National College of Ireland

Cyber-attack detection and response using open-source tools

MSc Research Project
Cybersecurity

Vanessa Pereira
Student ID: x21179875

School of Computing
National College of Ireland

Supervisor: Evgeniia Jayasekera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Vanessa Pereira
Student ID:	X21179875
Programme:	MSc Cyber Security **Year:** 2022-2023
Module:	Research Project
Supervisor:	Evgeniia Jayasekera
Submission Due Date:	18th September 2023
Project Title:	Cyber Attack Detection and Response using open source tools
Word Count:	6293 **Page Count** 18

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

Signature:	Vanessa Pereira
Date:	15th September 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

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

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

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

Cyber-attack detection and response using open source tools

Vanessa Pereira
X21179875
Master of Science in Cyber Security
National College of Ireland

Abstract

Strong and effective cybersecurity measures are now essential, especially for Small and Medium Enterprises (SMEs) with limited resources as the frequency and sophistication of cyberattacks continue to rise. This study attempts to determine the degree to which SMEs' capacity for cyber-attack detection and response may be improved by integrating open-source tools such the Wazuh, MISP (Malware Information Sharing Platform), TheHive and Cortex. The study will conduct a thorough literature analysis using a mixed-methods approach to identify research gaps and evaluate the effectiveness of the various tools. A realistic experimental setup will then be created to model various cyber-attack situations, and data will be gathered and examined. The study seeks to offer insightful information about the possible advantages of these integrated open-source tools, advancing cybersecurity practices in SMEs and boosting their resistance to online attacks. In the end, this research intends to equip SMEs with the tools they need to strengthen their cyber resilience and safeguard their vital assets from the always changing threat landscape.

Keywords: Open source, Security Operations Center, Incident Response

1. Introduction

People are more connected than ever thanks to technology breakthroughs. Smartphones and other smart home gadgets are now an essential part of daily life for both individuals and companies. The repercussions of incorporating technology into core business processes, however, are not well understood by many people and organizations, leaving a vulnerable attack surface that could be exploited and potentially result in the whole destruction of an organization. Because they have less financial resources and cybersecurity expertise, small firms are particularly vulnerable to cyberattacks (Worldpay editorial team, 2019). 43% of cyberattacks target small and medium-sized businesses, according to statistics from Verizon (Verizon, n.d.), and 60% of small businesses that are the victims of cyberattacks fail within six months (Johnson III, 2019). These concerning numbers are made even more concerning by the high average cost of a cyberattack, which is around $4.35 million (Tunggal, 2023).

The sophistication of current cyberattacks has rendered conventional security methods ineffective. A Security Operations Center (SOC) is the foundation of any strong cybersecurity defense. The SOC team serves as the central entity in charge of keeping track of the logs from various devices connected to the organization's network. In order to confirm the validity of triggered warnings, their main responsibility is to spot anomalies and perform thorough studies. This procedure frequently entails analyzing many notifications and applying various technologies to check their accuracy. In order to effectively detect and respond to cyber-attacks, there is a rising need for advanced technologies and procedures. In order to identify and respond

to host-targeting cyberattacks, this paper offers a unique system that makes use of Wazuh, MISP, TheHive, Cortex, and Shuffle.

Wazuh is an open-source security monitoring platform that offers security event correlation, log analysis, intrusion detection, and file integrity monitoring. It is intended to assist organizations in successfully detecting and responding to security threats. Based on the popular host-based intrusion detection system (HIDS) OSSEC, Wazuh enhances OSSEC's functionality by include features like centralized management, a better web interface, and support for various integrations (Wazuh, 2023). The Wazuh's components integrated are:

- Wazuh-Manager: The main element in charge of gathering and examining security-related data from multiple sources, such as agents, syslog, and logs from cloud platforms is the Wazuh-Manager.
- Wazuh Agents: Wazuh Agents are little pieces of software that are installed on the monitored endpoints, like computers, servers, and cloud instances.
- Wazuh-indexer: The data gathered by Wazuh agents and other integrated sources must be received, stored, and indexed by the Wazuh Indexer.
- Fluent-Bit: Wazuh collaborates with Fluent Bit, a compact and effective log collector and forwarder. It is used to collect log information from multiple sources on the monitored endpoints and send it to the Wazuh-Manager or Graylog.
- Graylog: Graylog is a platform for centralized log management that makes it easier to gather, process, and store log data. Graylog can replace the Wazuh-Manager and Indexer when it is linked with Wazuh, offering more flexibility and scalability for managing massive amounts of log data.

The acronym **MISP** stands for "Malware Information Sharing Platform & Threat Sharing." It is an open-source threat intelligence platform created to make it easier for cybersecurity experts and businesses to share structured threat information. MISP makes it possible to gather, store, and disseminate indicators of compromise (IOCs) like malicious IP addresses, domain names, URLs, file hashes, and other artifacts connected to cybersecurity concerns (CIRCL, n.d.). **TheHive** is an open-source security incident response tool that makes it easier to handle and look into cybersecurity problems. It acts as a focal point where security teams may come together to collaborate on problems, monitor development, and plan responses. **Cortex** is an open-source automation and analysis tool. It serves as a platform for threat intelligence enrichment and intelligent response. Cortex automates the enrichment and analysis of observables related to occurrences in TheHive by integrating with numerous other tools, sandboxes, and threat intelligence sources (Leonard, 2017).

Shuffle is an effective tool made for designing and implementing workflows that support automation and lessen the strain of excessive effort. The combination of these open-source tools presents intriguing opportunities for enhancing cybersecurity defenses and streamlining incident response in situations with limited resources. SMEs may be able to detect and mitigate security attacks more effectively by utilizing the capabilities of these products (Frikky, 2020).

