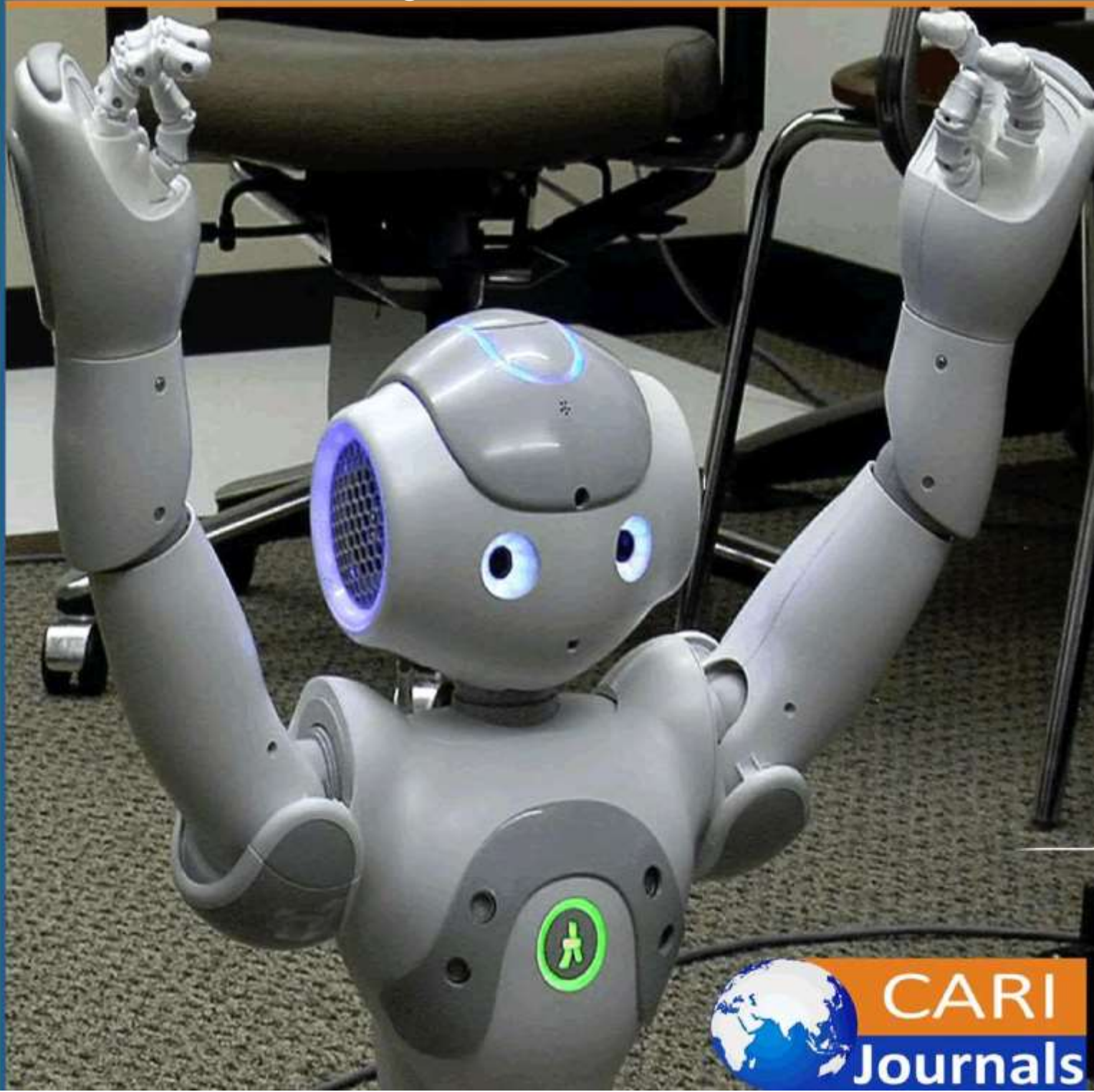


International Journal of **Computing and Engineering** (IJCE)

