International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 42 No. 2 January 2024, pp. 487-496

Zero Trust Architecture: A Comprehensive Approach to Incident Response Management

Muhamad Zein Satria[1], H.A Danang Rimbawa[2], I Made Wiryana[3]

[1]Cyber Defense Engineering Republic of Indonesia Defense University
Bogor, Indonesia
m_zein_s@rocketmail.com[1]

[2]Cyber Defense Engineering Republic of Indonesia Defense University
Bogor, Indonesia
hadr71@gmail.com[2]

[3]Gunadarma University
Depok, Indonesia
mwiryana@staff.gunadarma.ac.id[3]

Abstract— Zero Trust Architecture is a modern security strategy that is based on the principle of "never trust, always verify". This approach to security eliminates trust from an organization's network architecture and focuses on managing enterprise risk management practice throughout the four phases: identification, assessment, response, and monitoring and reporting. Incident response refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. An effective incident response plan can help cybersecurity teams detect and contain cyberthreats and restore affected systems faster, reducing the lost revenue, regulatory fines and other costs associated with these threats. Zero Trust architecture can be aligned with the four general categories of risk response strategies: tolerate, operate, monitor, and improve. By design, telemetry, state information, and risk assessment from threat protection feed into the Zero Trust policy engine to enable automatic response to threats. In this paper, we present a comprehensive approach to incident response management using Zero Trust Architecture. We discuss the key principles of Zero Trust Architecture and how it can be applied to incident response management to improve an organization's overall security posture..

Keywords— Zero Trust Architecture, Comprehensive Approach, Incident Response Management, modern security strategy

I. INTRODUCTION

Through the development of smarter tools and services, technological advancements lead to the creation of new and more practical ways of life. Organizations face a rising number of cyber risks and security breaches as IT systems develop. At the same time, hackers' and bad actors' skills are being adapted and improved at an astounding rate [1]. Antivirus software and firewalls are no longer enough to protect against these threats, which calls into question more traditional security measures. As a result, there is an increasing demand for more sophisticated security measures.

One such strategy is Zero Trust Architecture, a modern security approach based on the principle of "never trust, always verify". This approach eliminates trust from an organization's network architecture and focuses on managing enterprise risk management practice throughout the four phases: identification, assessment, response, and monitoring and reporting.

In this paper, we present a comprehensive approach to incident response management using Zero Trust Architecture. We

Corresponding Author: Muhamad Zein Satria

discuss the key principles of Zero Trust Architecture and how it can be applied to incident response management to improve an organization's overall security posture. We also provide practical examples and case studies to illustrate the effectiveness of this approach in real-world scenarios.

II. ZERO TRUST ARCHITECTURE (ZTA)

ZTA was proposed by Kindervag, principal analyst at Forrester in 2010. In a zero-trust architecture, all traffic cannot be trusted, and location cannot be used as a basis for security. Instead, security measures need to be taken for all access, minimum authorization policies and strict access control are adopted, and all traffic needs to be visualized and analyzed. These concepts are significantly different from the traditional perimeter-based security architecture, and the security is stronger [2].

The core goal of zero trust is to allow users in untrusted network areas to access trusted areas through authentication and policy control, as shown in Figure 1.

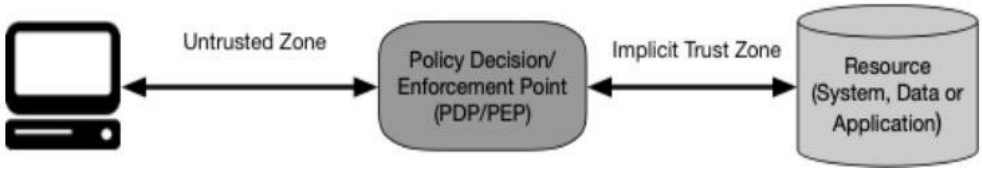

Figure 1: Zero Trust Access [3]

In order to reduce the security risk of the access process, a continuous dynamic security access control technology is required, which is not based on the network location of the access subject, but authorizes the access subject based on the security and trust status before each access object is allowed to access; continuously monitors the security of the entire access process and assesses the trust status; dynamically adjusts access rights and implements fine-grained security access control.