The suggested solution significantly adds to the pool of knowledge in the realm of cybersecurity. By incorporating powerful technologies, it addresses important issues in cyberattack detection and response. A complete and efficient system is created by combining Wazuh as a SIEM tool, MISP for exchanging threat intelligence, TheHive for collaborative incident response, and Cortex for automated threat analysis. The proposed method improves the effectiveness and speed of cyberattack detection, narrowing the window for successful attacks. In order to quickly mitigate possible risks, real-time log analysis, fast threat

intelligence exchange, and automated reaction capabilities are essential. Additionally, the suggested strategy offers both small and large businesses affordable security options. Businesses can streamline their cybersecurity operations without compromising security requirements by utilizing open-source tools to set up a security operation center (SOC). With this economical strategy, a strong defense against online threats is guaranteed while spending on cybersecurity operations is kept to a minimum. Overall, this research offers insightful knowledge and useful applications that can considerably improve cybersecurity processes.

Research Question. To what extent does the integration of Wazuh, MISP, TheHive, Cortex and Shuffle enhance the response time to security attacks in Small and Medium Enterprises?

The research report follows a prescribed format, starting with a literature review to contextualize and support the significance of the study issue. The research methodology section describes the strategy used for data collecting and analysis, while the design specification describes the architecture and specifications of the suggested solution. The last stage of the implementation process is discussed in the implementation part, and a thorough analysis of the outcomes is presented in the evaluation section. A thorough analysis of the results and their implications is provided in the discussion section. The report ends by summarizing the important findings and contributions made by the research and making insightful recommendations for future work.

2. Related Work

The escalating frequency and complexity of cyber security threats have spurred the need for a sophisticated solution that can swiftly detect and respond to potential attacks. There has been a fair amount of research conducted on the challenges the Security team in an organization faces and what can be done to improve the attack detection and response process. Elradi et al., (2021) delves into the intricate challenges confronting cybersecurity experts and propose an integrated platform solution to address these issues. The suggested platform encompasses a Security Information and Event Management (SIEM) system, a Threat Intelligence Platform (TIP), and a Security Orchestration, Automation, and Response (SOAR) platform. This fusion of methodologies and technologies makes it possible to recognize, respond to, and mitigate security events more quickly and effectively. Furthermore, the research conducted by Gibadullin and Nikonorov (2021) shows how the use of open-source system for automating incident management can minimize response times, decrease reliance on specialized personnel, and enhance process automation in incident management, by implementing a fault-tolerant operational scheme and a distributed, federated architecture.

In this report, a literature review is conducted to understand the various tools available and how integrating the tools can add value to the threat detection and response process. The literature review was carried out based the functionality of various tools and how they fit into the architecture. This was divided into various parts like identifying the SIEM solution for log monitoring and alerting, choosing an incident management solution that can help security teams to collaborate on the incidents and assign tasks for taking actions, finding a threat intelligence solution that can provide feeds for enriching the information gathered and finally identifying a tool for analyzing the indicators of compromise (eg. IP, Domain, Hash, etc). A further literature review provides insights on the features of the tools, various attack scenarios for detection, and challenges of the tools. Most of these papers talk about usage of tools in terms of either detection or in terms of response. The problem faced by security teams is the lack of an integrated solution that helps them to effectively detect and respond to threats.

Security teams have to rely on multiple tools which causes delays in effectively mitigating the attacks.

2.1. Choosing the SIEM tool

In 2022, Tariq et al., conducted a comprehensive comparative analysis of well-known open source SIEM solutions for small-to-medium-sized enterprises (SMEs). It contains mapping of the security requirements of SMEs against the capabilities of various open source SIEM solutions, providing meaningful insights and recommendations for SMEs to choose suitable SIEM systems. The paper highlights mandatory, basic, and advanced features of SIEM systems, such as log management, correlation engine detection, visualization tools, asset discovery, alerting, and reporting. This has helped in finalizing Wazuh as the SIEM tools for log monitoring and alerting.

2.2. Enhancing Attack Detection

Wazuh tool, a Host Intrusion Detection System, can be used to detect and prevent attacks on web servers. In 2022, Stanković et al., discusses Wazuh's capabilities, including security analytics, intrusion detection, log data analysis, and vulnerability detection. Wazuh is capable of detecting some of the well-known attacks on web servers, in particular the SSH brute force attack. Wazuh can monitor security events, integrity changes, policy compliance, and threat detection. Here the focus is on attack detection and not the response.

2.3. Holistic Network Security

Muhammad et al. (2021) present an integrated network security system for local environments using Wazuh, Dionaea honeypot, and Cuckoo Sandbox. Their research emphasizes the detection and mitigation of various attacks, shedding light on strategies to bolster SME security. Meanwhile, Suryantoro et al. (2013) expose the vulnerabilities associated with port 80, introducing OSCAR (Obtain Information, Strategies, Collect Evidence, Analyze and Report) methodology and emphasizing on SIEM solutions like Wazuh for cyber threat detection. This section explores these contributions and investigates potential avenues for integrating Wazuh into broader security frameworks. Although emphasizing SIEM solutions like Wazuh, integration nuances aren't explored.

2.4. Orchestrating Threat Intelligence with Integration

Srivastava et al. (2018) review malware detection, proposing an approach using online platforms and behavior analysis. Integration specifics are absent. Oujezsky et al. (2022) propose an automated incident response system for xPON networks, emphasizing TheHive's integration benefits. Groenewegen & Janssen (2021) evaluate TheHive's maturity and contributes to understanding incident response platforms, suggesting integration and automation improvements using tools like Shuffle. Preuveneers & Joosen (2021) propose a threat intelligence solution using MISP, TheHive, and Cortex, lacking integration details. Galdi et al. (2022) introduces a solution named ThePhish, which aims to enhance the efficiency of phishing email analysis using open-source tools like TheHive, Cortex, and MISP. It leverages TheHive for case management, Cortex for running analyzers on observables, and MISP for threat intelligence sharing. The integration of these tools offers a comprehensive solution for handling phishing incidents in Small and Medium Enterprises (SMEs). These papers helped to understand the functioning of TheHive, Cortex and MISP tools and identify various usecases on how the tools can be used to create the architecture.

