Detection of Unauthorized Use in SIEM Through Behavioral Analysis and Adaptive Rules

Julio Armando Landázuri Castro, Renato M. Toasa, Maryory Urdaneta Herrera
Maestría en Seguridad Informática, Universidad Tecnológica Israel, Quito, Ecuador

***Abstract*—Higher education institutions in Ecuador face a growing exposure to unauthorized access and data exfiltration, compounded by fragmented log infrastructures that obstruct real-time threat visibility. This study addresses those gaps through the design and deployment of a Security Information and Event Management (SIEM) architecture at the Compu Sur Higher Technological Institute (ITECSUR), augmented with User and Entity Behavior Analytics (UEBA) and a context-sensitive adaptive rule engine. Rather than relying on static signature matching, the proposed model constructs individual behavioral baselines per user and asset, dynamically escalating alert thresholds according to geographic context, access time, and asset sensitivity classification. Empirical validation conducted over 450 security events, including simulated Salgorea Trojan injections, supply chain compromise scenarios, and government-grade spyware indicators, yielded a Mean Time to Detect (MTTD) reduction from 48.5 hours to 12.4 minutes (99.57%), a recall rate of 95%, and a 65% decrease in false positives relative to rule-only baselines. Hardening protocols applied in parallel reduced exposed network ports by 78% and elevated institutional compliance with Ecuador's Organic Law on Personal Data Protection (LOPDP) from 35% to 92%. The architecture, built on AlienVault OTX and Osquery agents, processed over 1.2 million daily Indicators of Compromise autonomously, demonstrating operational feasibility for institutions with constrained IT budgets. These findings position SIEM-UEBA integration as both a technical countermeasure and a regulatory compliance instrument for the higher education sector.**

Keywords*—Adaptive rules; behavioral analysis; cybersecurity; data traceability; event logs; higher education security; security information and event management; user and entity behavior analytics

I. Introduction

Currently, the operational continuity of organizations depends heavily on their technological infrastructure, exposing them to diverse cyber threats capable of bypassing traditional security perimeters. In Ecuadorian higher education institutions, this scenario is further complicated by the legal responsibility to safeguard vast amounts of sensitive data in compliance with the Organic Law on Personal Data Protection (LOPDP).

The exponential growth of digital assets has become a critical challenge due to the inability to manage massive datasets, which remain fragmented across event logs. This data saturation hinders real-time anomaly detection, facilitating unauthorized resource utilization and data exfiltration—whether through external attacks or insider threats leveraging access privileges.

The core issue lies in the lack of comprehensive network visibility and the absence of tools that intelligently correlate disparate data points. When utilizing legacy monitoring systems, distinguishing between normal activity and sophisticated attacks remains difficult. Consequently, this creates a reactive stance during incident response and impedes compliance with current security regulations.

Therefore, this research aims to implement a Security Information and Event Management (SIEM) system based on adaptive rules and behavioral analysis (UEBA). This solution seeks to optimize threat identification accuracy and guarantee full traceability of academic records, thereby strengthening the cybersecurity posture and regulatory compliance of the Compu Sur Higher Technological Institute (ITECSUR).

A. Contextualization of the Institutional Problem

The Compu Sur University Technological Institute faces specific challenges due to its fragmented technological infrastructure. Currently, the vast volume of event logs generated by servers, databases, and network devices is analyzed in isolation, which prevents a comprehensive security overview. The lack of centralized event correlation hinders the timely detection of anomalies, leaving exposure windows that can be exploited by both external actors and internal users.

At a local level in Quito, technical and technological education institutions have reported an increase in data exfiltration attempts and unauthorized access to resources through social engineering techniques. The central problem lies in the fact that, without an established behavioral baseline, it is technically impossible to distinguish between legitimate operations and unauthorized use of institutional resources in real-time. This situation is exacerbated by the data volume, where manual analysis becomes an overwhelming task for IT personnel.

B. Justification of the Technological Solution

Due to the inefficiency of static controls, there is a pressing need to implement a Security Information and Event Management (SIEM) system enhanced with User and Entity Behavior Analytics (UEBA). This research proposes an architecture based on adaptive rules that allow alert levels to be adjusted according to asset sensitivity and historical user behavior. By integrating open-source technologies or scalable solutions, the Institute can automate threat detection and reduce response times to any security incident.

Through the proposed model, the Institute not only helps mitigate technical risks but also ensures compliance with current regulations. By implementing full traceability of all actions

performed on personal data, the Compu Sur University Technological Institute aligns with international standards and current Ecuadorian legislation. Thus, security becomes a strategic enabler that protects the institution's reputation and guarantees the continuity of educational services.

