HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 17, Sayı: 35, 296-314, 2026
Gönderilme Tarihi: 25 Mayıs 2026 Kabul Tarihi: 24 Haziran 2026

Research Article

INTEGRATING CONTINUOUS AUDITING INTO SOC OPERATIONS: AN AUDIT-DRIVEN THREAT MONITORING FRAMEWORK

(SÜREKLİ DENETİMİN SOC OPERASYONLARINA ENTEGRASYONU: DENETİM ODAKLI TEHDİT İZLEME MODELİ)

Kübra ASLAN[1,4], Azze ÖZEL[2,4], Onur CERAN[3]

ABSTRACT

This article develops a model that integrates real-time Security Operations Center (SOC) log analytics with continuous auditing processes and aims to bridge the technical gap between operational threat monitoring activities and the internal audit function. Although SOC units generate high volumes of data, including authentication records, network traffic, and endpoint activities, these data sources are not systematically used in internal audit activities. The developed structure treats real-time log streams as audit evidence for assessing control effectiveness, identifying risk indicators, and analyzing deviations. Within this scope, SOC rules, audit tests, and risk scenarios are linked within an integrated structure. Methodologically, the study is based on the Design Science Research (DSR) approach. To evaluate the feasibility of the model, a virtualized three-host SOC environment was designed and implemented. The model was tested through a proof-of-concept scenario based on privileged access activities occurring outside business hours. The findings indicate that log-level visibility reduces blind spots in internal audit, strengthens control design, and supports a proactive governance approach, particularly in sectors with high security requirements such as the defense industry.

Keywords: Continuous Auditing, SOC, Log Analytics, Internal Audit, Cybersecurity
JEL Codes: M42, C88, L86

ÖZ

Makalede, gerçek zamanlı Güvenlik Operasyon Merkezi (SOC) log analizlerini sürekli denetim süreçleriyle bütünleştiren ve operasyonel tehdit izleme faaliyetleri ile iç denetim fonksiyonu arasındaki teknik boşluğu kapatmayı amaçlayan bir model geliştirilmektedir. Günümüzde SOC birimleri, kimlik doğrulama kayıtları, ağ trafiği ve uç nokta aktiviteleri gibi yüksek hacimli veriler üretmesine rağmen, bu veriler iç denetim faaliyetlerinde sistematik olarak kullanılmamaktadır. Geliştirilen yapı, gerçek zamanlı log akışlarını kontrol etkinliğinin değerlendirilmesi, risk göstergelerinin belirlenmesi ve sapma analizlerinin yürütülmesi açısından denetim kanıtı olarak ele almaktadır. Bu kapsamda SOC kuralları, denetim testleri ve risk senaryoları bütünleşik bir yapı içerisinde ilişkilendirilmektedir. Yöntemsel olarak çalışma, Tasarım Bilimi Araştırması (Design Science Research - DSR) yaklaşımına dayanmaktadır. Modelin uygulanabilirliğini değerlendirmek amacıyla sanallaştırılmış üç sunuculu bir SOC ortamı tasarlanmış ve uygulanmıştır. Model, mesai saatleri dışında gerçekleştirilen ayrıcalıklı erişim faaliyetlerini temel alan bir kavram kanıtlama (proof-of-concept) senaryosu üzerinden test edilmiştir. Elde edilen bulgular, log seviyesindeki görünürlüğün iç denetimdeki kör noktaları azalttığını, kontrol tasarımını güçlendirdiğini ve özellikle savunma sanayi gibi yüksek güvenlik gereksinimi bulunan sektörlerde proaktif bir yönetişim yaklaşımını desteklediğini göstermektedir.