2.5. Summary

The research available so far emphasizes how crucial it is to detect and handle cybersecurity incidents effectively. While previous solutions have been helpful, there are still gaps in putting together different security tools and methods to create a strong overall security system. We need a complete approach that combines tools like SIEM, SOAR, threat intelligence, and automated incident management to improve how we deal with cybersecurity issues. This research aims to fill these gaps by suggesting a combined framework that makes managing incidents better and boosts overall cybersecurity.

From what we've seen in previous research, we know that tools like Wazuh can be used to monitor logs. Some studies also show how MISP, TheHive, and Cortex can be used for things like managing incidents, understanding cyber threats, and responding to cyberattacks automatically. Even though there's been a lot of research on different ways to stay secure online, there hasn't been much on how well tools like Wazuh, MISP, TheHive, Cortex, and Shuffle work together to stop cyberattacks.

So, this research plans to come up with a new system that can find and fight against cyberattacks, and then test how well it works for making small and medium-sized businesses more secure. The exciting thing is that this study will offer businesses a way to strengthen their cybersecurity defenses and respond faster to online threats.

SIEM - Security Incident and Event Management (Wazuh)
IM - Incident Management (TheHive)
IAR - Incident Analysis and Response (Cortex)
CTI - Cyber Threat Intelligence (MISP)
SOAR - Security Orchestration, Automation, and Response (Shuffle)

Survey Paper	Publication Year	Key Problem	SIEM	IM	IAR	CTI	SOAR
Elradi et al., 2021	2021	Presents a literature on solutions that helps overcome challenges for Cybersecurity professionals.	Y	N	N	Y	Y
Gibadullin and Nikonorov, 2021	2021	Presents the use of SOAR and automating incident response.	N	Y	N	N	Y
Tariq et al., 2022	2022	Presents a comparative analysis of the the SIEM solutions available.	Y	N	N	N	N
Stanković et al., 2022	2022	Presents Wazuh tools capabilities for detecting attacks on webservers	Y	N	N	N	N
Muhammad et al., 2021	2021	Presents an integrated network security system for local environments.	Y	N	N	N	N
Suryantoro et al., 2022	2022	Presents a network forensic approach to assess the effectiveness of SIEM Wazuh in detecting port 80 attacks on web servers.	Y	N	N	N	N
Srivastava et al., 2018	2018	Presents a solution that detects malware using MISP and behaviour-base analysis.	N	N	N	Y	N
Oujezsky et al., 2022	2022	Presents a system for automated reporting using TheHive, MISP and Cortex.	N	Y	Y	Y	N
Groenewegen and Janssen, 2021	2021	Presents the maturity of TheHive as a security incident response platform.	N	Y	Y	Y	N
Preuveneers and Joosen, 2021	2021	Presents cyber-threat intelligence solution using machine learning models and using open source tools to improve accuracy.	N	Y	Y	Y	N
Galdi et al., 2022	2022	Presents a framework for Phishing attack detection using ThePhish and use TheHive, Cortex and MISP to automate the analysis.	N	Y	Y	Y	N
This Article	-	Presents a solution that is created using open-source tools for Log Monitoring (SIEM - Wazuh), Incident Management (TheHive), Analysis (Cortex), Threat Intelligence (MISP) and Automated Response (SOAR - Shuffle) .	Y	Y	Y	Y	Y

3. Research Methodology

This section outlines the research methodology employed to achieve the objectives of the study, including the research procedure, equipment used, techniques applied, setup of scenarios/case studies, data collection, analysis, and statistical techniques used.

Research Procedure:

1. **Literature Review:** A thorough review of existing literature and related work on cybersecurity tools, incident response, and threat detection was conducted. This helped in understanding the tools and techniques commonly used in the field.
2. **Tool Selection:** The decision to use Wazuh, TheHive, Cortex, MISP, Shuffle, and other tools was based on the analysis of their capabilities and compatibility with the research objectives.
3. **System Setup and Configuration:**
    - Virtualized environment using VirtualBox VMs.
    - Four VMs: Wazuh, MISP, TheHive Cortex, and Shuffle.
    - Each VM has specified memory, storage, and CPU configuration running Ubuntu 22.04.
    - Apache webserver and DVWA set up on Shuffle VM (digininja, n.d.).
    - Wazuh agent installed on Shuffle VM.
    - Teler (HTTP IDS) integrated with Apache on Shuffle VM (Obahor, 2022).
    - Install and configure the required software components (Java, Cassandra, Elasticsearch, TheHive, Cortex, MISP, and Shuffle) as outlined in the provided configuration details.

	Memory (RAM)	Storage (HDD)	CPU	Operating System
Wazuh	8 GB	50 GB	2	Ubuntu 22.04
MISP	2 GB	25 GB	1	Ubuntu 22.04
TheHive / Cortex	4 GB	50 GB	2	Ubuntu 22.04
Shuffle/ Apache Webserver	6 GB	50 GB	2	Ubuntu 22.04

4. **Teler Configuration:**
    - Download and extract teler binary.
    - Download sample configuration file teler.example.yaml and rename to teler.yaml.
    - Modify log_format parameter in teler.yaml for Apache logs.
    - Configure logs parameter for logging and path for teler logs.
    - Add teler configuration block to Wazuh agent configuration.
5. **Wazuh Configuration:**
    - Add custom rules to local_rules.xml for teler alerts.
    - Restart Wazuh-Manager.
    - Use Nikto to emulate an attack against the DVWA.
6. **Wazuh Indexer and Dashboard Installation:**
    - Install Wazuh Indexer with specified memory settings and SSL configurations.
    - Deploy certificates for encryption and security.
    - Configure network and SSL settings in Wazuh Indexer.
    - Install and configure Wazuh Dashboard.
    - Secure the cluster by updating passwords and certificates.
7. **Graylog Installation and Integration:**
    - Install MongoDB for Graylog.
    - Install Graylog 5.x.
    - Configure Graylog with necessary parameters.
    - Configure Graylog to connect to Wazuh-Indexer.

