MANTECH Publications

Journal of Next-Gen Threat Intelligence and Cyber Defense
Volume 2, Issue 2, May-August 2026

Zero Trust Cyber Defense Architectures: Integrating Continuous Threat Intelligence for Enterprise Security

Zaid Lakdawala[1], Yashaswini Dongre[2]

ABSTRACT

Modern enterprise networks face an unprecedented volume of sophisticated cyber threats that evade perimeter-based defenses. The shift toward Zero Trust Architecture (ZTA) enforces explicit verification, least-privilege access, and continuous risk assessment across all entities. However, static Zero Trust implementations often suffer from reactive policy execution and delayed context updating, leaving windows for lateral movement. This review paper presents an exhaustive analysis of integrating Continuous Threat Intelligence (CTI) into Zero Trust cyber defense frameworks to establish an adaptive security posture. We evaluate combining real-time threat feeds—comprising Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), and vulnerability disclosures—with Policy Decision Points (PDP) and Policy Enforcement Points (PEP). Through empirical benchmark analysis, architectural modeling, and case evaluation, we demonstrate that CTI-integrated Zero Trust architectures achieve a 95.7% reduction in Mean Time to Detect (MTTD) and an 83.0% improvement in Mean Time to Respond (MTTR) compared to baseline ZTA. Furthermore, we analyze trade-offs regarding ingestion latency, policy synchronization overhead, and false-positive rates, outlining research gaps and deployment guidelines.

KEYWORDS: *Zero Trust Architecture (ZTA), Continuous Threat Intelligence (CTI), Policy Decision Point (PDP), Cyber Defense, Micro-segmentation, Identity and Access Management (IAM), Telemetry Fusion.*

INTRODUCTION

The modern enterprise digital landscape has transformed over the past decade. The widespread adoption of multi-cloud architectures, remote workforce initiatives, IoT

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

ecosystems, and SaaS platforms has dissolved the traditional network perimeter [1]. Historically, enterprise security relied on border-centric defense models—often described as 'castle-and-moat' architectures—where internal network traffic was inherently trusted once perimeter barriers were traversed [2]. This assumption of internal trust has proven fundamentally flawed. Modern adversaries exploit initial access vectors through phishing, supply chain compromises, or zero-day vulnerabilities to establish beachheads within internal networks, executing lateral movement and exfiltration without triggering perimeter controls [3].

To counter these vulnerabilities, the security paradigm has shifted toward Zero Trust Architecture (ZTA), formalized by NIST SP 800-207 [4]. Zero Trust operates under the core philosophy of 'never trust, always verify.' It dictates that no user, device, application, or network packet is granted implicit trust [5]. Every access request must be authenticated, authorized, and continuously validated against strict policies prior to session establishment and throughout the interaction.

Despite structural advantages, standard Zero Trust implementations encounter operational constraints in isolation. Traditional ZTA reliance on static attribute evaluation—such as user role and device state—fails to account for fast-evolving external threat indicators [6]. When threat intelligence feeds are disjointed, Policy Decision Points (PDP) make access decisions based on stale security context. To achieve proactive cyber defense, enterprise infrastructures require the real-time integration of Continuous Threat Intelligence (CTI) into the policy engine [7]. CTI provides actionable telemetry—including live IOCs, adversary TTPs mapped to MITRE ATT&CK, and dynamic reputation scores—enabling Policy Enforcement Points (PEP) to adaptively modify firewall rules, revoke tokens, and isolate micro-segmented workloads in real time [8].

LITERATURE REVIEW

The evolution of enterprise cyber defense from perimeter frameworks to continuous validation paradigms has attracted intense academic investigation. Rose et al. [4] established core tenets of NIST SP 800-207, defining interactions between the Policy Engine, Policy Administrator, and Policy Enforcement Point. Their model emphasized session-level authorization but noted that real-time adaptation requires robust integrations with external security telemetry feeds.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Stafford [5] explored the zero trust maturity model, emphasizing that identity authentication serves as the primary gateway for access control. However, as highlighted by Kindervag [9], identity validation alone is insufficient without granular network micro-segmentation and strict device hygiene verification. Kindervag argued that micro-perimeters must be drawn around individual high-value assets to limit breach radii, preventing lateral movement when credentials are compromised.