**Detection Engineering for Zero-Day Threats: Bridging
Intelligence and Automation**



**CARI
Journals**

Detection Engineering for Zero-Day Threats: Bridging Intelligence and Automation

 Bhuvan Bobba

<https://orcid.org/0009-0002-4356-8555>

Accepted: 21st Feb, 2023, Received in Revised Form: 10th March, 2023, Published: 21st March, 2023

Abstract:

Zero-day threats represent one of the most significant challenges in modern cybersecurity because they exploit previously unknown vulnerabilities before security vendors can develop signatures or patches. Traditional signature-based detection mechanisms are increasingly ineffective against these rapidly evolving attacks, creating a need for proactive, intelligence-driven detection strategies. Detection engineering has emerged as a discipline that combines threat intelligence, behavioral analytics, telemetry correlation, and automated response to identify malicious activity independent of known indicators of compromise. This paper examines how detection engineering can bridge cyber threat intelligence and security automation to improve the identification and mitigation of zero-day threats. It reviews the evolution of detection methodologies from static rule-based systems to behavior-based analytics supported by artificial intelligence, machine learning, and Security Orchestration, Automation, and Response (SOAR) platforms. The article further explores the integration of frameworks such as MITRE ATT&CK, threat hunting methodologies, endpoint detection and response (EDR), extended detection and response (XDR), and cloud-native security monitoring to build adaptive detection capabilities. Challenges including false positives, intelligence quality, adversarial evasion techniques, privacy considerations, and automation reliability are critically analyzed. The paper proposes a conceptual framework that integrates continuous threat intelligence, automated detection engineering, and adaptive response workflows to enhance organizational cyber resilience against zero-day attacks. The findings demonstrate that combining intelligence-driven detection engineering with automated security operations significantly improves early detection, reduces mean time to detect (MTTD), and strengthens defenses against previously unknown cyber threats.

Keywords: *Detection Engineering, Zero-Day Threats, Cyber Threat Intelligence, Security, Automation, SIEM, SOAR, MITRE ATT&CK, Threat Hunting, EDR, XDR, Artificial Intelligence*



1. INTRODUCTION

The evolution of cyber threats has significantly challenged traditional security mechanisms, particularly with the emergence of zero-day attacks that exploit previously unknown software vulnerabilities before vendors can develop security patches or detection signatures. Unlike conventional malware, zero-day threats often evade signature-based intrusion detection systems, resulting in substantial financial losses, operational disruption, and compromised critical infrastructure [1]. High-profile incidents such as Stuxnet and the exploitation of Microsoft Exchange Server vulnerabilities have demonstrated that sophisticated adversaries increasingly leverage zero-day exploits to achieve strategic objectives while remaining undetected for extended periods. Organizations require detection capabilities that emphasize behavioral analysis rather than reliance on known indicators of compromise (IOCs).

Detection engineering has emerged as a critical discipline within modern Security Operations Centers (SOCs), focusing on the systematic design, implementation, validation, and continuous improvement of high-fidelity detection logic. By integrating cyber threat intelligence (CTI), endpoint and network telemetry, and adversary tactics, techniques, and procedures (TTPs), detection engineering enables security teams to identify malicious behavior associated with previously unseen attacks [2]. Advances in Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Orchestration, Automation, and Response (SOAR) technologies have enabled automated correlation, prioritization, and incident response, reducing the mean time to detect and respond to emerging threats. This article explores how intelligence-driven detection engineering, supported by automation, can strengthen organizational resilience against zero-day threats. It examines current detection methodologies, discusses the integration of CTI and automation frameworks, and proposes a conceptual approach for developing adaptive detection capabilities that can respond effectively to sophisticated and previously unknown cyberattacks [3].

2. LITERATURE REVIEW

The increasing sophistication of cyberattacks has accelerated research into proactive detection methodologies capable of identifying previously unknown threats. Traditional signature-based detection systems remain effective against known malware but exhibit significant limitations when confronting zero-day exploits because they depend on predefined indicators of compromise. Contemporary cybersecurity research has shifted toward behavior-based detection, threat intelligence integration, and automated security operations that emphasize adversarial behaviors rather than static attack signatures [4].