- Set up input for Wazuh alerts.
- Install Fluent Bit to collect and forward Wazuh alerts.
- Configure Fluent Bit to read alerts.json and send to Graylog input.

8. **Techniques Applied:**
   - **Installation and Configuration:** The tools were installed and configure the tools to work together in a predefined workflow for incident detection and response.
   - **API Key Setup:** API keys and authentication tokens were generated and configured for seamless communication between tools.
   - **Automated Analysis:** Utilize Cortex to automatically analyze artifacts and gather reputation reports for observables.
   - **Workflow Automation:** Use Shuffle to automate the incident detection and response workflow triggered by Wazuh alerts.
9. **Scenario Setup and Case Studies:**
   - **Wazuh Alert Processing:** A scenario was set up to simulate the generation of alerts by the Wazuh-Manager. These alerts were processed through the configured Shuffle workflow.
   - **TheHive and Cortex Integration:** TheHive and Cortex were integrated to automate the incident response process. Cases were created in TheHive based on incoming alerts, and Cortex was used to run analyzers on artifacts.
   - **MISP Integration:** MISP was integrated with Cortex and other tools to enhance threat intelligence sharing and analysis.

Data Collection:

1. Data collected includes:
   - Logs generated by teler for Apache webserver.
   - Wazuh alerts triggered by teler.
   - Wazuh alerts forwarded to Graylog.
   - Log data from the emulation of attacks using Nikto.
   - Simulate SSH failed login on the webserver.

Workflow Definition:

1. Define the incident detection and response workflow using the integrated tools (TheHive, Cortex, MISP, and Shuffle). Specify how alerts are processed and escalated through the tools.

Data Analysis:

1. **Manual Workflow Analysis:** Here incidents are identified, reported, and analyzed using a manual approach. The following steps are taken:
   - **Incident Identification:** Alerts are manually identified by security personnel through continuous monitoring of incoming data.
   - **Case Creation:** Incidents are manually raised as cases in TheHive platform, detailing the alert information.
   - **Manual Analysis:** Analysts manually perform analysis on the incidents using Cortex and MISP, collecting and correlating threat intelligence data.
   - **Response:** Based on the analysis, security personnel manually devise and execute response strategies.
2. **Automated Workflow Analysis:** Here incidents are detected, reported, and analyzed automatically through integrated tools. The following steps are taken:

- **Automated Detection:** Alerts are automatically generated by the integrated tools based on predefined rules and threat intelligence feeds.
- **Case Automation:** Incidents are automatically raised as cases in TheHive, including relevant alert information.
- **Automated Analysis:** Cortex and MISP automatically perform analysis on the incidents, leveraging threat intelligence data and predefined workflows.
- **Automated Response:** Automated response actions are executed based on predefined playbooks and response strategies.

Evaluation Methodology:
To evaluate the effectiveness of the configured security environment:

- Assess the ability of Wazuh to detect and respond to the alerts triggered.
- Analyze the correlation and response time for detected attacks.
- Comparison between the manual and automated analysis.
- The performance of the solution is assessed in terms of improved cyber-attack detection, reduced response time, enhanced incident analysis, and effective workflow automation.

Conclusion:
This research methodology outlines the step-by-step process used to set up a security environment, generate data, analyze logs, and evaluate the capabilities of the integrated tools. By following this procedure, the research aims to provide insights into the effectiveness of the configured system in detecting and responding to potential cyber threats.

4. Design Specification

4.1. Overview

The design specification outlines the techniques, architecture, and framework underlying the implementation of the integrated incident detection and response system. It also presents the associated requirements and, where applicable, describes the functionality of the proposed model.

4.2. Architecture

The integrated incident detection and response system is designed as a multi-tool environment, incorporating Wazuh, TheHive, Cortex, MISP, and Shuffle, along with supporting components such as MongoDB, Java, Cassandra, and Elasticsearch. The architecture follows a modular approach, allowing seamless integration between these tools to facilitate efficient incident response.