To achieve this goal, more network elements are needed to support the entire zero trust architecture. The ZTA architecture given by NIST is shown in Figure 2.

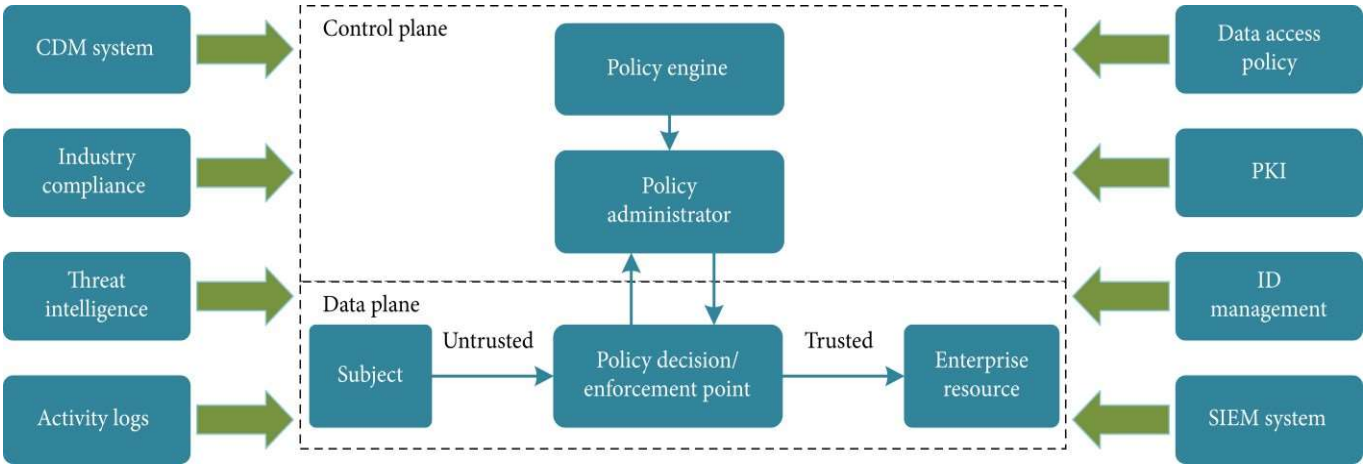

Figure 2. Typical zero trust architecture. [2]

Among them, the identity management (ID management) system and the enterprise public key infrastructure (PKI) are mainly used for the authentication of personnel and equipment, which is the basis. The data access policy mainly provides resource access policy, and the security information and event management system (SIEM system) provide the security information and event management of the entire architecture. At the same time, to integrate capabilities such as industrial compliance policies and threat detection, more attention needs to be paid to continuous diagnostics and mitigation (CDM) systems.

In general, the ZTA is based on identity, giving digital identities to people and devices, and setting minimum permissions for access subjects; aiming at business security, realizing business concealment, transmission encryption, and fine control; with continuous trust assessment as the guarantee, including user trust assessment, environmental risk determination, and abnormal

behavior discovery; using dynamic permission control as a means, including attribute-based access control baseline, trust level-based hierarchical access, and risk-aware dynamic permissions.

The zero-trust architecture focuses on the security capabilities of identity, trust, access control, permissions, and other dimensions, and these security capabilities are also an indispensable part of the information-based business system, so zero trust is inherently a kind of "endogenous security." In a sense, it is a spiral sublimation of business and security. From the initial business system to complete business goals, security equipment realizes the mutual independent system of security assurance, and integrates into a close relationship between security and business, and returns to security and application again.

III. Incident Response Management

Incident response management is a critical process within an organization's IT infrastructure. It involves the identification, investigation, and resolution of security incidents within a network. The goal of incident response management is to handle the situation in a way that limits damage and reduces recovery time and costs.

The first step in incident response management is the detection of an incident. This can be achieved through various means such as automated monitoring tools or reports from users. The detection phase is crucial as it sets the stage for the subsequent steps in the incident response process.

Once an incident has been detected, it's important to establish clear lines of communication. This involves setting up a dedicated chat room or conference call for the incident response team. Clear communication ensures that all team members are on the same page and can work together effectively to resolve the incident.

