African Multidisciplinary
Journal of Sciences and Artificial Intelligence

ISSN : 1595-7969

Index: Harvard, Boston, Sydney University, Dimensions, Lens, ResearchGet Scilit, Semantic, Google Scholar, Base etc

https://doi.org/10.58578/AMJSAI.v2i2.6805

Implementing and Evaluating an IoC-Driven Early Warning System for Enhanced Cybersecurity Resilience

Adereti Rasak Raji, Adenomon M. O., Gilbert I. O., Aimufua Steven I. Bassey
Nasarawa State University Keffi, Nigeria
dr.stevenba@gmail.com; deretirasak@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Jun 10, 2025	Jul 5, 2025	Jul 17, 2025	Jul 22, 2025

Abstract

In the contemporary digital landscape, organizations are increasingly confronted by sophisticated cyber threats that render traditional reactive security measures inadequate, particularly in the face of advanced persistent threats (APTs) and rapidly evolving attack vectors. This paper proposes the design, implementation, and evaluation of an Indicator of Compromise (IoC)-driven Early Warning System (EWS) to proactively bolster cybersecurity resilience. Grounded in the principles of Cyber Threat Intelligence (CTI) and Design Science Research (DSR), the proposed framework termed the Intelligent Detection and Early Warning (IDEW) System integrates multiple threat intelligence feeds, employs advanced analytics for real-time threat detection, and delivers actionable insights to support timely incident response. The study explores the theoretical foundations of CTI and DSR, outlines key architectural considerations for the IDEW System, and presents a conceptual case study illustrating its application in identifying and mitigating emerging threats, including the 'Salt Typhoon' APT campaign. Additionally, the paper addresses challenges in operationalizing CTI, such as data integration, contextual relevance, and alert fatigue, and underscores the importance of human expertise, robust data governance, and iterative refinement for effective system deployment. This research contributes to the

AMJSAI Journal is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

evolving discourse on proactive cybersecurity strategies, offering a structured, intelligence-driven approach to building adaptive and resilient defense mechanisms in a dynamic threat environment.

Keywords: Cyber Threat Intelligence; Early Warning System; Indicators of Compromise; Proactive Cybersecurity; Design Science Research; APT Detection

Introduction

The pervasive nature of digital transformation has rendered organizations increasingly susceptible to cyber-attacks, which continue to escalate in frequency, sophistication, and impact [1]. The traditional paradigm of cybersecurity, predominantly focused on perimeter defense and reactive incident response, is proving inadequate in the face of dynamic and stealthy adversaries. Advanced Persistent Threats (APTs), zero-day exploits, and highly targeted campaigns necessitate a shift towards more proactive and intelligence-driven defense mechanisms. Cyber Threat Intelligence (CTI) has emerged as a critical discipline in this evolving landscape, providing organizations with the knowledge and understanding of actual or perceived threats to inform their security decision-making [2].

Early Warning Systems (EWS) are instrumental in mitigating the impact of various hazards, from natural disasters to financial crises. In the realm of cybersecurity, an EWS, particularly one driven by Indicators of Compromise (IoCs), holds immense promise for providing timely alerts about impending or ongoing cyber threats, thereby enabling organizations to preemptively defend against attacks or significantly reduce their dwell time [3]. IoCs are forensic artifacts—such as malicious IP addresses, domain names, file hashes, or unusual network traffic patterns—that serve as evidence of a potential security breach or compromise [4]. By continuously monitoring and analyzing these indicators, an IoC-driven EWS can transform an organization's cybersecurity posture from reactive to proactive, anticipatory, and dynamic [2].

This paper aims to present a comprehensive framework for an IoC-driven Early Warning System, built upon the rigorous principles of Design Science Research (DSR) and informed by the latest advancements in Cyber Threat Intelligence. The proposed Intelligent Detection and Early Warning (IDEW) System is designed to address the critical need for timely and actionable threat intelligence, enabling organizations to enhance their cybersecurity resilience

effectively. We will explore the theoretical foundations, architectural components, implementation considerations, and evaluation methodologies for such a system. Furthermore, a conceptual case study will illustrate the practical application of the IDEW System in identifying and responding to sophisticated cyber campaigns.

The remainder of this paper is structured as follows: Section II provides a detailed overview of the theoretical background, encompassing Cyber Threat Intelligence (CTI) and Design Science Research (DSR). Section III outlines the architectural design and key components of the Intelligent Detection and Early Warning (IDEW) System. Section IV discusses the implementation considerations and challenges associated with deploying such a system. Section V presents a conceptual case study demonstrating the IDEW System's application. Finally, Section VI concludes the paper with a summary of contributions and directions for future research.

Theoretical Background

To effectively design and implement an IoC-driven Early Warning System, it is imperative to establish a robust theoretical foundation. This section elaborates on two core disciplines that underpin the proposed IDEW System: Cyber Threat Intelligence (CTI) and Design Science Research (DSR).

A. Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) is the process of collecting, processing, analyzing, and disseminating information about potential or actual threats to an organization's assets. Its primary goal is to provide actionable insights that enable proactive defense and informed decision-making [2]. CTI moves beyond raw data by transforming it into refined, relevant, and timely knowledge about adversaries, their motivations, capabilities, and attack methodologies. This transformation is crucial for shifting cybersecurity from a reactive to a proactive stance [2].

The CTI Lifecycle: The production of CTI typically follows a structured lifecycle, often adapted from traditional intelligence cycles. While variations exist, a common model includes the following phases:

1.Planning and Direction: This initial phase defines the intelligence requirements based on the organization's assets, risk appetite, and strategic objectives. It answers the

question of "what intelligence is needed?" and guides the entire intelligence process [2]. 2. Collection: This phase involves gathering raw data from various sources, both internal (e.g., logs, network traffic) and external (e.g., open-source intelligence, commercial threat feeds, dark web forums). The quality and diversity of collected data directly impact the richness of the resulting intelligence [2]. 3. Processing and Exploitation: Raw data is often unstructured and voluminous. This phase involves transforming raw data into a usable format through techniques such as data parsing, normalization, and enrichment. This might include extracting Indicators of Compromise (IoCs) from threat reports or correlating seemingly disparate pieces of information [4]. 4. Analysis and Production: This is the core of CTI, where processed data is analyzed to identify patterns, trends, and actionable insights. Analysts use various techniques, including statistical analysis, machine learning, and human expertise, to understand adversary behaviors, predict future attacks, and develop defensive strategies. The output of this phase is finished intelligence products, such as threat reports or alerts [2]. 5. Dissemination and Integration: Produced intelligence must be delivered to the relevant stakeholders in a timely and understandable manner. This involves tailoring the intelligence to different audiences (e.g., executives, security analysts, incident responders) and integrating it into existing security tools and workflows (e.g., SIEMs, SOAR platforms) [2]. 6. Feedback: The final, yet crucial, phase involves gathering feedback from consumers of the intelligence. This feedback helps refine intelligence requirements, improve collection methods, and enhance the overall effectiveness of the CTI program [2].

Types of CTI: CTI can be categorized into different levels based on its audience, purpose, and level of detail [5]:

•Strategic CTI: This high-level intelligence focuses on the "who" and "why" of cyber threats. It provides insights into the motivations, capabilities, and intentions of threat actors (e.g., nation-states, cybercriminal groups, hacktivists). Strategic CTI is typically consumed by senior leadership and helps inform long-term security investments and risk management strategies. It is often presented in reports or white papers [5].

•Tactical CTI: This mid-level intelligence focuses on the "how" of cyber threats. It provides details on the Tactics, Techniques, and Procedures (TTPs) used by adversaries. Tactical CTI is valuable for security analysts and incident responders, helping them understand attack methodologies and configure defensive controls. Indicators of Compromise (IoCs) are a key

component of tactical intelligence, providing specific artifacts that can be used for detection [5].

•Operational CTI: This low-level, highly technical intelligence focuses on the immediate details of specific threats. It includes real-time IoCs, attack signatures, and contextual information about ongoing campaigns. Operational CTI is directly consumed by security operations centers (SOCs) and automated security tools to enable rapid detection and response to active threats [5].

B. Design Science Research (DSR)

Design Science Research (DSR) is a research paradigm focused on creating innovative artifacts to solve real-world problems [6]. Unlike traditional behavioral science research, which aims to explain phenomena, DSR aims to build and evaluate solutions. It is particularly well-suited for Information Systems research, where the development of new IT artifacts can directly address complex organizational challenges. The IDEW System, as a novel cybersecurity solution, is developed and evaluated following DSR principles.

Key Principles of DSR: Hevner et al. [6] propose seven guidelines for conducting and evaluating DSR:

1.Design as an Artifact: The research output must be a purposeful and innovative artifact. In our case, the IDEW System itself is the artifact.

2.Problem Relevance: The research must address a relevant and important business problem. The escalating cyber threat landscape and the need for proactive defense clearly establish the relevance of an IoC-driven EWS.

3.Design Evaluation: The utility, quality, and efficacy of the designed artifact must be rigorously demonstrated. This involves evaluating how well the IDEW System performs its intended functions.

4.Research Contributions: The research must provide clear and verifiable contributions in the areas of design artifact, design foundations, or design methodologies. The IDEW System aims to contribute a practical framework for enhanced cybersecurity resilience.

5.Research Rigor: The research must apply rigorous methods in both the design and evaluation of the artifact. This includes drawing upon established theories and employing appropriate analytical techniques.

6.Design as a Search Process: The design process involves a search for an effective solution, which may include iterating through multiple designs and evaluations. This iterative approach is central to the development of the IDEW System.

7.Communication of Research: The research must be effectively communicated to both technical and management audiences. This paper serves as a primary means of communicating the IDEW System's design and evaluation.

