LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS6P05NI - Final Year Project

Assessment Weightage & Type

25% Final Year Project - Interim Report

Project Title : Automated Incident Response for Cyber Anomalies (AIRCA)

Year and Semester

2023-24 Autumn

Student Name:

London Met ID:

College ID:

Internal Supervisor:

External Supervisor:

Proposal Due Date:

Proposal Submission Date:

Word Count (Where Required): 3537

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Sample - BINIS.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:73855426

Submission Date
Dec 12, 2024, 2:05 PM GMT+5:45

Download Date
Dec 13, 2024, 8:54 AM GMT+5:45

File Name
Sample - BINIS.docx

File Size
35.6 KB

52 Pages

5,419 Words

30,551 Characters

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

56 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks

7 Missing Quotations 2%
Matches that are still very similar to source material

1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources

4% Publications

16% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **56** Not Cited or Quoted 5%
  Matches with neither in-text citation nor quotation marks
- **7** Missing Quotations 2%
  Matches that are still very similar to source material
- **1** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 8% Internet sources
- 4% Publications
- 16% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	National Institute of Business Management Sri Lanka on 2024-10-31 — 3%
2	Internet	www.coursehero.com — 2%
3	Submitted works	University of Greenwich on 2010-05-29 — 1%
4	Submitted works	Kingston University on 2024-01-07 — 1%
5	Submitted works	Ghana Technology University College on 2016-10-13 — 0%
6	Submitted works	UNITEC Institute of Technology on 2021-06-29 — 0%
7	Submitted works	The University of Wolverhampton on 2024-02-17 — 0%
8	Submitted works	Queen Mary and Westfield College on 2024-12-02 — 0%
9	Internet	uir.unisa.ac.za — 0%
10	Submitted works	Jose Rizal University on 2024-09-03 — 0%

Abstract

This report is about the description of the development process of the project “Automated Incident Response for Cyber Anomalies (AIRCA)”. It is a system that automatically detects, analyses, and responds to security incidents and is fully containerised which makes it lightweight, easy to deploy and ready to use in any environment. This report consists of 7 chapters: Introduction, Background, Development, Future Work, Conclusion, References, and Appendix.

Keywords: Cyber Anomalies, Cyber Threat Actors, Security Events and Incidents, Security Orchestration, Security Automation, Security Threat Detection and Response, Threat Intelligence, Vulnerability Identification, Correlation Analysis, Containerization.

Acknowledgement

It is always a pleasure to remind the fine individuals in Islington College for the sincere guidance I received to uphold my research and report writing in the **Final Year Project Module**.

I would like to express my deepest gratitude towards my supervisors, and , for their constant assessment, feedback, and guidance regarding the project. The interim report could not have been possible without the continuous suggestion and feedback from both supervisors.

I would also like to thank my seniors and colleagues for the support they provided me during different phases of the project. I appreciate everyone's support in this endeavour.

Lastly, I would like to thank Islington College for introducing the Final year project module which created a creative environment and helped me enhance myself in every aspect so that I could be ready for my future career and the industry ahead.

Table of Contents

Table of Contents

Table of Contents

Table of Figures

Table of Tables

Chapter I : Introduction

1.1. Topic Introduction

In today's digital landscape where everything relates to each other, people face an ever-increasing volume and complexity of cyber threats. The rapid evolution of cyberattacks demands a proactive and efficient approach to incident response to safeguard sensitive data, protect critical systems, and ensure the continuity of business operations. A system with Automated Incident Response enriched with the various capabilities of **Security Orchestration, Automation, and Response (SOAR)** (IBM, 2015), emerges as a crucial solution to meet this issue.

Traditional manual incident response processes, while effective to some extent, are often overwhelmed by the large scale and sophistication of modern cyber threats. This limitation necessitates a paradigm shift in incident response, where automation and orchestration play a very important role because cybersecurity incidents can have devastating consequences, from financial losses to reputational damage and various legal liabilities.

1.2. Problem Scenario

Cybercrime has become more prevalent as technology is advancing. Following the recent changes prior to the pandemic, the usage of technology and the internet has skyrocketed. At the same time, new types of cyber threats and anomalies emerge every day, increasing the damage. These threats include **Malware Attacks, Phishing Campaigns, Data Breaches, Advanced Persistent Threats (APTs)** and many more. The challenge lies not only in the frequency and sophistication of these attacks but also in the complexity of managing and responding to them effectively.

The escalating volume of daily emerging cyber threats, particularly those attributed to malware, poses a pervasive cybersecurity challenge worldwide. This statement is sharply illustrated through the comprehensive data statistics presented in *Figure 1* and *Figure 2* of SonicWall's threat report titled "**Mid-Year Update: 2023 SonicWall Cyber Threat Report**".

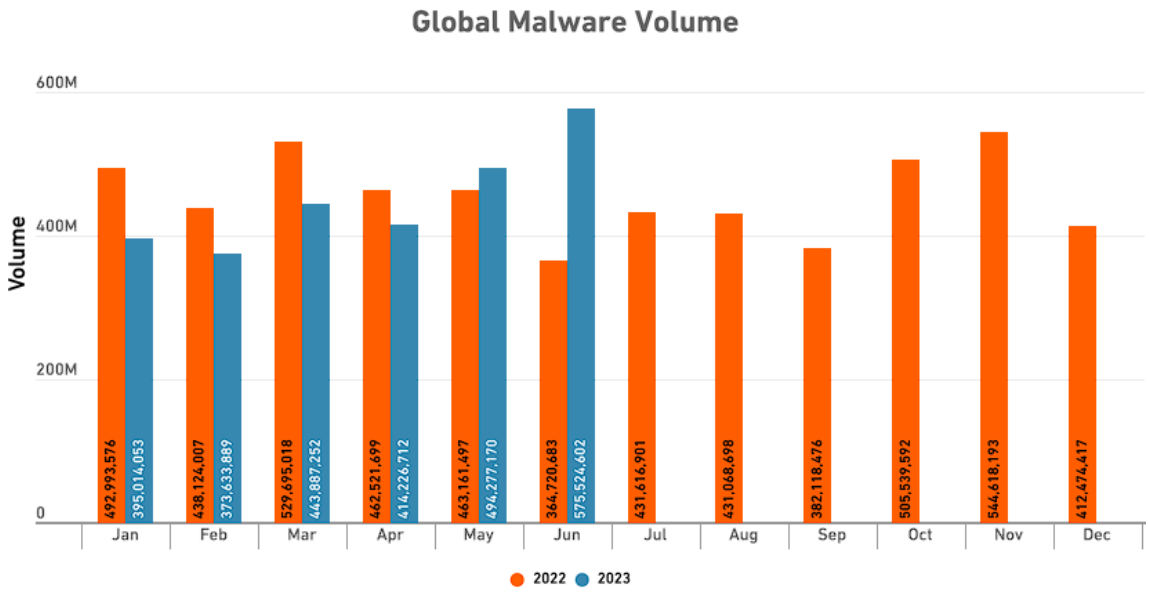

Figure 1 Global Malware Volume (SonicWall, 2023).

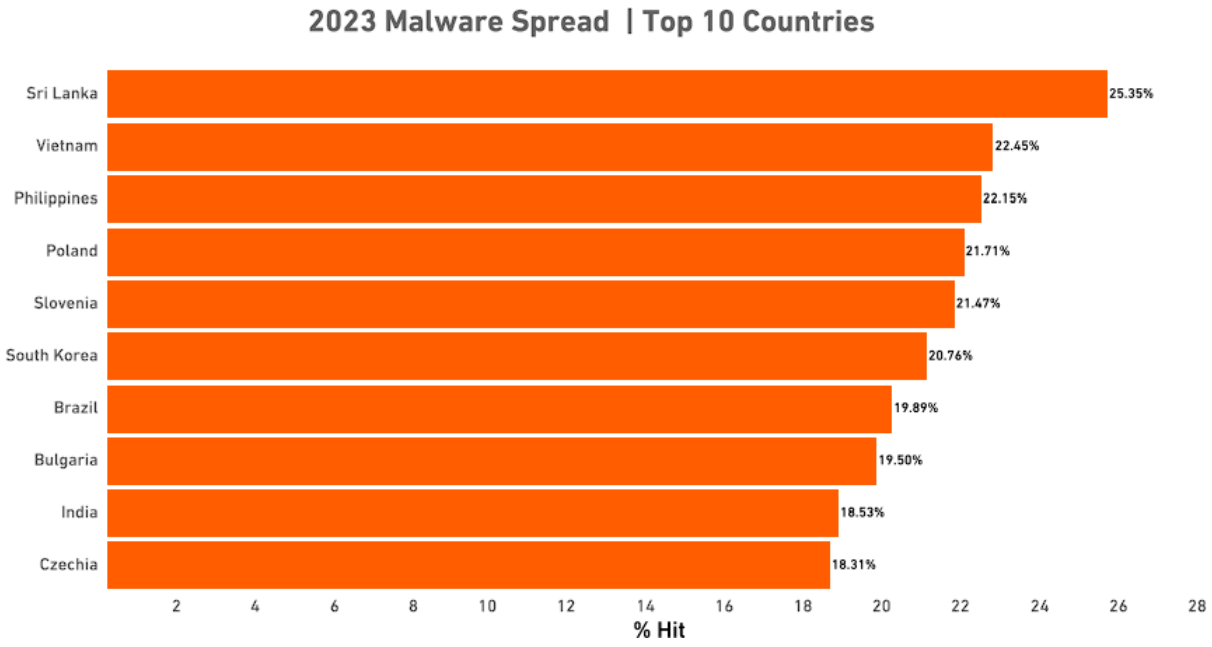

Figure 2 Top 10 Malware Spread by Countries (SonicWall, 2023) .

1.3. Project as a Solution

In response to the increasingly complex and relentless cybersecurity anomalies on organizations that reside in the systems totally being undetected which can be stated after looking through the data statistics in *Figure 1* and *Figure 2*, the development and implementation of an **Automated Incident Response for Cyber Anomalies (AIRCA)** system is proposed. This solution offers a comprehensive approach to detect different cyber anomalies and actively respond to them.

AIRCA will help in incident response by building a platform that will detect cyber anomalies on any devices in a network and automates the response for the detected threat. This automation not only alleviates the burden on security teams, but will accelerate response times, and can be setup in any environment. Moreover, the system will integrate with various security tools and platforms, including **Intrusion Detection System (IDS), Security Information and Event Management (SIEM)**, **Threat Intelligence Platform (TIP)** and many more, as per the project requires (SANS, 2023). This approach equips any environment with a better defence against cyber anomalies, strengthening cybersecurity posture and mitigating risks associated with data breaches and various losses.

1.4. Aim and Objectives

1.4.1. Aim

The main aim of this project is to develop a system with the proactive capability to swiftly respond to any detected cyber anomalies during comprehensive monitoring, ensuring immediate and effective incident resolution.

1.4.2. Objectives

The objective to achieve the aim of this project are as follows:

i. Designing a virtual system and network architecture to develop AIRCA.

ii. Implementing existing security infrastructure and integrate them with each other.

iii. Developing automation modules for the security infrastructure to actively monitor, detect and respond to any threat indicators.

iv. Integrating threat intelligence feeds for real-time data sharing and comprehensive threat analysis.

v. Logging each devices network and system activities for further investigations.

1.5. Report Structure

This section provides the contents of the whole report.

SN.	Title	Contents
1.	Chapter I : Introduction	• Topic Introduction • Problem Scenario • Project as a Solution • Aim and Objectives • Report Structure
2.	Chapter II : Background	• Understanding the Project - Automated Incident Response - Project Elaboration - Survey Analysis • Resource Requirement • Similar Projects Review - Comparison and Critical Analysis
3.	Chapter III : Development	• Project Methodology • Work Breakdown Structure • Project Milestones • Gantt Chart • System & Network Diagram • Progress Table • Progress Review - Current Scenario of Progress - Project Timeline - Action Plan
4.	Chapter IV: Future Work	• Phases and Tasks left for completion
5.	Chapter V: Conclusion	• Project Review/Summary
6.	Chapter VI: References and Bibliography	• List of sources used, referenced, and cited in the report
7.	Chapter VII: Appendix	• Survey Form and Responses • System Deployment and Development Progresses • Defining Project Methodology

Table 1 Structure of Report

Chapter II : Background

2.1. Understanding the Project

2.1.1. Automated Incident Response

Incident response refers to how a company deals with and handles problems like cyber threats or attacks on its computer systems. The idea is to catch and stop these issues early on, so they don't cause too much damage or disruption to the business (IBM, 2023).

Incident response automation is exactly what it sounds like. At its basic level, this might involve automating simple tasks like reporting and notifications. More advanced automation goes beyond that, automatically finding, evaluating, and dealing with security incidents and threats without needing human intervention (BlackBerry, 2023).

2.1.2. Project Elaboration

AIRCA is a system that automatically detects, analyses, and responds to security incidents and is fully containerised which makes it lightweight, easy to deploy and ready to use in any environment. AIRCA is based on Wazuh and takes advantage of its multiple features such as vulnerability identification, system auditing and reporting, security alerts generation, active response automation.

Wazuh is a free and open-source unified XDR and SIEM used for security threat prevention, detection, and response that can protect workloads across on-premises, virtualized, containerized, and cloud-based environments (Wazuh, 2023). The agent is one of the core features of Wazuh. AIRCA makes use of this feature because it helps actively monitor the endpoints' network and system behaviour and look for any anomalies and send this information back for analysis.

If suspicious activities are found or any alerts are triggered for the pre-written rules configured in Ossec which is another feature provided by Wazuh then, the python script that are specifically written for such rules will automatically run and perform necessary actions to

respond to such threats. This feature to respond to threats is what Wazuh refers as "**Active Response**".

For better correlation analysis, Wazuh is integrated with MISP which is another open-source software solution for collecting, storing, distributing, and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis (MISP, 2023).

2.1.3. Project Deliverables

Some of the deliverables of the system have been listed below:

i. **Pro-active response:** The system will be able to actively monitor the endpoint device and if any threat would be to be found, it will get responded quickly.

ii. **Vulnerability identification:** The system will use the features of Wazuh which already has many features to identify and vulnerability in the system. This feature will help the system grow much more to be fully functional system ready to be implemented in any environment.

iii. **Easy to deploy:** The system will use containerization which can be easily used to turn on the system and turn off whenever needed.

iv. **Correlation Engine:** The system will get integrated with threat intelligence feeds which will help correlate any incident/event for threat identification.

2.1.4. Survey Analysis

The survey for the project was carried out among various people from different background from people with no IT background to people working in Cyber Security as their professions. The survey form was majorly filled by students at Islington College and cyber security professionals from Nepali Cyber Security Companies such as Vairav Tech, Cryptogen Nepal, etc. These companies have been using different vendors' SIEM and other security solutions as well as their own in-house developed solutions with different features for incident response to threats.

Most of the survey participants were familiar with all the tools and technologies mentioned in the survey questions. All of them agreed that a system implementing the tools and technologies would probably help better increase defence against various cyber anomalies. They suggested some of their idea for the success of the project and mentioned that the system would help prevent some of the incidents that they faced in recent years. And through the survey form responses, it was concluded that automated incident response with integrated threat intelligence for responding to cyber threat and anomalies is very important and can help organizations or even individuals protect their assets from cyber threat actors.

The survey form questions can be found at *Pre-Survey Questions* and the responses can be found at *Pre-Survey Responses*. Please note that some of the survey responses were cleaned out because they contained unexpected responses.

2.2. Resource Requirement

2.2.1. Hardware Requirements

Some hardware recommendation for safer and smooth operation of the system have been listed below:

i. 8GB RAM

ii. 40GB Hard Disk

iii. 2.4 GHz Processor

iv. Network Interface Card (NIC)

2.2.2. Software Requirements

The software required for the system have been listed below:

i. **VMware:** It will be used for creating virtual machines that will serve as server and client for the project.

ii. **Linux:** It will be used to host the servers for the project.

iii. **Windows:** It will be used as an endpoint device which will be monitored for any threat detection.

iv. **Python:** It will be used for installing various libraries that will be needed for our ELK stack deployments. It will also be used for writing automation scripts for active response.

v. **Yara:** It will be used to write rules that will be used for finding any malicious patterns in a file.

vi. **Wazuh:** It is an ELK stack based open-source SIEM and XDR project that is widely used all over the world due to its stable and unique features for detection and response. It will be implemented for this project since it's already free to use.

vii. **Malware Information Sharing Platform (MISP):** It is yet another widely used and popular open-source platform that is used by cyber threat intelligence teams all over the world to share malware feeds which will be used in this project as well for malware detection.

viii. **Docker:** It will be used later in this project to deploy the servers for scalability and to reduce large hardware consumption.

2.3. Similar Projects

This section includes three projects which are somehow like AIRCA. They are briefly described below:

2.3.1. Project 1 : OpenEDR

OpenEDR is a free and open-source tool for detecting and responding to cyber threats on your computer. It helps analyse and understand potential threats by keeping an eye on activities in real-time. With features like Mitre ATT&CK visibility, it helps you connect the dots and figure out the root cause of any suspicious cyber behaviour. It's like a watchdog for your computer, available for everyone to use, no matter the size of their organization.

[*Learn more about OpenEDR at https://www.openedr.com/.*]

2.3.2. Project 2 : Graylog

Graylog is a log management platform designed to collect, index, and analyses both structured and unstructured data from nearly any source. Graylog serves as a robust platform, facilitating the efficient handling of logs for comprehensive insights. It enables users to make sense of diverse data types, whether structured or unstructured, from a wide range of sources.

[*Learn more about Graylog at https://graylog.org/.*]

2.3.3. Project 3 : Splunk

Splunk is a large-scale data platform designed to streamline the process of gathering and overseeing extensive amounts of machine-generated data, making it easier to search for specific information. This technology finds applications in business and web analytics, as well as in managing applications, ensuring compliance, and enhancing security measures.

[*Learn more about Splunk at https://www.splunk.com/.*]

2.4. Comparison Table of Similar Projects

S.N.	Features	Project 1	Project 2	Project 3	AIRCA
1.	Identifies vulnerabilities in endpoint	✓	×	×	✓
2.	Collects, Correlates and Visualizes Logs	✓	✓	✓	✓
3.	Integrates Cyber Threat Intelligence for correlation analysis	×	×	×	✓
4.	Generates alerts based on pre-written rules	✓	✓	✓	✓
5.	Automates response for alerts raised	×	×	×	✓

Table 2 Comparison between similar projects and AIRCA

2.5. Conclusion from the Similar Projects

Comparing all the feature provided above in the comparison table, those three similar product/projects don't have some of the features. By default, none of the mentioned products come with pre-built integrated CTI for correlation analysis and automated response for the alerts generated by the engine. Whereas AIRCA provides features along with the features that are common in other three similar projects. Those above core features altogether allows AIRCA is to improve visibility, increase correlation abilities and reduce time to detect and time to respond. This makes the AIRCA stand out from those other similar types of projects.

Chapter III : Development

3.1. Project Methodology

DSDM, or Dynamic Systems Development Method, is an agile project management and software development framework that prioritizes user involvement, incremental delivery, flexibility, continuous testing, and reversible changes to enhance adaptability and responsiveness throughout the development lifecycle (Aiman Khan Nazir, 2017).

