SASTRA

ENGINEERING · MANAGEMENT · LAW · SCIENCES · HUMANITIES · EDUCATION

DEEMED TO BE UNIVERSITY

(U/S 3 of the UGC Act, 1956)

THINK MERIT | THINK TRANSPARENCY | THINK SASTRA

THANJAVUR | KUMBAKONAM | CHENNAI

ZenGuard – A Zero Trust, ML-Driven SIEM–SOAR–UEBA Framework

Presented by,

Harish Siddartha – 127158018
Pranav Jai S S - 127003193
Gokulakannan B S - 127003077

Guided By,

Dr Rajakumaran M
Assistant Professor III, School of Computing

Abstract

- Traditional perimeter-based security is insufficient against insider threats, lateral movement, and advanced persistent attacks, requiring continuous Zero Trust enforcement.
- ZenGuard integrates SIEM, UEBA (Isolation Forest), and adaptive SOAR playbooks into a unified, vendor-neutral security automation framework.
- Behavioral risk scoring dynamically triggers MFA enforcement, endpoint isolation, IP blocking, and privilege revocation across identity, device, and network layers.
- Experimental evaluation demonstrates sub-10-second MTTR for network attacks and reduced false positives compared to static SIEM–SOAR systems.
- The framework provides scalable, explainable, and NIST SP 800-207–aligned Zero Trust automation for modern enterprise environments.

Base paper Details

- **Hassan, A., Rauf, A., Shafqat, N., Latif, R., & Khan, H. (2025).** ZenGuard: A machine learning–based Zero Trust framework for context-aware threat mitigation using SIEM, SOAR, and UEBA. *Scientific Reports, 15*, 35871.
- Base Paper Link: https://doi.org/10.1038/s41598-025-20998-4
- **Indexed in:** Scopus and Web of Science (SCI Expanded)
- **Year of Journal Base Paper Publication:** 2025

Literature Survey

Zero Trust Security Model (Palo Alto Networks Whitepaper, 2024)

- **Description:** Industry perspective on Zero Trust implementation strategies and micro-segmentation.
- **Drawback:** Vendor-specific and lacks open, ML-driven automation frameworks.
- **Inference:** Vendor-neutral, API-first Zero Trust architectures address interoperability limitations.
- **Source link:** https://www.paloaltonetworks.com/zero-trust

Literature Survey

Machine Learning in SIEM: A Survey on Intelligent Event Correlation and Anomaly Detection (2025, ResearchGate Preprint)

- **Description**: Reviews ML techniques applied in SIEM systems for event correlation, anomaly detection, and alert prioritization in SOC environments.
- **Drawback**: Primarily focuses on detection enhancement without integrating Zero Trust enforcement or adaptive SOAR automation.
- **Inference**: A gap exists in converting ML-based SIEM insights into real-time, risk-aware enforcement mechanisms.
- **Source-link**: https://www.researchgate.net/publication/398679746_MACHINE_LEARNING_IN_SIEM_A_SURVEY_ON_INTELLIGENT_EVENT_CORRELATION_AND_ANOMALY_DETECTION

Literature Survey

Zero Trust Architecture: A Comprehensive Survey (2021, arXiv)

- **Description**: Provides a detailed survey of Zero Trust models, architectural components, and deployment strategies across enterprise environments.
- **Drawback**: Emphasizes architectural theory but lacks operational ML-based behavioral scoring integration.
- **Inference**: There is scope for integrating Zero Trust with explainable UEBA and automated SOAR playbooks.
- **Source link**: https://arxiv.org/abs/2105.02334

Literature Survey

Reducing the Risk of Social Engineering Attacks Using SOAR Measures (2024, Computers & Security, Elsevier)

- **Description**: Evaluates SOAR-driven automation for mitigating social engineering and phishing attacks in enterprise SOC setups.
- **Drawback**: Uses largely static playbooks without context-aware behavioral risk scoring.
- **Inference**: Adaptive, ML-informed playbooks can improve contextual response precision.
- **Source link**: https://www.sciencedirect.com/science/article/pii/S0167404824004425

Literature Survey

Adoption of SOC Services to Global IT Service Portfolio (2024, Theseus Repository)

- **Description**: Discusses operational integration of SOC services and automation strategies within enterprise IT ecosystems.
- **Drawback**: Focuses on service integration rather than behavioral anomaly detection mechanisms.
- **Inference**: Combining SOC operational models with ML-driven UEBA enhances real-time Zero Trust compliance.
- **Source link**: https://www.theseus.fi/handle/10024/868840

Literature Survey

Developing a Comprehensive Framework for UEBA (2024, Journal of Communication Engineering & Systems – JoCES)

- **Description**: Proposes a structured UEBA framework integrating contextual machine learning for anomaly detection.
- **Drawback**: Limited discussion on SIEM–SOAR orchestration and real-time enforcement workflows.
- **Inference**: A unified architecture combining UEBA, SIEM, and automated response bridges this gap.
- **Source link:** https://journals.stmjournals.com/joces/

Literature Survey

UEBA for SIEM Systems: Preprocessing of CERT Dataset (2023, Journal of Smart Computing and Artificial Intelligence)

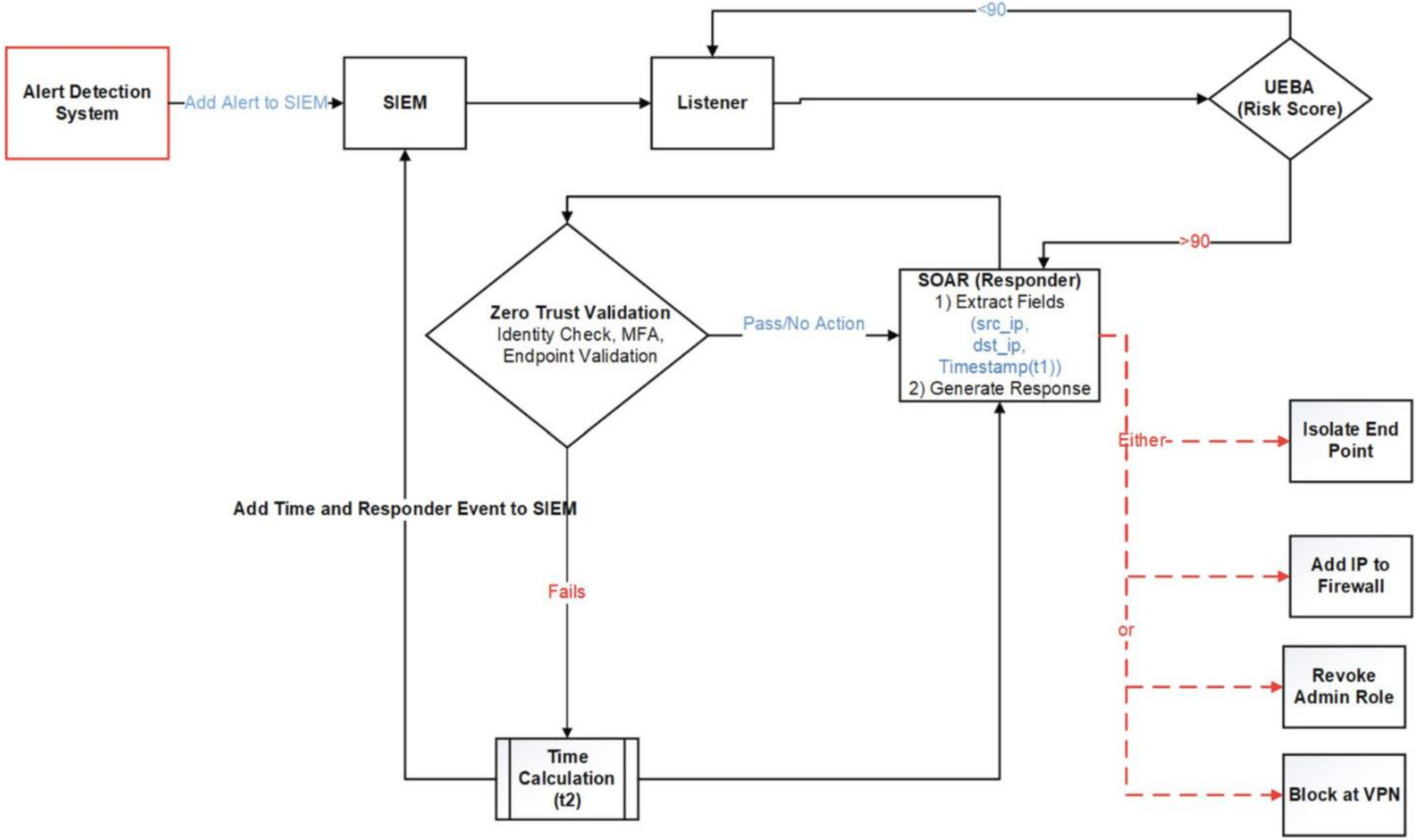
Description: Studies preprocessing and feature engineering techniques for UEBA integration with SIEM.

Drawback: Focuses on data preparation rather than adaptive SOAR enforcement.

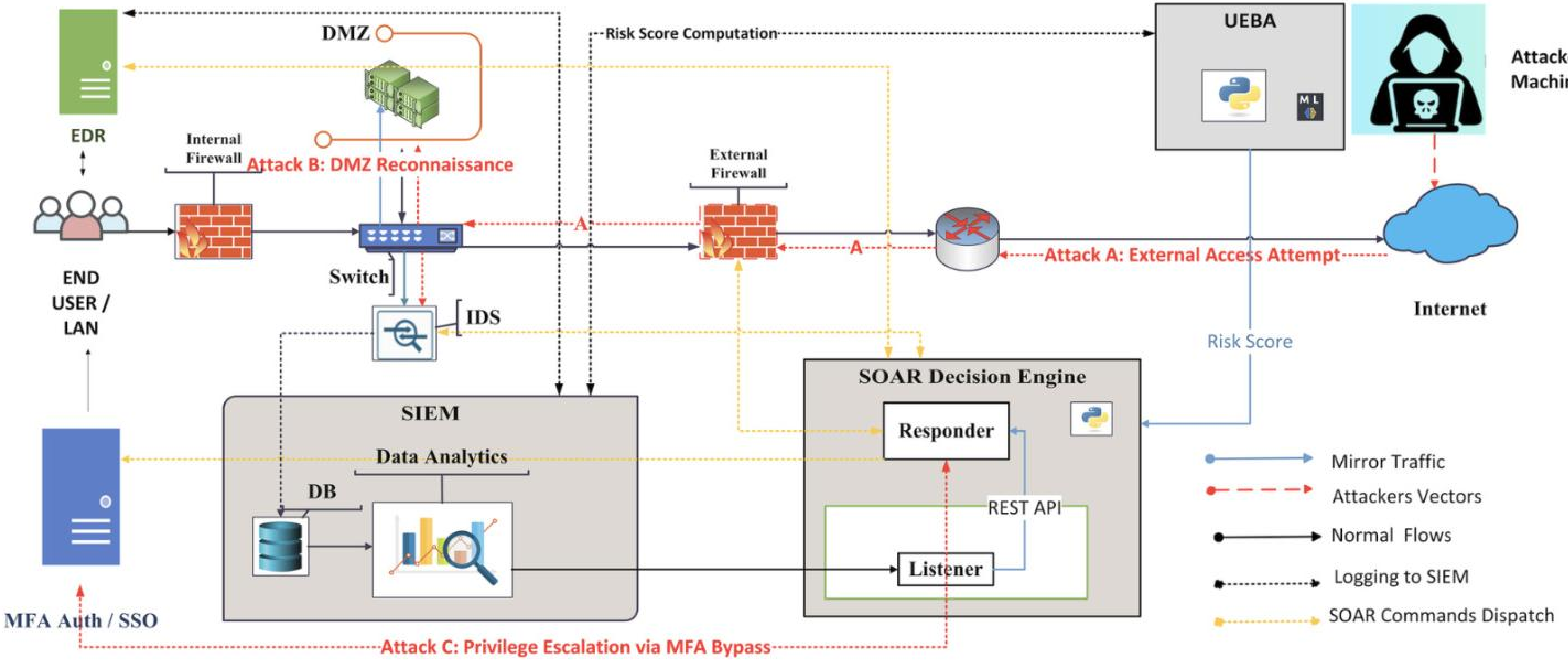
Inference: Real-time anomaly scoring must be coupled with automated remediation for effective Zero Trust.

Source link: https://dergipark.org.tr/en/pub/jscai/article/1213782

Work Flow Diagram



Architecture Diagram



Modules

Module 1: Log Aggregation & Feature Preparation

- Collect and normalize logs from SIEM sources (firewalls, IDS, EDR, IdP).
- Extract behavioral features such as session duration, failed logins, and privilege changes for UEBA processing.

Module 2: Anomaly Detection & Zero Trust Risk Scoring

- Apply Isolation Forest for behavioural anomaly detection.
- Convert anomaly scores into discrete risk levels to trigger identity validation, MFA enforcement, and device compliance checks.

Module 3: Automated Response & Enforcement (SOAR)

- Execute adaptive Python-based playbooks for IP blocking, endpoint isolation, and privilege revocation.
- Log actions in SIEM and display structured risk insights via the dashboard.

Dataset Description

Synthetic Behavioural Dataset

- Custom-generated enterprise session logs for UEBA training and validation.
- Features include session duration, failed logins, privilege change attempts, MFA bypass, device trust score, and external connections.
- 80% training / 20% validation split with 15% injected anomaly scenarios.

Public Benchmark Dataset:

- CERT Insider Threat Dataset (v6.2) – Insider misuse behavior modeling.
- LANL Authentication Dataset – User login and authentication analysis.
- UNSW-NB15 Dataset – Network intrusion and attack traffic patterns.
- CICIDS2017 Dataset – DDoS and multi-vector cyberattack scenarios.

Enterprise SIEM Log Dataset:

- Anonymized QRadar logs simulating real-world SOC operations.
- Integrated sources: firewalls, IDS, EDR, VPN, and Identity Providers.
- Used to validate scalability up to 1M+ events per hour.

Conclusion

- A unified Zero Trust framework was developed, integrating SIEM, Isolation Forest–based UEBA, and adaptive SOAR playbooks to enable context-aware, automated threat mitigation.
- Behavioural anomaly scores were transformed into actionable risk levels, triggering real-time identity validation, MFA enforcement, micro-segmentation, and endpoint isolation across user, device, and network layers.
- The system achieved sub-10-second MTTR for network-based attacks while reducing false positives compared to traditional static SIEM–SOAR pipelines.
- Future enhancements include distributed scalability, adaptive threshold tuning, self-learning playbooks, and expanded hybrid cloud Zero Trust enforcement.

References

- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*. doi:10.6028/NIST.SP.800-207.
- Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. doi:10.1109/ACCESS.2022.3159699.
- Marri, H., Patel, K., & Agarwal, P. (2024). Machine learning in SIEM systems: Enhancing threat detection capabilities. *IEEE Transactions on Information Forensics and Security, 19*, 250–270. doi:10.1109/TIFS.2023.3312345.
- Hariri, S., Moustafa, N., & Sitnikova, E. (2021). Adversarial machine learning in network intrusion detection: Current status and future challenges. *Neural Computing and Applications, 33*, 10231–10261. doi:10.1007/s00521-021-05920-0.

References

- Schlette, D., Empl, P., Caselli, M., Schreck, T., & Pernul, G. (2024). Do you play it by the books? A study on incident response playbooks and influencing factors. *IEEE Symposium on Security and Privacy*, 3625–3643. doi:10.1109/SP54263.2024.00074.
- Lin, P.-C., Chiu, Y.-H., & Chen, C.-H. (2019). Endpoint detection and response: A survey and open research issues. *IEEE Access, 7*, 170351–170365. doi:10.1109/ACCESS.2019.2953418.
- Guha, S., Mishra, N., Roy, G., & Schrijvers, O. (2016). Robust Random Cut Forest based anomaly detection on streams. *Proceedings of the 33rd International Conference on Machine Learning (ICML)*, 2712–2721.

THANK YOU