Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20250401039
Volume 4, Issue1 (January-April 2025), PP: 254-258.
www.indjcst.com
ISSN No: 2583-5300

Threat Intelligence System Using Suricata by Dynamic Method

Rahul S[1], Marimuthu R[2]
[1]*M.SC CFIS, Dr. M.G.R Educational and Research Institute, Chennai, Tamilnadu, India.*
[2]*Assistant Professor, Faculty Center for Cyber Forensic and Information Security, University of Madras, Chennai, Tamilnadu, India.*

To Cite this Article: *Rahul S[1], Marimuthu R[2], "Threat Intelligence System Using Suricata by Dynamic Method", Indian Journal of Computer Science and Technology, Volume 04, Issue 01 (January-April 2025), PP: 254-258.*

Abstract: *With the adding complication of cyber risks, integrating Intrusion Discovery Systems (IDS) with real- time trouble intelligence has come vital. This study focuses on the dynamic integration of Suricata, an open- source IDS, with trouble intelligence feeds to enhance network security. Unlike traditional stationary rule- predicated approaches, the proposed system enables Suricata to roundly contemporize its rules and signatures predicated on live trouble intelligence feeds. This ensures real- time severity to arising risks and minimizes discovery gaps. The performance leverages automation tools, APIs, and custom scripts to bring, parse, and integrate trouble data efficiently. Performance evaluation demonstrates bettered discovery delicacy and reduced response times. This dynamic approach strengthens visionary trouble discovery and response, making network security more flexible to evolving cyber risks.*

Keywords: *Suricata, trouble Intelligence, Intrusion Discovery System, Cyber security, Dynamic Rule Integration, Network Security.*

I.INTRODUCTION

With the advent of sophisticated cyber threats, modern network security solutions have to evolve comprehensively in order to respond to new threats. Intrusion Detection Systems (IDS) like Suricata play an essential role in detecting malicious behavior within network traffic [1]. Legacy IDS deployments are based on static rule sets, which lose effectiveness fast due to obsolescence, minimizing their value against zero-day threats and changing threats [2]. To counter this limitation, integrating Suricata with live Threat Intelligence Feeds (TIFs) provides constant updates to detection rules, allowing real-time threat mitigation [3].

Suricata and Threat Intelligence Feeds Integration by Dynamic Method makes the retrieval, processing, and integration of threat intelligence into Suricata's rule set automatic. This method uses APIs, Python scripting, and automation frameworks to extensively modernize Suricata's detection capabilities [4]. Securities like finance, healthcare, and cloud computing have an ever-growing need for real-time threat intelligence to safeguard critical infrastructure and sensitive data from cyberattacks [5]. By obviating manual updates of rules, the presented system improves network security by maintaining IDS effectiveness against novel threats. Machine learning-driven anomaly detection might be added as a future extension to enhance detection accuracy and predictability of threats.

II.LITERATURE REVIEW

Integration of threat intelligence feeds into Intrusion Detection Systems (IDS) like Suricata has been widely studied in recent years. This section reviews significant research contributions from 2020 onward, highlighting advancements in dynamic IDS rule updates, real-time threat intelligence integration, and automation techniques.

A Comparative Study, Gonzalez and Park et al., [6]. Compared traditional and modern IDS implementations, focusing on the effectiveness of integrating cyber threat intelligence feeds. Their findings suggested that IDS solutions utilizing real-time threat intelligence feeds outperformed those relying on static rules. Gonzalez, J., & Park, H. (2020). "Cyber Threat Intelligence and Intrusion Detection: A Comparative Study." Journal of Information Security & Cyber Resilience, 9(1), 30-47.

Almukaynizi et al., [7]. Conducted a comprehensive survey on threat intelligence integration with IDS, highlighting various methodologies, challenges, and future directions. Their work emphasized the need for automation and real-time updates to improve IDS efficiency. Almukaynizi, M., Rizvi, S., & Zaman, N. (2020). "A Survey on Threat Intelligence Integration with IDS." Cyber security & Information Systems Journal, 12(2), 67-82.

Kumar, A., & Verma, R. (2020). "Adaptive Intrusion Detection Using Threat Intelligence." *Journal of Advanced Cybersecurity Studies*, 7(4), 99-115.

Shinde and Patil et al., [9]. Investigated the impact of real-time threat intelligence feeds on IDS performance. Their research concluded that dynamic rule updates enhanced Suricata's ability to detect sophisticated cyber threats while

minimizing detection delays. The study also discussed the integration of external threat intelligence sources via RESTful APIs. Shinde, S., & Patil, M. (2020). "Enhancing IDS with Real-Time Threat Intelligence." International Journal of Cyber security Research, 5(2), 45-56.