The next step in the process is to assess the impact of the incident on the organization's operations and assign a severity level. This assessment helps prioritize the response efforts and ensures that resources are allocated appropriately. The severity level can range from low, indicating a minor issue, to critical, indicating a major threat to the organization's operations.

Keeping customers informed about the incident and what steps are being taken to resolve it is another important aspect of incident response management. This involves regular updates and transparent communication about the progress of the resolution efforts. It helps maintain trust between the organization and its customers during a potentially disruptive event.

Depending on the nature of the incident, it may be necessary to escalate it to specific individuals or teams within the organization. This could include senior management, legal counsel, or specialized IT teams. Escalation ensures that those with the necessary expertise and authority are involved in managing and resolving the incident.

Each member of the incident response team should have a clear understanding of their role and responsibilities during an incident. This includes knowing who is responsible for what tasks, how to communicate with other team members, and what actions to take at each stage of the process.

The final step in incident response management is resolving the incident and restoring normal service. This involves identifying and implementing a solution to the problem, testing to ensure that the solution is effective, and monitoring to prevent recurrence of the issue.

In addition to these steps, it's important for organizations to conduct a post-incident review. This involves analyzing what happened, why it happened, how it was handled, and what could be done better in the future. The insights gained from this review can help improve future incident response efforts.

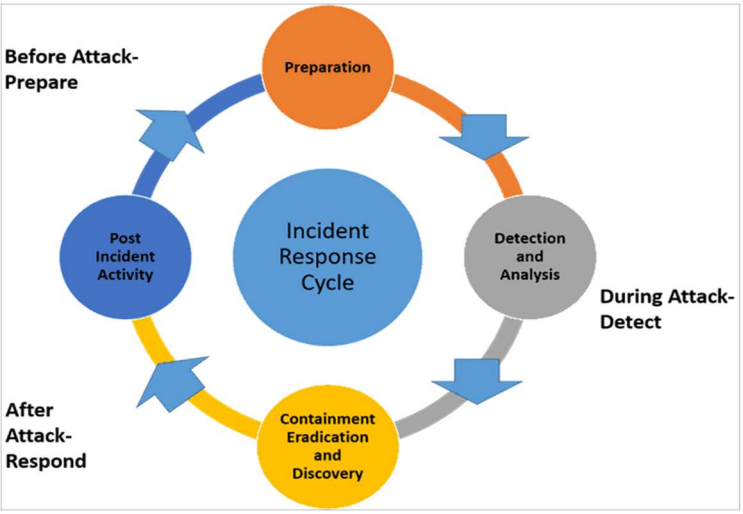

Figure 3. NIST Incident Response Cycle. [4]

3.1 Example Study Case Secure Growth at Retail Giant "ShopSmart" Ransomware Attack

ShopSmart, a leading retail chain with hundreds of stores and millions of online customers, faced increasing cybersecurity challenges. Their legacy security approach, reliant on perimeter defenses and limited access control, proved vulnerable to evolving threats like ransomware and data breaches. To safeguard sensitive customer data, operational integrity, and brand reputation, ShopSmart embarked on a strategic Zero Trust Architecture (ZTA) implementation aligned with the NIST Cybersecurity Framework and its incident response lifecycle.

Challenges:

- Distributed network: Hundreds of physical stores and diverse online systems created a complex attack surface and management challenges.
- Data security concerns: Customer financial information, purchase data, and loyalty program details required robust protection.
- Remote workforce: An expanding remote workforce necessitated secure access solutions beyond traditional VPNs.
- Incident response limitations: The existing setup hindered efficient detection, investigation, and containment of security incidents.

ZTA Implementation:

To address these challenges, ShopSmart partnered with a cybersecurity specialist to design and implement a ZTA solution aligned with the NIST incident response lifecycle. The core components included:

- Identity and Access Management (IAM): Centralized platform for user authentication, authorization, and multi-factor authentication (MFA) for all access attempts.
- Micro-segmentation: Network segmentation of stores, online systems, and data based on function and sensitivity, limiting lateral movement in case of breaches.
- Least Privilege Access: Granular access control policies granting users only the minimum privileges required for their roles and tasks.
- Continuous Monitoring: Real-time monitoring of user activity, device posture, and network traffic for anomalous behavior and potential threats.
- Security Information and Event Management (SIEM): Centralized platform for collecting and analyzing security events, facilitating incident detection and investigation.