Detection engineering has emerged as a systematic approach for developing, validating, and continuously improving detection logic based on attacker tactics, techniques, and procedures (TTPs). Unlike conventional security monitoring, detection engineering combines telemetry from endpoints, networks, cloud environments, and identity systems with structured threat intelligence

to create high-confidence detections. This paradigm is strongly influenced by adversary emulation frameworks, particularly the MITRE ATT&CK knowledge base, which provides a standardized taxonomy for mapping attacker behaviors across the cyber kill chain. The adoption of ATT&CK has improved detection coverage assessments, facilitated threat hunting, and enhanced collaboration among security analysts by enabling behavior-centric detection strategies rather than vulnerability-specific signatures [5].

Parallel advances in Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Orchestration, Automation, and Response (SOAR) platforms have further transformed modern security operations. These technologies aggregate and correlate telemetry from diverse sources, enrich alerts using cyber threat intelligence, and automate repetitive investigation and response tasks. Researchers have shown that automation can substantially reduce analyst workload while improving consistency in incident response, provided that automated workflows are continuously validated and supported by high-quality intelligence. Nevertheless, challenges remain, including false positives, adversarial evasion techniques, intelligence quality, and the explainability of artificial intelligence models used in cybersecurity. These limitations highlight the need for integrated detection engineering frameworks that effectively bridge intelligence-driven analytics with adaptive automation to improve resilience against zero-day threats [6].

3. DETECTION ENGINEERING ARCHITECTURE

Detection engineering architecture provides the technical foundation for identifying malicious activities associated with zero-day threats through continuous collection, analysis, and correlation of security telemetry. Unlike traditional intrusion detection systems that primarily depend on known attack signatures, detection engineering architectures emphasize behavioral analytics, adversary techniques, and intelligence-driven detection logic. A well-designed architecture integrates multiple layers of security monitoring to transform raw telemetry into actionable detections while supporting continuous improvement through feedback from threat hunting and incident response activities [7].

The architecture begins with comprehensive data acquisition from heterogeneous sources, including endpoint devices, network sensors, cloud workloads, identity management systems, application logs, Domain Name System (DNS) records, authentication events, and threat intelligence feeds. These diverse telemetry sources provide visibility across the attack surface, enabling analysts to observe attacker behaviors throughout different stages of the intrusion lifecycle. To ensure interoperability, collected data are normalized into standardized schemas before being forwarded to centralized repositories such as Security Information and Event Management (SIEM) platforms or data lakes. Data normalization facilitates efficient querying, correlation, and long-term storage while reducing inconsistencies among heterogeneous log formats [8].

The analytics layer constitutes the core of the detection engineering architecture. At this stage, detection rules combine signature-based techniques with behavioral analytics, statistical anomaly detection, heuristic analysis, and machine learning models to identify suspicious activities that may indicate previously unknown attacks. Detection logic is increasingly mapped to adversary tactics, techniques, and procedures (TTPs) defined in the MITRE ATT&CK framework, enabling behavior-based monitoring rather than vulnerability-specific detection. Correlation engines further enhance detection fidelity by linking events across endpoints, networks, cloud services, and user identities, thereby reducing false positives and improving contextual awareness [9].