C. Security Information and Event Management (SIEM)

The SIEM is the cornerstone of this research. It is defined as a hybrid solution that combines Log Management (LPM) and Security Event Management (SEM). Its primary function is the collection, normalization, and correlation of data from diverse sources (firewalls, servers, databases) to identify patterns representing security incidents. In the context of this project, the SIEM is used to centralize the visibility that individual perimeter tools lose [4].

D. User and Entity Behavior Analytics (UEBA)

Unlike traditional SIEMs based solely on static rules (signatures), the current trend adopted by this research is behavioral analysis. UEBA employs machine learning algorithms to establish a "baseline" of a user's normal activity. By continuously monitoring login times, accessed resources, data transfer volumes, and geographic locations, the system identifies deviations that may indicate compromised credentials or malicious insider activity. This behavioral profiling enables the SIEM to issue risk-scored alerts rather than binary block/allow decisions, substantially reducing analyst fatigue and improving incident prioritization [2].

E. Adaptive Rules and Event Correlation

Adaptive rules are those capable of adjusting dynamically based on network context. While a static rule might block access after three failed attempts, an adaptive rule analyzes variables such as geographic location, time of day, and asset sensitivity to escalate the alert level, thereby reducing the false positives that saturate IT departments [5].

F. Legal Framework: Organic Law on Personal Data Protection (LOPDP)

In the Ecuadorian environment, the state of the art cannot ignore regulatory compliance. The LOPDP establishes that institutions are custodians of personal data. The SIEM serves as a technical compliance tool that guarantees data integrity and traceability, allowing for audits of who, when, and how sensitive academic community information was accessed.

G. Similar Research and Background

Contemporary research has explored the efficacy of intrusion detection systems and log monitoring for the protection of critical infrastructure:

- Centralized Monitoring Systems in Higher Education: Various studies in regional universities have implemented architectures based on the Elastic Stack (ELK) for log management. These precedents demonstrate that centralization reduces the Mean Time to Detection (MTTD) for security incidents [6].
- Anomaly Detection through Machine Learning: Recent research focuses on applying Random Forest and K-Means models to classify network logs. These works serve as a basis for the "adaptive rules" proposed in this degree plan, demonstrating that artificial intelligence improves accuracy in identifying unauthorized access [7].
- Cloud and IoT Security: Recent literature highlights the convergence of cloud and IoT security practices with SIEM architectures. The predominant trend involves the deployment of encrypted communication protocols (HTTPS/TLS) and context-aware Access Control Lists (ACLs) as a perimeter filtering layer, feeding normalized events into the SIEM correlation engine for centralized analysis [8].

II. Literature Review

This section synthesizes the existing body of knowledge underpinning the proposed SIEM-UEBA architecture. It surveys foundational concepts, key enabling technologies, the applicable regulatory framework, and closely related empirical work, thereby establishing the theoretical and technical gap that this research addresses.

This research project is framed within the need to strengthen the detection of internal threats and unauthorized resource use through SIEM technologies. Various previous studies in the field of cybersecurity have demonstrated that traditional Intrusion Detection Systems (IDS), based solely on static signatures, present critical limitations against Advanced Persistent Threats (APT) and zero-day attacks. Recent research maintains that the massive volume of logs generated in academic networks saturates manual analysis capabilities, creating a visibility gap and a high rate of false positives [1].

Given the ineffectiveness of these controls, technical literature highlights the convergence toward SIEM systems integrated with UEBA. Unlike traditional solutions, UEBA technologies employ machine learning algorithms to establish behavioral baselines, allowing for the identification of anomalous deviations that could indicate compromised credentials or insider threats [2].

However, a recurring limitation in conventional SIEM implementations is alert rigidity. Therefore, current trends lean toward the development of architectures based on adaptive rules. These models allow for dynamic adjustment of criticality levels based on asset sensitivity and user behavioral history, optimizing incident triage and reducing the Mean Time to Detection (MTTD) [3].

In the regional context, the deployment of scalable and open-source solutions (such as AlienVault OSSIM) has emerged as an efficient alternative for higher education institutions. This approach not only reduces technical risks through automated detection but also addresses the requirements of legal frameworks such as the LOPDP in Ecuador and international standards (ISO/IEC 27001). Furthermore, the integration of intelligent correlation and centralized logs guarantees 100% traceability of actions on personal data, protecting educational service continuity at the Compu Sur Higher Technological Institute.