Anahtar Kelimeler: *Sürekli Denetim, SOC, Log Analitiği, İç Denetim, Siber Güvenlik*
JEL Kodları: *M42, C88, L86*

[1] Lider Denetçi, ASELSAN A.Ş., İç Denetim Başkanlığı, BT ve Bilgi Güvenliği Denetim Birimi, 0009-0005-4457-0421, 25833904005@gazi.edu.tr
[2] Siber Güvenlik Uzmanı, UITSEC International Bilgi Teknolojileri A.Ş., Siber Güvenlik Operasyon Merkezi, 0009-0005-2702-711X, 25833901008@gazi.edu.tr
[3] Doç. Dr., Gazi University, Faculty of Applied Sciences, Department of Management Information Systems, Ankara, Türkiye, 0000-0003-2147-0506, onur.ceran@gazi.edu.tr
[4] Information Security Engineering, Graduate School of Natural and Applied Sciences, Gazi University, Ankara, Turkey

1. INTRODUCTION

In today's rapidly evolving cybersecurity landscape, organizations face increasingly sophisticated threats that require continuous monitoring, rapid detection, and proactive response mechanisms. Security Operations Centers (SOC) have emerged as critical organizational units responsible for real-time threat detection and operational security monitoring. At the same time, internal audit functions are expected to provide assurance regarding the effectiveness of control mechanisms, risk management processes, and governance structures.

Despite these developments, a significant disconnect remains between SOC operations and internal audit practices. While SOC units generate high-volume, real-time log data—including authentication logs, endpoint activities, and network events—these data sources are rarely utilized systematically within internal audit processes. Instead, internal audit practices often rely on periodic assessments, document reviews, and retrospective evaluations, limiting their ability to provide timely and data-driven assurance.

The literature reflects this fragmentation. SOC-oriented studies primarily focus on technical detection capabilities, log visibility, and threat intelligence frameworks such as MITRE ATT&CK, whereas internal audit research emphasizes governance, control design, and risk assessment. Similarly, continuous auditing literature highlights automation and monitoring but lacks a structured integration with real-time SOC log streams. This gap indicates the absence of a holistic framework that connects operational security data with audit evidence generation and control evaluation processes.

To address this gap, an integrated framework is developed to enable the use of real-time log analytics as audit evidence within continuous auditing processes. The central aim is to demonstrate how SOC-generated data can be systematically mapped to audit controls, risk indicators, and performance metrics, thereby transforming operational security outputs into auditable insights.

Accordingly, the research is guided by the following questions: how real-time log analytics can support continuous auditing activities; how SOC operations and internal audit functions can be integrated both technically and operationally; and how log-based outputs can be transformed into measurable audit indicators reflecting control effectiveness and risk levels. Furthermore, the study aims to evaluate the organizational and technical requirements necessary for implementing such an integrated model in high-security environments.

For this purpose, a Design Science Research (DSR) methodology is adopted, and a framework based on a virtualized SOC environment is developed. The proposed model integrates log collection, correlation mechanisms, and audit evaluation processes into a unified structure, enabling continuous and evidence-based auditing.

By connecting SOC operations with internal audit functions, the article contributes to the literature through an audit-driven threat monitoring approach. The approach not only enhances real-time risk visibility but also repositions the internal audit function as an active and data-driven component of cybersecurity governance.

2. LITERATURE REVIEW

A substantial body of literature exists in the fields of cybersecurity, continuous auditing, and data analytics. These studies indicate that these disciplines have largely evolved independently, each addressing its own research problems. SOC-oriented research focuses predominantly on increasing operational visibility, expanding the scope of log sources, and strengthening detection capabilities through threat frameworks such as MITRE ATT&CK. Studies conducted within this scope enhance the technical defense competencies of institutions and support incident response processes (Chamkar, Maleh & Gherabi, 2024; Le et al., 2025).

In contrast, research on continuous auditing and compliance mainly addresses automated control testing, policy compliance, configuration monitoring, and process continuity. This line of research suggests that the audit function should move beyond periodic approaches and increasingly rely on technology-aided assurance mechanisms (Torkura et al., 2021; Kestane, 2021). However, many of the audit mechanisms discussed in this literature are not explicitly linked to the high-volume, real-time log streams produced in SOC environments. In addition, the literature does not provide a technical-level explanation of how operational security outputs can be incorporated into audit processes. The foundations of continuous auditing extend beyond automated compliance testing and rely on the continuous or near-continuous collection and evaluation of digital evidence. Early and subsequent studies in this field demonstrate that automated monitoring, exception reporting, and analytic procedures can reduce the time between the occurrence of a control deviation and its identification by the audit function (Vasarhelyi & Halper, 1991; Vasarhelyi et al., 2004; Alles

et al., 2008). Prior studies establish the theoretical basis for data-driven and technology-supported assurance. However, they primarily focus on financial transactions, business processes, and automated control environments, while the systematic use of real-time SOC telemetry as continuous internal audit evidence remains insufficiently explored.