- Automated Response: Integration with SOAR (Security Orchestration, Automation, and Response) to automate containment and remediation actions.

NIST Incident Response Cycle and ZTA Effectiveness:

Table 1. NIST Phase related to ZTA contribution

NIST Phase	ZTA Contribution
Preparation	
* Identify: Continuous monitoring and SIEM identified unusual network activity in a specific store.	ShopSmart's security operations center (SOC) received an alert from the SIEM about suspicious file transfers initiated from a POS terminal in Store #123.
* Protect: Micro-segmentation and least privilege access limited the potential impact.	The attack only affected POS systems within Store #123 due to micro-segmentation, and limited user access prevented attackers from encrypting critical back-office data.
* Contain: Automated response measures quickly isolated the threat.	SOAR automatically shut down network access to the compromised POS terminal, preventing further lateral movement and encryption attempts.
Detection and Analysis	
* Detect: Continuous monitoring and anomaly detection flagged suspicious activity.	The SIEM and network anomaly detection system identified unusual outbound traffic patterns and unauthorized file access attempts on the compromised POS terminal.
* Analyze: Detailed logs and audit data from ZTA facilitated investigation.	ShopSmart's incident response team used detailed logs and user activity data to trace the attack vector and identify the specific vulnerability exploited.
Containment, Eradication, and Recovery	
* Contain: Micro-segmentation prevented further spread.	Micro-segmentation ensured the attack remained confined to Store #123, minimizing downtime and data loss across other stores and online systems.
* Eradicate: Automated response and manual intervention neutralized the threat.	SOAR quarantined the infected POS terminal, and the IT team swiftly patched the exploited vulnerability.
* Recover: Backups and disaster recovery plan enabled swift restoration.	ShopSmart restored the affected POS terminal from backups and resumed operations within minimal downtime.
Post-Incident Activity	
* Lessons Learned: Detailed data and logs informed future prevention strategies.	The incident response team analyzed logs and identified a need for additional training on phishing awareness and stricter endpoint security posture checks.
* Improvement: ZTA facilitated continuous adaptation and refinement.	ShopSmart implemented stricter MFA policies, enhanced endpoint security monitoring, and further segmented sensitive data access based on lessons learned.

IV. Benefits Of Zta In Incident Response Management

Incident Response Management is a critical aspect of cybersecurity, aimed at effectively detecting, containing, and mitigating security incidents. Zero Trust Architecture (ZTA) introduces a paradigm shift that offers several significant benefits to the incident response process.

One of the key benefits of ZTA in incident response management is enhanced incident detection and response. ZTA mandates continuous monitoring of network activities, ensuring that security incidents are detected in real- time or near-real-time. This proactive approach allows incident response teams to identify potential threats as they emerge, reducing the dwell time of attackers within the network.

ZTA also enforces granular access controls, meaning that entities are only allowed access to resources they explicitly require for their tasks (the principle of least privilege). This significantly reduces the attack surface, making it harder for attackers to move laterally within the network undetected. Continuous authentication is a core component of ZTA. Users and devices are continuously authenticated as they interact with network resources. Any deviations from expected behavior trigger alerts and potentially lead to access revocation. This proactive approach ensures that only authorized entities are granted access.

Another benefit of ZTA in incident response management is increased incident response agility. ZTA's emphasis on micro-segmentation allows for the immediate containment of security incidents. When a breach is detected, affected segments can be isolated swiftly, preventing the incident from spreading further. ZTA also allows for the dynamic enforcement of security policies based on real-time data. If an entity's behavior becomes suspicious or non-compliant with policies, the system can automatically adjust access controls or trigger alerts, enhancing incident response agility.

To illustrate the tangible benefits of ZTA in incident response management, it is useful to consider case studies or examples of organizations that have successfully implemented ZTA and experienced improved incident response outcomes. These examples can highlight instances where ZTA played a crucial role in early threat detection, rapid containment, and effective mitigation of security incidents. They can also showcase how ZTA contributed to minimizing the impact of security breaches, reducing recovery times, and ultimately enhancing an organization's overall cybersecurity posture.

