Optimizing endpoint detection and monitoring in enterprise solution : A cyber threat intelligence approach

by

Apurba Sarker
18301256
Joty Prokash Mondal
18301146
Suzaur Rashid Pran
18301223
AR Rafiu Islam
18301298

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

Department of Computer Science and Engineering
Brac University
September 2024

© 2024. Brac University
All rights reserved.

Declaration

It is hereby declared that

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

Student's Full Name & Signature:

Apurba Sarker ID: 18301256	Joty Prokash Mondal ID:18301146
Suzaur Rashid Pran ID:18301223	AR Rafiu Islam ID:18301298

Approval

The project titled "Optimizing endpoint detection and monitoring in enterprise solution : A cyber threat intelligence approach" submitted by

1. Apurba Sarker, ID:18301256
2. Joty Prokash Mondal, ID:18301146
3. AR Rafiu Islam , ID:18301298
4. Suzaur Rashid Pran, ID: 18301223

Of fall, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October 7, 2024.
Examining Committee:

Supervisor:

Mehnaz Seraj
Senior Lecturer
Department Of CSE
BRAC University

Co-supervisor:

Dr.Jannatun Noor
Assistant Professor
Department Of CSE
Brac University

Abstract

Advanced cyber threat intelligence systems are crucial in a time when enterprise solutions are increasing and are being targeted by more sophisticated cyberattacks. This research aims to study ways to improve endpoint detection and monitoring in an enterprise company by installing a Security Information and Event Management (SIEM) system based on Wazuh with integration into ELK Stack. The report performs an inside-out examination of the integration and deployment capability for each technology, focusing on real-time anomaly detection and threat mitigation toolkits at complied states. Together, these techniques create a powerful combination of analytical security, intrusion detection, log data analysis, file integrity monitoring, and vulnerability management capabilities being adopted in a variety of industries that handle sensitive data. This infrastructure uses the Wazuh active response module to detect security threats and look for indications that one is starting up. Denial of Service (DoS), brute-force attacks, simulations, and integrity file delinquencies with tests as proofs tell stories about a good performance estimation when Elasticsearch and FileBeat application is used jointly. Wazuh provides a robust and cost-effective solution for enhancing the security posture of enterprise solutions. Wazuh instantly detects and monitors simulated attacks such as denial-of-service (DoS) attacks by spotting suspicious file changes in real-time, logging failure authentication attempts, and identifying the root source of the flood of requests. This study also provides useful insights on designing and deploying comprehensive cybersecurity solutions with open-source tools such as Wazuh, making visual insights for file integrity monitoring (FIM) in real time.

Table of Contents

List of Figures

Chapter 1

Introduction

Organizations are more vulnerable to a wide range of advanced cyberattacks in the modern digital environment. Enterprise networks' security in general is compromised by such risks, which threaten data availability, confidentiality, and integrity. The swift development and integration of information and communication technologies (ICT) have led to greater reliance on the Internet, necessitating the implementation of robust safety protocols to protect confidential information and ensure uninterrupted business solutions. Since they provide real-time analysis, detection, and reaction to security threats, Security Information and Event Management (SIEM) systems are now essential weapons in the cybersecurity toolbox. SIEM solutions also aggregate data from various sources, such as servers, network devices, and applications, to offer a complete monitoring capability, making it easier for threat detection. This allows enterprises to more easily correlate security events and integrate risk detection across their interaction with the products. The open-source SIEM (Security Information and Event Management) software Wazuh provides a useful way to improve endpoint detection and can work with the Elastic Stack for ELK clusters of Elasticsearch, Logstash, or Beats. This integration makes it possible to use strong security analytics, log data analysis, file integrity monitoring, and vulnerability identification. This automated threat mitigation feature of Wazuh lowers the potential harm as it responds to risk in real time, making an even more powerful security foundation. This case study illustrates the efficacy of this SIEM solution in providing unified, next-generation real-time threat detection and response by leveraging extensive modeling of a range of cyberattacks such as file integrity breaches, brute-force attacks, and denial-of-service (DoS) attacks. For any administrator in the administration of a web server, it is an important responsibility to detect all possible threats correctly, since this can corrupt once and for all (or be inaccessible by a considerable portion of users [3]. Cybersecurity is an extremely challenging market owing to the dynamic nature of these industries, which are characterized by continuous innovation and evolving consumer behavior.

1.1 Problem statement

Over time, the security landscape for businesses has become increasingly complex because of advanced cyberattacks that not only affect data availability but also its confidentiality and integrity. When traditional security measures have failed to detect and react against these attacks in real time, enterprises suffer huge financial losses yet tarnish their reputations. The greatest hurdle is to effectively implement and integrate fully-featured

Security Information and Event Management (SIEM) solutions that may provide automated response, abnormal event detection, and real-time alerts.
Because there are multiple competitive SIEM solutions on the market, deploying them can get expensive and complex very quickly, especially with small to medium enterprises. This research addresses a major need from the market to have an open-source, scalable, reliable, and cheap SIEM-enhancing monitoring detection on endpoints. The research highlights the following problems and addresses them:

- Detection and Response Failures: Our systems today cannot detect or respond adequately to advanced threats, delaying incident responses and putting consumers at additional risk.

- Integration Complexities: Especially for businesses with limited resources, the challenge of integrating multiple best-of-breed security tools into a unified framework poses significant implementation problems.

  Scalability and Costs: Smaller companies looking for scalable security solutions may not be able to justify the high costs and resource requirements of commercial SIEM products.

- Coverage Gap: Existing technologies often fail to provide comprehensive protection against a range of cyber-attacks, including Brute-force attacks, denial-of-service (DoS), and File Integrity Breaches.
  To solve these issues, this research aims to create and evaluate an integrated SIEM solution that makes use of Wazuh and the elastic Stack. The study attempts to show how this open-source method can enhance enterprise networks' cybersecurity posture through the use of comprehensive attack simulations and real-time analysis.

1.2 Objectives

The primary objective of this thesis is to investigate the significance of endpoint detection and monitoring CTI activities to improve the efficacy and efficiency of cyber defense operations. The following are the precise goals:

a) To comprehend the function and significance of CTI in contemporary cybersecurity.

b) To investigate the difficulties organizations encounter when monitoring CTI processes.

c) To investigate the advantages of monitoring, response, and Connectivity in CTI and any potential effects.

d) To assess the capabilities and characteristics of the FileBeat, Elasticsearch, Kibana, and WAZUH tools.

e) To rewrite a combined and comprehensive script for automating the open-source tools.

f) To look into the integration and connectivity elements of the used tools.

g) To monitor file integrity monitoring (FIM) for multiple agents both for Windows and Linux operating systems.

h) To orchestrate a brute force SSH authentication attack and monitor the system behavior.

To orchestrate a Distributed Denial of Service attack and monitor how the system behaves.

1.3 Research Problem

Organizations can increase their security and situational awareness by utilizing Cyber Threat Intelligence (CTI). The thesis's central research question is
How can CTI be used to improve an organization's cybersecurity?
The main research question is broken into three sub-research questions to clarify the research problem:

- How can CTI be used to help organizations make decisions?
- How should the organization use the given information to maintain its cybersecurity posture?
- How might CTI help organizations improve their cyber situational awareness?

1. Integration and technical Challenges:

   In this section, we will talk about how Filebeat is integrated into Kibana (Elasticsearch+Wazuh) with a stress on system compatibility and likewise efficient data flow along the lines of scaling but at the same time maintaining security above all by making sure that you encrypt your information as well control access.

   Integration Issues: One of the main research questions is how to properly integrate Filebeat, Kibana, and Elasticsearch along with WAZUH. This includes understanding technology compatibility (so data can flow and systems communicate), interoperability with the current security architecture, etc.

   Scalability and Performance: businesses are confronted with a huge volume of CTI data; as such, scalability and performance are important research problems. This necessitates the study of how well the integrated WAZUH system can scale with increased data volume, as well as the impact on security infrastructure in general (compared to).

   Privacy and Data Protection: With CTI containing transmission of sensitive data and handling, security concerns come in. Research Problem: Studies on secure measures and protection of data in the SIEM- WAZUH integration analysis How to access log files securely and get alerts if there is any attack that has happened This analysis involves examining what methods are in place to keep shared CTI data confidential and to support effective threat detection, response, and collaboration — access controls upgrading, data encryption or anonymization, etc.

2. Threat Detection and Incident Response :
   With Elasticsearch, Wazuh, and Kibana you can automate the incident response process to drastically improve threat detection rates as well as ensure that more reliable intelligent event data is received.

   Endpoint Threat Detection: This is another research query into how a corporation can enforce the task of maintaining its danger detection system with elastic

seek, Kibana, and Wazuh. Among the things that we will look at are how these systems can automatically gather, assess, and correlate threat intelligence data, identify potential indicators of compromise (IoCs) and then alert or provide actionable intelligence for security teams.

Incident Response Optimization: A critical part of security operations is incident response. The question this research tries to answer is whether considering them together could improve incident response. This cannot only build the foundation for understanding sophisticated new cyber-attack methods but also eventually hint at applications of these technologies in improving event handling response time and automation response operations together with aiding in effective communication between incident response teams to combat threats more efficiently.

Quality and Accuracy of the Threat Intelligence Data: The understanding activities associated with how accurate and worthwhile the threat intelligence data has been gained a primary adversary. This involves scrutinizing every CTI source, and checking if it is reliable and valid for the process followed by robust procedures to guarantee that high-quality data scavenged from these are consumed in automated threat detection response systems.

3. Information Compliance and Cost Optimization : Integration with Filebeat, Elasticsearch, Kibana, and WAZUH; cost optimization in the cloud for gives compliance with GDPR, HIPAA, or PCI-DSS.

   Effective Communication: Information sharing is crucial for enhancing collective defense against cyber attacks. Research problem: to assess how the integration of Filebeat, Elasticsearch, and Kibana with WAZUH promotes information sharing between Fintech organizations. Such as more with the data exchange mechanisms, building trust connections amongst this, and dealing with privacy concerns.

   Cost Optimization: A large CTI infrastructure can be costly to build, establish, and manage. Finding the cost-effectiveness of this integrated system is the main research challenge. This will include the financial impact, resource implications, and return investment (ROI) around more effective ways to detect threats faster with lower incident response time to achieve greater security posture.

   Regulatory Compliance: Bearing in mind the type of regulations and industry standards about data security, privacy, etc which the businesses are subject to An ongoing problem is dealing with the regulatory and legal issues of SIEM/WAZUH integration This can include confirming how far the data management and sharing practices are compliant to above laws while considering their alignment strategy with respect all other relevant requirements like GDPR, HIPAA or PCI-DSS.

   Solving these extended research problems would also allow businesses to provide additional fix-points of the integrated system, helping them validate the efficacy efficiency, and compliance in their automated threat detection procedures along with implementation.

Chapter 2

Background and Related work

A rapid increase in cyber threats is giving a marked edge to industries that own powerful endpoint detection response solutions. In this literature survey, we present the results of a variety of scientific research on both, integrated studying SIEM system security information and event management (SIEM) as well as its effectiveness, particularly for Wazuh an open-source solution. To learn how businesses can optimize their security architecture, the integration of Wazuh using different tools and technologies is investigated. This innovation however does bring about important cybersecurity challenges, that continue to increase in sophistication and intensity. The vulnerability to organizational data and services in terms of availability, confidentiality, and integrity has grown since the rise of sophisticated cyber-attacks.

2.1 Optimized SIEM for security posture

For an organization to collect, analyze, and respond to security information from multiple sources, SIEM solutions are important. By providing real-time insights on security events, such solutions assist organizations in rapidly identifying and preventing such attacks. Hussein and Hamza (2022)[19] emphasize the significance of integrating Wazuh and the Elastic Stack into an "all-in-one" SIEM architecture for network device detection of anomalies. By enhancing active response and real-time monitoring, this strategy greatly raises the security of an organization. Gabriela Ioana Enache (2022) is notable [17] for its identification of the primary cyber risks that computer product supply chains face and the inclusion of risk mitigation measures. The study divides the difficulties into three categories: stealing updates, compromising code signing, and erasing free access codes. It then offers a thorough framework to guard against cyber risks in the supply chains through risk management, vulnerability management, and procedures for disclosing discovered vulnerabilities.
The research highlights how the rapid pace and overseas characteristics of industry innovations cause serious cybersecurity challenges [8], such as greater vulnerability to cyber risks and potential fraud. In the Republic of Moldova from 2015 to 2020, emphasizing [16]the immense impact on critical national infrastructure, particularly the financial banking industry. The utilization of cyberinfrastructure for illegal activities is increasing, and challenges in detecting and resisting such risks are addressed in the article. This is particularly relevant for critical industries like banking and national defense. Therefore, cybersecurity techniques in industries need to be adaptable and innovative, and able to evolve along with the technology environment.

2.2 Related Works

An array of related processes can also be combined to improve automated identification and executions, well beyond just MISP with HIVE WAZUH. This broad cybersecurity plan, composed of these interrelated processes, improves the performance of this integrated system. Next, we go deeper into these associated facilities.

Threat Intelligence Feed: There is a possibility of including the external threat intelligence feed over there MISP, HIVE WAZUH to collect more accurate data from inside. The feeds provide context, such as motive data about new risks and indicators of compromise (IoCs), along with evaluation from credible sources — together with cybersecurity businesses, commercial enterprises, or governmental establishments. Businesses can utilize these feeds to stay current on the newest threats and better detect the threats.

Artificial Intelligence and Machine Learning: Using AI /ML technologies can provide advanced capabilities for auto-detect threats, and auto-response operations. Such machine learning models can analyze historical data to detect patterns, anomalies, and correlations in security threats. Thereafter such models can be encapsulated in the system to auto-detect dangers inherently judge inbound data. Using Artificial Intelligence (AI) techniques AI solutions can automate the response activities and decision-making process, decreasing the number of human labor required for incident responses. Wazuh can integrate with machine learning as described in [12]

Continuous Monitoring and Feedback Loop: Continuous monitoring of the integrated system ensures that it remains effective and adaptive to evolving threats. By monitoring the performance, accuracy, and effectiveness of threat detection and response, organizations can identify areas for improvement, fine-tune algorithms, and update threat intelligence sources. Additionally, a feedback loop with incident responders, threat analysts, and system administrators allows for continuous improvement based on their real-world experiences and insights.
A study proposes a new blockchain-based model[7] to securely distribute Cyber Threat Intelligence (CTI) data, addressing challenges faced by CSIRT in sharing valuable and confidential information, and demonstrates its effectiveness through a testbed using Hyperledger Fabric and the STIX 2.0 protocol. Due to challenges such as data management and a lack of appropriate tools or skills, ultimately placing a greater burden on security teams; the paper aims to address these issues by providing a comprehensive understanding of CTI and its benefits and analyzing the use of Artificial Intelligence and Machine Learning to generate actionable CTI, with the main goal of assisting organizations in making informed decisions regarding CTI[13].In 2015, highlighting the use of a machine learning application called EldeRan that dynamically analyzes and classifies ransomware based on specific characteristics, achieving a high detection rate and aiding in the early detection of new variants, providing possible solutions for managing and performing dynamic analysis[14]. Also a neural network model[8]to detect malware in embedded systems by analyzing electromagnetic side-channel signals, aiming to provide an effective and efficient detection approach leveraging the unique characteristics of these signals and the power of neural networks. The architecture of a threat detection data pipeline is built on top of machine learning and real-time streaming [11]. It starts with raw data collection using MISP API events that are the feed of threat intelligence. Real-time streaming using Kafka API to stream this data Machine learning models are implemented for threat detection and risk mitigation in the analysis phase.