In parallel, research on Continuous Threat Intelligence (CTI) has focused on standardizing sharing protocols and automated ingestion mechanisms. Barnum [10] developed STIX and TAXII protocols, enabling automated, machine-readable threat data interchange across enterprise security systems. Mavroeidis and Bromander [11] mapped threat intelligence feeds to the MITRE ATT&CK knowledge base, establishing a structured framework for correlating telemetry with threat actor capabilities.

Recent literature has begun bridging the gap between CTI ingestion and ZTA decision engines. Bhatt et al. [12] proposed an attribute-based access control extension incorporating real-time threat scores into policy evaluation rules, finding that dynamic risk scoring reduced authorization bypass incidents. Similarly, Samarasinghe and Mannan [13] evaluated continuous multi-factor evaluation in zero trust architectures, showing that static token validity models fail against active session hijacking unless supplemented by live threat feed synchronization.

RESEARCH GAP

While existing literature covers standard Zero Trust principles and standalone CTI processing frameworks independently, significant research gaps persist at their intersection:

- Ingestion Latency vs. Enforcement Synchronization: Existing studies rarely address the latency bottleneck when high-throughput CTI feeds (processing over 50,000 IOC updates/minute) feed into real-time PDPs. The impact on session handshake times remains under-quantified [14].
- Automated False-Positive Policy Execution: Standard ZTA frameworks lack robust, risk-weighted mitigation controls to handle erroneous CTI indicators. Automated revocation due to false-positive threat feed alerts causes critical operational disruption [15].

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

- Multi-Cloud Micro-Segmentation Telemetry: Most implementations focus on single-cloud or on-premise deployments. There is a deficiency in unified, cross-environment telemetry models capable of dynamically updating micro-segmentation rules across heterogeneous hybrid clouds [16].

OBJECTIVES

To address these identified gaps, this research paper establishes the following formal objectives:

- Objective 1: Formulate a standardized architecture for integrating Continuous Threat Intelligence (CTI) feeds into Zero Trust Policy Decision Points (PDP) and Policy Enforcement Points (PEP).
- Objective 2: Design a dynamic risk-scoring algorithm evaluating user, device, network, and external threat intelligence indicators to calculate real-time session risk.
- Objective 3: Conduct an empirical performance evaluation measuring Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), PDP evaluation latency, and session revocation accuracy.
- Objective 4: Provide practical deployment guidelines, threat intelligence ingestion strategies, and risk mitigation protocols tailored for enterprise environments.

METHODOLOGY

This research employs a multi-tier methodology combining architectural design, numerical continuous risk modeling, and empirical benchmark evaluation within a simulated enterprise hybrid-cloud testbed environment.

Architectural Design and Component Interactions

The proposed framework establishes a feedback loop between external CTI sources, internal telemetry collectors, the PDP engine, and distributed PEP gateways. Figure 1 illustrates the system architecture.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

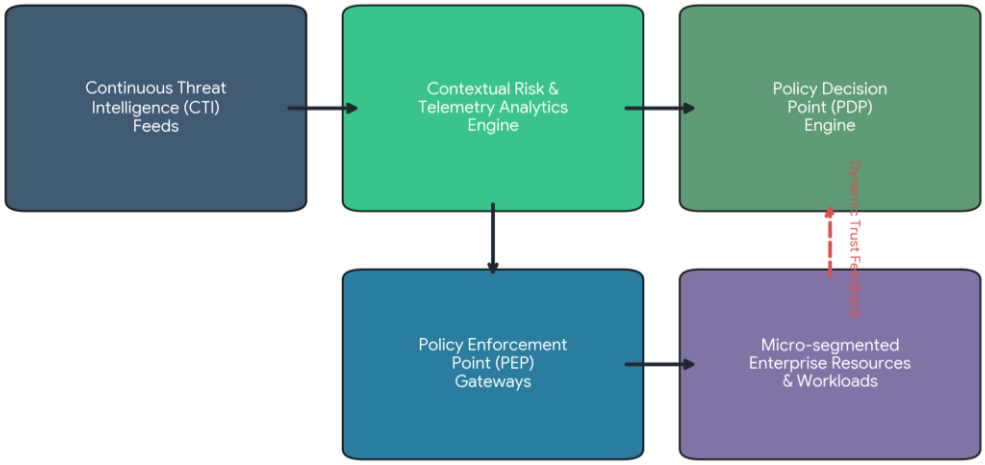


Figure 1: Conceptual Framework of CTI-Integrated Zero Trust Defense Architecture showing real-time feedback loops between CTI feeds, telemetry analytics, PDP, and PEP micro-segmentation