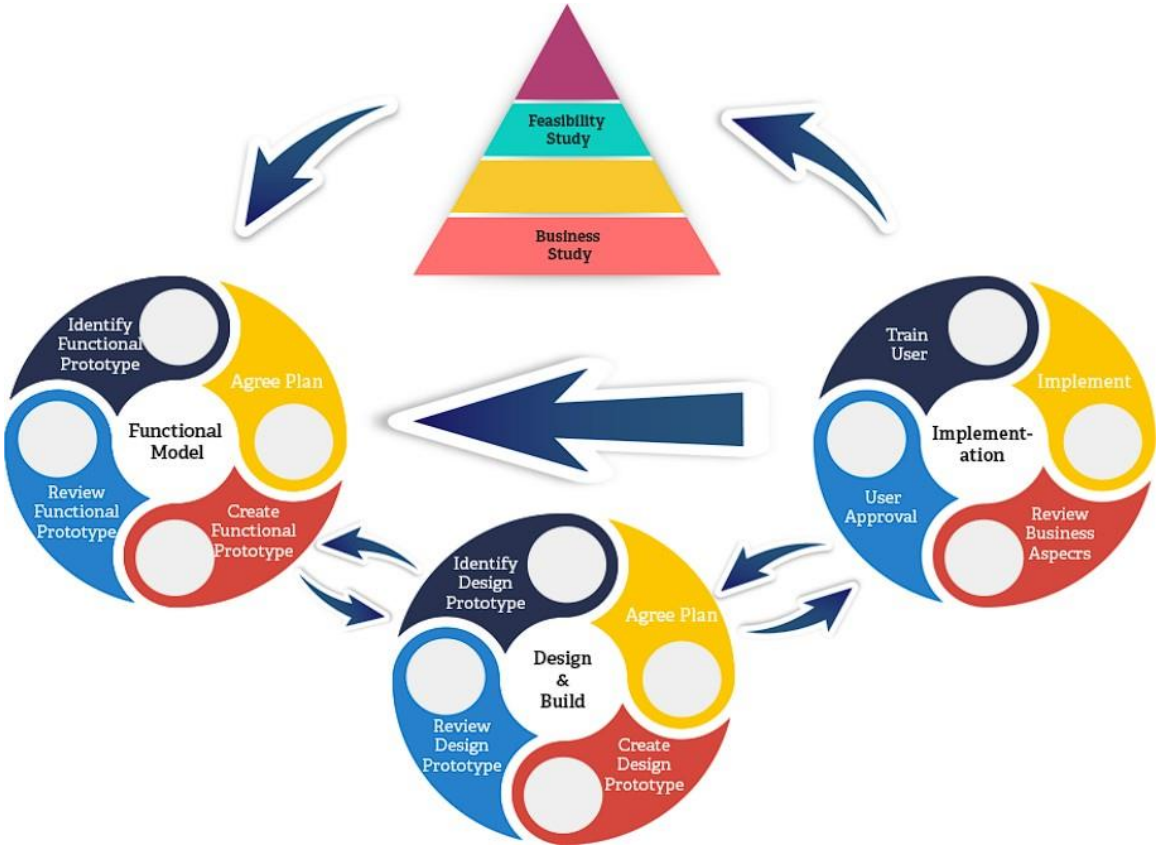

Figure 3 DSDM Process Model (Aiman Khan Nazir, 2017)

For this project, DSDM project was selected since it is driven by its user-centric approach, supporting active involvement throughout development, and its flexibility, enabling better adaptation to evolving cyber threat scenarios, aligning well with the project's dynamic and security-sensitive nature.

[*Note: For better understanding the DSDM model, please refer to "Defining DSDM".*]

3.2. Work Breakdown Structure

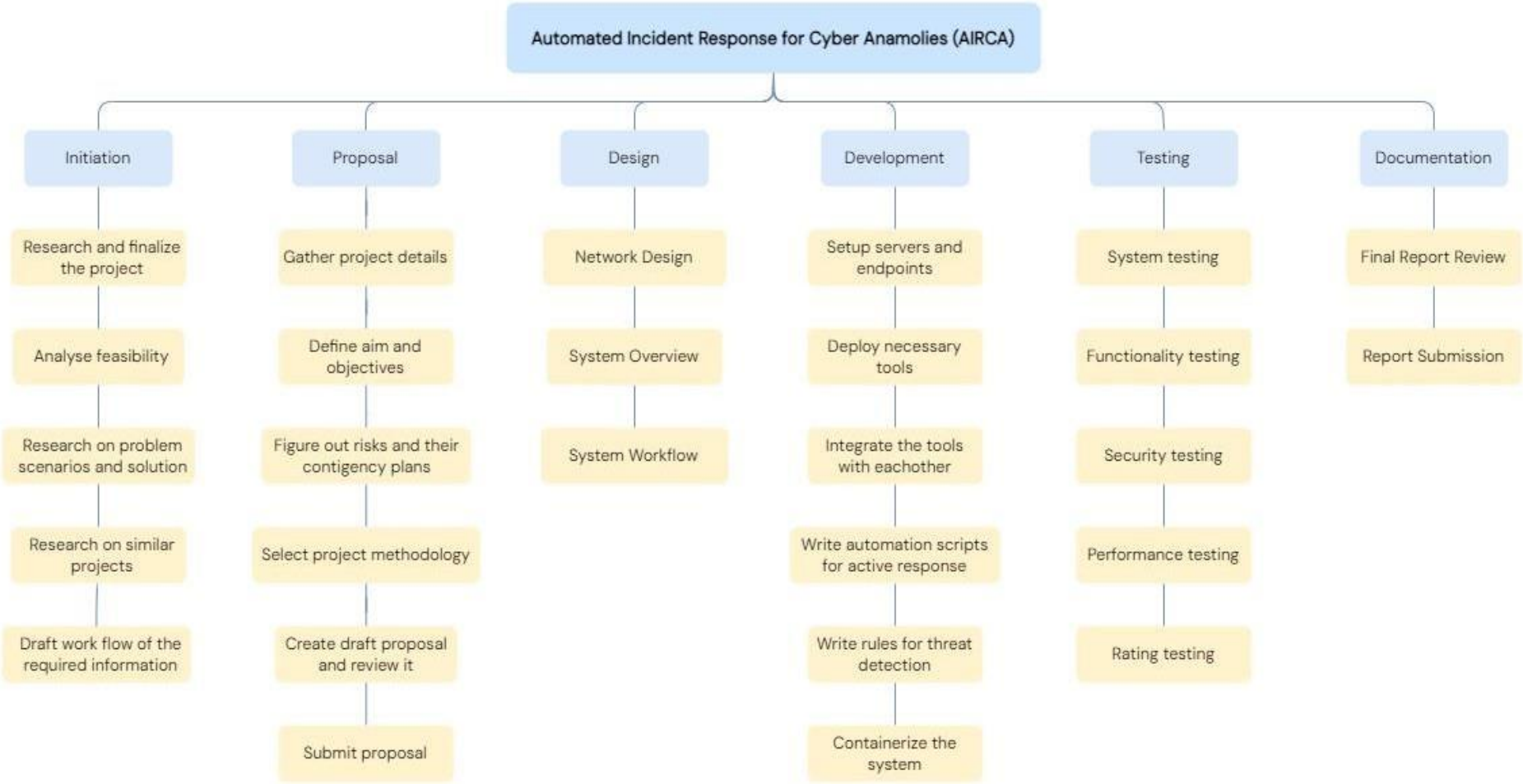

Figure 4 Work Breakdown Structure

3.3. Milestones

Figure 5 Project Milestones

3.4. Project Gantt Chart

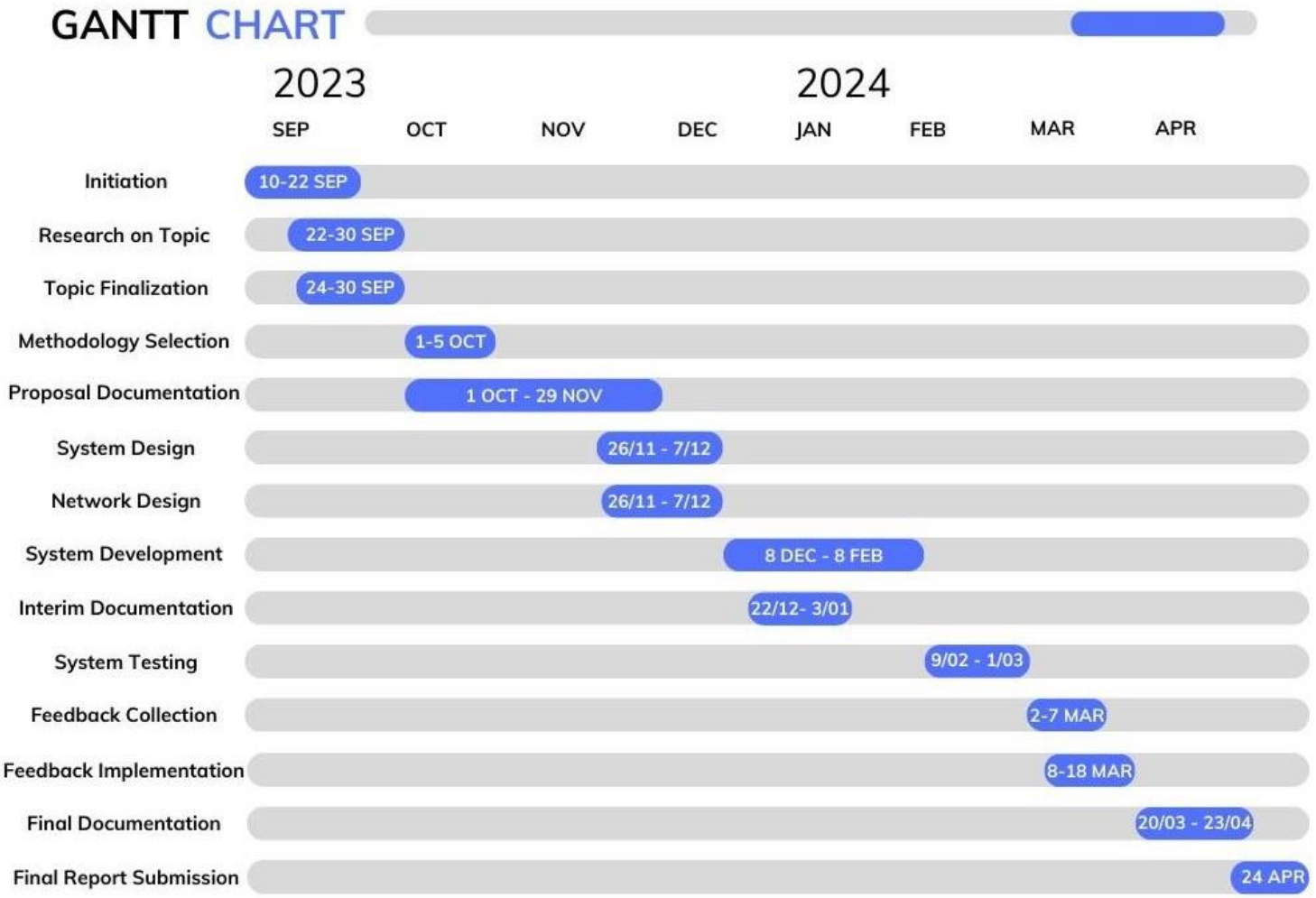

Figure 6 Gantt Chart

3.5. System & Network Diagram

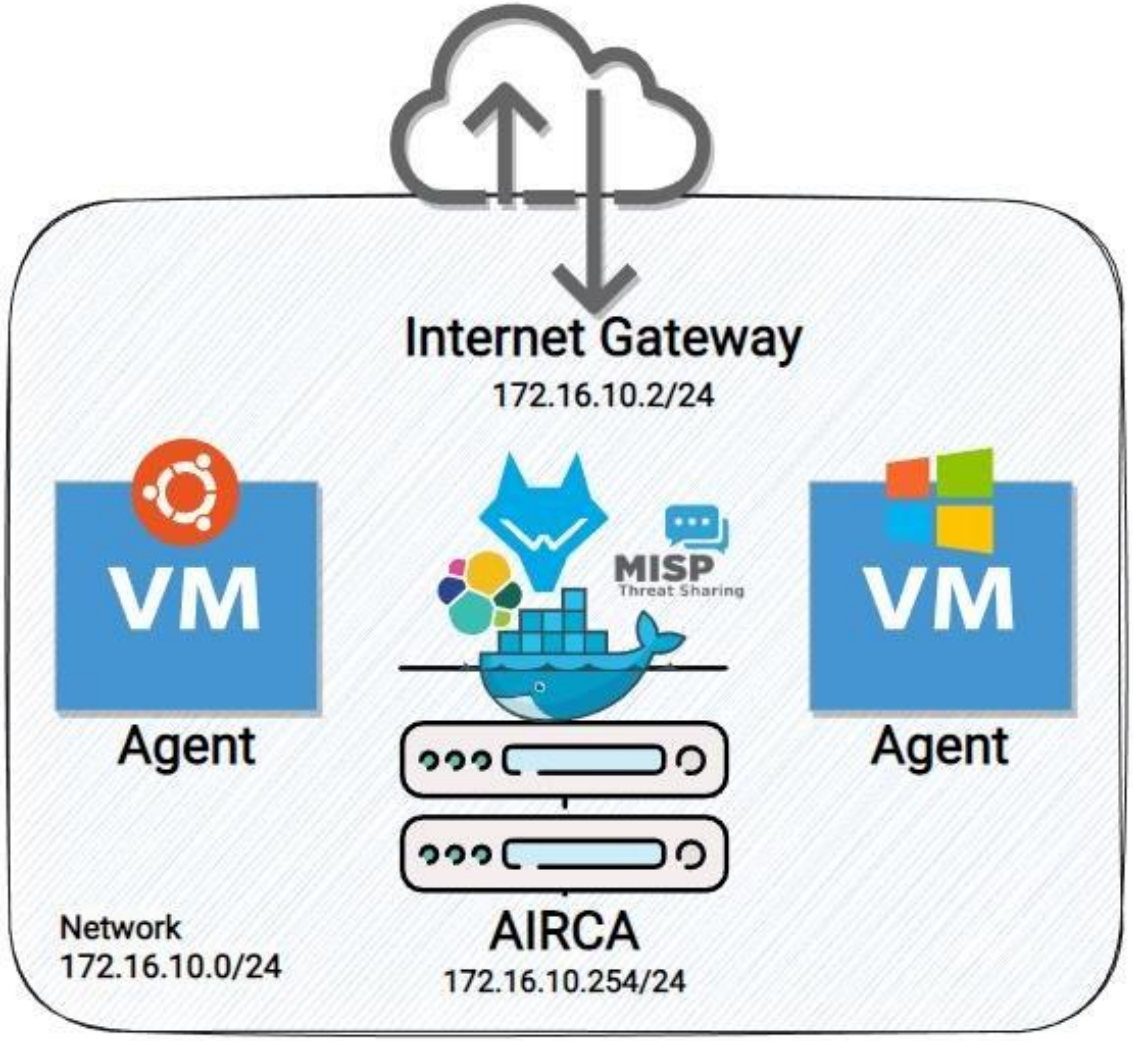

Figure 7 System and Network Architecture Diagram

3.6. Progress Table

S.N.	Task	Status	Progress (%)
1.	Research and finalize the project	Completed	100%
2.	Analyse Feasibility	Completed	100%
3.	Research on problem scenario and solution	Completed	100%
4.	Define aim and objectives	Completed	100%
5.	Figure out risks and their contingency plans	Completed	100%
6.	Proposal review and submission	Completed	100%
7.	System and Network Design	Completed	100%
8.	Setup servers and endpoints	Completed	100%
9.	Deploy Wazuh and MISP	Completed	100%
10.	Setup agents for the endpoints	Completed	100%
11.	Integrate Wazuh with MISP	Initiated	25%
12.	Clean up possible false positive/duplicate threat intel feeds	Initiated	25%
13.	Containerize the system	In progress	75%
14.	Interim report documentation	Completed	100%
15.	Add rules for threat detection	To do	0%
16.	Write automation scripts for active response	To do	0%
17.	Testing and Review	To do	0%
18.	Feedback Collection and Implementation	To do	0%
19.	Final Documentation	To do	0%
20.	Project Submission	To do	0%

Table 3 Project Progress Table

3.7. Progress Review

3.7.1. Current Scenario of Progress

3.7.1.1. Phase 1: Pre-Project Phase

The project was officially initiated on 29th September 2023, by elaborating the plans and with the suggestion of proposed project with the supervisors. The tools that were going to be used were verified and once the topic was accepted, the depth research was carried out for the tool's concepts, its modules/features, different detection rules and automation scripts, and required software development method for the project. After all the proposal of project was submitted on 27th November 2023.

3.7.1.2. Phase 2: Project Life Cycle Phase

3.7.1.2.1. Phase 2.1 : Feasibility Study

Once the proposal was accepted, the total estimated costs and technical feasibility were highly considered. Since, the tools that were being used for this project were all open-sourced project, the feasibility for the project development was completed. Likewise, the research on similar project and the needed resources for the development were listed out.

[*Note: Find the hardware and software requirements for the system at "Resource Requirement".*]

3.7.1.2.2. Phase 2.2 : Business Study

The proposed solution and future use of project was widely discussed with the supervisors. Pre-survey was done about the proposed project to acknowledge the business domain of the project for better understanding.

[*Note: Pre-survey questions and responses can be found at "Pre-Survey".*]

3.7.1.2.3. Phase 2.3 : Functional Model Iteration

Going through the Gant chart, after the proposal submission, which was on 29th November 2023, system and network architecture design of the project was designed for visualizing the proposed system. Eventually from 8th of December 2023, System development

was started, setting up virtual machines for AIRCA, Windows and Ubuntu were done. And by 30th December 2023, Network configurations, and Deployment of Wazuh and MISP were completed using docker containerization in the server's virtual machine. And in the windows and ubuntu endpoints, the server's agents were installed which indicates that 40% project has been completed and this phase is under development and within allocated time.

[*Note: The system and network design can be found at "System & Network Diagram".*]

Until now, the project development has reach up to phase 2.3 Functional Model Iteration and the remaining phases to be completed are listed below:

- Ongoing phase 2.3: Functional Model Iteration
- Phase 2.4: System Design and Build Iteration
- Phase 2.5: Implementation
- Phase 3: Post-Project Phase

[*Note: The system deployment, agent installation and other progresses can be found at "System Deployment and Development Progresses".*]

3.7.2. Project Timeline

The project was started with the goal of completing each task according to the Gantt chart within the specified time frame. So far, all work done has been completed within the specified time frame.

3.7.3. Action Plan

The remaining tasks of this project will be completed according to the updated Gantt Chart, as some tasks have been dropped and new tasks have been added. Certain tasks, such as Integration for Correlation analysis, Ossec configuration, Active response scripts, Vulnerabilities Identification, Collection of Yara rules, Testing, and Final documentation, will be performed parallel to keep the project on track.

Chapter IV : Future Work

4.1. Phases to Complete

Almost 45% of the overall project has been completed. However, there are specified tasks that must be accomplished soon within the period allotted in the Gantt Chart. These tasks comprise 55% of Integration for Correlation analysis, Ossec configuration, Active response scripts, Vulnerabilities Identification, Collection of Yara rules, Testing, Project Readjustment, and Final Documentation. The following phases are yet to be completed going through the DSDM methodology:

4.1.1. Phase 2 : Project Life Cycle Phase

4.1.1.1. Phase 2.3 : Functional Model Iteration

- **System Deployment and Integration**
  System deployment has been completed and integration between Wazuh and MISP will be started after interim report submission.
- **Detection Rules**
  Ossec configuration will be done and Yara rules will be collected from various sources for proper detection and analysis of maliciousness of a file seen in the endpoints.
- **Response Rules**
  Python scripts will be written for the active response for the malware detected and verified after Yara analysis in the endpoint.
- **System Containerization**
  The Wazuh and MISP server were deployed via docker-compose and were successfully deployed. But both were deployed using separate docker-compose files. So, a single file will be made for the deployment.
- **Testing**
  Once the development gets completed a series of testing will be performed to check the functionality, security, system, and performance testing. The series of testing of will be started from 9th February 2024 to 1st March 2024.

4.1.1.2. Phase 2.4 : System Design and Build Iteration

There will be need of project refinement in terms of certain features and functionality based on the output of test series, supervisors review and post survey form. According to Gantt chart Refine include feedback collection and feedback implementation which will be carried out from 2nd March 2024 to 18th March 2024.

4.1.1.3. Phase 2.5 : Implementation

The demonstration will be given to the people who involved in the project's pre-survey and post survey will be done for their review and feedback.

4.1.2. Phase 3 : Post-Project Phase

Measurements on how the system is performing after being deployed and what further maintenance are required are carried out accordingly.

4.1.3. Final Documentation

As per the Gantt Chart, the final documentation will be initiated from 20th March 2024 and will be completed on 23rd April 2022. The documentation process will be carried out and in within this timeframe, feedback from the supervisors for the report will be taken and implemented which will fulfil the requirements for the project completion.

Overall, about 40% of the work has been completed while 60% of the work of proposed system will be completed in future. Thereby multiple tasks will be done in a simultaneously with frequent reviews and suggestions from supervisors which will help in completing the project with allocated time.

Chapter V: Conclusion

In today’s digital world, the rise of cyber threats demands a proactive defence. This project provides an Automated Incident Response for Cyber Anomalies (AIRCA) system, designed to swiftly detect, and respond to emerging threats. Using the dynamic system development model (DSDM), the approach prioritizes adaptability, collaboration, and iterative development, ensuring a resilient and user-centric system.

Recognizing potential risks like hardware failures and query limitations, the project incorporates contingency plans to navigate these challenges. AIRCA aims to strengthen cybersecurity measures with expected outcomes including improved response efficiency and enhanced threat detection. From hardware recommendations to essential software components, each requirement is carefully considered to create a safer and more efficient operation. In essence, this project is not just about technology, it's a proactive step towards building a secure digital future where cyber threats are met with swift and effective responses.

Chapter VI : References

Abdullahi Sani, A. F. S. R. J. I. G., 2013. A Review on Software Development Security Engineering using Dynamic System Method (DSDM). *International Journal of Computer Applications,* pp. 33-44.