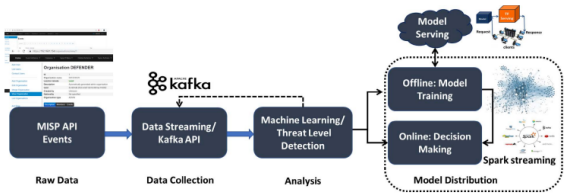

Figure 2.1: I2SP Architecture [11]

It includes a model-serving part that operates Spark streaming in order both to train its models offline and make online decisions. We retrain the model using historical data through offline training and this lets immediate threat detection and response with real time decision-making. The new architecture allows for continuous monitoring and threat detection — all you have to do is 'feed' the model by giving it some API access.
As shown in Paper[14], the Wazuh tool is to be used for the analysis of those solutions that attempt to identify attacks only within their built-up honeypot.

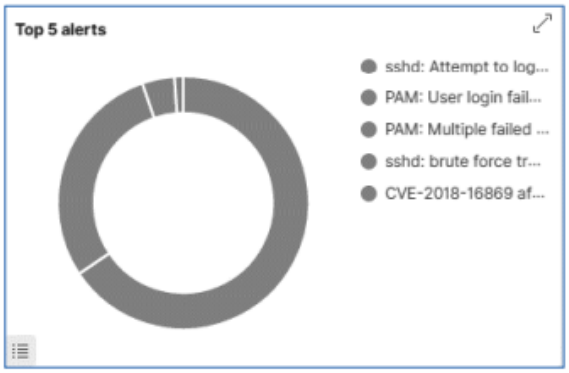

Figure 2.2: Top 5 alerts [14]

The chart creates a "Top 5 Alerts" donut chart to show the most common alerts by system alert. One of the top five alert types is aligned with each section of the donut, as shown on the right side. Alerts like "sshd: Attempt to log in", "PAM: User login failed", 'PAM: Multiple failed login attempts "," sshd : brute force attempt" and CVE-2018–16869. The segment that shows its ratio of occurrences represents each alert. The chart showcases (in a positive way) what needs to be improved for additional system security in terms of important cybersecurity struggles such as failed logins and brute force attacks.

2.3 Capabilities of Wazuh SIEM

Wazuh is a comprehensive open-source platform designed for intrusion detection, integrity monitoring, and compliance monitoring. By integrating different tools, it provides a complete security solution.

- Active Response and Integration:
  - A powerful architecture for log data analysis, file integrity monitoring, intrusion detection, and vulnerability recognition in security analytics is provided by Wazuh combined with Elasticsearch, Filebeat can Kibana. One area where this setup excels is in boosting real-time monitoring and compliance solutions[25].

- A study that is centered on the active response modules of Wazuh which neutralize threatening future effects through improvising with context-aware interventions for attacking cyber defacements [20].

- Implementation and Testing:
  - Wazuh deployment involves developing a system architecture using Wazuh agents and managers, along with changing internal settings and data flow processes. This setup provides real-time threat detection and monitoring[25].

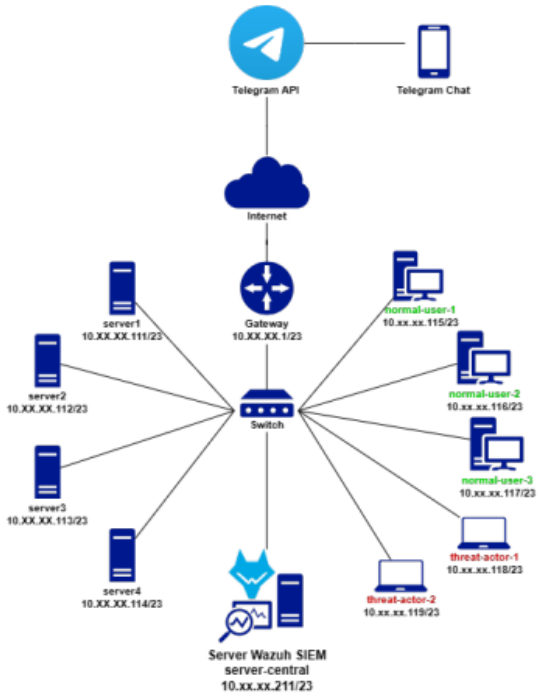

Figure 2.3: Simulated system topology [25]

The following diagram illustrates a Wazuh SIEM server monitoring servers and users. It has three regular users, two threat actors, and some servers all behind a central switch. Through an API, it sends alerts or notifications to a Telegram chat, and data goes on the network through a gateway out to the internet.

  - Wazuh highlights its capabilities in detecting recognized cyber attacks in a study that combined it with NIDS and used Metasploit as the attacking tool. This suggests that Wazuh could be an economically viable alternative to enterprise SIEM systems for small organizations[6].
  - One of the most well-known studies [17] was conducted by Gabriela Ioana Enache (2022), who provided a deep evaluation of cyber risks faced by computer product supply chains and somehow covered risk prevention techniques. The paper breaks down these challenges into three groups: theft of updates, code-signing hijacks, and free entitlements deletions. It then presents a comprehensive supply-chain cyber security risk management framework followed by implementable practices for vulnerability identification and remediation as well as procedures to report observed vulnerabilities.

2.4 Mitre attack module for Wazuh

ATTACK framework is adversary tactics, techniques, and procedures with a knowledge base of attacker (s) behaviors helpful for detection. This data can help security analysts be thorough in researching and monitoring adversarial behavior. By launching the ATTACK framework, MITRE expands on its mission to expose a safer world by collectively defining more effectively how cyber security works.
ATTACK IS FREE AND OPEN TO ANY PERSON OR ORGANIZATION.
The attacks were conducted using Atomic Red Team, a project that consists of 170 different roles all associated with MITRE tactics [26].

2.5 The Role of Host Intrusion Detection Systems (HIDS)

The most crucial component of FinTech cybersecurity is host intrusion detection systems (HIDS). HIDS, such as Wazuh himself, monitor internal systems to detect any sign of malicious activity or invasion anywhere in a system set. Here are several functions that they offer:

1. Unauthorized Access Detection: HIDS can find out the Unauthorized attempt made [1] over ai to get unauthorized access to systems or data; This is a key concept in FinTech, where unauthorized access can lead to serious financial losses and data breaches.

2. Detecting Anomaly: While it is not a silver bullet, the HIDS solution can be effective in detecting potential deviations from the expected behavior of the system that could signal cyber risks.

3. Log analysis: Applications of this type scour system logs with the idea that unusual events are cause for looking further to determine if a security breach is taking place.

4. File Integrity: HIDS, like Wazuh, assesses vital system data to be sure the information has been modified The authenticity and privacy of financial information must be protected.

The active response functionalities implemented, its link through Telegram, and integration with the SIEM Wazuh solution are expected to bring good insights in terms of feasible combinations people can build inside companies at affordable costs in their information security area..[25]

2.6 Regulatory Compliance and Reporting

With Support for GDPR and PCI DSS Compliance: Deploying full-spectrum cybersecurity solutions allows financial services to remain compliant with governing laws, such as the General Data Protection Regulation (GDPR) or Payment Card Industry Security Standard(PCI-DSS). The legislation must also include rigorous privacy protections and data security safeguards.

1. Automated Compliance Reporting: Implementation of technologies such as Wazuh can allow FinTech companies to create compliance reports without any manual effort, certifying that they follow numerous regulatory regulations.

2. Data Protection and Privacy: FinTech companies can more effectively safeguard client data and assure privacy, which is essential to staying in line with legal requirements, by integrating powerful HIDS and analytics technologies. In the framework of regulatory monitoring, reporting, and compliance, this article addresses the function of regulatory technology (RegTech) in financial markets, solutions, and institutions. It draws attention to how RegTech has evolved beyond the digitization of manual reporting and regulations to allow proportional, real-time regulatory regimes that manage risks and promote effective regulatory compliance. [2]

2.7 Wazuh events and case studies:

There are specific implications for real-world threat detection and monitoring. Some of them are:

- Enterprise IoT security:
  An agentless Wazuh module for enterprise IoT networks that improves security by analyzing device traffic while deploying agents on endpoints. IoT network security is one area in which this strategy excels [24].

- Web Applications Security:

  Wazuh's functionality in securing web applications was evaluated by Willerton and Gustafsson[23] compared to other HIDS. Wazuh worked well for securing web applications because it performed better than alternatives in the areas of threat detection and hardware performance.

- Integration of Big Data: According to Bhatnagar, sentiment analysis on Twitter data may be efficiently performed using Elasticsearch, Logstash, and Kibana (ELK Stack). With the ability to be scaled to cybersecurity monitoring, this connection demonstrates the ELK Stack's capacity for managing and monitoring massive data sets [10].

- Network Security and Traffic Analysis:
  Network security is a set of operations for protecting data, applications, devices, and systems connected to the network. It focuses on the system design, operation, and management of the architecture to provide network accessibility, integrity, continuity, and reliability. Traffic analysis (often called Network Traffic Analysis) is a subdomain of the Network Security domain, and its primary focus is investigating the network data to identify problems and anomalies[4].
  Stanković provides an outline of Wazuh's web server attack detection capabilities. The study highlights how Wazuh is an integrated security monitoring solution due to its use in security analytics, intrusion detection, log data analysis, and file integrity monitoring [20].

2.8 A Comparative Analysis of Wazuh, with existing infrastructure

Organizations need to consider several kinds of aspects when selecting an integrated security infrastructure and security information and event management (SIEM) solution, including cost, scalability, functionality, user-friendly use, and integration posture. Why Wazuh might be preferred above alternative top platforms, which include IBM QRadar, Microsoft Azure Directory, and Splunk Infrastructure, is the primary focus of this research.

1. Cost Optimization

   Wazuh: As Wazuh is an open-source infrastructure, enterprises of all sizes may utilize it for very little expense. It eliminates the requirement for a specialized SIEM solution license. The only expenses that go with this will be linked to technology (cloud hosting, on-premises servers, etc.) along with, while necessary, specialized technical assistance.

   IBM QRadar: For massive implementations specifically, QRadar provides a commercial solution that comes with expensive licensing and maintenance costs. For small to medium-sized companies, all of the expenses may be impossible to afford.

   Though Microsoft Azure Directory offers robust identity and access control, integrating it with a full-fledged SIEM solution often requires additional Azure services (such as Azure Sentinel), that can quickly drive high expenses, particularly when managing high data ingestion rates.

   Splunk Infrastructure: While Splunk is often criticized for its costly expenses, it is widely recognized for its robust analytical capabilities. Splunk expenses depend on the volume of data used, which may pose an important drawback for companies that deal with big data sets. It is not as suitable for economical businesses as overall expenses may increase quickly.

2. Open-Source Flexibility

   Wazuh: Being open-source, Wazuh offers unmatched flexibility. Users can customize and extend the platform to meet specific requirements. The open nature of the platform also encourages a vibrant community that contributes to plugins, integrations, and updates, making Wazuh highly adaptable.

   IBM QRadar: While QRadar is feature-rich, it is a proprietary solution, limiting the ability to customize or extend the platform beyond what IBM offers. This can be a limitation for organizations with unique or complex needs.

   Microsoft Azure Directory: Azure Directory is just one small piece of the Azure ecosystem. At a high level docker for Azure provides integration but only at an architectural level, not what one can customize in the application. It is often limited in functionality and to extend the capabilities, you need additional Microsoft Services or other third-party tools.

   Splunk Infrastructure: While the app ecosystem does offer some flexibility, most customization is limited to whatever spare parts Splunk has sitting inside its walls. Moreover, this system also does not function well with non-standard data sources

or custom-built applications and may require some expert interface to be set up as per the organization's needs.

3. Ease of Deployment

   Wazuh: Deploying Wazuh is not that hard, especially in the cloud. Along with security professionals, this technology has been also designed to simplify operation for system administration from a web-based user interface (GUI), combined with appropriate documentation. Scaling the deployment is easier through various environments.

   IBM QRadar: Although QRadar is a powerful tool, it can be difficult to configure and deploy without the help of experts (either from your staff or through third-party consulting). Big systems hurt most of all when you are just beginning.

   Microsoft Azure Directory: Azure Directory integrates well with other Azure services, which will make the transition smoother for businesses that are already using the Azure cloud. However, the setup and integration can be pretty difficult for someone not well-versed with Azure.

   Splunk Infrastructure: Although Splunk is a good foundation, deployment can be difficult — especially in bigger, multi-cloud computing or hybrid use cases. The intricate procedures of setting up data sources, scaling to many users, and fine-tuning performance might demand mastery.

4. Integration and Compatibility

   Wazuh: Wazuh natively integrates with hundreds of systems and log formats, including Docker logs. It works exceptionally well with all other open-source tools such as Elasticsearch and Kibana, providing the same experience for enterprises who are already in an OSS ecosystem. Wazuh also has a good number of third-party integrations hence it is more versatile in different scenarios.

   IBM QRadar: While QRadar provides integration capabilities with IBM and third-party tools. Its closed-source nature means some integrations may need extra licensing or professional service. QRadar is extremely solid because of its integration into the IBM ecosystem.

   Microsoft Azure Directory: Azure Directory integrates very well with other Azure services, which helps organizations that are highly invested in Microsoft products. But Azure Directory offers integration with non-Microsoft setups that can be a bit more difficult, needing third-party tools or customization.

   Splunk Infrastructure: Splunk is known for aggregating and analyzing data from a plethora of sources. It has strong integration functionality, but it can be complex to maintain these interfaces especially if one is working with multiple or hybrid scenarios. The third-party integrator typically requires scripting or programming capabilities to accomplish a custom integration.

5. Scalability

   Wazuh: It can scale from a small environment with startups to large multinational companies. Being able to exploit cloud infrastructure and work with Elasticsearch has made it excellent at managing large amounts of data. Scaling Wazuh can be

difficult and it may require some planning; which if carefully prepared (like in larger operations) shouldn´t be a problem.

