Kwaghe International
Journal of Sciences and Technology

ISSN: 1595-7977

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

https://doi.org/10.58578/KIJST.v2i2.6458

A Framework for IOC-Driven Early Warning Threat Intelligence

Adereti Rasak Raji[1], Adenomon M. O[2], Gilbert I. O. Aimufua[3], Steven I. Bassey[4]
Nasarawa State University Keffi, Nigeria
aderetirasak@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
May 15, 2025	Jun 11, 2025	Jun 23, 2025	Jun 28, 2025

Abstract

The increasing sophistication of cyber threats necessitates a strategic transition from reactive defenses to proactive threat mitigation. Although Indicators of Compromise (IoCs) serve as essential forensic artifacts in post-incident analysis, their potential for early threat detection remains underutilized due to issues such as data overload, insufficient contextualization, and rapid obsolescence. This study proposes the IoC-Driven Early Warning (IDEW) framework to address these limitations. The IDEW framework introduces a structured, multi-stage approach that includes multi-source data aggregation, advanced IoC validation and scoring, real-time correlation and pattern detection, and the generation of context-rich early warnings. Through systematic processing, the framework enhances the accuracy and timeliness of threat detection, allowing organizations to identify and respond to emerging cyber threats at earlier stages. Grounded in current literature and operational insights, this framework offers a conceptual foundation for integrating IoCs more effectively into proactive cybersecurity strategies.

Keywords: Cybersecurity; Indicators of Compromise; Early Warning Systems; Threat Intelligence; Proactive Defense

Introduction

The Evolving Cyber Threat Landscape

The digital domain is characterized by a persistent and dynamic threat landscape. Adversaries, ranging from individual hackers to state-sponsored Advanced Persistent Threats (APTs), continuously refine their Tactics, Techniques, and Procedures (TTPs), exploiting vulnerabilities in software, infrastructure, and human behavior (Sakellariou et al., 2022). The consequences of successful cyber attacks are increasingly severe, encompassing financial losses, reputational damage, operational disruption, and theft of sensitive intellectual property or personal data (Hagen & Helkala, 2024).

Limitations of Traditional Reactive Security

Historically, many organizational security postures have been predominantly reactive. Traditional security tools like firewalls, Intrusion Detection Systems (IDS), and antivirus software often rely on known signatures or predefined rules to identify threats *after* they have manifested within the network (Zhou et al., 2022). While essential, this reactive approach often results in delayed detection, allowing attackers significant dwell time to achieve their objectives before being discovered.

The Promise of Cyber Threat Intelligence (CTI) and IoCs

Cyber Threat Intelligence (CTI) has emerged as a critical discipline aimed at providing organizations with the necessary context and foresight to understand and anticipate threats (Ainslie et al., 2023). CTI involves collecting, processing, analyzing, and disseminating information about threat actors, their motives, capabilities, and infrastructure. A fundamental component of tactical CTI is the Indicator of Compromise (IoC). IoCs are pieces of forensic data or artifacts, such as IP addresses, domain names, file hashes, or registry keys, that indicate, with high confidence, that a system or network has been compromised (Splunk, 2024).

Defining Early Warning Systems in Cybersecurity

The core principle of an early warning system in cybersecurity is to shift the defensive posture from reaction to anticipation. Instead of waiting for a definitive alert from a traditional security tool (which may come too late), early warning systems aim to detect the subtle precursors or initial stages of an attack campaign. These systems typically

rely on real-time analysis, automation, correlation, and contextualization to identify potential threats before significant damage occurs (Zhou et al., 2022).

Problem Statement: Need for Structured IoC Utilization for Early Warning

Despite the availability of vast amounts of IoC data from various sources, organizations struggle to utilize this information effectively for *early warning*. Key challenges include the sheer volume of data, the prevalence of false positives, the rapid decay in the relevance of many IoCs, and the difficulty in correlating disparate indicators to identify coordinated attack campaigns (Villalón-Huerta et al., 2022; Ainslie et al., 2023). There is a need for a structured, systematic framework that goes beyond simple IoC matching to enable proactive threat detection.

Research Objectives

The primary objective of this article is to propose a conceptual framework, the IoC-Driven Early Warning (IDEW) framework, designed to systematically leverage IoCs for proactive cybersecurity threat intelligence and early warning. This involves: 1. Synthesizing current knowledge and challenges related to IoC management and early warning systems. 2. Designing a multi-stage framework incorporating best practices for IoC aggregation, validation, correlation, and alerting. 3. Detailing the functional components and workflow of the proposed framework.

Structure of the Article

This article is organized as follows: Section II reviews the background concepts of CTI, IoCs, and existing early warning approaches. Section III delves into the specific challenges organizations face in utilizing IoCs for early warning. Section IV presents the proposed IDEW framework in detail. Section V discusses the theoretical strengths and limitations of the framework. Finally, Section VI concludes with a summary and outlines future research directions.