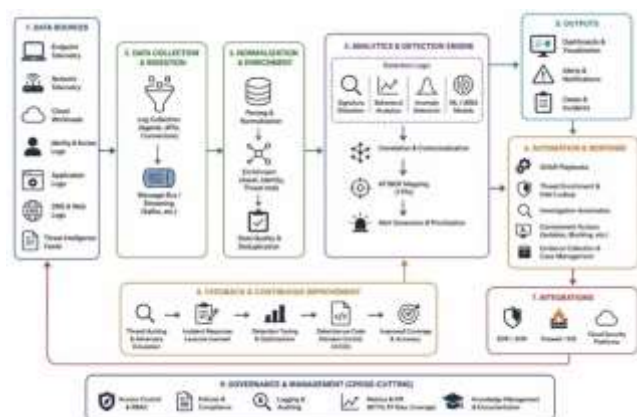


Figure 1. Detection Engineering Architecture

Automation represents another critical architectural component. Security Orchestration, Automation, and Response (SOAR) platforms integrate with SIEM, Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) solutions to automate alert enrichment, threat intelligence lookups, evidence collection, case creation, and incident response workflows. Automated playbooks accelerate investigation while maintaining consistency in containment procedures. Simultaneously, detection engineering adopts software engineering practices through Detection-as-Code, where detection rules are version-controlled, continuously tested, peer-reviewed, and deployed using continuous integration and continuous deployment (CI/CD) pipelines. This approach enables rapid adaptation to evolving adversary behaviors while improving rule quality, reproducibility, and governance [10].

Continuous feedback mechanisms ensure that the architecture evolves alongside the threat landscape. Insights obtained from incident investigations, threat hunting exercises, purple-team assessments, and adversary emulation activities are incorporated into detection logic to improve coverage and accuracy. This iterative process creates a resilient detection ecosystem capable of identifying emerging attack techniques, including zero-day exploits, before they can cause significant operational impact. Detection engineering architecture serves as the bridge between cyber threat intelligence, advanced analytics, and automated security operations, enabling organizations to develop adaptive defenses against sophisticated cyber threats.

4. BRIDGING INTELLIGENCE AND AUTOMATION

The increasing complexity and speed of modern cyberattacks have made it insufficient for organizations to rely solely on manual security analysis or isolated threat intelligence. Bridging cyber threat intelligence (CTI) with security automation has become a fundamental principle of modern detection engineering, enabling organizations to rapidly identify, investigate, and respond to zero-day threats. Cyber threat intelligence provides contextual information regarding adversary capabilities, motivations, infrastructure, and tactics, techniques, and procedures (TTPs), while automation operationalizes this intelligence by incorporating it into detection rules, alert prioritization, and incident response workflows. The integration of these capabilities enhances the adaptability of security operations centers (SOCs) by reducing detection latency and improving decision-making accuracy [11].

Threat intelligence serves as the knowledge layer of detection engineering by enriching security telemetry with contextual information obtained from commercial, open-source, governmental, and industry-specific intelligence feeds. Rather than focusing exclusively on indicators of compromise (IOCs), contemporary detection engineering increasingly emphasizes behavior-based intelligence derived from adversary TTPs documented in knowledge repositories such as the MITRE ATT&CK framework. This behavioral perspective enables organizations to detect unknown attacks that exhibit recognizable operational patterns despite employing previously unseen malware or exploiting undisclosed vulnerabilities. Intelligence-driven detection also supports proactive threat hunting, allowing analysts to formulate hypotheses based on emerging adversary behaviors and validate them using enterprise telemetry [12].

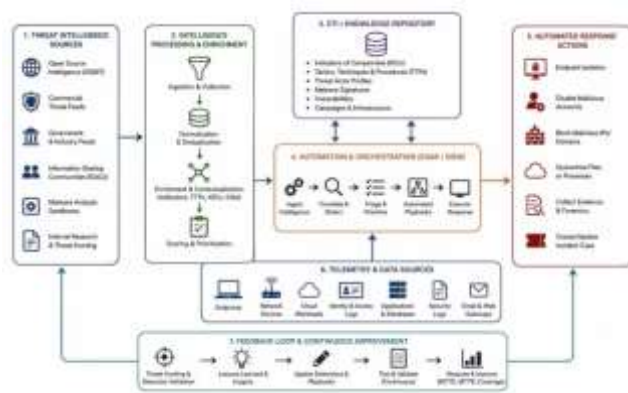


Figure 2. Bridging Intelligence and Automation

Automation complements threat intelligence by transforming analytical knowledge into executable detection and response mechanisms. Security Information and Event Management (SIEM) platforms aggregate and correlate security events from multiple environments, while Security Orchestration, Automation, and Response (SOAR) platforms automate repetitive operational tasks such as threat intelligence enrichment, alert triage, evidence collection, case

creation, and containment actions. Automated playbooks can isolate compromised endpoints, disable malicious user accounts, block network communications, or initiate forensic acquisition based on predefined decision logic. This orchestration significantly reduces the mean time to detect (MTTD) and mean time to respond (MTTR), enabling security teams to focus on higher-value investigative activities rather than routine operational tasks [13].