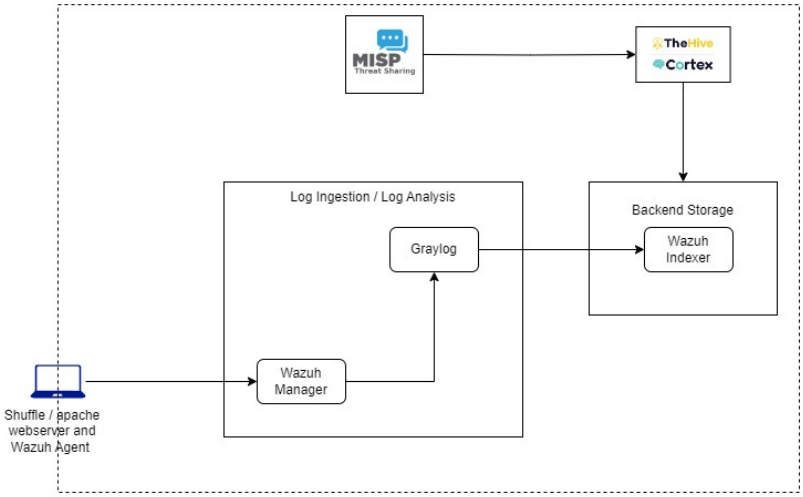

Figure 1: Architecture Diagram

4.2.1. Components and Integration

1. **Wazuh Indexer:**
   - It is responsible for storing all our security events. This is our backend storage.
   - It stores logs for a particular timeframe making it easier for our analyst to search for logs within the desired timeframe.
   - In this architecture a 1 node cluster is deployed however more nodes can be added for higher availability.
2. **Graylog:**
   - It is responsible for collecting logs from our network devices and endpoints.
   - Along with log ingestion it also helps in normalization and enrichment.
   - It also helps in caching logs incase the indexer is down.
3. **Fluent-bit:**
   - Will grab the logs from the Wazuh-Manager in json format and ship it to the listening input of the graylog.
4. **MongoDB:**
   - It holds the configuration data of graylog.
5. **Wazuh-Agents:**
   - It collects logs from endpoints and sends to Wazuh-Manager. It is very light-weight.
   - Also it does file integrity monitoring, vulnerability scanning, etc.
   - When it first starts it will register with the manager on port 1515. The manager will generate a client key, which is a symmetric key.
   - Both the client and manager will keep a copy of this key which will be used to encrypt and decrypt the traffic between the endpoints and the manager.
   - The logs will be sent over port 1514 to the Wazuh-Manager.
6. **Wazuh-Manager:**
   - Allows us to collect logs and ingest them from any log sources along with providing us full visibility to our endpoints.
   - Every time wazuh receives a log and wants to save it, it will write it to alerts.json file.
   - This file is then sent by fluent-bit to graylog for further analysis and to write it to the wazuh-indexer. Wazuh-Agent and Wazuh-Manager allows to collect logs from devices at scale.
7. **Packetbeat:**
   - It helps analyse network traffic from Linux hosts in real time

8. **TheHive:**
    - Serves as the central platform for case management, alert aggregation, and collaboration among analysts.
    - Integrates with Cortex for automated analysis and response actions.
    - Communicates with MISP for threat intelligence sharing.
9. **Cortex:**
    - Provides automated artifact analysis using various analyzers, enhancing incident investigation. Analyzers for Virustotal, AbuseIPDB and MISP are integrated that help with analysis (AbuseIPDB, n.d.) (VirusTotal, n.d.).
    - Receives alerts from TheHive, runs analyzers, and returns reputation reports to TheHive.
10. **MISP:**
    - Offers a threat intelligence platform for sharing indicators of compromise (IOCs) and contextual information.
    - Integrates with TheHive and Cortex to enrich alerts with threat intelligence data.
11. **Shuffle:**
    - Orchestrates the incident response workflow triggered by Wazuh alerts.
    - Integrates Wazuh with TheHive to automate the escalation and response process.

4.3. Techniques

4.3.1. Workflow Automation

Shuffle is employed to automate the incident response workflow upon Wazuh alerts. The system listens for incoming alerts, processes them, and triggers predefined actions through TheHive and other integrated tools. This technique ensures swift and consistent incident handling.

4.3.2. Automated Analysis

Cortex utilizes various analyzers to automatically analyze artifacts, such as IP addresses, domains, or file hashes. This technique enhances the accuracy and speed of incident investigation by providing analysts with reputation reports and contextual information.

4.4. Proposed Model

Automated Workflow Execution:

1. Upon receiving a Wazuh alert, Shuffle initiates the workflow in TheHive.
2. TheHive triggers automated actions, such as creating a case and adding observables to the case.
3. A notification is sent to Microsoft teams channel.
4. Cortex is invoked to analyze artifacts associated with the alert.
5. Cortex runs analyzers and returns reputation reports to TheHive.
6. TheHive enriches the alert with threat intelligence from MISP.
7. Analysts review the enriched alert, investigate artifacts, and execute necessary response actions.
8. TheHive updates the case with analysis results, facilitating informed decision-making.

4.5. Requirements

1. **Software Requirements:**
    - Java Virtual Machine for running TheHive and Cortex.
    - Apache Cassandra as the scalable database for TheHive.
    - Elasticsearch for Cortex's indexing and search capabilities.

    - TheHive and Cortex for incident case management and automated analysis.
    - MISP for threat intelligence sharing and enrichment.
    - Shuffle for workflow automation triggered by Wazuh alerts.
2. **Integration Requirements:**
    - Proper configuration of TheHive, Cortex, MISP, and Shuffle to enable seamless communication.
    - API keys for authentication and authorization between tools.
    - Connectivity between tools for real-time data exchange.
3. **Functionality Requirements:**
    - TheHive should be able to create and manage incident cases, assign tasks, and enrich alerts with threat intelligence.
    - Cortex should run analyzers on artifacts, generate reputation reports, and communicate with TheHive.
    - MISP integration should allow enrichment of alerts with contextual threat intelligence.
    - Shuffle should listen for Wazuh alerts, trigger the predefined workflow, and execute automated response actions.
4. **Performance Requirements:**
    - The system should process alerts and trigger responses within an acceptable time frame.
    - Cortex's analyzers should provide accurate and timely reputation reports.
    - Workflow automation using Shuffle should operate reliably and efficiently.

5. Implementation

The implementation of the proposed incident detection and response system involves several stages, from setting up the required components to configuring integrations and orchestrating incident response workflows. In this section, the final stage of the implementation is described, focusing on the outputs produced, tools used, and key actions taken.

5.1. Incident Investigation and Response Workflow

The final stage of the implementation focuses on demonstrating the incident investigation and response workflow using TheHive and Cortex. This stage involves the following key steps:

1. **Alert Generation:** The incident detection system (Wazuh) monitors the Teler-generated logs and triggers alerts based on predefined rules. These alerts are related to potential web attacks detected in the Apache web server logs.
2. **Alert Forwarding:** The generated alerts are forwarded from Wazuh to Graylog. Fluent Bit plays a crucial role in collecting the Wazuh alerts and forwarding them to the Graylog server.
3. **Graylog Processing:** Graylog processes the incoming Wazuh alerts and stores them in the Wazuh-Indexer. The processed alerts are then made available for further analysis and investigation.
4. **Incident Creation:** Using TheHive's integration with Shuffle, triggered Wazuh alerts are automatically transformed into incidents in TheHive. These incidents represent potential security threats that require investigation.
5. **Automated Analysis:** Shuffle triggers Cortex analyzers to perform automated analysis on the incidents. Cortex analyzers are pre-configured tools that gather additional information and context about the incidents from various external sources.