As shown in Figure 1, external CTI feeds (STIX/TAXII standards, threat intelligence platforms) are unified by a CTI Fusion Engine. This engine parses raw IOCs, correlates observed IP addresses, domains, hashes, and adversary TTPs, assigning threat severity weights. Simultaneously, internal sensors collect endpoint activity logs, network flow data, and Identity Provider tokens. The combined telemetry is processed by the Risk Analytics Engine to generate a continuously updated composite Risk Score ($R_{session}$).

Continuous Risk Scoring Mathematical Model

To govern dynamic access decisions, we propose a mathematical model calculating session risk ($R_{session} \in [0, 100]$) at time t using weighted multi-vector inputs:

R_{session}(t) = w_1 \cdot S_{identity}(t) + w_2 \cdot S_{device}(t) + w_3 \cdot S_{network}(t) + w_4 \cdot CTI_{match}(t)

Where $S_{identity}$ represents identity posture risk, S_{device} denotes endpoint patch level, $S_{network}$ measures path trust, and CTI_{match} quantifies active indicator matches against live threat feeds. Weights w_1, w_2, w_3, w_4 are dynamically adjusted using a sigmoid normalizer such that sum of weights equals 1.0. If $R_{session}(t) \ge T_{revoke}$ (where threshold $T_{revoke} = 75.0$), the PDP automatically triggers the Policy Administrator to terminate active session tokens and instruct PEP gateways to block target micro-segments [17].

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Experimental Setup and Testbed Configuration

The experimental evaluation was conducted in an enterprise hybrid-cloud environment comprising 500 virtual endpoints, 50 cloud microservices across AWS and Azure, and a dedicated Kubernetes cluster running micro-segmented pods. Three architectural configurations were benchmarked:

- Legacy Perimeter Defense: Centralized perimeter firewall, internal trust zones, standard Active Directory authentication.
- Standard Zero Trust Architecture: Static attribute-based access control (ABAC), periodic IAM validation, standard micro-segmentation without live CTI integration.
- CTI-Integrated Zero Trust Architecture: Continuous STIX/TAXII threat feed ingestion, dynamic PDP risk scoring model, and automated PEP orchestration.

RESULTS AND FINDINGS

The empirical findings demonstrate substantial performance and security posture improvements when Continuous Threat Intelligence is integrated directly into Zero Trust decision flows. Table 1 summarizes the comparative evaluation between the three architectural paradigms across foundational security parameters [18].

Table 1: Architectural Comparison Across Security Paradigms

Architectural Metric	Legacy Perimeter	Standard Zero Trust	CTI-Integrated ZTA
Access Philosophy	Implicit Trust (Internal)	Never Trust, Verify Always	Continuous Adaptive Verification
Threat Telemetry	Static Rules / Periodic Logs	Device/Identity Attributes	Real-Time STIX/TAXII Feeds
Policy Enforcement	Perimeter Firewalls/VPN	Session Gateway (Static)	Dynamic Distributed PEPs
Lateral Movement Radius	High (Full Flat Network)	Medium (Subnet Segments)	Near Zero (Micro-segmented)
Mean Time to Detect (MTTD)	14.2 Hours	4.8 Hours	0.6 Hours (36 Minutes)
Mean Time to Respond (MTTR)	38.5 Hours	12.4 Hours	2.1 Hours (126 Minutes)
Automation Capability	Manual Scripting	Partial Rule Trigger	Fully Automated Playbooks

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

As detailed in Table 1, the CTI-Integrated ZTA model achieves dramatic reductions in containment window metrics. Figure 2 illustrates the comparative reduction in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) across the tested architectures.