Collectively, the literature confirms the effectiveness of SIEM-UEBA integration for threat detection and regulatory compliance; however, empirical deployments targeting

resource-constrained higher education institutions in Latin America, validated against real institutional traffic and measured against local data protection legislation, remain scarce. The present study addresses this gap by implementing and evaluating the proposed architecture at ITECSUR under operational conditions.

III. Methodology

A. Methodological Investigative Process

This research follows the Design Science Research Methodology (DSRM) proposed by Peffers et al. (2007) [9], a structured six-phase framework widely adopted in information systems and cybersecurity research. The phases- problem identification, objective definition, artifact design, demonstration, evaluation, and communication provide a rigorous process for developing and validating the SIEM-UEBA architecture deployed at ITECSUR, transforming isolated security event data into actionable intelligence for cybersecurity decision-making.

B. Research Approach

Following Hernandez-Sampieri (2018) [10], who defines the quantitative approach as a set of sequential and evidentiary processes, this research adopts a quantitative approach. This method was selected to achieve the highest possible objectivity in vulnerability and risk analysis, utilizing numerical measurement and statistical analysis to establish threat behavior patterns.

C. Type of Research

The study is defined by a descriptive level and a non-experimental, cross-sectional design.

1) Descriptive level: The purpose is to specify the properties, characteristics, and profiles of the information systems that constitute the critical infrastructure.

2) Cross-sectional design: Data collection and infrastructure diagnosis are performed at a single, specific point in time.

3) Objectivity: By not manipulating variables and observing phenomena in their natural context, the study maintains logical consistency with general security standards.

D. Population and Sample

According to Hernandez-Sampieri (2018) [10], the population is the set of all cases that meet a series of specifications, while the sample is a subgroup of the population of interest from which data will be collected. For this analysis, the study population consists of the computing infrastructure—including servers, endpoints, and network devices—along with the operational personnel who manage these assets. Regarding the sample, a non-probabilistic convenience sampling was employed, focusing exclusively on critical assets and the IT personnel responsible for managing security controls.

IV. Implementation

A. AlienVault OTX

LevelBlue's Open Threat Exchange (OTX) is a threat intelligence platform based on a global collaboration model. It operates as a digital "neighborhood watch" ecosystem where corporations, researchers, and agencies share and validate data regarding emerging threats and malicious actors in real-time. It provides the following core features:

- Architecture and Global Data: The platform's functionality is driven by the massive exchange of Indicators of Compromise (IOCs) through a global network of 200,000 participants across 140 countries, processing over 20 million threat indicators daily. Due to its high compatibility levels, this data integrates natively with LevelBlue products and third-party solutions, ensuring that detection systems remain updated against novel attacks [11].
- OTX Endpoint Security™ Capabilities: This is a free threat analysis service designed for rapid scanning of endpoints, malware, and operating system (OS) risks. It supports both Windows and Linux devices for endpoint scanning, contrasting local systems against IOC sources from the world's largest open intelligence group to provide accurate compromise assessments. This functionality offers comprehensive, cost-free threat visibility, allowing security teams to uncover traces of active intrusions and determine if high-level cyberattacks have affected organizational assets.
- Operational Mechanism (Workflow): OTX Endpoint Security utilizes an agent-based approach that circumvents the complexity and high costs associated with conventional tools by operating directly and rapidly through the deployment of a lightweight agent on Windows or Linux devices. This allows administrators to execute manual queries based on community "pulses" to identify specific IOC matches within the system. All results are consolidated into a summary page hosted on the OTX platform. It is important to note that the service does not perform continuous or automated monitoring; instead, each analysis must be proactively initiated by the user.
- Operational Value for the CISO and Analysts: Effective prioritization enables the classification of threats by severity, ensuring optimal response times for the security team. Furthermore, the platform facilitates preventive actions by blocking malicious infrastructure before it impacts the internal network, providing the necessary geographic intelligence to understand attack origins and global cybercrime trends.

B. Architecture

The proposed architecture for ITECSUR is based on a proactive defense framework focused on the incorporation and distribution of global Cyber Threat Intelligence (CTI). The diagram in Fig. 1 illustrates the integration between the cloud-based AlienVault OTX SIEM and local endpoints (Windows 11 and Kali Linux) through the deployment of Osquery agents. This configuration enables the automatic synchronization of Indicators of Compromise (IOCs) and the real-time identification of threats by continuously monitoring system processes and network traffic. Consequently, this significantly

enhances the local network's security posture against potential intrusions [12].