IBM QRadar: QRadar is scalable for large companies, though scaling up can be costly with licensing costs and hardware requirements. It was made for big instances but is expensive on both money and ops.

Microsoft Azure Directory: Developing on this theme, Azure Directory scales well within the same place (the land of Microsoft), so larger enterprises that are all in with Azure as their platform should think hard about using it. This will mean a large number of underlying store rows which can start to become expensive with high data ingest/retention.

Splunk Infrastructure: Splunk promises the ability to do great things with data, but scaling — even databases containing only "time series" without any relational across time relationships can take substantial investment and effort. This makes the license cost even more expensive and is hence problematic for enterprises with less capital.

6. Security and Compliance

   Wazuh: The highlight of Wazuh is its powerful security features like log analysis, file integrity monitoring (FIM), vulnerability detection, and configuration assessment. It ensures adherence to most of the popular regulatory standards including but limited to PCI DSS, GDPR, and HIPAA. Its open-source framework enables versatility and quick time-to-market to cater to any country-specific regulations.
   IBM QRadar: QRadar is a key player in taking care of compliance and security concerns with reactive threat detection, and behavioral analytics combined with comprehensive regulations. It is often selected by larger international companies subject to strong regulatory requirements, but the high costs may be a burden for small or medium-sized businesses.

   Microsoft Azure Directory: Active Directory offers robust security capabilities, especially for authentication and authorization. One can have a great SIEM solution when you combine it with Azure the Sentinel. Still, its primary concentration is on the Azure landscape, so it may not be very usable by non-Microsoft users.

   Splunk Infrastructure: While you can add advanced security analytics and compliance features within Splunk, these tend to look very similar but getting them running can be quite hard especially early on. Splunk: Splunk is known to have a very good analytics functionality, especially in the field of security but may be an overkill for most simple use cases.

7. Community Support and Vendor Lock-In

   Wazuh: Wazuh is an extensive and growing open-source ecosystem of plugins, integrations services. Not being locked into a vendor has immense benefits, enabling enterprises to take full control over their security architecture without depending on any one player.

   IBM QRadar: QRadar has major vendor support, yet its dependency on IBM's ecosystem could contribute to vendor lock-in. The high expenditures and exclusive features of the solution make it challenging to migrate to alternate ecosystems.

Microsoft Azure Directory: If Azure Directory is rolled into the Azure stack, then it would be a classic example of vendor lock-in — especially when other Microsoft services are in play. While community engagement is crucial, much of it winds up on the broad Azure silo.

Splunk Infrastructure: Splunk has a large community and great vendor support, but it is also very expensive and closed-source, which may make a non-preferable target for its lock-in. Major enterprises are unlikely to easily move on from Splunk, not least due to infrastructure investment and the complexity of configuring its setup.

Wazuh is an attractive alternative for organizations seeking an affordable, flexible, and expandable SIEM solution. whereas IBM QRadar, Microsoft Azure Directory, and Splunk Infrastructure each have advantages, Wazuh's open-source environment, low cost, straightforward use, and absence of vendor lock-in make it a popular option, particularly to enterprises that seek flexibility, transparency, and authority over their security infrastructure.Here's a summary of the comparison :

Feature	**Wazuh**	**IBM Qradar**	**Microsoft Azure Directory**	**Splunk**
Cost	Free and open-source. Expenses related to infrastructure and optional support	High-cost licenses, especially in large deployments	It can get expensive with additional Azure services and ingesting large data	High licensing costs, particularly based on data ingested.
Open-Source Flexibility	Fully open-source, highly customizable and extendable.	Limited customization, depends on IBM-provided features	Integration mostly within Azure with additional services	Proprietary; customization possible but complex, especially for non-standard data sources.
Ease of Deployment	Relatively easy to deploy with good documentation	Complex deployment requiring specialist workforce	Easy within Azure, challenging outside ecosystem	Complex setup, especially in large or hybrid environments.
Integration	Broad integration with open-source tools (e.g., Elasticsearch, Kibana) and third-party services	Broad, but often requires additional licenses and services	Seamless within Azure but difficult with non-Microsoft environments	Strong integration capabilities but complex in diverse environments.
Scalability	Highly scalable with proper tuning, suitable for diverse environments	Scales well but requires high buy-in for larger enterprises	Scales efficiently within Azure, but costs can rise	Scalable, but scaling comes with high costs and complexity.
Security Compliance	Supports major compliance standards (PCI DSS, GDPR, HIPAA)	Great for compliance, but can be costly	Strong in identity management, full SIEM requires additional Azure services	Powerful analytics, but complex and costly to configure for compliance.
Community Support	Large open-source community, no vendor lock-in	Vendor support available, risk of vendor lock-in	Strong support in the Azure ecosystem, risk of vendor lock-in	Large community and vendor support, risk of vendor lock-in and high costs.

Table 2.1: Comparative analysis of Wazuh, IBM QRadar, Microsoft Azure Directory, and Splunk

Chapter 3

Methodology

3.1 Wazuh's Capabilities

Wazuh, having a robust and flexible Host Intrusion Detection System (HIDS), includes a wide range of capabilities that are highly significant and helpful to the FinTech industry. This includes:

Intrusion Detection: Wazuh's initial proficiency for detecting unauthorized access and harmful activity is critical for FinTech organizations, which are frequently targets of extensive attacks via the internet.

Monitoring File Integrity: This function maintains the authenticity of financial data and transaction storage by making sure that essential financial data and system files are not changed.

Log Analysis: A way to evaluate and understand massive quantities of log data in real-time is essential for FinTech companies that conduct thousands of transactions every day.

Identifying Vulnerabilities: Wazuh's vulnerability detection technique identifies and addresses security holes in programs and applications, which is crucial to FinTech firms that depend significantly on software solutions.

Compliance with regulations: Wazuh aids FinTech organizations in corresponding to multiple regulations, including GDPR and PCI DSS, with fully integrated monitoring and reporting features.

3.2 Elasticsearch, Filebeat, and Kibana's Roles and Synergies in Cybersecurity

- Elasticsearch: As an efficient searching and analytical engine, Elasticsearch considerably boosts Wazuh's analysis skills. To detect and respond to threats in real time, FinTech organizations need to be capable of fast sorting through and analyzing massive amounts of data.

- Kibana: To facilitate the interpretation and understanding of the data analyzed by Wazuh and saved in Elasticsearch, Kibana is used to give visualization functionalities. Kibana's visualizations and dashboards may provide FinTech organizations

with informative perspectives on compliance status, possible security risks, and transaction trends.

- Filebeat: This lightweight log shipper works smoothly with Elasticsearch and Wazuh. Filebeat can effectively handle and transfer logs from several sources in a FinTech setting, guaranteeing that all operational and transactional data is kept an eye out for security risks.

3.3 Deploying the Theoretical Ideas for Industries

Theoretical foundations provide an adequate context for implementing Wazuh inside the cybersecurity domain. Applying these ideas to industries comprises:

- Custom Security Policies: Applying Wazuh's decoding machines and rules to identify anomalies and patterns unique to transactional data from the fintech industry.
- Scalable and Efficiency Optimization: The Case of Wazuh's interfaces using Elasticsearch and Filebeat must be optimized to handle massive datasets quickly, especially given the enormous number of transactions in the FinTech industry.
- Compliance Reporting: Implementing distinctive compliance reporting capabilities in Wazuh to fulfill the particular financial needs of the businesses.
- Real-time Data Processing and visualization: Integrating the real-time data analytics of Elasticsearch with the visualization powers of Kibana to deliver useful insights for instant decision-making in a rapid FinTech environment.

3.4 Environment Configuration

The thesis on enterprise platforms includes all the components essential to the sector's operations and is built following the architecture of a typical financial technology company. Among them are:

- Transaction Systems: Internet-based platforms for managing high-voltage transactions in finance, including the processing of payments and trading in stock systems.
- Data Storage: Sensitive financial data, that includes transaction records and client information, can be securely kept in protected databases.
- Infrastructure of Network: A sophisticated network configuration that consists of wired and wireless connections, cloud-based services, and channels for both internal and external communication.
- Endpoint UI: Web-based financial platforms and mobile banking apps are examples of end-user interfaces, which are programs that interact with customers.

- Compliance with Regulation: Methods and procedures put in place to guarantee adherence to financial laws such as PCI DSS, GDPR, and AML (anti-money laundering) requirements.
- Reflecting the demanding security requirements of the FinTech sector, this environment is equipped with firewalls, intrusion detection systems, and encrypted data connections.

3.5 Data Flow

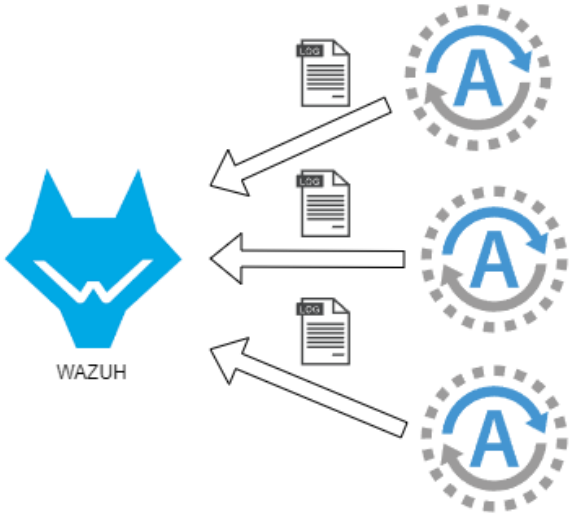

Figure 3.1: Wazuh Data Flow

With many Wazuh agents deployed throughout the FinTech infrastructure, Wazuh serves as the primary intrusion detection and monitoring solution for the cybersecurity architecture. The Wazuh manager's and its agents' setup and data flow are depicted in the diagrammatic model (see Figure 6.1).

1. Wazuh Manager: All of the agent-collected data converges at the Wazuh manager, which serves as the setup's core. Data analysis, security alerts, and threat response synchronization are within the scope of its authority. Along with managing the ongoing security monitoring procedure, it saves intelligence data.

2. Wazuh Agents: Installed on a variety of endpoints, including servers housing transactional systems, data storage devices, and user interface components, Wazuh agents distribute themselves throughout the network.An instance of the efficiency of the Wazuh forensic tool in tracking and recognizing botnet attacks on systems in real time. The study demonstrates how the Wazuh agent may greatly improve cybersecurity when installed on a server by effectively recognizing and disclosing different kinds of cyberattacks as they happen.**12**

3. Log Files Monitoring: The Wazuh system's detection techniques rely heavily on the log files. Every agent keeps a close eye on the log files it has been assigned, which include a detailed history of all system operations, transactions, and operative events.

4. Dynamic Data Flow: The environments, rules, and updates are distributed across the agents in this design, represented by the arrows pointing towards the Wazuh manager in their direction. Through this approach, the cybersecurity team's most recent security regulations are certain that they are executed by every agent. In contrast, the agents provide the management with the gathered log data back so that it may be centrally analyzed, correlated, and alerted.

Real-time monitoring and immediate response are guaranteed by the configuration. An abnormality in access patterns, a mismatch in file integrity, or a possible security breach are examples of events that a Wazuh agent can identify and report back to the management when it finds them. Following that, the manager uses correlation criteria to evaluate the alert's legitimacy and severity, maybe combining it with data from other sources, before sending out alerts or initiating automatic reactions. This architecture enables the essential requirement of sustaining secure and continuing financial services in the setting of a FinTech business. FinTech businesses can ensure the security of their financial transactions and the confidentiality of their data while also abiding by the strict laws and regulations placed on the sector by putting in place such a watchful and responsive system.

3.6 Pipelining Data Process

Figure 6.2 shows the data processing pipeline, which shows the step-by-step approach from log file collection to the presentation of data files, Filebeat, Elasticsearch, and Kibana are the four main parts of the pipeline. They are all vital for the flow and transformation of data, which makes it possible for the FinTech company to efficiently track, analyze, and manage cybersecurity events.

Figure 3.2: Data Pipelining

1. Collection of log files: The pipeline begins with a compilation of log files. These are thorough logs of all the events that occurred within the FinTech network. Multiple systems and applications produce log files, which record all user activity, system faults, security events, and transactions.

2. Filebeat: Filebeat is set up as the data carrier whenever log files arrive. Monitoring specified log files for adaptations, collecting recent data, and delivering it to Elasticsearch is its primary role. With a focus on productivity and small volume, Filebeat is capable of handling enormous amounts of data while utilizing limited resources. Within the ELK stack, Filebeat is a useful tool for gathering and initial analysis of log data. Regarding the administration of log files for the PanDA infrastructure [5]. Given the heavy pressure of high transaction rates characteristic of FinTech processes, it assures the data is transported securely and without incident.

3. Elasticsearch: Elasticsearch functions as the analysis and engine for searching after it gets the data. This indexes the data so that it may be analyzed and accessed. In this phase, Elasticsearch additionally performs information enhancement tasks like transformations and aggregations, which are essential for identifying patterns and anomalies. Its scalability and robustness are vital for processing the enormous amount of data created by the FinTech sector and essential for real-time analysis. Elasticsearch [18] arrange environments may be optimized using the Sequential The disturbance Stochastic Approximation approach. By dynamically altering the configuration parameters, this optimization technique is demonstrated to significantly boost Elasticsearch's performance, especially when processing massive datasets. The result is a boost in data-inserting capability and system reaction time of over 40

4. Kibana: Inside the pipeline, Kibana acts as a visualization component. Consumers may explore and visualize data stored within Elasticsearch using the user interface. Kibana's dashboards provide an approach to organizing complex sets of data into understandable, relevant data for security personnel and FinTech experts. It's here that information transforms into insight, providing potential risks in a user-friendly way, highlighting patterns, and spotting anomalies. immediate comprehension of the present level of cybersecurity and operational health is made possible by Kibana's capability to customize dashboards to fulfill distinctive security and organizational goals. For the visualization and analysis of data, with a particular emphasis on the sentiment analysis of data from Twitter. It shows how Kibana, a component of the ELK stack, offers a user-friendly graphical user interface for real-time data analysis and visualization, making it an effective instrument for collecting insights from social media data[9] ,

3.7 System Architecture

We define the comprehensive architecture of the Wazuh deployment, illustrated by Figure Z, as part of our cybersecurity structure for FinTech operations. The interfaces between the server and agent components are presented in this architecture, which shows an integrated method for security monitoring, analysis, and responses.
Server Element: The server element, which consists of the following elements, constitutes the core command structure:

1. Wazuh Manager: Engine Analysis: The engine analysis component evaluates security event data acquired by the agents. It employs sophisticated computer algorithms and rule-driven monitoring to find anomalies breaches, and different evidence of vulnerability.

2. Connection Service: Specifies consistent secure channels for interaction with every agent to ensure data transfer and security policy synchronization.