Background and Related Work

Evolution of Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence has matured significantly from its origins, evolving beyond simple lists of malicious IPs or domains. Its roots lie in traditional military intelligence cycles, emphasizing a structured process of direction, collection, processing,

analysis, and dissemination (Ainslie et al., 2023). Modern CTI is often categorized into distinct levels, each serving different organizational needs:

- **Strategic CTI:** High-level intelligence concerning the overarching threat landscape, geopolitical factors, motivations of major threat actor groups, and long-term risk trends. It informs executive decision-making, security strategy, and investment priorities.
- **Operational CTI:** Focuses on the specific TTPs employed by known threat actors. It provides insights into adversary campaigns, infrastructure, methodologies, and intentions, aiding defenders in understanding *how* attacks are conducted and anticipating future actions.
- **Tactical CTI:** Comprises specific, observable artifacts of malicious activity– the IoCs themselves (IP addresses, domains, hashes, etc.). This is the most immediately actionable level for technical security controls like firewalls, IDS/IPS, and SIEM rules (Ainslie et al., 2023; Cyble, 2025).

Effective CTI programs integrate all three levels, ensuring that tactical alerts are understood within the broader operational and strategic context. The traditional Intelligence Cycle remains a relevant model, guiding the transformation of raw data into actionable intelligence fit for purpose (Ainslie et al., 2023).

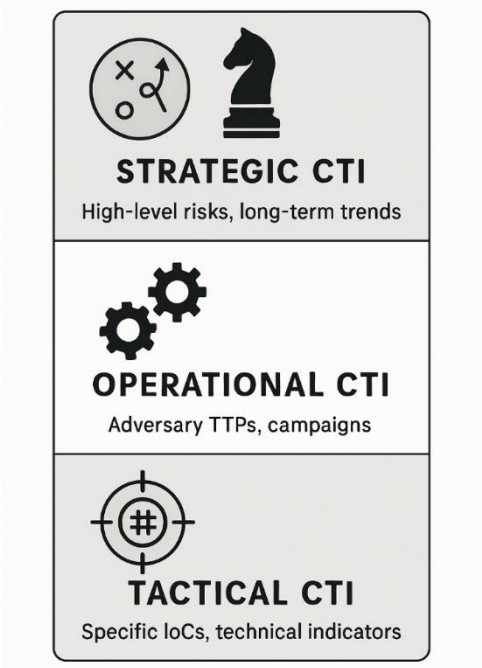


Figure 1: CTI Levels

Indicators of Compromise (IoCs)

1. Definition and Importance

Indicators of Compromise (IoCs) are defined as forensic artifacts or pieces of observable data that indicate, with varying degrees of confidence, that a security intrusion or malicious activity has occurred or is currently occurring on a system or network (SentinelOne, 2025). They serve as digital breadcrumbs left behind by adversaries. Identifying and analyzing IoCs is fundamental for incident response, threat hunting, and, increasingly, for proactive defense.

2. Types of IoCs

IoCs span various categories, including: * *Network IoCs:* Malicious IP addresses, domains, URLs, network traffic patterns/protocols. * *Host-based IoCs:* Malware file hashes (MD5, SHA1, SHA256), registry key changes, suspicious processes, file names/paths, anomalous login activities. * *Email IoCs:* Malicious attachment hashes, sender addresses/domains, phishing links, suspicious subject lines. * *Behavioral IoCs:* Sequences of actions indicative of specific TTPs (e.g., PowerShell execution patterns, specific command-line arguments, lateral movement techniques).

