CYBER SECURITY INCIDENT RESPONSE AND MANAGEMENT

Naveen
CSE-IS
Chandigarh Univeristy
Mohali
21BCS3572@cuchd.in

Saurav Vatsyaayan
CSE-IS
Chandigarh University
Mohali
21BCS3541@cuchd.in

GoravSaini
CSE-IS
Chandigarh University
Mohali
21BCS4344@cuchd.in

Dhanesh Kumar Patel
CSE-IS
Chandigarh University
Mohali
21BCS4263@cuchd.in

Ms.Komal Mehta
Department of AIT-CSE
Chandigarh University
Kharar Punjab India

Abstract— The aim of the Cyber Security Incident Response and Management initiative is to create a structured approach for detecting, managing, and recovering from cybersecurity incidents. In light of the rise in advanced cyber threats, organizations need to be prepared to tackle situations that could threaten data integrity, operational continuity, and corporate reputation. Besides post-event evaluation for continuous enhancement, this project provides a comprehensive structure that encompasses threat detection, incident categorization, containment, elimination, and recovery strategies.

Through advanced monitoring systems, problems are detected instantly within this framework, and rapid response actions are implemented based on an established system of classification and urgency. Threats are effectively removed and systems are reinstated without any outstanding vulnerabilities due to containment and eradication methods.

This initiative establishes a proactive, equipped response team for the business by implementing established response protocols, playbooks, and regular training sessions. This initiative significantly reduces the potential effects of cyber attacks on the company by safeguarding digital assets, maintaining operational continuity, and enhancing the overall security posture.

The Cyber Security Incident Response and Management initiative provides a structured approach for overseeing the entire lifecycle of cybersecurity incidents, from detection to recovery. Organizations need to be proactive in their defensive strategies as cyber attacks rise in frequency and complexity. This initiative aims to reduce the impact of such disasters by creating a systematic approach to tackle them, protecting sensitive information, ensuring business continuity, and strengthening the overall security framework.

Keywords— Intrusion Detection System, Network Monitoring , Traffic Analysis.

I. INTRODUCTION

The danger and complexity of cyberattacks have increased dramatically with the size and complexity of digital systems, requiring enterprises to make tremendous efforts to protect their infrastructure and data. Cyber Security Incident Response and Management (CSIRM) techniques are essential for quickly identifying, assessing, and reacting to security incidents in order to counter these new threats. Reactions that are prompt and effective can minimize damage, safeguard private information, and uphold legal compliance.

The development of a Security Information and Event Management (SIEM) system, which is essential to an active CSIRM strategy, is the main goal of this research project. A SIEM system gathers and analyzes security data from throughout an organization's network, enabling it to recognize, assess, and respond to potential threats. By employing advanced threat detection capabilities and real-time monitoring , SIEM systems assist firms in identifying anomalous patterns, gaining insight into possible dangers, and successfully handling events.

Our project's goal is to create a tailored SIEM solution that improves the process for incident detection and response, hence bolstering organizational cybersecurity resilience.This article will explore the SIEM framework, methodologies for acquiring and analyzing data, rules for detecting incidents, and integration of incident management, detailing how these components interact to increase security incident response effectiveness. We will also examine how our SIEM design aligns with established security frameworks and adapts to different organizational needs, providing a scalable, reliable solution for modern cybersecurity challenges.

By demonstrating a comprehensive incident response approach that enhances security operations and successfully lowers risks through the use of a customized SIEM system, this project aims to further the field of cybersecurity.

II. LITERATURE SERVEY

Cybersecurity Incident Response and Management (CIRM) is essential for organizations to efficiently identify, assess, and reduce security incidents. A vital aspect of CIRM is the deployment of a Security Information and Event Management (SIEM) system. SIEM tools collect, standardize, and evaluate data from multiple sources to detect possible security risks in real-time. By automating the gathering and assessment of security-related information, SIEM systems enhance incident detection and reaction abilities, which are crucial for mitigating the effects of cyberattacks.

Studies emphasize the importance of SIEM in enhancing incident response through ongoing surveillance of network activities, system logs, and user actions, aiding security teams in detecting suspicious behavior promptly (Patel et al., 2018). SIEM systems utilize event correlation methods to identify intricate attack patterns, including insider threats or advanced persistent threats (APTs), that may remain undetected by conventional security tools (Khanna & Manogaran, 2019). These tools additionally utilize machine learning algorithms to minimize false positives and enhance the precision of alerts, allowing security teams to concentrate on real threats.