3. RESTful API: Automated interaction with external apps and services using a standard framework. Data obtained through the Wazuh manager gets automatically collected, transformed, and analyzed thanks to it.

4. Filebeat: Filebeat is positioned [5]inside the server's infrastructure and is responsible for moving log data through the Wazuh to Elasticsearch in an efficient way.

Its configuration optimizes system strain while processing high volumes streams of data.

5. Elasticsearch:Operates as a distributed real-time [18]search and analytic engine. It is optimized for rapid indexing, quick data consumption, and advanced searches that offer rapid insight into the vast quantities of data that are typical of FinTech organizations.

6. Kibana: Users can generate and manage [9]dashboards containing visual illustrations of the security data through the use of Kibana, which integrates with Elasticsearch to provide the visualization front-end. For end users to completely comprehend and respond to the information provided, these illustrations are important.

7. Endpoint User: This element depicts the security analysts, SOC professionals, or system administrators who connected with the system. Employing Kibana dashboards, they analyze security alerts in real time, look into events, and make sure that financial constraints are continuously followed.

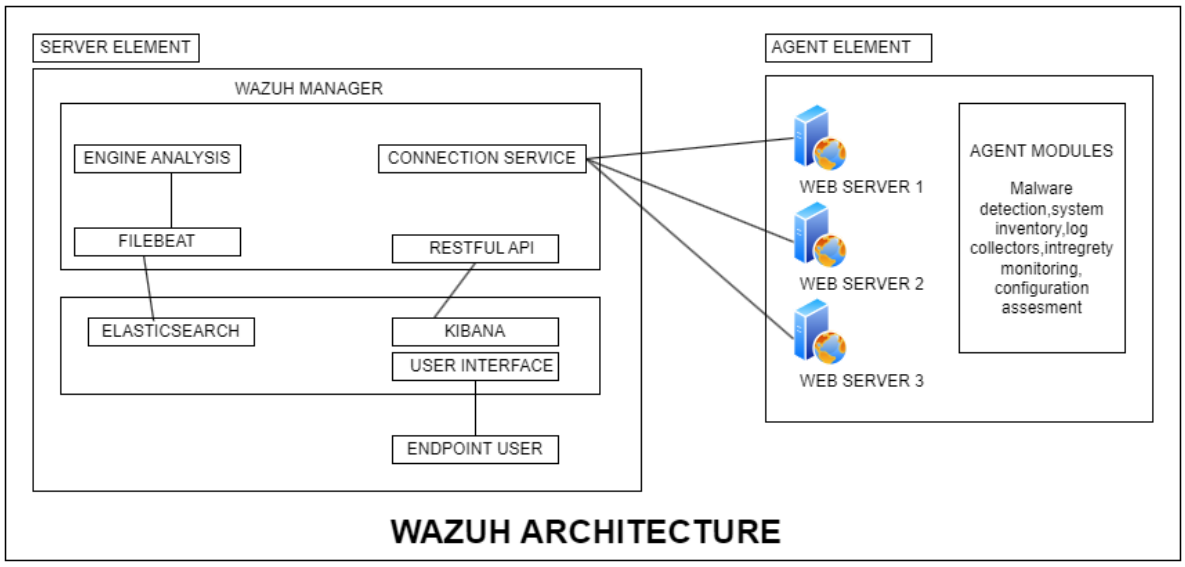

Figure 3.3: System Architecture

Agent Element: Along the boundary of the infrastructure, the agent component includes: **Web Servers:** Such indicate distributed nodes integrated with Wazuh agents within the infrastructure of the FinTech organization. Their deployment involves the monitoring of specific system elements such as network traffic, application logs, and transactions by users.
Agent Modules: Every agent comprises multiple types of modules suited to perform specific security tasks:

1. Malware Detection: Scans to identify if the host machines face any malicious software.

2. System Inventory: Monitors changes in hardware and software, facilitating asset management and legal compliance

3. Log Collection: collects logs from systems and applications for monitoring purposes, including security and functional.

4. Integrity Monitoring: Inspects the file systems and essential configurations for unauthorized modifications.

5. Configuration Assessment: Guarantees that security criteria are followed while configuring systems.

Data flow interaction:
This architecture's interactions follow a defined path:

1. Data Collection: The agent module consistently collects data from the host systems concerning security. The following includes identified anomalies log entry points, and changes to the system status.

2. Data Transmission: The Wazuh Manager gets collected data via the Connections Service, which validates and manages the incoming feeds.

3. Log Shipping: The Wazuh Manager implements Filebeat to transmit the selected logs to Elasticsearch to ensure they can be instantly indexed and correlated when the data has been analyzed.

4. Analysis and Visualization: Kibana retrieves the data from Elasticsearch and minimizes it for complex searches, which Elasticsearch then uses to generate visual representations for endpoint users.

5. Administrative Control: The system administrator can use the interface with the Kibana dashboards, monitor safety incidents, perform searches, and start responses with the assistance of visual data.

Implementing this architecture, security data is constantly handled and made accessible to the individuals in the role of maintaining the organization's cyber defenses, thus guaranteeing each component of the FinTech infrastructure is always monitored. Active security posture becomes possible by the integrated system, helping the FinTech organization instantly detect, analyze, and act on potential risks.

Chapter 4

System Implementation

4.1 SIEM setup

The integrated security system consisting of Wazuh, Elasticsearch, Filebeat, and Kibana, is explained in the implementation chapter which also provides clarification on the procedures for configuring and deploying this system. An array of scripts meant to automate the setup, prevent human error, and ensure consistency within the installation service as the base for this section. The [21] research involves monitoring and analyzing incidents on a web server's port 80 using the SIEM Wazuh system. It analyzes how well SIEM Wazuh performs in detecting and mitigating these threats using network forensic techniques using OSCAR and detecting techniques. The study illustrates how SIEM Wazuh can help security personnel monitor and protect corporate IT assets from these kinds of attacks.

Processor and Memory Usage: For intermediate workload, the Wazuh agent is deployed on a system with an AMD Ryzen 7 5700U processor and 3.78GB of memory for RAM, it is a setup that provides a balance between cost and performance. As part of AMD's Ryzen 7 family, the Ryzen 7 5700U has strong multi-threading capabilities that are essential to managing multiple tasks at once—a requirement for security monitoring when incidents occur simultaneously and unpredictably.

Performance Under Load: While the processor is powerful, it encounters challenges while there's a lot of data being consumed, like at high data input and while performing essential rule-based log analysis, because of the RAM's relatively small capacity. Such circumstances are critical as they have an immediate impact on the capacity of real-time intrusion detection. RAM restrictions can lead to delays in the processing of logs, which could result in delays in the generating of alerts, which allows malicious activity to continue undetected.

System's Processing Capacity: Maintaining security postures requires a way to process huge volumes of logs efficiently while avoiding major delays or queuing. The RAM limitation is a constraint that needs to be fixed to improve real-time analysis abilities, yet the Ryzen 7's architecture aids in processing speed.

Operating System Details: The Wazuh agent runs on an operating system of Ubuntu 22.04.4 LTS. This OS option is important as Wazuh is a security-focused application, and Ubuntu is widely used, has a strong support system, and emphasizes security.

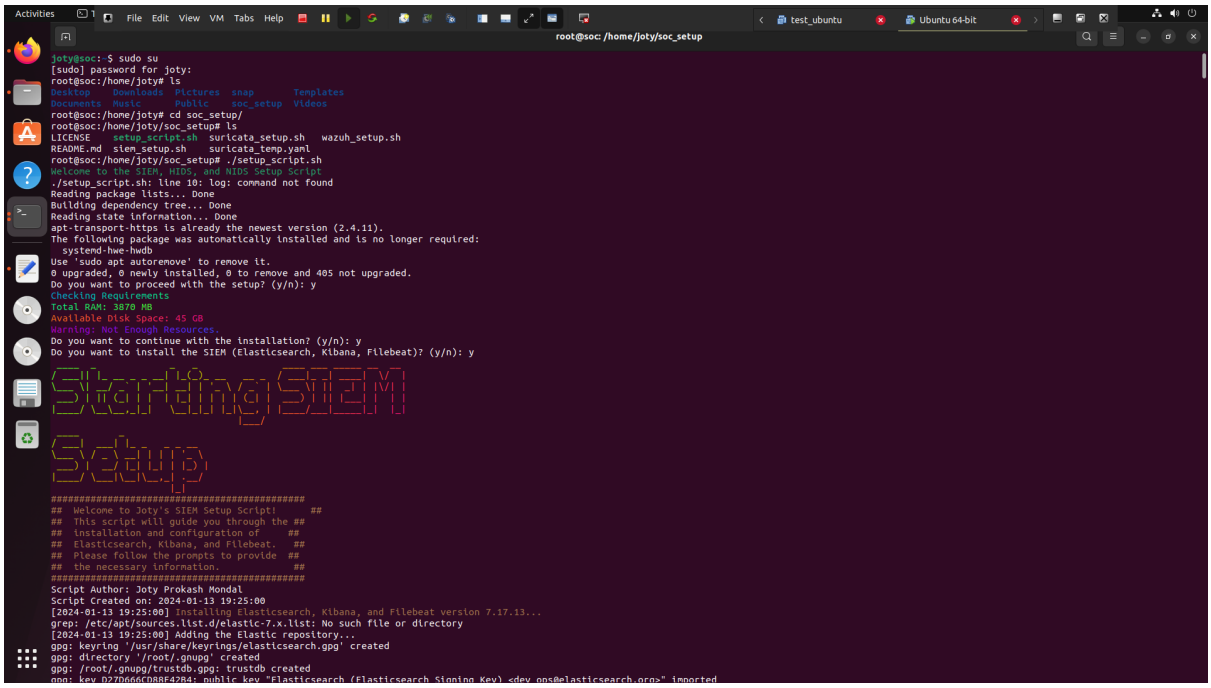

Figure 4.1: SIEM Validation

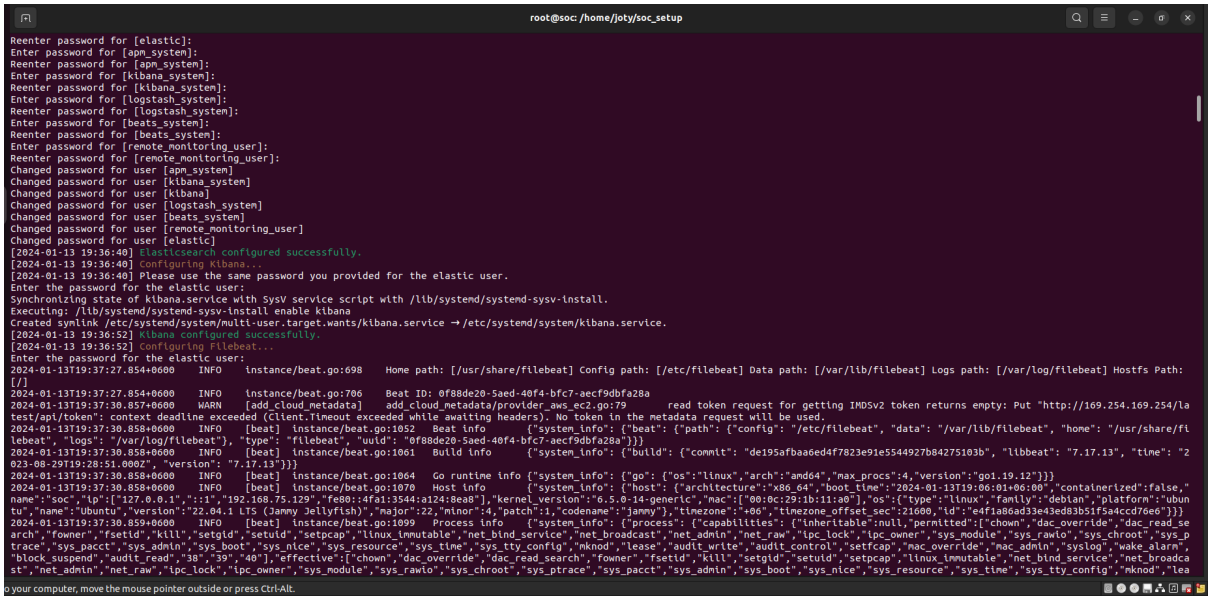

Figure 4.2: Configuring Validation

4.2 Deployment of Wazuh, Elasticsearch, Filebeat, and Kibana

As color-coded messages are utilized, the deployment process begins with an informational and eye-catching welcome message. It not only builds the overall tone for the next few phases but also supplies vital information as the author of the script and the execution timestamp. This portion of the script provides an illustration of how essential user experience is, particularly with technological configurations. To ensure the system is prepared to accept the setting up of the new components, prior setup inspections of integrity are needed. Half or incomplete installations may occur because of interrupted or prevented dpkg processes, which the script seeks for and repairs. Also, it ensures identification in any present Wazuh installations. Users are provided with the chance to delete such sets once they discover them, minimizing any installation issues.

4.3 Configuration and Customization Steps

After verifying that the components are ready for installation, the script then proceeds into the setting up stage. This is a diligent process that goes from step to step from installing software to setting up a repository to installing the Wazuh manager and interacting with Filebeat. This script will simply reset the list of packages to supply from in the Wazuh repository on all available and install the GPG key for the Wazuh repo. For this reason, the Filebeat configuration file needs to be supplied with specific settings for Wazuh and Filebeat can work together. This will make it easier for Filebeat to get logs from Wazuh, which we´ll analyze on our previous ELK environment step. In addition, the script is responsible for installing and enabling all required templates and modules so that you can properly analyze your log data in Kibana.

4.4 Integration Testing and Security Baseline Establishment

A range of checks are conducted when configuring the integration and operational functionality of Wazuh. These checks should verify you have set up the Wazuh management services correctly and are running successfully.
The last phase after completing a series of installations is the Filebeat setup. At this point, the script configures Filebeat by linking it to Elasticsearch and Kibana as well as ensuring all relevant log data processing pipelines are loaded. The script has been designed to offer the user obvious error messages if the setup doesn't work, aiding them in recognizing and correcting the issue at hand. The script terminates the process via a success message, which acts as both a completion indication and a sign that the system has been set up for safety measures. The interactive aspects of the script, which involve user prompts and straightforward feedback, are meant to preserve users active and well-informed at every stage of the procedure. The operationalized security environment within the FinTech infrastructure, that employs Wazuh attached to the Elastic Stack, is explored realistically in this chapter. The results are presented through a collection of Kibana dashboards, offering information about the system's real-time monitoring abilities, compliant status, and alarm systems.