Research on log analytics and anomaly detection offers advanced technical approaches, including big data processing infrastructures, machine learning-based prediction models, and synthetic data generation (Reddy, 2024; Danish, 2025; Huang et al., 2024). These studies primarily aim to improve the timeliness and accuracy of threat detection. However, these technical outputs are primarily designed for operational decision-support mechanisms; their transformation into auditable evidence, measurement of control effectiveness, or continuous auditing indicators remains outside the scope of such research. This situation is a natural consequence of focusing on different problem domains rather than a deficiency in the respective studies.

The internal audit literature primarily examines cybersecurity through the lenses of governance, organizational structure, risk management, and institutional capacity. Risk-oriented audit frameworks and cyber maturity models strengthen the strategic role of internal audit; however, the integration of SOC workflows, SIEM correlation rules, and real-time log analyses into audit tests is addressed only to a limited extent (Antunes et al., 2022; Islam et al., 2018). Nevertheless, studies examining the relationship between audit policies and technical monitoring outputs reveal that log analysis is a critical input not only for operational security but also for audit assurance (Behloul et al., 2015). The transformation of security logs into audit evidence also requires a control and governance foundation. NIST SP 800-92 emphasizes that centrally collected and consistently managed log records support accountability, incident analysis, and the verification of security-related activities (Kent & Souppaya, 2006). From an internal control perspective, the monitoring component of the COSO Internal Control Framework provides a basis for assessing whether controls remain present and continue to operate effectively over time (COSO, 2013). At the organizational level, the IIA Three Lines Model establishes that operational functions and internal audit may exchange risk-relevant information, provided that internal audit does not assume management responsibilities and maintains its independent assurance role (IIA, 2020). Taken together, these approaches indicate that SOC-generated data may support continuous assurance. Such evidentiary use, however, depends on appropriate log governance, access controls, and clearly defined organizational responsibilities.

Recent bibliometric analyses demonstrate a growing convergence among audit, compliance, and cybersecurity research, indicating increasing interest in integrating technical data sources into audit methodologies (Tharwat et al., 2025). Taken together, prior research points to a critical gap in the structured and auditable integration of real-time operational security data into internal audit processes. Although existing studies emphasize the importance of continuous auditing and advanced log analytics, they largely remain confined to their respective domains and do not establish a systematic linkage between technical security outputs and audit assurance mechanisms. This fragmentation limits the ability of internal audit functions to leverage real-time data for evaluating control effectiveness and risk exposure. Accordingly, the present article develops an audit-driven threat monitoring framework that bridges SOC operations and internal audit processes by transforming log-level outputs into audit-relevant insights and enabling a data-driven, proactive audit approach.

3. CONCEPTUAL FRAMEWORK

Prior research in cybersecurity, SOC operations, continuous auditing, and log analytics is technically mature and extensive. However, the majority of these studies focus either on the operational security and threat detection perspective or address audit and compliance processes primarily at the level of governance, policy, and control design. As criticism of periodic and document-based audit approaches has increased, interest in using real-time technical data in audit activities has also grown (Tharwat et al., 2025). These developments indicate that internal audit should evolve from a primarily retrospective assurance function into a dynamic and technology-aided role.

SOC-centric research, by comparison, contributes significantly to log coverage, correlation rule development, and operational visibility through threat models such as MITRE ATT&CK. Similarly, the continuous auditing literature provides value to corporate structures in areas such as automated control tests, policy compliance, and configuration monitoring. Nevertheless, these two research streams have largely evolved in parallel; however, systematic links between SOC-generated technical outputs and the audit evidence, control testing, and assurance mechanisms required by internal audit remain largely absent. The limited number of studies showing that log analysis can be associated with audit policies and compliance controls demonstrates that such integration is both possible and meaningful (Behloul et al., 2015).