6. **Collaborative Investigation:** Incident handlers (security analysts) use TheHive's collaborative workspace to investigate the incidents. They can add notes, tasks, and tags to the incidents, and collaborate with other team members in real-time.
7. **Manual Analysis:** While Cortex performs automated analysis, analysts can also perform manual analysis by reviewing the gathered information, logs, and context. This helps in making informed decisions about the severity and nature of the incidents.
8. **Incident Triage:** Based on the analysis, incidents are triaged to determine their criticality and potential impact. High-priority incidents may require immediate response actions, while others can be categorized for further monitoring or mitigation.
9. **Integrations:**
    - Cortex is integrated with TheHive for automated analysis of incidents.
    - TheHive is integrated with Microsoft Teams to notify the team about incidents.
    - TheHive is integrated with Cortex and MISP for further analysis and artifact enrichment.
10. **Workflow:**
    - A Shuffle workflow is created to:
        1. Receive alerts from Wazuh triggered by web attacks.
        2. Create a case in TheHive with relevant information.
        3. Notify the team on Microsoft Teams.
        4. Perform automated analysis using Cortex.
        5. Enrich the case with analysis results.

5.2. Outputs Produced

The outputs produced in this final stage of the implementation include:

- Integrated and configured security tools: Wazuh, TheHive, Cortex, and Shuffle are set up and interconnected to facilitate incident detection, response, and analysis.
- Automated Workflow: The Shuffle workflow is created and configured to automatically handle incoming Wazuh alerts, create cases in TheHive, notify the team on Microsoft Teams, run automated analysis using Cortex, and enrich case information.
- Collaborative Incident Handling: TheHive provides a collaborative workspace for security analysts to investigate and respond to incidents. Analysts can add notes, tasks, and tags to incidents, ensuring effective teamwork.

5.3. Tools and Languages Used

The final stage of the implementation utilizes the following tools and languages:

- Operating Systems: Ubuntu 22.04 for Wazuh, TheHive, Cortex, and Shuffle VMs.
- Wazuh: Used for intrusion detection and alert generation.
- Teler: Integrated with Apache web server for generating logs.
- TheHive: Utilized for incident management, collaboration, and case creation.
- Cortex: Used for automated analysis of incidents and artifacts.
- Microsoft Teams: Integrated with TheHive for incident notifications.
- Shuffle: Used to create and manage the incident response workflow.
- MISP: For threat Intelligence feeds.

The implementation is focused on achieving an automated incident detection and response system using the integrated tools and workflows. The final stage outlined in this section completes the setup and configuration, enabling the system to effectively handle and respond to security incidents in a collaborative and efficient manner.

6. Evaluation

In this section, we will comprehensively evaluate the differences between the manual and automated incident response workflows. Analysis of the results and implications of each approach in terms of efficiency, accuracy, and overall effectiveness is carried out. For evaluation the attack chosen is a web application attack and a SSH brute force attack as these are some of the most common attacks on webservers (Thompson, 2023).

Manual Workflow Analysis: Evaluate the efficiency and effectiveness of the manual incident response workflow.

Results and Findings:

- Incident Identification: Manual identification of alerts is time-consuming and relies heavily on human vigilance. The process is prone to delays and missed alerts, leading to potential security gaps.
- Case Creation: Manually creating incident cases in TheHive is labor-intensive and may introduce inconsistencies in case details. This process is prone to human errors and delays.
- Manual Analysis: Analysts manually collect and correlate threat intelligence data, which can lead to delays in response and limited context for decision-making.
- Response: Manual response strategies depend on analyst expertise and may result in delayed or inconsistent actions. Collaboration among analysts can be challenging due to communication gaps.

Implications:

- The manual workflow is time consuming, which could impact incident resolution time.
- Analysts' expertise and availability significantly affect the efficiency and accuracy of incident analysis and response.

Automated Workflow Analysis: Evaluate the efficiency and effectiveness of the automated incident response workflow.

Results and Findings:

- Automated Detection: Alerts are automatically generated based on predefined rules. This approach ensures quick and consistent alert identification.
- Case Automation: Automated case creation in TheHive includes accurate and standardized alert information, reducing manual effort and ensuring consistent case details.
- Automated Analysis: Cortex and MISP automatically perform analysis using predefined workflows and threat intelligence data. This leads to faster and more accurate decision-making.
- Notification: A message is posted in the Micorosoft teams channel notifying the analyst that an incident has triggered.

Implications:

- The automated workflow significantly reduces incident identification and reporting time, improving overall incident response time.
- Automated case creation and analysis enhance the accuracy and consistency of incident details and analysis.

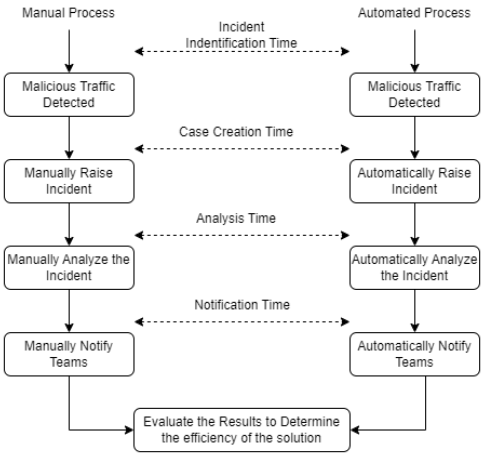

Figure 2: Evaluation Process

6.1.Experiment / Case Study 1: Web Attack Detection.