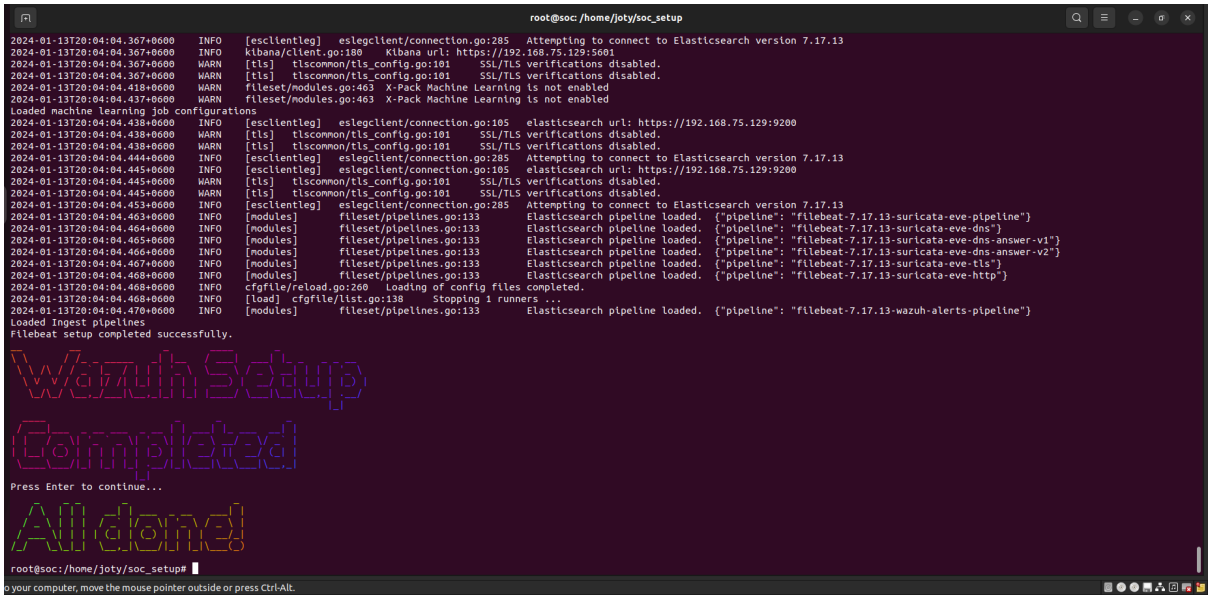

Figure 4.3: Wazuh setup

4.5 Attack Simulation

This section explains how we created a security monitoring system relying on Wazuh and ran various attacks to evaluate the capacity of such a system in terms of detecting malicious behavior. In this case, a laptop is an attacker and also it emulates the Security Information and Event Management (SIEM) system but one more needs to note that here desktop computer is a victim.

Configuration Information:

- Attacker and SIEM (Laptop)
  Ip Address:192.168.0.105
- Victim(Desktop)
  IP Address: 192.168.99.128

Nmap is a free and open-source tool that can be used, depending on how it cannot get use of the detection phase. for network discovery by security auditors in pen-testing(which indicates a planned attack against the computer system) DevSecOps. During penetration testing, it identifies open ports, and services that help in port scanning and also helps to find out vulnerabilities about target systems within a security assessment. Nmap is used to check the security status, compliance, and exposure of network configuration in DevSecOps.

Strategy:

Wazuh SIEM shows that attempted attacks and ports are attacking the local machine on port 22 (SSH).

1. We map the network to see which ports are open.
2. Ensured that the victim's computer kept port 22 open.
3. Utilized Hydra to launch a brute-force attack with SSH.

Operation	*Description*	*Use Cases*	*Offensive security use case*
Network Discovery	In a network it identifies all the working devices	Discovers the network devices	Point out the effective targets for the attacks
Port Scanning	Identify the open ports on the devices	On server it checks all the open services	Checks the vulnerable services to exploit
Service Version	Identifies the versions of the working services	It checks whether the software versions are up to date	Checks the expired vulnerable services
OS Detection	Checks the operating systems of all the network services	Manages the OS-Specific vulnerabilities for exploitation	Targets all the specific OS vulnerabilities for exploitation

Table 4.1: Nmap Overview

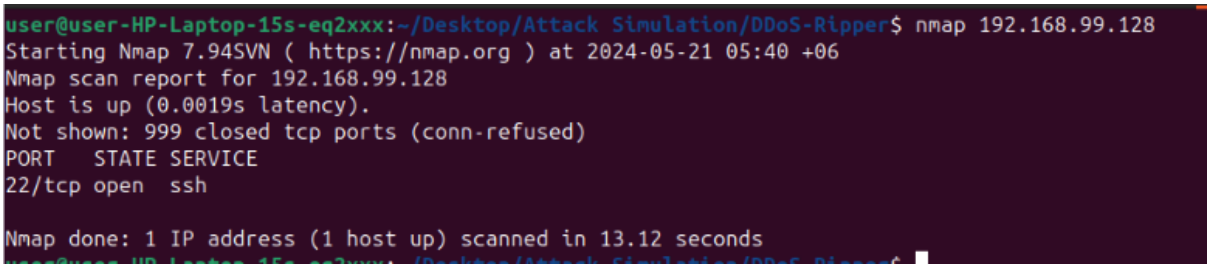

Figure 4.4: Network Mapping

Operation	Description	Use Cases	Tools Availability
A parallelized login cracker is called Hydra.	auditing of passwords	Looking for weak passwords	User manual available on official website
Several protocols, such as FTP, HTTP, and SMTP, are supported.	Assessments of network security	Attacks using brute force on network services	GitHub: https://github.com/vanhauser-thc/thc-hydra
tries to guess passwords via dictionary attacks.	Penetration testing	breaking remote access protocols such as SSH	Kali Linux docs for Hydra
able to be combined with additional instruments for thorough security examination	Verifications of security compliance	Finding errors in the configuration of authentication systems	Community discussion boards and forums

Table 4.2: Overview of Hydra

Attack 1: SSH Authentication Attack
We also used an offensive security tool in the way of Hydra which is open source and conducted an SSH authentication attack on our victim's machine. This attack aims to observe whether the system can detect and inform the victim about port 22 (SSH) vulnerability.

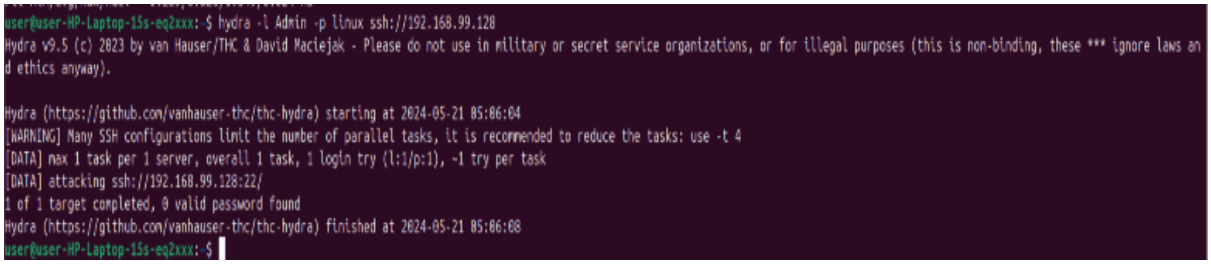

Figure 4.5: SSH Authentication

Hydra is an open-source tool powered by many login attempts a second by brute forcing network logins, fuzzing web forms simultaneously. It is a very fast and versatile tool that can be utilized for things like HTTP, FTP, or SSH protocols being used which also makes it imperative for security professionals to have. Hydra is anchored in extensive documentation and community support to help users perform comprehensive security testing.

Operation	*Use Cases*	*Offerings*	*Documentation*
produces a large number of network packets	Network infrastructure stress testing	Resilience testing using DDoS assault simulation	Github Repository: https://github.com/palahsu/DDoS-Ripper.git
targets a number of protocols, such as TCP, UDP, and HTTP	Assessing the server's capacity	Recognizing possible DDoS weaknesses	Contributions from the community on GitHub
Floods targets with distributed systems	Benchmarking of network performance	Testing methods for mitigating	Forums and discussion boards
Can be configured for different attack intensities	Exercises and drills related to security	Evaluating how well security measures work	

Table 4.3: DDos Overview

4.6 Attack 2: Distributed Denial of Service (DDoS) Attack

Simulating a DDoS attack means that we are applying attacks on a few applications running over the victim's machine to check if the system detects it, and monitors it or not.
In this section, we describe an open-source application named DDoS Ripper to mirror Distributed Systems that run inside the cluster deploying it. It will enable attackers to send thousands of unique individual requests to each targeted system. A DDoS to ripper (Educational Highly efficient security testing tool in the cybersecurity field) would help administrators understand the repercussions of such attacks and get a better insight into improving their security posture. Because it is an affordable unit with more than a little potential, both security professionals and hobbyists have gravitated toward the alternative.
Configuration:

- Laptop accessed by the attacker (IP: 192.168.0.105)
- Desktop Computer: Victim Machine (IP: 192.168.99.128)
- Target Port: A particular application port on the attacked system

Attack Summary:

- Tried to see the server's limits/response, Attackers Flood it with traffic Using Distributed Denial of Service.
- This attack overloaded traffic over a few minutes, closing down one particular service.

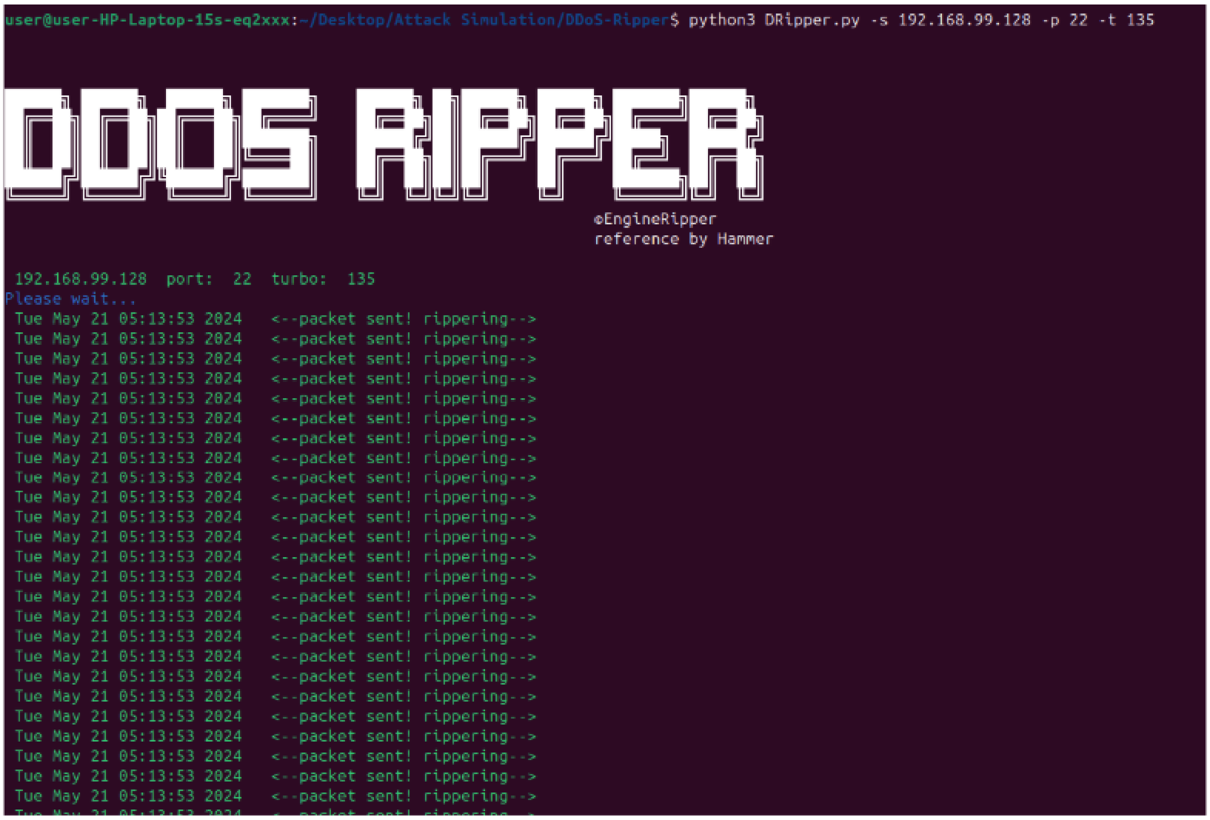

Figure 4.6: DDos Attack

Its installations with attack simulations demonstrate how Wazuh SIEM can detect and inform victims of DDoS attacks as well as SSH authentication. That complete configuration is an example of how Wazuh can be deployed and used to monitor and secure different perspectives of the network from other cyber threats.

4.7 File Integrity Monitoring (Windows)

File Integrity Monitoring (FIM) from a cybersecurity standpoint is the process involved in maintaining the files and directories on a system. Wazuh, an open-source infrastructure continuously monitors security system that provides enterprise-grade File Integrity Monitoring capabilities for trends to files and directories protecting from unauthorized changes, thus enabling the organizations to keep system security and compliance.
1. File Integrity Monitoring: Wazuh keeps books located on file systems up-to-date for real-time monitoring.
the status of files upon creating or updating them, detecting any changes made to the file such as modifications additions, or deletions — all based on the configured. exclude patterns.
directories.
2. Hash-based Verification: Wazuh calculates some cryptographic hashes (like MD5 and SHA) for the files anticipated to be modified, and periodically compares them with currently used values before notifying that the file is indeed altered.
It computes the hash value (example: MD5, SHA-1, SHA-256) of files and compares it with a predefined baseline.

values to detect any inconsistencies that point to tempering.
3. Policy Customization: Wazuh even lets its users define their requirements based as per their security needs, well-suited monitoring and detection of critical files and directories.
4. Alerting and Response: Upon detecting unauthorized changes, Wazuh generates alerts and notifications in real-time, enabling prompt response to potential security incidents. These alerts can be integrated with SIEM platforms for centralized monitoring and analysis.
5. Centralized Management: Wazuh centralized management such as its management server may have capabilities to simplify the lines of certain services
FIM agents deploying and monitoring across multiple endpoints
6. Compliance Auditing: Wazuh FIM assists organizations in meeting compliance requirements by providing detailed audit trails and reports of file system activity, helping demonstrate adherence to regulatory standards such as PCI DSS, HIPAA, GDPR, and more.
7. Scalability and Flexibility: Wazuh FIM is highly scalable and adaptable. suitable for environments ranging from small businesses to large enterprises, on-premises or in the cloud
In my SOC lab environment, the Wazuh Server in KVM and Windows11-agent on VMware are running.

