National College of Ireland

Implementing Zero Trust Architecture in Detecting and Mitigating Threats: An APT Focused ZTA Framework

MSc Research Project
MSc in Cybersecurity

Nirav Ratilal Patel
Student ID: x23268859@student.ncirl.ie

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Nirav Ratilal Patel
Student ID:	x23268859@student.ncirl.ie
Programme:	MSc in Cybersecurity **Year:** 2024-2025
Module:	MSc Research Project
Supervisor:	Joel Aleburu
Submission Due Date:	11/08/2025
Project Title:	Implementing Zero Trust Architecture in Detecting and Mitigating Threats: An APT Focused ZTA Framework
Word Count:	9590 **Page Count** 24

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: Nirav Ratilal Patel

Date: 11/08/2025

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):	

Implementing Zero Trust Architecture in Detecting and Mitigating Threats: An APT Focused ZTA Framework

Nirav Ratilal Patel
X23268859@student.ncirl.ie

Abstract

This research focuses on the development of the cybersecurity threats focused on the zero-trust architecture framework and detecting and mitigating the threats. The integration of the NIST SP 800-207 along with the MITRE ATT&ACK tactics and techniques through the controlled environment setup and testing and conducting all the use case scenarios and detecting it using Wazuh SIEM (Security information and event management) an open-source tool. The implementation has achieved the successful detection of all the security events triggered and reduced the noise in the environment The results signifies that it achieved near real time detection which is mean time to detect for all the attack scenarios and also was successful in achieving the mean time to response (MTTR) for the selected automation policies.

1 Introduction

This study mainly focuses on the development of the zero-trust architecture (ZTA) for the detection and mitigation of the Advanced persistent Threats (APTs), The research also focuses on the NIST SP 800-207 standards and mapping the MITRE ATT&CK tactics and techniques. All the testing has been conducted in a controlled environment using the open Source SIEM (Security information event management) tool known as Wazuh.

The cybersecurity world has been facing a lot of challenges as the adversaries has been coming up with new emerging tactics and techniques and they also deploy the advanced attack like advanced persistent threats (APTs) that have the capabilities of by finding the critical vulnerabilities in the traditional security infrastructures. The high-profile incident, the solar winds supply chain attack which affected number of government agencies and many other companies. This showed that there are critical weaknesses in the system which consists of the conventional security models. This showcases how the threat actors can leverage these legitimate credentials and can easily be persistent access in the infrastructure and perform privilege escalation, lateral movement and also data exfiltration and still can remain unidentified in the system. All these traditional perimeter-based security models and different architectures have been inadequate against these modern APT threat actors that utilize the user accounts which are legitimate and several compromised endpoints. As soon as the remote work culture was introduced, the weaknesses in these traditional security models have proven insufficient and there is a need to change the fundamental defensive strategies and equip with the most advanced security mechanisms. Zero Trust Architecture provides a

solution to it, which basically operates on the principles called never trust always verify, this approach provides a new and advanced defensive strategy. The NIST SP 800-207 framework provides the in-depth guidance for the zero-trust architecture implementation and focusses on the micro-segmentation, least privilege access and ability for continuous monitoring. This research addresses the gap zero trust architecture theoretical frameworks and practical APT mitigation with the help of developing an APT focused zero trust environment and also with the integration of the MITRE ATT&CK framework and provides the measurable security improvements. The research methodology consists of all the APT attack scenarios run under the controlled lab environment and using the open-source tools and using Wazuh SIEM tool for the real time threat detection and automated response. This study signifies in demonstrating the measurable improvements in the Meantime to detect (MTTD) and mean time to response (MTTR) metrics which provides the practical implementation steps and procedures and helps to defend against the sophisticated APT attacks.

Research objectives

- Security Mechanism Effectiveness and Analysis: Identification and evaluation of the critical security mechanisms within the zero-trust architecture implementation which will provide the measurable protection against the APT techniques.
- Measuring the APT Attack prevention: To Quantify the effectiveness of the integrated Zero Trust Architecture Components in preventing the different lateral movements and data exfiltration attempts from the different APT campaigns.
- Testing the APT focused framework environment: This will provide and validate the frameworks through the comprehensive testing and simulation and showcase the security improvements.

2 Related Work / Literature Review

The Karabacak and Whittaker (2022) states that the most the research papers mainly focus on the detection methods for the sophisticated attacks in today's modern cybersecurity world, but there a critical need for the prevention methods as well for the advanced persistent threats. The prevention tools such as firewalls, Intrusion detection systems (IDS) and Intrusion prevention systems (IPS) and other solutions and also there is a need for security awareness and accurate security policies to be placed but sill many of these solutions lack the complete techniques for mitigating the modern-day threats. Also, they state that the MITRE ATT&CK framework can provide the threat intelligence which consists of the 14 different tactics and more than 180 techniques and also more than 375 sub techniques which can easily track the adversaries behaviour and can be very useful for the different use cases such as leveraging the threat detection, performing security assessment and many other use cases. They state that the literature review zero trust architecture can used as an vital framework for protection against these modern cyber security threats which focuses on the principle that the trust is never granted explicitly which can very useful for preventing these kind of attacks. Also, most of the studies focus on the applications like cloud technologies and different microservices rather then specific methodologies of the prevention of these attacks.

The Rose et al. (NIST SP 800-207) provides the different three policies with components such as policy engine (PE), policy enforcement point (PEP) and policy administrator (PA) and mainly focuses on micro segmentation and provides crucial insights about the division of

the network in to different broader zones and implying to these will be more than sufficient and will be significantly greater to apply these controls.

The Ahn, G. et. al. (2024), provides study about the integration of the ZTA with the MITRE ATT&CK framework for enhancing the cyber resilience with the help of the virtual simulation testing in the Korean public sector organisations. This research emphasizes that there is 30%-50% improvements in the cyber resilience metrics which includes the MTTR, MTTD while implementing the ZTA with the MITRE ATT&CK frameworks. The study mainly addresses all the challenges in the public sector organisations which are facing cyberattacks such as phishing, Ransomware, insider threats and APTs. This study also focuses on providing guidance for government sector companies for the implementation of the ZTA frameworks within the regulatory and compliance. These researchers have identified the seven core principles of the zero-trust security model. They start with the continuous verification, of all the access present, policy of least privilege, micro-segmentation of the networks, Multifactor authentication must be implied, the device security verification, continuous monitoring and policy-based access controls. This paper examines the MTIRE ATT&CK tactics and techniques for the proper understanding of the adversary's behaviour and also for the establishment of the defensive plans against these modern threat actors and also provide an in-depth analysis of the traditional security models and the zero trust principles. The research consists of the Cyber resilience engineering framework (CREF) as an approach for understanding both problem and solution in cyber security. The critical limitations in this research is that it its focus on Korean public sector only which brings some restrictions and also lacks comparative analysis with the other security methods. The Ahn, G. et. al. (2024) has proposed for combining the zero trust with the integration of the MITRE ATT&CK framework for writing and executing the policies which specifically targets the behaviours of the adversaries which includes prevention of lateral movements, detection and blocking of malicious processes.