Incorporating these elements into your research paper will provide a comprehensive understanding of how Zero Trust Architecture (ZTA) positively influences incident response management by bolstering incident detection, response agility, and overall security resilience. It is through such benefits that ZTA has the potential to transform incident response strategies in the face of evolving cyber threats.

The implementation of Zero Trust Architecture can help organizations improve their overall security posture by providing a more secure and robust framework for managing incidents. By continuously monitoring network activities and enforcing granular access controls, ZTA helps reduce the attack surface and makes it harder for attackers to move laterally within the network undetected.

Continuous authentication is another key component of ZTA that helps enhance incident detection and response. By continuously authenticating users and devices as they interact with network resources, any deviations from expected behavior can trigger alerts and potentially lead to access revocation. This proactive approach ensures that only authorized entities are granted access.

ZTA's emphasis on micro-segmentation also allows for increased incident response agility. When a breach is detected, affected segments can be isolated swiftly, preventing the incident from spreading further. The dynamic enforcement of security policies based on real-time data also enhances incident response agility by allowing the system to automatically adjust access controls or trigger alerts if an entity's behavior becomes suspicious or non- compliant with policies.

Zero Trust Architecture offers several significant benefits to the incident response process by enhancing incident detection and response, increasing incident response agility, and improving overall security resilience. By incorporating case studies and examples of successful implementations of ZTA into your research paper, you can provide a comprehensive understanding of how this modern security approach positively influences incident response management in the face of evolving cyber threats. [5]

V. Limitations Of Zta In Incident Response Management

Although Zero Trust Architecture (ZTA) has a number of important advantages for incident response management, it is not without drawbacks.[6]

ZTA's key drawback is that it necessitates constant observation of network activity. This can be time- and resource-consuming, and it might call for sizable investments in technologies and monitoring systems. Furthermore, the sheer amount of data produced by continuous monitoring can be deafening, making it challenging for incident response teams to discern possible dangers from the background noise.

Granular access limitations that ZTA implements are still another drawback. While this helps lessen the attack surface, it can also make managing access rights more difficult1. With so many users and resources, large enterprises can make this especially difficult.

A key element of ZTA, continuous authentication, might potentially pose difficulties. While implementing continuous authentication properly might increase security, it can also reduce user irritation. Users may resist implementing the ZTA model because they find frequent authentication requests annoying.

ZTA's focus on micro-segmentation makes it possible to immediately contain security problems. Micro- segmentation implementation, however, can be difficult and time-consuming. It necessitates a thorough comprehension of the network architecture and the relationships between the various network components.

The ZTA's dynamic policy enforcement is another element that might be problematic. To reflect changes in the threat environment and organizational requirements, policies must be revised frequently. The incident response team must continue to put up effort and be vigilant in this regard.

It's crucial to remember that ZTA is still a relatively new method to cybersecurity despite these drawbacks. As the model develops and more firms use it, many of its problems are probably going to be solved. Furthermore, especially in settings where security is a top priority, the advantages of ZTA frequently outweigh its drawbacks.

While ZTA has a number of important advantages for incident response management, it is not without drawbacks. The resource-intensive nature of continuous monitoring, the difficulty of managing granular access controls, user resistance to continuous authentication, the difficulty of establishing micro-segmentation, and the continual work needed for dynamic policy enforcement are a few examples. However, as the model develops and more businesses use it, these shortcomings are probably going to be overcome.[7].

VI. Implementation Of Zta In Incident Response Management Strategy

There are several important procedures and factors to take into account when using Zero Trust Architecture (ZTA) in incident response management strategy. The "never trust, always verify" tenet forms the basis of ZTA, a contemporary security strategy. With this strategy, trust is removed from the network architecture of a business and enterprise risk management is managed through the four steps of identification, assessment, reaction, and monitoring and reporting.