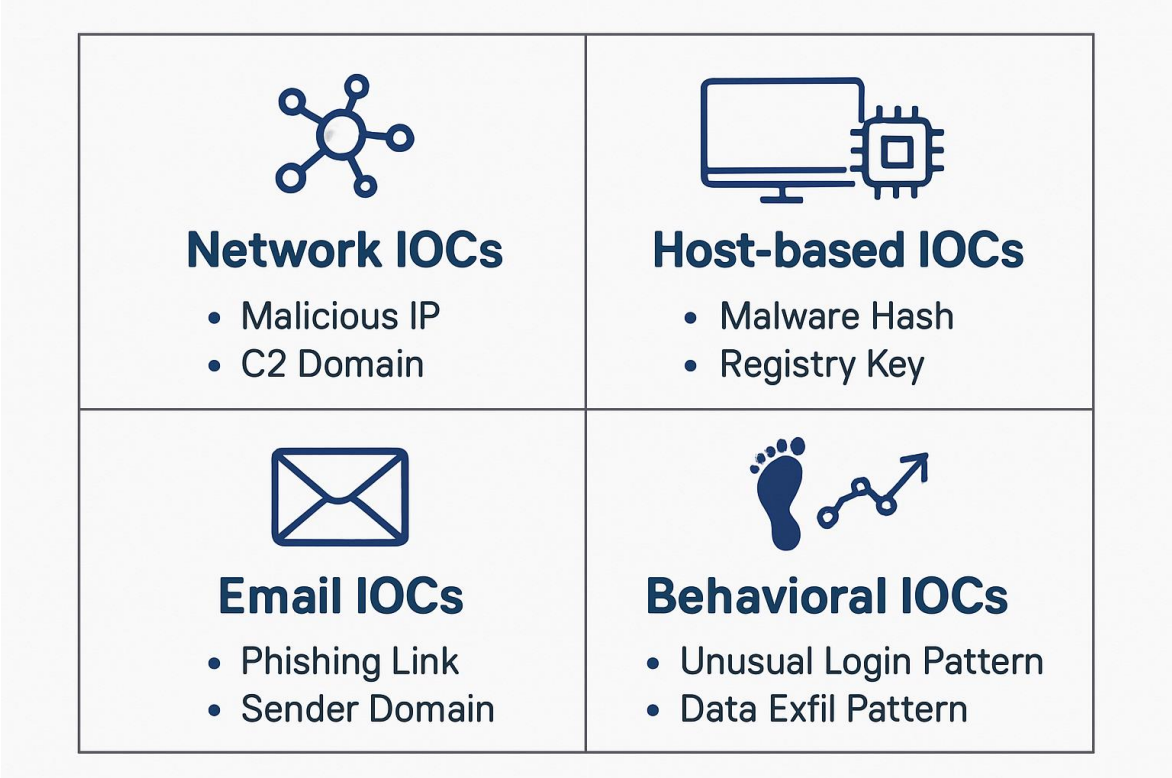
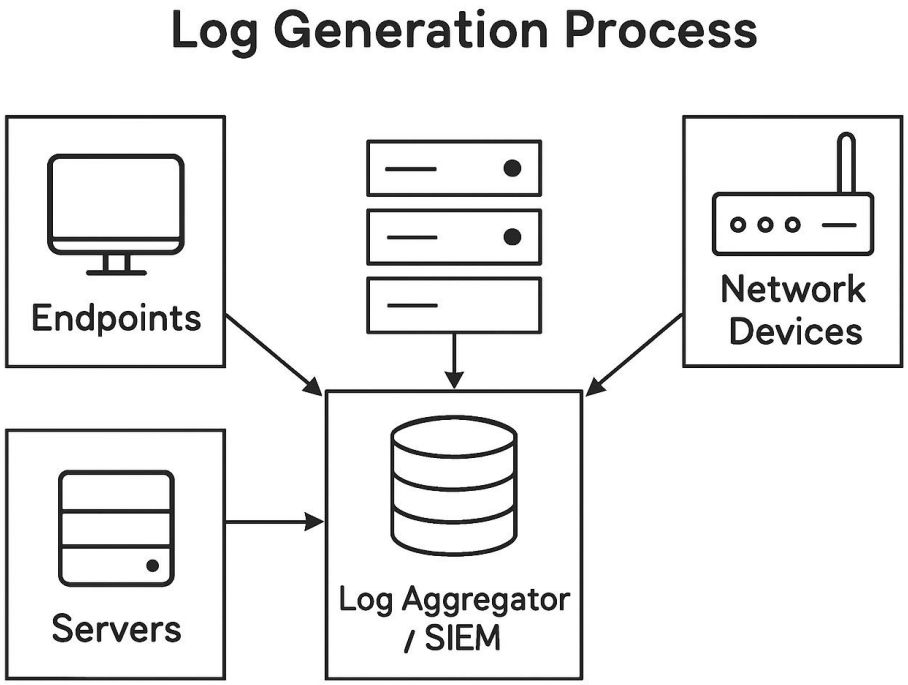