The DSR Process: The DSR methodology typically involves an iterative

process of building and evaluating artifacts. While specific models vary, a common DSR cycle includes:

•Problem Identification and Motivation: Clearly defining the research problem and justifying the value of a design-science approach.

•Objective of a Solution: Specifying the objectives for the new artifact, including its functionalities and desired performance.

•Design and Development: Creating the artifact, which involves conceptual design, detailed design, and implementation.

•Demonstration: Showing the artifact's utility and feasibility in a relevant environment.

•Evaluation: Assessing how well the artifact meets its objectives and solves the identified problem. This can involve various methods, from technical performance testing to case studies.

•Communication: Documenting the research process, the artifact, and its contributions to both academic and practical communities.

By adhering to DSR principles, the development of the IDEW System ensures that the solution is not only theoretically sound but also practically relevant and rigorously evaluated.

The Intelligent Detection and Early Warning (IDEW) System: Architectural Design

The Intelligent Detection and Early Warning (IDEW) System is designed as a multi-layered architecture that integrates various components to achieve comprehensive threat intelligence processing, real-time detection, and actionable alerting. The system leverages the principles of CTI to transform raw security data into actionable intelligence, and its development is guided

by the iterative nature of DSR. Figure 1 illustrates the high-level architecture of the IDEW System.

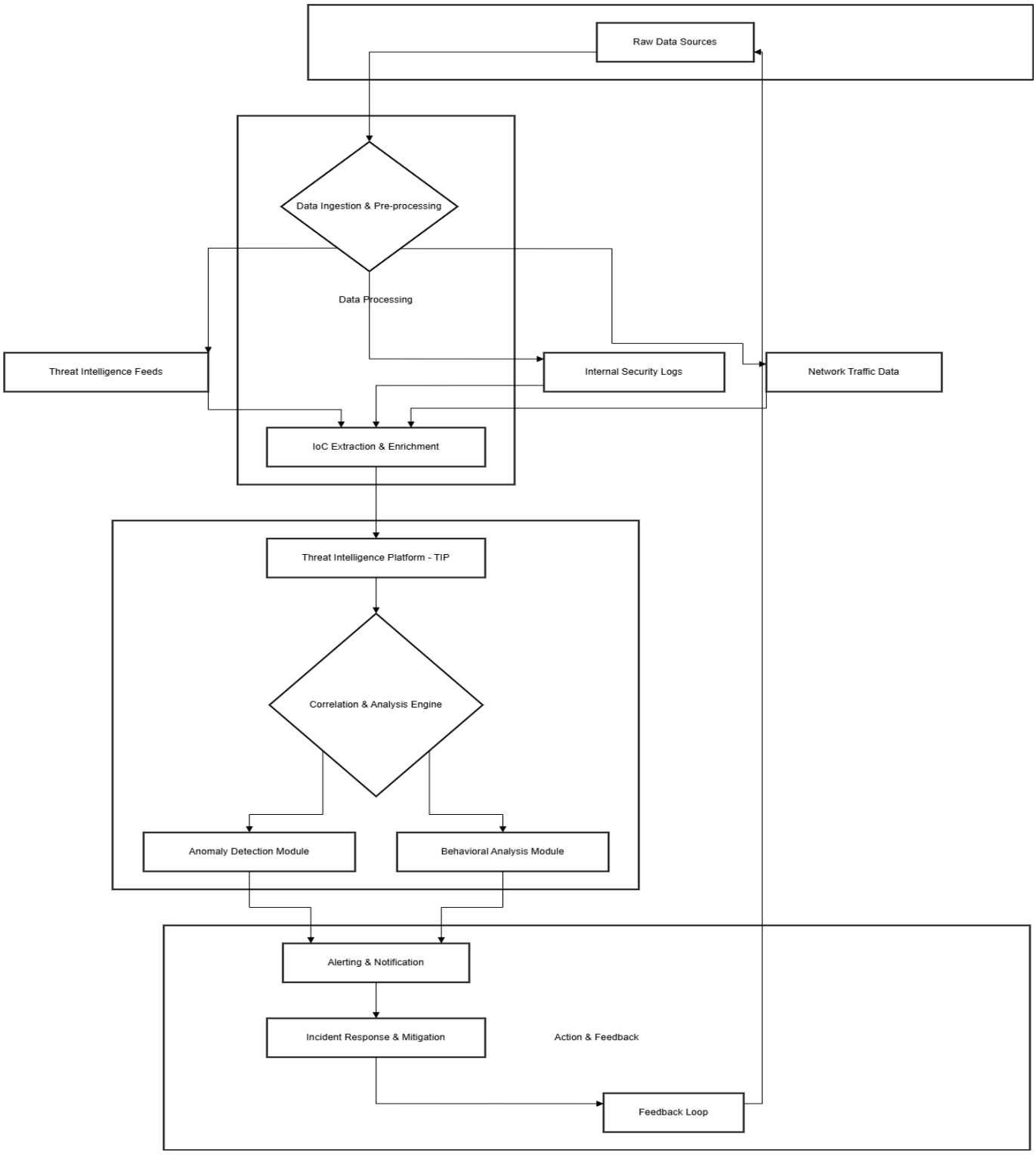


Figure 1: High-Level Architecture of the Intelligent Detection and Early Warning (IDEW) System