The framework draws upon four complementary theoretical foundations. Primarily, continuous auditing research conceptualizes assurance as a technology-supported process in which digital evidence is collected and evaluated at shorter intervals rather than being examined solely through periodic and retrospective procedures (Vasarhelyi & Halper, 1991; Vasarhelyi et al., 2004; Alles et al., 2008). Within this perspective, automated monitoring and exception-based analysis enable auditors to focus on deviations that may indicate changes in risk exposure or control performance. Other, the information security log management literature establishes that centrally collected, normalized, and protected event records can support accountability, incident reconstruction, and the verification of control operation (Kent & Souppaya, 2006).

Also, the monitoring component of the COSO Internal Control Framework provides the control-oriented basis of the proposed model. From this perspective, ongoing monitoring and separate evaluations are complementary mechanisms for determining whether internal controls remain present and continue to function as intended (COSO, 2013). Lastly, the IIA Three Lines Model provides the governance basis for collaboration between SOC operations and internal audit. Although operational functions and internal audit may exchange risk-relevant information, internal audit must remain independent of management responsibilities and should not assume ownership of threat detection or incident response activities (Institute of Internal Auditors [IIA], 2020).

The solution integrates these theoretical streams into a sequential process. SOC telemetry constitutes the initial operational evidence; SIEM correlation rules and behavioral analyses transform this telemetry into risk-relevant signals; predefined audit criteria associate these signals with control objectives and potential control deviations; and internal audit independently evaluates the selected outputs to provide continuous assurance. Accordingly, the model does not merge the SOC's operational responsibilities with internal audit's assurance responsibilities. Instead, it establishes a governed and traceable evidence interface between the two functions. In Design Science Research terms, the study represents the exaptation of established SOC and log analytics capabilities to the domain of continuous internal audit assurance (Gregor & Hevner, 2013).

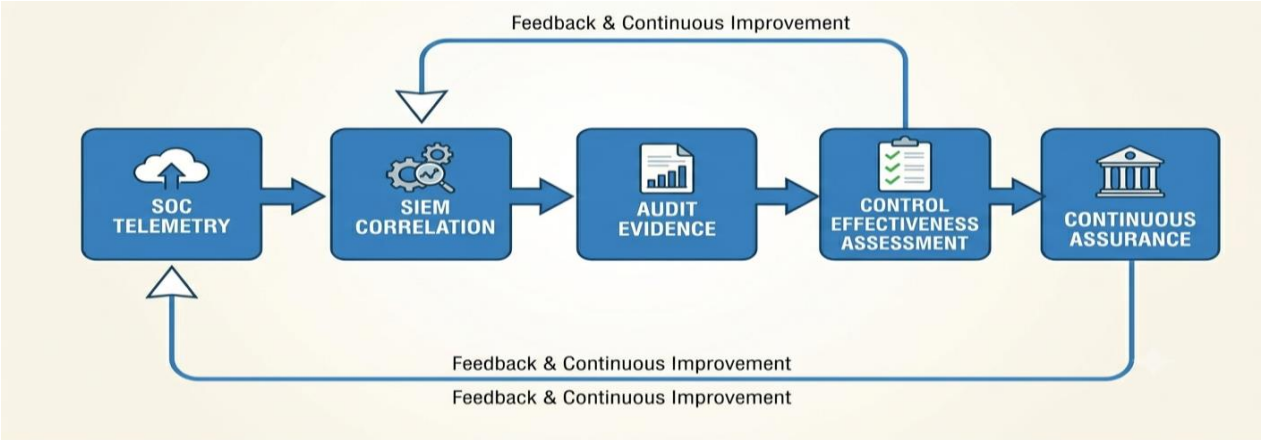
The conceptual framework developed in this study is based on the re-interpretation of real-time log data produced by SOC operations from an internal audit perspective. The framework assumes that technically detected threats, anomalies, and policy violations are not limited to operational security outputs. They can also serve as audit evidence for assessing control design adequacy, control operation effectiveness, and risk management maturity.

The framework therefore brings SOC, continuous auditing, and log analytics that fields mostly addressed separately in the literatüre, onto a shared conceptual ground and shifts auditing toward a real-time, data-driven structure.

Accordingly, audit-driven threat monitoring refers to the use of real-time threat, anomaly, and security breach outputs produced by SOC operations. These outputs are then evaluated by internal audit to support continuous assurance regarding control design, control operation, and risk management effectiveness.