Furthermore, the integration of SIEM systems with Security Orchestration, Automation, and Response (SOAR) platforms is becoming more frequent in contemporary cybersecurity frameworks. This integration facilitates automated reactions to incidents, including isolating affected devices, blocking harmful IP addresses, or activating containment measures, thus decreasing the duration needed to address attacks and lessening the opportunity for attackers (Schultz et al., 2020).

Nonetheless, in spite of the many advantages, SIEM systems face certain challenges. They frequently produce vast amounts of data, which can overwhelm security teams if not handled correctly. Furthermore, the challenge of combining SIEM with other security solutions and the struggle to adjust detection rules to minimize false positives continue to be major obstacles (Hassan & Khaled, 2017)

In conclusion, SIEM systems are vital to effective cybersecurity incident response, providing real-time visibility and automation that enhances the detection, analysis, and mitigation of threats. Their integration with other security tools and the adoption of machine learning techniques continues to evolve, improving incident response efficiency while addressing ongoing challenges in the field.

III . LITERATURE REVIEW

In Cyber Security Incident Response and Management, we can investigate different scholarly articles that concentrate on the approaches, techniques, and resources for handling incidents. The subsequent research papers can offer a thorough insight into the field, emphasizing both conceptual structures and applied methods.

Fig : Image to show the necessary steps in SIEM

Paper 1: "An Examination of Literature on Cybersecurity Incident Response"

Main Emphasis: This document offers a comprehensive examination of the current status of incident response methods throughout sectors, examining how companies manage cyber events. It also assesses the cybersecurity frameworks and incident response models such as NIST, ISO/IEC 27001, and SANS.

Main Discoveries: Phases of Incident Response: The document examines the typical stages involved in incident response, encompassing preparation, identification, containment, elimination, recovery, and insights gained.
Difficulties in Incident Response: It emphasizes frequent difficulties like a shortage of qualified staff, insufficient readiness, and delayed incident identification.

Incident Response Frameworks: It additionally contrasts various incident response frameworks, highlighting the efficiency of the NIST framework within large organizations.

Paper 2: " A Framework for Improving Cybersecurity Incident Response with Machine Learning"

Main Emphasis: This document introduces a novel framework aimed at enhancing incident detection and response utilizing the combination of machine learning (ML) and artificial intelligence (AI) technologies. It investigates the application of predictive models and anomaly detection to improve real-time incident identification.
Main Discoveries: AI and ML for Detection: The research demonstrates how ML algorithms are capable of examining past incidents information to forecast upcoming cyber hazards.
Automated Response: The article explores the ways in which automated systems for incident response can minimize response duration and enhance the precision of containment measures.
Challenges and Constraints: The document additionally highlights difficulties in implementing AI and ML for incident handling, including concerns related to data privacy

and system intricacy.

Paper 3: " A Survey on Cyber Incident Response and Prevention in Organizations"
Main Emphasis: This research paper examines the various methods that organizations, regardless of size, utilize to address incident reaction. The research analyzes the readiness for incident response and the duration of response across different sectors, offering a statistical evaluation of their efficiency.

Main Discoveries:
Incident Prevention vs. Response: The study reveals that numerous organizations emphasize prevention over response plan .

Organizational Readiness: It highlights the usual deficiencies found in organizations, encompassing insufficient employee training, obsolete incident response strategies, and inadequate interaction during emergencies.

Recommended Strategies: The document provides numerous recommended strategies for enhancing incident response, such as standard exercises, upholding current response strategies, and enhancing interdepartmental

Paper 4: "Improving Cyber Incident Response through Post-Incident Reviews"

Main Emphasis: This document highlights the review process that follows an incident, an essential component of ongoing enhancement in incident management. The authors contend that examining previous occurrences and Recognizing weaknesses can enhance upcoming responses.

Conclusions:
Post-Incident Evaluation: Highlights the necessity for an organized post-incident assessment, in which Each phase of the incident management process is examined forenhancement.

III. DESIGN FLOW OF SIEM SYSTEM

Establishing a SIEM system necessitates meticulous planning, design, and execution, usually adhering to a structured process to meet particular needs. The workflow for a SIEM project encompasses the subsequent stages:

1. Collecting and Analyzing Requirements

• Identify Security Goals: Recognize the specific security requirements of the organization, its tolerance for risk, and compliance obligations (e.g., GDPR, HIPAA).

• Identify Data Sources: Ascertain which data sources are essential for monitoring (e.g., firewalls, IDS/IPS, web servers,applications,endpoints).

• Assess Compliance Requirements: Recognize the regulatory obligations that the SIEM needs to fulfill, including data retention, audit logs, and incident documentation

2. Design of Architecture

- SIEM Elements and Implementation Model: Select from on-premises, cloud, or hybrid options according to the organization's resources and security protocols.