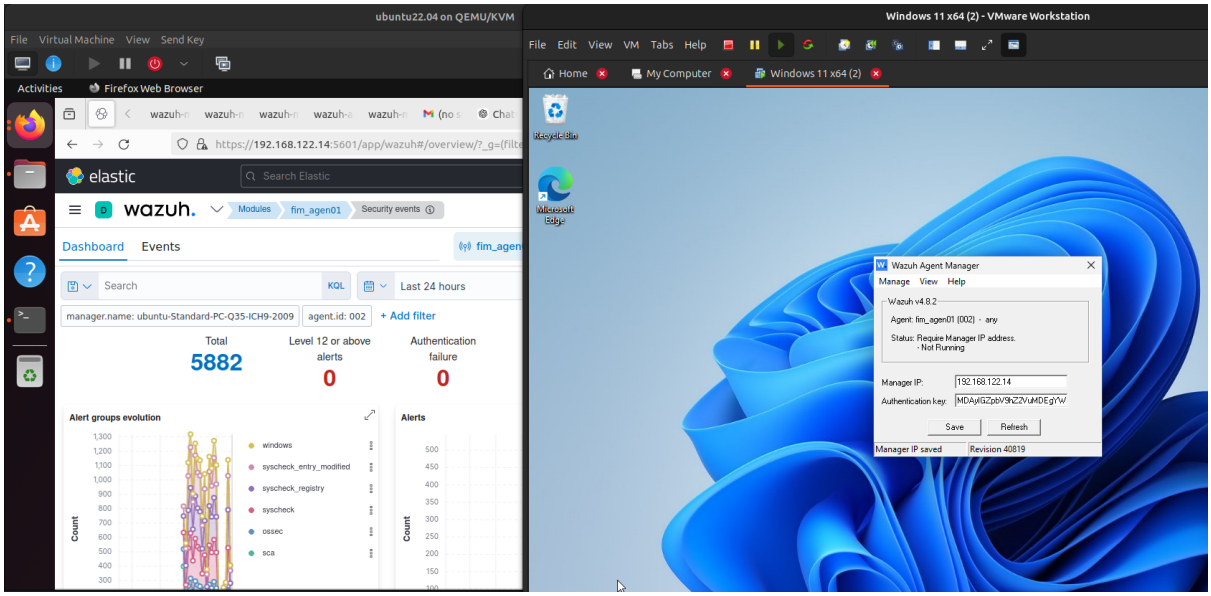

Figure 4.7: Wazuh manager and agent

Here is the "ossec.conf" file, in "File integrity Monitoring" section. Here is the SysSYS check configuration available.
We monitored the Downloads folder files' integrity. Copied the path of this folder and edited this line.
After creating, modifying, and deleting random files in the download folder, the integrity monitoring dashboard keeps generating log events.
In the implementation of FIM using Wazuh, the system continuously monitors the integrity of critical files and directories.
FIM module scans pre-determined directory servers at regular intervals and monitors those setups in real-time for changes. The paths to monitor can be configured at the

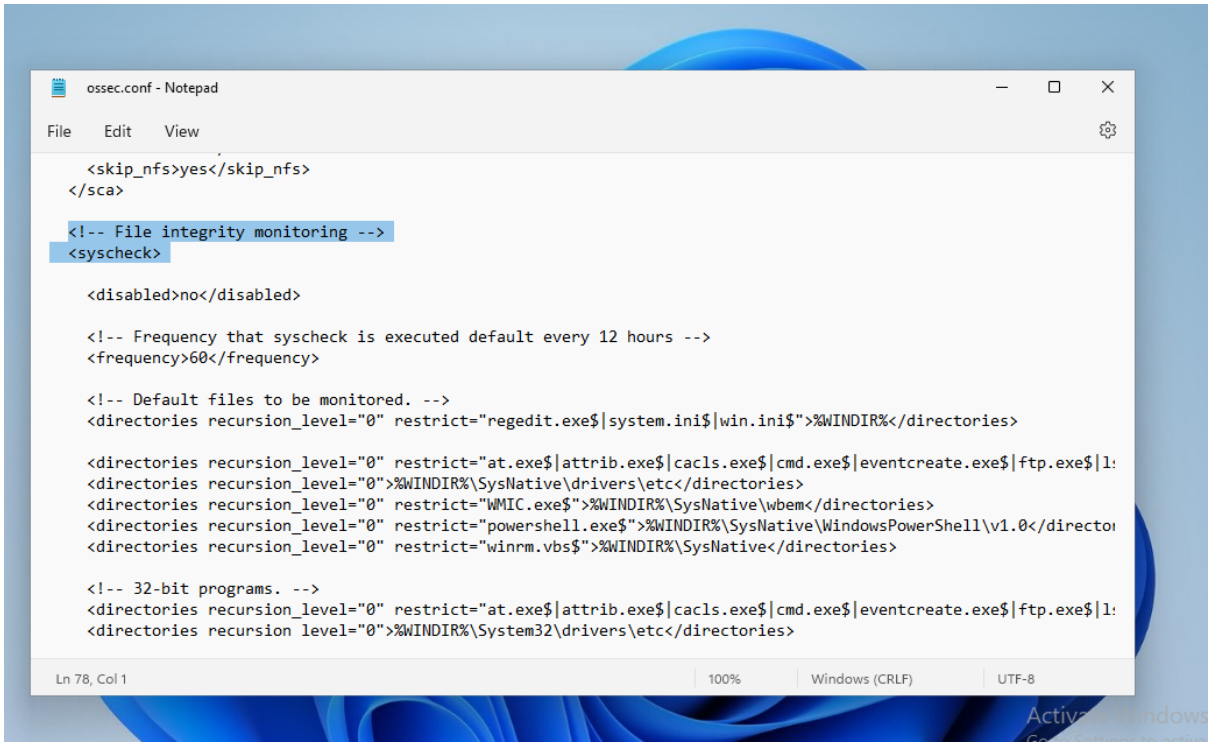

Figure 4.8: Ossec.conf

```
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
<directories report_changes="yes" check_all="yes" realtime="yes"> C:\Users\apurb </directories>

<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>
```

Figure 4.9: File Editing

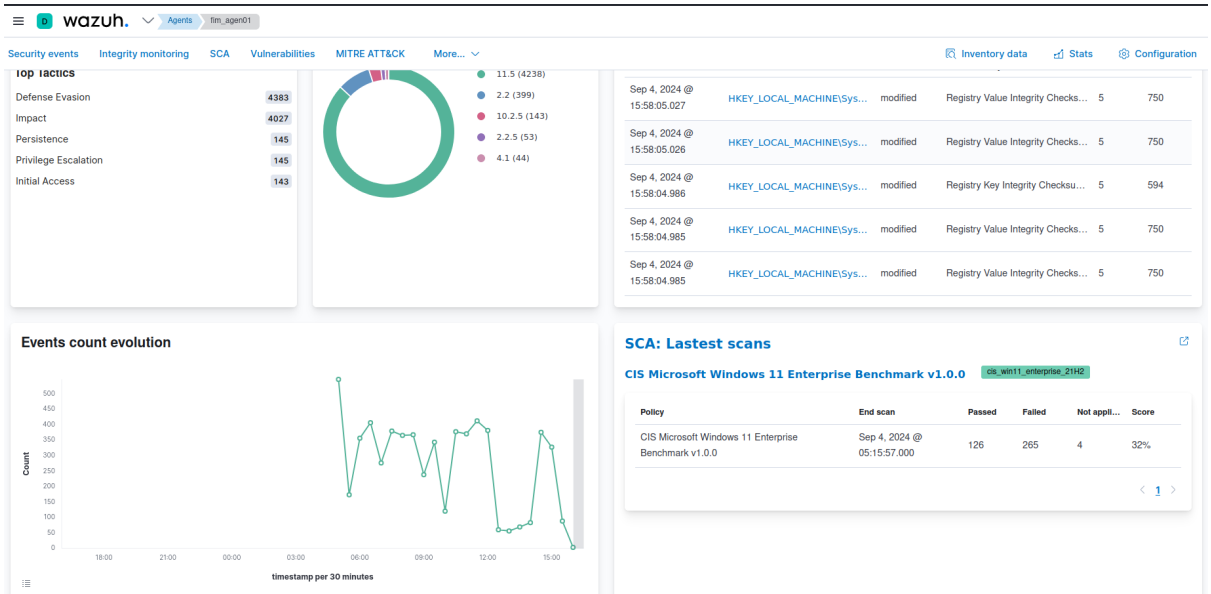

Figure 4.10: Wazuh Dashboard

Wazuh agent and manager settings. FIM generates and saves file checksums and attributes that are locally stored in a database on endpoints.

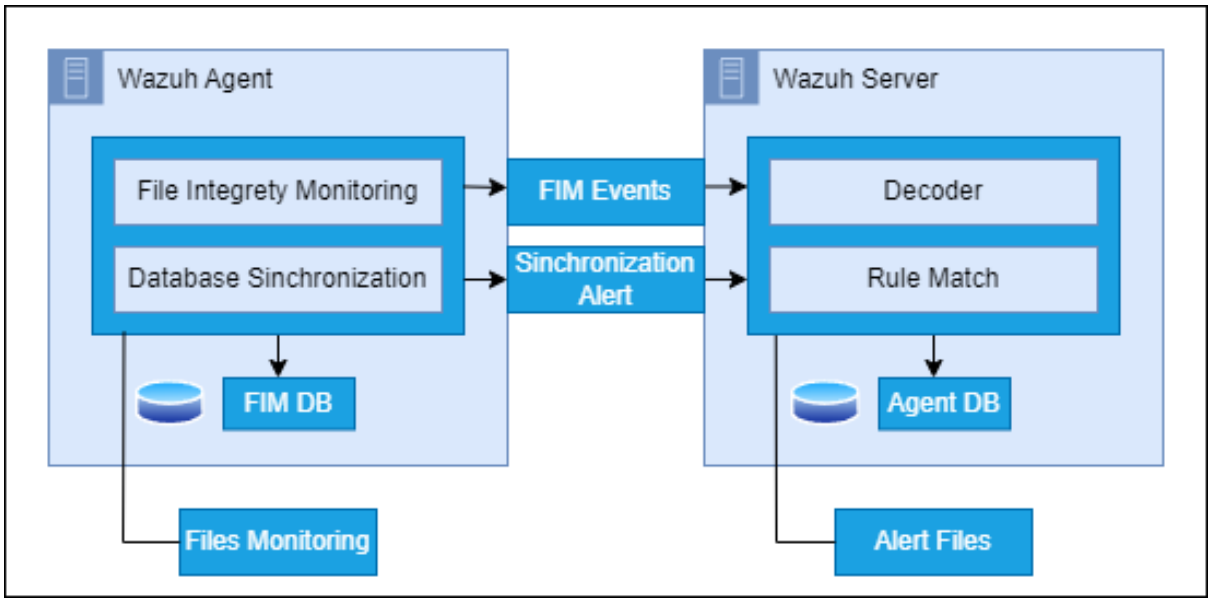

Figure 4.11: FIM Architecture

To achieve this, FIM implements two independent databases: a local SQLite database in the endpoint and an agent database in the Wazuh server managed by the wazuh-db. It synchronizes the changes in its files (log messages) on the agent side to keep this up-to-date which is present in the Wazuh server database.
The dashboard provides a summary of top security tactics like defense evasion and impact, along with detailed event logs, showing specific file or registry changes on the monitored Windows machine. The Event Count Evolution graph tracks the number of integrity events over time, providing insights into periods of heightened activity.
The integration of Wazuh with FIM enables real-time detection and alerting of unauthorized changes, crucial for maintaining system security and compliance.
Analysis of FIM Events: The graph demonstrates that most of the system activity throughout the day focuses on modifications, with little addition or deletions.

Figure 4.12: FIM Events

1. File Modifications (Green) :

High Activity: Most of the activity relates to file or registry modifications. These modifications happen in breaks apart, with maxima occurring: Around 5:00 and 9:00: In certain instances, activity spans between 120 and almost 280 changes. From 09:00 to 14:00, there were approximately 100-160 file modifications suggesting an ongoing pattern. After 15:00, there's a substantial decrease in modification activity, which continues stable but lower (60) till 18:00, when there are still no recorded modifications.

2. File Deletions (Blue):

   Low Activity: During the monitoring time frame, the number of deletions remained quite small. A slight rise may be detected around 04:30 and 06:00, with a slight increase of roughly 20 deletions. The remaining part of the era stays stable, with just over ten deletions.

3. File Additions (Pink):

   Minimal Activity: The number of additions stays low, as it occurs with deletions. Slight spikes occurred around 05:00-07:00 and 09:00, with increases averaging just below 20 entries. The remaining portion of the day is going to be relatively quiet.

   The graph highlights that most of the system activity during the day is centered on modifications, with very few additions or deletions.

The below graphic contains 3 pie charts that provide insight into multiple aspects of file integrity monitoring (FIM):

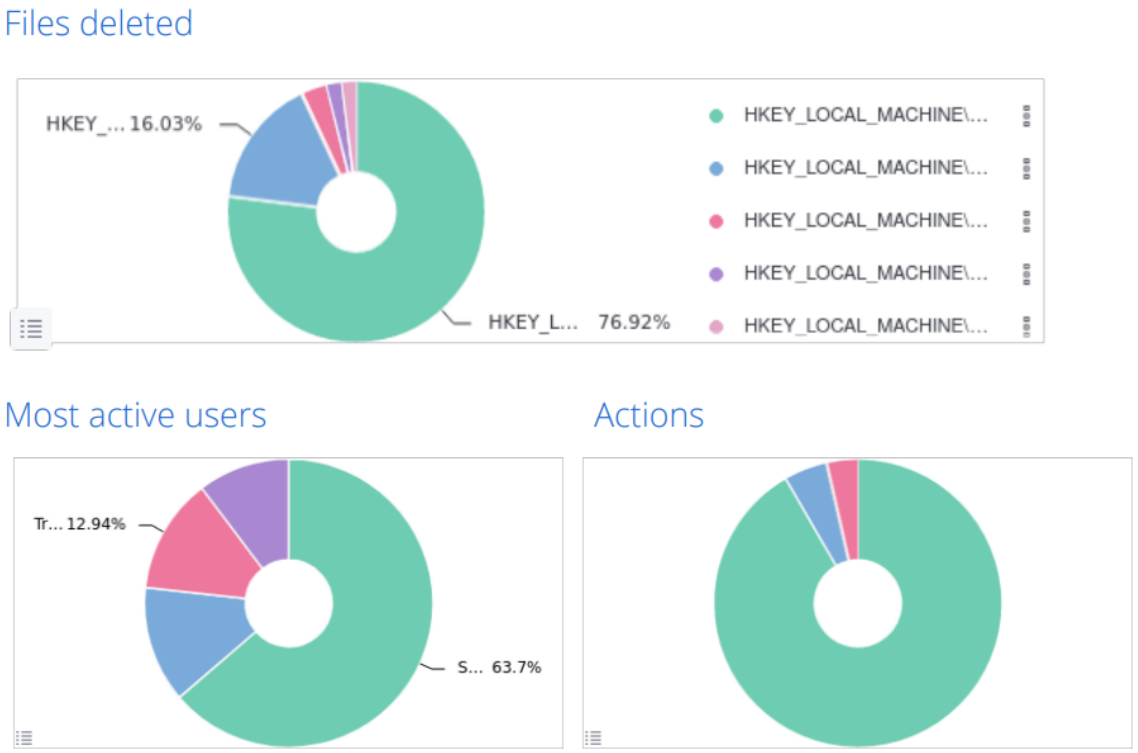

Figure 4.13: FIM action analysis

1. Files Deleted:
   The pie chart illustrates the order of deleted files, with an emphasis on registry routes inside HKEY-LOCAL-MACHINE. A majority of deleted entries (76.92%) are connected to a single registered path, demonstrating that the deletions were caused by a certain key. Other registry entries provide fewer percentages, with 16.03% and other tiny entries. The deletions focus on files in the registry, which might suggest cross-system modifications or cleanup actions.