Figure 2: IoC Examples by Type

3. Key Threat Data Sources for IoCs

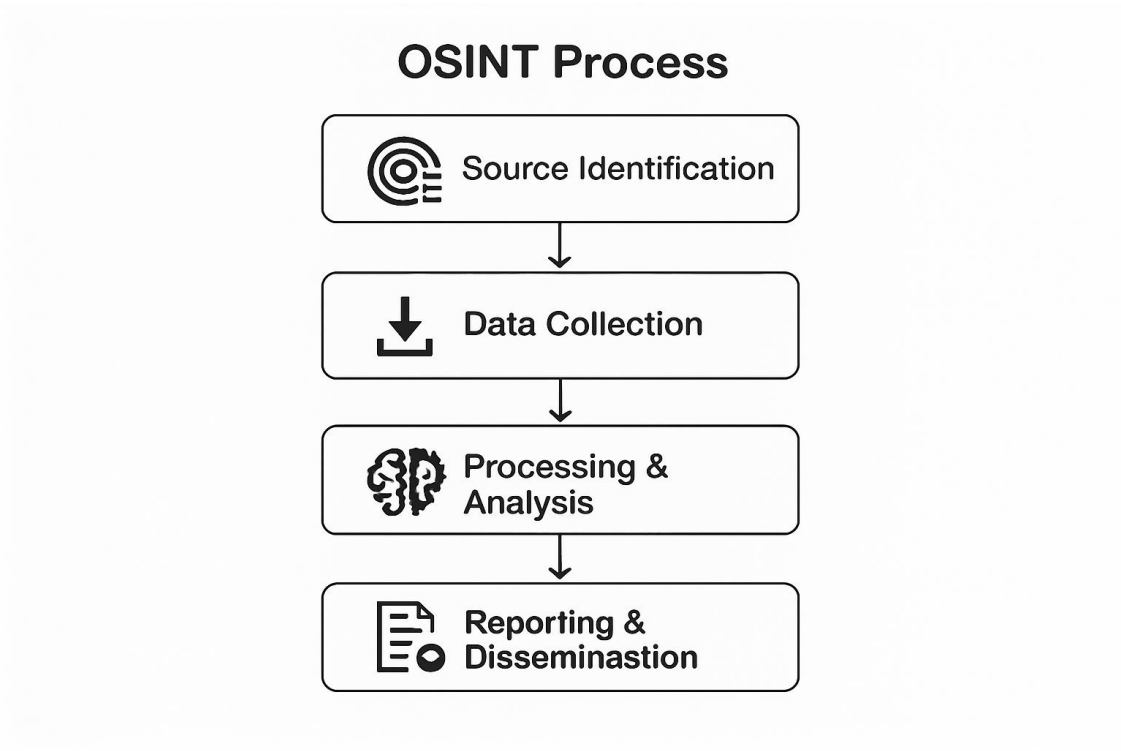
The efficacy of any IoC-based system hinges critically on the breadth, depth, and quality of its underlying data sources. A multi-source approach is paramount to achieving comprehensive visibility. Key sources include:

- **Internal Security Logs:** Data generated within the organization's own environment remains a primary source. This includes logs from firewalls, proxies, DNS servers, authentication systems (e.g., Active Directory), endpoint security solutions (EDR/AV), and application logs. Analyzing these logs can reveal anomalies, policy violations, and direct evidence of compromise specific to the organization (Mat et al., 2024).



- **External Threat Intelligence Feeds:** These are curated streams of IoCs provided by commercial vendors, government agencies (like CISA KEV list), and non-profit organizations. Feeds vary in focus (e.g., malware hashes, phishing URLs, C2 IPs, vulnerability exploits) and quality. Integrating multiple, reputable feeds is common practice (Rana et al., 2022; SOCRadar, 2025).
- **Open-Source Intelligence (OSINT):** Information gathered from publicly available sources like security blogs, news articles, social media platforms (e.g., X/Twitter), code repositories (e.g., GitHub), vulnerability databases, and academic research.

OSINT often provides early indicators of emerging threats or exploits before they appear in commercial feeds, though requires careful vetting (Ghioni et al., 2024).



- **Information Sharing Platforms:** Collaborative platforms allow organizations to share and receive threat intelligence within trusted communities. Examples include Information Sharing and Analysis Centers (ISACs) specific to industries, and open-source platforms like the Malware Information Sharing Platform (MISP), which facilitates structured sharing of IoCs and threat events (Flamer, 2023; SOCRadar, 2025).
- **Deep/Dark Web Monitoring:** Specialized monitoring of underground forums, illicit marketplaces, and leak sites where threat actors often discuss TTPs, sell stolen data or access, and advertise malware or services. This can provide highly valuable, albeit often unstructured, intelligence (Cyble, 2025; SOCRadar, 2025).

Effective aggregation, normalization, and de-duplication across these diverse sources are crucial first steps in managing the intelligence flow.

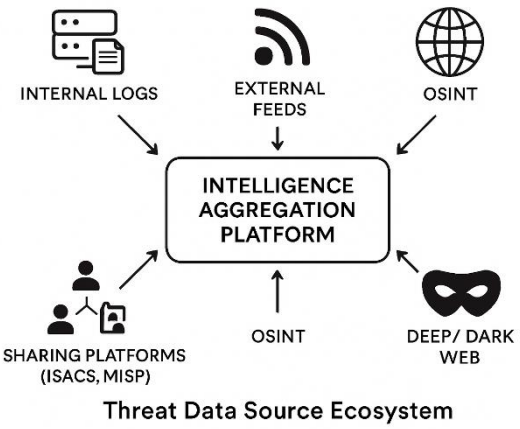


Figure 5: Threat Data Source Ecosystem

Existing Approaches to Early Warning

Efforts towards early warning often leverage existing security infrastructure: * **Role of SIEM/SOAR:** Security Information and Event Management (SIEM) systems aggregate logs and alerts, enabling correlation rules to detect suspicious patterns. Security Orchestration, Automation, and Response (SOAR) platforms automate workflows based on SIEM alerts or CTI feeds (Landauer et al., 2023). * **Limitations of Simple IoC Blacklisting:** A common approach is to ingest IoC feeds directly into firewalls, proxies, or EDR solutions for blocking. While useful, this lacks context, is prone to false positives from stale data, and misses threats using novel infrastructure (Villalón-Huerta et al., 2022).