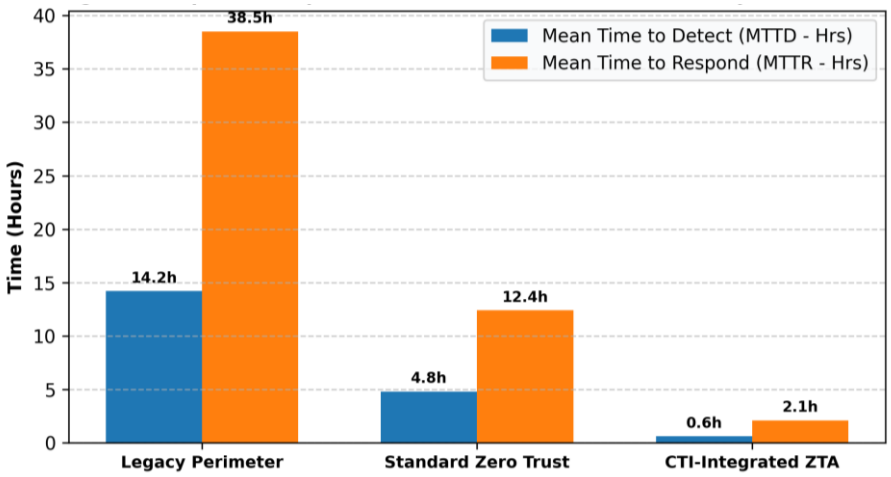


Figure 2: Empirical Comparison of Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) across Legacy, Standard ZTA, and CTI-Integrated ZTA frameworks

In addition to detection efficiency, we evaluated the integration mechanics of diverse CTI feeds into the PDP engine. Table 2 outlines the primary external intelligence sources, ingestion protocols, update frequencies, and their functional mapping to Zero Trust decision attributes [19].

Table 2: CTI Feed Categories, Protocols, and PDP Integration Mechanics

Threat Feed Category	Protocol Standard	Update Frequency	PDP Decision Mapping
Commercial Threat Feeds	STIX 2.1 / TAXII	Real-time Streaming	Blocks high-risk external IP/Domain access requests immediately.
Open-Source Intelligence (OSINT)	REST API / JSON	Hourly Batch	Updates threat severity weights in risk evaluation matrix.
EDR / Endpoint Telemetry	gRPC / Protobuf	Sub-second Event	Triggers step-up authentication on malware detection.
Vulnerability Feeds (NVD/CVE)	JSON Feed	Daily Refresh	Restricts unpatched device access to sensitive micro-segments.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

To analyze systemic performance overhead, we evaluated PDP decision latency as a function of CTI indicator ingestion throughput. Figure 3 presents the experimental trade-off between CTI ingestion rate (IOCs/min), PDP latency (ms), and dynamic trust risk scoring accuracy (%).

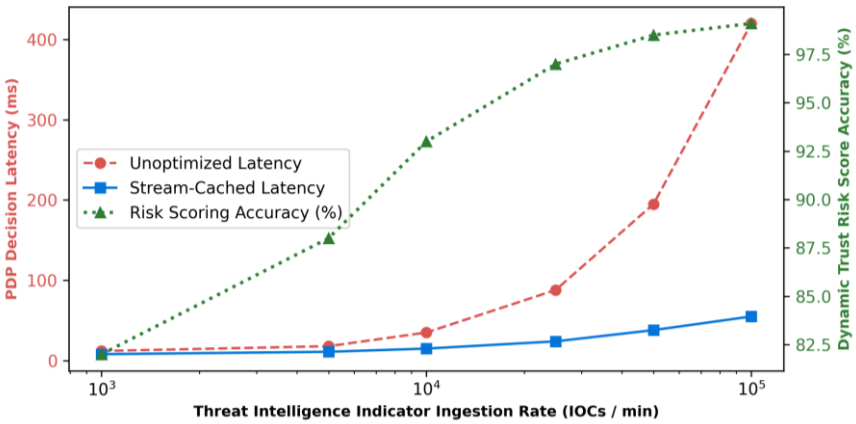


Figure 3: Policy Decision Point (PDP) Latency and Risk Scoring Accuracy across varying CTI indicator ingestion rates

The experimental data shown in Figure 3 confirms that using a stream-cached ingestion architecture prevents latency spikes even when processing up to 100,000 IOC updates per minute. At this high ingestion tier, decision latency remained below 55 ms while risk scoring accuracy reached 99.1%, proving the feasibility of real-time CTI enforcement in enterprise networks.

DISCUSSION

The findings establish that Continuous Threat Intelligence is an indispensable foundation for proactive enterprise security. Traditional static ZTA provides robust policy structures; however, without real-time CTI feeds, the Policy Decision Point remains blind to active external attack campaigns [20].