Aiman Khan Nazir, I. Z. M. A., 2017. The Impact of Agile Methodology (DSDM) on. *Circulation in Computer Science: International Conference on Engineering, Computing & Information Technology (ICECIT 2017),* pp. 1-6.

BlackBerry, 2023. *What Is Automated Incident Response?.* [Online]
Available at: https://www.blackberry.com/us/en/solutions/endpoint-security/managed-security-services/incident-response/automated-incident-response
[Accessed 26 December 2023].

Boehm, B. a. H. W., 2001. The Spiral Model as a Tool for Evolutionary Acquisition. *CrossTalk.*

Boehm, B. W., 1988. Computer. *TRW Defense Systems Group,* pp. 61-72.

IBM, 2015. *What is SOAR?.* [Online]
Available at: https://www.ibm.com/topics/security-orchestration-automation-response
[Accessed 25 November 2023].

IBM, 2023. *What is incident response?.* [Online]
Available at: https://www.ibm.com/topics/incident-response
[Accessed 26 December 2023].

MISP, 2023. *MISP (core software) - Open Source Threat Intelligence and Sharing Platform.* [Online]
Available at: https://github.com/MISP/MISP
[Accessed 26 December 2023].

SANS, 2023. *Glossary of Cyber Security Terms.* [Online]
Available at: https://www.sans.org/security-resources/glossary-of-terms/
[Accessed 25 November 2023].

SonicWall, 2023. *Mid-Year Update: 2023 SonicWall Cyber Threat Report,* s.l.: s.n.

Wazuh, 2023. *Wazuh - The Open Source Security Platform. Unified XDR and SIEM protection for endpoints and cloud workloads.*. [Online]
Available at: https://github.com/wazuh/wazuh
[Accessed 26 December 2023].