The effectiveness of intelligence-driven automation depends on maintaining accurate and continuously updated detection content. Detection engineering therefore adopts iterative feedback mechanisms in which intelligence analysts, threat hunters, incident responders, and detection engineers collaboratively refine detection rules based on lessons learned from investigations and adversary emulation exercises. Detection-as-Code practices further support this process by applying software engineering principles including version control, peer review, automated testing, and continuous integration/continuous deployment (CI/CD) to the lifecycle of detection content. These practices improve traceability, governance, and detection reliability while facilitating rapid adaptation to newly observed attack techniques [14].

Despite these advantages, integrating intelligence and automation introduces several operational challenges. Intelligence feeds may contain incomplete or outdated information, automated workflows may generate false positives if detection logic is insufficiently validated, and adversaries increasingly employ evasion techniques designed to bypass automated defenses. Organizations should balance automation with expert human oversight, ensuring that automated actions remain transparent, explainable, and continuously evaluated. An effective detection engineering strategy therefore combines high-quality cyber threat intelligence, behavior-based analytics, adaptive automation, and continuous validation to establish resilient defenses capable of detecting and mitigating sophisticated zero-day threats before significant organizational impact occurs.

5. PROPOSED CONCEPTUAL FRAMEWORK

The proposed conceptual framework aims to integrate cyber threat intelligence (CTI), detection engineering, behavioral analytics, and security automation into a unified architecture capable of detecting and responding to zero-day threats. Unlike conventional security models that rely primarily on signature-based detection, the proposed framework adopts a behavior-centric approach that emphasizes adversary tactics, techniques, and procedures (TTPs), continuous telemetry analysis, and automated response mechanisms. The framework is designed to improve cyber resilience by enabling adaptive detection, reducing response latency, and continuously refining detection capabilities through operational feedback [15].

The framework consists of seven interconnected layers that collectively support the lifecycle of intelligence-driven detection engineering. The first layer, Threat Intelligence Collection, acquires structured and unstructured intelligence from commercial feeds, open-source intelligence (OSINT), Information Sharing and Analysis Centers (ISACs), malware repositories, vulnerability

databases, and internal threat-hunting activities. Intelligence is normalized, validated, and mapped to standardized frameworks such as MITRE ATT&CK and Structured Threat Information Expression (STIX) to ensure interoperability and contextual consistency [16].

The second layer, Telemetry Collection and Data Integration, continuously gathers security events from endpoint devices, network sensors, cloud platforms, identity services, application logs, Domain Name System (DNS) records, email gateways, and authentication systems. Data are normalized and enriched using contextual information, including asset criticality, user identity, geolocation, and threat intelligence attributes. Centralized Security Information and Event Management (SIEM) platforms aggregate these heterogeneous data sources to establish comprehensive organizational visibility and facilitate efficient event correlation.



Figure 3. Proposed Conceptual Framework

The third layer, Detection Engineering and Behavioral Analytics, constitutes the analytical core of the framework. Detection logic combines signature-based rules, heuristic analysis, statistical anomaly detection, user and entity behavior analytics (UEBA), and machine learning techniques to identify suspicious activities indicative of previously unknown attacks. Detection rules are mapped to adversary TTPs rather than individual indicators of compromise, enabling the identification of evolving attack techniques that may exploit zero-day vulnerabilities. Continuous threat hunting and adversary emulation activities validate and improve detection effectiveness while minimizing false positives [17].

The fourth layer, Automation and Orchestration, operationalizes detection outcomes through Security Orchestration, Automation, and Response (SOAR) workflows. Automated playbooks perform contextual enrichment, alert prioritization, evidence collection, ticket creation, endpoint isolation, malicious account suspension, firewall updates, and threat containment based on predefined response policies. This layer substantially reduces the mean time to detect (MTTD) and mean time to respond (MTTR), while ensuring consistent execution of incident response procedures.