A. Data Ingestion and Pre-processing

The foundation of any effective EWS lies in its ability to collect and process vast amounts of diverse data. The IDEW System ingests data from multiple sources, ensuring a comprehensive view of the threat landscape. These sources include:

Threat Intelligence Feeds: These are external sources of CTI, providing information on known IoCs, TTPs of threat actors, and emerging threats. Examples include commercial threat intelligence platforms, open-source intelligence (OSINT) feeds, industry-specific information sharing and analysis centers (ISACs), and government advisories [7].

Internal Security Logs: Logs from various internal security devices and applications, such as firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint detection and response (EDR) solutions, web proxies, and authentication servers, provide crucial insights into internal network activity and potential anomalies [8].

Network Traffic Data: Deep packet inspection (DPI) and flow data (e.g., NetFlow, IPFIX) offer granular visibility into network communications, enabling the detection of suspicious connections, data exfiltration attempts, and command-and-control (C2) communications [9].

Upon ingestion, raw data undergoes a rigorous pre-processing phase, which includes data parsing, normalization, and deduplication. This ensures data consistency and prepares it for subsequent analysis. Data enrichment, such as geo-locating IP addresses or resolving domain names, is also performed to add context to the raw data [10].

B. IoC Extraction and Enrichment

Indicators of Compromise (IoCs) are the cornerstone of the IDEW System's early warning capabilities. This module is responsible for automatically extracting IoCs from ingested data and enriching them with additional contextual information. IoCs can manifest in various forms [4]:

•Atomic IoCs: These are single, unambiguous indicators, such as specific IP addresses, domain names, file hashes (MD5, SHA1, SHA256), and email addresses. While easy to detect, their utility can be short-lived as adversaries quickly change them [4].

Computed IoCs: These are derived from multiple atomic IoCs or behavioral patterns, such as a combination of suspicious network connections and unusual process executions. They are more resilient to evasion techniques but require more sophisticated analysis [4].

Behavioral IoCs: These describe patterns of malicious activity, such as specific TTPs used by threat actors. Behavioral IoCs are the most valuable as they are difficult for adversaries to change and can indicate the presence of sophisticated attacks [5].

Enrichment involves correlating extracted IoCs with known threat intelligence databases, vulnerability databases (e.g., CVE), and internal asset inventories. This process helps to determine the severity and relevance of each IoC within the organization's specific context [11].

C. Threat Intelligence Platform (TIP)

The Threat Intelligence Platform (TIP) serves as the central repository and management hub for all collected and processed threat intelligence. It aggregates IoCs, TTPs, and other contextual information from various sources, providing a unified view of the threat landscape. Key functionalities of the TIP include:

Data Aggregation and Storage: Securely storing large volumes of diverse threat intelligence data in a structured and searchable format.

Contextualization: Linking IoCs to specific threat actors, campaigns, and vulnerabilities, providing a richer understanding of the threat [12].

Prioritization: Ranking IoCs based on their severity, relevance to the organization, and potential impact, enabling security teams to focus on the most critical threats.

Sharing and Collaboration: Facilitating the secure sharing of threat intelligence within the organization and with trusted external partners, adhering to relevant information sharing protocols (e.g., STIX/TAXII) [13].

Lifecycle Management: Managing the lifecycle of IoCs, including their creation, validation, expiration, and archival, as IoCs can decay in their effectiveness over time [3].

D. Correlation and Analysis Engine

This is the analytical core of the IDEW System, responsible for identifying suspicious activities and potential threats by correlating IoCs with internal security data. The engine employs a combination of rule-based detection, anomaly detection, and behavioral analysis techniques.

Rule-Based Detection: This involves defining specific rules based on known IoCs and TTPs. For example, a rule might trigger an alert if an internal IP address attempts to communicate with a known malicious C2 server [14].

Anomaly Detection Module: This module uses machine learning algorithms to establish baselines of normal network and system behavior. Deviations from these baselines, even if they don't match known IoCs, can indicate anomalous or suspicious activity. This is particularly effective in detecting novel or zero-day attacks [15].

Behavioral Analysis Module: This module focuses on identifying malicious patterns of behavior rather than just individual IoCs. It analyzes sequences of events, user activities, and system interactions to detect sophisticated attacks that might evade traditional signature-based detection. For instance, a series of failed login attempts followed by successful access from an unusual location could indicate a brute-force attack [16].

E. Alerting and Notification

Upon detection of a potential threat, the IDEW System generates alerts and notifies relevant stakeholders. The alerting mechanism is designed to be timely, accurate, and contextualized, minimizing false positives and providing sufficient information for rapid response. Alerts can be delivered through various channels, including security information and event management (SIEM) systems, email, SMS, or integrated into incident response platforms [17].