- The experiment involves hosting a vulnerable website called DVWA on the same server as Shuffle. A simulated Cross-site scripting attack is executed on the DVWA website. The Wazuh-Agent installed on the webserver sends the generated logs to the Wazuh-Manager.
- The traffic is compared against predefined rules in wazuh, which triggers a predefined workflow in Shuffle. As a result, Shuffle generates an incident ticket in TheHive and subsequently sends a notification to a designated Microsoft Teams channel.
- The incident created includes automatically added observables, and the Cortex system analyzes the IP address against installed analyzers, producing a comprehensive report. This aids the analyst team in making swift and informed decisions.
- A manual replication of the same scenario is conducted, involving manual steps for detecting the alert, initiating the incident, adding observables, analyzing the IP address, and sending a message in the Microsoft Teams channel.
- The time take for both the process is as follows:

Manual Workflow Analysis:	**Time Taken**
Incident Identification:	5 mins
Case Creation:	3 mins
Manual Analysis:	7 mins
Notification	16 mins

Automated Workflow Analysis:	**Time Taken**
Automated Detection:	52 seconds
Case Automation:	31 seconds
Automated Analysis:	31 seconds
Notification	52 seconds

6.2.Experiment / Case Study 2: SSH Brute Force

- In this case study, a simulation of an SSH brute force attack is executed. Similar to the previous experiment, the Wazuh-Agent on the webserver forwards logs to the Wazuh-Manager.
- The traffic undergoes rule-based analysis in wazuh, leading to the activation of a predefined workflow in Shuffle. The ensuing process involves the creation of an incident ticket in TheHive and the transmission of a notification to a Microsoft Teams channel.

- Automatic addition of observables to the incident is carried out, followed by the Cortex system's analysis of the IP address through installed analyzers, resulting in a detailed report. This empowers the analyst team to swiftly respond to the threat.
- As in the first case study, a manual replication of the entire process is performed, encompassing alert detection, incident initiation, observable addition, IP address analysis, and message dissemination via Microsoft Teams.
- The time required for each stage in both the automated and manual methods is provided below:

Manual Workflow Analysis:	**Time Taken**
Incident Identification:	10 mins
Case Creation:	3 mins
Manual Analysis:	5 mins
Notification	18 mins

Automated Workflow Analysis:	**Time Taken**
Automated Detection:	40 seconds
Case Automation:	15 seconds
Automated Analysis:	15 seconds
Notification	40 seconds

6.3.Discussion

The discussion will delve into an in-depth analysis of the outcomes from the conducted experiments and case studies. The results of the both the experiments highlight the efficacy of the automated workflow in promptly detecting and responding to web attacks. The integration of tools such as Wazuh, Shuffle, TheHive, and Cortex showcased a seamless process of incident identification, case creation, analysis, and response. Notably, the automated approach significantly reduced the time between incident detection and response, leading to swift mitigation measures.

The comparison with the manual workflow underscored the efficiency gained through automation. In the manual scenario, the delay in incident identification, case creation, and analysis was evident, showcasing the potential for extended exposure to threats. This contrast reinforces the value of integrating automated tools for real-time threat management.

However, the experiment also revealed areas for potential improvement. While the automated workflow demonstrated speed and accuracy, there is room for improvement. If more system resources are to be made available, the setup can work even better as some of the tools require a lot of processing power which in turn slows down the setup.

The setup process for most of these tools was relatively uncomplicated, with the main complexity arising during the configuration phase. This entailed referring to documentation, blogs, or troubleshooting resources to navigate through errors and determine the precise settings suitable for your specific setup. These individual tools offer substantial flexibility and encompass a multitude of applications, allowing for the creation and implementation of tailored solutions in accordance with your unique environment. The architecture, in its entirety, is impressive and holds practical value for real-world implementation scenarios.

6.4.Limitations

The setup is quite resource-intensive and need to have adequate resources for the implementation. The established setup for this project was designed to be minimal, resulting in occasional latency problems. To efficiently manage these resources, certain systems had to be temporarily deactivated, ensuring availability for the proper functioning of the tools. For instance, the Wazuh Machine had to be temporarily shut down after forwarding logs to the

Shuffle workflow, after which the remaining machines were reactivated to finalize the procedure. Due to resource constraint testing on windows logs is not conducted. Also the webserver is installed on the same system as Shuffle.

7. Conclusion and Future Work

In this study, our primary aim was to develop and evaluate an integrated workflow for automated incident detection, analysis, and response, leveraging a combination of security tools. The research question revolved around comparing the effectiveness of an automated workflow against a manual approach in terms of incident handling and response. The objectives included setting up an integrated environment, simulating various attack scenarios, and assessing the performance of both manual and automated workflows.

The results of our experiments demonstrate the feasibility and efficiency of the automated workflow in incident management. By integrating tools like Wazuh, Shuffle, TheHive, Cortex, and MISP, we were able to create a seamless process that automates incident identification, analysis, and response. This automated approach not only reduces the response time but also ensures consistent and standardized handling of incidents. Our findings reveal that the automated workflow significantly outperforms the manual approach in terms of speed, accuracy, and effectiveness.

The implications of our research are noteworthy from both academic and practical perspectives. Academically, our study contributes to the existing body of knowledge by showcasing the advantages of automated incident response workflows and providing insights into the integration and orchestration of various security tools. Practically, our research offers a valuable solution for organizations aiming to enhance their incident response capabilities by adopting an automated approach.

However, our research is not without limitations. The setup we used was minimal and may not fully represent the complexities of large-scale enterprise environments. Moreover, while we integrated several tools successfully, the effectiveness may vary based on specific use cases and configurations. Additionally, the practical implementation of the automated workflow could be influenced by factors such as tool compatibility, version updates, and evolving threat landscapes.