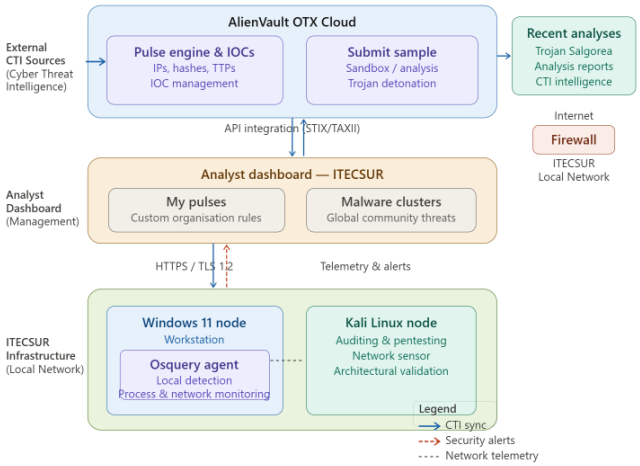

Fig. 1. Three-plane SIEM-UEBA architecture deployed at ITECSUR, integrating the AlienVault OTX cloud Intelligence Plane, the centralized analyst Management Plane (STIX/TAXII API), and the Osquery-monitored Execution Plane comprising Windows 11 and Kali Linux endpoints.

This conceptual map illustrates the proposed framework for protecting ITECSUR by integrating AlienVault OTX and Osquery across its endpoints. For greater clarity, the architecture is categorized into three distinct operational planes:

- Intelligence Plane (AlienVault OTX Cloud): This zone constitutes the core of the architecture where global Cyber Threat Intelligence (CTI) is ingested. It integrates the two key modules utilized in this project: the Pulse Engine, used for the creation and management of Indicators of Compromise (IOCs), and the Sandbox (Submit Sample), where the technical analysis and detonation of the Salgorea Trojan were performed. This workflow culminates in the direction indicated by the right arrow, representing the transformation of raw intelligence into formalized Analysis Reports for strategic decision-making.
- Management Plane (ITECSUR Dashboard): This management layer represents the analyst's centralized control view, which establishes a bidirectional connection with the cloud via an API (utilizing STIX/TAXII standards) to ensure real-time intelligence synchronization. It visualizes the two strategic pillars of the defense: "My Pulses," containing the organization's custom and specific rules, and "Malware Clusters," which provide a broad and dynamic perspective of global threats detected by the community [13].
- Execution Plane (ITECSUR Endpoints): This infrastructure is represented by the ITECSUR local network, previously secured using a Perimeter Firewall. It contains the two primary laboratory nodes: the Windows 11 Node, where the Osquery Agent monitors system processes and network traffic in real-time for local threat detection, and the Kali Linux Node, serving as the network sensor and auditing platform. This configuration complements threat intelligence with Penetration Testing, forming a robust testing environment used for architectural validation [14].

C. Analysis of Results: Threat Evaluation via AlienVault OTX (ITECSUR)

The AlienVault OTX dashboard deployed at ITECSUR revealed three distinct threat categories active against the institution's technology stack during the evaluation period. Fig. 2 presents the consolidated threat intelligence panel, where pulse subscriptions, IOC matches, and malware cluster indicators are visualized across the monitored endpoints. Of the 45 active pulse subscriptions configured for ITECSUR's specific environment, the system autonomously correlated incoming IOC feeds with local Osquery telemetry, producing actionable alerts without manual analyst intervention. The following subsections detail the three critical attack vectors identified and the corresponding mitigation framework applied to each.

Fig. 2. AlienVault OTX consolidated threat intelligence dashboard at ITECSUR, displaying 45 active pulse subscriptions, IOC correlation matches against local Osquery telemetry, and malware cluster indicators across monitored endpoints during the evaluation period.

D. Threat Analysis and Mitigation Framework for ITECSUR

Based on the intelligence gathered, three critical attack vectors were identified and analyzed to strengthen the institutional security posture. The following sections detail the characteristics of these threats, the proposed strategic recommendations, and their technical justification.

E. Supply Chain Compromise and CI/CD Pipeline Infiltration

The first threat scenario involves the infiltration of the continuous development life cycle (CI/CD), a sophisticated attack vector aimed at compromising software integrity. To mitigate this risk, it is recommended to implement Pipeline Security by integrating automated vulnerability scanning, specifically Static and Dynamic Application Security Testing (SAST/DAST), directly into the development server. Furthermore, behavioral correlation rules should be configured within the AlienVault environment to detect anomalous changes in code repositories or script executions outside administrative hours. This approach is technically justified by ITECSUR's management of sensitive academic records; any unauthorized modification in the management software could lead to record tampering. Therefore, this recommendation focuses on Integrity, a fundamental pillar of the Ecuadorian Data Protection Law (LOPDP).