The Gambo, M.L. & Almulhem, A. (2025) gives the significant analysis of the Zero trust architecture including the research from year 2016 – 2025 and indicating the PRISMA framework for investigating and examining the ZTA applications and provides the insights in ZTA principles in Cybersecurity and as the traditional perimeter-based security models have now gradually become inadequate in the modern cybersecurity world. It also provides the theoretical foundation by contrasting the ZTA architecture with the perimeter-based security models and addresses how the conventional and traditional security methods fails to address the internal threats and these systems lack the flexibility for the modern work infrastructure. It basically introduces the three main principles which are main and logical components which are given in the NIST SP 800-207 which are Policy Engine (PE), Policy Enforcement Point (PEP) and Policy Administrator (PA) which is the key foundation for the ZTA implementation. There are limitations to the validity of the meta-analysis research of ZTA. the search strategy used only one group of databases related to relevant publications, and this aspect might have missed relevant publications. Second, the systematic review was conducted according to the PRISMA framework, which is characterized by the existence of possible publication bias, which is likely to overestimate positive results. The fading interest in ZTA as shown by the reduction in the number of studies over time, is signalling either market saturation or the lack of fundamental theoretical options.

Hasan (2024) examines the ability of zero-trust architecture (ZTA) to treat vulnerabilities and insider threats. Applying a mixed-methodology that combines with case studies (ex: Cimpress, financial institutions) and industry reports (IBM, Verizon, Cisco, and Google

Cloud), the research suggests that the minimized implementation of ZTA leads to significant decreases in the breach-related costs (30 %) and also insider threats till 25%-45% and malware and phishing cases till 35%-40% in the main sectors such as health care sectors, finance sector and technology. It also highlights and emphasizes the importance of micro-segmentation and continuous verification and behavioural analytics. he major assets of the article include insides based on the data, the thoroughness, and sector scope, as well as practical instructions on use. The major drawbacks relate to challenges that arise during the process of integrating ZTA with legacy systems, the fact that it is not scalable to suit organisations of different sizes, high initial cost and the existence of cultural resistance. As a result, the author suggests the best practices, which include the solutions that are environment-independent, automation, and complex staff training, and goes further to promote the research on the capabilities of artificial intelligence (AI), machine learning (ML), and blockchain association in ZTA.

Phiayura & Teerakanok (2023) study extends the findings of a review of peer-reviewed literature and industry analysis to provide a general, step-by-step process that will serve as a guide to moving to Zero Trust Architecture (ZTA). The authors identify six essential steps of migration strategizing, context assessment, architecture design, transformation, monitoring, and optimization and show why and how DevOps principles can be used to increase stakeholder input, discovery of the existing assets, and continuous monitoring. The framework deals with three key technical and organizational issues such as legacy integration, user disruption, and regulatory compliance. Despite its step-by-step structure, and despite the disciplined nature of formulating it, the framework also has weaknesses in the form of minimal empirical validation, and the fact that it is not founded on any quantitative cost-benefit analysis. The authors thus recommend the need to conduct more research studies on dynamic migration techniques and integrating other emerging technologies into the faster and stronger ZTA use.

Shushan and Ceylan (2024) explores the transition to zero-trust architecture (ZTA) and its advantage- including dynamic authentication, enhanced endpoint security, and the stringent control of the flow of the data, as well as highlighting the challenges that organizations face, in particular, the network identity management and continuous data monitoring. This paper provides a theoretical framework that uses NIST SP 800-207 and the need to focus on ongoing verification and the least privilege access. The authors believe in the implementation method of being gradual, step wise and compatible with older systems as well. They can be credited with providing a clear description of the strengths and weaknesses of ZTA as well as some practical impediments, but this does not go far enough since it lacks empirical evidence and quantitative dimensions. Therefore, the authors insist on further real-word analyses and technical reviews to support their recommendations.

The below table provides the key findings and the main focus of the different research papers for the literature review.

Author	**Focus**	**Pros**	**Key Findings**	**Limitations**
Karabacak & Whittaker (2022)	The ZTA effectiveness Against the APT 29	Systematic mapping Of the ZTA to APT techniques, Utilized real	ZTA could have Prevented solar winds Breach with help of 13	Provided the theoretical analysis And has a static pattern

		world case study	Mapped MITRE ATT&CK Controls	
NIST SP 800-207 (2020)	Framework for ZTA Standardization	Significant framework, provides Industry adoption and provides Detailed insights for theory to Practice	Provides core ZTA tenets For implementation, establishment For PE/PA/PEP architecture with 7 deployment models	Lacks APT specific information And guidance
Ahn et al. (2024)	ZTA with MITRE ATT&CK migration	Provides practical validation, provides measurable improvements	30%-50% improvement in metrics such as MTTC, MTTD with integration of ZTA With MITRE ATT&CK framework	Limited to only the Korean public sector.
Gambo & Almulhem (2025)	Systematic Literature review for ZTA	Provides PRISMA framework and identified research gaps	Categorization of ZTA application across the different sectors	Mainly focuses on theoretical study and publication bias
Tsai et al. (2024)	Strategy for ZTA implementation	Significant implementation road map	Provides 7 pillar cyclic ZTA model	Complexity in implementation, lacks Practical validation
Hasan (2024)	Effectiveness of ZTA in Enterprise security	Provides real world industry validation	25%-45% reduction in data breaches, Phishing and other cases in critical sectors	Case study selection bias
Phiayura & Teerakanok (2023)	Framework for ZTA migration	Well defined process Oriented approach	Provides 6 step migration framework	Does not focus on cost effectiveness, limited technical depth
Suzen & Ceylan (2024)	Challenges in ZTA transition and advantages	Provides vital insights in practical	Provides legacy integration challenges	Provides limited technical depth and resource

		implementation Barriers		constraint analysis

Table 1: Comparison of Literature Review

3 Research Methodology

This study follows a streamlined approach and different methods for the evaluation of the zero-trust architecture for the mitigation of the advanced persistent threats (APTs). Adhering to the NIST SP 800-27 framework and also the foundational knowledge base of the MITRE ATT&CK base which comprises of 14 tactics and more then 250 techniques and more than 300 sub techniques. The methodology includes the combination of hands-on experiments in a controlled virtual environment and its different use cases and the qualitative assessment for producing the results. This research methodology consists of the different phases which are the planning and design of the framework, Environmental setup and the network architecture, APT simulation scenarios, Analysis and investigation of the scenarios and final step will be reporting. All of these phases are completely interconnected with each other and forms an APT focused ZTA framework.