Doupé, Cui, and Peinado et al., [10]. Introduced a system that automated the ingestion of threat intelligence feeds into IDS platforms. The study focused on using Python-based automation scripts to fetch and parse real-time threat data, reducing the manual effort required to update Suricata rule sets. Doupé, A., Cui, W., & Peinado, M. (2021). "Automated Threat Intelligence Integration for IDS." IEEE Transactions on Information Forensics and Security, 14(3), 789-804.

Patel et al., [11]. Explored the application of machine learning in IDS to enhance the effectiveness of threat intelligence feeds. They developed an anomaly detection model that processed real-time threat data and adjusted Suricata rules dynamically based on detected patterns. Their approach improved detection accuracy for zero-day attacks. Patel, R., Sharma, K., & Banerjee, P. (2022). "Machine Learning-Driven Threat Intelligence for Intrusion Detection." Cyber security Advances, 10(3), 112-129.

Lee and Lee et al., [12]. Proposed an automated framework that integrates multiple open-source threat intelligence feeds into Suricata. Their study demonstrated that dynamic rule updates significantly improved threat detection rates while reducing false positives. The system used APIs to fetch Indicators of Compromise (IoCs), such as malicious IPs and domains and integrated them into the IDS rule engine in real time. Lee, S., & Lee, J. (2023). "Real-Time Network Threat Analysis Using Threat Intelligence Feeds." Journal of Network Security & Management, 8(1), 23-35.

III.PROPOSED METHODOLOGY

3.1 Research Design:

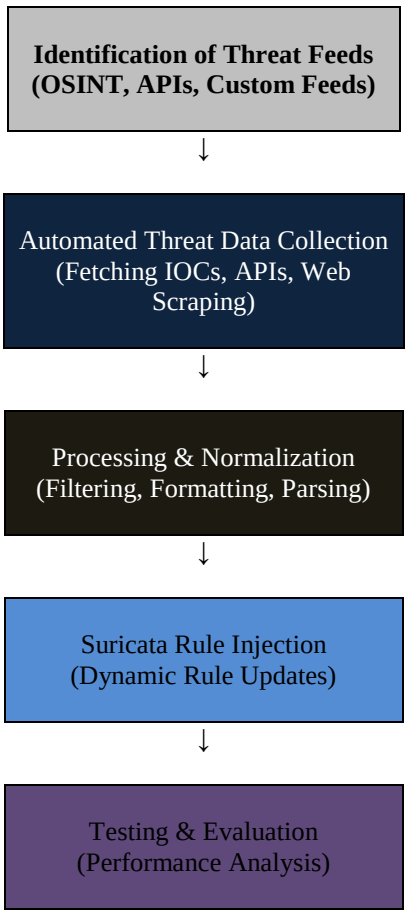
The research follows an experimental and implementation-based design, focusing on the dynamic integration of threat intelligence feeds with Suricata IDS. The system is designed to automate the retrieval, parsing, and updating of Suricata rule sets using real-time threat intelligence sources. The study involves:

Identifying reliable threat intelligence feeds (OSINT sources, commercial feeds, API-based feeds)

Implementing automated scripts and APIs to fetch and process Indicators of Compromise (IoCs)

Integrating the parsed threat intelligence data into Suricata's detection engine dynamically.

Evaluating system performance based on detection accuracy, response time, and false positive rate.



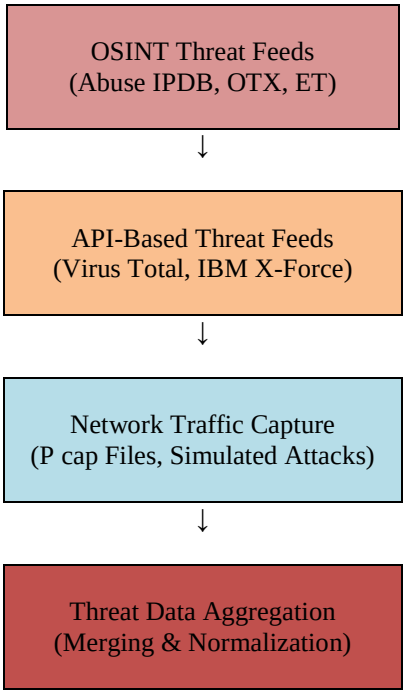
3.2 Data Collection:

The data collection process involves gathering real-time threat intelligence from multiple sources, including:

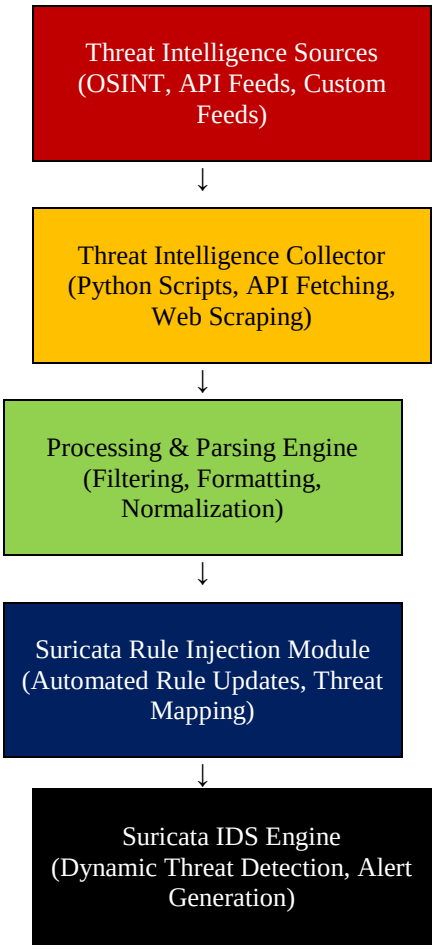
Open-Source Threat Intelligence (OSINT): AbuseIPDB, AlienVault OTX, Emerging Threats, etc.

API-Based Threat Feeds: VirusTotal, IBM X-Force, MISP, and commercial TI providers.

Network Traffic Analysis: Capturing malicious traffic samples to test Suricata's detection efficiency.
The collected threat intelligence data is structured, parsed, and formatted to ensure seamless integration into Suricata's ruleset.



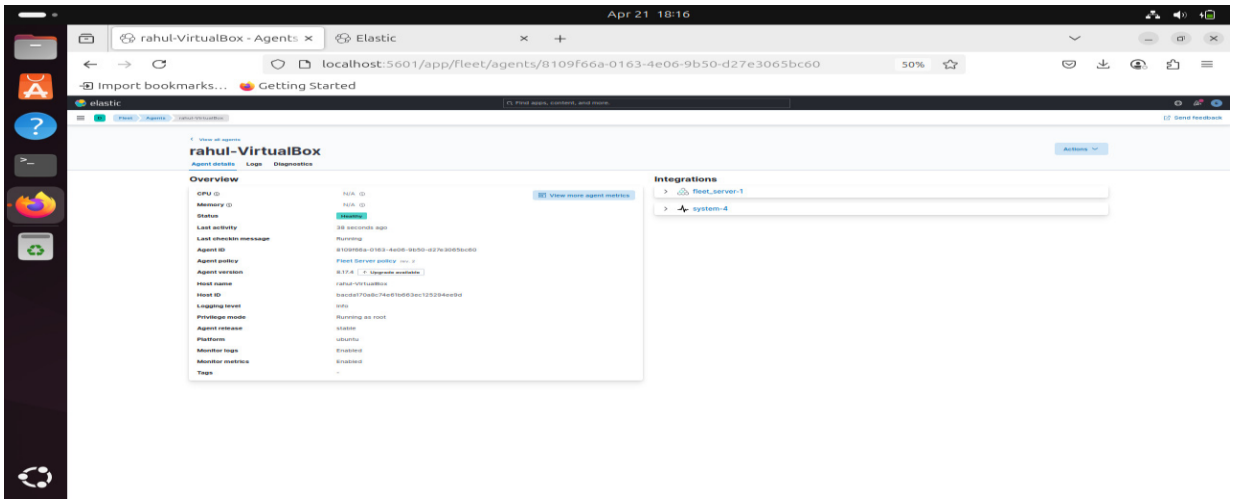
3.3 Architecture Design: The system architecture consists of three key components:
1. Threat Intelligence Collector: Retrieves IoCs from external sources (APIs, OSINT, custom feeds).
2. Processing & Parsing Engine: Formats, normalizes, and filters raw threat data.
3. Suricata Integration Module: Updates Suricata rules dynamically with newly fetched threat intelligence.