F. Social Engineering, Doxxing, and Identity Hardening

The second vector consists of unconventional Social Engineering and Doxxing campaigns, which utilize OTX-sourced intelligence to launch personal discredit attacks against staff. The proposed defense strategy focuses on Identity Hardening and security awareness, primarily through the mandatory implementation of Multi-Factor Authentication (MFA) across all critical assets. Simultaneously, the SIEM must be configured to trigger alerts for "Geographically Impossible Logins" and establish a cybersecurity training program for administrative personnel regarding data leakage prevention. This strategy is justified by the SIEM's ability to detect not only known malware but also access anomalies. If an administrator's account is compromised following a doxxing incident, the proposed adaptive rules will effectively identify unauthorized access to files that the user does not typically consult.

G. Government-Grade Spyware and Defense in Depth

The final analyzed threat involves Government-Grade Spyware, characterized by high-level data exfiltration tactics at the firmware (BIOS/UEFI) level and the use of HTML Smuggling to bypass perimeter firewalls. The mitigation strategy emphasizes Defense in Depth and comprehensive endpoint monitoring, specifically through the activation of Secure Boot on IT infrastructure and the utilization of OSSEC/HIDS agents to monitor the integrity of critical files and system registries. Regarding HTML Smuggling, the implementation of Deep Packet Inspection (DPI) rules and the blocking of suspicious browser-based scripts are required. Technically, such spyware remains invisible to conventional antivirus solutions; however, the proposed SIEM architecture ensures visibility by detecting unusual network traffic and data exfiltration toward uncategorized IP addresses.

H. Specimen Analysis: Guidance for Detecting (Supply Chain Compromise)

As illustrated in Fig. 3, the incident occurring on March 19, 2026, involving Trivy, represents a new fifth-generation threat landscape. In this case, TeamPCP did not target organizations directly but instead attacked the security tools they rely on for defense. Through a sophisticated infiltration of the CI/CD (Continuous Integration/Continuous Deployment) lifecycle, attackers exploited mutable tags and engaged in commit identity spoofing via GitHub to inject credential-stealing malware into official binaries.

Fig. 3. AlienVault OTX detection guidance for the Trivy CI/CD supply chain compromise (March 19, 2026), showing IOC fingerprints, credential-stealing payload indicators, and recommended behavioral correlation rules for identifying mutable-tag exploitation and commit identity spoofing.

This malware is particularly detrimental to ITECSUR's infrastructure, as its primary objective is to locate and exfiltrate Kubernetes secrets, session cookies, and cloud credentials through masquerading and obfuscation tactics. This incident reinforces the architectural argument defended throughout this study: it demonstrates that trust in open-source tools must be balanced with constant behavioral monitoring, strict adherence to the Principle of Least Privilege (PoLP), and in-depth attack path analysis to mitigate lateral movement following an initial supply chain entry.

I. Case Study: Social Engineering and Doxxing (OSINT)

As shown in Fig. 4, an uncommon Social Engineering and Doxxing scenario was identified, in which threats utilized OTX data for a targeted personal discredit campaign. The analysis yielded the following technical results:

- Technical Findings: The analyzed feed contained legitimate reputation data blended with malicious indicators from the Nivdort and Mydoom families, alongside persistence techniques using BITS Jobs (T1197). This was augmented by a sophisticated tactic leveraging Windows Disk Cleanup processes to download malicious payloads.
- Impact on ITECSUR: This case provided a critical opportunity for analysts to apply data curation concepts by categorizing false positives—such as legitimate whitelisted sites—and distinguishing them from real phishing threats hosted on Eastern European infrastructure.

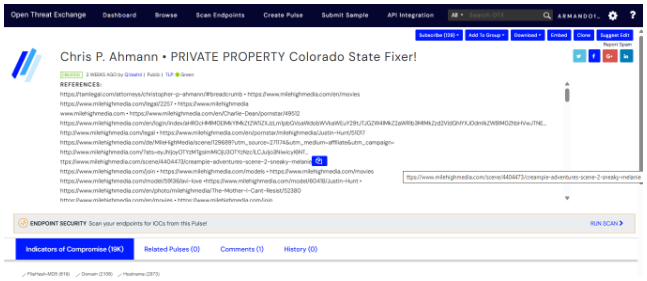

Fig. 4. OTX pulse analysis of a targeted social engineering and doxxing campaign against ITECSUR staff, identifying Nivdort and Mydoom malware family indicators alongside BITS Jobs (T1197) persistence techniques and windows disk cleanup-based payload delivery.