Building on this conceptual framework, this study proposes a model for integrating real-time log analytics into audit processes while establishing the principles governing collaboration between SOC operations and the internal audit function. Thus, the limitations of document-based audit approaches mentioned in the literature and the need to transform technical security outputs into auditable value are addressed under a holistic and applicable structure.

Figure 1. Audit Assurance Mechanism



To operationalize the conceptual foundation established in this study, a model illustrating the transformation of technical security outputs into audit assurance mechanisms has been developed (Figure 1). Its core premise is that real-time telemetry generated by SOC operations can be systematically converted into audit-relevant information through sequential analytical and evaluative processes. Within this structure, security events collected from operational environments are first processed through SIEM-based correlation and behavioral analysis mechanisms to identify anomalies, policy deviations, and indicators of potential control weaknesses.

The resulting outputs are subsequently reinterpreted from an internal audit perspective and transformed into audit evidence that supports the evaluation of control design, operational effectiveness, and risk management processes. By linking real-time security monitoring activities with continuous auditing mechanisms, the model enables the internal audit function to move beyond periodic assessments and provide continuous assurance based on technical evidence. As a result, SOC operations, log analytics, and continuous auditing are integrated into a unified structure that supports both organizational governance and cybersecurity resilience.

4. METHODOLOGY

4.1. Research Design

The research design proposes and validates a framework that integrates real-time Security Operations Center (SOC) outputs into continuous auditing processes through an audit-driven threat monitoring approach. For this purpose, the Design Science Research (DSR) methodology is adopted, as it is widely adopted for designing, developing, and evaluating innovative information systems artifacts (Hevner et al., 2004; Kuzu, 2013).

The adopted DSR process consists of problem identification, conceptual framework development, artifact design, implementation, and evaluation. Initially, the conceptual gap between operational cybersecurity monitoring and internal audit assurance activities was identified through a comprehensive literature review. On this basis, an integrated approach was designed to transform SOC-generated security telemetry into audit-relevant evidence. The approach was then implemented and evaluated in a controlled virtualized environment to assess its technical feasibility and practical applicability.

Rather than evaluating a specific cybersecurity threat or attack technique, the research focuses on the integration mechanism itself. Instead, it seeks to demonstrate how operational security findings can be systematically converted into continuous audit evidence and incorporated into internal audit workflows. Accordingly, the methodology centers on designing and validating an integration model that establishes a structured relationship between SOC monitoring activities and internal audit assurance processes.

4.2. Experimental Environment and Data Sources

For feasibility assessment, a controlled virtual environment was established to simulate both SOC operations and internal audit activities. The environment was implemented on VMware-based infrastructure and designed as a three-host architecture consisting of:

- A log-generating endpoint system,
- A centralized SOC/SIEM analysis platform,
- An independent internal audit and notification system.

The three-host architecture was intentionally designed to preserve the functional independence of the internal audit function while enabling the automated sharing of audit-relevant security findings. This separation reflects governance principles commonly adopted in corporate environments, where operational security monitoring and independent assurance activities are performed by different organizational functions.

The dataset used in this study consists of system-generated log records reflecting authentication activities, process execution events, system operations, and user behavior indicators. These logs represent the type of telemetry data commonly generated within operational security environments and utilized by SOC teams for monitoring and incident detection purposes.

A centralized log management approach was adopted to ensure the collection, normalization, indexing, and analysis of log data. Splunk Enterprise was utilized as the Security Information and Event Management (SIEM) platform responsible for aggregating logs from monitored systems, correlating events, and identifying anomalous behaviors

through predefined analytical rules. Endpoint telemetry was transmitted to the centralized SIEM environment using Splunk Universal Forwarder components.

4.3. Scenario Selection and Behavioral Modeling

In the model design, a systematic mapping was performed between the tactical/technical structures used by SOC operations and the control/risk assessment models of internal audit. The primary goal of this mapping is to ensure that technical security incidents are identified in a consistent and repeatable manner regarding which audit control areas and risk dimensions For validation, a proof-of-concept scenario based on privileged activities occurring outside normal business hours was selected. The choice of this scenario was intentional and motivated by both cybersecurity and auditing considerations.