F. Incident Response and Mitigation

While the IDEW System primarily focuses on early warning, it is tightly integrated with the organization's incident response (IR) processes. Upon receiving an alert, IR teams can leverage the contextual information provided by the IDEW System to quickly investigate, contain, eradicate, and recover from security incidents. The system can also trigger automated mitigation actions, such as blocking malicious IP addresses at the firewall or isolating compromised endpoints [18].

G. Feedback Loop

A crucial aspect of the IDEW System, aligned with DSR principles, is the continuous feedback loop. Information from incident response activities, new threat intelligence, and performance evaluations are fed back into the system to refine its detection capabilities, update threat models, and improve overall effectiveness. This iterative process ensures that the IDEW System remains adaptive and resilient in the face of evolving cyber threats [2, 6].

Implementation Considerations and Challenges

Implementing an IoC-driven Early Warning System like IDEW presents several technical, organizational, and operational challenges. Addressing these challenges effectively is crucial for the successful deployment and sustained efficacy of the system.

A. Data Quality and Volume

The effectiveness of an IoC-driven EWS is directly proportional to the quality and relevance of the data it ingests. Poor data quality, including inaccuracies, incompleteness, or outdated information, can lead to a high rate of false positives or, worse, missed detections [19]. The sheer volume of security data generated by modern enterprises also poses a significant challenge. Processing, storing, and analyzing petabytes of data in real-time requires robust infrastructure and scalable solutions. Organizations must invest in data governance strategies to ensure data integrity, consistency, and timeliness across all sources [20].

B. Integration with Existing Security Infrastructure

Most organizations already have a complex ecosystem of security tools and platforms. Integrating the IDEW System seamlessly with existing Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, firewalls, and endpoint security solutions can be a daunting task. Interoperability issues, lack of standardized APIs, and vendor lock-in can hinder effective data exchange and automated response capabilities [21]. A phased integration approach, starting with critical data sources and gradually expanding, can help mitigate these challenges.

C. Skill Gap and Human Expertise

While automated tools are essential, human expertise remains indispensable for effective CTI and EWS operations. Analyzing complex threat intelligence, interpreting anomalous behaviors, and fine-tuning detection rules require highly skilled security analysts. There is a significant global shortage of cybersecurity professionals with the necessary expertise in threat intelligence, data science, and incident response [22]. Organizations must invest in training and upskilling their existing workforce and consider recruiting specialized talent to manage and operate the IDEW System effectively.

D. IoC Lifecycle Management and Decay

Indicators of Compromise have a limited shelf life. Malicious IP addresses and domain names can be quickly taken down or changed by adversaries, rendering older IoCs ineffective [3].

This phenomenon, known as IoC decay, necessitates continuous updating and validation of threat intelligence feeds. The IDEW System must incorporate mechanisms for automated IoC validation, aging, and retirement to prevent the accumulation of stale or irrelevant indicators that can lead to alert fatigue and reduced detection accuracy [3].

E. False Positives and Alert Fatigue

One of the most significant operational challenges in any EWS is managing false positives. An excessive number of false alerts can lead to alert fatigue among security analysts, causing them to overlook genuine threats. The IDEW System must employ sophisticated correlation and analysis techniques, including machine learning and behavioral analytics, to minimize false positives. Continuous tuning of detection rules, anomaly thresholds, and behavioral models based on feedback from incident response teams is essential to maintain a high signal-to-noise ratio [23].

F. Privacy and Legal Considerations

Collecting, processing, and sharing threat intelligence, especially across organizational boundaries, raises significant privacy and legal concerns. Regulations such as GDPR, CCPA, and industry-specific compliance requirements (e.g., HIPAA, PCI DSS) dictate how personal and sensitive data can be handled. Organizations must ensure that their CTI and EWS operations comply with all applicable laws and regulations, implement robust data anonymization and pseudonymization techniques where necessary, and establish clear data sharing agreements with external partners [24].

G. Cost and Resource Allocation

Implementing and maintaining a comprehensive IoC-driven EWS requires substantial financial and human resources. This includes investments in hardware, software licenses, threat intelligence subscriptions, and skilled personnel. Organizations must conduct a thorough cost-benefit analysis and secure adequate funding to ensure the long-term viability and effectiveness of the IDEW System. Prioritizing critical assets and focusing on high-impact threats can help optimize resource allocation [25].

Addressing these challenges proactively during the planning and implementation phases is critical for maximizing the value and effectiveness of the IDEW System in enhancing an organization's cybersecurity resilience.

Conceptual Case Study: Detecting and Mitigating the 'Salt Typhoon' APT Campaign with IDEW

To illustrate the practical application and efficacy of the Intelligent Detection and Early Warning (IDEW) System, we present a conceptual case study focusing on the detection and mitigation of a sophisticated Advanced Persistent Threat (APT) campaign, hypothetically named 'Salt Typhoon.' This scenario will demonstrate how the various components of the IDEW System work in concert to provide proactive defense against a real-world threat.