The fifth layer, Incident Response and Continuous Feedback, closes the detection lifecycle by incorporating lessons learned from incident investigations, digital forensics, penetration testing, purple-team exercises, and threat-hunting operations. These insights are translated into improved detection logic through Detection-as-Code practices, where detection content is version-controlled, peer-reviewed, automatically tested, and continuously deployed using software engineering methodologies. The continuous feedback mechanism enables the framework to evolve alongside changing adversary behaviors and emerging threat landscapes [18].

The proposed conceptual framework establishes a continuous intelligence-driven detection cycle in which cyber threat intelligence informs detection engineering, behavioral analytics improve detection accuracy, automation accelerates operational response, and feedback mechanisms ensure continuous optimization. This integrated approach strengthens organizational capabilities for identifying and mitigating sophisticated zero-day threats while enhancing the scalability, consistency, and adaptability of modern Security Operations Centers (SOCs).

6. CHALLENGES

Despite significant advances in detection engineering, cyber threat intelligence (CTI), and security automation, organizations continue to face numerous challenges in effectively detecting and mitigating zero-day threats. Zero-day attacks exploit previously unknown vulnerabilities and often exhibit limited or no historical indicators of compromise (IOCs), rendering traditional signature-based detection techniques inadequate. Detection engineering increasingly relies on behavioral analytics, anomaly detection, and intelligence-driven correlation. These approaches introduce new technical, operational, and organizational complexities that must be addressed to ensure reliable and resilient security operations [19].

One of the primary challenges is the high incidence of false positives generated by behavior-based detection systems. Modern Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) platforms continuously process vast volumes of heterogeneous telemetry from endpoints, cloud infrastructures, identity systems, and network devices. While behavioral detection improves visibility into unknown attacks, distinguishing malicious activity from legitimate user behavior remains difficult. Excessive false-positive alerts contribute to analyst fatigue, increase investigation costs, and may delay responses to genuine security incidents. Effective detection engineering therefore requires continuous rule validation, detection tuning, contextual enrichment, and risk-based prioritization to improve detection fidelity [20].

Another significant challenge concerns the quality, timeliness, and interoperability of cyber threat intelligence. Threat intelligence feeds frequently contain incomplete, duplicated, or outdated indicators that may not accurately reflect evolving adversary tactics, techniques, and procedures (TTPs). Organizations often consume intelligence from multiple commercial, governmental, and open-source providers using heterogeneous data formats, complicating automated intelligence

fusion and contextual analysis. Standardized intelligence-sharing frameworks such as STIX and TAXII have improved interoperability, yet intelligence validation and prioritization remain essential for preventing inaccurate detections and unnecessary automated responses. Detection engineers must therefore continuously evaluate intelligence sources while correlating external intelligence with internal organizational telemetry.

Automation also introduces operational and governance challenges. Although Security Orchestration, Automation, and Response (SOAR) platforms significantly reduce mean time to detect (MTTD) and mean time to respond (MTTR), poorly designed automation workflows may inadvertently disrupt legitimate business operations through inappropriate containment actions or excessive alert escalation. Machine learning models used in anomaly detection are susceptible to concept drift, adversarial manipulation, and reduced explainability, making it difficult for analysts to understand or validate automated decisions. These concerns underscore the importance of maintaining human oversight, transparent decision-making processes, and rigorous testing of automated detection content before production deployment.

Cloud computing, hybrid infrastructures, and remote work environments further complicate detection engineering. Modern enterprises operate across multiple cloud service providers, containerized workloads, software-defined networks, and distributed endpoints, generating diverse telemetry that must be collected, normalized, and correlated in near real time. Ensuring consistent visibility across these heterogeneous environments while maintaining regulatory compliance and protecting user privacy presents substantial architectural and governance challenges. The growing adoption of encrypted communications limits the effectiveness of traditional network monitoring techniques, increasing dependence on endpoint telemetry and identity-based analytics.