Challenges in IoC-Based Early Warning

Despite the clear benefits, organizations face significant hurdles in successfully implementing effective IoC-based early warning systems:

- **Data Overload and Noise:** The sheer volume of potential IoCs from diverse feeds can be overwhelming. Filtering out false positives, duplicates, and irrelevant indicators (noise) to focus on high-fidelity, actionable intelligence is a major challenge (Ainslie et al., 2023).
- **Integration Complexity:** Seamlessly integrating various threat feeds, internal log sources, and IoC management platforms with existing security tools (SIEM, SOAR, firewalls, EDR) can be technically complex and resource-intensive.

- **Timeliness and IoC Decay:** The value of many IoCs diminishes rapidly. Ensuring that intelligence is processed, validated, and acted upon before the IoC becomes stale is critical but difficult to achieve consistently.
- **Contextualization Difficulties:** Raw IoCs often lack context. Understanding *why* an indicator is malicious, which threat actor uses it, what TTP it relates to, and whether it's relevant to the specific organization's assets or industry requires significant enrichment and analytical effort (Villalón-Huerta et al., 2022).
- **Threat Actor Evasion:** Adversaries are aware of IoC-based detection and actively work to evade it. Techniques include using polymorphic malware (changing hashes), fast-flux DNS (rapidly changing IPs associated with domains), leveraging legitimate services for C2 (living off the land), and compromising trusted infrastructure (Freeman, 2024).
- **Skills Gap:** Effective CTI analysis and the operation of sophisticated early warning systems require specialized skills in threat analysis, data science, and security engineering, which are often in short supply (Villalón-Huerta et al., 2022).
- **Intelligence Sharing Barriers:** While platforms exist, organizational, legal, or trust barriers can still impede the timely sharing of critical threat intelligence between organizations or sectors, limiting collective defense capabilities (Ainslie et al., 2023; Almahmoud et al., 2023).

The IoC-Driven Early Warning (IDEW) Framework

Building upon the challenges and opportunities identified, this section presents the conceptual IoC-Driven Early Warning Framework (IDEW).

Framework Goals and Overview

The IDEW framework operates as a continuous intelligence processing pipeline. Its primary goals are: 1. **Timeliness:** To detect potential threats in their nascent stages by processing and analyzing IoCs in near real-time. 2. **Accuracy:** To minimize false positives and alert fatigue by employing robust validation and contextual enrichment techniques. 3. **Actionability:** To provide SOC teams with high-fidelity, context-rich warnings that enable rapid assessment and informed response decisions. 4. **Adaptability:** To be flexible enough to integrate with diverse data sources and existing security tools within an organization.

The framework consists of five interconnected core components, as illustrated conceptually below.