A. Background: The 'Salt Typhoon' APT Campaign

The 'Salt Typhoon' APT campaign is characterized by its stealthy tactics, advanced evasion techniques, and persistent targeting of critical infrastructure sectors, particularly in government and defense. This campaign, as documented by cybersecurity agencies, often leverages supply chain compromises, sophisticated phishing attacks, and zero-day vulnerabilities to gain initial access [26]. Once inside a network, 'Salt Typhoon' actors employ living-off-the-land techniques, custom malware, and encrypted command-and-control (C2) channels to maintain persistence, escalate privileges, and exfiltrate sensitive data [27]. Their TTPs are constantly evolving, making traditional signature-based detection challenging.

B. IDEW System in Action: Detection Phases

1. Initial Compromise Detection (Data Ingestion & IoC Extraction)

The 'Salt Typhoon' campaign often begins with a highly targeted spear-phishing email containing a malicious attachment or a link to a compromised website. The IDEW System's Data Ingestion and Pre-processing module would continuously collect and analyze email gateway logs, web proxy logs, and endpoint security telemetry. If the phishing email contains a known malicious file hash or a URL associated with 'Salt Typhoon' (obtained from external Threat Intelligence Feeds), the IoC Extraction and Enrichment module would immediately identify these atomic IoCs. For instance, a newly observed SHA256 hash of a 'Salt Typhoon' dropper malware, shared by an ISAC, would be ingested and flagged [28].

2. Post-Exploitation Activity Detection (Correlation & Analysis Engine)

Even if the initial atomic IoCs are unknown or bypassed, the 'Salt Typhoon' actors' post-exploitation activities would trigger the IDEW System's advanced analytical capabilities. For example, after successful execution, the malware might attempt to establish a C2 connection to a specific domain. The Network Traffic Data ingestion, combined with the Correlation &

Analysis Engine, would detect this. If the domain is a newly registered domain (NRD) or exhibits unusual traffic patterns (e.g., beaconing at regular intervals, high volume of encrypted traffic to an unusual destination), the Anomaly Detection Module would flag it. Furthermore, the 'Salt Typhoon' actors are known to use specific PowerShell commands for reconnaissance and lateral movement. The Behavioral Analysis Module would identify these sequences of commands, even if individual commands are benign, as a deviation from normal user behavior, indicating malicious activity [29].

3. Privilege Escalation and Lateral Movement (Behavioral Analysis & TIP)

As 'Salt Typhoon' actors attempt to escalate privileges or move laterally within the network, their actions would be monitored by the IDEW System. For instance, attempts to dump credentials using tools like Mimikatz, or unusual access to sensitive systems from a compromised user account, would be detected by the Behavioral Analysis Module. The Threat Intelligence Platform (TIP) would play a crucial role here by providing context. If the observed TTPs (e.g., specific lateral movement techniques, use of particular tools) match known 'Salt Typhoon' behaviors stored in the TIP, the confidence level of the detection would significantly increase, triggering a higher-priority alert [30].

4. Data Exfiltration Detection (Anomaly Detection & Alerting)

The final stage of a 'Salt Typhoon' attack often involves data exfiltration. The IDEW System would detect this through various means. Large volumes of data being transferred to external, unapproved cloud storage services or unusual outbound traffic to suspicious IP addresses would be flagged by the Anomaly Detection Module. If these activities occur outside of normal business hours or from unusual user accounts, the anomaly score would increase. The Alerting & Notification module would then immediately dispatch high-severity alerts to the Security Operations Center (SOC) and incident response team, providing detailed context, including the compromised assets, observed IoCs, and suspected TTPs [31].

C. Mitigation and Feedback Loop

Upon receiving the high-severity alerts from the IDEW System, the incident response team would initiate their protocols. The detailed information provided by IDEW would enable rapid containment, such as isolating compromised hosts, blocking malicious C2 domains at the firewall, and revoking compromised credentials. The Incident Response & Mitigation module, integrated with the IDEW System, could also trigger automated responses for known

'Salt Typhoon' IoCs, such as deploying specific endpoint detection rules or updating network access control lists.

Crucially, the Feedback Loop mechanism would then come into play. Information gathered during the incident response—new IoCs discovered, variations in 'Salt Typhoon' TTPs, and the effectiveness of mitigation strategies—would be fed back into the IDEW System. This continuous learning process would update the Threat Intelligence Feeds, refine the Correlation & Analysis Engine's rules and models, and enhance the overall detection capabilities against future 'Salt Typhoon' attacks or similar APT campaigns. This iterative improvement, a core tenet of DSR, ensures the IDEW System remains agile and effective against evolving threats [2, 6].