3.1 Planning and Design of the Framework

This is the first phase in which there is the establishment of the foundational research which is being carried out by assessing the literature review of the relevant papers and also selecting the use cases of APT simulation attack scenarios and ensures that it aligns with the industry standards which is NIST SP 800-207. This research's objective and the research questions mainly focuses on the foundational ZTA principles and all the APT techniques which are mentioned in the MITRE ATT&CK framework. The research questions were formed to address all the APT threats which can be detected and mitigated effectively through the open source SIEM tool and also through implying ZTA principles. Also, it focuses on calculating the Mean time to detect (MTTD) and Mean time to respond (MTTR), and it also states all the implementation challenges faced by using open-source tools for reducing the cost effectiveness. The different APT attack scenarios were considered and also mapping it with the MITRE ATT&CK tactics and techniques. The attack scenarios which are considered are SSH Brute force, Multiple Authentication failures, Integration of File integrity monitoring for protection against data exfiltration and insider threats, detection of shell shock attacks, Detection of unauthorised processes, Integration of Active response for the Brute force attacks and SQL Injection attacks. All of these attacks are mapped with their specific MITRE tactics and techniques. An in-depth strategy and plan about all the resource requirements, all the timelines and all the mitigation strategies are being documented.

3.2 Environment Setup and the System Architecture

This phase consists of the whole lab setup which is a virtual infrastructure which is subjected to the ZTA controls and for mitigation and detection of APT threats. An infrastructure network setup is implemented which is in isolated environment and in virtual host-only

environment. A Five VM setup is initialized on virtual box with host specifications includes a 16 GB RAM and 1 TB storage of the host machine. The lab environment consists of the five VMs which are Ubuntu-SIEM machine, ZTA controller machine on Ubuntu machine, Kali Linux Attacker machine and the Ubuntu server and Windows server 2022 as the victim machine.

The Wazuh SIEM VM is installed on the ubuntu 22.04 version with specifications such as 8 GB of RAM and 100 GB of storage in it and its IP address is 192.168.1.86/24. It consists of the Wazuh manager, Wazuh Indexer and Wazuh Dashboard which are used for indexing, management of rules, triaging the alerts, integration of active response and many other things. The Wazuh manager is being configured for different rulesets and is being used for custom rulesets for detecting the different APT attacks such as SSH brute force attacks, Multiple login failures, SQL injection attacks and detection of unauthorised access and its rule IDs are 5763,5710,2502, and integration of active response for Brute force attacks which is triggered when the specific thresholds are reached and gives "firewall-drop" in the packet and blocks the attacker's malicious IP automatically and the connection is completely closed from the attacker's machine. The ZTA controller VM is the Ubuntu machine with its latest version 22.04 with the 4 GB of RAM and 60 GB of storage and its IP address is 192.168.1.81/24. The ZTA controller consists of the Spire server which is used for the workload management and also k3s Kubernetes and cilium is also installed for enforcing the networking policies. The spire server trust domain is named as "zta-lab local." Cilium is used for implying ZTA policies such as default deny policies, APT mitigation policy which will restrict the lateral movement.

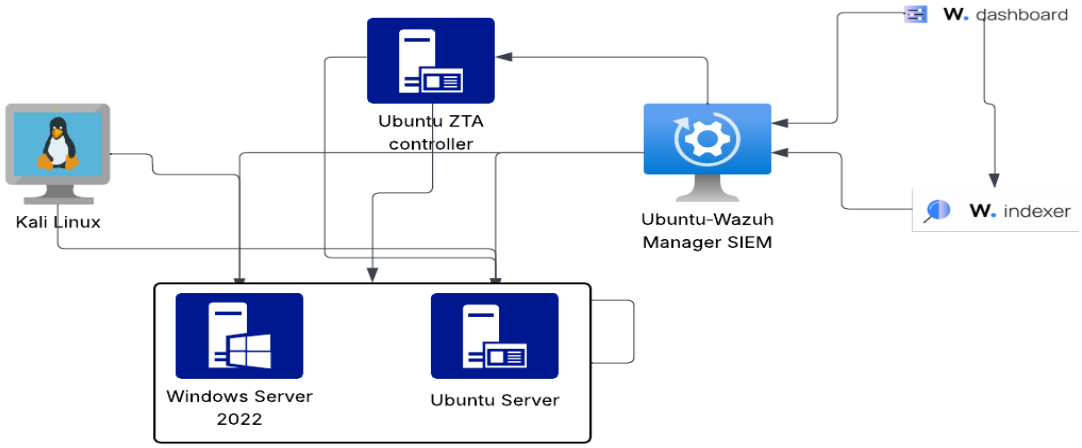

Figure 1: Network Architecture

The Kali Linux Attacker machine consists of the kali 2025.2 version and consists of 4 GB of RAM and 40 GB of storage. Hydra tool is installed in Linux which is used for many purposes and for performing APT attacks such as SSH brute force attacks, password spraying attack, initial access, credential access (T1110) and running custom scripts for SQL injection vulnerability and shell shock attack and other APT attacks. The victim machines include Windows server 2022 and Ubuntu server 22.04 LTS. The windows server consists of 4 GB of RAM and 60 GB of storage with the IP address 192.168.1.72/24 and the ubuntu server 22.04 VM comprises of the 2 GB of RAM and 40 GB of storage in it and the IP address associated

with it is 192.168.1.77/24. On Both of the Victim VMs, the wazuh agent is installed successfully for log forwarding process to Wazuh SIEM.

All the virtual machines are on a single host only network which is 192.168.1.0/24 which is providing isolated environment and there is not any connection from the external networks All the connectivity and segmentation is performed and thoroughly tested and performed the validation of test via the ICMP ping and connectivity tests of Cilium and other cilium network policies in YAML file.

3.3 Controlled Simulation Scenarios and Collection of Data

This phase three consists of the conducting the various APT simulation attack scenarios and capturing the data for the detection and response. The detection and response actions will be taken on the Wazuh SIEM tool which is configured accordingly. In this phase a total of eight scenarios and use cases with ZTA controls which are enforced the detection and response part with all the log collection and deep dive investigation will be carried out and all the performance metrics such as Mean time to detect (MTTD) and mean time to response (MTTR) have been recorded for calculating and evaluating the use cases. In the attack scenarios are performed and are executed form the Kali Linux attacker VM machine. Initially, Hydra is used for attempting the multiple logins for exploiting the SSH service on the ubuntu server which is the victim machine. The Rule ID 5763 which is SSH Brute force attack detected is being detected as soon as the eight failed login attempts are done within the span of 180 seconds. For the non-existing user failed login attempts the SSH service is being targeted and rule ID for wazuh is 5710 is expected to trigger when the users which does not belong to the infrastructure will try to login. Also, there is a use case where the successful login which is followed by the multiple login failures are being detected, initially it basically exhausts the valid accounts password's threshold and then it provides the correct password which will trigger rule ID 40112. There is also the integration of one other rule ID 2502 for multiple authentication failures in short time without the successive login.