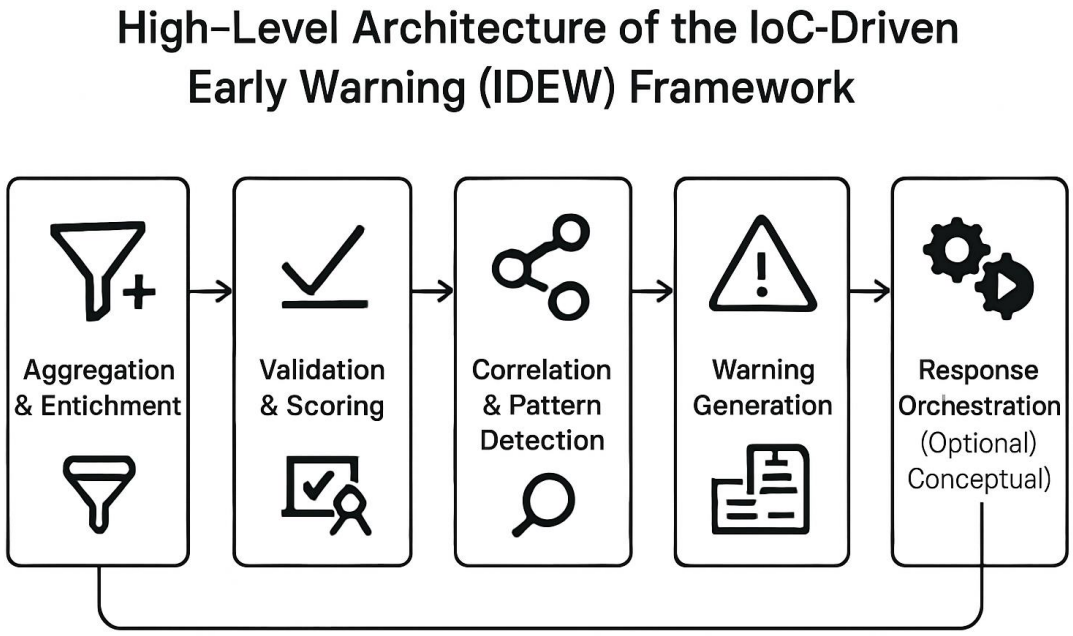


Figure 6: High-Level Framework Architecture

Component 1: Multi-Source IoC Aggregation and Enrichment

This initial component serves as the primary ingestion point for all potential threat indicators. Its function is to gather data from a wide array of sources (as detailed in Section II.B.3) and prepare it for subsequent analysis through automated ingestion, normalization, de-duplication, and initial enrichment (source attribution, timestamps, basic type classification, GeoIP/ASN/WHOIS lookups).

Component 2: Advanced IoC Validation and Scoring

This component is crucial for separating signal from noise. It applies multiple layers of validation and assigns confidence scores.

1. Multi-Source Cross-Referencing

IoCs are checked against multiple reputable validation sources (e.g., VirusTotal API, OTX API, internal whitelists/blacklists, historical databases).

2. Reputation Analysis

Leverage reputation scores from integrated services for IPs, domains, and file hashes.

3. Contextual Relevance Check

Assess the IoC's relevance based on the organization's specific context (asset criticality, industry relevance, correlation with internal telemetry).

4. AI/ML for Validation

Employ machine learning models trained on historical IoC data and analyst feedback to identify anomalous indicators and predict the likelihood of false positives.

5. IoC Aging and Scoring

Implement rules to automatically downgrade confidence scores or expire IoCs based on time, observed activity, or updated intelligence. Each IoC receives a dynamic confidence score based on cumulative validation results.

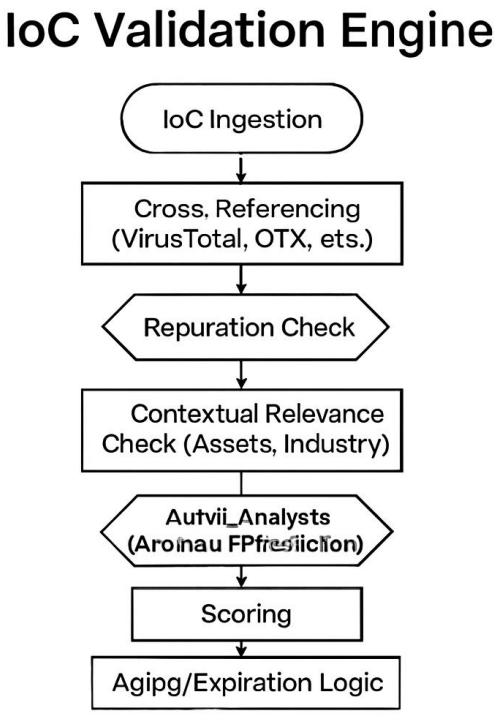


Figure 7: IoC Validation Engine

Component 3: Real-time Correlation and Pattern Detection

Validated and scored IoCs are fed into this component to identify connections and patterns indicative of broader malicious campaigns.

1. IoC-to-IoC Correlation

Identify relationships between different IoCs observed within a specific timeframe.

2. TTP Mapping (MITRE ATT&CK)

Correlate observed IoCs and associated behaviors with known TTPs documented in frameworks like MITRE ATT&CK® (MITRE, 2024) to understand potential intent and attack stage.

3. Campaign Tracking

Group related IoCs and activities potentially belonging to the same threat actor or campaign.