This conceptual case study demonstrates how the IDEW System, by integrating diverse data sources, leveraging advanced analytics, and maintaining a continuous feedback loop, can provide a robust early warning capability against sophisticated cyber threats like the 'Salt Typhoon' APT campaign, significantly enhancing an organization's cybersecurity resilience.

Conclusion

In an era defined by escalating cyber threats and the increasing sophistication of malicious actors, the imperative for proactive and intelligence-driven cybersecurity defenses has never been more critical. This paper has presented a comprehensive framework for an Intelligent Detection and Early Warning (IDEW) System, an IoC-driven solution designed to significantly enhance organizational cybersecurity resilience. By meticulously integrating principles from Cyber Threat Intelligence (CTI) and adhering to the rigorous methodology of Design Science Research (DSR), the IDEW System offers a structured and adaptive approach to identifying, analyzing, and mitigating emerging cyber threats.

We have elucidated the multi-layered architecture of the IDEW System, detailing its core components: robust data ingestion and pre-processing, intelligent IoC extraction and enrichment, a centralized Threat Intelligence Platform (TIP), a sophisticated correlation and analysis engine (comprising anomaly and behavioral detection modules), and integrated alerting, incident response, and continuous feedback mechanisms. This holistic design ensures that raw security data is transformed into actionable intelligence, enabling timely detection and rapid response to potential compromises.

The discussion on implementation considerations and challenges highlighted the complexities inherent in deploying such a system, including issues related to data quality and volume, integration with existing infrastructure, the critical cybersecurity skill gap, the dynamic nature of IoC decay, the persistent challenge of false positives, and crucial privacy and legal considerations. Addressing these challenges proactively is paramount for the successful operationalization and sustained effectiveness of the IDEW System.

The conceptual case study involving the 'Salt Typhoon' APT campaign vividly demonstrated the IDEW System's potential to detect and respond to advanced threats across various stages of the attack lifecycle—from initial compromise to data exfiltration. The iterative feedback loop, a cornerstone of the IDEW's DSR foundation, underscores its capacity for continuous learning and adaptation, ensuring its relevance and efficacy against an ever-evolving threat landscape. The IDEW System, therefore, represents a significant step towards building more resilient and proactive cybersecurity postures for organizations in the face of persistent and sophisticated cyber adversaries.

Future Work

While the IDEW System framework provides a robust foundation, several avenues for future research and development warrant exploration:

Advanced Machine Learning Integration: Further research into integrating more advanced machine learning and deep learning models for predictive analytics, particularly for identifying novel attack patterns and predicting adversary movements, could significantly enhance the IDEW System's capabilities. This includes exploring techniques like graph neural networks for complex threat relationships and reinforcement learning for adaptive defense strategies.

Automated Remediation and Orchestration: Expanding the automated incident response capabilities to include more sophisticated remediation actions, orchestrated through advanced SOAR platforms, could further reduce response times and minimize human intervention in routine tasks.

Human-in-the-Loop Intelligence: Investigating optimal human-in-the-loop models for CTI analysis, where AI augments human analysts rather than replaces them, to leverage the strengths of both artificial and human intelligence in complex decision-making scenarios.

Standardization and Interoperability: Contributing to the development and adoption of open standards for threat intelligence sharing (beyond STIX/TAXII) to facilitate seamless interoperability between diverse security tools and platforms.

Economic Impact and ROI Analysis: Conducting empirical studies to quantify the economic benefits and return on investment (ROI) of implementing IoC-driven EWS like IDEW, providing a stronger business case for organizations.

Ethical AI in Cybersecurity: Exploring the ethical implications of using AI in cybersecurity, particularly concerning privacy, bias in detection algorithms, and the potential for misuse, and developing guidelines for responsible AI deployment.

Sector-Specific Adaptations: Developing tailored versions of the IDEW System for specific critical infrastructure sectors (e.g., healthcare, energy, finance), addressing their unique threat landscapes, regulatory requirements, and operational constraints.

By pursuing these research directions, the IDEW System can continue to evolve, offering increasingly sophisticated and effective solutions for enhancing cybersecurity resilience in a perpetually challenging digital world.

References

[1] Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

[2] Goel, N., Mansi, & Sethi, N. (2022). CYBER THREAT INTELLIGENCE: A SURVEY ON PROGRESSIVE TECHNIQUES AND CHALLENGES. International Journal of Advances in Science Engineering and Technology, 10(3), 65-70. https://iraj.in/journal/IJASEAT/paper_detail.php?paper_id=18902&name=Cyber_Threat_Intelligence:_A_Survey_on_Progressive_Techniques_and_Challenges

[3] Sree, G. N., & Modali, S. (2022). Understanding the behaviour of IOCs during their lifecycle. Blekinge Institute of Technology. https://www.diva-portal.org/smash/get/diva2:1721508/FULLTEXT02.pdf

[4] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28(1), 75-105. https://wise.vub.ac.be/sites/default/files/thesis_info/design_science.pdf

[5] MITRE. (n.d.). ATT&CK® Design and Philosophy. Retrieved from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[6] CISA. (2024, February 7). PRC-Sponsored Cyber Actors Known as Volt Typhoon Target U.S.