This experimental design is focused on the APT attacks which can be simulated within a controlled environment. The Threat model scope contains of the attack vectors which are covered are Initial access with SSH brute force attack, web application exploitation such as shell shock attack and SQL injection attack, credential harvesting and lateral movement within the infrastructure and File system compromise and malicious process injection and all the APT techniques use are T1110 (Brute force), T1071 (Application Layer Protocol), T1070 (Indicator Removal), T1190 (Exploiting Public Facing application), T1049 (System network connections discovery). The validation of the real world APT attack which signifies the real world APT campaigns which are the APT 29, APT 40, APT 28 and Lazarous group.

The File integrity monitoring (FIM) is also being integrated which basically has the capabilities to monitor the integrity of the system and all the application files. This is an important feature for the defensive layer for monitoring the sensitive assets. It has the feature for timely scanning and verifying the integrity of the file which is useful as it helps to determine any changes in the vital files in the systems. It stores the cryptographic checksum of the files which are monitored. As soon as the user makes some changes in the file, modifying the file or deleting the file, this module accurately compares the checksum and attributes the baseline, and it will trigger the alert if there is any mismatch. It displays all the logs such as every change in the file, any modifications and deletion process, it will generate

the alert in real time. For the Web application attack simulations, the simple web application is being hosted on the ubuntu server, which is the victim machine, SQL injection attack is being executed by trying to inject the SQL payloads in the query parameters which will basically trigger the rule in Wazuh for SQL injection attack detection. Also, the Shell shock attack is simulated which basically sends the malicious crafted HTTP headers which will exploit the bash vulnerability and will trigger the alert in the wazuh SIEM. The unauthorised process running on the victim machine can be detected, if the adversary is trying to launch net cat session by running on the non-approved binaries on the victim machine, it will trigger the alert in the Wazuh SIEM about the detection of unauthorized processes in real time on the console.

All the data is being collected and are exported to CSV format for summarizing the average Mean time to detect (MTTD) and Mean time to response (MTTR) is being calculated for all the scenarios conducted.

3.4 Validation and Reporting

In this phase we will be gathering all the vital measurements from all the APT simulations performed and how much time to took to detect each and every attack which is called mean time to detect (MTTD) and how many automated responses or how many numbers of malicious attempts were blocked successfully (MTTR). Also, a systematic mapping of each simulated attack scenarios with the MITRE ATT&CK table for mapping its tactic and technique and document how they prevented or detected the attack, and it show all the threat pathways in a significant way and also if there are any gaps in it. Next step is to blend our findings in qualitative way with proper insights provided and providing in-depth recommendations.

4 Design Specification

The design consists of the Advanced persistent threats focused on zero trust architecture framework integrates with the multiple open-source tools and technologies which are cilium for network policy enhancement, Wazuh SIEM for real time security monitoring and investigations which are deployed on a host only network of 192.168.1.0/24 in a virtual network which comprises of 5 virtual machines This is the layered architecture which provides network segmentation, least privilege access and proactive threat detection according to the NIST SP 800-207 framework and providing specific mitigations for the known APT attacks and mapping it with the MITRE ATT&CK Framework. This study provides the insights about the logical layering, all the network topologies and software components and the collection of different tools which are used for detecting, blocking as well as auto responding to the threats. This provides a clarification that the design principles and the functional requirements with the proof of concept using he open-source tools for implementation and with the minimal configuration of 16GB of RAM for the host machine and mapping all the threats with the attack tactics and techniques used by the adversaries.

The kali Linux machine which is the attacker virtual machine and the ZTA controller virtual machine and the two victims which are ubuntu server and windows server 2022 and the

dedicated SIEM machine which includes Wazuh v4.12 Indexer, dashboard and manager which is responsible for the security monitoring and threat detection and both of the victim machines consists of the wazuh agents which will help in log ingestion and log forwarding to the Wazuh manager. The ZTA controller has the cilium and k3s cluster installed and running where it comprises of multiple policy enforcements which includes the cilium network policy which is called default-deny-all which will drop everything that is explicitly not allowed and it also includes ZTA management access which will directly allow wazuh manager for shipping the logs. The APT mitigation policy is in place where the policy is designed to mitigate the attacks and will not allow SSH 22/TCP from any external network except from the internal network communication. Wazuh v4.12 agents have deployed on every virtual machine in the network with the 1514/UDP and 1515/TCP.

Configuration of Zero Trust Policies

Default-Deny-All Policy: The creation of the default deny policy, (default-deny-policy. yaml) for the zero trust which basically denies everything and only allowing the necessary traffic. Also, no incoming traffic or any outgoing traffic is allowed unless and until it is explicitly permitted. This enforces the establishment of zero trust which states never trust and always verify. It has the capabilities of stopping any unwanted communication from the outside traffic. This policy ensures that the environment is fully secured and only required communications are allowed and if there's any additional policies in place than the ports can be opened later for communication purpose.

ZTA Management Policy: This policy is basically one of the important policies in the network as it has two rules in it, as it allows to send TCP traffic on port 8081 for the spire server and it allows to send wazuh agent traffic which is UDP 1514 port for the logs and TCP 1515 for the commands executed on the wazuh manager. No inbound rules are set or any predefined rules.

APT Mitigation policy: This policy is created for the purpose of blocking the lateral movement and there is a secured communication and channel for HTTPS and SSH between the two-victim zone and the management zone. Because of this there is network segmentation created, there is only minimal set of traffic flow across the infrastructure.

Detection Logic of the Attack Simulations

Attacks/Use cases	**Rule Ids**	**Detection Logic**	**Importance of the Policies**
SSH Brute Force Attack	5763	This rule triggers when there is a SSH Failed login more than eight times from a Single IP address and within the time span of 180 seconds	It is critical for detecting and preventing credential-based attacks for the zero-trust defensive framework
Multiple Authentication Failures	2502	This rule is triggered when the multiple or repeated authentication failures appear within the short span of time and all the password attempts	This is a significant sign of the credential attack where it supports the principle of continuous monitoring

		are failure.	
Non-Existing User Login Attempts	5710	This rule triggers when the adversaries tried to perform reconnaissance technique and it detects the authentication attempts and its severity level is 5	It is vital as it is sign of the initial reconnaissance in the zero-trust network, it is an early detection of threat
File Integrity Monitoring (FIM)	550,554	This rule is triggered when the integrity checksum is changed and the modification in file is detected or any new file creation is detected	This is one of the cores zero trust requirements for maintaining the system integrity and indicates the policy violations and compromise
Detection of Unauthorized processes	100051	This rule is triggered when the command monitoring detects that there is a net cat session listening process list, "nc -l" which is a indication of the unauthorized reverse shell	This is important because process monitoring make sure that only the authorised tool should run and it prevents the unauthorised processes and communication which tried to by the zero trust controls
Detection of SQL Injection Attack	31103,31106	This policy will trigger when it matches the SQL injection patterns such as Union+ or select+ etc and successful SQL injection with HTTP 200 response which indicated the data exfiltration	It is vital for protecting the data integrity in the network infrastructure
Detection of Shell shock Attack	31168	This rule basically detects the all the HTTP requests with the bash function exploit pattern in the user agent header which is then followed by the shell commands	This is the indication of the defence against the exploitation attempts
Successful logins after multiple failed attempts	40112	This rule is triggered when there are multiple failed login which is followed by the successful login and is an indication of the brute force attack	It is vital as it is an high priority detection which shows the successful activity of credential compromise