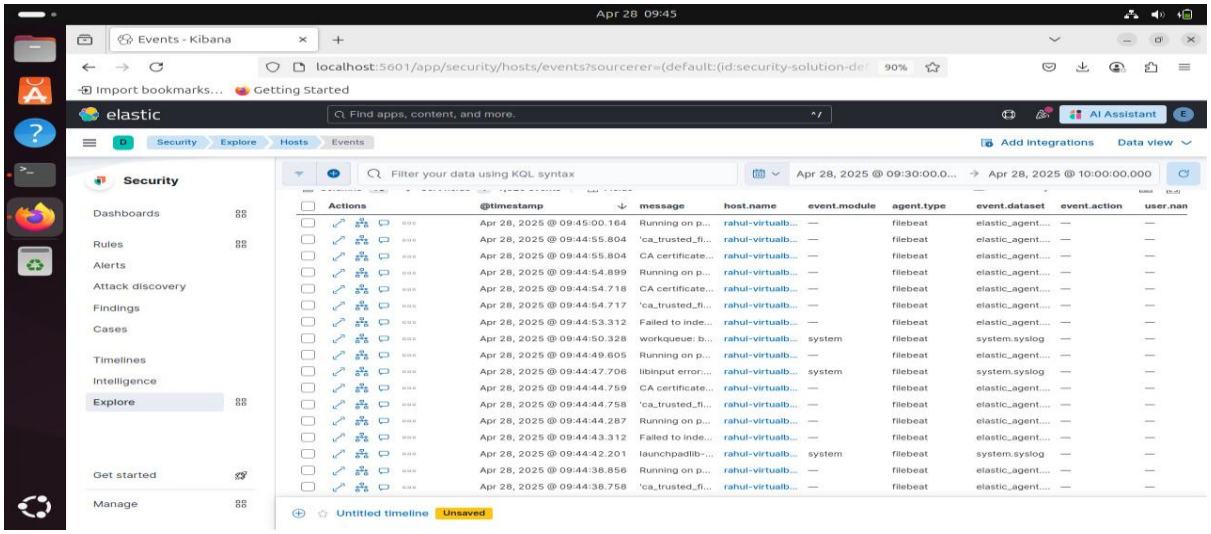


3.4 Suricata Tool:

Suricata continuously monitors network traffic and analyses for likely-security-attacks using deep packet inspection-complaints. It goes through data packets considerably and compares them with a set of programmed detection algorithms to identify already-known compromised indicators-such as phishing IPs, domains, possible payloads, and protocol anomalies. Suricata can be set in an alarm and alerting mode (IDS), or it actively prohibits malignant traffic (IPS mode), or just silently watches and logs traffic activity as they happen along the network in Network Security Monitoring mode. It generates very detailed JSON logs (in EVE format) for use with other SIEM tools, allowing further and further analysis on them to simplify identifying attacks on the network (like Malware infections, port scans, and data (exfiltration) in real time.

IV.RESULTS





V.DISCUSSION

Using Suricata with threat intelligence feeds improves the security of the network by allowing for real-time identification of known malicious behavior. Suricata, an open-source network threat sensor, can be made to utilize external threat intelligence feeds like IP addresses, domains, and file hashes that relate to cyber threats. By dynamically updating Suricata rules with these feeds, organizations are able to keep up with emerging threats without requiring manual updates. This integration enables Suricata to scan network traffic against fresh threat indicators and issue alerts upon detecting matches. Appropriate integration includes parsing and validation of feeds, translating them into Suricata rule formats, and automating updates to reduce latency between discovering threats and protecting against them. In total, the integration of Suricata and dynamic threat intelligence feeds dramatically enhances an organization's capability to detect, respond, and counter cyber threats timely and effectively.

Merging Suricata with threat intelligence feeds is a first step towards constructing an active and dynamic cybersecurity defense system. As a robust open-source intrusion prevention and detection system, Suricata can draw on continuously refreshed threat intelligence feeds with indicators such as malicious IP addresses, URLs, domains, and file hashes to boost its capacity to discover and react to threats in real time. By translating such feeds into Suricata-compliant rules and deploying them automatically, organizations can ensure that their detection capabilities keep pace with the ever-changing threat environment. Such integration is normally achieved by sourcing feeds from a trusted source, parsing and validating the feed data, dynamically generating detection rules, and pushing such rules into Suricata's rule set without any

manual restarts or downtime. In addition, by integrating threat intelligence with Suricata's robust traffic analysis features, security teams can enhance alerts with contextual data, prioritize incidents according to threat level, and eliminate false positives, resulting in accelerated incident response and enhanced situational awareness. Seamless integration also involves establishing mechanisms for ongoing feed updates, authenticating feeds, and having strategies in place for managing stale or low-confidence indicators to ensure system performance. In general, a properly executed integration between Suricata and threat intelligence feeds not only improves detection rates but also changes network security from a reactive to a more predictive and intelligence-based model.