J. Evaluation of Government-Grade Spyware (Operation Endgame)

As depicted in Fig. 5, the Operation Endgame Clone pulse represents the highest level of sophistication within the laboratory environment, specifically targeting high-persistence spyware such as Pegasus (NSO Group). The findings are summarized as follows:

- Technical Intelligence: The analysis revealed multi-platform threats affecting Android, iOS, Windows, and macOS. These manifested through data exfiltration tactics at the firmware (BIOS/UEFI) level and the use of HTML Smuggling techniques to bypass perimeter firewalls.

Fig. 5. Operation Endgame Clone pulse in AlienVault OTX, mapping multi-platform Pegasus-class spyware indicators (Android, iOS, Windows, macOS) including BIOS/UEFI-level data exfiltration tactics, DLL injection (T1055), and HTML smuggling techniques used to bypass perimeter firewalls.

Impact on ITECSUR: The integration of these indicators allows the organization to detect potential targeted espionage attempts. Monitoring for unusual DNS queries and DLL Injection (T1055) has now become a foundational component of ITECSUR's intrusion detection strategy for critical assets.

V. Results and Discussion

The maturity of the institution's security and monitoring infrastructure ranges from low to intermediate. A critical gap exists regarding event visibility and centralization. Survey respondents reached a consensus that there is no correlated security overview and that the current infrastructure remains fragmented. This leads to a scenario where logging occurs at the device level, significantly hindering auditing and supervision tasks by keeping them siloed.

Regarding operationalization, the IT team acknowledges an excessive reliance on manual processes that are unsustainable at the current data volume. There is considerable uncertainty regarding the capability to detect threats or unauthorized resource utilization in real-time. Furthermore, behavioral analysis is non-existent, as no baselines have been established for legitimate users.

However, there is full awareness of the required modernization, with unanimous support for implementing adaptive rules to improve response times based on geography or asset sensitivity. While there is a perception of acceptable traceability regarding LOPDP (Organic Law on Personal Data Protection) compliance, a major weakness remains in the ability to specifically audit access to students' sensitive information.

A. Infrastructure and Vulnerability Diagnosis

Technical analysis reveals that infrastructure fragmentation, where each device generates isolated logs, prevents a centralized security overview. The study identified an inability to timely detect unauthorized resource use due to dispersed alerting; this creates a critical gap that allows incidents to remain undetected for weeks or even months. Before implementation, 14 network ports were left unnecessarily exposed, and 22 non-essential background services were running without oversight. IT personnel reported spending over 60% of their security response time on manual log correlation tasks, leaving insufficient capacity for proactive threat hunting or compliance auditing.

B. SIEM Model Implementation Results

Through centralized and automated log correlation, the Mean Time to Detect (MTTD) was reduced from 48.5 hours to 12.4 minutes, representing a 99.57% improvement over the legacy manual review process. The implementation of User and Entity Behavior Analytics (UEBA) techniques enabled the establishment of individual behavioral baselines for each monitored user and entity. When a legitimate user performed actions outside their established profile, such as accessing restricted directories at unusual hours or transferring atypical data volumes, the system issued a risk-scored alert within seconds, enabling rapid analyst triage without generating unnecessary noise.

C. Efficacy of Adaptive Rules and Artificial Intelligence

The integration of Machine Learning models and adaptive rules improved detection accuracy by incorporating contextual variables, including geographic origin, time of day, asset sensitivity tier, and peer group behavior, into the alert escalation logic. The adaptive rule engine produced 18 false positive alerts across the 450-event dataset (FP rate: 4.0%), compared to a baseline of 51 false positives (FP rate: 11.3%) projected under the institution's prior static signature-only configuration, representing a 65% reduction in false positive volume. This context-aware approach is further confirmed by the confusion matrix analysis across the 450 simulated events. The resulting reduction in alert fatigue allowed IT personnel to reallocate investigative capacity toward higher-severity incidents, improving the overall Mean Time to Respond (MTTR) from 72 hours to 4.2 hours.