Table 2: Detection Logic

5 Implementation

The Implementation phase provides the insights about the how the zero-trust environment was built and configured with the virtual lab setup and all the advanced persistent threats attack simulation were taken placed and evaluated. It provides information about the different operating systems used and also all the open-source tools used and performing eight attack simulations and collecting the results. All the virtual machines are host-only network which is an isolated network and no NAT network or bridge network were selected. All the virtual machines were in 192.168.1.0/24 network and they were able to ping each other successfully. There was a setup of the custom rule sets in Wazuh SIEM for all the eight tailored attacks and also the mapping of the all the attacks with the MITRE ATT&CK techniques and techniques was performed.

Rule sets

The custom rule sets in wazuh are detection rules and logs which are tailored which in in the "/var/ossec/etc/rules.xml". Also, instead of relying on the general rule sets, there were some changes performed in the rule sets so that to it will be getting triggered in the best possible way. Changing the frequency thresholds of the incidents and the timeframes and the MITRE ATT&CK tags in it. The below table provides in sights about the use cases and the rule IDs associated with it and the severity of the incidents and its thresholds.

Use-cases	Rule Ids	Thresholds	Severity
SSH Brute Force	5763	Eight Failed attempts in 180 seconds	10
Multiple Authentication Failures	2502	Five Failed attempts in 120 seconds	7
Non-Existing User Login Attempts	5710	1 Event	5
File Integrity Monitoring (FIM) for checksum changed	550	N/A (As soon as the checksum changes)	7
File Integrity Monitoring (FIM) for Creation of new file	554	N/A (new file creation)	5
Detection of Unauthorized processes	100051	1 unauthorized process	7
Detection of SQL Injection Attack	31103,31106	1 hit	10
Detection of Shell shock Attack	31168	1 hit	15
Successful logins after multiple failed attempts	40112	Equal to 3 or more failure then success in 120 seconds	12

Table 3: Rule Sets

All the above custom rule basically hardens the security environment by setting and changing the required frequency thresholds and implementing precise active response in the critical infrastructure. The total of eight attacks is performed in which Host-based rules send 5763 into action where the SSH brute-force attempt fails after 8 futile attempts to log in within 180 seconds and 2502 sets out a flag in case five consecutive missing flags were called within 30 seconds, where 5710 reports non-existent usernames, and 40112 alerts when an effective

crack has already been done. On the network end, there is the detection rule 31168 and 31103/31106, which detects the Shellshock and SQL-injection activities respectively. There is one process rule Id 100051 that can identify Netcat listener activity. Each degree of severity of the rules is given the range of 5-15 allowing a quick escalation of the high-risk behaviours and minimal noise on the reconnaissance signals.

The below table provides information about each APT attacks with the rule Ids and its mapping to the MITRE ATT&CK tactics and techniques.

Use cases	**MITRE ATT&CK Tactic**	**MITRE ATT&CK Technique**	**Rule Id**
SSH Brute Force Attack	Credential Access	T1110 (Brute Force), T1110.001 (Password Guessing)	5763
Multiple Authentication Failures	Credential Access	T1110 (Brute Force), T1110.003 (Password Spraying)	2502
Non-Existing User Login Attempts	Discovery	T1110 (Brute Force), T1598.002 (Gathering victim-host information)	5710
File Integrity Monitoring (FIM)	Impact	T1565.001 (Stored data Manipulation)	550,554
Detection of Unauthorized processes	Discovery	T1049 (System network connections discovery)	100051
Detection of SQL Injection Attack	Initial Access Execution	T1190 (Exploit public facing application), T1059.007 (Command and scripting Interpreter SQL)	31103,31106
Detection of Shell shock Attack	Initial Access Privilege Escalation	T1190 (Exploit public facing application), T1068 (Exploitation for Privilege escalation)	31168
Successful logins after multiple failed attempts	Credential Access Initial Access	T1078 (Valid Accounts), T1110 (Brute Force)	40112

Table 4: MITRE ATT&CK Mapping

This significant mapping of all the eight APT attacks to MITRE ATT&CK framework shows that how the detection rules align with the specific adversaries tactics and techniques which is crucial and provides defence capabilities for zero trust architecture environment.

Application Security Layer

The authentication-based attacks which are SSH based brute force, Multiple failure login attempts and non-existing user logins and successful login after failures significantly maps the credential access and discovery tactics and which is being targeted as brute force attacks and valid accounts, T1110 and T1078. These are one of the rules which incorporate the foundation structure of the zero-trust principle such as never trust, always verify which is the vital principle which makes sures that the credential bases attacks are detected and blocked so that that they cannot create any damage to the infrastructure.

System Integrity Protection

The Impact tactic has been explicitly mitigated by the File Integrity Monitoring (Rules 550, 554) which is a necessary mechanism to ensure trustworthiness of the Zero Trust environment. This allows preventing the adversaries trying to weaken the trusted baseline with unauthorized modifications to critical files by quickly noticing changes in the critical files.

Application Layer Defence

The Shellshock attack detection and SQL Injection attack detection rules defend against Initial Access attempts through T1190 (Exploit Public-Facing Application), demonstrating the defence-in-depth at the network level of Zero Trust measures. These types of policies are vital and are critical for the organization due to the ability of vulnerabilities which have the capabilities for bypassing the traditional network segmentation and access-based controls.

Network discovery and Process Control

The discovery rule Id 100051 for Detection of unauthorized process is aligned with the Discovery tactic of the T1049 (System Network Connections Discovery) framework and as such protects a Zero Trust architecture since it blocks operations on unauthorized processes thus preventing the installation of stealthy communication routes that bypass test-controlled network restrictions and identity verification.

6 Evaluation

The evaluation part of this study provides in depth information about the statistical analysis in Zero Trust Architecture for the mitigation and detection of the APT attacks. The evaluation approach for this study is an experimental method by using and performing the real-world attack simulations and implementation of metrics such as Mean Time to Detect (MTTD) and Mean time to Response (MTTR) as the key indicators for the performance and providing detailed description and analysis and also about the testing and performance analysis. Below are all the simulations of the Attack scenarios.

6.1 SSH Brute Force Attack

The SSH Brute force attack (5763) represents the APT technique called credential access which is critical and the attack vector uses this technique getting the initial access in to the network infrastructure with targeting the SSH services and using the sophisticated tools like Hydra for brute force and attempt to exploit the SSH services. This is can be implemented using different methods using the automated dictionary and using different combination of the usernames and passwords for the database or using the customised password list and can also use the rockyou.txt which is the most used password list for performing this attack.