The practice of thoroughly identifying assets and risks is the first step in integrating ZTA into an incident response management strategy. Based on effect analysis, the system and information that are processed, stored, and communicated are categorized. Prioritization is followed by efforts to detect threats and asset vulnerabilities. The identity, endpoint, network, data, application, and infrastructure pillars are the six components that make up the Zero Trust architecture, which places an emphasis on the complete coverage of organizational assets throughout the whole digital estate. Following the reference design would give firms a comprehensive understanding of their IT environments and the risks involved.

The implementation of granular access restrictions is the next stage after the identification and evaluation of the assets and hazards. ZTA upholds the principle of least privilege by enforcing granular access rules, which limit an entity's access to resources that they explicitly need to complete a task. Because of the large reduction in the attack surface, it is more difficult for attackers to move covertly around the network. [8]

Another crucial ZTA component that must be deployed as part of an incident response management plan is continuous authentication. In order to access network resources, users and devices must continually authenticate themselves. Any departure

from the intended behavior sets off alerts and could result in access being revoked. By being proactive, access is restricted to just authorized parties.

The ZTA's focus on micro-segmentation is essential for incident response management as well. When a breach is found, the impacted areas can be quickly segregated, stopping the situation from getting worse. This makes it possible to quickly contain security incidents.

Another ZTA component that must be incorporated as part of an incident response management plan is dynamic policy enforcement. ZTA enables real-time data-driven dynamic security policy enforcement. The system can automatically change access limits or raise alarms if an entity's activity starts to look suspect or out of line with policy requirements, improving the agility of incident response.

Numerous important procedures and factors must be taken into account when implementing Zero Trust Architecture in incident response management approach. The implementation of granular access controls, continuous authentication, micro-segmentation, and dynamic policy enforcement are a few of these. They also entail undertaking a thorough asset discovery and risk identification procedure. Organizations can improve their incident response skills and overall security posture by implementing these measures and the ZTA tenets.[9]

The importance of ongoing improvement in your ZTA implementation that can follow Zero Trust Operations: Continuous Improvements. This means that should regularly review ZTA policies, procedures, and technologies to ensure that they are still effective in meeting your security needs.

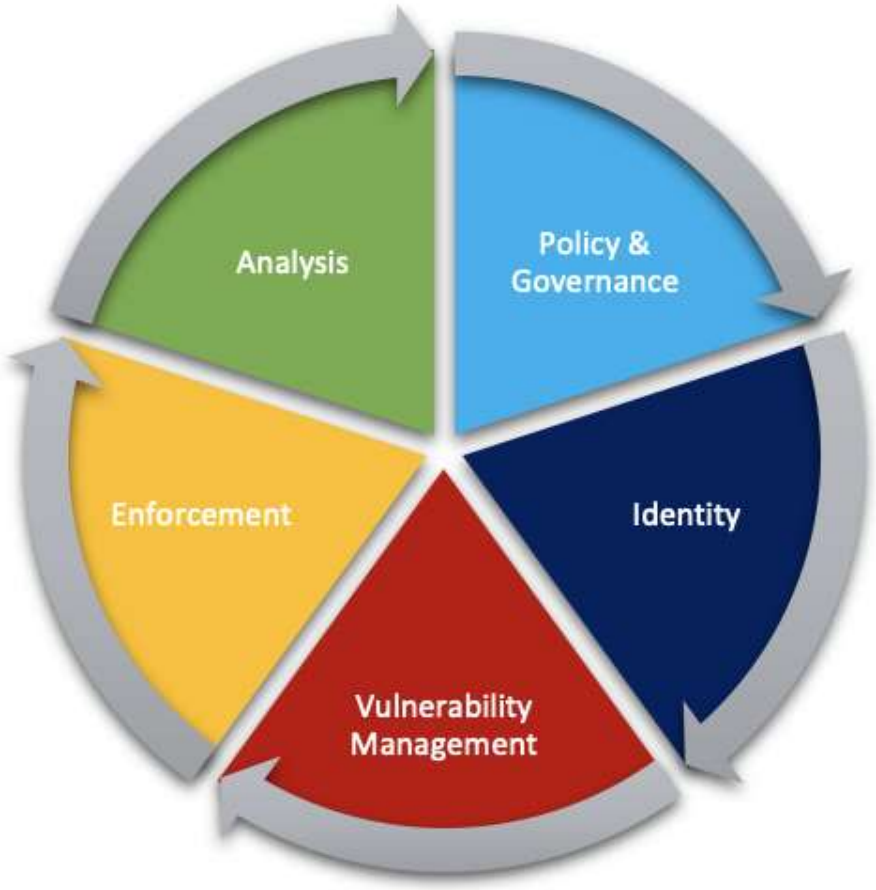

Figure 4. Zero Trust Operations: Continuous Improvements. [10]