Chapter VII : Appendix

7.1. Pre-Survey

7.1.1. Pre-Survey Questions

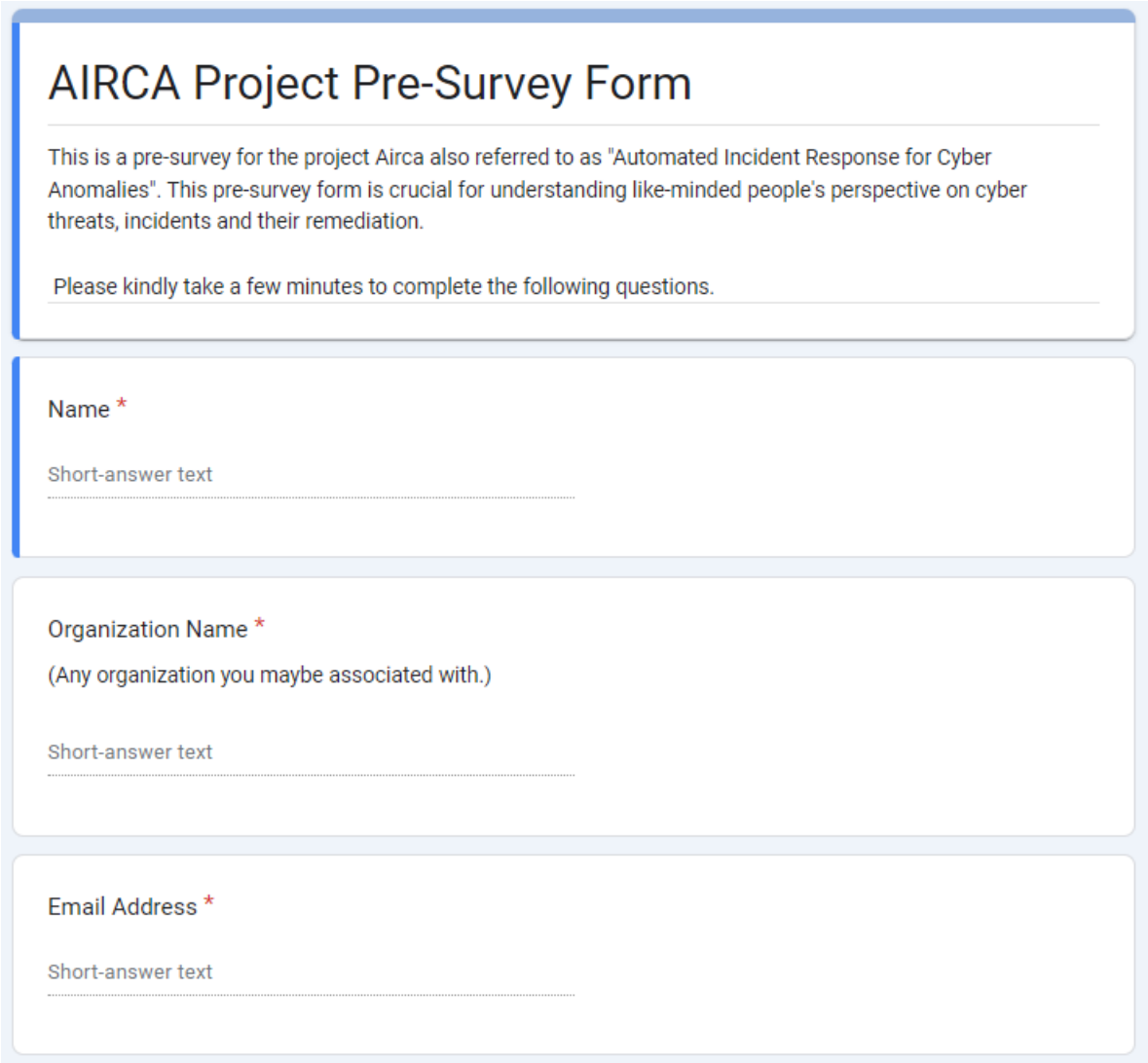

Figure 8 Pre-Survey Form : Personal Details

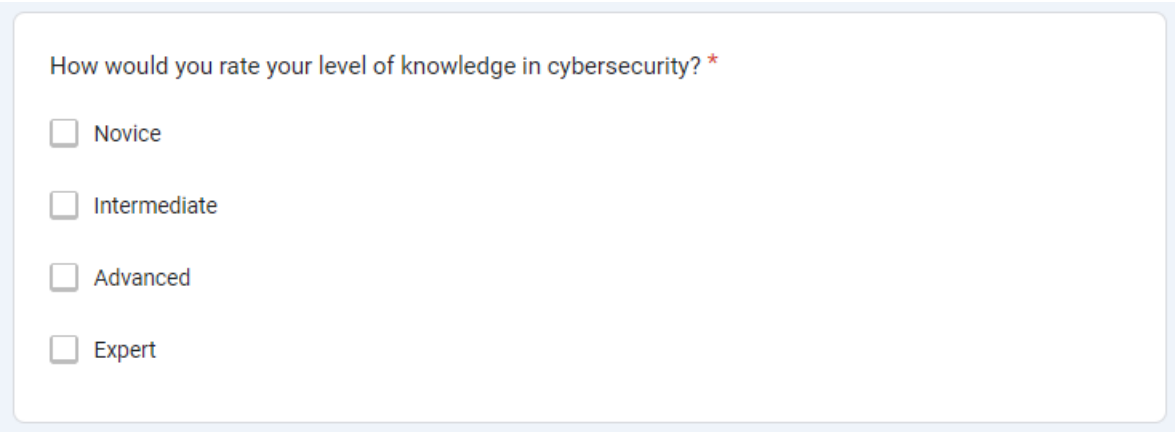

Figure 9 Pre-Survey : Question 1

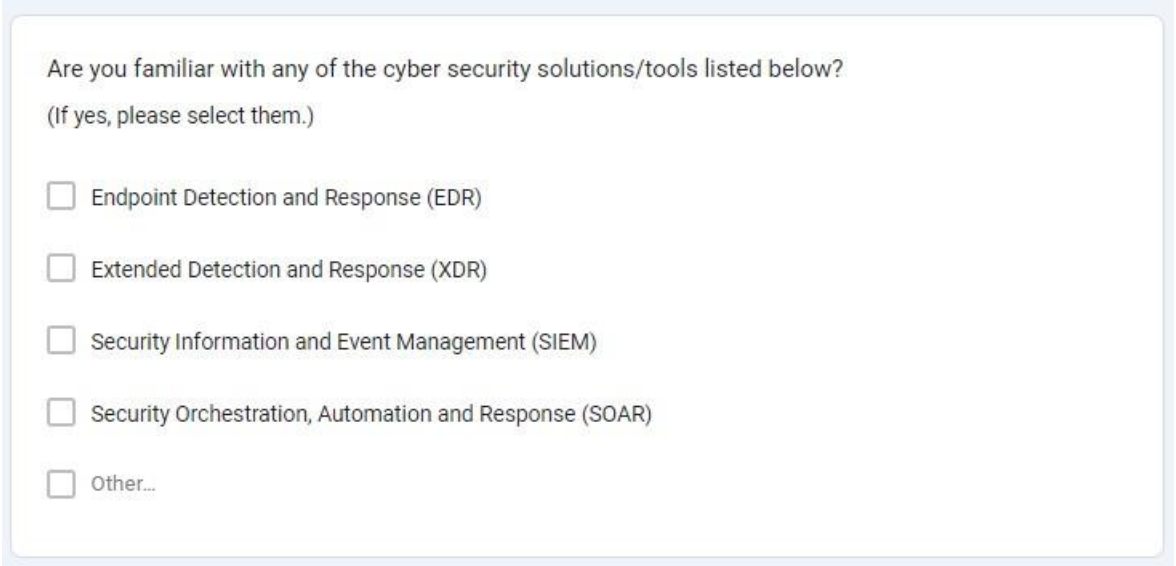

Figure 10 Pre-Survey : Question 2

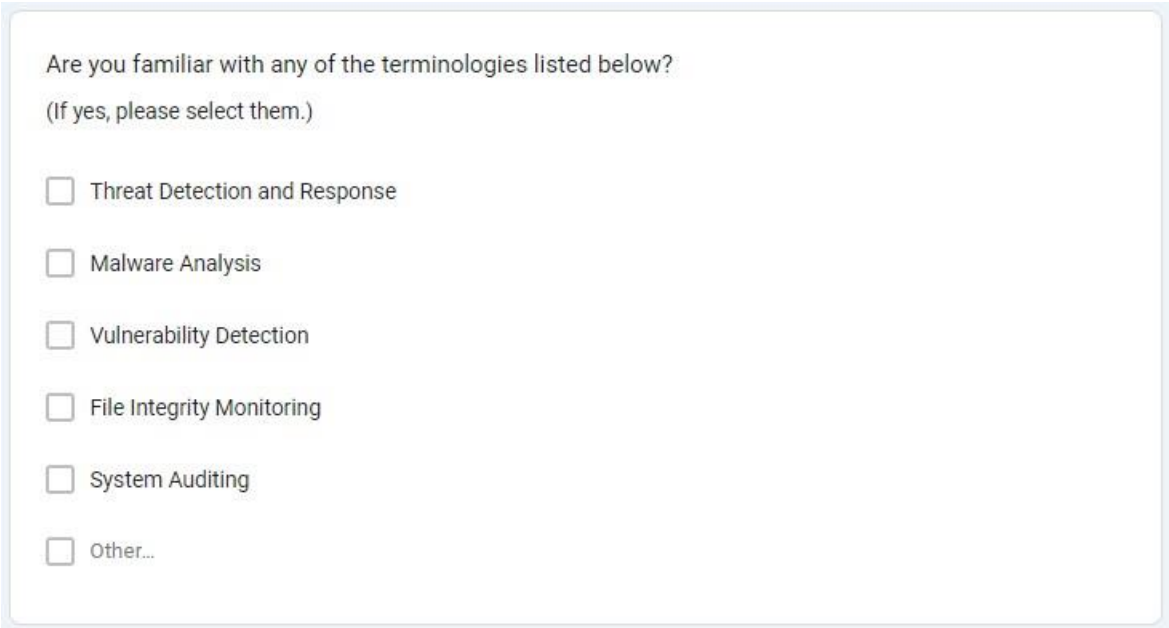

Figure 11 Pre-Survey : Question 3

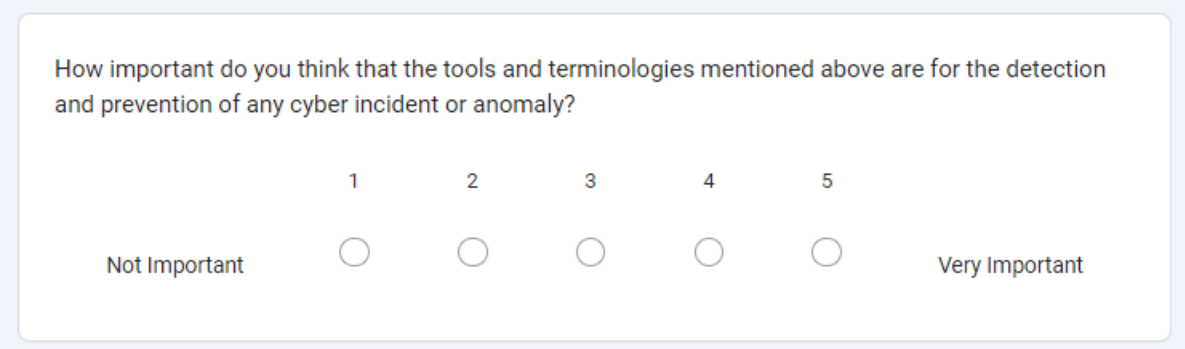

Figure 12 Pre-Survey : Question 4

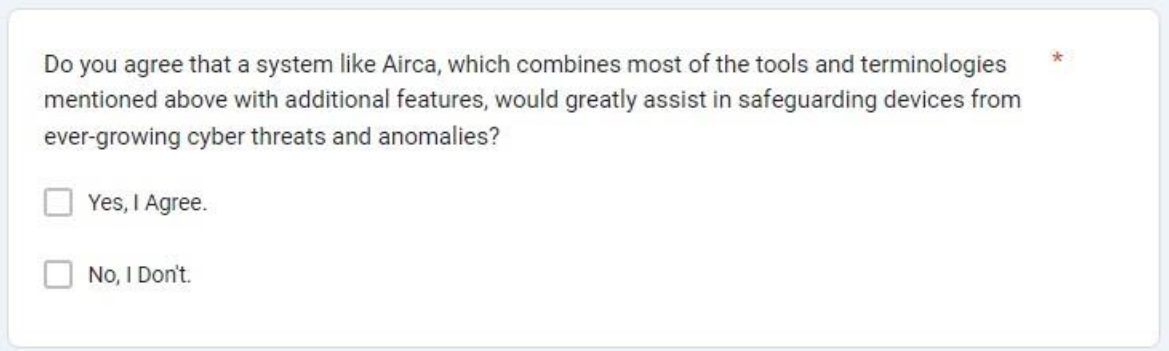

Figure 13 Pre-Survey : Question 5

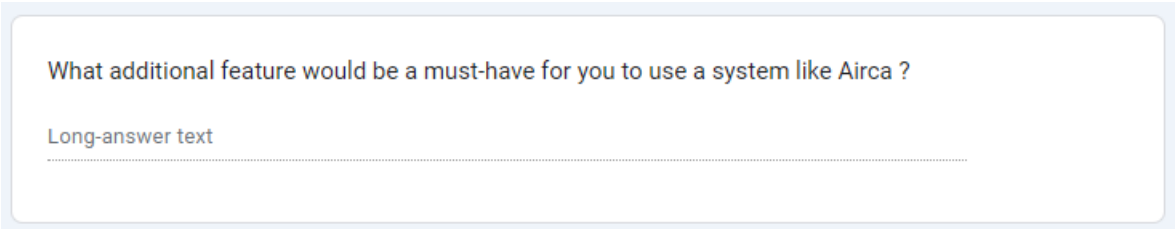

Figure 14 Pre-Survey : Question 6

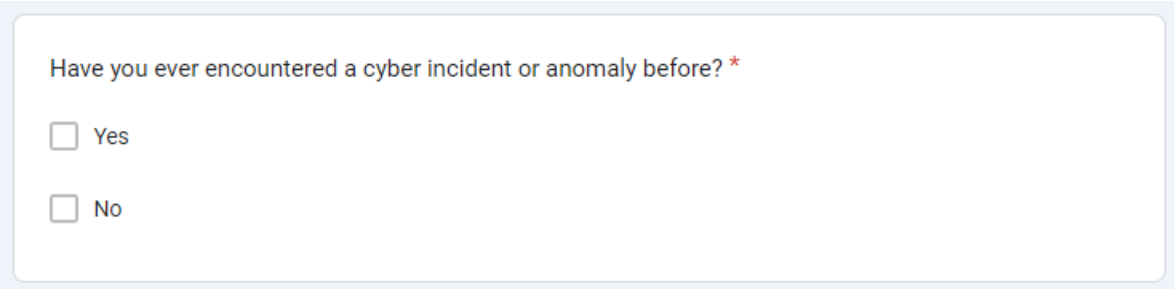

Figure 15 Pre-Survey : Question 7

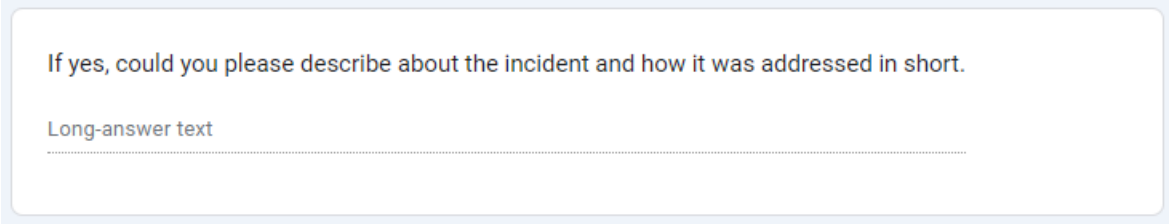

Figure 16 Pre-Survey : Question 8

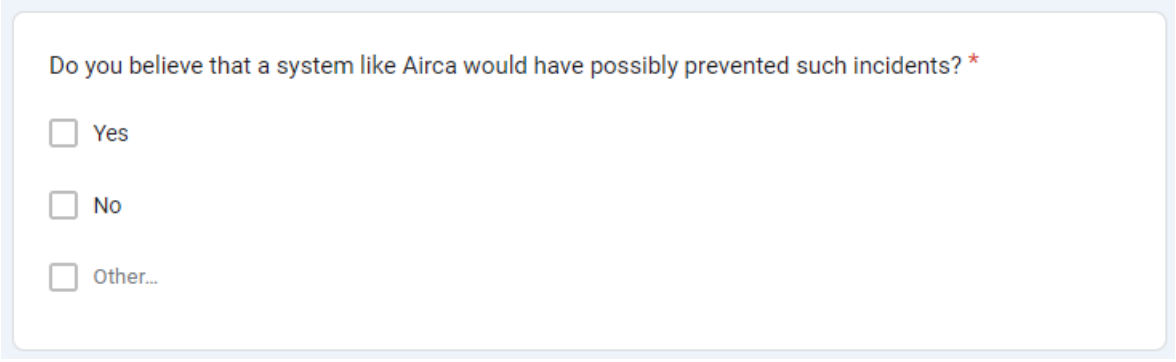

Figure 17 Pre-Survey : Question 9

Figure 18 Pre-Survey : Question 10

7.1.2. Pre-Survey Responses

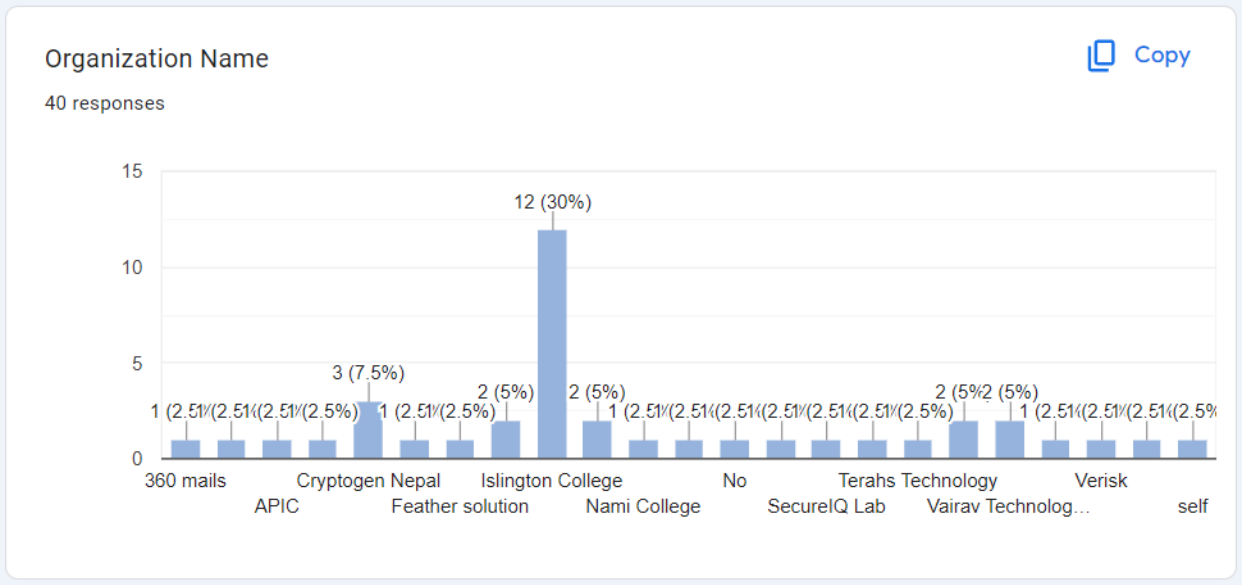

Figure 19 Pre-Survey Response : Organizations

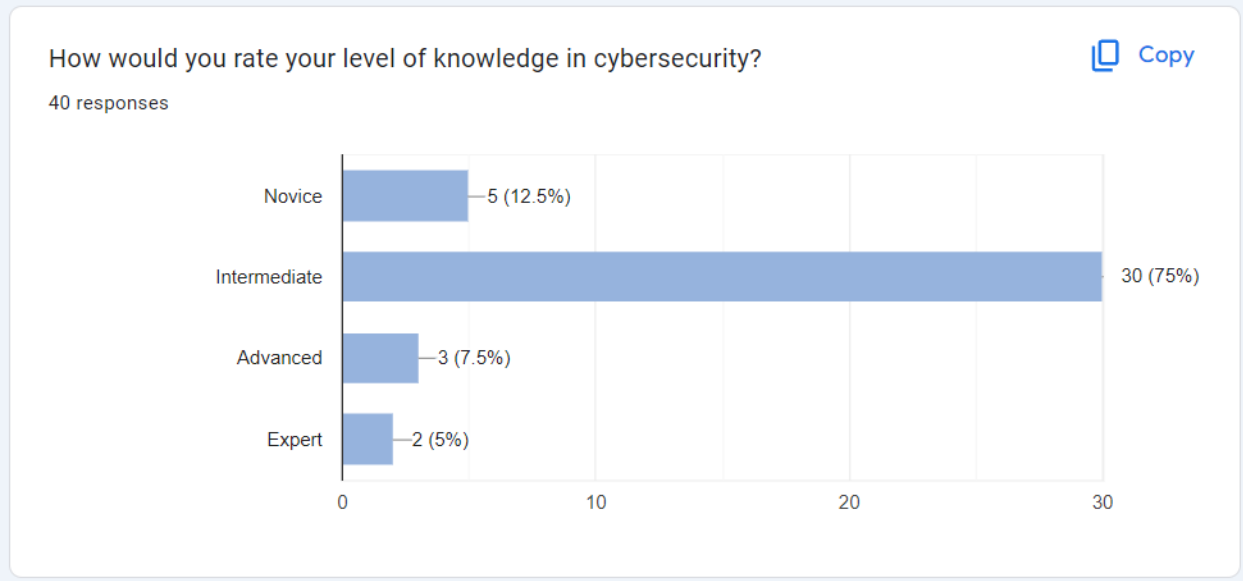

Figure 20 Pre-Survey Response : Question 1

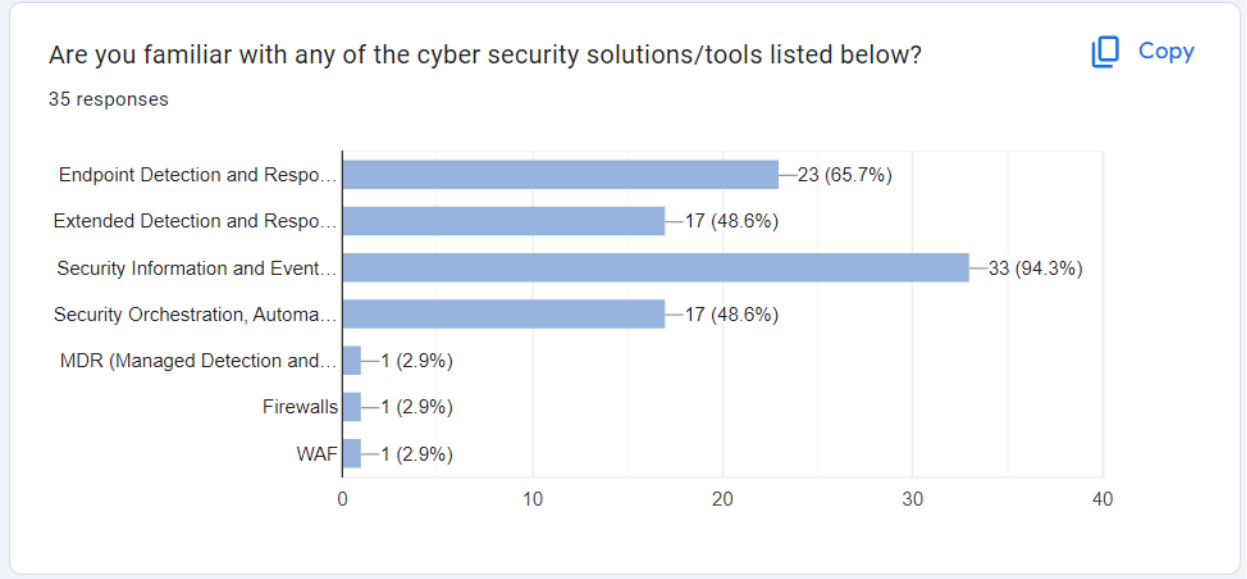

Figure 21 Pre-Survey Response : Question 2

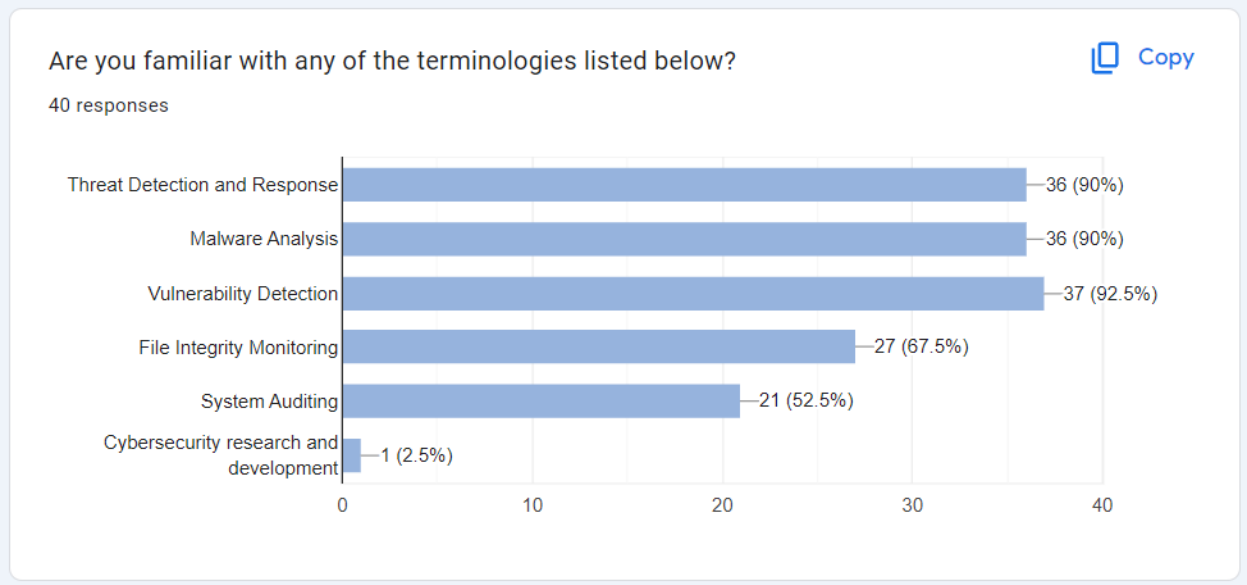

Figure 22 Pre-Survey Response : Question 3

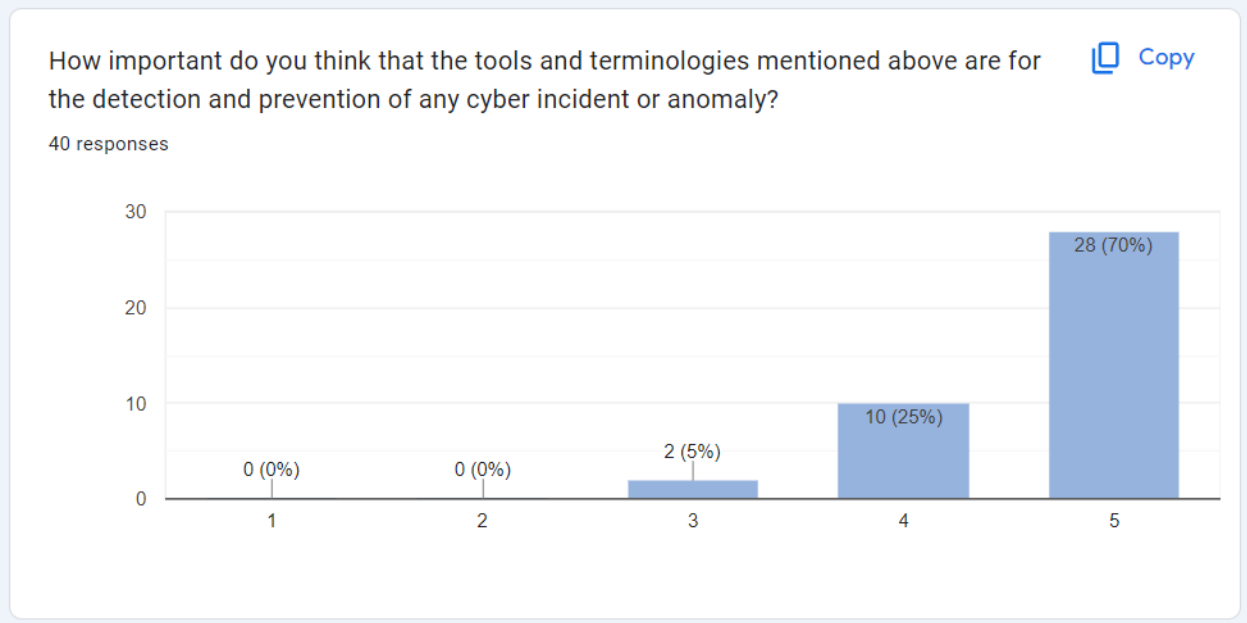

Figure 23 Pre-Survey Response : Question 4