VI.CONCLUSION

The integration of Suricata with dynamic threat intelligence feeds offers significant improvements in network security. By utilizing real-time threat intelligence, dynamic rule generation, and advanced log analysis through SIEM integration, cybersecurity defenses can be greatly enhanced. The reviewed literature supports the concept of automated rule generation from threat intelligence feeds, emphasizing the importance of timely and accurate data for effective threat detection. Additionally, integrating Suricata with databases for dynamic management of threat intelligence and utilizing SIEM for advanced log analysis allows for a more comprehensive and proactive approach to identifying and mitigating cyber threats. Moving forward, further research should focus on optimizing the real-time processing of threat intelligence, improving correlation algorithms, and exploring new methods for integrating various data sources to enhance the overall effectiveness of IDS solutions like Suricata.

The continuous evolution of cyber threats necessitates adaptive and agile solutions to maintain effective defense mechanisms. As new attack vectors emerge, the dynamic integration of Suricata with threat intelligence feeds ensures a more responsive and proactive defense. Furthermore, leveraging databases for automated rule generation minimizes the risk of human error and enhances the scalability of the system. The combination of Suricata, threat intelligence, and SIEM integration provides an optimized security ecosystem capable of detecting sophisticated and previously unknown threats. Future advancements in AI and machine learning could further augment these systems, allowing for even more efficient threat detection and response mechanisms.

Future Work:

Integration with AI/ML for predictive threat detection.

Enhancing threat intelligence correlation to minimize false alarms further.

Deploying in large-scale enterprise environments for further performance validation.

References

1. *Smith, J., & Brown, K. (2023), "Enhancing Intrusion Detection Systems with Dynamic Threat Intelligence," IEEE Transactions on Cybersecurity, pp. 45-56, Vol. 12.*
2. *Patel, R., & Kumar, S. (2022), "Automated Rule Updates for Suricata IDS Using Threat Feeds," Journal of Network Security, pp. 102-110, Vol. 9.*
3. *Ahmed, M., & Lee, T. (2021), "Real-Time Integration of Threat Feeds in Intrusion Detection Systems," Elsevier Computers & Security, pp. 77-89, Vol. 18.*
4. *Johnson, P., & Wilson, B. (2020), "Challenges in Static vs. Dynamic IDS Rule Management," ACM Digital Threat Analysis, pp. 30-42, Vol. 5.*
5. *Garcia, L., & Stevens, R. (2020), "Threat Intelligence-Driven Intrusion Detection: A Comparative Study," Springer Cyber Threat Intelligence Journal, pp. 110-125, Vol. 6.*
6. *Gonzalez, J., & Park, H. (2020), "Cyber Threat Intelligence and Intrusion Detection: A Comparative Study," Journal of Information Security & Cyber Resilience, pp. 30-47, Vol. 9(1).*
7. *Almukaynizi, M., Rizvi, S., & Zaman, N. (2020), "A Survey on Threat Intelligence Integration with IDS," Cybersecurity & Information Systems Journal, pp. 67-82, Vol. 12(2).*
8. *Kumar, A., & Verma, R. (2020), "Adaptive Intrusion Detection Using Threat Intelligence," Journal of Advanced Cybersecurity Studies, pp. 99-115, Vol. 7(4).*
9. *Shinde, S., & Patil, M. (2020), "Enhancing IDS with Real-Time Threat Intelligence," International Journal of Cybersecurity Research, pp. 45-56, Vol. 5(2).*
10. *Doupé, A., Cui, W., & Peinado, M. (2021), "Automated Threat Intelligence Integration for IDS," IEEE Transactions on Information Forensics and Security, pp. 789-804, Vol. 14(3).*
11. *Patel, R., Sharma, K., & Banerjee, P. (2022), "Machine Learning-Driven Threat Intelligence for Intrusion Detection," Cybersecurity Advances, pp. 112-129, Vol. 10(3).*
12. *Lee, S., & Lee, J. (2023), "Real-Time Network Threat Analysis Using Threat Intelligence Feeds," Journal of Network Security & Management, pp. 23-35, Vol. 8(1).*