Critical Infrastructure. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[7] Fortinet. (n.d.). What are Indicators of Compromise (IoCs)?. Retrieved from https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise

[8] Splunk. (n.d.). Indicators of Compromise (IoCs): An Introductory Guide. Retrieved from https://www.splunk.com/en_us/blog/learn/ioc-indicators-of-compromise.html

[9] Cisco. (n.d.). What Are Indicators of Compromise (IOC)?. Retrieved from https://www.cisco.com/site/us/en/learn/topics/security/what-are-indicators-of-compromise-ioc.html

[10] SentinelOne. (n.d.). What are Indicators of Compromise (IoCs)? A Comprehensive Guide. Retrieved from https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-are-indicators-of-compromise-iocs-a-comprehensive-guide/

[11] CrowdStrike. (n.d.). Indicators of Compromise (IOC) Security Explained. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/indicators-of-compromise-ioc/

[12] Group-IB. (n.d.). Indicators of Compromise (IoCs): Detect & Prevent Cyber Attacks. Retrieved from https://www.group-ib.com/resources/knowledge-hub/iocs/

[13] IKARUS Security. (n.d.). Indicators of Compromise (IoC) and Indicators of Attack (IoA). Retrieved from https://www.ikarussecurity.com/en/security-news-en/ioc-and-ioa-definition-examples-benefits/

[14] Microsoft. (n.d.). What Are Indicators of Compromise (IOC)?. Retrieved from https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc

[15] Wiz. (n.d.). IOC Security: The Role Of Indicators Of Compromise In Cybersecurity. Retrieved from https://www.wiz.io/academy/ioc-security

[16] Cyble. (n.d.). What Is IOC In Cybersecurity? | Indicators Of Compromise. Retrieved from https://cyble.com/knowledge-hub/what-is-ioc-in-cybersecurity/

[17] Arctic Security. (2023, January 27). How do Early Warning Systems improve cyber and IT effectiveness?. Retrieved from https://www.arcticsecurity.com/resources/how-do-early-warning-systems-improve-cyber-and-it-effectiveness

[18] Number Analytics. (2025, May 25). Early Warning Systems: A Key to International Security. Retrieved from https://www.numberanalytics.com/blog/early-warning-systems-international-security

[19] UNDRR. (2023, December 2). Global Status of Multi-Hazard Early Warning Systems 2023. Retrieved from https://www.undrr.org/media/91954/download

[20] UNU-EHS. (2024, March 15). Assessment of early warning systems in four Indian Ocean island states. Retrieved from https://unu.edu/ehs/project/assessment-early-warning-systems-four-indian-ocean-island-states-ioc-ews

[21] UNISDR. (2005, February 16). Evaluation and strengthening of Early Warning Systems in the Indian Ocean. Retrieved from https://www.unisdr.org/2006/ppew/tsunami/pdf/flash-appeal-TEWS-project.pdf

[22] ResearchGate. (2024, August 30). (PDF) Early Warning Systems for Natural Disasters. Retrieved from https://www.researchgate.net/publication/383565185_Early_Warning_Systems_for_Natural_Disasters

[23] IEEE Xplore. (2024). Early-warning systems built on an AI-powered, IoT-driven multi-gas sensor platform. Retrieved from https://ieeexplore.ieee.org/document/10658655/

[24] ScienceDirect. (2024). A critical review of digital technology innovations for early warning systems. Retrieved from https://www.sciencedirect.com/science/article/pii/S2212420923006313

[25] SpringerLink. (2025). An expert-based assessment of early warning systems in the South Ethiopia Regional State. Retrieved from https://link.springer.com/article/10.1007/s43621-025-00943-1

[26] Congress.gov. (n.d.). CRS Product IF12798. Retrieved from https://www.congress.gov/crs-product/IF12798

[27] U.S. Department of Justice. (n.d.). Cybersecurity & Infrastructure Security Agency (CISA) Advisory: PRC-Sponsored Cyber Actors Known as Volt Typhoon Target U.S. Critical Infrastructure. Retrieved from https://www.justice.gov/opa/pr/cybersecurity-infrastructure-security-agency-cisa-advisory-prc-sponsored-cyber-actors-known

[28] MITRE. (n.d.). ATT&CK® Navigator. Retrieved from https://attack.mitre.org/navigator/

[29] Mandiant. (n.d.). APT41: A Dual Espionage and Cyber Crime Operation. Retrieved from https://www.mandiant.com/resources/apt41-dual-espionage-cyber-crime-operation

[30] FireEye. (n.d.). APT28: A Look Back at a Decade of Russian Cyber Espionage. Retrieved from https://www.fireeye.com/blog/threat-research/2020/03/apt28-decade-of-russian-cyber-espionage.html

[31] Palo Alto Networks. (n.d.). Unit 42: Threat Intelligence. Retrieved from.