For future work, meaningful avenues include:

- **Enhanced Scalability:** Conducting experiments in more complex and scalable environments to evaluate the performance of the automated workflow under diverse conditions.
- **Machine Learning Integration:** Integrating machine learning models for anomaly detection and pattern recognition to enhance the accuracy of incident identification.
- **User-Friendly Interfaces:** Designing user-friendly interfaces and dashboards for streamlined incident visualization and management.
- **Using Cloud Resources:** The setup can be deployed in the cloud environment to manage high availability and scalability.
- **Integrate other devices:** Integrate log sources like Windows logs, Firewall logs etc.

In conclusion, the research has successfully demonstrated the effectiveness of an automated incident response workflow using a combination of integrated tools. While there are certain limitations, the findings highlight the potential benefits of adopting such automated approaches and offer directions for future research to further refine and expand upon the work.

References

AbuseIPDB. (n.d.). AbuseIPDB. Available at: https://www.abuseipdb.com/

Digininja. (n.d.). *Digininja/DVWA*. Available at: https://github.com/digininja/DVWA#linux-packages

CIRCL. (n.d.). *MISP - Open Source Threat Intelligence Platform.* Available at: https://www.circl.lu/services/misp-malware-information-sharing-platform/

Elradi, M. D., Abdelmajeed, K. A., & Abdulhaleem, M. O. (2021). Cyber Security Professionals' Challenges: A Proposed Integrated Platform Solution. *Electrical Science & Engi neering*, 03(02). doi: 10.30564/ese.v3i2.3376. https://doi.org/10.30564/ese.v3i2.3376

Frikky. (2020). *Introducing Shuffle—An Open Source SOAR platform part 1*. Available at: https://medium.com/shuffle-automation/introducing-shuffle-an-open-source-soar-platform-part-1-58a529de7d12

Galdi, E., Perrone, G., & Romano, S. P. (2022). ThePhish: An Automated Open-Source Phishing Email Analysis Platform. *ITASEC'22: Italian Conference on Cybersecurity.* Rome, Italy. Available at: https://ceur-ws.org/Vol-3260/paper6.pdf

Gibadullin, R., & Nikonorov, V. (2021). Development of the System for Automated Incident Management Based on Open-Source Software. *2021 International Russian Automation Conference (RusAutoCon)* (pp. 521 - 525). Kazan, Russia: IEEE. doi: https://doi.org/10.1109/RusAutoCon52004.2021.9537385

Groenewegen, A., & Janssen, J. S. (2021). TheHive Project: The maturity of an open-source Security Incident Response platform [SNE/OS3.nl - Offensive Technologies: Project Report]. University of Amsterdam. *ResearchGate*. Available at: https://www.researchgate.net/publication/352715439_TheHive_Project_The_maturity_of_an_open-source_Security_Incident_Response_platform

Johnson III, R. (2019). *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked. Cybercrime Magazine*. Available at: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Leonard, J. (2017). *TheHive, Cortex and MISP: How They All Fit Together*. Available at: https://blog.thehive-project.org/2017/06/19/thehive-cortex-and-misp-how-they-all-fit-together/

Muhammad, R. M., Irawati, I. D., & Iqbal, M. (2021). Integrated Security System Implementation for Network Intrusion. *Journal of Hunan University (Natural Sciences)*, Vol. 48. No. 6. Available at: http://jonuns.com/index.php/journal/article/view/619

Obahor, V. (2022). Detecting web attacks using Wazuh and teler. Available at: https://wazuh.com/blog/detecting-web-attacks-using-wazuh-and-teler/

Oujezsky, V., Horvath, T., & Holik, M. (2022). Security Incident Response Automation for xPON Networks. *Journal of Communications Software and Systems*, 18(2), 144–152.

Preuveneers, D., & Joosen, W. (2021). Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. *Journal of Cybersecurity and Privacy*, 140–163. doi: https://doi.org/10.3390/jcp1010008

Srivastava, A., Chauhan, A. S., Gupta, S., Gautam, A., & Kaur, Dr. G. (2018). Malware Detection using Online Information Sharing Platforms and Behavior Based Analysis. *3rd International Conference on Internet of Things and Connected Technologies, ICIoTCT 2018*. Information systems & ebusiness network, Noida, Uttar Pradesh, pp. 726-729.

Stanković, S., Gajin, S., & Petrović, R. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. *Proceedings, IX international conference IcETRAN*, Novi Pazar, Serbia, pp. 6 - 9. Available at: https://www.etran.rs/2022/zbornik/ICETRAN-22_radovi/068-RTI2.6.pdf

Suryantoro, T., D.P., B. P., & Andriyani, W. (2022). 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)*, Yogyakarta, Indonesia. doi: https://doi.org/10.1109/ISRITI56927.2022.10052950

Tariq, A., Manzoor, J., Aziz, M. A., Tariq, Z. U. A., & Masood, A. (2022). Open source SIEM solutions for an enterprise. *Emerald Publishing Limited 2056-4961*, Vol. 31 No. 1, pp. 88–107. doi: https://doi.org/10.1108/ICS-09-2021-0146

Thompson, K. (2023, February 27). *The 10 Most Common Website Security Attacks*. Available at: https://www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself

Tunggal, A. T. (2023). *What is the Cost of a Data Breach in 2023?* Available at: https://www.upguard.com/blog/cost-of-data-breach#:~:text=What%20is%20the%20Average%20Cost,reach%20%245%20million%20in%202023.

Verizon. (n.d.). (2019) *Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/2019/2019-data-breach-investigations-report.pdf

VirusTotal. (n.d.). VirusTotal. Available at: https://www.virustotal.com/gui/home/upload

Wazuh. (2023). *Getting started with Wazuh/Components*. Available at: https://documentation.wazuh.com/current/getting-started/components/index.html

Worldpay editorial team. (2019). *Small Business Data Breach: The Consequences of a Cybercrime Data Breach*. Available at: https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses