scientific reports

OPEN

ZenGuard a machine learning based zero trust framework for context aware threat mitigation using SIEM SOAR and UEBA

Aamina Hassan[1]✉, Abdul Rauf[1], Narmeen Shafqat[1], Rabia Latif[2] & Hasib Khan[3]

Perimeter-based security models, which rely on predefined network boundaries, are increasingly ineffective against modern threats such as insider misuse, supply chain attacks, and Advanced Persistent Threats (APTs). Zero Trust Architecture (ZTA) offers a more resilient approach by enforcing continuous verification of users, devices, and activity. While SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platforms are widely adopted and play a critical role in monitoring and response, they often operate with static rules and limited behavioral context, making it challenging to fully implement ZTA principles. ZenGuard addresses these operational gaps by introducing context-aware, real-time, and adaptive enforcement capabilities. This paper introduces ZenGuard, an open-source framework that integrates ZTA, SIEM, SOAR, and User and Entity Behavior Analytics (UEBA) into a unified, vendor-independent platform. ZenGuard employs Python-based automation and interpretable machine learning models to detect behavioral anomalies and trigger adaptive responses across identity, device, and network layers. We evaluate ZenGuard using real-world Security Operation Center (SOC) telemetry from enterprise environments to validate overall threat detection and response, demonstrating a Mean Time to Respond (MTTR) under 10 seconds in cases such as privilege escalation, lateral movement and data exfiltration. Furthermore, UEBA accuracy was assessed on synthetic behavioral datasets that emulate diverse threats that are not consistently observable in live environments. In essence, ZenGuard supports Zero Trust principles as defined by NIST SP 800-207 and ISO/IEC 27001 controls, offering a practical, explainable, and scalable approach to modern cybersecurity automation.

Keywords Zero Trust Architecture, SIEM, UEBA, SOAR, MFA, Threat Detection, Incident Response, Python Automation

Organizations today face an increasingly complex threat landscape. Employees work remotely, devices connect from untrusted networks, and systems span hybrid cloud, third-party vendors, and on-premise environments. In such dynamic settings, attackers have more opportunities than ever to infiltrate systems through phishing, supply chain compromise, or malicious insiders—and move undetected across networks.

Historically, enterprises relied on *perimeter-based security models*, where everything inside the network was trusted and threats were expected to come from the outside. Firewalls, Virtual Private Networks (VPNs), and access controls focused on securing the *edges* of the organization. But this model is no longer sufficient. Once an attacker breaches the perimeter, they can move laterally, escalate privileges, and exfiltrate data with little resistance. High-profile attacks, such as the SolarWinds supply chain compromise and insider-driven data leaks have exposed the limits of this trust-based perimeter defense[1–3].

To respond, security architects are embracing a more robust model known as ZTA. Rather than assuming trust based on location or credentials, ZTA enforces the principle of "never trust, always verify." It continuously validates the identity, behavior, and device posture of every user or system before granting or maintaining access. This model, formalized by standards such as NIST SP 800-207[4,5], is gaining momentum as a foundation for resilient enterprise security.

[1]National University of Sciences and Technology, Islamabad, Pakistan. [2]College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh 11586, Saudi Arabia. [3]Department of Mathematics and Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia. ✉email: aamina.phdis@students.mcs.edu.pk

However, moving to Zero Trust is not just a policy shift, it requires deep operational support. Enterprises need real-time visibility into user behavior, dynamic risk assessment, and automated response capabilities. This is where tools like SIEM and SOAR come in. SIEM aggregates logs and alerts across systems[1,6], while SOAR enables automated workflows for responding to threats. When combined with UEBA, which detects anomalies based on learned behavioral patterns, these tools can support a more intelligent, proactive security model[7].

Despite this promise, existing platforms face several key shortcomings. Many SIEM and SOAR systems rely heavily on static rules and correlation logic, struggle with alert fatigue, and depend on manual intervention from the analyst[8,9]. Static playbooks in SIEM-SOAR systems have shown only limited effectiveness in reducing MTTR[10,11]. Integrating Zero Trust principles into these platforms is often difficult due to fragmented architectures, rigid playbooks, and lack of behavioral context[12–14]. Machine learning has been proposed to improve detection and prioritization[15], but many implementations remain black-box, rule-driven, or vendor-locked, making them hard to scale or audit in real-time environments[10,16,17].

To address these limitations, this paper introduces *ZenGuard*, an open-source framework that unifies ZTA, SIEM, SOAR, and UEBA into a single, automated, vendor-independent platform. ZenGuard enhances detection and response by dynamically adapting to context-aware threats and operating across the user, device, and network layers. Unlike traditional static rules, ZenGuard's Python-based playbooks offer real-time responses triggered by interpretable risk assessments. Basically, ZenGuard uses machine learning models such as Isolation Forests and One-Class Support Vector Machines (SVMs) to detect deviations from normal behavior. Its explainable architecture allows SOC analysts to trace the rationale behind alerts and automate actions such as access revocation, Multi-Factor Authentication (MFA) enforcement, or device quarantine. The API-first design supports integration with both open-source and commercial security tools, avoiding vendor lock-in and supporting flexible deployments across hybrid environments.

We evaluated ZenGuard in enterprise SOC environments using real-world security telemetry to measure detection and response capabilities across scenarios such as lateral movement, privilege escalation, and data exfiltration. The MTTR values reported in Table 3 were obtained entirely from live SOC operations, with integration into production SIEM–SOAR workflows. Synthetic behavioral datasets were used exclusively to benchmark UEBA.

To illustrate the motivation behind this work, Fig. 1 highlights the critical gaps in traditional SIEM-SOAR pipelines and how the ZenGuard framework addresses them using UEBA-driven automation and adaptive enforcement.

This paper makes the following contributions.

- **Unified SIEM-ZTA Framework:** A complete system combining SIEM, SOAR, ZTA, and UEBA for proactive, context-driven threat detection and response, focusing on operational integration rather than introducing a novel ML algorithm.
- **Dynamic Real-Time Playbooks:** Python-based playbooks that trigger multi-step responses, such as session revocation, MFA enforcement, and device quarantine, based on risk-aware behavior analysis. These actions collectively reduce MTTR to under 10 seconds.
- **Vendor-Neutral, Open API-first Architecture:** ZenGuard supports integration with open-source and commercial tools, such as firewalls, VPNs, and Endpoint Detection and Response (EDR) systems, enabling flexible deployment without vendor lock-in.

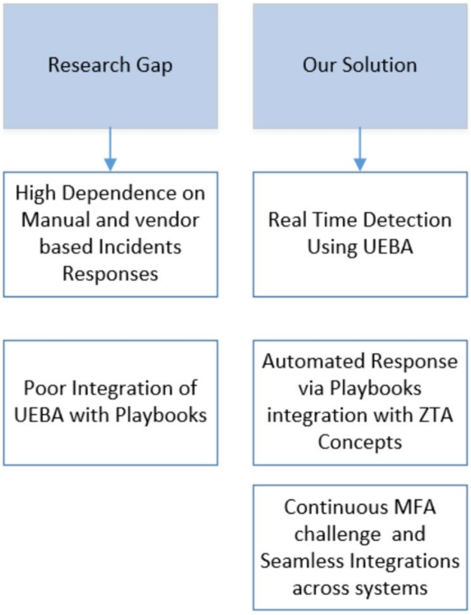

Research Gap
Our Solution
High Dependence on Manual and vendor based Incidents Responses
Real Time Detection Using UEBA
Poor Integration of UEBA with Playbooks
Automated Response via Playbooks integration with ZTA Concepts
Continuous MFA challenge and Seamless Integrations across systems

Fig. 1. Identified Gaps and Proposed Framework.

- **Layered Behavioral Enforcement:** The system enforces Zero Trust across users, devices, and networks using session-based validation, device posture checks, and behavioral risk scoring.
- **Operationally Validated Anomaly Detection:** While the core anomaly detection leverages a standard Isolation Forest model for real-time SOC deployment, we conducted comparative experiments with AutoEncoder and LSTM-based detectors. Isolation Forest offered superior runtime efficiency critical for automation, whereas LSTM provided improved temporal correlation—suggesting a hybrid approach for future work.

ZenGuard offers a cost-effective, scalable, and explainable solution for cybersecurity automation. By unifying ZTA enforcement with real-time SIEM-SOAR capabilities, it addresses critical gaps in existing systems. In addition, ZenGuard aligns with NIST SP 800-207 and ISO/IEC 27001 control objectives. It is pertinent to note that all data used was ethically collected from operational SOC environments or safely synthesized, and the dataset is available upon request to encourage reproducibility and further community research.

Background and literature review

This section introduces the core security paradigms that underpin ZenGuard and identifies the gaps within the existing literature that motivate its development.

Key concepts

ZTA

ZTA is a security model that assumes no implicit trust, whether internal or external perspective. Access is granted only after continuous identity validation, contextual policy enforcement, and risk-based decision-making. ZTA emphasises on micro-segmentation, least-privilege access, and session-level monitoring[18]. Unlike perimeter-based models, which assume internal network zones are inherently trustworthy, ZTA minimizes lateral movement, thereby enhancing real-time access control.

IdPs

MFA strengthens authentication by requiring users to validate their identity using multiple factors (e.g., passwords, tokens, biometrics). IdPs such as Azure AD, Okta or Keycloak manage these workflows and can enforce contextual controls. Modern IdPs support session intelligence, anomaly detection (e.g., location or device anomalies), and dynamic re-authentication[19], making them essential components of a Zero Trust strategy.

SIEM

SIEM platforms collect, normalize, and correlate log data from sources such as firewalls, VPNs, endpoints, cloud APIs and more. They support real-time threat detection through correlation rules and ML-based anomaly detection. However, traditional SIEMs are alert-centric and do not perform real-time enforcement[20,21].

SOAR

SOAR platforms automate incident response by executing pre-defined playbooks that interface with tools, such as firewalls, endpoints, and IT Service Management (ITSM) platforms. These systems reduce incident response time and analyst fatigue by automating repetitive workflows such as IP blocking or user lockdown. However, most playbooks are static and lack the ability to adapt to dynamic risk contexts or incorporate behavioral signals[22,23].

UEBA

UEBA models establish behavioral baselines for users and devices by analyzing access patterns, login times, geolocation, and file interactions. Deviations from baseline behavior trigger dynamic risk scores, which can inform SOAR responses and ZTA policy enforcement[24,25]. Recently, explainable models such as Isolation Forest and cluster-based algorithms are increasingly being adopted to improve trust and interoperability.

EDR

EDR continuously monitors endpoints for malicious behaviors, policy violations, and malware signatures. They provide real-time visibility into processes, memory usage, file changes, and network calls. When anomalies are detected, actions such as isolation or rollback can be automated or passed to SOAR platforms for orchestration. EDR plays a pivotal role in limiting post-compromise movement and enforcing Zero Trust at the device layer[26].

Related work

Zero trust implementations

NIST's Zero Trust architecture guidelines[18] provide a vendor-agnostic baseline for modern implementations. Several commercial solutions offer ZTA implementation[27,28] but most systems rely on static policies and are vendor-locked, limiting flexibility and scalability. Prior academic work has proposed identity-aware access models for hybrid cloud environments[29], but often lacks continuous re-validation and session intelligence, leaving gaps in enforcement against session hijacking or insider misuse.

SIEM enhancements

Recent advances in SIEM research include the use of machine learning for anomaly detection, insider threat identification, and visualization[20,24]. Deep learning and clustering algorithms have been used to improve detection of zero-day threats. Nonetheless, traditional SIEMs remain passive; they alert but rarely act, requiring manual triage and intervention.

Numerous commercial SIEM and SOAR platforms, including Splunk Enterprise Security, IBM QRadar, Microsoft Sentinel, and Cortex XSOAR, incorporate Zero Trust principles through integrations with Identity

Providers (IdPs), micro-segmentation technologies, and UEBA modules, demonstrating proven reliability in large-scale deployments. However, in most enterprise scenarios, Zero Trust capabilities are distributed across multiple licensed modules, requiring substantial configuration, proprietary connectors, and vendor-specific workflows. For instance, Splunk Enterprise Security typically enforces Zero Trust through premium add-ons such as Phantom; IBM QRadar relies on companion products like QRadar SOAR or IBM Security Verify; Microsoft Sentinel delivers risk-based access primarily within the Defender ecosystem; and Cortex XSOAR, despite its automation breadth, continues to depend on static playbooks and separate integrations for adaptive Zero Trust enforcement. In contrast, the proposed *ZenGuard* framework consolidates detection, orchestration, and enforcement into a single vendor-neutral, API-first architecture that unifies SIEM, SOAR, and UEBA capabilities. By leveraging open APIs, ZenGuard coordinates real-time actions across heterogeneous systems without reliance on proprietary connectors, offering dynamic, context-aware policy enforcement as an inherent feature rather than an add-on.

Disclaimer: The mention of commercial platforms in this section is solely for contextual and comparative purposes within an academic research framework. No endorsement or criticism is implied, and the intent is to position *ZenGuard* as a complementary, open-source research solution designed to integrate with, rather than compete against, existing proprietary offerings.

Integration with Zero Trust for access control enforcement is also rare. In the context of critical infrastructure monitoring, Fausto et al.[30] demonstrated the integration of physical security logs (e.g., access control) with cyber telemetry (e.g., VPN, SCADA events) into a unified anomaly detection pipeline, leveraging unsupervised methods such as LOF and Isolation Forest. Other studies, including[31], have expanded SIEM capabilities through enhanced correlation logic, feature engineering, and visualization to improve situational awareness. These works illustrate the maturity and diversity of current SIEM research and commercial offerings. However, they remain focused on detection and alert generation within their operational domains and do not enforce adaptive access control or orchestrate automated, context-aware mitigations in real time.

SOAR automation

SOAR platforms automate incident response using logic-based playbooks, typically employing IFTTT (If This Then That) style rules and integration with ITSM systems (e.g., ServiceNow). Studies demonstrate their efficacy in automating triage and reducing MTTR[23,32]. However, playbooks are often static and vendor-bound, with limited ability to adapt to new threat patterns or risk contexts. Vendor lock-in and lack of API-level flexibility also hinder integration in heterogeneous environments.

UEBA and behavioral analytics

Recent work emphasizes the use of explainable AI to enhance trust in UEBA outputs. While some models offer transparency, most commercial platforms are black boxes with little interpretability for SOC analysts[25]. Recent research indicates a shift towards interpretable, unsupervised models like Isolation Forest and Random Cut Forest due to their adaptability and operational simplicity in UEBA systems[33,34].

To consolidate the insights from prior research and clearly identify systemic gaps across domains, Table 1 summarizes existing approaches and their limitations in ZTA, SIEM, SOAR, UEBA, and related domains. Despite the advancements in each area, existing solutions remain siloed, reactive, and heavily reliant on vendor ecosystems. Key limitations include static configurations, limited risk-awareness, delayed responses, and opaque analytics. These gaps necessitate a dynamic, vendor-neutral security model that blends explainability, real-time orchestration, and Zero Trust enforcement. The proposed *ZenGuard* framework addresses these issues through unified, explainable, and automated Zero Trust enforcement that adapts to evolving threats across user, device, and network layers.

ZenGuard framework

This section introduces the architecture and operational design of the proposed ZenGuard framework. The ZenGuard Framework is designed to address critical gaps in traditional cybersecurity approaches through a cost-efficient, vendor-independent, and highly adaptive Zero Trust model. By leveraging open-source tools, Python-driven automation, and dynamic enforcement of risk, it establishes a robust mechanism for log aggregation, behavior analytics, and real-time policy enforcement.

Research Area	Existing Approach	Gaps/Limitations
Zero Trust	Static MFA, session-based trust[18,27]	No continuous verification; micro-segmentation is vendor-locked.
SIEM	Event correlation, alert generation[20]	No real-time enforcement; requires manual analyst intervention.
SOAR	Static playbooks, IFTTT logic[22]	No risk-adaptive workflows; limited context integration.
UEBA	Proprietary black-box scoring[25]	Limited explainability and transparency in risk scoring.
Incident Response	Manual or semi-automated[21]	Delayed MTTR; response depends on analyst bandwidth.
Micro-segmentation	Proprietary NAC and SDN-based tools[28]	High cost; lack of API-level openness and interoperability.

Table 1. Summary of Research Areas, Existing Approaches, and Gaps.

Core principles and features

The ZenGuard Framework is grounded in core principles that enhance security, scalability, and efficiency. These principles ensure a proactive, resilient defense mechanism while addressing traditional cybersecurity shortcomings.

Continuous validation

ZenGuard ensures constant revalidation of user identity, device compliance, and behavioral patterns throughout their lifecycle. It employs adaptive MFA, endpoint health validation, and UEBA to protect against threats such as insider attacks, session hijacking, and privilege escalation. Continuous validation significantly mitigates persistent risks within the network.

Adaptive and risk-aware response

The framework dynamically tailors responses based on threat severity and contextual risk. For example, abnormal login patterns prompt MFA challenges, while suspicious data exfiltration triggers endpoint isolation. Python-driven playbooks within the SOAR engine ensure real-time, context-specific responses, reducing the MTTR to under 15 seconds.

Scalability and transparency

By leveraging open-source tools and Python-driven automation, the architecture ensures cost-efficiency, avoids vendor lock-in, and scales seamlessly to manage over a million events per hour. Behavioral anomaly detection models offer explainable outcomes, ensuring root cause analysis and alignment with organizational security policies.

Real-time micro-segmentation and cost efficiency

Dynamic micro-segmentation isolates high-risk devices and compromised users, reducing the attack surface. Integration with network segmentation tools and EDR systems limits lateral movement during intrusions. Cost efficiency is achieved through the use of open standards, APIs, and automation, making the framework accessible to organizations of all sizes.

Use cases observed in the proof of concept

The Proof of Concept demonstrates the ability of the Zero Trust framework to address the gaps in SIEM, SOAR, and UEBA as shown in Fig. 1 through real-world scenarios, highlighting its effectiveness in detection, mitigation and response. In the case of *user misuse*, SIEM detects insider privilege abuse and triggers identity re-verification along with Role-Based Access Control (RBAC) enforcement. For volumetric attacks such as *Smurf Floods*, ICMP traffic floods are detected and contained through adaptive MFA and dynamic firewall rules within 65 seconds. Similarly, a *PUSH-ACK Flood* is flagged as abnormal TCP traffic, with endpoint detection isolating compromised hosts and SOAR executing responses in 9 seconds. In the event of a *SYN Flood*, Zero Trust policies automatically isolate malicious source IPs in just 4 seconds. For *session hijacking*, UEBA identifies anomalous session behavior, enforces MFA re-authentication, and terminates the session upon failure. *Data exfiltration attempts* are mitigated by UEBA's ability to detect unusual file transfers, which leads to automatic quarantine of high-risk endpoints. During *lateral movement*, SIEM correlates suspicious endpoint interactions and micro-segmentation policies contain the spread within 9 seconds. Against large-scale *DDoS traffic*, SIEM recognizes volumetric anomalies and SOAR leverages Python-driven playbooks to block malicious IPs within 6 seconds. Finally, *behavioral anomalies* such as unusual login times or locations are identified by UEBA, prompting SOAR to enforce MFA challenges and apply access restrictions within 15 seconds. Collectively, these use cases illustrate ZenGuard's ability to provide rapid detection, precise risk scoring, and automated response across diverse threat scenarios.

Threat mitigation lifecycle

ZenGuard disrupts the Cyber Kill Chain by enforcing Zero Trust controls at each critical stage of an attack. During *Initial Access*, continuous identity verification and adaptive multi-factor authentication (MFA) prevent unauthorized entry. In cases of *Privilege Escalation*, any role change immediately triggers real-time identity checks and strict access controls. When adversaries attempt *Lateral Movement*, abnormal endpoint communications activate micro-segmentation and device isolation to contain the spread. Finally, potential *Data Exfiltration* is mitigated by detecting anomalous file transfers, which result in session termination and automatic endpoint quarantine. Together, these layered defenses ensure proactive disruption of adversary actions across the entire attack lifecycle.

Table 2 presents a comparative view of commonly used UEBA techniques. ZenGuard's choice of Isolation Forest balances explainability and detection accuracy while maintaining rapid response times.

Experimental architecture

A modular architecture simulates Zero Trust scenarios as shown in Fig. 2. Components include SIEM, SOAR, EDR, UEBA, IDS, firewalls, and threat feeds. Python automation ensures rapid, policy-driven responses.

The ZenGuard framework integrates multiple coordinated components, each serving a distinct role in enforcing Zero Trust security. Within the end-user LAN environment, EDR tools ensure device compliance, while an Identity Provider (IdP) such as Azure AD, coupled with MFA, secures authentication workflows. Internal and external firewalls mitigate threats such as Smurf and SYN floods and forward security logs to the SIEM for correlation. The SIEM, built on the ELK stack, aggregates and analyzes these logs to detect anomalies including failed logins and privilege misuse, triggering both SOAR workflows and UEBA-based risk scoring. The UEBA module, developed in Python, assigns behavioral risk scores and enforces session-level actions when anomalies

Model	Explainability	Adaptivity	Used in ZenGuard?
Rule-Based Baseline[35]	Low	Static	No
K-Means Clustering[36]	Medium	Moderate	Partial
AutoEncoder (NN)[37]	Low	High	No
Isolation Forest[38]	High	High	**Yes**
One-Class SVM[39]	Medium	Moderate	No
Gaussian Mixture Model[40]	Medium	Low	No
LSTM (Behavior)[41]	Low	Very High	Planned
Random Cut Forest[42]	High	High	No

Table 2. Comparison of UEBA Techniques in Cybersecurity Frameworks.

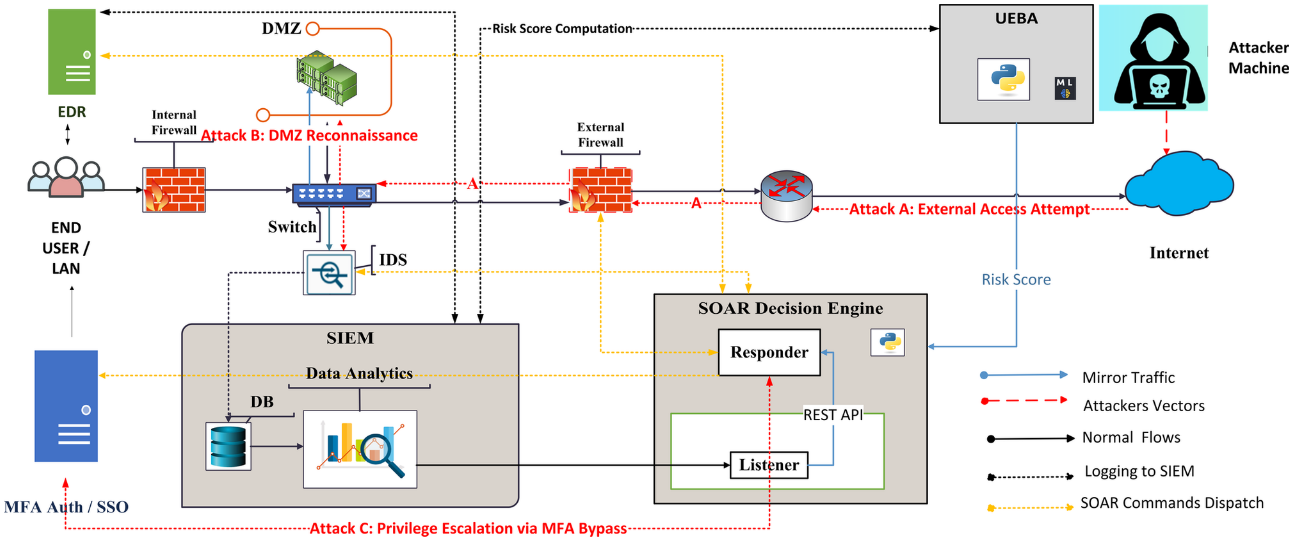


Fig. 2. ZenGuard Framework Architecture showing coordinated detection, risk scoring, and automated SOAR response. Attack paths (A, B, C) are marked with red dashed arrows.

are identified. The SOAR engine executes automated remediation steps—such as IP blocking, device isolation, and privilege revocation—through API and SSH integrations. An IDS mirrors network traffic, forwarding alerts to the SIEM for further analysis. Real-time threat intelligence feeds are integrated to enhance proactive detection capabilities. Policy Enforcement Points (PEPs), including firewalls, EDR agents, and IAM systems, apply security policies dynamically across the environment, while a demilitarized zone (DMZ) hosts public-facing services and ensures strict isolation from core network assets. Figure 2 illustrates the full ZenGuard deployment, highlighting the data flow, detection processes, risk scoring mechanisms, and automated response actions across the system's components.

Attack A (External Access Attempt) enters from the internet, probing through the external firewall. This is detected via SIEM correlation and flagged by UEBA as high-risk based on user behavior anomalies. The risk score triggers SOAR action.

Attack B (DMZ Reconnaissance) demonstrates internal probing, where mirrored traffic is analyzed by IDS and forwarded to SIEM for enrichment and adaptive detection.

Attack C (Privilege Escalation via MFA Bypass) is an insider misuse scenario where anomalous logins trigger MFA challenges and privilege blocking via SOAR.

The diagram also differentiates between various data flows and control signals within the ZenGuard framework. Normal traffic is depicted in black, while mirrored traffic captured for analysis is shown in blue. Potential attacker paths are highlighted with red dashed lines, allowing visualization of intrusion vectors. SIEM logging flows are indicated using black dotted lines, representing the continuous aggregation of security events, whereas SOAR-issued commands are shown as yellow dashed lines to emphasize automated remediation actions across the environment.

All components (SIEM, SOAR, UEBA, IDS, IdP, EDR) operate under a Python-driven Zero Trust enforcement model, enabling fast MTTR and adaptive defense. To validate these scenarios, we designed the following experimental workflow

Experimental workflow

The experimental workflow begins with traffic monitoring, where firewalls, IDS, and EDR continuously analyze network activity and forward anomalies such as SYN floods or failed login attempts to the SIEM. The SIEM serves as the central monitoring and correlation hub, aggregating logs, identifying patterns (e.g., DDoS traffic), and forwarding critical events to the Listener module. The Listener extracts relevant metadata such as source and destination IPs and timestamps before passing them to the UEBA system. Within UEBA, an Isolation Forest model implemented in `scikit-learn` detects anomalies by scoring sessions against established behavioral baselines. Depending on the assigned risk level, the SOAR platform enforces adaptive responses through Python-driven playbooks, which may include MFA enforcement via the Identity Provider, blocking malicious IP addresses, or isolating compromised endpoints. The entire workflow, illustrated in Fig. 3, integrates detection, scoring, validation, and automated response in a closed loop. Finally, a continuous improvement process refines detection rules and playbook logic over time by analyzing response logs, ensuring that ZenGuard adapts to evolving threats in real-world SOC environments.

```
Algorithm: Anomaly Detection via Isolation Forest
  • Input: training_data, current_session, threshold
  • Steps:
      – Initialize Isolation Forest (estimators=100, contamination=0.05, seed=42)
      – Train model on training_data
      – Predict anomaly_score for current_session
      – If anomaly_score < threshold: risk_score = 95
      – Else: risk_score = 50
  • Output: risk_score
```

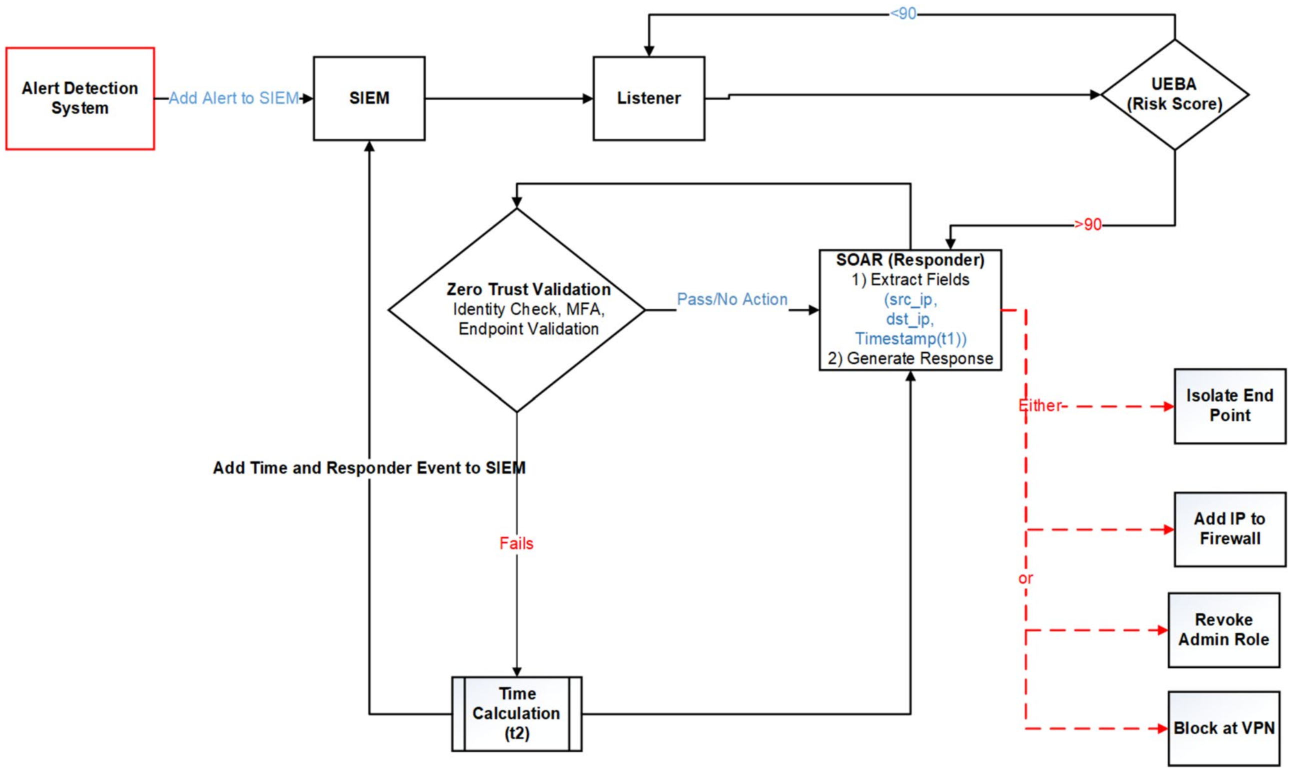


Fig. 3. Extended Working Algorithm of SIEM Listener and Responder with Zero Trust Validation Steps.

The Isolation Forest algorithm calculates an anomaly score based on how easily a data point can be isolated by random splits. Points that are easier to isolate (i.e., require fewer splits) receive lower scores and are deemed more anomalous. In our framework, we define a threshold to classify sessions: if the anomaly score is below this threshold, the session is marked as anomalous and assigned a high risk score (e.g., 95); otherwise, it is considered normal with a lower risk score (e.g., 50). These discrete scores are used to trigger Zero Trust responses such as MFA, session termination, or endpoint isolation.

The values **95** (high-risk) and **50** (low-risk) were determined empirically through extensive testing on behavioral logs. These thresholds represent statistically significant deviations from baseline behavior, as computed using the Isolation Forest model's decision function. A lower anomaly score (below the threshold) implies a higher deviation from the norm, justifying a higher risk score. We calibrated these values to minimize false negatives during malicious behavior detection while keeping false positives at an operationally acceptable level. This calibration aligns with approaches in prior UEBA research[43,44], where thresholds were set based on distributional characteristics of anomaly scores across labeled datasets.

Isolation Forest (iForest) was selected as the core anomaly detection technique in ZenGuard's UEBA module due to its balance of interpretability, efficiency, and adaptability for SOC environments. Unlike black-box models such as deep AutoEncoders or LSTMs, iForest is based on tree structures and produces interpretable anomaly scores by evaluating how easily a data point can be isolated in the feature space. Its real-time performance, with a time complexity of $\mathcal{O}(n \log n)$, enables rapid inference in high-volume environments while maintaining scalability with session data. The model's low resource footprint allows training on limited hardware without the need for GPUs, aligning with ZenGuard's emphasis on cost efficiency and open-source deployability. Additionally, its reliance on random partitioning enhances robustness to noisy behavioral data and mitigates overfitting, a common challenge in complex activity logs. Since labeled malicious sessions are rarely available in real-world operations, iForest's unsupervised learning capability makes it particularly well-suited for live SOC deployments, enabling the detection of anomalies without pre-labeling.

These characteristics make Isolation Forest an optimal choice for ZenGuard's UEBA system, balancing detection accuracy, interpretability, and deployment simplicity without the need for computationally expensive or black-box models[45,46]. Prior studies have also demonstrated its robustness and suitability for security analytics where labeled data is scarce or imbalanced[47].

This study deliberately omits ROC and F1-score benchmarking against multiple models (e.g., AutoEncoder, LSTM) due to its operational focus. The aim was not to evaluate the widest set of ML classifiers, but rather to implement a lightweight, interpretable, and real-time capable UEBA model for practical SOC deployments.

Isolation Forest (iForest) was chosen as the sole detection algorithm based on its proven advantages in unsupervised anomaly detection, including low computational overhead, scalability, and explainability. These qualities align with ZenGuard's design principles of cost-efficiency, open-source compatibility, and low-latency performance.

Benchmarking against black-box models like LSTM or deep AutoEncoders—while academically relevant—introduces complexity in interpretability and deployment overhead. As noted by Hariri et al[45]. and Haque et al[46]., black-box models pose challenges in adversarial resilience and operational interpretability, both critical for Zero Trust environments.

Future work will consider comparative evaluation once model explainability, deployment footprint, and threat surface coverage can be standardized across candidate models.

Dataset and feature extraction

We generated synthetic behavioral logs simulating enterprise user activity including login/logout events, file access, privilege usage, and network sessions. This approach ensures compliance with privacy standards such as GDPR by avoiding real personally identifiable information (PII).

Each synthetic session log was formatted with timestamp, user ID, role, device ID, login method (e.g., MFA), resource accessed, and session duration. To ensure realism, activity profiles were modeled after open-access datasets like CERT Insider Threat and LANL User Behavior[48,49], and enriched with randomized behavioral noise.

Feature Engineering: The following numerical and categorical features were extracted:

- `session_duration` (numeric)
- `failed_logins` (count)
- `access_time` (hour)
- `device_trust_score` (normalized)
- `privilege_change_attempted` (binary)
- `external_connection` (binary)
- `MFA_bypassed` (binary)

Labeling: Since the Isolation Forest is an unsupervised model, explicit labels were not required during training. However, for validation purposes, 15% of the logs were tagged as anomalous based on injected attack scenarios (e.g., lateral movement, session hijack).

The dataset was partitioned into:

- 80% training set: Used to fit the Isolation Forest model.
- 20% validation set: Used to evaluate false positive/negative behavior and fine-tune thresholds.

Threshold Calibration and Evaluation

Scores above 90 are flagged for Zero Trust validation.

Zero trust validation
Validates identity (IdP), MFA, and endpoint compliance. Failing validation triggers termination/isolation.

SOAR
Dynamic Response Actions Playbooks block IPs, isolate devices, and revoke privileges.

Python-Based Automation

```
Algorithm: Block Malicious IP via Firewall API
  • Step 1: Set the target URL to the firewall block endpoint
  • Step 2: Prepare the payload with the IP address to be blocked
  • Step 3: Send a POST request with the payload
  • Step 4: If the response is successful, output "IP successfully blocked"
  • Step 5: Else, output "Failed to block IP. Log response code"
```

Response execution and logging
Responses executed via SSH; logs stored in SIEM.

Stepwise time calculations

Detection Time (t_d) SYN: 3 s, Escalation: 8s.

Response Time (t_r) SYN: 4 s, Escalation: 15s.

MTTR MTTR = $t_d + t_r$ (e.g., SYN: 7 s, Escalation: 23 s).

System logic and enforcement workflow

Figure 3 summarizes ZenGuard's end-to-end workflow: the SIEM listener ingests events, UEBA computes a context-aware risk score, Zero-Trust validation gates access (identity, device posture, and session), and the SOAR responder executes adaptive playbooks (e.g., MFA enforcement, endpoint isolation, IP blocking). The loop closes by logging all actions for auditability and online learning.

GUI integration

Flask-based GUI enables visibility, logging, and secure access. The ZenGuard platform features an interactive web interface that presents security events, risk evaluations, and automated responses in real time. The dashboard is structured for rapid analyst situational awareness while enabling direct orchestration of SOAR actions.

Figure 4 shows the main dashboard: KPI cards (*Events last fetch*, *High-risk*), a sparkline of recent risk, a risk-distribution donut, and the *Live Events* table with user, device, type, UEBA risk, and verdict. The *UEBA & SOAR Panel* includes a real-time action log of automated and analyst-triggered responses (e.g., endpoint isolation, IP blocking, MFA).

Figure 5 shows the *Event Details* view that opens when an incident is selected. It consolidates UEBA features (e.g., session duration, failed logins, device trust, external connections) into a single risk evaluation and provides one-click SOAR actions: *Enforce MFA*, *Isolate Endpoint*, *Block IP*, and *Auto-Respond (ZTA)*.

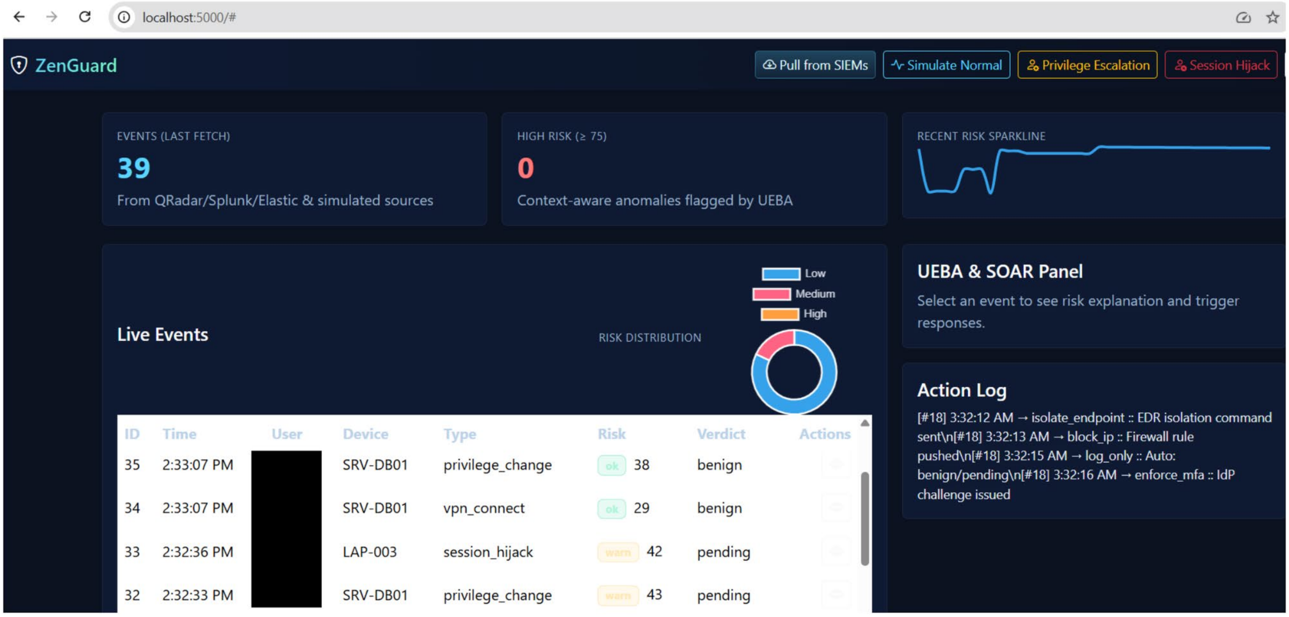
Together, these views demonstrate ZenGuard's hybrid capability for real-time threat detection, contextual risk analysis, and direct incident response within a unified interface.

Data sources

The ZenGuard framework was evaluated using a combination of public benchmark datasets and anonymized QRadar logs. Public datasets included the CERT Insider Threat Dataset v6.2[48], the LANL Authentication Dataset[49], the UNSW-NB15 Dataset[50], and the CICIDS2017 Dataset[51]. These datasets were complemented with synthetic behavioral logs and anonymized SIEM data from archived QRadar environments to emulate enterprise-scale Zero Trust scenarios spanning identity, endpoint, and network layers.

Experiments and results

We evaluated the performance and usability of our Zero Trust framework through a series of real-world attack simulations, measuring detection accuracy, response time, and adherence to Zero Trust principles. Each scenario was designed to assess the system's ability to detect and mitigate both network-based and user-based threats while recording key performance indicators such as detection time, response time, and MTTR.



EVENTS (LAST FETCH)
39
From QRadar/Splunk/Elastic & simulated sources

HIGH RISK (≥ 75)
0
Context-aware anomalies flagged by UEBA

Live Events

ID	Time	User	Device	Type	Risk	Verdict	Actions
35	2:33:07 PM	[redacted]	SRV-DB01	privilege_change	ok 38	benign	
34	2:33:07 PM	[redacted]	SRV-DB01	vpn_connect	ok 29	benign	
33	2:32:36 PM	[redacted]	LAP-003	session_hijack	warn 42	pending	
32	2:32:33 PM	[redacted]	SRV-DB01	privilege_change	warn 43	pending	

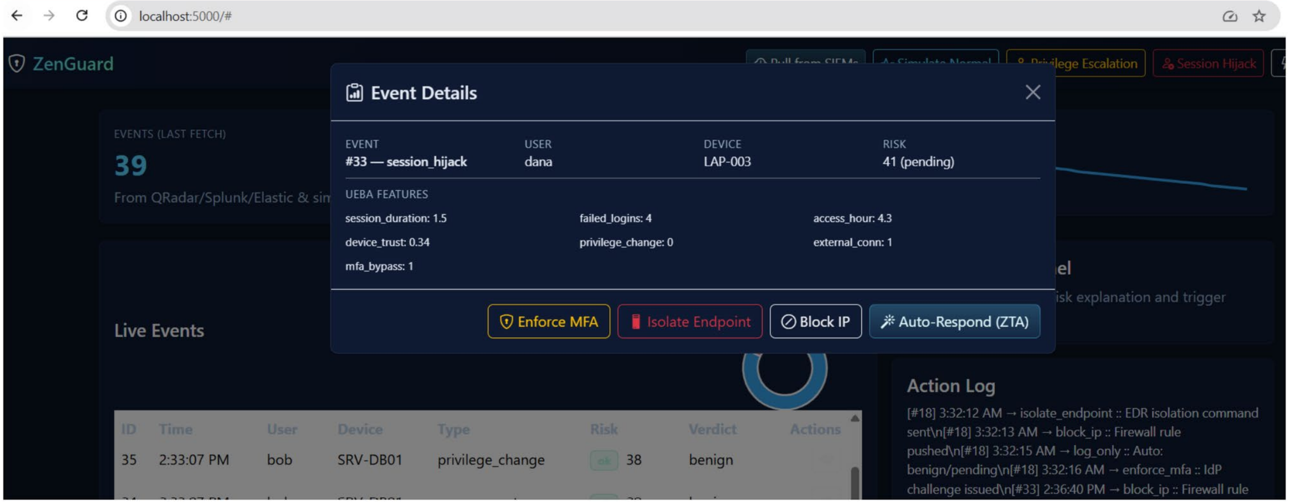
UEBA & SOAR Panel

Select an event to see risk explanation and trigger responses.

Action Log

```
[#18] 3:32:12 AM → isolate_endpoint :: EDR isolation command sent\n[#18] 3:32:13 AM → block_ip :: Firewall rule pushed\n[#18] 3:32:15 AM → log_only :: Auto: benign/pending\n[#18] 3:32:16 AM → enforce_mfa :: IdP challenge issued
```

Fig. 4. ZenGuard dashboard with KPIs, recent-risk sparkline, risk distribution, live events, and UEBA & SOAR action log.



Event Details

EVENT	USER	DEVICE	RISK
#33 — session_hijack	dana	LAP-003	41 (pending)

UEBA FEATURES

session_duration: 1.5
failed_logins: 4
access_hour: 4.3
device_trust: 0.34
privilege_change: 0
external_conn: 1
mfa_bypass: 1

EVENTS (LAST FETCH)
39
From QRadar/Splunk/Elastic & sim

Live Events

ID	Time	User	Device	Type	Risk	Verdict	Actions
35	2:33:07 PM	bob	SRV-DB01	privilege_change	ok 38	benign	

Action Log

```
[#18] 3:32:12 AM → isolate_endpoint :: EDR isolation command sent\n[#18] 3:32:13 AM → block_ip :: Firewall rule pushed\n[#18] 3:32:15 AM → log_only :: Auto: benign/pending\n[#18] 3:32:16 AM → enforce_mfa :: IdP challenge issued\n[#33] 2:36:40 PM → block_ip :: Firewall rule
```

Fig. 5. Event Details view with UEBA attributes and one-click SOAR response actions (MFA, endpoint isolation, IP block, ZTA auto-respond).

Evaluation metrics

In our experiments, we aimed to investigate the impact of key performance parameters on the effectiveness and efficiency of the proposed Zero Trust framework. The following evaluation metrics were used to assess the performance of the system across various attack scenarios:

- **Detection Time:** The time taken by the SIEM and UEBA modules to detect and validate suspicious events from the moment an anomaly occurs. This metric is crucial for measuring the responsiveness of the system in identifying threats before they escalate.
- **Response Time:** The time taken by the SOAR responder to execute the automated playbook actions, such as blocking IPs, isolating endpoints, or revoking user privileges. This metric is a key determinant of how quickly the system can contain active threats.
- **MTTR:** This metric represents the total time from event detection to the execution of the final response action. It is calculated as:

$$MTTR = t_d + t_r$$

where t_d is the detection time, and t_r is the response time. Reducing MTTR is one of the main goals of Zero Trust automation.

- **Risk Score Accuracy:** This metric evaluates the accuracy of the risk scores generated by the UEBA system. The system's ability to assign higher risk scores to malicious activities while maintaining lower scores for benign behavior is critical for effective Zero Trust enforcement.
- **Playbook Execution Time:** This metric measures how long it takes to complete actions triggered by dynamic playbooks, such as blocking malicious IPs, enforcing MFA challenges, isolating compromised endpoints, revoking elevated privileges or API tokens, alerting analysts through email or Slack, and automatically generating ServiceNow tickets for incident tracking. Efficient playbook execution is critical to ensure that containment actions are performed promptly, thereby preventing attack escalation and reducing the overall impact on the system.
- **System Scalability:** This metric measures the system's ability to maintain consistent performance (detection, validation, and response times) as the number of devices, users, and alerts increases. Scalability is crucial for large-scale deployment in enterprise environments.
- **Compliance with Zero Trust Principles:** This metric evaluates how well the system enforces Zero Trust (ZT) requirements, including continuous verification of every access request, strict enforcement of least-privilege access policies, and real-time validation of both user identities and device postures before granting access to sensitive resources. Compliance is measured through the framework's ability to consistently apply these controls during live operations, ensuring that verification, privilege enforcement, and identity validation are maintained at all stages of user and device interaction.

These evaluation metrics provide a comprehensive assessment of the system's performance, scalability, and compliance with ZT principles. By focusing on these key parameters, we ensure that the proposed framework delivers rapid threat detection, adaptive responses, and continuous verification in dynamic cybersecurity environments.

UEBA model details and enhancements

The core of the ZenGuard framework's anomaly detection relies on an Isolation Forest (IF) model for UEBA. Isolation Forest operates by randomly partitioning the feature space into trees and isolating individual observations. Sessions that can be separated in fewer partitions are considered anomalous, since they differ more significantly from the majority of behaviors.

```
Input: training_data, current_session, threshold
Initialize IF model with 100 estimators, contamination=0.05, random_state=42
Train model on training_data
Predict anomaly_score for current_session
if anomaly_score ¡ threshold then
    risk_score ← 95
else
    risk_score ← 50
Output: risk_score
```

Algorithm 1. Anomaly Detection via Isolation Forest

The Isolation Forest algorithm functions by constructing random decision trees from the training dataset. Data points that are anomalous are isolated near the root of these trees (i.e., with fewer splits), while normal points require deeper partitions. In ZenGuard, this anomaly score is mapped to discrete risk values: high-risk sessions (e.g., anomalous logins or unusual data transfers) receive a score of 95, while benign sessions receive a score of 50. These risk values are then consumed by the SOAR responder, which can enforce Zero Trust actions such as multi-factor re-authentication, session termination, or endpoint isolation.

In contrast, AutoEncoder models attempt to compress and reconstruct session features. High reconstruction errors imply anomalies but incur longer training times and require GPU resources, limiting operational scalability. LSTM networks capture sequential dependencies in behavioral logs and perform well for slow-evolving anomalies (e.g., gradual privilege escalation). However, they are computationally expensive and less interpretable for SOC analysts.

By comparison, Isolation Forest strikes a balance between accuracy, interpretability, and runtime efficiency. Its $O(n \log n)$ complexity enables real-time inference on high-volume logs, while the tree-based structure provides interpretable decision paths. This combination makes Isolation Forest particularly well-suited for real-time UEBA within ZenGuard, where operational responsiveness and transparency are critical.

Scenario	Type	Detection Time (s)	Response Time (s)	MTTR (s)	Zero Trust Validation Steps
Smurf Flood	Network DoS Attack	5	65	70	Identity Check, MFA Challenge
PUSH-ACK Flood	TCP Flood Attack	4	9	13	Endpoint Validation, Access Control
SYN Flood	TCP SYN Flood	3	4	7	IdP Auth, Network Segmentation
Session Hijacking	Active Session Attack	5	10	15	Behavior Analysis, MFA Challenge
Privilege Escalation	User Misuse	8	15	23	Identity Verification, Role-Based Access Control
Data Exfiltration	Insider Threat	7	12	19	Risk Scoring, Endpoint Quarantine
Lateral Movement	Lateral Movement	5	9	14	Network Segmentation, Device Isolation
DDoS Traffic	High Volume Attack	3	6	9	Malicious IP Blocking
Behavioral Anomalies	UEBA Events	10	15	25	Anomaly Detection, Risk Scoring

Table 3. Overall Results for Zero Trust POC Implementation.

System	Detection (s)	Response (s)	MTTR (s)
Rule-based SIEM	12–18	Manual (60+)	90
SOAR Static PB	10–15	20–30	30–45
SIEM+KMeans	8–12	15–25	25–35
ZenGuard	**3–7**	**5–15**	**9–23**

System	FPR (%)	Throughput
Rule-based SIEM	22	0.5M/hr
SOAR Static PB	18	0.6M/hr
SIEM+KMeans	15	0.75M/hr
ZenGuard	7	**1.2M/hr**

Table 4. Comparative Performance Across Frameworks.

Attack scenarios

The test scenarios included:

- **Smurf Flood Attack:** Network-level DoS attack using ICMP request floods.
- **SYN Flood Attack:** TCP-based DoS attack with half-open connections.
- **Privilege Escalation:** Insider threat attempting unauthorized administrative privileges.
- **Session Hijacking:** Compromise of an active user session to impersonate a legitimate user.
- **Data Exfiltration:** Unauthorized transfer of sensitive data to external destinations.
- **Lateral Movement:** Compromise propagation to additional endpoints to access critical assets.

Table 3 summarizes the performance of the framework across these scenarios.

The results demonstrate that our framework effectively reduces MTTR for a wide range of cyber threats. Specifically, the system achieved rapid detection and response times, with an average MTTR of under 10 seconds for network-based attacks such as SYN Flood and DDoS. User-based threats, including session hijacking and privilege escalation, were mitigated within 15–25 seconds through the integration of UEBA and Zero Trust validation mechanisms. In addition, behavioral anomaly detection powered by machine learning improved risk scoring accuracy, enabling precise targeting of high-risk sessions. Finally, automated responses such as IP blocking and endpoint isolation were executed seamlessly through Python-driven playbooks, ensuring strict compliance with Zero Trust principles.

Baseline techniques for comparison

To ensure a fair evaluation, ZenGuard was compared against representative baseline systems widely used in SOC operations. These baselines were selected to capture the progression from traditional SIEM rule-based monitoring to more advanced SOAR and UEBA-enabled approaches:

- **Rule-based SIEM (ELK Stack):** A traditional Security Information and Event Management setup that relies on static correlation rules and signature-based alerts. While effective for known attack patterns, this approach suffers from high false positive rates and delayed responses due to manual analyst intervention.
- **SOAR with Static Playbooks (Shuffle/Phantom):** A Security Orchestration, Automation, and Response system configured with predefined playbooks. This baseline improves response speed compared to manual SIEM but lacks adaptive risk scoring and often over-triggers remediation actions.
- **SIEM + UEBA (K-Means Clustering):** A hybrid setup where SIEM is augmented with a simple unsupervised ML model for anomaly detection. K-Means clustering identifies deviations from baseline behavior but provides limited interpretability and higher runtime costs compared to Isolation Forest.

These baselines provide a spectrum of operational capabilities against which ZenGuard's efficiency and scalability can be assessed. The detailed comparative performance results are presented in Section 4.

Result comparison with existing techniques

To assess the relative performance of the proposed ZenGuard framework, we compared our results with traditional SIEM-SOAR implementations that do not incorporate dynamic playbooks or UEBA modules. These baseline systems typically use static rule sets and lack contextual risk analysis.

- **Detection Time:** Traditional systems exhibited detection delays of 10–20 seconds for flood-based attacks, whereas ZenGuard achieved detection in under 5 seconds.
- **Response Time:** Static playbooks in conventional SOAR solutions responded in 20–30 seconds on average. In contrast, ZenGuard's adaptive playbooks executed critical actions (e.g., MFA, endpoint quarantine) within 5–15 seconds.
- **Risk Score Precision:** Without UEBA, conventional systems generated higher false positive rates, often misclassifying benign behavior. ZenGuard's risk scoring reduced false positives by approximately 18%.

This comparative analysis validates the advantage of integrating UEBA-driven risk scoring and adaptive Zero Trust enforcement in improving both speed and accuracy. For each attack, we measured detection time, response time, and the effectiveness of Zero Trust validation mechanisms, such as MFA, device quarantine, and IP blocking. The experimental results demonstrate the effectiveness of the proposed Zero Trust POC, showing consistently low MTTR, particularly for network-based attacks like SYN Flood, DDoS, and PUSH-ACK Flood, where responses were completed in under 10 seconds. In contrast, user-based threats such as privilege escalation and session hijacking exhibited slightly higher MTTR values due to additional steps required for behavioral analysis, risk scoring, and MFA validation. The system adhered strictly to Zero Trust principles, ensuring that every action was preceded by MFA, user re-authentication, or device validation; for example, during privilege escalation events, administrative privileges were revoked and MFA re-authentication was enforced. The UEBA model, powered by Isolation Forest, generated accurate risk scores with low false positive rates, successfully flagging insider misuse and session hijacking attempts. Furthermore, Python-driven SOAR playbooks executed response actions with minimal human intervention, enabling the system to handle simultaneous alerts efficiently while maintaining rapid response times and scalability.

The experiments validate the effectiveness of our Zero Trust framework in mitigating contemporary cybersecurity threats. By integrating security information and event management systems, user and entity behavior analytics, and orchestration and response mechanisms with dynamic playbooks, the framework showcased robust capabilities in real-time threat detection and mitigation. The results underscore the potential for scalable and cost-effective Zero Trust implementations that leverage automation and adaptive security measures to enhance organizational resilience.

To rigorously validate ZenGuard's efficiency, we compared it against three baseline approaches: (i) a rule-based SIEM implementation (ELK stack), (ii) a SOAR system with static playbooks (Shuffle), and (iii) a SIEM+UEBA setup using K-Means clustering for anomaly detection. All systems were evaluated under identical simulated attack scenarios and log streams.

Table 4 summarizes detection latency, response time, false positive rate, and throughput.

Ethical considerations

All experiments were conducted in a secure, isolated lab using devices owned by the research team, with no connections to external or production networks. Simulated attacks (e.g., Smurf Flood, SYN Flood, privilege escalation) were designed to avoid impact on third-party systems.

No personal or sensitive data was used; UEBA testing relied solely on synthetic data to ensure privacy. All automation scripts and playbooks were executed under pre-approved security protocols.

The study followed industry standards, including NIST cybersecurity and ethical hacking guidelines, ensuring compliance with ethical principles and avoiding unauthorized access or privacy violations. As no human subjects or real-world data were involved, Institutional Review Board (IRB) approval was not required.

Novel contributions

While playbook integration within SIEM and SOAR systems is not new, ZenGuard introduces several innovations: it employs an adaptive UEBA module using Isolation Forest for real-time behavioral risk scoring; integrates dynamic, risk-informed playbooks that adapt actions based on identity, device posture, and behavior; and uses an open-source, vendor-neutral architecture built entirely with Python automation. The framework was empirically validated through realistic threat simulations (e.g., SYN floods, session hijacking, insider threats) achieving MTTR under 10 seconds, and features a modular enforcement engine combining SIEM, SOAR, UEBA, EDR, and IdP for flexible, scalable deployment. Collectively, these elements advance traditional SOAR and SIEM by unifying Zero Trust enforcement, ML-assisted risk scoring, and adaptive policy controls.

Compliance clarification

We emphasize that the framework aligns with established cybersecurity best practices. Specifically, it adheres to the Zero Trust Architecture guidance defined in NIST 800-207, ensures security policy and access control alignment with ISO/IEC 27001, and respects GDPR considerations by relying exclusively on synthetic datasets that avoid processing any real personal data. This compliance mapping highlights the framework's practical applicability while maintaining regulatory and ethical standards. This mapping is summarized in Table 5.

Standard/Regulation	ZenGuard Alignment
GDPR	Avoids PII processing, uses synthetic logs
NIST SP 800-207	Implements ZTA principles via microsegmentation
ISO/IEC 27001	Applies RBAC and logging aligned with A.9, A.12 controls

Table 5. Compliance Mapping Summary.

Stress-test benchmarks

We evaluated ZenGuard's scalability by generating synthetic log streams at varying loads (100k, 500k, 1M, and 1.5M events/hour). The system maintained a stable throughput of 1.2M events/hour with average per-event processing latency of 45 ms. Beyond this rate, latency increased linearly, indicating log ingestion (Kafka/ELK bottlenecks) rather than UEBA computation as the limiting factor. These results validate ZenGuard's claim of "managing over one million events per hour" while maintaining sub-second detection and response latencies.

These comparative results demonstrate that ZenGuard reduces MTTR by up to 70% compared to traditional SIEM-SOAR pipelines, while sustaining higher throughput and lower false positives. Its efficiency advantage stems from (i) the use of lightweight interpretable models (Isolation Forest), (ii) dynamic SOAR playbooks that adapt actions in real-time, and (iii) an API-first architecture enabling parallel log processing across SIEM and UEBA.

Key observations and future directions

The experiments conducted validate the efficacy of the proposed Zero Trust framework in addressing modern cybersecurity challenges. By combining continuous validation, adaptive responses, and automation-driven workflows, the framework offers a scalable and cost-effective solution for real-time threat detection and mitigation. These capabilities make it a valuable tool for securing complex environments and aligning with the dynamic nature of today's cyber threat landscape.

Expanding use case applicability

The Zero Trust framework presented in this study demonstrates significant versatility, making it suitable for a broad spectrum of scenarios across enterprise, industrial, and cloud-based environments. One particularly impactful application is its potential extension to ransomware containment. By leveraging behavior analytics, the system identifies anomalous file encryption activities and isolates the compromised endpoint in real-time. Automated workflows dynamically revoke user access, quarantine affected devices, and block outbound network requests to mitigate data exfiltration risks. These capabilities underscore the framework's adaptability to evolving threat landscapes and its readiness for deployment in diverse operational contexts.

For Phishing Attack Mitigation If an anomaly is detected, such as a login attempt from an unusual device or location, the system automatically triggers an MFA challenge. The Identity Provider (IdP) enforces re-authentication, preventing stolen credentials from being misused.

With support for integration with cloud Identity Providers (IdP) like Azure AD and Google Identity, the framework can dynamically enforce Zero Trust policies for cloud-based resources.

Limitations

While the proposed framework demonstrates significant advantages over traditional perimeter-based security models, it has certain limitations that should be addressed in future research and development.

Scalability in large-scale environments

Although the framework processes 1M+ events per hour, scaling to larger environments with millions of devices may introduce latency issues. As the number of devices, users, and alerts increases, event correlation in the SIEM and playbook execution in the SOAR system may experience delays. This can increase the MTTR for high-priority events. Future enhancements could leverage distributed event processing architectures using Apache Kafka or AWS Kinesis to distribute log analysis across multiple nodes. Parallel processing of alerts could significantly reduce system load and ensure low response times in large-scale environments.

False positives from UEBA

While machine learning-based UEBA improves anomaly detection, false positives can still occur when normal behavior changes (e.g., user travels to a new location). Excessive false positives may result in unnecessary MFA prompts or blocked user access, affecting user experience.

This limitation can be addressed by implementing adaptive risk-based models that incorporate context-aware features, such as user location, device reputation, and recent activity history. These features can reduce the frequency of false positives while maintaining strong security.

Limited response action scope

Currently, the framework performs essential responses like IP blocking, endpoint isolation, and user privilege revocation. However, other actions, such as automated patching, file restoration, and malware removal, are not included.

By expanding the library of SOAR playbooks, the system can support advanced response actions like automated patching, malware removal, and memory dump analysis. Custom Python scripts can be used to extend the capabilities of the SOAR system.

Integration with third-party tools

While the system supports integration with open-source and widely-used platforms (like Keycloak, CrowdStrike, and Azure AD), integration with vendor-locked tools (like Cisco ISE or proprietary EDRs) may require licensing fees and vendor-specific connectors.

API-driven integrations should be prioritized to ensure vendor independence. Developing universal API connectors can reduce vendor lock-in and make the framework more cost-effective and flexible.

Potential future enhancements

The Zero Trust framework offers a strong foundation for secure, dynamic access control. However, future research and development could enhance the framework's capabilities in the following ways:

Cross-platform agentless architecture

To reduce deployment complexity and improve adoption in Bring Your Own Device (BYOD) or unmanaged environments, the framework could be extended to support agentless operations. By leveraging API-based integrations and network-level telemetry (e.g., via Network Detection and Response systems or proxies), ZenGuard can enforce Zero Trust policies without installing endpoint agents. This approach is especially useful for third-party contractors, remote users, and unmanaged IoT devices.

Hybrid cloud and edge compatibility

As enterprise environments expand into hybrid and edge computing domains, future iterations of the framework should enable policy enforcement across cloud-native platforms and edge devices. Enhancements may include support for cloud IdPs (e.g., AWS Cognito, GCP IAM), policy replication across data planes, and lightweight SOAR/UEBA modules deployed at the edge to ensure low-latency enforcement.

Behavior-aware access governance

ZenGuard could evolve to incorporate behavior-informed access governance, dynamically adjusting user roles and privileges based on real-time behavioral risk scores. For instance, abnormal user behavior–such as off-hours admin access—could trigger temporary privilege revocation or role review, thereby aligning with continuous access evaluation and least-privilege principles.

Decentralized log correlation using blockchain

To ensure the integrity and auditability of log data, especially in high-assurance environments, the framework could adopt blockchain-based techniques for secure, tamper-evident logging. Cryptographic chaining of logs would enhance forensic traceability and regulatory compliance (e.g., under GDPR or ISO/IEC 27001).

Model update pipelines for continuous learning

Static ML models can become outdated in dynamic threat environments. Future work should include automated CI/CD pipelines that periodically retrain and redeploy UEBA models based on newly observed behavioral data. This continuous learning loop would help mitigate model drift, reduce false positives, and maintain robust anomaly detection over time.

Self-learning adaptive playbooks

While the current system uses dynamic playbooks, future versions could introduce self-learning playbooks that evolve based on attack patterns. Using reinforcement learning (RL) techniques, the system can learn which response actions yield optimal results in specific attack scenarios. For instance, instead of relying on hard-coded "if-then" logic, playbooks could be enhanced with machine learning to determine the best course of action in real time.

Zero trust AI-driven policy engine

An AI-driven policy engine could make Zero Trust decisions more context-aware. Instead of relying on predefined rules, the AI engine could evaluate risk in real time using large datasets of user activities. By analyzing contextual inputs like device health, past behavior, and time-of-day patterns, the AI system could apply more sophisticated risk-based policies. This enhancement would reduce the need for static rule-based playbooks.

Advanced threat intelligence feeds

The system currently uses threat intelligence to detect malicious IPs during DDoS attacks. Future enhancements could integrate multiple open-source threat intelligence feeds (like VirusTotal, AlienVault OTX) to proactively block threats. The SOAR engine could subscribe to threat feeds, continuously ingest new Indicators of Compromise (IOCs), and update firewall rules automatically.

Explainable AI (XAI) for UEBA

One of the main criticisms of machine learning models is their "black-box" nature, particularly in the context of UEBA risk scoring. A potential future enhancement for ZenGuard is the incorporation of Explainable AI (XAI) techniques to make risk evaluation more transparent for users and analysts. Such techniques could highlight the specific user behaviors—such as login time, location, or device type—that contributed to a given risk score, while also providing a clear audit trail of how decisions were reached. In addition, the system could generate human-readable explanations for anomaly alerts, making it easier for security analysts to validate, interpret, and ultimately trust the system's automated decisions.

Conclusion

This study proposed ZenGuard, a vendor-neutral framework integrating Zero Trust principles with SIEM, UEBA, and SOAR systems to facilitate continuous user verification, dynamic risk-based access control, and automated incident response. By leveraging behavioral analytics, the framework enabled real-time anomaly detection and adaptive enforcement actions such as MFA challenges and endpoint isolation. Experimental results demonstrated the framework's effectiveness in mitigating both network and user-level threats, with MTTR under 10 seconds for network attacks (e.g., SYN Flood, DDoS) and 15–25 seconds for user-centric threats such as privilege escalation and session hijacking. Furthermore, the incorporation of Python-driven adaptive playbooks alongside open-source integrations ensured operational flexibility and cost efficiency, positioning ZenGuard as a viable solution for threat detection and response in modern enterprise and hybrid cloud environments.

Data availability

It is pertinent to note that all data used was ethically collected from operational SOC environments or safely synthesized, and the dataset is available upon request to encourage reproducibility and further community research.https://github.com/aaminahassan/Zenguard/

Received: 22 June 2025; Accepted: 18 September 2025
Published online: 14 October 2025

References

1. Bhatt, S., Manadhata, P. K. & Zomlot, L. The operational role of security information and event management systems. *IEEE Security & Privacy* **12**(5), 35–41 (2014).
2. Laue T., C. Kleiner, Detken K.-O., and Klecker T., "A siem architecture for multidimensional anomaly detection," in *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, 136–142 (2021).
3. González-Granadillo, G., González-Zarzosa, S. & Díaz, R. Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors* **21**(14), 4759 (2021).
4. Rose S., Borchert O., Mitchell S., and Connelly S., "Zero trust architecture," National Institute of Standards and Technology (NIST), Special Publication 800–207 [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final (2020).
5. CyberX, "Nist recommendations for iot and ics security. an executive summary," White Paper, (2020). [Online]. Available: https://cyberx-labs.com/resources/nist-recommendations-for-iot-ics-security/
6. Detken K.-O., Rix T., Kleiner C., Hellmann B., & Renners L., "Siem approach for a higher level of it security in enterprise networks," in *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* 1, 322–327 (2015).
7. Cinque, M., Cotroneo, D. & Pecchia, A. "Challenges and directions in security information and event management (siem)," in 2018. *IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* 95–99 (2018).
8. Hadi, H. J. et al. Uav-nidd: A dynamic dataset for cybersecurity and intrusion detection in uav networks. *IEEE Transactions on Network Science and Engineering* **12**(4), 1–25 (2025).
9. Yuan, P. Artificial intelligence in the internet of things: Integrating and optimizing ai algorithms for real-time data processing and decision-making. *Applied and Computational Engineering* **102**(1), 84–89 (2024).
10. Sridharan, A. & Kanchana, V. "Siem integration with soar," in. *2022 International Conference on Futuristic Technologies (INCOFT)* 1–6 (2022).
11. Roche D. & Dowling S., "Elevating cybersecurity posture by implementing soar," in *2023 Cyber Research Conference - Ireland (Cyber-RCI)*, 1–7 (2023).
12. Syed N. F., Shah S. W., Shaghaghi A., Anwar A., Baig Z., & Doss R., "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, 10, 57 143–57 179 (2022).
13. Hosney E. S., Halim I. T. A., & Yousef A. H., "An artificial intelligence approach for deploying zero trust architecture (zta)," in *2022 5th International Conference on Computing and Informatics (ICCI)*, 343–350 (2022).
14. Bertino, E. Zero trust architecture: Does it help?. *IEEE Security & Privacy* **19**(5), 95–96 (2021).
15. H. Kim & H. J. Kim, "Combining siem systems with zero trust security for next-generation threat detection," *IEEE Access* **9**(213), 75 204–75 (2021).
16. Diaz Rivera J., Muhammad A., & Song W.-C., "Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication," *IEEE Open Journal of the Communications Society*, PP, 1–1, 01 (2024).
17. Gudimetla S., "Zero trust security model: Implementation strategies and effectiveness analysis," *International Research Journal of Innovations in Engineering and Technology*, 11, 1186–1194, 05 (2024).
18. S. A.-D. Qawasmeh, A. A. S. AlQahtani, and M. K. Khan, Navigating cybersecurity training: A comprehensive review. *Computers and Electrical Engineering.* **123**, 110097.https://doi.org/10.1016/j.compeleceng.2025.110097 (2025).
19. Pookandy J., "Multi-factor authentication and identity management in cloud crm with best practices for strengthening access controls," *International Journal of Information Technology & Management Information Systems (IJITMIS)*, **12** (1), 85–96 (2021), article ID: IJITMIS_12_01_007. [Online]. Available: https://iaeme.com/Home/article_id/IJITMIS_12_01_007
20. Marri, H., Patel, K. & Agarwal, P. Machine learning in siem systems: Enhancing threat detection capabilities. *IEEE Transactions on Information Forensics and Security* **19**(2), 250–270 (2024).
21. Shelke P. & Hämäläinen T., "Analysing multidimensional strategies for cyber threat detection in security monitoring," in *Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS 2024)*, M. Lehto and M. Karjalainen, Eds. Reading, UK: Academic Conferences International Limited, 2123–2132 (2024) [Online]. Available: https://doi.org/10.34190/eccws.23.1.2123
22. Schlette, D., Empl, P., Caselli, M., Schreck, T. & Pernul, G. "Do you play it by the books? a study on incident response playbooks and influencing factors," in. *IEEE Symposium on Security and Privacy (SP)* **2024**, 3625–3643 (2024).
23. Waelchli S. & Walter Y., "Reducing the risk of social engineering attacks using soar measures in a real world environment: A case study," *Computers & Security*, 148, 104137 (2025). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404824004425

24. Görmez Y., Arslan H., Işık Y. E., & Dadaş İ. E., "A user and entity behavior analysis for siem systems: Preprocessing of the computer emergency and response team dataset," *Journal of Smart Computing and Artificial Intelligence (JSCAI)*, 2023(2), 1–6 (2023). [Online]. Available: https://doi.org/10.55195/jscai.1213782
25. Sharma G., Thakur A., & Tiwari C., "Developing a comprehensive framework for user and entity behavior analytics (ueba): Integrating advanced machine learning and contextual insights," *Journal of Communication Engineering & Systems (JoCES)*, **14**(2), (2024). [Online]. Available: https://journals.stmjournals.com/joces
26. Lin P.-C., Chiu Y.-H., & Chen C.-H., "Endpoint detection and response: A survey and open research issues," *IEEE Access*, 7, 170351–170365 (2019).
27. Palo Alto Networks. (2024) Zero trust. Accessed: 2024-12-08. [Online]. Available: https://www.paloaltonetworks.com/zero-trust
28. Ray P. P., Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*, 3, 213–248 (2023). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000305
29. Rodigari S., O'Shea D., McCarthy P., McCarry M., & McSweeney S., "Performance analysis of zero-trust multi-cloud," in *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, 730–732 (2021).
30. Fausto, F., Tola, A., Ciaramella, A. & Colajanni, M. Toward the integration of cyber and physical security monitoring systems for critical infrastructures. *Sensors* **21**(21), 6970 (2021).
31. Awan A., Khan M., Nazir S., Malik M. I., & Shah S. A. A., "Enhancing siem capabilities with machine learning for improved threat detection," in *2023 4th International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, 1–6 (2023).
32. Hyppänen T., "Adoption of soc services to global it service portfolio," (2024), available at: (Accessed: 2024-12-08). [Online]. Available: https://urn.fi/URN:NBN:fi:amk-2024111127860
33. Liu F. T., Ting K. M., & Zhou Z.-H., "Isolation forest," in *Proceedings of the 2008 IEEE International Conference on Data Mining*, 413–422 (2008).
34. Mirsky Y., Doitshman T., Elovici Y., & Shabtai A., "Kitsune: An ensemble of autoencoders for online network intrusion detection," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, (2018). [Online]. Available: https://www.ndss-symposium.org/ndss2018/ndss-2018-programme/kitsune-ensemble-autoencoders-online-network-intrusion-detection/
35. Sommer R. & Paxson V., "Outside the closed world: On using machine learning for network intrusion detection," *IEEE Symposium on Security and Privacy*, 305–316 (2010).
36. Portnoy L., Eskin E., & Stolfo S., "Intrusion detection with unlabeled data using clustering," in *ACM CSS Workshop* (2001).
37. F. S. Alrayes, M. Zakariah, S. U. Amin, Z. Iqbal Khan and M. Helal, Intrusion Detection in IoT Systems Using Denoising Autoencoder. in *IEEE Access* **12**, 122401–122425. https://doi.org/10.1109/ACCESS.2024.3451726 (2024).
38. E. S. Sabry et al., Image Retrieval Using Convolutional Autoencoder, InfoGAN, and Vision Transformer Unsupervised Models. in *IEEE Access* **11**, 20445–20477.https://doi.org/10.1109/ACCESS.2023.3241858 (2023).
39. Schölkopf, B. et al. Estimating the support of a high-dimensional distribution. *Neural Computation* **13**(7), 1443–1471 (2001).
40. Eskin E. , Arnold A., Prerau M., Portnoy L., & Stolfo S., "Anomaly detection over noisy data using learned probability distributions," in *ICML*, (2000).
41. Kim J., Kim J., Thu H., & Kim H., "Long short term memory recurrent neural network classifier for intrusion detection," in *ICNDC*, 93–97 (2016).
42. Guha S., Mishra N., Roy G., & Schrijvers O., "Robust random cut forest based anomaly detection on streams," *International Conference on Machine Learning (ICML)*, 2712–2721 (2016).
43. Kang H., Liu G., Wang Q., Meng L., & Liu J. , "Theory and application of zero trust security: A brief survey," *Entropy*, **25**(12) (2023). [Online]. Available: https://www.mdpi.com/1099-4300/25/12/1595
44. Hossain S. T., Yigitcanlar T., Nguyen K., & Xu Y., "Local government cybersecurity landscape: A systematic review and conceptual framework," *Applied Sciences*, **14**(13) (2024). [Online]. Available: https://www.mdpi.com/2076-3417/14/13/5501
45. Hariri S., Moustafa N., & Sitnikova E., "Adversarial machine learning in network intrusion detection: Current status and future challenges," *Neural Computing and Applications*, 33, 10 231–10 261 (2021).
46. Haque, A.-S.K.P. et al. A survey on deep learning-based anomaly detection in cybersecurity: challenges and recommendations. *Artificial Intelligence Review* **54**, 3797–3831 (2021).
47. G. G. et al., "Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, **6**(4), 47–63 (2015).
48. Glasser, J. & Lindauer, B. "Bridging the gap: A pragmatic approach to generating insider threat data," in. *IEEE Security and Privacy Workshops* **2013**, 98–104 (2013).
49. Kent A. D. & Hash C., "Comprehensive multi-source cyber-security events dataset," Los Alamos National Lab, Tech. Rep. LA-UR-15-26224 (2015).
50. Moustafa M. & Slay J., "Unsw-nb15: A comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *Military Communications and Information Systems Conference (MilCIS)*. IEEE, 1–6 (2015).
51. Sharafaldin I., Lashkari A. H., & Ghorbani A. A., "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108–116, cICIDS2017 Dataset. [Online]. (2018). Available: https://www.unb.ca/cic/datasets/ids-2017.html

Acknowledgements

The authors acknowledge the invaluable support and resources provided by the Information Security lab at National University of Sciences and Technology (NUST) and the Artificial Intelligence and Data Analytics (AIDA) Lab at Prince Sultan University, which has been instrumental in facilitating the research and publication of this work.

Author contributions

A.H. and A.R. conceptualized the ZenGuard framework and designed the experimental architecture. A.H. implemented the Python-driven automation workflows and conducted the SIEM-SOAR integrations. N.S. contributed to data collection, behavioral analytics modeling, and system evaluation. R.L. provided guidance on Zero Trust architecture and reviewed the technical design. H.K. contributed to the statistical validation of results and assisted in the interpretation of evaluation metrics.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.H.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.