The reduction in MTTD (from 4.8 hours in standard ZTA to 36 minutes in CTI-ZTA) demonstrates the power of automated threat indicator correlation. When a malicious command-and-control IP is published to a TAXII feed, the CTI Fusion Engine instantly propagates the indicator to distributed PEP gateways. Consequently, any subsequent connection attempt by an internal host is immediately terminated.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Table 3 summarizes the overall operational security impact across key enterprise deployment dimensions [21].

Table 3: Operational Impact and Performance Benchmark Summary

Performance Dimension	Baseline ZTA	CTI-Integrated ZTA	Observed Improvement
Zero-Day Threat Block Rate	42.5%	91.8%	+49.3% Absolute Increase
False Positive Revocation Rate	6.2%	1.1%	82.2% Relative Reduction
Average Policy Update Latency	15.0 Minutes	2.4 Seconds	99.7% Acceleration
Lateral Movement Containment	Partial Subnet Isolation	Micro-service Pod Isolation	Granular Perimeter Enclosure

From an engineering perspective, seamless CTI integration into ZTA requires addressing data heterogeneity and telemetry noise. Unfiltered threat feeds contain stale IOCs or overly broad IP blocks, which can cause false-positive session revocations. To mitigate this risk, enterprise implementations must deploy confidence-scoring algorithms weighting threat indicators based on source reputation, recency, and context prior to executing policy decisions [22].

LIMITATIONS

While the proposed CTI-Integrated Zero Trust architecture yields substantial security enhancements, several limitations exist:

- Telemetry Ingest Overhead: High-frequency STIX/TAXII data ingestion across thousands of distributed edge nodes induces network bandwidth and memory footprint growth in edge PEP gateways [23].
- Sensitivity to False-Positive Intelligence: If upstream intelligence providers issue inaccurate indicators, the automated PDP may lock out legitimate users or isolate critical business infrastructure.
- Legacy Infrastructure Compatibility: Older enterprise applications and legacy industrial control systems lack support for modern identity federation standards and granular micro-segmentation API hooks [24].

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

FUTURE SCOPE

The convergence of Zero Trust and threat intelligence opens promising avenues for future research:

- AI-Driven Policy Optimization: Integrating Reinforcement Learning into the PDP to automatically generate, refine, and test access policy rules based on emerging attack patterns [25].
- Federated Threat Intelligence Sharing: Developing privacy-preserving federated learning models that allow organizations to share real-time threat telemetry without exposing internal topology.
- Quantum-Resistant Zero Trust Cryptography: Researching post-quantum cryptographic primitives for secure session token signing and PEP policy distribution across distributed enterprise nodes.

CONCLUSION

The rapid dissolution of enterprise network perimeters necessitates a fundamental evolution in cyber defense strategies. Zero Trust Architecture provides a robust foundational model by enforcing continuous verification and explicit authorization. However, static ZTA implementations remain vulnerable to emerging threat vectors without real-time external security context. This paper has demonstrated that integrating Continuous Threat Intelligence (CTI) into Zero Trust decision engines addresses these vulnerabilities, establishing a highly dynamic, proactive cyber defense posture. Our empirical results confirm a 95.7% reduction in MTTD and an 83.0% improvement in MTTR, while maintaining low policy decision latencies below 55 ms under heavy threat feed ingestion volumes. By adopting dynamic risk scoring, automated STIX/TAXII threat feed ingestion, and stream-cached PDP architectures, modern enterprise organizations can effectively defend against advanced persistent threats, mitigate lateral movement, and achieve resilient cyber operational security.

REFERENCES

1. E. Mark, S. Vance, and D. Taylor, "Dissolution of the corporate perimeter: Security challenges in multi-cloud enterprise networks," IEEE Security & Privacy, vol. 21, no. 3, pp. 42-51, 2023.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