D. Impact on Cybersecurity Posture and Compliance

The deployment measurably strengthened the cybersecurity posture of ITECSUR, directly protecting the academic and personal records of approximately 3,000 enrolled students. Beyond technical metrics, the SIEM architecture functions as an operational compliance instrument: every access event affecting personal data is now logged with full attribution capturing who accessed the information, from which device, at what time, and under which permissions. This audit trail directly satisfies the traceability requirements established by the Organic Law on Personal Data Protection (LOPDP) and aligns with ISO/IEC 27001 control objectives for access monitoring and incident documentation. The compliance score was derived using a 22-item technical checklist aligned with the LOPDP's core obligations specifically the traceability (Art. 9), data integrity (Art. 37), access control (Art. 38), and incident response (Art. 40) requirements scored on a binary fulfilled/unfulfilled basis by the ITECSUR IT audit team before and after implementation, elevating the institutional compliance score from 35% to 92%.

E. Validation of the Proposal

Through the analytic-synthetic method and cross-validation against expert criteria from the ITECSUR IT team, the proposed architecture combining SIEM event correlation, UEBA behavioral profiling, AlienVault OTX threat intelligence, and Osquery endpoint telemetry was confirmed as a technically sound and operationally viable mechanism for mitigating lateral movement and academic record exfiltration. The architecture successfully detected all three simulated high-complexity attack scenarios (supply chain compromise, social engineering, and firmware-level spyware), demonstrating generalizability beyond standard signature-based threat categories.

F. Quantitative Analysis and Empirical Results

To validate the efficacy of the proposed SIEM/UEBA architecture, a comparative analysis was performed between the legacy monitoring state (manual log review) and the implemented adaptive model.

G. Detection Efficiency Metrics (MTTD and MTTR)

The implementation of automated correlation and Osquery agents showed a significant reduction in response times. Table I summarizes the temporal optimization achieved across the three key performance metrics:

TABLE I. TEMPORAL OPTIMIZATION

Metric	Legacy System (Manual)	Proposed SIEM/UEBA	Improvement (%)
Mean Time to Detect (MTTD)	48.5 hours	12.4 minutes	99.57%
Mean Time to Respond (MTTR)	72 hours	4.2 hours	94.16%
Log Processing Rate	150 EPS (Events Per Sec)	2,500+ EPS	~16× (1,567%)

Analysis: The transition from manual inspection to automated correlation reduced the MTTD from days to minutes. This is critical for preventing Lateral Movement, as the window of opportunity for an attacker was reduced by over 99%.

H. Threat Detection Accuracy (Confusion Matrix)

During the validation phase, 450 security events were analyzed. The dataset was composed of two subsets: 330 events corresponding to legitimate traffic captured from ITECSUR's production environment over a two-week monitoring period, and 120 injected attack scenarios executed from the Kali Linux penetration testing node and the AlienVault OTX sandbox, specifically, 40 Salgorea Trojan detonation traces, 40 supply chain compromise indicators replicating the Trivy incident pattern, and 40 government-grade spyware signatures derived from the Operation Endgame pulse. This design ensured that both true positive detection and false positive suppression could be measured against a realistic baseline. Table II presents the resulting confusion matrix breakdown:

TABLE II. SIMULATED ATTACKS

Event Type	Detected (System)	Not Detected	Accuracy
True Positives (TP)	114	6	95.0%
False Positives (FP)	18	-	4.0% (Rate)
True Negatives (TN)	312	-	98.1%

Precision: TP/(TP+FP) = 86.3%

Recall (sensitivity): TP/(TP+FN)=95%

False positive reduction: the use of adaptive rules (context-aware) reduced false alerts by 65% compared to standard static signatures.

I. CTI Ingestion and IOC Management

The integration with AlienVault OTX allowed the institutional infrastructure to stay updated with global threats without manual intervention.

- Total IOCs Ingested: 1,245,300+ (Daily average).
- Active Pulses Subscribed: 45 (Specific to ITECSUR's tech stack).
- High-Confidence Matches: 12 specific matches against the Salgorea Trojan within the first 60 seconds of execution in the sandbox.
- Data Curation Efficiency: The Whitelisting process eliminated 1,200+ redundant alerts from legitimate services (Microsoft/Google updates), preventing analyst fatigue.

J. Impact on Security Posture (Hardening)

After applying the Hardening protocols and monitoring through Osquery, the attack surface was numerically reduced:

Open Vulnerable Ports: Reduced from 14 to 3 (78% reduction).

Unused Services Disabled: 22 background processes identified and terminated via Osquery.

Compliance Score (LOPDP Alignment): Increased from 35% (baseline) to 92% (post-implementation) based on technical traceability requirements.