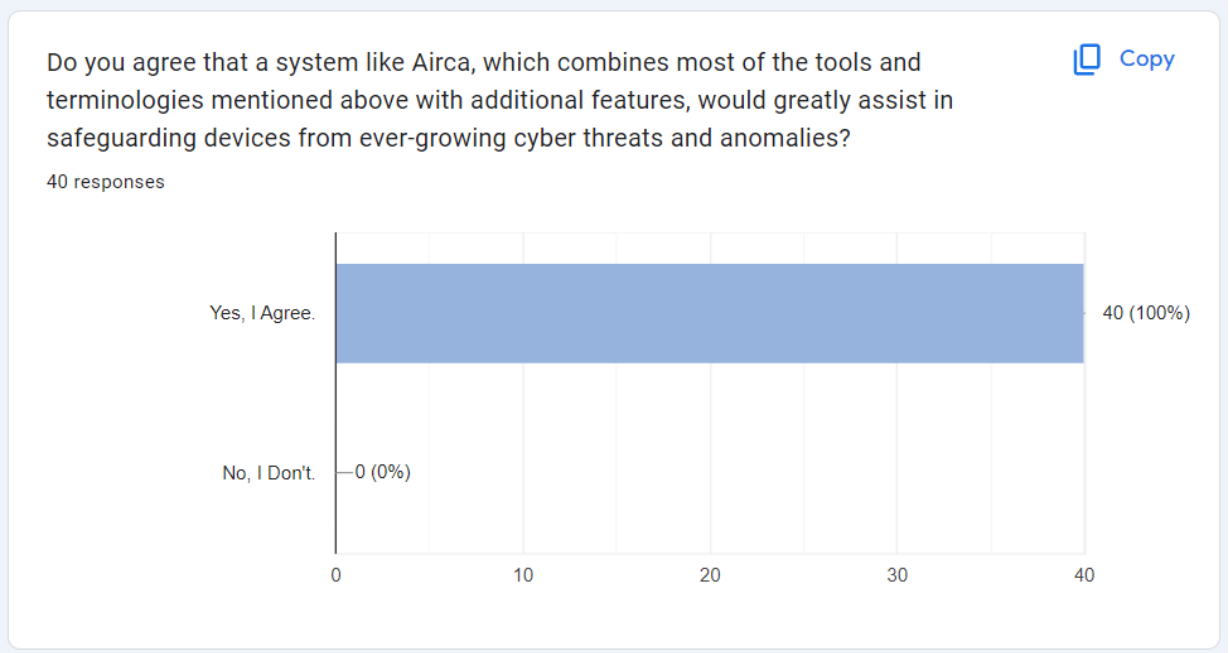

Figure 24 Pre-Survey Response : Question 5

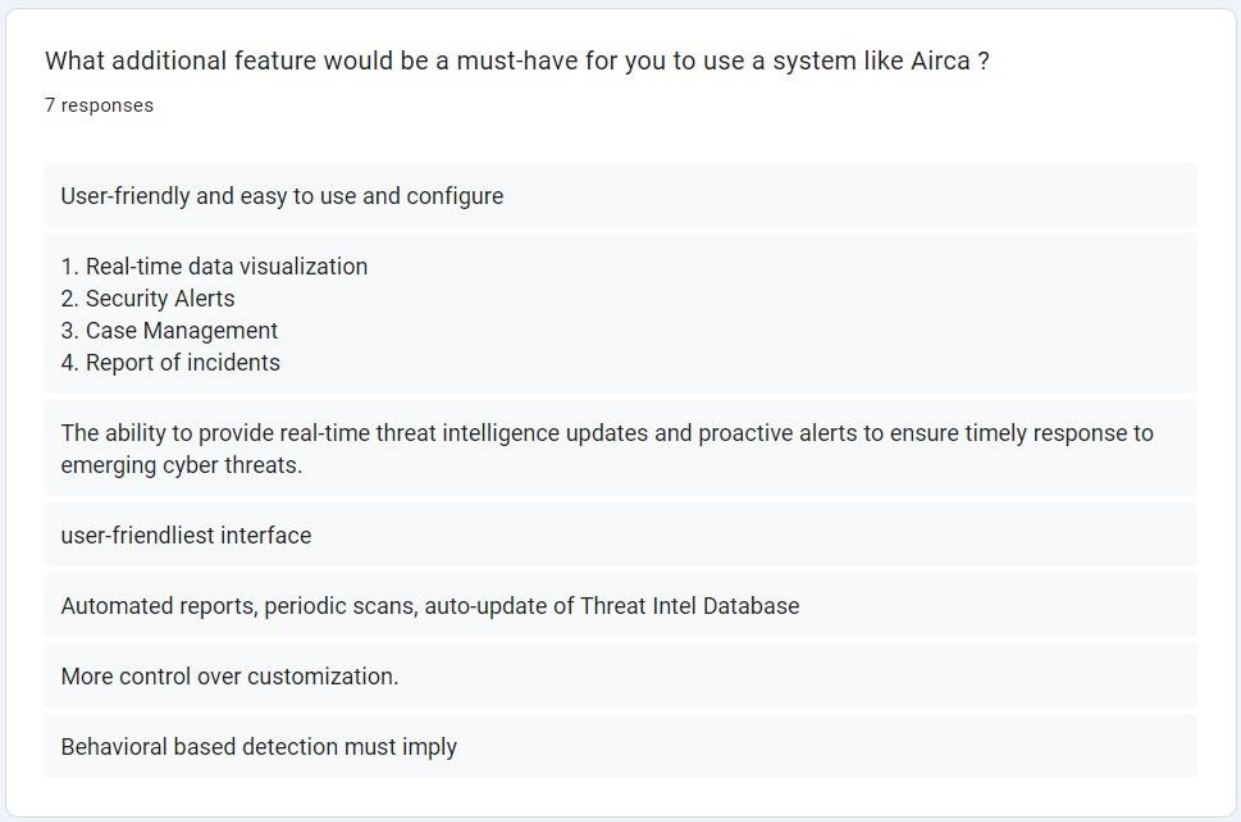

Figure 25 Pre-Survey Response : Question 6

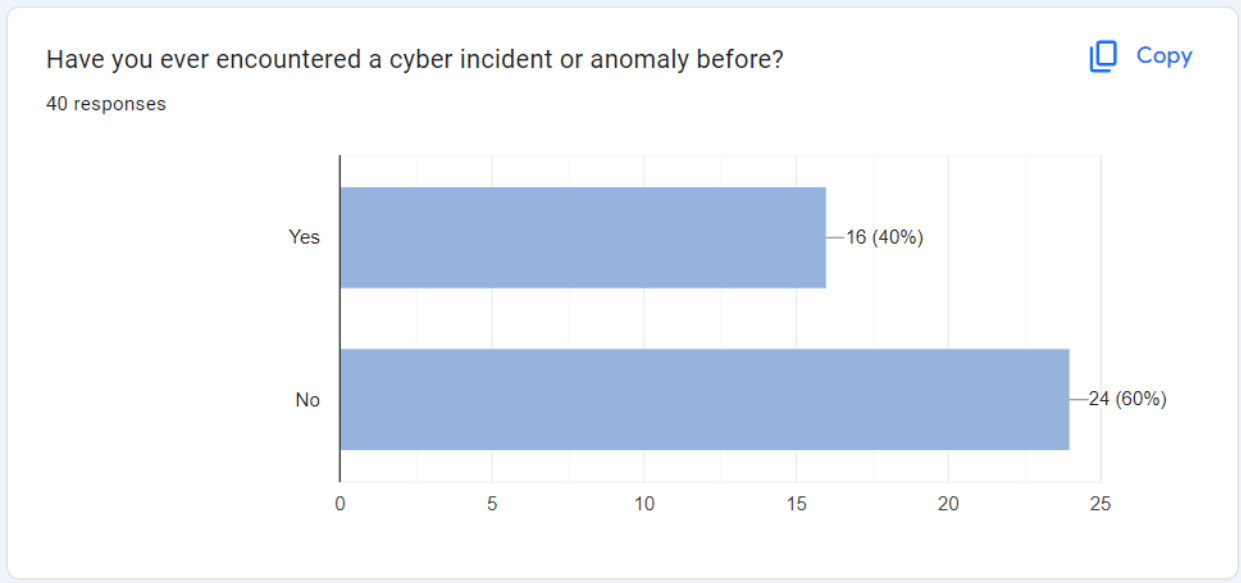

Figure 26 Pre-Survey Response : Question 7

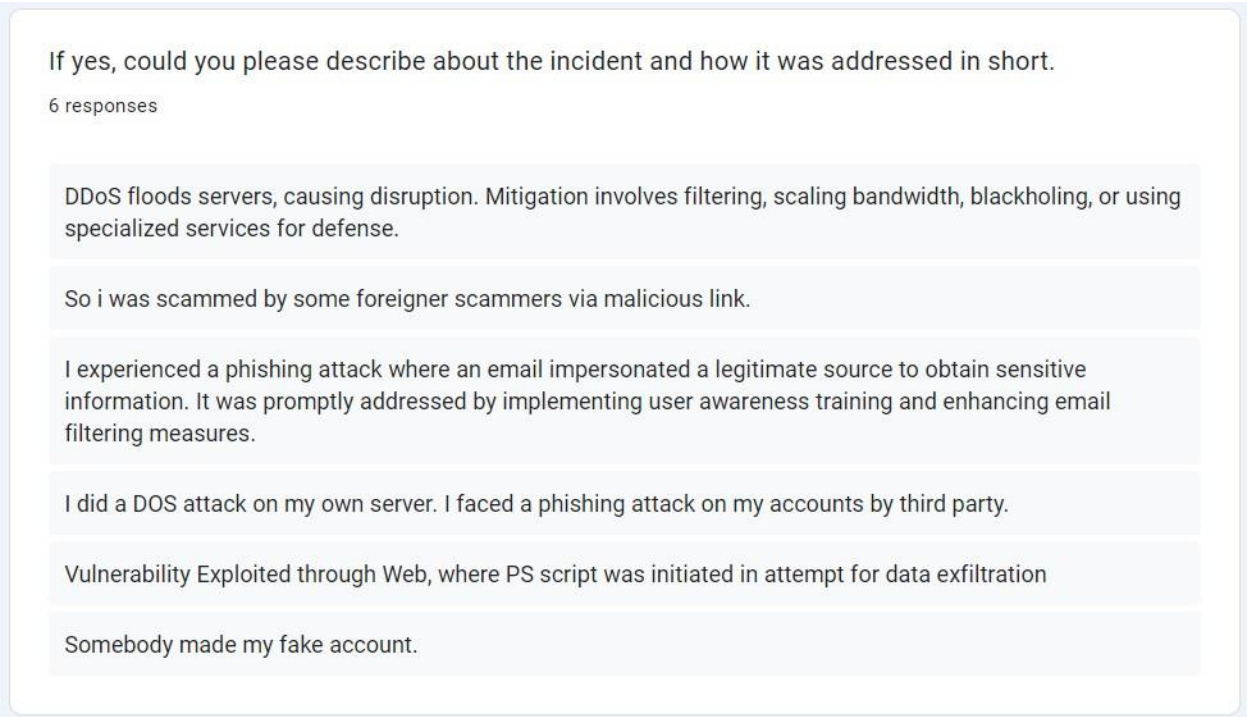

Figure 27 Pre-Survey Response : Question 8

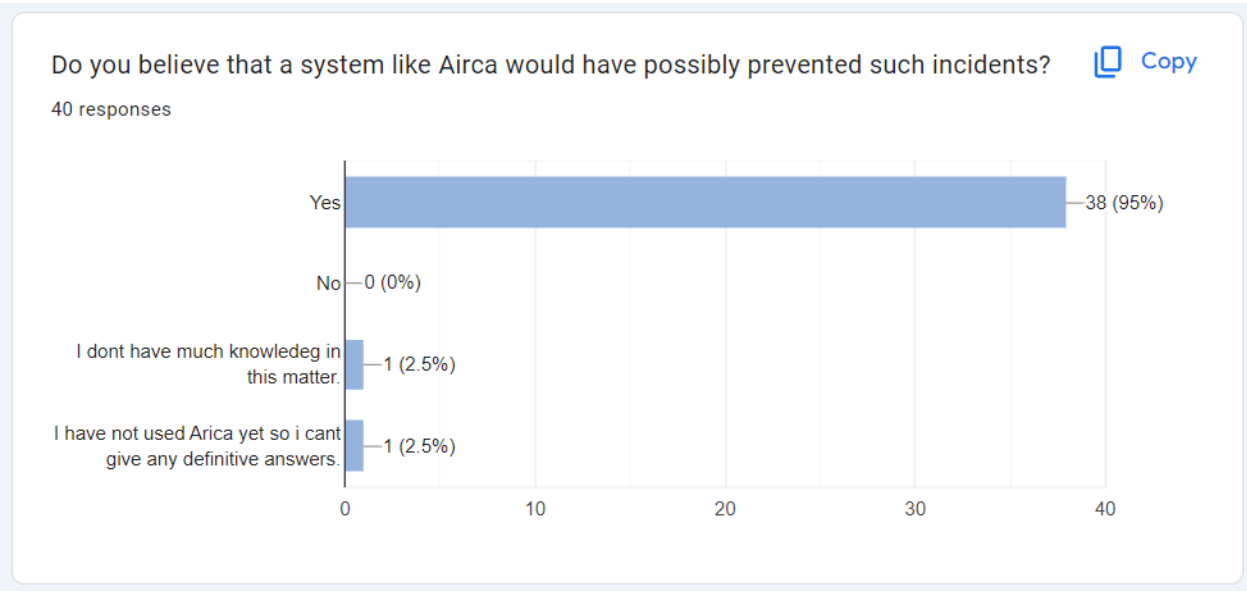

Figure 28 Pre-Survey Response : Question 9

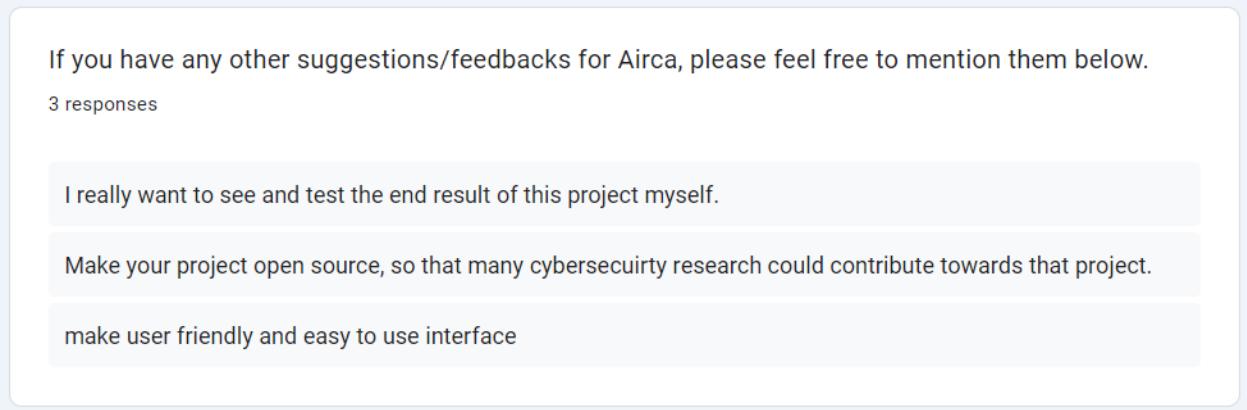

Figure 29 Pre-Survey Response : Question 10

7.2. System Deployment and Development Progresses

7.2.1. Machines Resource Information

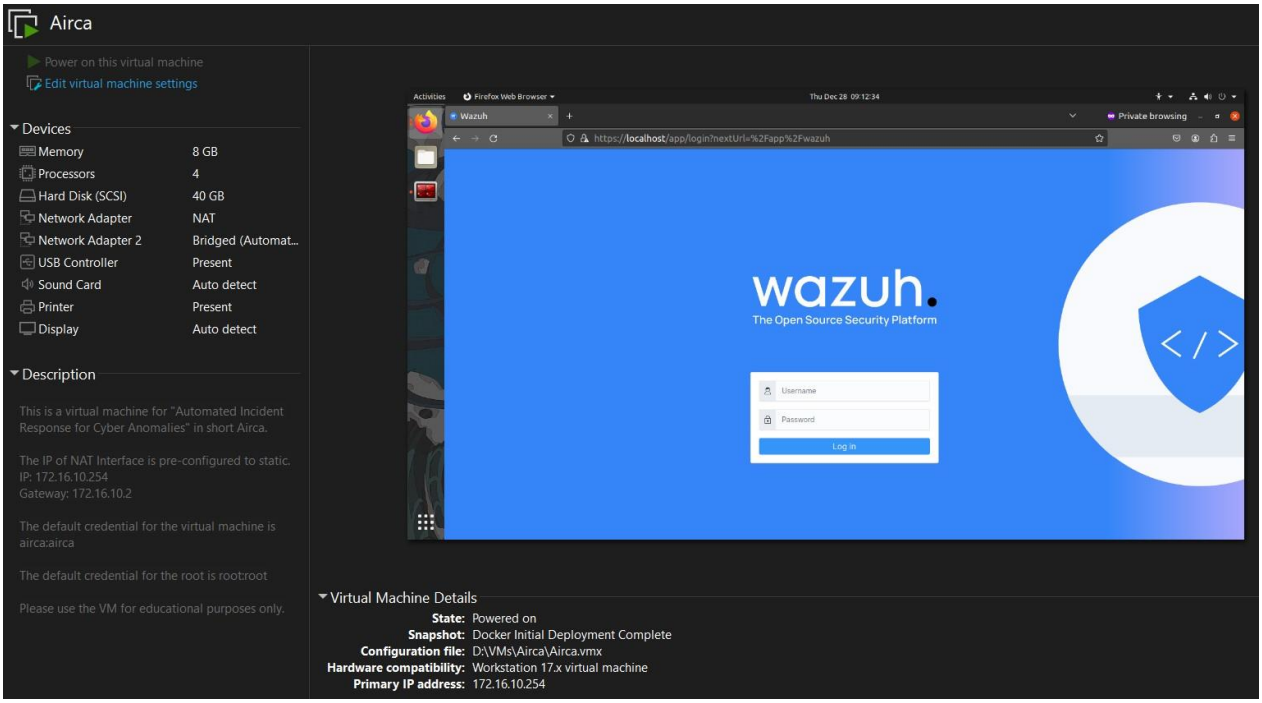

Figure 30 AIRCA's Machine Information

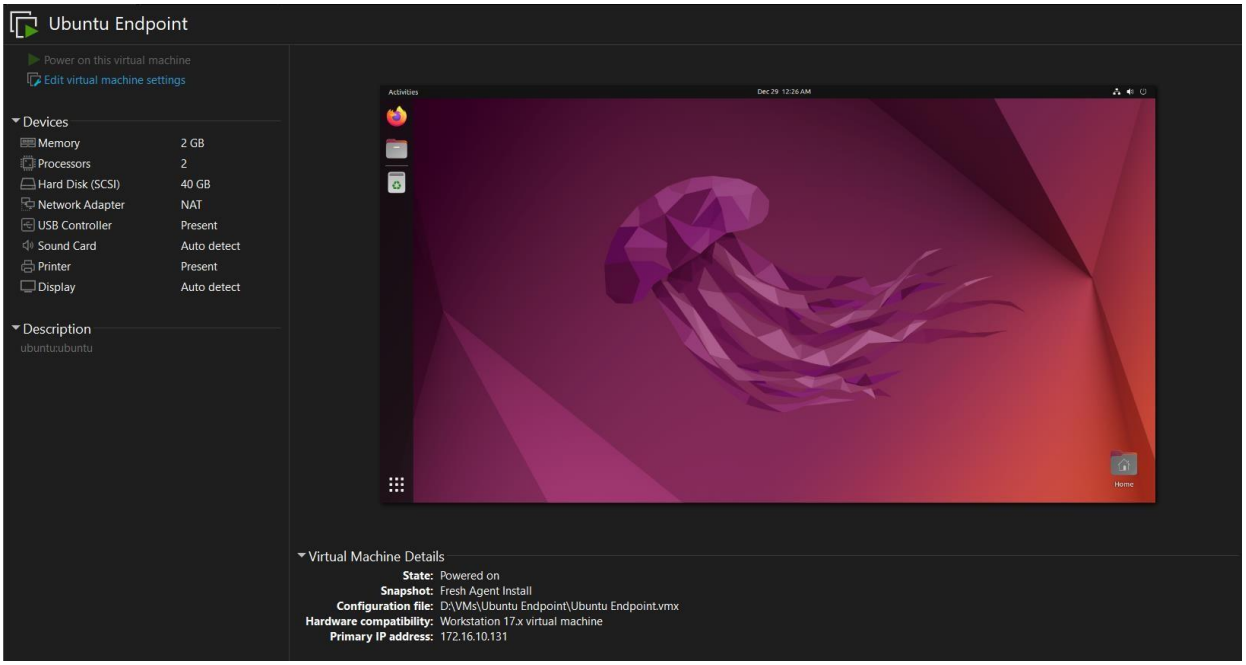

Figure 31 Ubuntu Endpoint's Information

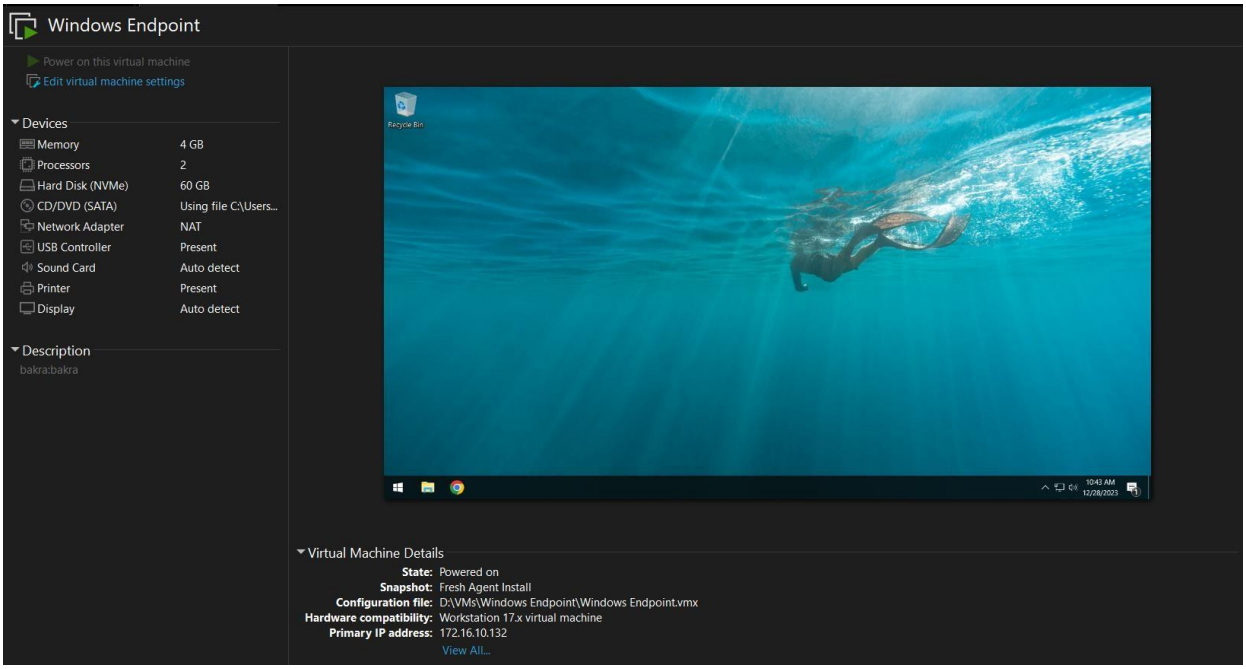

Figure 32 Windows Endpoint's Information

7.2.2. Docker Installation and Verification

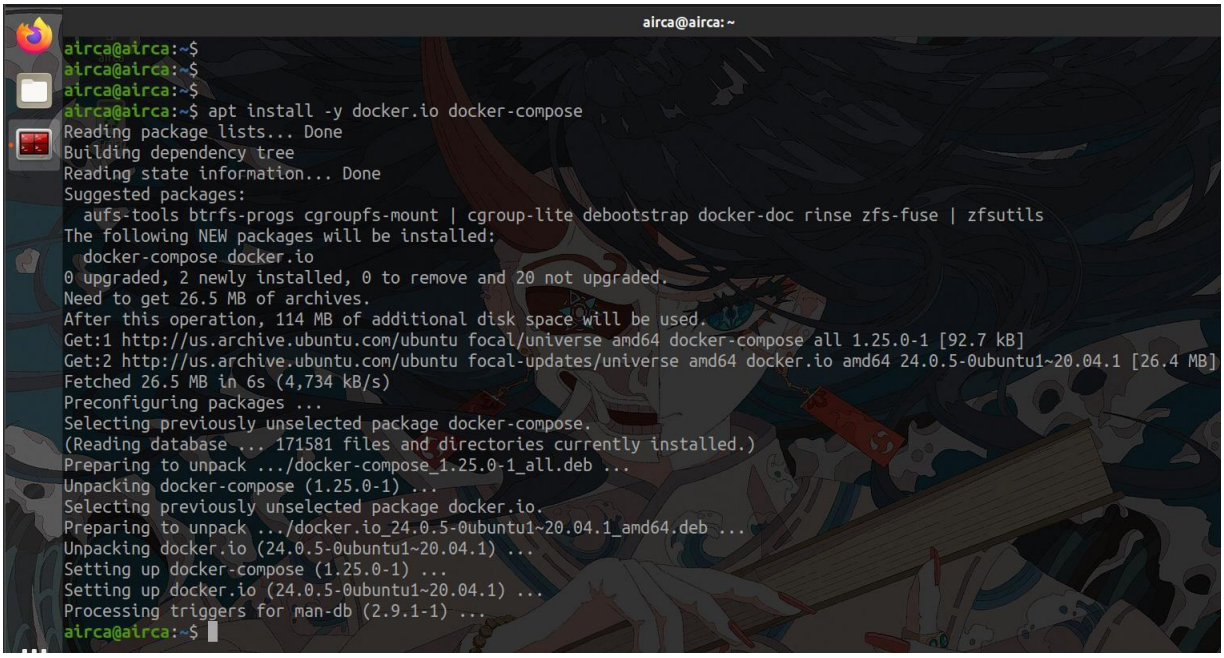

Figure 33 Installing docker and docker-compose

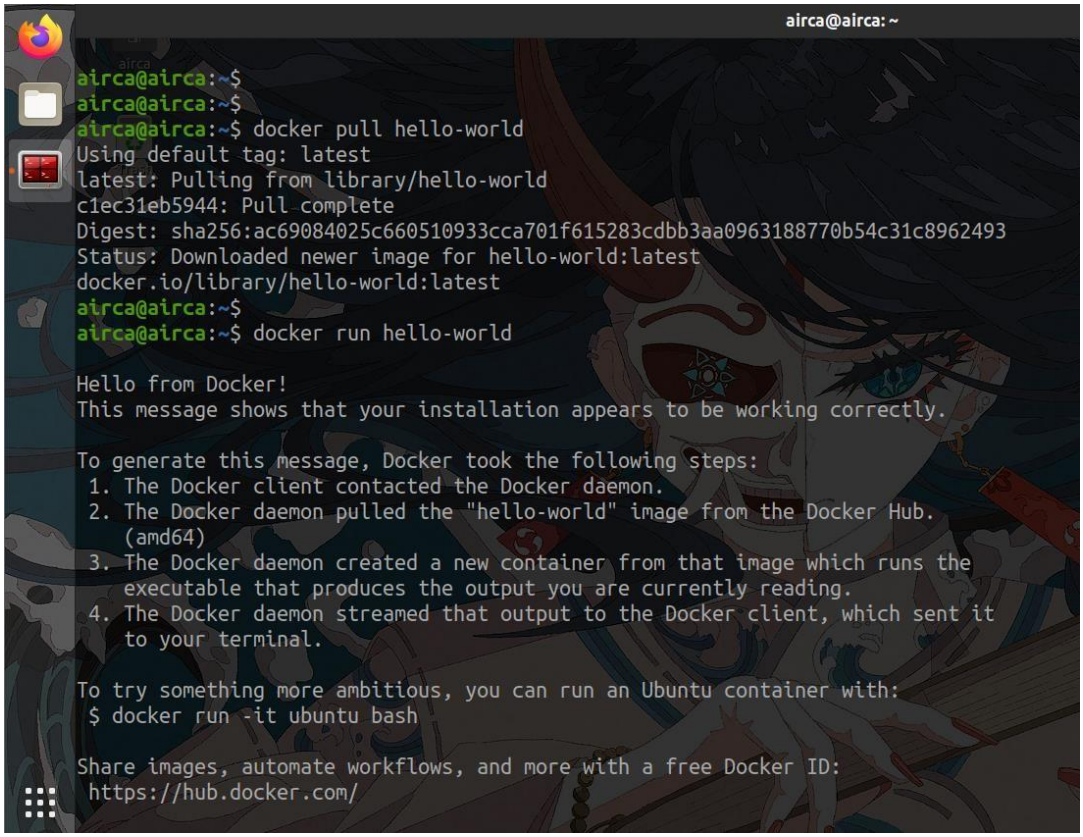

Figure 34 Verifying installation of docker

7.2.3. Wazuh Installation and Dashboard Overview

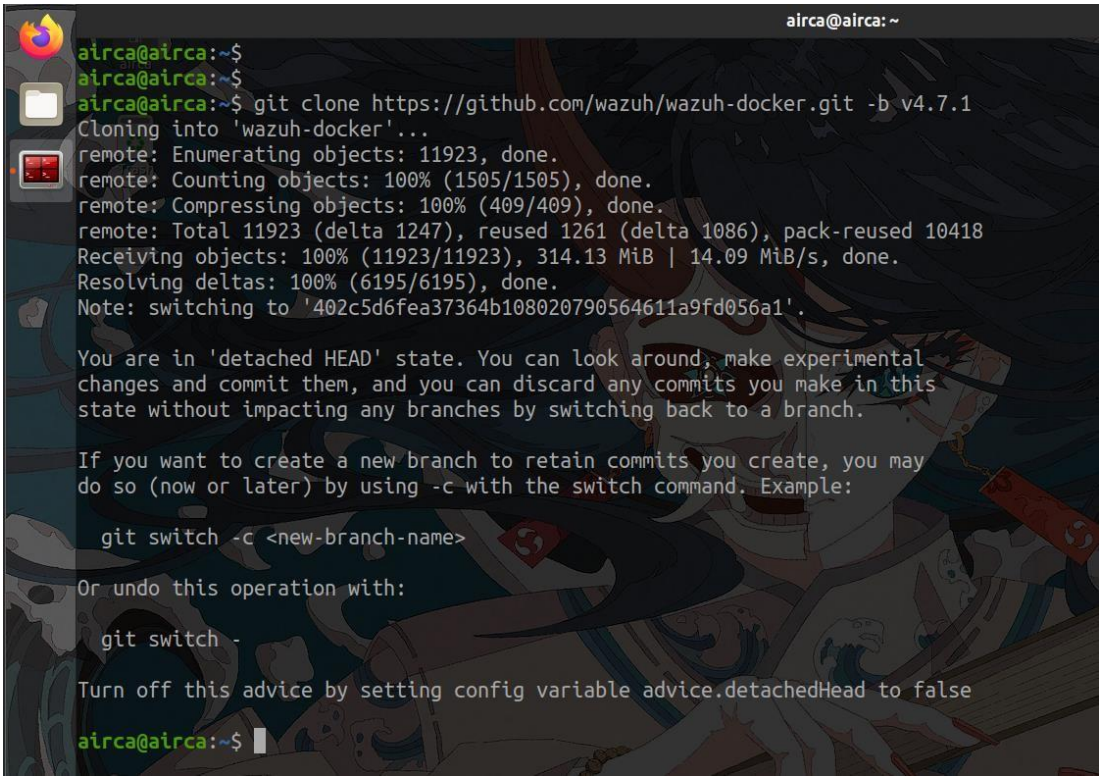

Figure 35 Cloning wazuh-docker repository

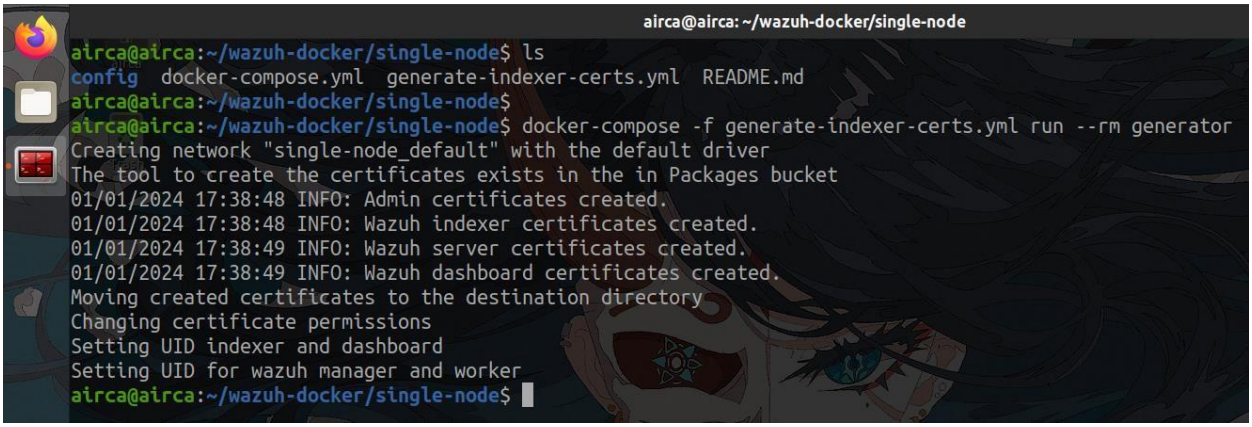

Figure 36 Generating certificates for Wazuh indexer, server, and dashboard

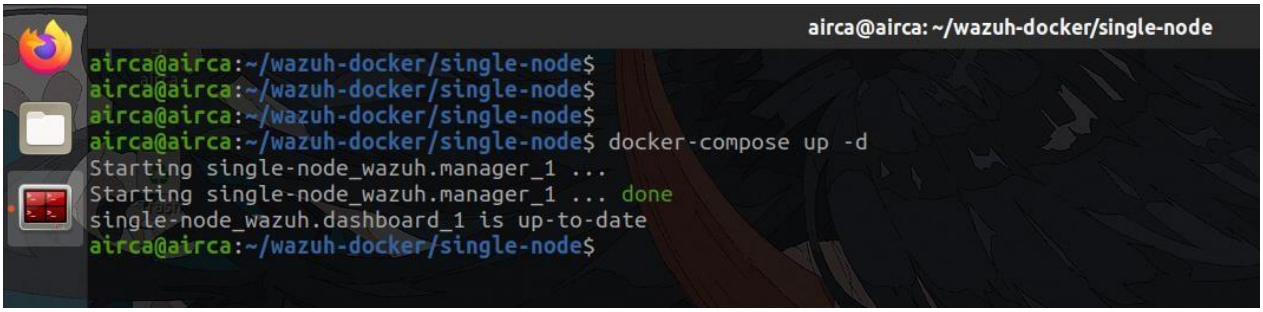