2. Most Active Users:
   The following chart illustrates the users who started the most actions.(63.7%) is the most active user, performing a majority of actions. Other users (Tr..., etc.) generate a lesser amount of activity, including the second most active user, providing 12.94%. This breakdown indicates that one user (is heavily involved with implementing changes).

3. Actions : The "Actions" representation demonstrates a breakdown across multiple action groupings.

4. Overview of files added and modification:
   The pie charts represent an overview of system activity which incorporates registry modifications:

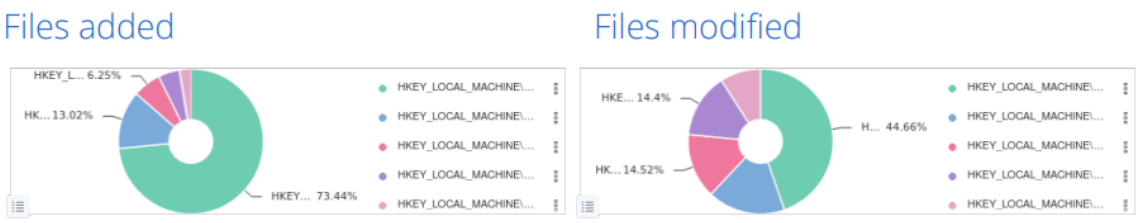

Figure 4.14: File analysis

Files Added: Most (73.44%) of additions occurred inside the HKEY-LOCAL-MACHINE System registry and lower percentages on other registry entries.

Files Modified: Most of the changes (44.66%) happened to HKEY-LOCAL-MACHINE, while further modifications were scattered among different entries in the registry. These actions usually involve system-level modifications, usually connected to core services or networking setups.

Chapter 5

Result and findings

5.1 Inventory Data Analysis

Installed Critical Packages: The packages that are installed on the Wazuh agent system may enhance or make security more vulnerable. A summary of the important packages mentioned in the inventory is provided below.

Name	Architecture	Version	Vendor	Description
hydra-gtk	amd64	9.2-1ubuntu1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	very fast network logon cracker - GTK+ based GUI
libwhisker2-perl	all	2.5-1.2	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	Perl module geared for HTTP testing
net-tools	amd64	1.60+git20181103.0eebece-1ubuntu5	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	NET-3 networking toolkit
nikto	all	1:2.1.5-3.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	web server security scanner
xfonts-scalable	all	1:1.0.3-1.2ubuntu1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	scalable fonts for X
libgeocode-glib0	amd64	3.26.2-2build2	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	geocoding and reverse geocoding GLib library using Nominatim
libdrm-intel1	amd64	2.4.113-2~ubuntu0.22.04.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>	Userspace interface to intel-specific kernel DRM services -- runtime

Table 5.1: Installed critical packages

Not every Linux distro has this package installed by default, though since it is a key development-related variation to the hydra-gtk utility (a very fast network logon cracker that supports many different services and hash major language extensions and cracks faster than object concepts).
HTTP testing with libwhisker2-perl (CORE, Ninja-corE) is a powerful toolset when looking to find potential issues website.
The net-tools provide ipconfig networking utilities, and the legacy system that is used for old network configurations offers functions for Linux users.
Nikto is among the more popular web server security scanners, with a great deal of support and an easy-to-understand list of vulnerabilities for anything it finds. - xfonts-scalable:

Scalable fonts for X window system, making the text more readable libgeocode-glib0 : Geocoding and reverse geocoding for location-based services (or as utilized in gnome-maps) libdrm-intel1 -Be certain you are using a new enough Intel driver which supports SNA or UXA.

5.2 MITRE ATTaCK Integration Analysis

This section demonstrates ways the Wazuh system utilizes information collected from system logs to detect, categorize, and respond to various cyber security threats. The Wazuh system is integrated with the MITRE ATTaCK frameworks. The type of alerts, strategic distribution, and the security posture of the system are the primary focus of the study.

Operation	*Use Cases*	*MITRE ATT&CK TTPs*	*Impact on Wazuh*
lists and describes hostile strategies and methods	identifying attack routes	Use strategies like exploit public-facing applications and phishing to simulate attack vectors.	enhances the identification of particular attack vectors
maps to different attack phases	Increasing the level of danger intelligence	Resolve weaknesses with Continuous Monitoring	combines to track and notify on particular methods
updated often with fresh methods	Planning for incident reaction	Create barriers with Network Segmentation	gives useful information for preventing attacks
Open-source and acknowledged by the industry	evaluation of the security posture	Enhance detection with Defence Evasion	increases capacity to identify, prioritise, and address risks

Table 5.2: MITRE ATTaCK Overview

- High-Frequency Alerts: Primary Alert: When a brute-force attack approach occurs, the most frequent indication is "Attempt to login using a non-existent user." This underscores the prevalent threat of unsanctioned entry attempts, which are likely initial attempts by attackers taking advantage of lax authentication protocols.
- Insight into System's Response: The regularity and management of such alerts are critical since they merely indicate the current threat yet put the system to the test in regards to the way it can uphold security regulations. This covers speed limitations, alarms resulting in, and IP address auto-blocking linked to recurrently unsuccessful login attempts. Regulatory compliance requirements have been mapped to the Wazuh rules to give regulatory compliance support [22]
- Broader Implications: If these alerts persist, it could indicate a sign that improved network perimeter protections, like multi-factor authentication (MFA) or dynamic IP blacklisting techniques, are required.

- Activity Over Time: The graphic shows that as the hours draw on, particularly following midnight, the frequency of notifications increases. Noted tactics like SSH attacks and password guessing intensify in the early morning, reaching their peak at 06:00.

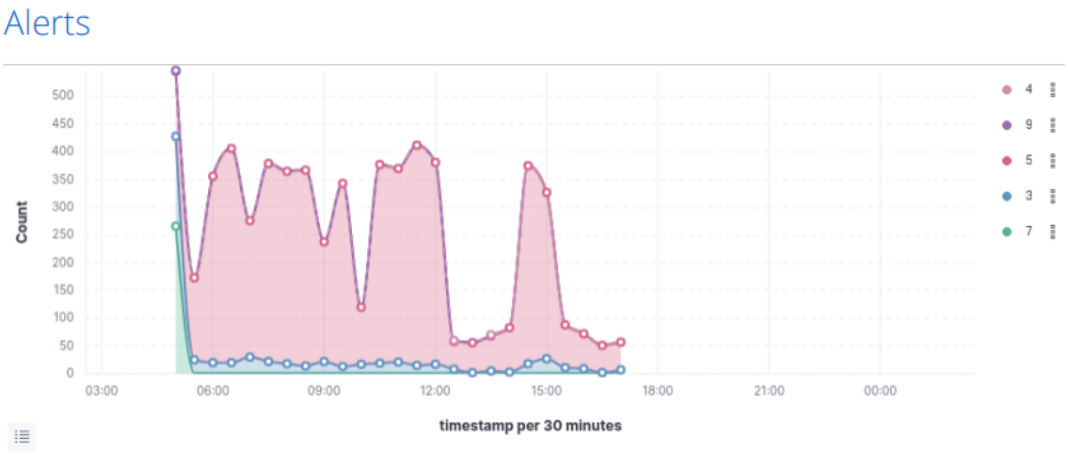

Figure 5.1: Timestamp per 30 minutes

Item Specific Tactics Observed: Password Guessing and SSH: The most significant rise is shown in both of these approaches, indicating a focused attempt to take advantage of network functions and authentication protocols when less monitoring is probably essential. Sudo and Sudo Caching: Moreover, there is an apparent increase in the use of sudo, which might indicate the rise in capabilities of an attacker or the completion of valid administrative tasks. Item Security Implications: Critical Hours: The increase in critical techniques like password guessing in the early hours of the morning suggests a possible window of vulnerability where attackers may anticipate less attention.

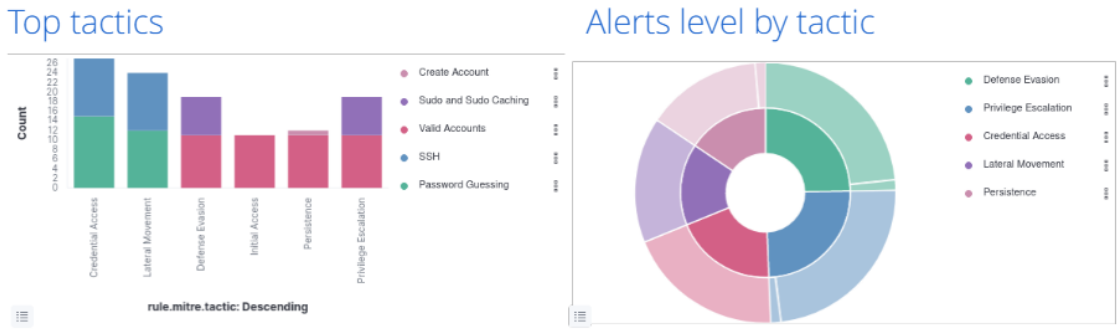

Figure 5.2: Alert evolution

In this part, we showcase and analyze the outcomes of our tests deploying the Wazuh tool for detecting multiple security risks. The data gathered from targeted web servers during a specific period forms the basis of the analysis. Two essential diagrams—"Top Tactics" and "Alerts Level by Tactic"—visualize the results.

Figure 5.3: Alert tactics

- Initial Access: The technique, which has 18 incidents, describes ways adversaries deploy to establish their initial foothold inside a network.
- Persistence and Privilege Escalation: The analysis of 16 instances of each approach suggests that adversaries are attempting to secure themselves onto their position and obtain higher-level authorization, alternately.
- Credential Access: Based on a count of 24 incidents, this technique was the most commonly used. Account name and password theft is one of its objectives.
- Lateral Movement: This technique, which has 22 instances, focuses on ways attackers can travel through a network to seek more access points or critical data.
- Defense Evasion: With 20 events, this group of events highlights the techniques used by adversaries to stay undetected during a breach.

These figures demonstrate the typical tactics that attackers use and emphasize the significance of strong security at various network nodes.

5.3 Security alert analysis

Alert Level Evolution :
To ensure system integrity and privacy, this section emphasizes critical alerts that require to be addressed shortly.

- High-Level Alert:
  Integrity checksum changed: 180 events.
  This high number indicates that key files may have been intentionally tampered with or altered without authorization. It is crucial to assess these changes to avoid vulnerabilities in security.
  Debian Package(Dpkg) half configured: 18 events.
  New software installations could introduce new vulnerabilities. These instances should be assessed to ensure that only authorized trustworthy software is installed.

- Medium level alert:
  File added to the system: 44 events
  Frequent file uploads may signal the spread of malware or unauthorized changes. Each instance must be assessed for authenticity. Attempt to log in using a non-existent user: 12 events
  This indicates unauthorized access or brute force attacks. These attempts can be monitored and restricted to stop illegal access.

- Low-level alert:
  PAM: Login session opened: 14 events
  Monitoring login sessions aid in the identification of unusual activity. Analyzing such events can help identify patterns that suggest potential security issues.

Figure 5.4: Alert analysis

PAM: Login session closed: 10 events Monitoring the closure of login sessions confirms that every single session is correctly closed, minimizing the risk of unauthorized access.

  - The time is May 21, 2024, at 04:23:45.606.
  - On May 21, 2024, at 04:17:45.478 21 May 2024 at 04:11:44.914 As a result of a new port being either opened or closed, this warning shows that the state of listened ports has changed.
  - Grade: 7
  - ID of the Rule: 533
    The significance of frequent port status changes is that they may signal network scanning activity or configuration modifications, which could be signs of more focused attacks.

Time	Description	Level	Rule ID
May 21, 2024 @ 04:24:35.606	Listened ports status (netstat) changed (new port opened or closed)	7	533
May 21, 2024 @ 04:17:45.478	Listened ports status (netstat) changed (new port opened or closed)	7	533
May 21, 2024 @ 04:16:41.914	Listened ports status (netstat) changed (new port opened or closed)	7	533
May 21, 2024 @ 04:01:56.182	sshd: connection reset	4	5782
May 21, 2024 @ 04:01:56.179	sshd: connection reset by peer	4	5740
May 21, 2024 @ 04:01:56.177	sshd: connection reset	4	5782

Table 5.3: Port Status and Connection Alerts

Analyses: It indicates that there were multiple attempts to either open or close ports based on all three notifications that were sent out in 12 minutes. This can be part of an attacker's attempt to discover open ports and services that are operating on the system through network reconnaissance **Suggestions:** Verify that the firewall is configured properly to avoid unauthorized port access. To spot odd trends, keep an eye on and record any port changes.

- SSHD Connection Reset Alert

  Time: 04:01:56. 182 on May 21, 2024 2024 May 21 at 04:01:56.179 21 May 2024 at 04:01:56.177
  These alerts show the SSH connection was restarted, possibly as a result of a mistake or a deliberate action.
  Level: Four IDs for rules: 5740 and 5762
  Impacts Rebooting connections frequently may be a sign of ongoing SSH brute-force attacks. Password-guessing machines are probably being utilized by attackers, leading to multiple connection resets.

Three connection reset events occurred in a single second, as shown by the alerts at 04:01:56. The pattern of clustering points to a brute-force attack in which the attacker is quickly attempting several credentials.

Suggestions: Placing a speed limiter in place for SSH login tries to impede brute-force assaults.To add even more protection, make multi-factor authentication (MFA) mandatory.

