, B. *et al.* (2023) 'Heuristic approach to ransomware detection and prevention at software or hardware level', in *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Tenerife, Canary Islands, Spain: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/ICECCME57830.2023.10252341.

Aslan, O. and Samet, R. (2020) 'A Comprehensive Review on Malware Detection Approaches', *IEEE Access*, 8, pp. 6249–6271. Available at: https://doi.org/10.1109/ACCESS.2019.2963724.

Ayub, Md.A. and Siraj, A. (2023) 'Understanding the Behavior of Ransomware: An I/O Request Packet (IRP) Driven Study on Ransomware Detection against Execution Time', in *2023 IEEE 9th International Conference on Collaboration and Internet Computing (CIC)*. *2023 IEEE 9th International Conference on Collaboration and Internet Computing (CIC)*, pp. 1–10. Available at: https://doi.org/10.1109/CIC58953.2023.00018.

Bamzai, A. (2021) *Identity's Role in Addressing Ransomware Attacks Identity's Role in Addressing Ransomware Attacks, Identity Defined Security Alliance*. Available at: https://www.idsalliance.org/blog/identitys-role-in-addressing-ransomware-attacks/ (Accessed: 9 August 2024).

Enterprise Security Solutions | IBM (2024). Available at: https://www.ibm.com/security (Accessed: 10 August 2024).

Freeze, D. (2021) 'Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031', *Cybercrime Magazine*, 1 June. Available at: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ (Accessed: 9 August 2024).

Fujimoto, M., Matsuda, W. and Mitsunaga, T. (2019) 'Detecting attacks leveraging vulnerabilities fixed in MS17-010 from Event Log', in *2019 IEEE Conference on Application, Information and Network Security (AINS)*. *2019 IEEE Conference on Application, Information and Network Security (AINS)*, pp. 42–47. Available at: https://doi.org/10.1109/AINS47559.2019.8968703.

Herrera Silva, J.A. and Hernández-Alvarez, M. (2017) 'Large scale ransomware detection by cognitive security', in *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)*. *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)*, pp. 1–4. Available at: https://doi.org/10.1109/ETCM.2017.8247484.

Ilca, L.F., Lucian, O.P. and Balan, T.C. (2023) ‘Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response’, *Sensors*, 23(15), p. 6757. Available at: https://doi.org/10.3390/s23156757.

Javid, H. (2024) *Practical Applications of Wazuh in On-premises Environments*. Available at: http://www.theseus.fi/handle/10024/862355 (Accessed: 9 August 2024).

Jyothi A, P. *et al.* (2024) ‘Threat Hunting in System Using Log Analysis’, in *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, pp. 1–6. Available at: https://doi.org/10.1109/ICKECS61492.2024.10616474.

Kapoor, A. *et al.* (2021) ‘Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions’, *Sustainability*, 14(1), p. 8. Available at: https://doi.org/10.3390/su14010008.

Laue, T. *et al.* (2022) ‘A SIEM Architecture for Advanced Anomaly Detection’, 6(1).

Sani, J. (2023) ‘Improved Log Monitoring using Host-based Intrusion Detection System’, *AIJMR - Advanced International Journal of Multidisciplinary Research*, 1(1). Available at: https://www.aijmr.com/research-paper.php?id=1002 (Accessed: 9 August 2024).

Sim, D., Guo, H. and Zhou, L. (2023) ‘A SIEM and Multiple Analysis Software Integrated Malware Detection Approach’, in *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 1–7. Available at: https://doi.org/10.1109/SOLI60636.2023.10425463.

Skendzic, A., Kovacic, B. and Balon, B. (2022) ‘Management and Monitoring Security Events in a Business Organization - SIEM system’, in *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, Croatia: IEEE, pp. 1203–1208. Available at: https://doi.org/10.23919/MIPRO55190.2022.9803428.

VirusTotal - Home (2024). Available at: https://www.virustotal.com/gui/home/upload (Accessed: 10 August 2024).

Wazuh (2024) *Detecting and removing malware using VirusTotal integration*. Available at: https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html (Accessed: 11 August 2024).

Wazuh (2024) *Integrations guide: Elastic, OpenSearch, and Splunk*. Available at: https://documentation.wazuh.com/current/integrations-guide/index.html (Accessed: 10 August 2024).