Figure 37 Starting Wazuh via docker-compose

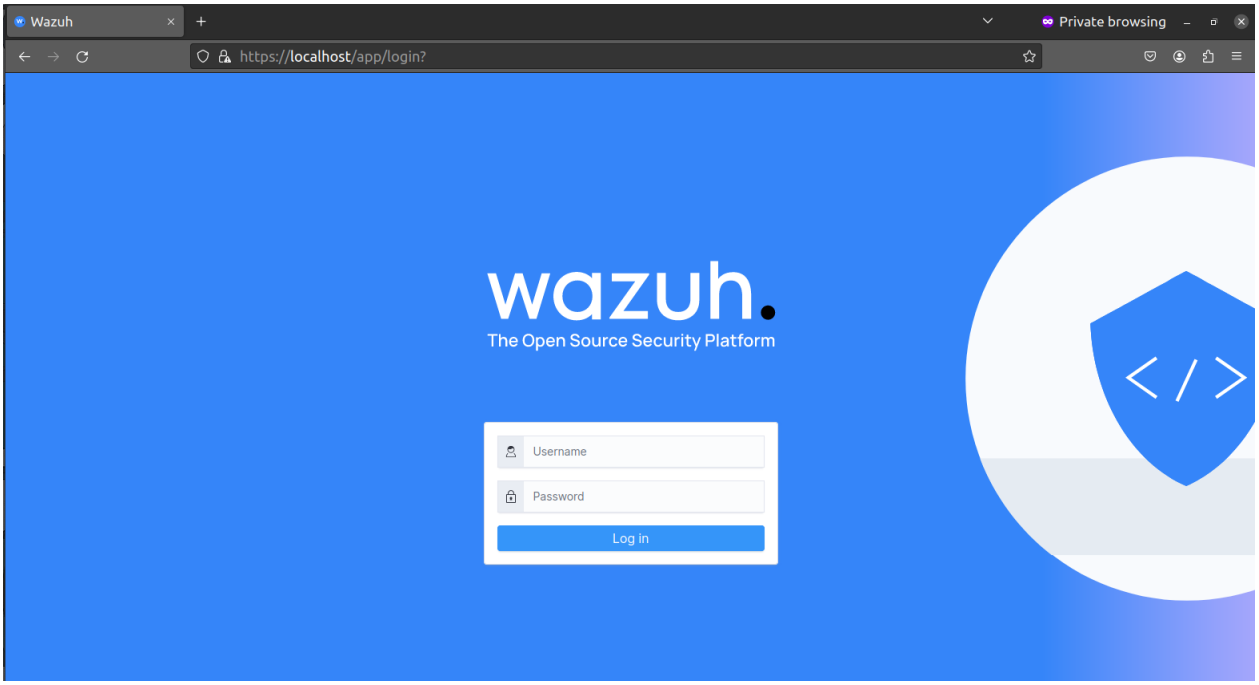

Figure 38 Navigating Wazuh Login Page

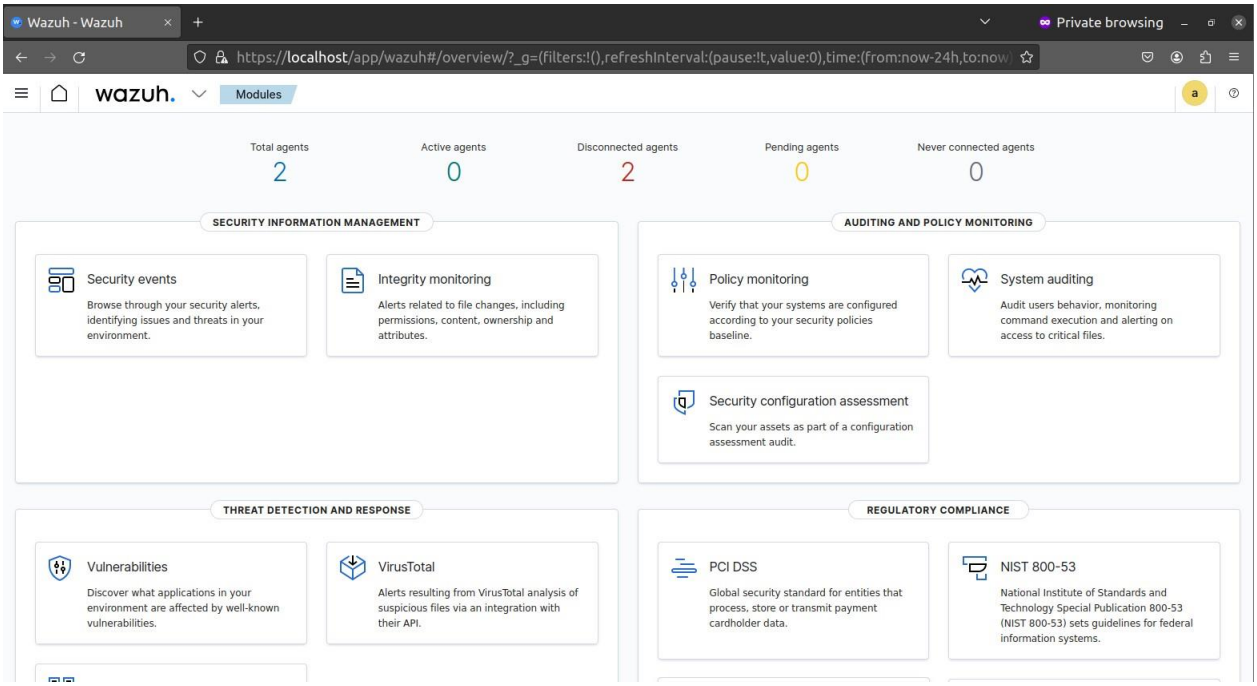

Figure 39 Wazuh Modules Overview

7.2.4. MISP Installation and Dashboard Overview

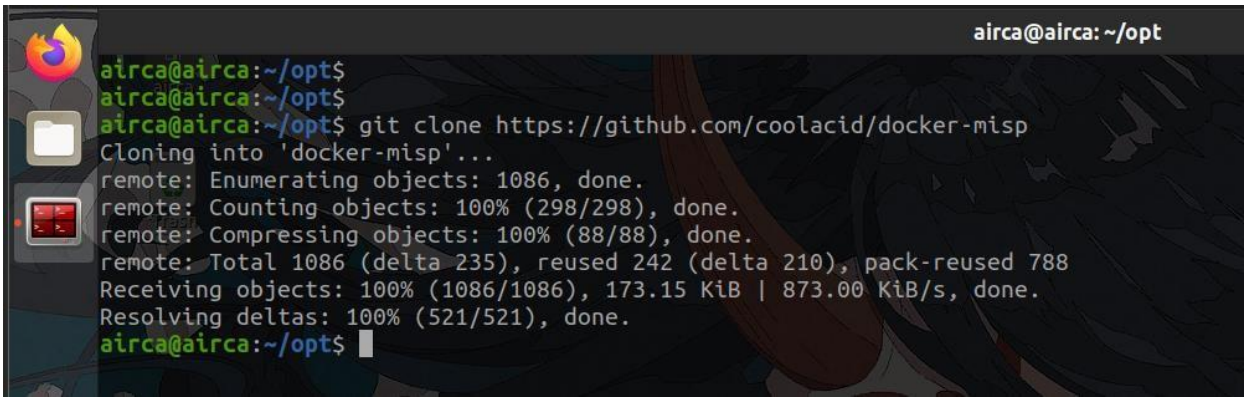

Figure 40 Cloning docker-misp repository

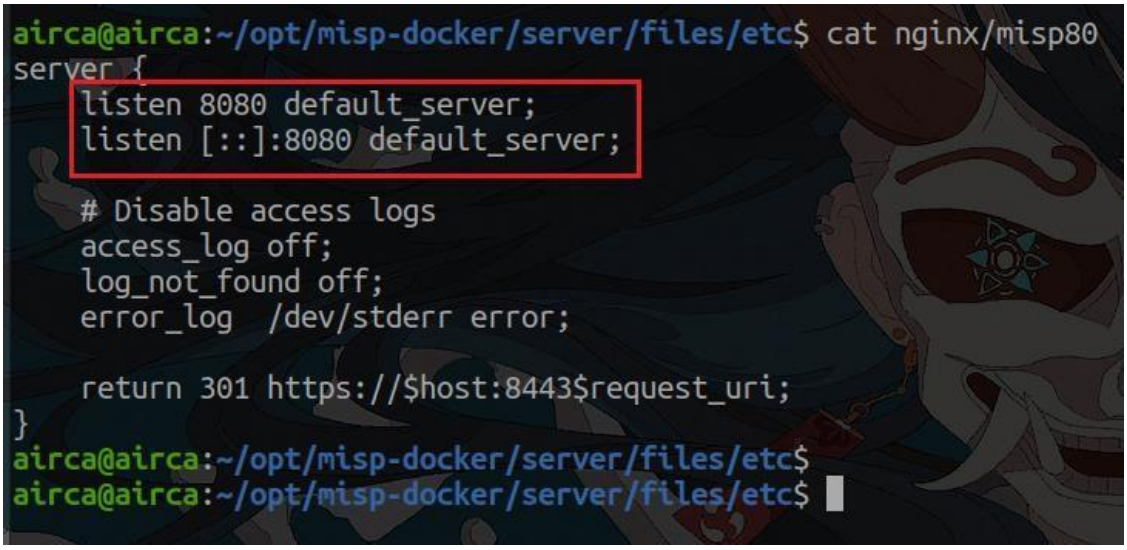

Figure 41 Changing MISP http port to 8080

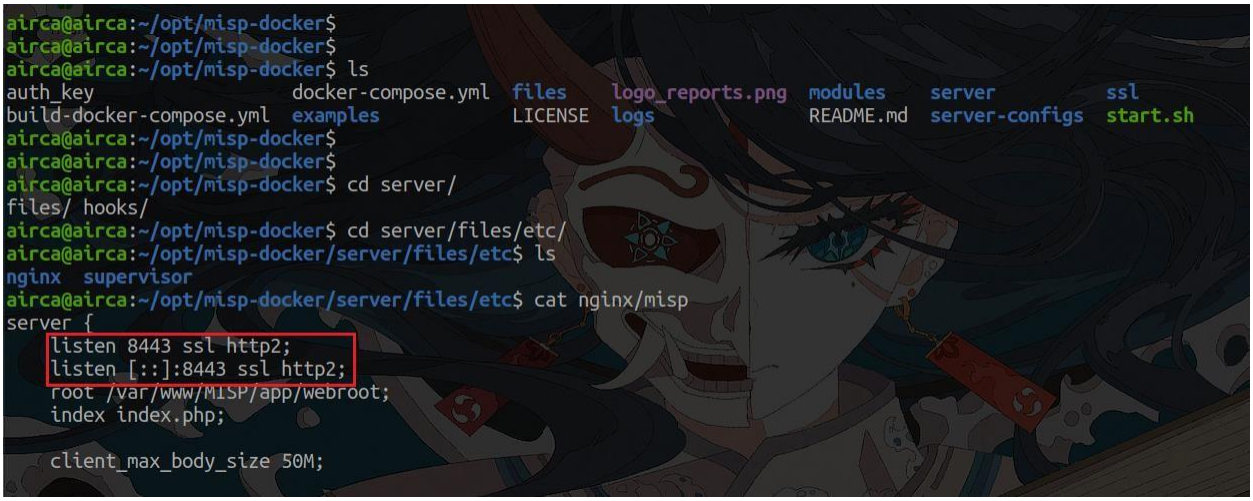

Figure 42 Changing MISP https port to 8443

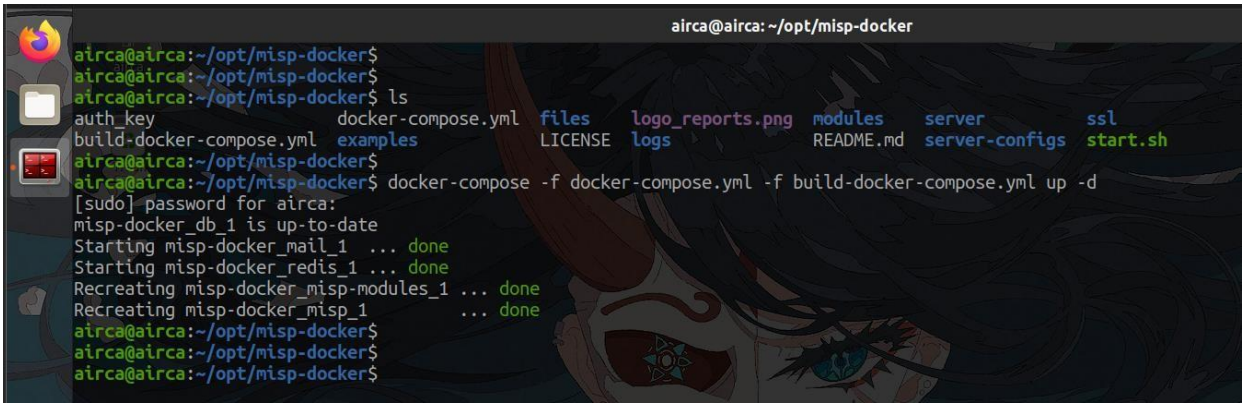

Figure 43 Starting MISP via docker-compose

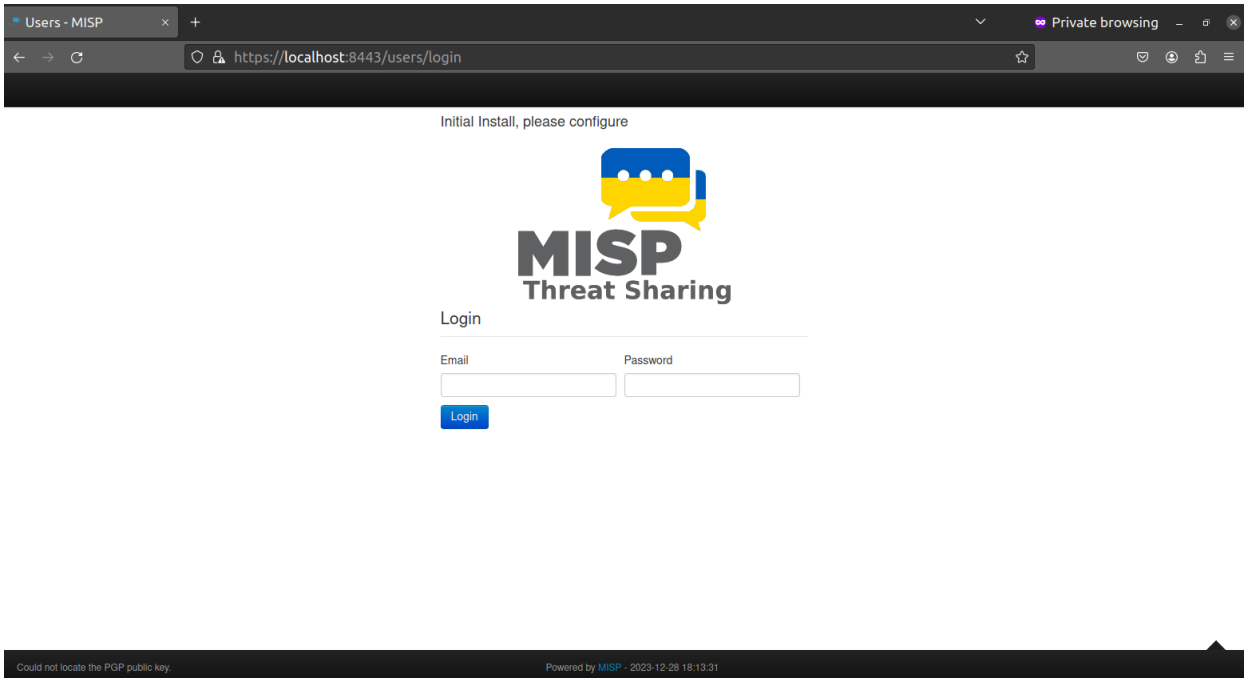

Figure 44 Navigating MISP Login Page

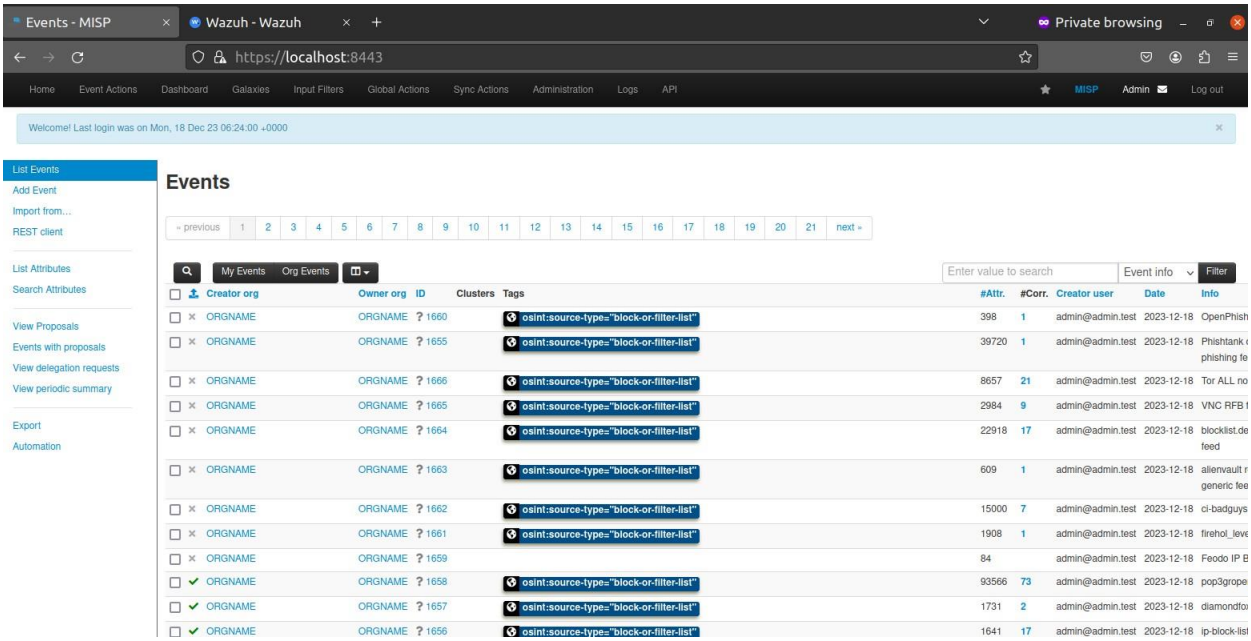

Figure 45 MISP Events

7.2.5. Agent Installation Process for Windows Endpoint

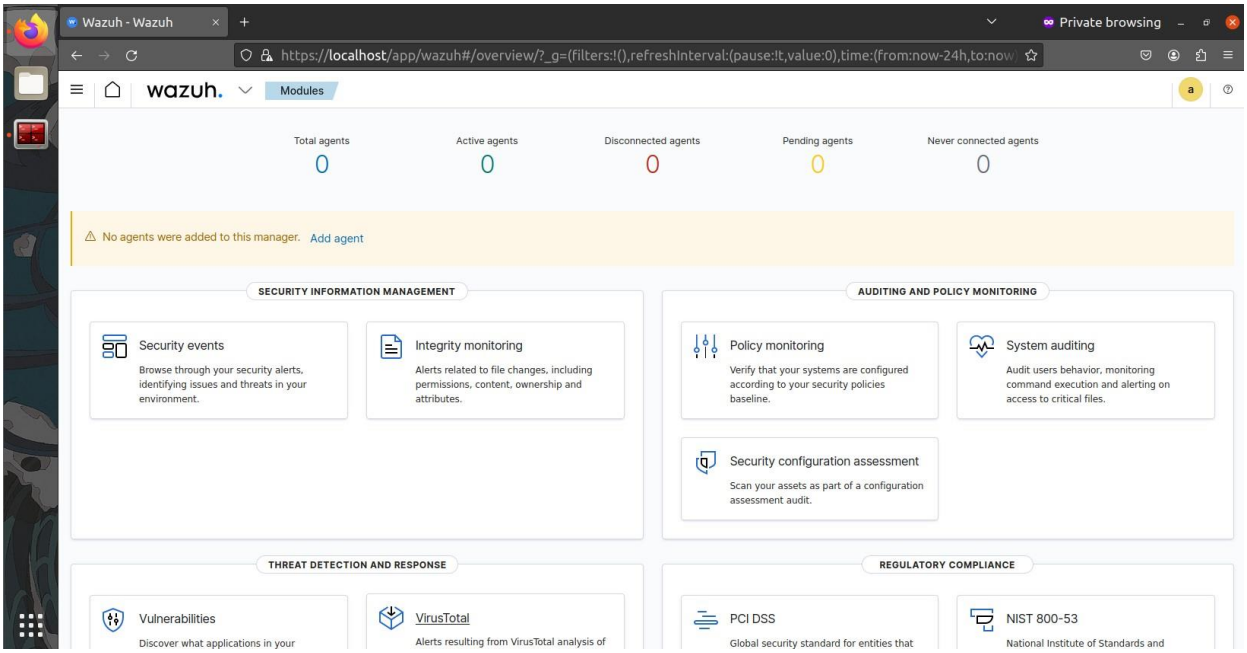

Figure 46 Adding an agent

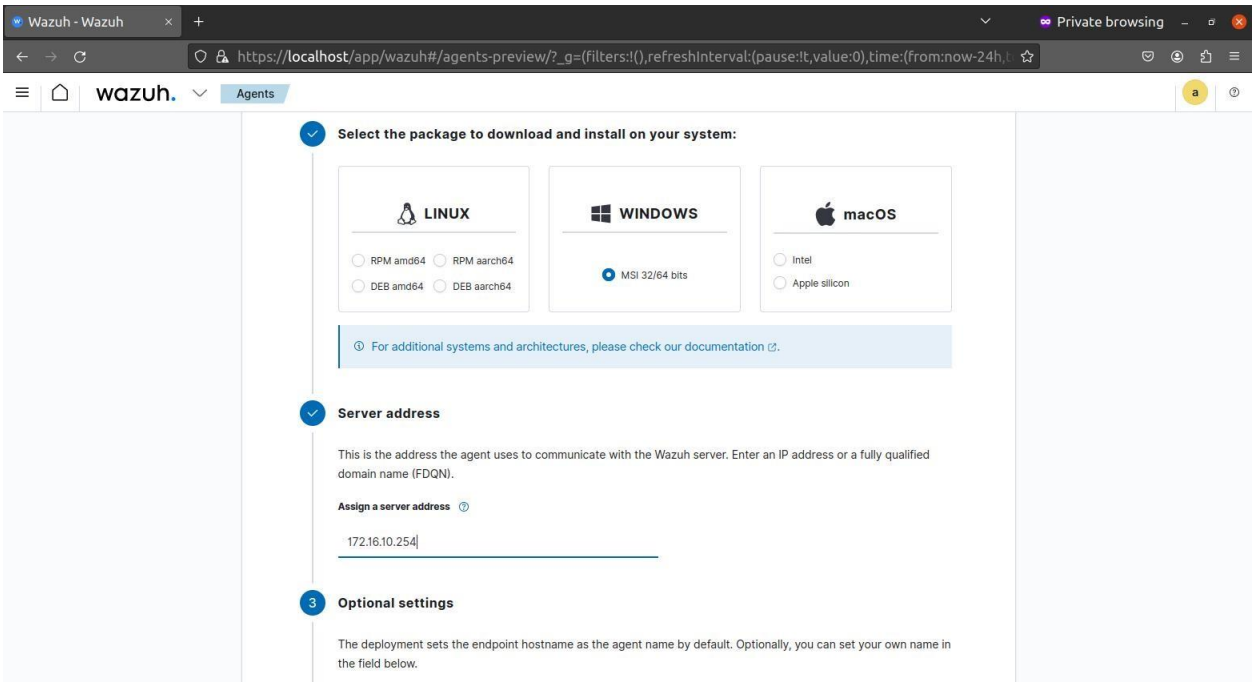

Figure 47 Setting up server address for windows agent

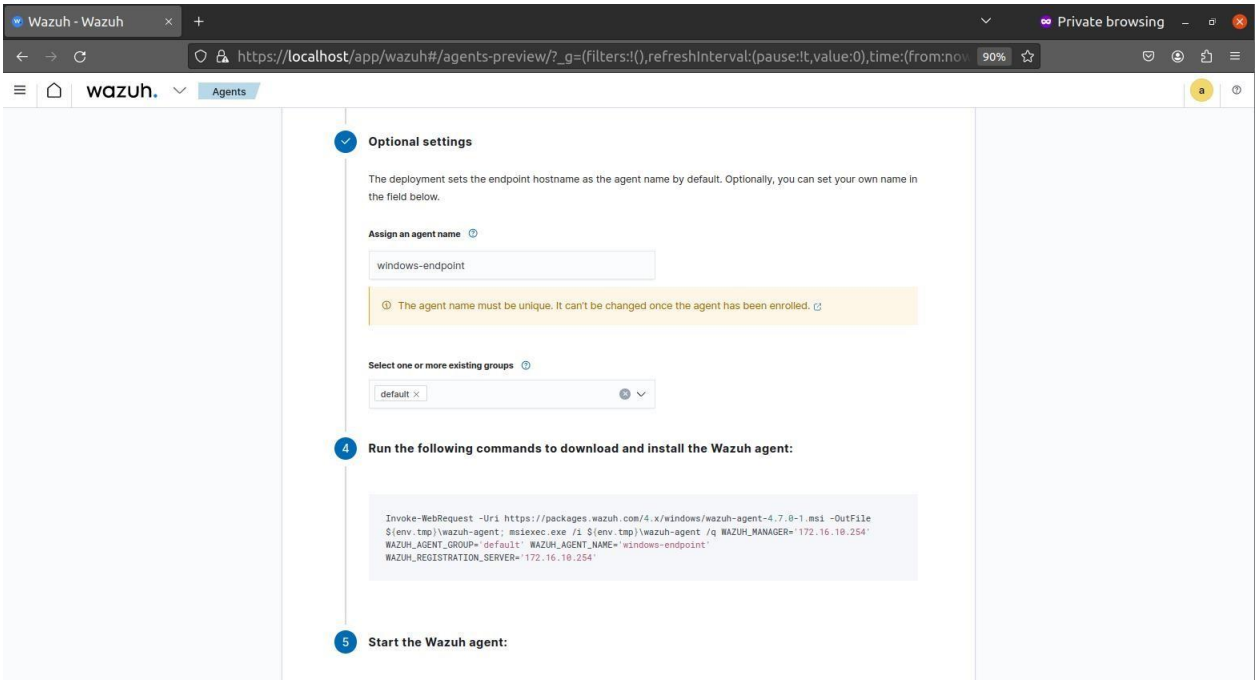

Figure 48 Assigning name to windows agent

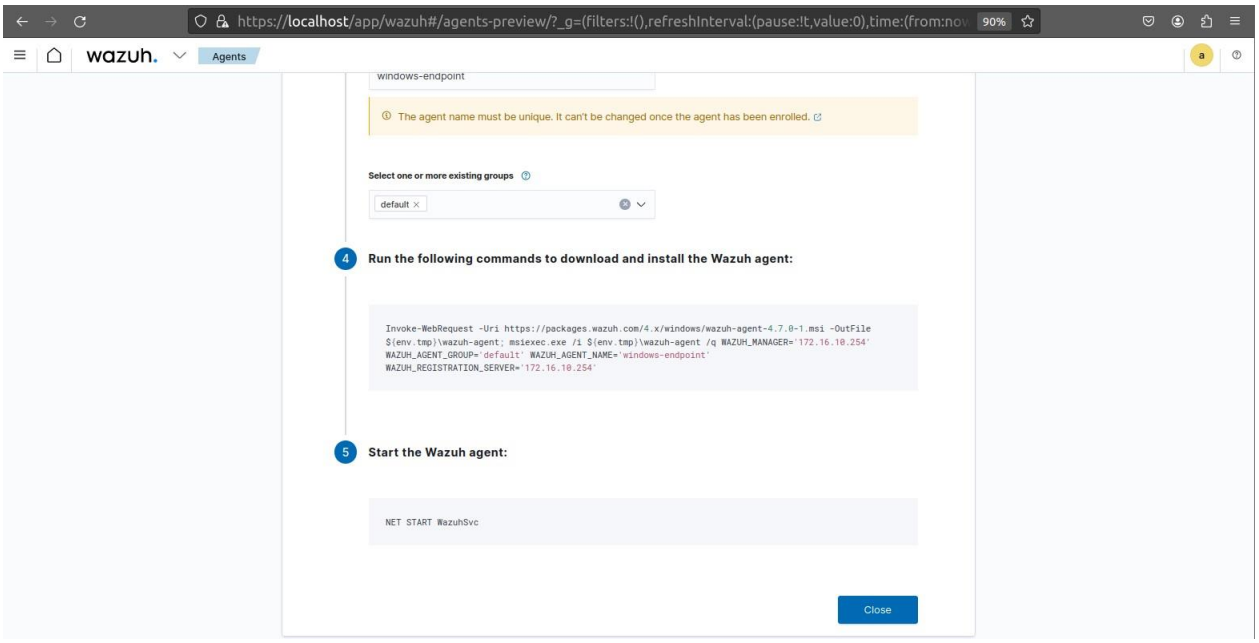

Figure 49 Commands to download, install and start the windows agent

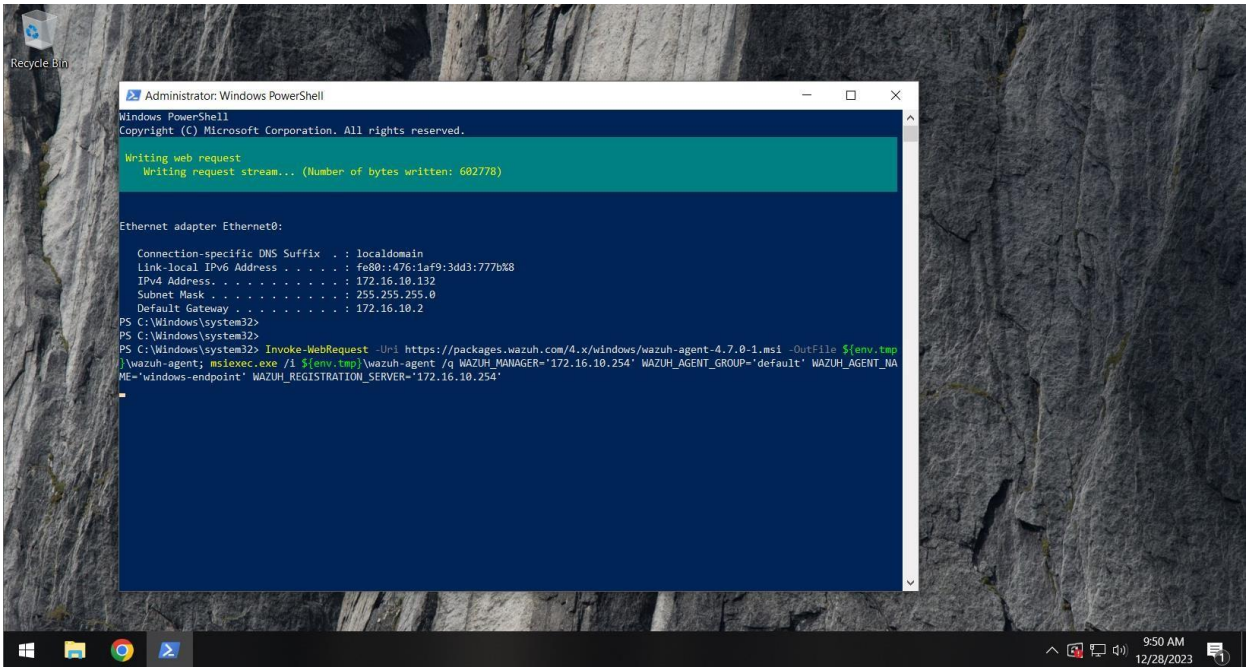

Figure 50 Running the command to download and install the windows agent

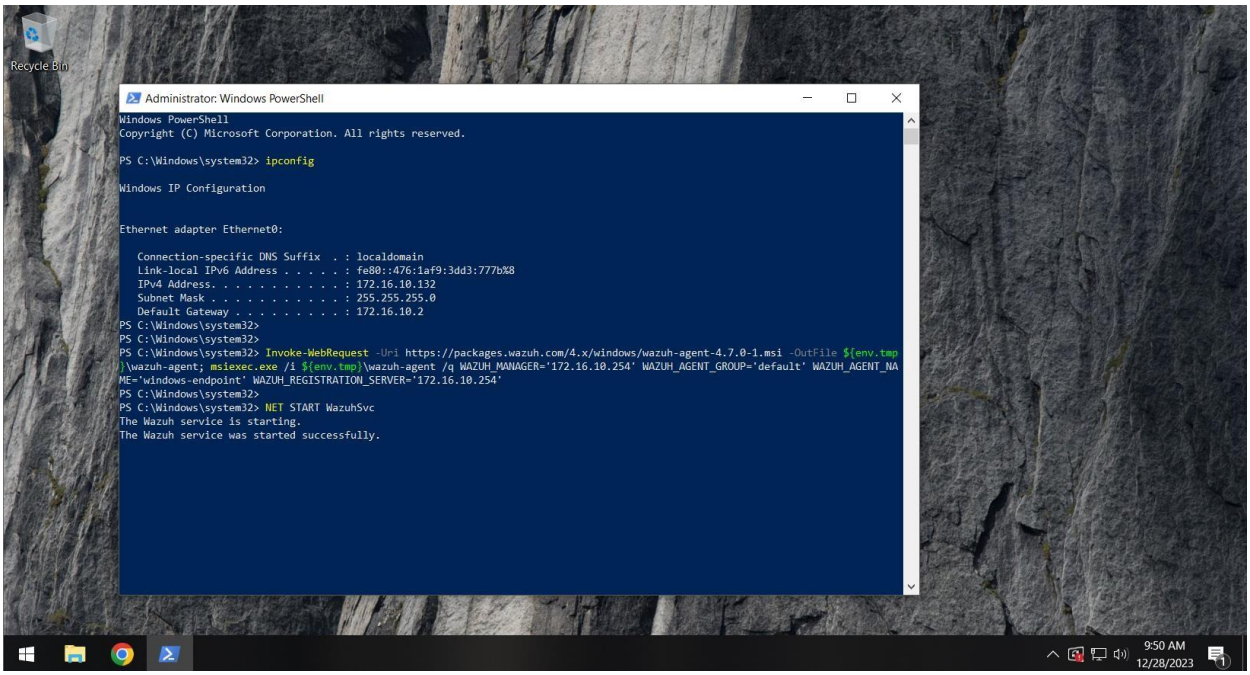

Figure 51 Starting the windows agent

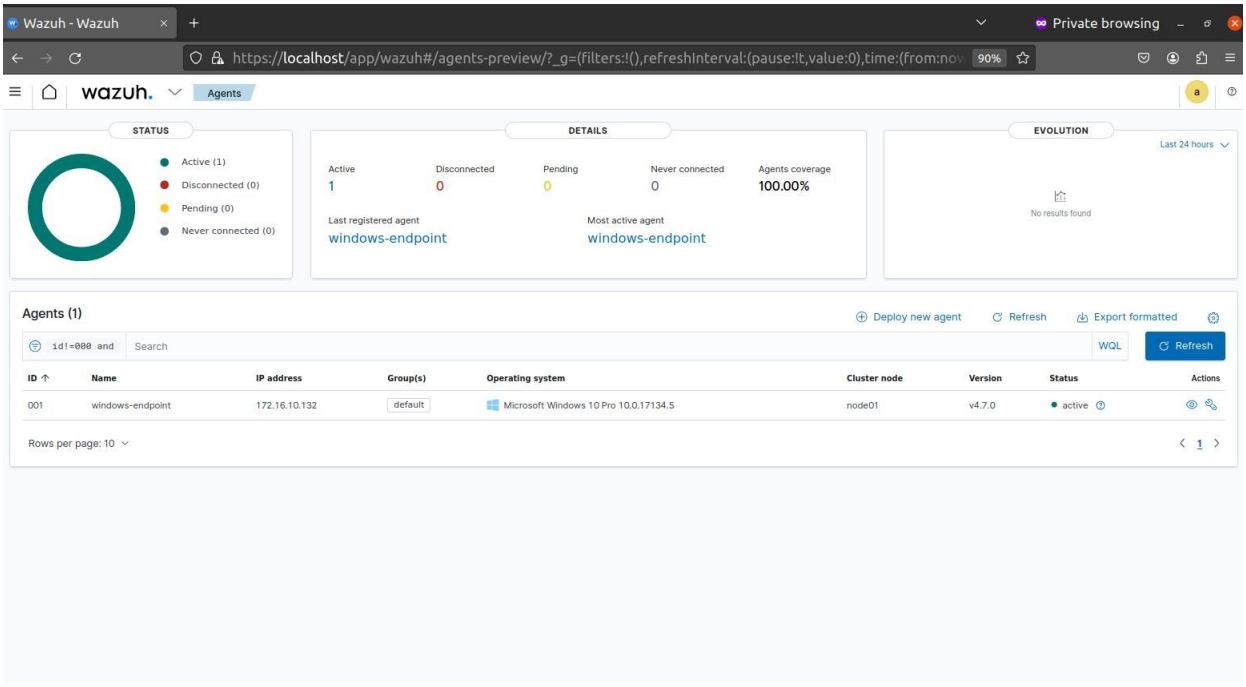