According to the detection logic and the zero trust implementation, there is a specific threshold mechanism for triggering of the policy, and it is being set to eight. If there are eight or more than eight failed SSH login attempts from a single source IP address within a span of the 180 seconds. Also, the implementation of active response enabled the automated capabilities via the automated blocking the host immediately by “Firewall-drop” with its active response.

The total of 22 incidents were detected for the SSH Brute force and the mean time to detect (MTTD) is around 72.28 seconds which is 1.2 minutes. For all the incidents for this policy active response has been enabled and configured due to which the mean time to response (MTTR) achieved is 0.46 seconds which represented a huge improvement as compared to the traditional methods which shows the zero trust and automated response.

6.2 Multiple Authentication Failures

The Multiple authentication failures (2502) is basically a password spraying method or technique which is representing a more of a subtle approach as compared to the brute force attacks. The adversaries usually use these kinds of technique for testing credentials across the multiple accounts and also to avoid the lockout policies in the system infrastructure. The detection logic and thresholds work in a way that there are multiple authentications attempts which are failure and those attempts occur within short span of time in timeframe of 120 seconds. As far as the performance results are compared, a total of 86 incidents were detected providing exceptional performance and providing mean time to detect (MTTD) of around 5 seconds. The quick and rapid detection capabilities are the sign of the credential-based attacks and which supports the principle of the zero trust in which continuous verification and rapid threat detection.

6.3 Non-Existing User Login Failure Attempts

This use case represents that the adversaries are trying to perform reconnaissance techniques for the identification of the user accounts which are valid and they try to recon them before launching the attacks, in this way they can probe the authentication network systems. The implementation of the zero-trust architecture provides the rapid detection of the any authentication attempts from the external or non-existing user (5710) or any usernames which are invalid. This scenario has shown great detection capabilities with more then 630 incidents detected. All these incidents were detected in less than 10 seconds, the mean time to detect (MTTD) for this use case is less than 10 seconds. Due to this use case, it mainly prevents the adversaries from gathering information and intelligence about the victims.

6.4 File Integrity Monitoring (FIM)

File Integrity monitoring (550,554) has the capabilities of monitoring all the important files and directories and if any one tries to modify the critical files or delete files or create any new file, (/etc/, /var/, /home/, /tmp/) it will trigger the FIM policy in near real time. The attacker tries to establish the access by deploying the reverse back door “reverse_shell.txt” and tries to perform data manipulation for maintain the long-term access in all the compromised system and how the zero-trust principle’s will be successful for defeating all the attempts. It is mainly used for real-time detection for the files, significant monitoring of the directories for protection against these threats. The total of 164 incidents were observed for this incident category and achieved the mean time to detect (MTTD) around 30 seconds which is 0.5 minutes which shows the near real time identification of the attempts of file modification or creation or deletion of file. This shows the rapid incident detection and containment.

6.5 SQL Injection Attack

The SQL injection attack executes and exploits the public facing application and it is used as a primary attack vector by the adversaries for gaining the access of the systems through the vulnerabilities present in the web application. The tool named SQL map was used and

implemented the pattern matching for all the SQL injection signatures such as Select, Union etc. The total of the 288 incidents were observed of this sophisticated attack and this method is mainly used by the attackers. This system had detected the real tie detection of all of these incidents of less than 10 seconds which near real time which show cases the immediate the detection capability of the solution. Also, there is another detection rule (31152) which triggered for Multiple SQL injection attempts from same source IP address and the total incidents observed for this particular event is 40 and the detection time for the incidents is less than 10 seconds.

6.6 Shell Shock Attack

The shell shock attack (31166, 31168) exploitation demonstrates the critical vulnerability which is being exploited by the APT groups for the remote code execution. This evaluation utilized the Metasploit framework modules for simulating the bash vulnerability with the crafted HTTP packets. The system had detected the bash functions and exploit patterns in HTTP and detected in real time. The total number of events which are captured are around 70 events and the detection time is less then 15 seconds.

6.7 Successful Login After Failed Login Attempts

This policy provides information about the possible credential attack for achieving the successful authentication after multiple failure attempts (40112) and it is an indication of the account which has been compromised. The corelation and detection technique work in a way where multiple authentication failure occurs followed by the successful login in the time span of 240 seconds. The total of 6 incidents were captured and the mean time to detect the incident was 240 seconds.

6.8 Detection of Unauthorised Process

This scenario demonstrates that all the processes which are unauthorised and running and network listeners for the command-and-control communications. The evaluation consists of the testing and monitoring the running processes for the net cat which are net cat listening sessions which is an indication for the backdoor access. The total of 8 incidents were observed and achieved the mean time to detect of around 900 seconds. This detection time provides and reflects the schedules process and detecting in near real time.

Below is the graph for the APT scenarios chart

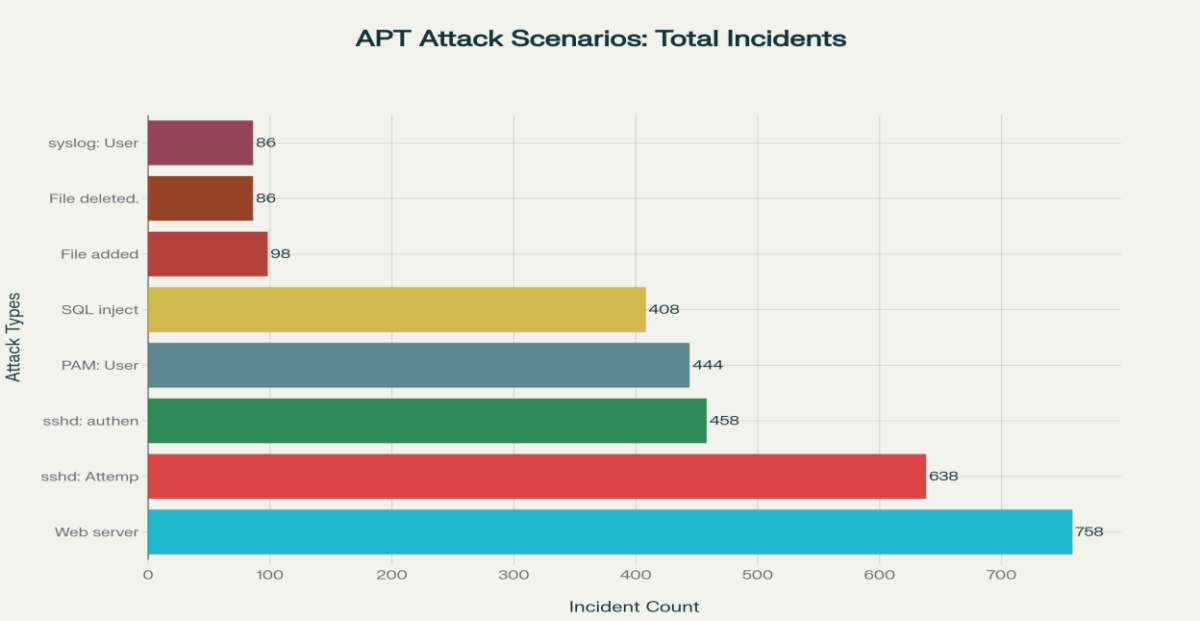

Figure 2: Incident Count

Below is the graph for the MITRE ATT&CK Techniques used in the specific APT scenarios.