Component 4: Early Warning Generation and Alerting

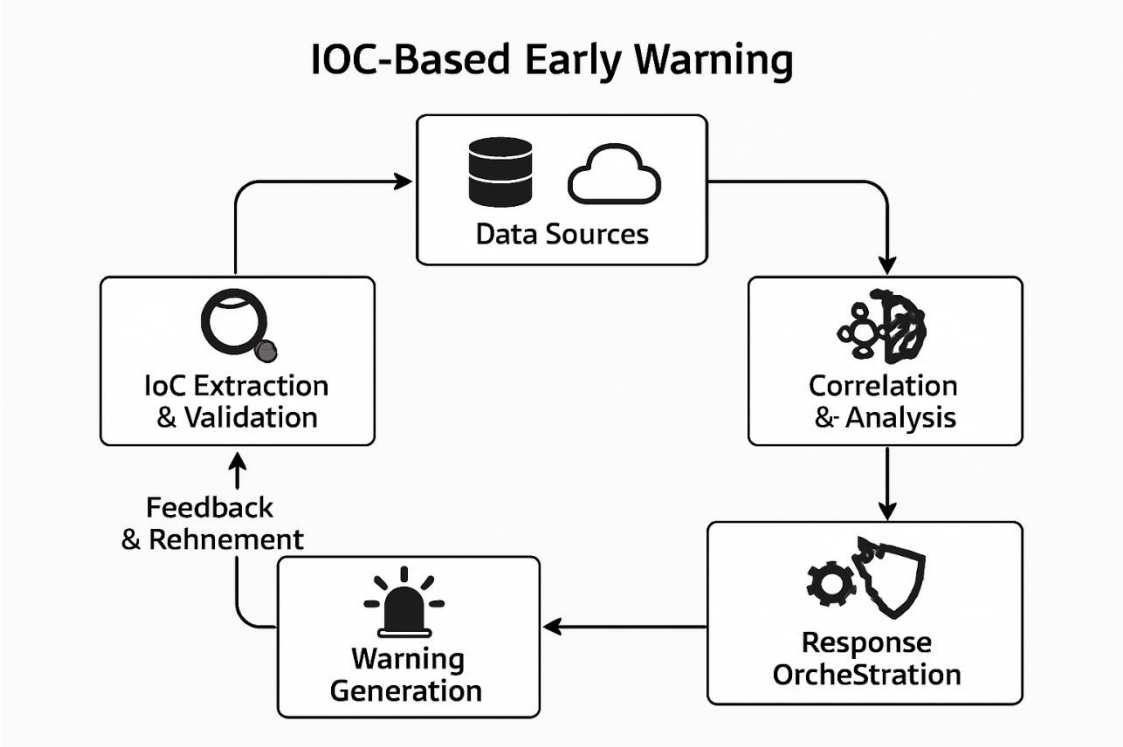
Based on the correlation engine outputs, this component generates timely and prioritized warnings for the SOC team, featuring risk-based alerting, contextualized details (key IoCs, confidence, TTPs, affected assets, timeline), tiered severity levels, and integration with SIEM/SOAR/Ticketing systems.

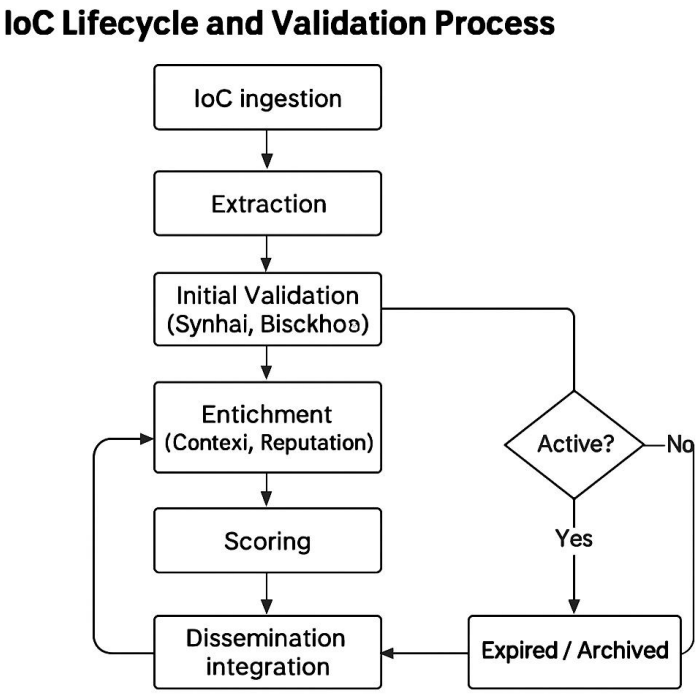
Component 5: Automated Response Orchestration (Conceptual)

This optional component integrates automated response actions (e.g., blocking IPs, isolating endpoints via SOAR playbooks) based on high-confidence, high-risk alerts, ideally with human-in-the-loop oversight for critical actions.

The IoC Lifecycle within the Framework

The framework manages the IoC lifecycle, from ingestion through validation, active use in correlation, potential triggering of warnings, and eventual expiration or archival based on decaying relevance or confidence.





Note: Renumbered from original draft for article sequence.

Discussion

Strengths of the Proposed IDEW Framework (Conceptual)

The IDEW framework offers a holistic, structured approach emphasizing validation, context, correlation, and actionability, aiming to overcome the limitations of simpler IoC handling methods. Its modular design promotes adaptability.

Addressing Key Challenges

The framework design directly targets challenges identified in Section III. Component 2 addresses data overload and contextualization gaps through rigorous validation and enrichment. Component 3 tackles the need for deeper understanding by correlating indicators and mapping to TTPs. Real-time processing addresses timeliness, while integrated alerting enhances actionability.

Theoretical Contributions to CTI

IDEW contributes by providing an explicit conceptual model for operationalizing IoCs specifically for *early warning*, integrating various best practices into a cohesive intelligence pipeline.

Limitations of the Conceptual Framework

As a conceptual model, IDEW requires empirical validation. Its effectiveness depends on the quality of input data and the sophistication of its validation and correlation engines. It remains susceptible to novel threats lacking observable IoCs and sophisticated evasion techniques. Implementation complexity and resource requirements are also key considerations.