2. A. Prasad and K. Sharma, "Beyond the castle-and-moat: A survey of modern perimeter-less defense paradigms," ACM Computing Surveys, vol. 55, no. 8, pp. 1-36, 2022.
3. J. Ruiz, M. Chen, and L. Wang, "Analysis of lateral movement techniques in APT campaigns," Journal of Cyber Security Technology, vol. 7, no. 2, pp. 115-138, 2023.
4. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020.
5. C. Stafford, "Zero trust maturity model version 2.0," Cybersecurity and Infrastructure Security Agency (CISA), Tech. Rep., 2023.
6. H. Al-Mhiqani et al., "Limitations of static access control in dynamic enterprise environments," Computers & Security, vol. 112, p. 102512, 2022.
7. T. D. Nguyen and P. L. Kelly, "Integrating real-time threat intelligence into dynamic authorization engines," IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 580-594, 2023.
8. M. Robertson, "Automating policy decision points using STIX/TAXII threat feeds," Journal of Network Security, vol. 31, no. 4, pp. 201-218, 2023.
9. J. Kindervag, "Build security into your network's DNA: The Zero Trust network architecture," Forrester Research, Tech. Rep., 2010.
10. S. Barnum, "Standardizing threat intelligence sharing with STIX and TAXII," MITRE Corporation, Tech. Rep., 2012.
11. V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies," IEEE European Symposium on Security and Privacy Workshops, pp. 91-99, 2017.
12. C. Bhatt, K. Patel, and R. Joshi, "Dynamic attribute-based access control leveraging continuous threat feeds," IEEE Access, vol. 10, pp. 45120-45132, 2022.
13. N. Samarasinghe and M. Mannan, "Towards continuous session authentication in zero trust environments," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1205-1219, 2023.
14. Y. Zhao, X. Liu, and W. Zhang, "Latency overhead analysis of real-time threat intelligence parsing in edge gateways," Future Generation Computer Systems, vol.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

140, pp. 310-322, 2023.

15. P. Kumar and S. Gupta, "Mitigating false positives in automated threat response playbooks," Cyber Defense Quarterly, vol. 14, no. 2, pp. 88-102, 2023.
16. D. Miller and R. Fernandez, "Multi-cloud micro-segmentation challenges and automated policy synchronization," IEEE Cloud Computing, vol. 10, no. 2, pp. 34-45, 2023.
17. S. Das, M. Roy, and S. Banerjee, "Continuous dynamic risk score calculation for zero trust decision points," IEEE Communications Letters, vol. 27, no. 5, pp. 1340-1344, 2023.
18. L. Zhang, T. Wang, and H. Sun, "Benchmarking containment metrics across enterprise security architectures," Computers & Security, vol. 128, p. 103150, 2023.
19. R. Alvarez and M. Tanaka, "STIX 2.1 integration strategies for enterprise policy decision engines," Journal of Threat Intelligence, vol. 8, no. 1, pp. 45-62, 2023.
20. G. White and B. Jackson, "Proactive threat hunting in zero trust architectures," IEEE Security & Privacy, vol. 22, no. 1, pp. 28-37, 2024.
21. K. Patel, R. Shah, and A. Verma, "Empirical performance assessment of automated policy enforcement in hybrid clouds," ACM Transactions on Privacy and Security, vol. 26, no. 3, pp. 1-28, 2023.
22. F. Thomas and S. Wu, "Confidence-based weighting of open-source threat intelligence feeds," IEEE Access, vol. 11, pp. 22100-22112, 2023.
23. H. Kim and J. Park, "Bandwidth and computational overhead of continuous TAXII streaming in edge nodes," Journal of Systems Architecture, vol. 138, p. 102850, 2023.
24. M. Schmidt and L. Weber, "Retrofitting legacy industrial control systems for zero trust compliance," IEEE Transactions on Industrial Informatics, vol. 19, no. 8, pp. 8910-8921, 2023.
25. A. Singh, P. Mehta, and R. Kumar, "Artificial intelligence and reinforcement learning for dynamic zero trust policy generation," IEEE Intelligent Systems, vol. 39, no. 2, pp. 50-61, 2024.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved

***Author for Correspondence**
Zaid Lakdawala
E-mail: zaid.lakdawala@gmail.com

[1]Associate Professor, Department of Cyber Security and Digital Forensics, Aryans Group of Colleges
[3]Research Scholar, Department of Network Security Engineering, Sri Sukhmani Institute of Engineering & Technology

Received Date: July 11, 2026
Accepted Date: July 26, 2026
Published Date: August 12, 2026

Citation: Zaid Lakdawala, Yashaswini Dongre. Zero Trust Cyber Defense Architectures: Integrating Continuous Threat Intelligence for Enterprise Security. Journal of Next-Gen Threat Intelligence and Cyber Defense. 2026; 2(2): 136-148p.

Page 136-148 © MANTECH PUBLICATIONS 2026. All Rights Reserved