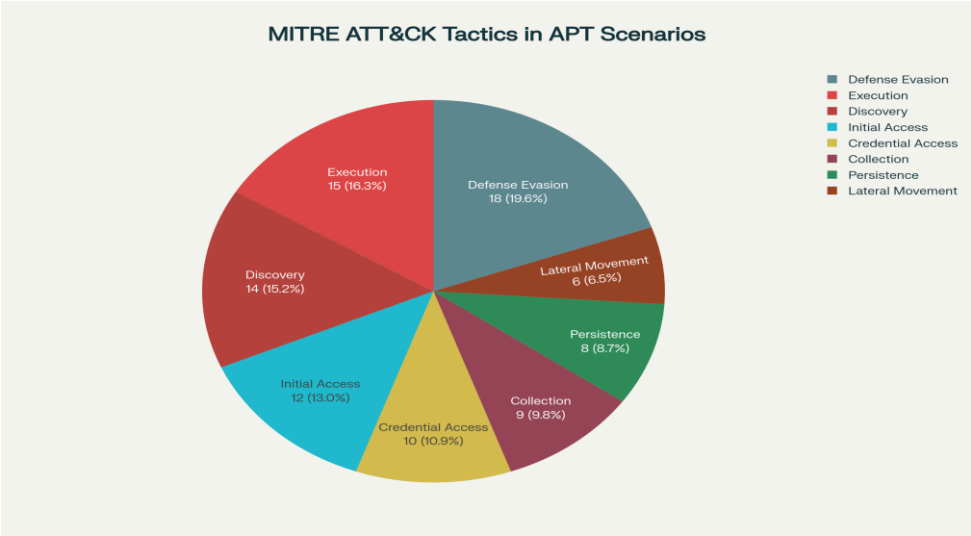

Figure 3: MITRE ATTACK Graph

6.9 Discussion

The Discussion part of the study provides in-depth information about the key findings and the evaluation about the detection and mitigation of the APT threats using zero trust architecture and utilizing Wazuh as security monitoring tool for the whole detection and mitigation process. The below table includes the whole summary of the total events occurred and the false positives identified and about all the raw events.

Metrics	Values

Total Raw Events	3772
False positive Events	2510
Relevant Incidents Identified	1262
Noise Reduction	33.45%
Attack vectors	8
MITRE ATT&CK Techniques Covered	7
Detection Precision of Security Events	100%

Table 5: Metrics

The implementation results of the key performance metrics are as follows

Use-cases	**Total Incidents**	**Mean Time to Detect (MTTD)**	**Mean time to Respond (MTTR)**	**Performance category**
SSH Brute Force	22	72.28 Seconds	0.46 seconds	Fast detection and response
Multiple Authentication Failures	86	5 Seconds	N/A	Fast
Non-Existing User Login Attempts	630	<5 seconds	N/A	Real Time
File Integrity Monitoring (FIM)	164	30 seconds	N/A	Fast
Detection of Unauthorized processes	8	900 seconds	N/A	A bit slow compared to others
Detection of SQL Injection Attack	288	<5 seconds	N/A	Real Time
Detection of Shell shock Attack	50	<5 seconds	N/A	Real Time
Successful logins after multiple failed attempts	6	240 seconds	N/A	Medium

Table 6: Key Performance

False Positive Management

The Implementation of automated responses to all eight rules of detection can lead to the lot of operations risks in the system infrastructure. Rules such as non-existing user attempts (5710), files integrity monitoring (550/554) and some failed access and then subsequent successful logins (40112) need contextual analysis which can only be provided by human intervention These rules could be triggered by legitimate system updates or user typos, or the administrative activity, and the ban in case of automation may lead to stop and disrupt important business processes.

Performance and Detection Capabilities

The implemented framework has successfully processed 3772 security events and out of which 1262 were identified as the incidents which were related to the APT attack scenario and achieved 34% effectiveness rate for detection and automated response to threats. The performance of the framework exceeds the expectation in the field of real time detection of threats as all the detection of threats was 76% and were detected in near real time. Also, the ability of the framework of detecting the high volume of security incidents indicates the robustness and maintains 100% detection rate precisely.

Comparative Analysis with the Base Paper

As per the comparison with the base paper which is the foundational research paper by Ahn et al. (2024) demonstrates that the comparable and higher-level performance metrics. It basically reported the reduction in MTTD up to 40%-50% and improvements in MTTR up to 30% in the research and produced more significant improvements in the results through the real time detection capabilities. The framework provided around 76% detection capabilities with relation to APT attack scenarios signifies the proactive threat management abilities of the proposed framework. Also, the framework's exceptional capabilities of noise reduction of around 66% percent are up to the mark as per the industry standards and provide efficiency in filtering the relevant events from the regular and routine system events and activities.

Mapping of the MITRE ATT&CK Integration and its Effectiveness

The mapping of seven different MITRE ATT&CK techniques to the six stages of the cyber kill chain confirms how the framework can cover all stages of the cyber kill chain. The integration allows specific grouping of the attack vectors, initial reconnaissance (T1087.001), exploitation (T1190, T1068), command and control activities (T1071.001). Also, the framework's efficiency and detecting efficiency in SQL injection attacks (288 incidents) and shellshock attack (50 incidents). These types of incidents are strategic weaknesses that form key access points most commonly used in initiation vectors of APT Threats. Their real-time detection of these two classes of attacks effectively prevents the lateral movement and the undermining of privileges of any kind after its timely detection.

7 Conclusion and Future Works

This research provides in-depth insights about providing effectiveness for zero trust architecture and the mitigation of the threats with the help of the significant experimental study. This research provides and explains the answers to both of the research questions and also showcased the practical effectiveness of zero trust architecture in real world attack scenarios. According to the research questions the vital security mechanisms which are used in zero trust architecture for mitigation of threats are as follows:

Continuous Authentication and verification are represented in the implementation part which is on the principle never trust, always verify shows significant effectiveness and achieved exceptional and immediate detection rate and was able to successfully prevent the lateral movement attempts and all the credential-based attacks across all the attack scenarios. The Real time behaviour and security monitoring in which the integration of Wazuh SIEM tool and its custom detection rules provided the accurate threat detection and mapping all the attack scenarios with MITRE ATT&CK tactics and techniques. Network Isolation and micro segmentation is achieved through cilium network policies and its policies based in YAML demonstrated micro segmentation with file integrity monitoring accurately detected 164 incidents and within 30 seconds which is near real time detection. A perfect performance outcome was obtained through the strategic use of automated responses to SSH brute force attacks (Rule 5763) that realized an outstanding sub second response which is a near real time response, MTTR that is 100 percent enhancement as compared to manual responses. The appropriate mapping of all the detection rules with the seven MITRE ATT&CK tactics (T1110, T1078, T1190, T1565.001, T1049, T1059.007 and T1068) as a whole, covered well all the tactics of Initial Access, Credential Access, Discovery, and Impact providing the opportunity to proactively defend against known Adversaries methods.