Figure 52 Viewing Windows Agent in Wazuh

7.2.6. Agent Installation Process for Ubuntu Endpoint

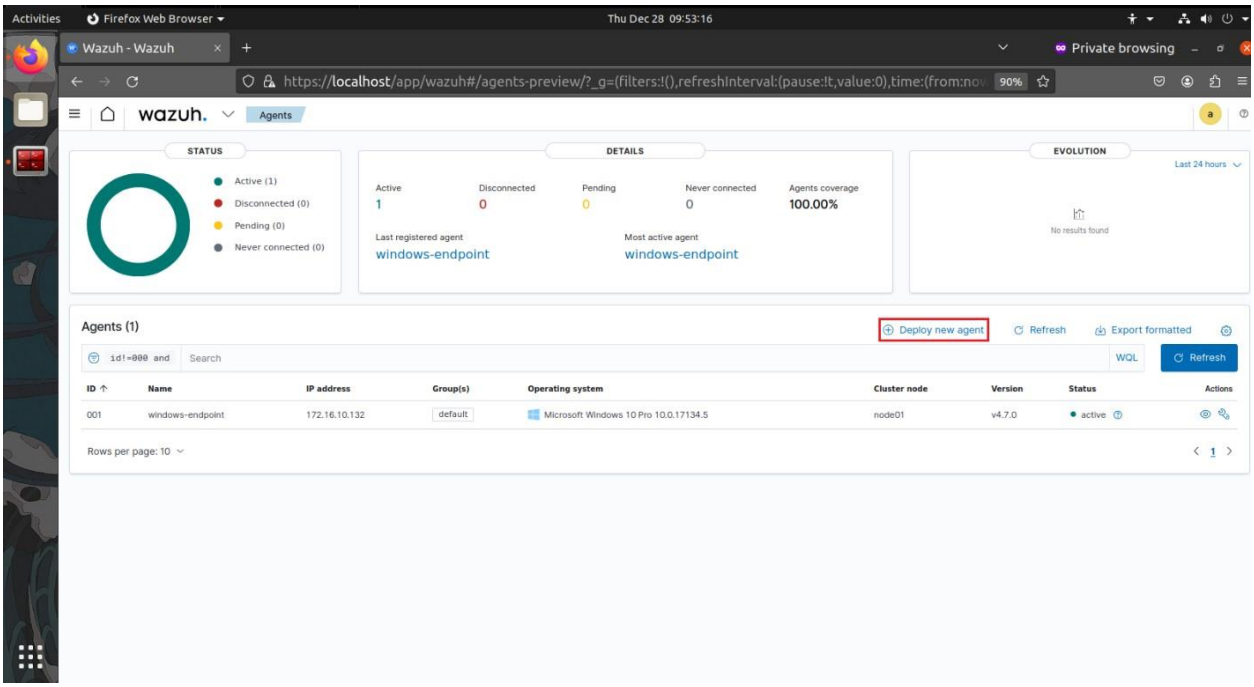

Figure 53 Deploying new agent for Ubuntu

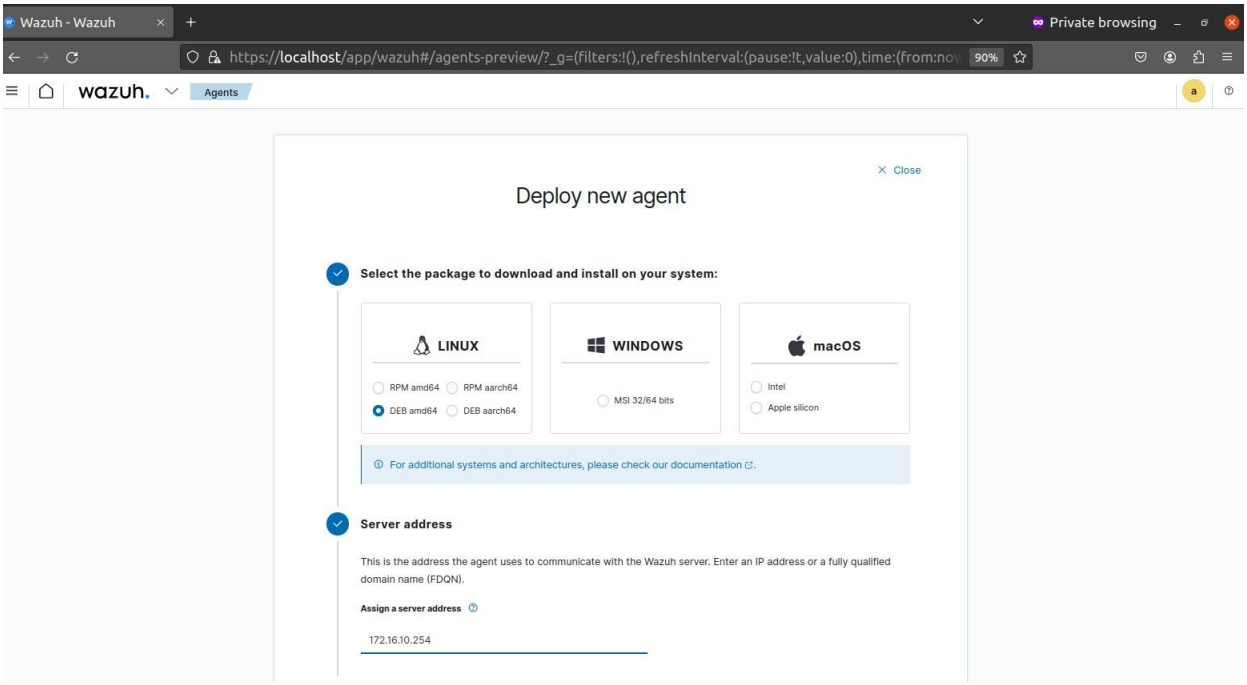

Figure 54 Setting up server address for ubuntu agent

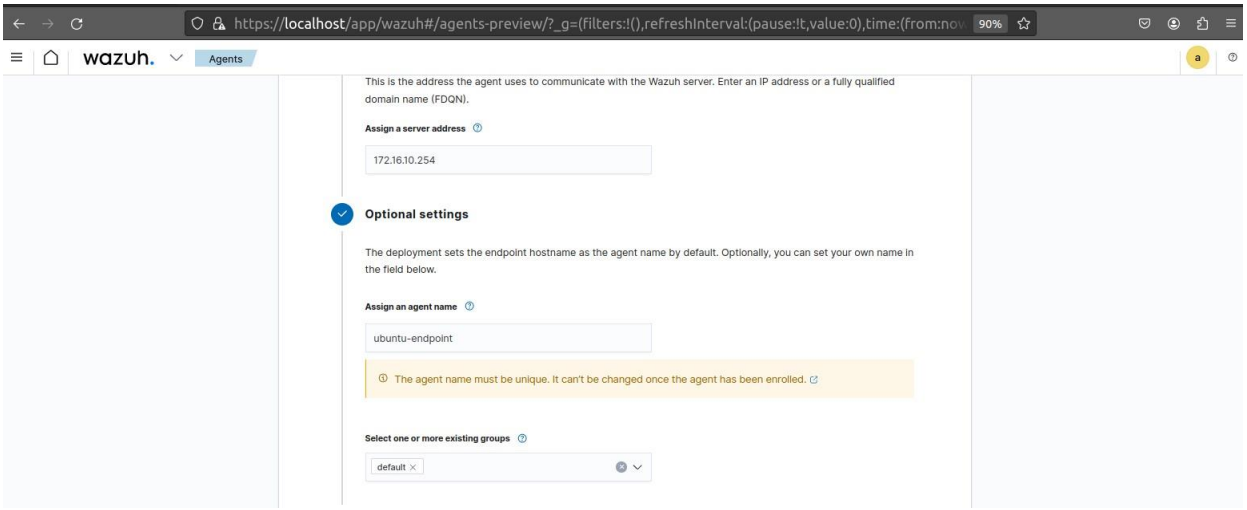

Figure 55 Assigning name for ubuntu agent

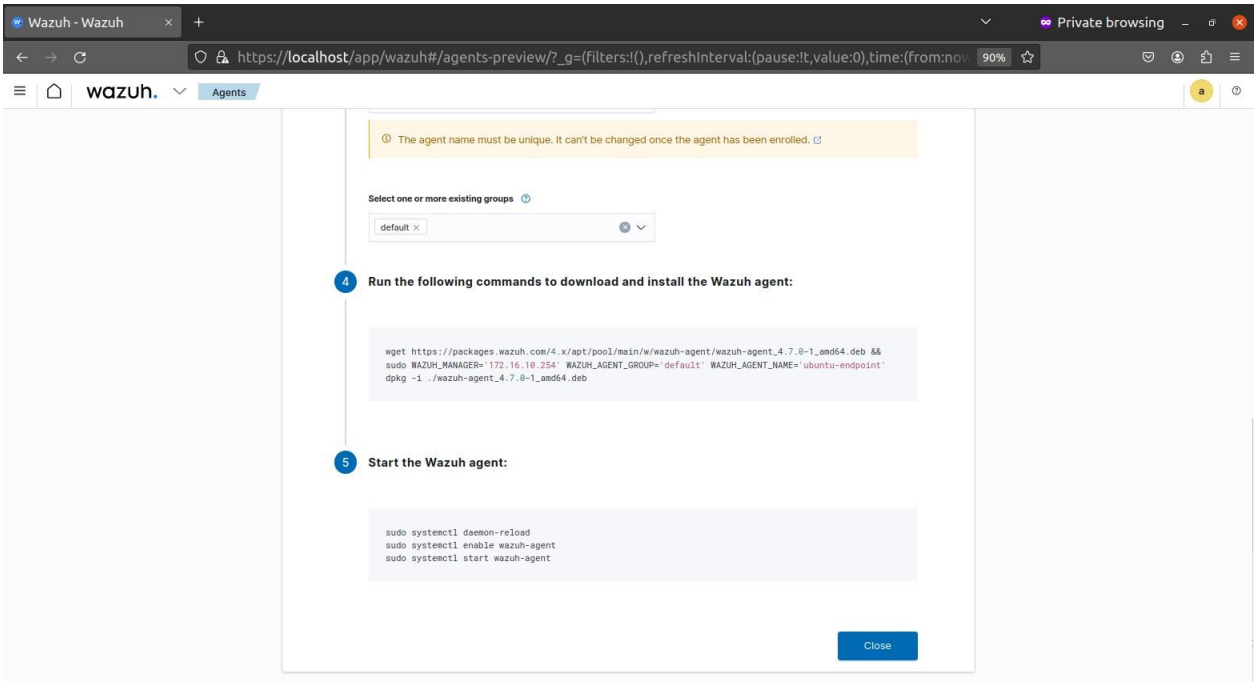

Figure 56 Commands to download, install and start the ubuntu agent

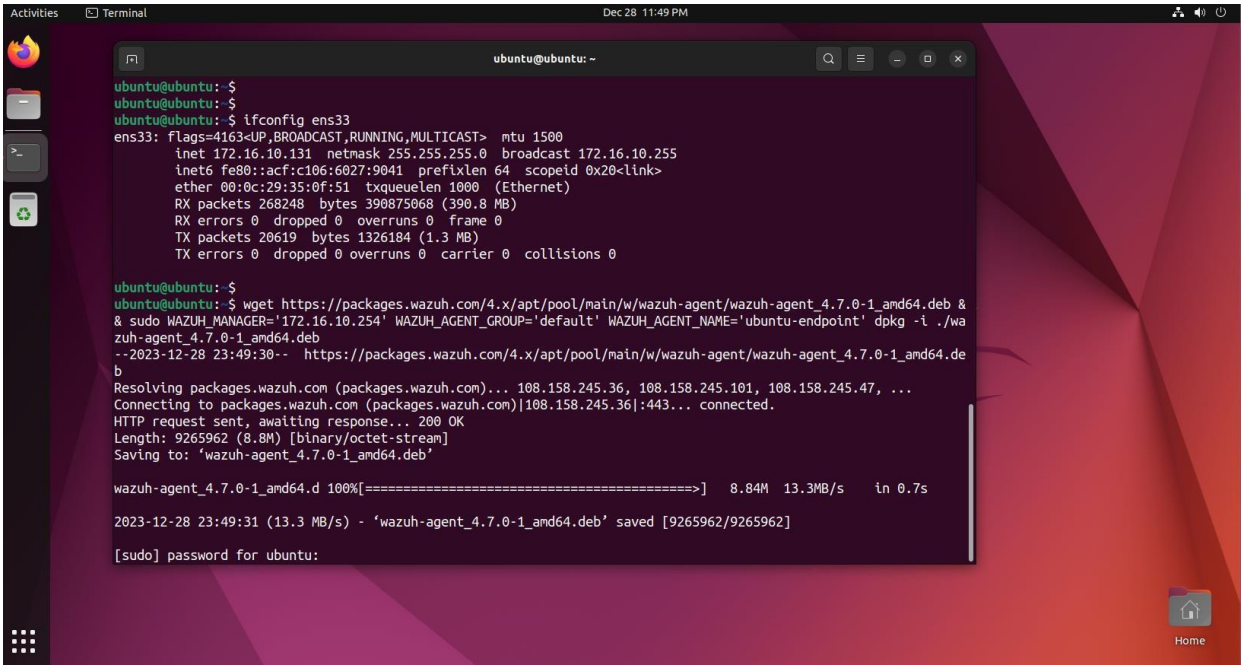

Figure 57 Running the commands to download and install the ubuntu agent

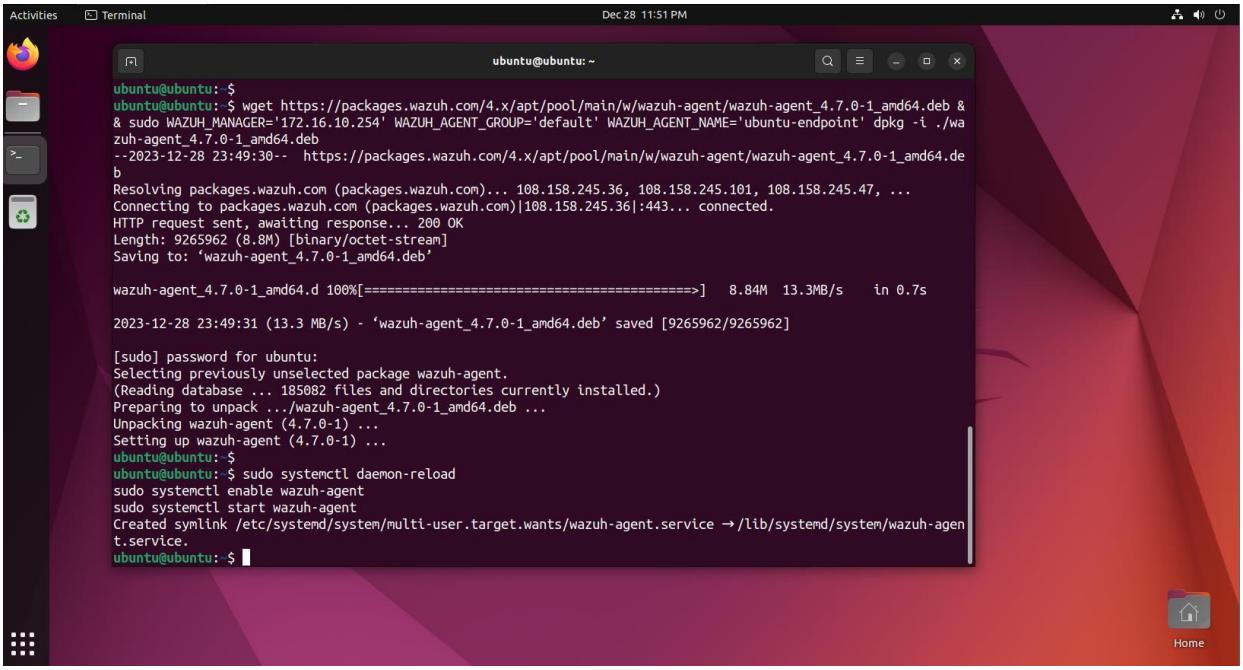

Figure 58 Starting the ubuntu agent

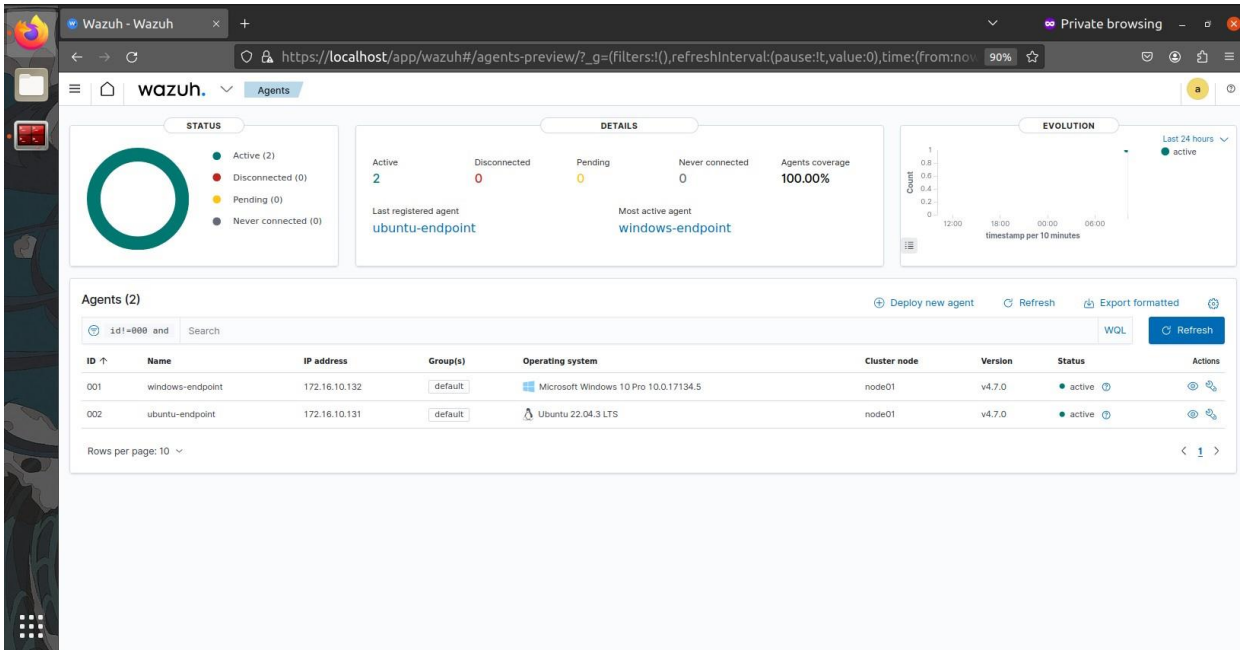

Figure 59 Viewing Ubuntu Agent in Wazuh

7.3. Defining DSDM

The dynamic system development methodology (DSDM) represents an agile software development approach characterized by its iterative and incremental nature, emphasizing swift delivery and sustained user involvement throughout the project (Abdullahi Sani, 2013). DSDM facilitates the dynamic development of systems, accommodating both object-oriented and functional design approaches. Particularly suitable for projects with evolving or unfixed requirements, DSDM permits revisiting earlier phases of the software development life cycle.

DSDM consists of five phases:

i. **Feasibility Study:** Assess the technical and business feasibility of the project. Identify scope, constraints, risks, and potential benefits.

ii. **Business Study:** Understand the business processes and user needs. Gather and refine requirements, possibly creating a prototype to visualize the solution.

iii. **Functional Model Iteration:** Develop and refine core functionalities in an iterative manner and create a working prototype for user review and testing in this phase.

iv. **Design and Build Iteration:** Incrementally design the system architecture and build the software. Each iteration adds features and refines existing ones based on feedback.

v. **Implementation:** Implement the system based on design specifications. This phase involves coding, testing, and integrating components.

DSDM, the dynamic system development model also shown in *Figure 3*, follows key principles for effective project management. It prioritizes active user involvement, grants decision-making power to teams, and emphasizes regular product deliveries for ongoing feedback. Acceptance is based on business needs, and development is gradual with reversible changes (Abdullahi Sani, 2013). The model maintains high-quality standards, integrates testing at every stage, and promotes collaborative teamwork. Overall, DSDM aims for user-focused and successful project outcomes.