Addressing these challenges requires a continuous improvement strategy that integrates intelligence-driven detection engineering, automation, behavioral analytics, and collaborative threat hunting. Detection-as-Code methodologies, adversary emulation exercises, purple-team assessments, and continuous validation enable organizations to refine detection logic, reduce false positives, and improve resilience against emerging zero-day threats. The successful integration of intelligence and automation depends not only on advanced technologies but also on effective governance, skilled security personnel, and an adaptive organizational security culture capable of responding to an evolving cyber threat landscape [21].

7. FUTURE RESEARCH DIRECTIONS

One promising direction is the application of artificial intelligence (AI) and explainable machine learning (XML) in detection engineering. Although machine learning has demonstrated effectiveness in anomaly detection and behavioral analysis, many existing models operate as "black boxes," limiting analysts' ability to interpret detection decisions. Future studies should investigate explainable AI techniques that provide transparent reasoning, confidence metrics, and interpretable feature attribution to improve analyst trust, facilitate incident investigations, and

support regulatory compliance. Research into continual learning and federated learning could enable detection models to adapt dynamically to evolving adversarial behaviors while preserving data privacy across distributed environments.

Another important research area involves the advancement of Detection-as-Code (DaC) methodologies. Applying software engineering principles including version control, automated testing, continuous integration/continuous deployment (CI/CD), and policy-as-code to detection content has significantly improved detection reliability. Standardized frameworks for automated detection validation, quality assurance, performance benchmarking, and governance remain underdeveloped. Future research should establish formal methodologies for measuring detection quality, including metrics such as detection precision, recall, coverage, mean time to detect (MTTD), and detection resilience against adversarial evasion.

The integration of Large Language Models (LLMs) and Generative Artificial Intelligence (GenAI) into Security Operations Centers (SOCs) represents another emerging research direction. LLMs have the potential to assist security analysts by automatically generating detection rules, translating threat intelligence into detection logic, summarizing incident investigations, recommending mitigation strategies, and accelerating threat hunting activities. Future work should investigate the reliability, security, explainability, and governance of AI-assisted detection engineering while addressing concerns such as hallucinations, prompt injection attacks, data confidentiality, and model bias.

Future research should also explore threat-informed autonomous security operations, where cyber threat intelligence continuously drives automated detection, orchestration, and response. Intelligent SOAR platforms could dynamically adapt playbooks based on adversary behavior, contextual risk assessment, and real-time intelligence updates. Such adaptive automation would reduce analyst workload while improving response consistency and operational scalability. Research into reinforcement learning and autonomous decision-making algorithms may further enhance the capability of security platforms to optimize response strategies without compromising human oversight.

Another promising avenue is the development of predictive threat intelligence through advanced analytics and graph-based knowledge representation. Rather than reacting to known attacks, predictive detection systems could leverage attack graphs, knowledge graphs, digital twins, and historical adversary behaviors to anticipate potential attack paths before exploitation occurs. Integrating MITRE ATT&CK, MITRE D3FEND, STIX, TAXII, and vulnerability intelligence into predictive analytical models may significantly improve proactive cyber defense against zero-day threats.

Future detection engineering research should prioritize adaptive intelligence integration, explainable artificial intelligence, autonomous security operations, cloud-native detection, predictive analytics, and human-centered security design. These advances will contribute to more

resilient cybersecurity ecosystems capable of proactively detecting, understanding, and mitigating sophisticated zero-day threats in increasingly complex digital environments.

8. RECOMMENDATIONS

Organizations should adopt intelligence-driven detection engineering that integrates cyber threat intelligence (CTI), behavioral analytics, and automation to strengthen defenses against zero-day threats. Behavior-based detection aligned with frameworks such as MITRE ATT&CK can identify adversary tactics, techniques, and procedures (TTPs) that traditional signature-based methods may overlook. Detection-as-Code (DaC), supported by version control, automated testing, CI/CD, and regular adversary simulations, can improve the reliability and governance of detection rules. High-quality threat intelligence should be continuously validated, prioritized, and standardized using frameworks such as STIX and TAXII before being incorporated into detection workflows. SOAR platforms should automate repetitive, low-risk activities while retaining human oversight for high-impact response decisions. Finally, organizations should continuously refine behavior-based detection using endpoint, network, identity, and UEBA telemetry, with artificial intelligence supporting analysts through improved event correlation, prioritization, and decision-making.