According to the research question, there are some implementation challenges and limitations as well which are the complexity in the automation of all the policies which gets triggered in the environment and the strategy regarding the false positive and the approach regarding how to deal with the cases of detecting SQL injection, files integrity monitoring, and process detection without being sudden increase in the false positives and the limitation is that there is a need for the context analysis AI-based policies for the implementations in future. As the framework is designed for smaller organizations and all the experiments were performed in a controlled environment and in a virtual environment and there were some integration complexities which would append in the production environment as well. The key achievements include that the detection excellence provided the near real time detection for most of the attack scenarios and 0 seconds of immediate detection for 37% for the attack scenarios and real time detection which is around less than 30 seconds of detection for the remaining 63% of the scenarios and the resources optimization for the selected automated response for the specific policy provided 100% MTTR improvement and also the selective mapping of the MITRE ATT&CK tactics and techniques against the attack scenarios.

Some of the Limitations of the research are as follows

The scope of Automation: The elective automation as well-constructed but it can maximize the use of zero-trust architecture (ZTA) automation, but only 12.5 percent of the detection regulations have automatic reaction to incident with an impressive progression potential that can be achieved with adequate defences in place and the Virtual laboratory environments does not have enough complexity to provide the same level of stimulation as an enterprise network that contains a variety different systems, as well as regulatory restrictions and time constraints. The estimation of around 1200-1500 security incidences under analysis in this

paper are a rather small number when compared to those that are reported by enterprise infrastructures that report in more than 3,000 security incidents on a daily basis in this type of the environment. The scalability of the considered mechanisms therefore requires the help of the additional studies involving environments that produce much, higher amounts of alerts on daily basis and in the production environment.

Future Work

This research provides a foundational scope for the future investigation processes which can provide comprehensive advancements for zero trust implementation capabilities for mitigations of threats.

Integration of Threat Intelligence: Integration of Wazuh's cyber threat intelligence for CTI feeds which can improve the indicators of compromise (IOC) and indicator of attack (IOA), which are the detection capabilities.

Advancements in AI-driven analysis: Future work should focus on the development of (AI) models that can perform contextual analysis during complicated scenarios of attacks which even now require manual operation. On the basis of the SQL injection response patterns, file integrity violation patterns, and process anomaly handling patterns, safe automation of such routines could be implemented using machine-learning algorithms trained on the types of patterns found in the responses in order to minimize false positive and false negative risks and Behavioural Baseline Learning which a kind of a method where the adaptive artificial intelligence is present as time progresses to take the form of statistically representative standard organizational behaviour. It is believed that such ability will boost the success rate of finding insider threats and any other hidden adversary tactics and techniques due to its long-term and cumulative operational construct, in which detection success is inhibited in the rule-based framework of defence.

Implementation for Large scale Enterprises: Conduction the studies in the actual enterprise that can provide the validation of the study and can also provide real-world effectiveness and scalability for the automation approach. Designing specialized (ZTA) frameworks relevant to specific industries, such as healthcare, finance, government, would allow addressing such compliance requirements in each of the required industry, the unique threat profile within the industry and other operational challenges.

References

Ahn, G., Jang, J., Choi, S. and Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. *IEEE Access*, 12, pp.89291–89309. doi:https://doi.org/10.1109/access.2024.3417182.

Gambo, M.L. and Almulhem, A. (2025). *Zero Trust Architecture: A Systematic Literature Review*. [online] arXiv.org. Available at: https://arxiv.org/abs/2503.11659.

Hasan, M. (2024). *Enhancing Enterprise Security with Zero Trust Architecture*. [online] arXiv.org. Available at: https://arxiv.org/abs/2410.18291.

Karabacak, B. and Whittaker, T. (2022). Zero Trust and Advanced Persistent Threats: Who Will Win the War? *International Conference on Cyber Warfare and Security*, 17(1), pp.92–101. doi:https://doi.org/10.34190/iccws.17.1.10.

Phiayura, P. and Teerakanok, S. (2023). A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access*, 11, pp.19487–19511. doi:https://doi.org/10.1109/access.2023.3248622.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020). Zero trust architecture. *NIST Special Publication 800-207*, (800-207). doi:https://doi.org/10.6028/nist.sp.800-207.

Süzen, A.A. and Ceylan, O. (2024). THE ADVANTAGES AND IMPLEMENTATION CHALLENGES WITHIN THE SCOPE OF THE BASIC PRINCIPLES OF TRANSITION TO ZERO TRUST ARCHITECTURE. *International Journal of 3D Printing Technologies and Digital Industry*, 8(3), pp.416–427. doi:https://doi.org/10.46519/ij3dptdi.1556319.

Tsai, M., Lee, S. and Shiuhpyng Winston Shieh (2024). Strategy for Implementing of Zero Trust Architecture. *IEEE Transactions on Reliability*, pp.1–8. doi:https://doi.org/10.1109/tr.2023.3345665.

MITRE (2025). *MITRE ATT&CK*. [online] Mitre.org. Available at: https://attack.mitre.org/.

Ghasemshirazi, S., Shirvani, G. and Alipour, M.A. (2023). *Zero Trust: Applications, Challenges, and Opportunities*. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.2309.03582.

Ojo, A.O. (2025). Adoption of Zero Trust Architecture (ZTA) in the Protection of Critical Infrastructure. *Path of Science*, 11(1), p.5001. doi:https://doi.org/10.22178/pos.113-2.

Gupta, A., Gupta, P., Upendra Pratap Pandey, Pradeep Kushwaha, Bhanu Prakash Lohani and Kushank Bhati (2024). ZTSA: Zero Trust Security Architecture a Comprehensive Survey. doi:https://doi.org/10.1109/ic3se62002.2024.10593067.

Fernandez, E.B. and Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, [online] 89, p.103832. doi:https://doi.org/10.1016/j.csi.2024.103832.

Iordache, C.A., Dragomir, A.V. and Marian, C.-V. (2022). Public Institutions Updated Enhanced Biometric Security, Zero Trust Architecture and Multi-Factor Authentification. *2022 International Symposium on Electronics and Telecommunications (ISETC)*, [online] pp.1–4. doi:https://doi.org/10.1109/ISETC56213.2022.10010127.

Abdelmagid, A.M. and Diaz, R. (2025). Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems. *Risk Analysis*. doi:https://doi.org/10.1111/risa.70026.