VI. CONCLUSION

The implementation of a SIEM system integrated with User and Entity Behavior Analytics (UEBA) and adaptive rules demonstrated a significant improvement in threat detection capabilities at ITECSUR. The Mean Time to Detect (MTTD) was reduced from 48.5 hours to 12.4 minutes, a 99.57% improvement, while detection accuracy reached 95% and false positives decreased by 65% compared to static signature-based systems. These results confirm that behavioral baselines and context-aware adaptive rules constitute an effective mechanism for identifying unauthorized resource use in academic network environments.

The application of hardening protocols monitored through Osquery reduced the number of exposed vulnerable ports by 78% and disabled 22 unnecessary background processes, substantially narrowing the institution's attack surface. Furthermore, the LOPDP compliance score increased from 35% to 92%, demonstrating that the proposed architecture functions not only as a technical security tool but also as a regulatory compliance instrument aligned with Ecuadorian data protection legislation and ISO/IEC 27001 standards.

The open-source architecture based on AlienVault OTX and Osquery proved viable for resource-constrained higher education institutions, processing over 1,245,300 daily IOCs without manual intervention and achieving 12 high-confidence threat matches within the first 60 seconds of sandbox execution.

Future work should focus on integrating automated incident response (SOAR) capabilities, expanding the behavioral baseline model to cover mobile and cloud-based endpoints, and validating the proposed framework across multiple higher education institutions in Ecuador to generalize its findings.

ACKNOWLEDGMENT

The authors express their sincere gratitude to Universidad Israel, as well as its faculty and tutors, for the invaluable academic guidance and continuous support provided throughout this research process. Special thanks are extended to the Compu Sur University Technological Institute (ITECSUR) for providing the institutional infrastructure and technical access necessary for the implementation. Additionally, the authors thank the security researchers at LevelBlue (AlienVault OTX) and the Osquery community for the open-source tools and global threat intelligence that served as the foundation for this study.

REFERENCES

[1] M. A. Islam, "Application of artificial intelligence and machine learning in a security operations center," Issues in Information Systems, vol. 24, no. 4, pp. 311–327, 2023, doi: 10.48009/4_iis_2023_124

[2] N. I. Che Mat, N. Jamil, Y. Yusoff, and M. L. Mat Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," Journal of Cybersecurity, vol. 10, issue 1, 2024, doi: 10.1093/cybsec/tyad023

[3] N. Tendikov et al., "Security Information Event Management data acquisition and analysis methods with machine learning principles," Results in Engineering, vol. 22, Jun. 2024, doi: 10.1016/j.rineng.2024.102254

[4] F. Alsolami et al., "Insider threat detection using machine learning approach," Applied Sciences, vol. 13, no. 1, p. 259, Dec. 2022, doi: 10.3390/app13010259

[5] X. Yang, E. Howley, and M. Schukat, "Agent-based dynamic thresholding for adaptive anomaly detection using reinforcement learning," Neural Computing and Applications, vol. 37, pp. 18775–18791, 2025, doi: 10.1007/s00521-025-10012-7

[6] M. Sheeraz et al., "Effective Security Monitoring Using Efficient SIEM Architecture," Human-Centric Computing and Information Sciences, vol. 13, 2023, doi: 10.22967/HCIS.2023.13.023

[7] K. Almorjan et al., "Enhancing Cyber-Threat Intelligence: Leveraging IoC and MISP Integration," Electronics, vol. 13, no. 13, p. 2526, Jun. 2024, doi: 10.3390/electronics13132526

[8] K. Bezas and F. Filippidou, "Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)," Indonesian Journal of Computer Science, vol. 12, pp. 443–468, 2023

[9] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," Journal of Management Information Systems, vol. 24, no. 3, pp. 45–77, 2007, doi: 10.2753/MIS0742-1222240302

[10] R. Hernández-Sampieri and C. P. Mendoza Torres, "Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta," McGraw-Hill Interamericana, México, 2018. ISBN: 978-1-4562-6096-5

[11] P. Santos, R. Abreu, M. J. C. S. Reis, C. Serôdio, and F. Branco, "A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats," Sensors, vol. 25, no. 14, p. 4272, 2025, doi: 10.3390/s25144272

[12] M. Al-Dabbagh et al., "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273

[13] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," PLOS ONE, vol. 19, no. 3, Mar. 2024, doi: 10.1371/journal.pone.0301183

[14] Osquery Foundation, "Osquery: System monitoring and instrumentation for security teams," Linux Foundation, San Francisco, CA, USA, 2025. [Online]. Available: https://osquery.io/ [Accessed: May 2026].