9. CONCLUSION

Zero-day threats continue to challenge conventional cybersecurity practices by exploiting previously unknown vulnerabilities that evade signature-based detection mechanisms. This article examined how detection engineering can bridge cyber threat intelligence and security automation to improve the detection and mitigation of sophisticated zero-day attacks. The study highlighted the importance of integrating behavior-based detection, intelligence-driven analytics, Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), Endpoint Detection and Response (EDR), and Detection-as-Code into a unified detection architecture. A conceptual framework was proposed that combines continuous threat intelligence collection, telemetry integration, behavioral analytics, automated orchestration, and continuous feedback to enhance detection accuracy and operational resilience. The analysis also identified key challenges, including false positives, intelligence quality, automation governance, cloud complexity, and adversarial evasion, which must be addressed to ensure effective implementation. Future research opportunities involving explainable artificial intelligence, autonomous security operations, predictive threat intelligence, and cloud-native detection architectures were discussed. Intelligence-driven detection engineering provides a proactive and adaptive approach for modern Security Operations Centers to counter evolving cyber threats. By integrating continuous intelligence, advanced analytics, and automated response capabilities, organizations can significantly improve their ability to detect, investigate, and respond to zero-day attacks while strengthening overall cyber resilience in an increasingly dynamic threat environment.

REFERENCES

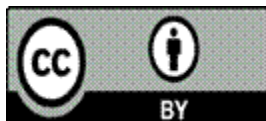
- [1] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, pp. 80–106, 2011.
- [2] S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 186–205, Aug. 2000.
- [3] MITRE Corporation, MITRE ATT&CK®: Design and Philosophy, Technical Report, MITRE, McLean, VA, USA, 2020.
- [4] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 305–316.
- [5] MITRE Corporation, MITRE ATT&CK® Evaluations: A Roadmap for Measuring Enterprise Security Capabilities, McLean, VA, USA, 2021.
- [6] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. San Francisco, CA, USA: No Starch Press, 2013.
- [7] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. San Francisco, CA, USA: No Starch Press, 2013.
- [8] A. O. Balogun and S. Basri, "Cyber security event management: A review of SIEM architecture, challenges and future directions," *Journal of Information Security and Applications*, vol. 58, Art. no. 102748, 2021.
- [9] MITRE Corporation, MITRE ATT&CK®: Design and Philosophy, McLean, VA, USA, Technical Report, 2020.
- [10] D. Bianco, "The Pyramid of Pain," *Pyramid of Pain Project*, 2014.
- [11] M. Conti, T. Dargahi, and A. Dehghantanha, "Cyber threat intelligence: Challenges and opportunities," in *Cyber Threat Intelligence*, Cham, Switzerland: Springer, 2018, pp. 1–25.
- [12] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, SANS Industrial Control Systems, 2016.
- [13] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Revision 2, Gaithersburg, MD, USA, Aug. 2012.
- [14] D. Bianco and J. Spring, *Detecting the Adversary with ATT&CK®*, MITRE Engenuity Center for Threat-Informed Defense, McLean, VA, USA, 2022.
- [15] OASIS, STIX™ Version 2.1. Part 1: STIX Core Concepts, Committee Specification 01, OASIS Open, Feb. 2021.
- [16] OASIS, TAXII™ Version 2.1. Trusted Automated eXchange of Indicator Information, Committee Specification 01, OASIS Open, Feb. 2021.
- [17] MITRE Engenuity Center for Threat-Informed Defense, *Summitting the Pyramid: Constructing a Threat-Informed Defense Program*, McLean, VA, USA, 2021.

[18] National Institute of Standards and Technology (NIST), Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, Gaithersburg, MD, USA, Sept. 2020.

[19] National Institute of Standards and Technology (NIST), Guide for Cybersecurity Event Recovery, NIST Special Publication 800-184, Gaithersburg, MD, USA, Dec. 2016.

[20] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 305–316.

[21] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2022, Heraklion, Greece, 2022.



©2023 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>)