Policy & Governance: Clearly defined policies and governance structures are essential for ensuring that everyone in the organization understands and adheres to the principles of ZTA. This helps to minimize the risk of unauthorized access and data

breaches.

Identity: Strong identity management practices are crucial for accurately identifying and authenticating users and devices before granting them access to resources. This helps to prevent attackers from impersonating legitimate users and gaining access to sensitive data.

Vulnerability Management: Regularly identifying and patching vulnerabilities in systems and applications is essential for reducing the attack surface and making it more difficult for attackers to exploit vulnerabilities.

Enforcement: Implementing granular access controls and security measures helps to prevent unauthorized access and limit the damage that can be caused by a security incident.

Analysis: Continuously monitoring and analyzing network activity, user behavior, and system logs helps to detect suspicious activity and identify potential security incidents early on.

VII. CONCLUSIONS

Zero Trust Architecture is a modern security approach that offers a comprehensive solution to incident response management. By eliminating trust from an organization's network architecture and focusing on managing enterprise risk management practice throughout the four phases of identification, assessment, response, and monitoring and reporting, Zero Trust Architecture provides a robust framework for detecting and responding to cyberthreats. An effective incident response plan, aligned with the principles of Zero Trust Architecture, can help cybersecurity teams detect and contain cyberthreats, restore affected systems faster, and reduce the costs associated with these threats. In this paper, we have presented a comprehensive approach to incident response management using Zero Trust Architecture and discussed how its key principles can be applied to improve an organization's overall security posture. By adopting this approach, organizations can enhance their incident response capabilities and better protect themselves against evolving cyber threats.

By implementing ZTA aligned with the NIST incident response lifecycle, organizations can significantly improve their incident response capabilities in the following ways: Faster detection and isolation: ZTA's micro-segmentation and continuous monitoring capabilities can help to quickly identify and isolate security incidents, minimizing the potential damage. Improved containment and remediation: ZTA's least privilege access and automated response capabilities can help to contain security incidents and remediate them more quickly and effectively. Enhanced forensics: ZTA's detailed logging and auditing data can provide valuable insights for incident investigation and root cause analysis. The "never trust, always verify" approach and granular access controls minimized their attack surface, enabled faster threat detection and containment, and ensured business continuity and data security.

REFERENCES

[1] Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. Security and Communication Networks, 2021, 1-10.

[2] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022.

[3] Stafford, V. A. (2020). Zero trust architecture. NIST special publication, 800, 207.

[4] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST Special Publication, 800(61), 1-147.

[5] Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436.

[6] community paper (n.d.). The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment. Www3.Weforum.org. Retrieved September 7, 2023, from https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf

[7] John P. Pironti (2020, April 1). Five Key Considerations When Adopting a Zero-Trust Security Architecture. Www.Isaca.org. Retrieved September 7, 2023, from https://www.isaca.org/resources/news- and-trends/newsletters/atisaca/2020/volume-7/five-key-considerations-when-adopting-a-zero-trust- security-architecture

[8] Kudrati, A. (2022, May 23). What's risk management and why is it important? Microsoft. Retrieved September 7, 2023, from https://www.microsoft.com/en-us/security/blog/2022/05/23/how-to-improve-risk- management-using-zero-trust-architecture/

[9] Kerman, A., Borchert, O., Rose, S., & Tan, A. (2020). Implementing a zero-trust architecture. National Institute of Standards and Technology, 2020, 17-17.

[10] Green-Ortiz, C., Fowler, B., Houck, D., Hensel, H., Lloyd, P., McDonald, A., & Frazier, J. (2023). Zero Trust Architecture. Cisco Press