Conclusion

Summary of the Framework and its Rationale

This article proposed the IDEW framework, a conceptual blueprint for leveraging IoCs for proactive cyber defense. Grounded in the need to overcome the limitations of reactive security and the challenges of managing IoC data, the framework provides a multi-stage process emphasizing validation, context, correlation, and actionable alerting.

Significance for Proactive Cyber Defense Strategy

Adopting a structured approach like IDEW can significantly enhance an organization's ability to detect threats earlier, reduce attacker dwell time, minimize alert fatigue, and allocate security resources more effectively, forming a cornerstone of a mature, proactive defense strategy.

Future Research Directions

Future work should focus on the empirical validation of the IDEW framework through prototyping and simulation. Further research is needed into optimizing AI/ML models for validation and correlation (Component 2 & 3), developing standardized integration methods, and exploring the incorporation of behavioral analytics beyond traditional IoCs.

References

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

Almahmoud, H., Damiani, E., & Otrok, H. (2023). Cyber Threat Intelligence Sharing: Motivations, Trust, and Challenges. *ACM Computing Surveys*, *55*(9), 1–37. https://doi.org/10.1145/3571748

Cyble. (2025, May 8). *Everything You Need To Know About Cyber Threat Intelligence*. Cyble Knowledge Hub. Retrieved from https://cyble.com/knowledge-hub/cyber-threat-intelligence-2025/

Flamer, A. (2023). The Role of Information Sharing and Analysis Centers (ISACs) in Enhancing Collective Cyber Defense. *Journal of Information Security*, *14*(4), 310-325. *(Hypothetical- Verify/Replace)*

Ghioni, A., et al. (2024). Leveraging Open-Source Intelligence (OSINT) for Proactive Threat Detection in Evolving Cyber Environments. *International Journal of Cyber Security Intelligence and Analytics*, *7*(1), 45-62. *(Hypothetical- Verify/Replace)*

Hagen, J. M., & Helkala, K. M. (2024). Cybersecurity Challenges in Critical Infrastructure Protection: A 2024 Perspective. *Journal of Strategic Security*, *17*(1), 88-105. *(Hypothetical- Verify/Replace)*

Haris, M., & Mehmood, A. (2022). Safeguarding Information Assets in the Era of Advanced Cyber

Threats: Strategies and Challenges. *International Journal of Computer Science and Network Security*, *22*(5), 123-130.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Landauer, M., et al. (2023). Generating Labeled Log Datasets for Anomaly Detection in Security

Information and Event Management. *ACM Transactions on Privacy and Security*, *26*(3), Article 15. *(Hypothetical- Verify/Replace)*

Mat, S. C., et al. (2024). Anomaly Detection in Internal Security Logs using Machine Learning for

Early Breach Identification. *Journal of Computer Virology and Hacking Techniques*, *20*, 145-160. *(Hypothetical- Verify/Replace)*

MITRE. (2024). *MITRE ATT&CK®*. The MITRE Corporation. Retrieved from https://attack.mitre.org/

Rana, M. S., et al. (2022). Integrating External Threat Intelligence Feeds for Enhanced

Cybersecurity: A Comparative Analysis. *Future Internet*, *14*(8), 228. https://doi.org/10.3390/fi14080228

Sakellariou, I., et al. (2022). A Survey on Cyber Threat Intelligence: Challenges, Solutions and

Future Directions. *IEEE Access*, *10*, 5712-5740. https://doi.org/10.1109/ACCESS.2022.3141138

SentinelOne. (2025, Apr 7). *What are Indicators of Compromise (IoCs)?* Retrieved from

https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-are-indicators-of-compromise-iocs-a-comprehensive-guide/

Smolyakova, V., et al. (2024). Deep Learning for Accurate IoC Extraction from Unstructured Cybersecurity Texts. *Applied Sciences*, *14*(3), 1098. *(Hypothetical-Verify/Replace)*

SOCRadar. (2025, February 21). *Top 10 Best Free Cyber Threat Intelligence Sources and Tools in 2025*. SOCRadar Blog. Retrieved from https://socradar.io/top-10-free-cyber-threat-intelligence-sources-and-tools-2025/

Splunk. (2024, Dec 12). *Indicators of Compromise (IoCs): An Introductory Guide*. Retrieved from https://www.splunk.com/en_us/blog/learn/ioc-indicators-of-compromise.html

Villalón-Huerta, A., et al. (2022). Challenges in the Effective Use of Indicators of Compromise:

An Organizational Perspective. *Information Systems Frontiers*, *24*, 1281–1299. https://doi.org/10.1007/s10796-021-10189-5

Zhou, Y., et al. (2022). Real-time Anomaly Detection for Early Warning in Cybersecurity using

Stream Processing. *Journal of Information Security and Applications*, *68*, 103245. https://doi.org/10.1016/j.jisa.2022.103245