5.4 Alert Summary

The table illustrates multiple different alarm types that were recently stimulated, together with details on how severe they are and how often they have been activated.
The most common warnings are:

Rule ID	Description	Level	Count
550	Integrity checksum changed.	7	180
554	File added to the system.	5	44
2904	Dpkg (Debian Package) half configured.	7	18
2902	New dpkg (Debian Package) installed.	7	17
5501	PAM: Login session opened.	3	14
5710	sshd: Attempt to login using a non-existent user	5	12
5502	PAM: Login session closed.	3	10
2901	New dpkg (Debian Package) requested to install.	3	8
533	Listened ports status (netstat) changed (new port opened or closed).	7	7
5402	Successful sudo to ROOT executed.	3	7
510	Host-based anomaly detection event (rootcheck).	7	6
52002	Apparmor DENIED.	3	4
5403	First time user executed sudo.	5	3
5503	PAM: User login failed.	5	3
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure /tmp is a separate partition.	7	2

Table 5.4: Alert Summary

- **Rule ID 550 — Integrity checksum changes (180 counts)**: This means that many changed files or system components have been updated; this could be through the intervention of an authorized party.
- **Rule ID 554 - File additions:** 44 instances of Rule ID 554 were present, which implies that new files had been loaded into the operating system. Because of either its tendency to be installed legally, or for unknown files getting added (which may pose a security risk).
- **Debian Package Changes (Rule IDs 2904, 2902, 2901)**: 43 counts in total for Debian Package Changes. This is normal behavior in Debian-based distributions, but it could also be an indication of suspect software being added.
- **Login Activities (Rule IDs 5501, 5502, 5503):**Shows login sessions opening and closing along with failures which could be user access attempts or brute force attacks.
- **Anomaly Detection Access Violations (Rule IDs 510,52002)**: There are multiple anomalies and access denials. Two of the events are AppArmor DENIED(4 counts) as well as a host-based anomaly detection event suggesting some set security policies were enforced and could have blocked nefarious actions.
- **Root and Sudo Access (Rule IDs 5402, 5403)**:It gave information on sudo access such as first-time sudo executions along with successful changes over to root

actions of which there were a total of ten counts. These are important touch points which should be tightly watched to avoid privilege escalation.

The alert summary is indicative of high system activity that includes a blend of typical administrative activities and possible security events (e.g., integrity modifications, unsuccessful logins, as well as admittance denials). The next step is to delve deeper into the user activity and verify that this behavior accords with real use.

5.4.1 SSH attack analysis for existing infrastructure

Figure 6 demonstrates a comparative analysis of Wazuh, Splunk, and IBM QRadar in detecting SSH brute force attacks based on detection efficiency and resource performance on a proportional generic events count approach. Brute Force Detection from IBM QRadar analyzes unauthorized login attempts by examining login events, conducting statistical analysis, and generating multi-layered user profiles **ibm**.

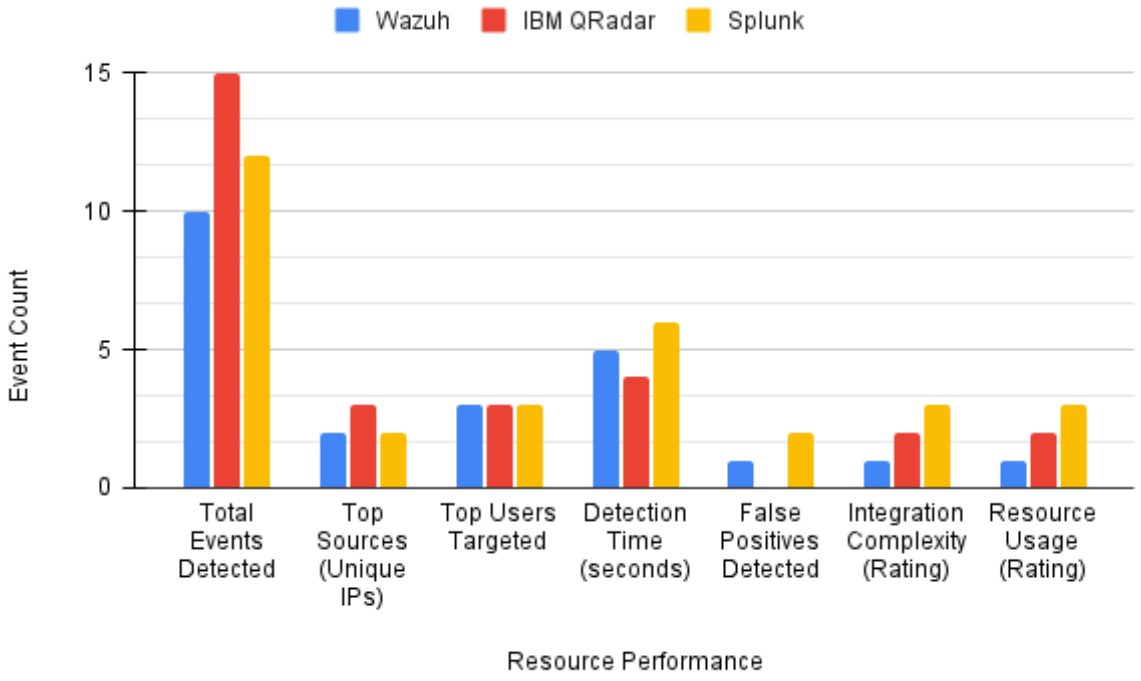

Figure 5.5: SSH attack analysis for existing infrastructure

Splunk analyzes SSH brute-force attacks by monitoring SSH logs for invalid login attempts **sp**, extracting information like attempting usernames and IP addresses, and analyzing the data regionally and in charts. IBM QRadar provides wide event detection capabilities but is frequently coupled by higher resource utilization and complexity. Splunk strikes a balance by offering strong performance throughout metrics, but at the cost of increased utilization of resources and integration complexity. Wazuh, on the other hand, provides a more focused and proportional approach, leading to higher efficiency with faster detection times, fewer false positives, and lower consumption of resources. It renders Wazuh an excellent alternative for enterprises looking for streamlined, cost-effective solutions without compromising efficiency.

Chapter 6

Conclusion and future improvement

6.1 Conclusion

This thesis has successfully displayed how Wazuh and the Elastic Stack may be combined to boost cybersecurity in the finance technology sector. The setup demonstrated that a robust safety record requires a well-coordinated cyber threat intelligence system that involves incident detection, continuous tracking, and regulatory compliance management. An operational monitoring environment was created by the process of implementation, demonstrated by the 100% active agent penetration and PCI DSS compliance. With the Wazuh-Elastic Stack integration, the warning system can identify potential security incidents and enable prompt responses to reduce risks. The present architecture provides tons of opportunities for advancement and expansion as we look to the development of cybersecurity in FinTech.

6.2 Future improvement

The inclusion of the components that follow into this cybersecurity architecture are discussed as future versions:

1. Suricata Integration: A further degree of safeguarding will be provided with the setting up of Suricata, a Network Intrusion Detection System (NIDS), which analyzes network traffic for illicit activity using an extensive array of rules and signatures.The works [21]concert with the open-source Network Intrusion Detection System (NIDS) Suricata to keep an eye on and evaluate intrusions conducted at port 80 of a web server. To evaluate how well Suricata and Wazuh operate together to detect and address these risks, the research uses network forensic approaches such as OSCAR (Objective, Systematic, Consistent, Accurate, and Reliable) and detection methodologies.

2. MISP for Threat Intelligence Sharing: The incorporation of the Malware Information Sharing Platform (MISP) would make it possible for financial institutions to communicate threat intelligence more readily, increasing situational awareness and collective defenses. The system's objectives are to ensure continuous operation, mitigate cascading effects on infrastructure, and enable coordinated identification of substantial cyber-human security and privacy events and attacks.[15]

3. TheHive for Incident Response: The combination of TheHive, a cybersecurity incident response platform, will quicken incident management protocols and help security teams to rapidly assess, inquire into, and react to risks

4. Machine Learning integration: Threat detection systems can function more effectively and precisely if machine learning approaches for anomaly detection and predictive analytics are incorporated with them [19].

5. Active response Enhancement: Increasing the level of sophistication of active response systems and their capacity to respond to emerging threats instantly strengthens organizations' security stance [25].

In the future, a symbiotic ecosystem will be developed, with Wazuh giving host-based intrusion detection, Suricata giving network-level monitoring, MISP allowing the sharing of threat intelligence, and TheHive managing the response to incidents. This integrated plan intends to deliver an entire security solution that swiftly responds to evolving vulnerabilities while offering defense against developed threats. Additionally, sustaining a lead over highly skilled hackers will require the development of automated response capabilities, machine learning models for anomaly detection, and strong correlation algorithms. The intent is to establish a proactive, open-to-change, and resilient security architecture that secures financial assets while also maintaining the anonymity and security of FinTech industry consumers.
The requirement for inventive and dynamic safety measures will surely grow as the FinTech industry expands. This thesis's work offers a base for the next inquiries and the practical use of deeper and complete cybersecurity solutions. The author intends for the results and concepts to be an important addition to the conversation surrounding cybersecurity and function as a flame for additional developments in the sector.

Bibliography

[1] Z. Affendi, "Host-based intrusion detection system (hids)," 2005, Accessed: YYYY-MM-DD. [Online]. Available: https://consensus.app/papers/hostbased-intrusion-detection-system-hids-affendi/56baa466e0a457b48eb73daba2ab4881.

[2] D. Arner, J. Barberis, and R. P. Buckley, "The emergence of regtech 2.0: From know your customer to know your data," *Monetary Economics: International Financial Flows*, 2016, Accessed: YYYY-MM-DD. DOI: 10.2139/ssrn.3044280. [Online]. Available: https://consensus.app/papers/emergence-regtech-from-know-your-customer-know-your-data-arner/798e9b3efd725d918edd139ace6e44c6.

[3] M. Moh, S. Pininti, S. Doddapaneni, and T. Moh, "Detecting web attacks using multi-stage log analysis," in *6th IEEE International Conference on Advanced Computing*, 2016. DOI: 10.1109/IACC.2016.141.

[4] S. Samtani, R. Chinn, H. Chen, and J. F. Nunamaker Jr, "Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence," *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1023–1053, 2017.

[5] A. Alekseev, F. G. Barreiro Megino, A. Klimentov, T. Korchuganova, T. Maendo, and S. Padolski, "Building analytical platform with big data solutions for log files of panda infrastructure," *Journal of Physics: Conference Series*, vol. 1015, 2018. DOI: 10.1088/1742-6596/1015/3/032003. [Online]. Available: https://consensus.app/papers/building-platform-data-solutions-files-panda-alekseev/0dc5093f39a95b6e9089fea8f223c79e.

[6] L. F. Bernardo, "Targeted attack detection by means of free and open source solutions," Ph.D. dissertation, MSc Thesis. Jan. 7, 2019.(Visited on 01/10/2021), 2018.

[7] N. Arnold, M. Ebrahimi, N. Zhang, *et al.*, "Dark-net ecosystem cyber-threat intelligence (cti) tool," in *2019 IEEE*, Jul. 2019.

[8] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, and A. Zajić, "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals," *Journal of Hardware and Systems Security*, vol. 3, pp. 305–318, 2019.

[9] D. Bhatnagar, R. Subalakshmi, and V. C, "Twitter sentiment analysis using elasticsearch, logstash and kibana," *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pp. 1–5, 2020. DOI: 10.1109/ic-ETITE47903.2020.351.

[10] D. Bhatnagar, R. J. SubaLakshmi, and C. Vanmathi, "Twitter sentiment analysis using elasticsearch, logstash and kibana," in *2020 international conference on emerging trends in information technology and engineering (ic-ETITE)*, IEEE, 2020, pp. 1–5.

[11] K. Fotiadou, T. H. Velivassaki, A. Voulkidis, K. Railis, P. Trakadas, and T. Zahariadis, "Incidents information sharing platform for distributed attack detection," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 593–605, 2020.

[12] O. Negoita and M. Carabas, "Enhanced security using elasticsearch and machine learning," in *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, Springer, 2020, pp. 244–254.

[13] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani, A. Hosseinian-Far, and A. Daneshkhah, "Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*. 2021, pp. 47–64.

[14] R. M. Muhammad, I. D. Irawati, and M. Iqbal, "Integrated security system implementation for network intrusion," *Journal of Hunan University Natural Sciences*, vol. 48, no. 6, 2021.

[15] D. Skias, S. Tsekeridou, T. Zahariadis, A. C. Voulkidis, T. Velivassaki, and K. Fotiadou, "Pan-european cybersecurity incidents information sharing platform to support nis directive," *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021. DOI: 10.1145/3465481.3470477.

[16] D. Turcanu, N. Spinu, S. Popovici, and T. Ţurcanu, "Cybersecurity of the republic of moldova: A retrospective for the period 2015-2020," *Journal of Social Sciences*, 2021. DOI: 10.52326/JSS.UTM.2021.4(1).10.

[17] G. I. Enache, "Formulas for counteracting cyber threats in regards to computer products supply chains," *Proceedings of the International Conference on Business Excellence*, vol. 16, pp. 1420–1428, 2022. DOI: 10.2478/picbe-2022-0129.

[18] H. Haugerud, M. Sobhie, and A. Yazidi, "Tuning of elasticsearch configuration: Parameter optimization through simultaneous perturbation stochastic approximation," *Frontiers in Big Data*, vol. 5, 2022. DOI: 10.3389/fdata.2022.686416.

[19] M. A. Hussein and E. K. Hamza, "Secure mechanism applied to big data for iiot by using security event and information management system (siem).," *International Journal of Intelligent Engineering & Systems*, vol. 15, no. 6, 2022.

[20] S. Stanković, S. Gajin, and R. Petrović, "A review of wazuh tool capabilities for detecting attacks based on log analysis," *No Nama Agent Integrity File Added Delete Modified*, vol. 1, 2022.

[21] T. Suryantoro, B. Purnomosidi, and W. Andriyani, "The analysis of attacks against port 80 webserver with siem wazuh using detection and oscar methods," *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 1–6, 2022. DOI: 10.1109/ISRITI56927.2022.10052950.

[22] *Wazuh documentation: Regulatory compliance*, https://documentation.wazuh.com/current/getting-started/usecases/regulatory-compliance.html, Last visited on April 29, 2022, 2022.

[23] A. Willerton and R. Gustafsson, *Evaluating the efficiency of host-based intrusion detection systems protecting web applications*, 2022.

[24] H. Zahid, S. Hina, M. F. Hayat, and G. A. Shah, "Agentless approach for security information and event management in industrial iot," *Electronics*, vol. 12, no. 8, p. 1831, 2023.

[25] F. I. F. Farrel, I. Mardianto, M. Kom, and M. Ir Adrian Sjamsul Qamar, "Implementation of security information & event management (siem) wazuh with active response and telegram notification for mitigating brute force attacks on the gt-i2ti usakti information system," *Intelmatics*, vol. 4, no. 1, pp. 1–7, 2024.

[26] Red Canary, *Atomic-red-team*, Accessed: 2024-01-15, 2024. [Online]. Available: https://github.com/redcanaryco/atomic-red-team.