- Data Gathering Layer: Establish techniques for collecting logs and events from various sources, such as network devices, endpoints, servers, and cloud infrastructures.

- Data Storage: Design a scalable data storage system that accommodates large-scale log ingestion while ensuring performance and satisfying retention needs.

3. Correlation of Events and Detection of Threats

• Correlation Guidelines: Create tailored guidelines to spot threats suited to the organization's unique threat environment, integrating indicators of compromise (IoCs) to highlight incidents.

• Machine Learning (Optional): Incorporate ML models to examine behavior and identify anomalies that could suggest zero-day attacks or insider threats.

4. Reporting and Analyzing After an Incident

• Incident Documentation and Reporting: Create templates for post-incident evaluations, encompassing root cause and impact analysis.

• KPI Monitoring: Establish monitoring for metrics like Mean Time to Detect (MTTD) and Mean Time to Respond.

IV. CONCLUSION

In the modern, highly interconnected world, cybersecurity stands as one of the most vital components of an organization's framework. As companies grow their digital presence, the occurrence, complexity, and consequences of cyber-attacks are on the rise. To successfully address these shifting threats, organizations must create strong security frameworks that not only avert but also identify, react to, and handle cybersecurity incidents. Creating a Security Information and Event Management (SIEM) system in the context of Cybersecurity Incident Response and Management (CIRM) is crucial for reaching these goals. This initiative aimed at creating and executing a SIEM system that improves the capacity of organizations to identify, handle, and react to security events in real-time.

V. REFERENCES

[1]. "Deep Learning-Based Sign Language Recognition and Translation: A Survey" by

Heng Zhang, Yi Wang, and Xin Yu. (Published in 2020)

[2]. Han, J., Zhang, D., Xu, C., & Shao, L. (2013). Enhanced computerized facial recognition using advanced statistical discriminant measures and neural network-based fusion.
IEEE Transactions on Instrumentation and Measurement, 62(1), 206-220.

[3]. Improving Sign Language Recognition and Translation with Transformer Models" by Julia Mendez, Carlos Gómez, and Isabel García. (Published in 2021).

[4]. Lazar, J., Feng, J. H., & Hochheiser, H. (2017). Research methods in human-computer interaction. Morgan Kaufmann.
[5]. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (CCS '15).
[6]. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389-399
[7]. Kwaśniewska, A., & Przybyszewski, K. (2020). AI-based solutions for visually impaired people: Challenges and prospects. Journal of Assistive Technologies, 14(2), 156-166.
[8]. Ahmed, S., & Gupta, A. (2019). Sign language recognition using deep learning: A review. Pattern Recognition Letters, 123, 33-40.
[9]. Zhou, H., & Huang, T. (2020). Real-time sign language recognition using convolutional neural networks. IEEE Transactions on Human-Machine Systems, 50(5), 441-450.
[10]. Smith, A., & Jones, B. (2021). Accessibility and AI: Bridging the communication gap for the blind. Journal of Artificial Intelligence Research, 12(3), 201-215.
[11].https://images.app.goo.gl/eYjYArfFwKNQEWcw6

[12] Northcutt, S., Novak, J., & McLachlan, J. (2001). Network Intrusion Detection: An Analyst's Handbook. New Riders Publishing.
[13]Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou, N., Abu-Nimeh, S., & Lee, W.

(2012). From throw-away traffic to Bots: Detecting the rise of DGA-based malware. In USENIX Security Symposium (pp. 24-24).
[14]Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., & Kruegel, C. (2011). Your botnet is my botnet: analysis of a botnet takeover. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 635-647).

[15]Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001).
Estimating the support of a high-dimensional distribution. Neural computation, 13(7), 1443- 1471.
[16]Vapnik, V. N. (2013). The nature of statistical learning theory. Springer science & business media.
[17]Kohavi, R. (1995). A study of cross-validation and bootstrap for accuracy estimation and model selection. In Proceedings of the 14th international joint conference on Artificial intelligence-Volume 2 (pp. 1137-1143). Morgan Kaufmann Publishers Inc. [18]Bishop, C. M. (2006). Pattern recognition and machine learning. springer.
[19]Liu, H., & Motoda, H. (Eds.). (2012). Feature selection for knowledge discovery and data mining (Vol. 454). Springer Science & Business Media.
[20]Kim, Y., & Kim, J. (2017). Deep learning in medical imaging. In Deep learning for medical image analysis (pp. 3-24). Academic Press.
[21]Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning (Vol. 1). MIT press Cambridge.
[22]Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. science, 313(5786), 504-507. [12] Lecun, Y., Bengio, Y., & Hinton, G.
(2015). Deep learning. nature, 521(7553), 436-444.

-
.