For SOC teams, privileged activities performed outside predefined working hours are generally treated as high-risk events since they may indicate unauthorized access attempts, insider threats, misuse of administrative privileges, compromised accounts, or attempts to bypass established security controls. Such activities frequently appear in security monitoring use cases and behavioral anomaly detection models.

For internal auditors, after-hours privileged access is explicitly linked to critical control domains, including access management, segregation of duties, governance practices, and control effectiveness assessments. Consequently, deviations from established working-hour policies can be interpreted as potential indicators of control weaknesses or governance deficiencies.

The scenario therefore represents a shared risk domain that can be evaluated simultaneously by operational security and internal audit functions. Since working-hour policies and privileged access controls exist in most organizations regardless of sector, the scenario also provides a broadly applicable and easily interpretable demonstration of the structure.

Within the experimental environment, process creation events recorded under Windows Event ID 4688 were used as the primary data source. Behavioral thresholds were defined to distinguish isolated events from recurring patterns. Single occurrences were not treated as significant findings. Repeated after-hours activities exceeding predefined thresholds were instead evaluated as potential indicators of control deficiencies requiring audit attention.

4.4. Cross-Framework Mapping

A systematic mapping process was established to connect operational security findings with internal audit control assessments. The objective of this mapping was to ensure that technical security events could be consistently interpreted as control indicators and risk signals within the audit process.

Three complementary frameworks were employed:

- NIST Cybersecurity Framework (CSF) to categorize security monitoring and incident response activities,
- MITRE ATT&CK Framework to classify attacker behaviors and detection scenarios at tactical and technical levels,
- COSO Internal Control Framework to evaluate identified events in terms of control design and operational effectiveness.

Through this mapping process, SOC alerts become more than technical security events; they are transformed into auditable indicators reflecting potential control deficiencies, governance weaknesses, or emerging organizational risks.

4.5. Control Mapping and Audit Evidence Generation

To establish a direct relationship between SOC-generated findings and internal audit activities, a three-stage control mapping methodology was developed consisting of three stages:

- Identification of control domains frequently assessed by internal audit functions, including access management, segregation of duties, configuration management, session security, and privileged account governance.
- Definition of log-based indicators capable of demonstrating potential control violations or deviations.

- Development of threshold-based alert logic capable of transforming recurring security observations into audit-relevant findings.

Within the proposed model, the SIEM platform continuously monitors security telemetry against predefined behavioral criteria. When specified thresholds are exceeded, automated notifications are generated and transmitted to a dedicated audit host. These notifications contain structured information regarding the affected asset, event characteristics, timestamps, and related control objectives.

The resulting alerts are treated as digitally generated audit evidence and represent the operational implementation of the continuous auditing concept proposed in this study. By automating the transfer of selected SOC outputs into audit workflows, the model enables near real-time visibility into potential control weaknesses while preserving the independence of the internal audit function.

All data utilized in this research were generated within a controlled laboratory environment. No real organizational data, employee information, or production systems were used during the study, ensuring compliance with ethical and security requirements.

5. THE PROPOSED FRAMEWORK

At the architectural level, the framework is organized as an end-to-end data flow in which system-generated digital traces are collected, analyzed, filtered, and transferred to the internal audit layer as audit-relevant outputs. The process begins with data generation at the endpoint, continues with centralized analysis in the SOC/SIEM environment, and concludes with the transmission of threshold-based findings to the audit unit.

The architecture relies on three functionally separated hosts that distinguish operational security activities from the internal audit function. This segregation ensures the preservation of internal audit independence while allowing SOC outputs to be utilized effectively in governance and control assessment processes (Moeller, 2016).

To assess feasibility, a scenario was constructed around “privileged access outside of business hours,” a critical risk area in corporate environments. Correspondingly, access attempts occurring after-hours were simulated on an endpoint system, and the logs generated from this system were transferred to a centralized monitoring unit (SOC) equipped with Splunk Enterprise, as illustrated in Figure 2.

When the threshold value defined in the central system was exceeded, three repetitions in this implementation, the resulting findings were automatically transmitted to the internal audit unit via email. The implementation illustrates an integrated process in which suspicious after-hours access is technically detected by the SOC and then evaluated by internal audit from a control perspective. This scenario provides the operational basis for testing the proposed data flow.

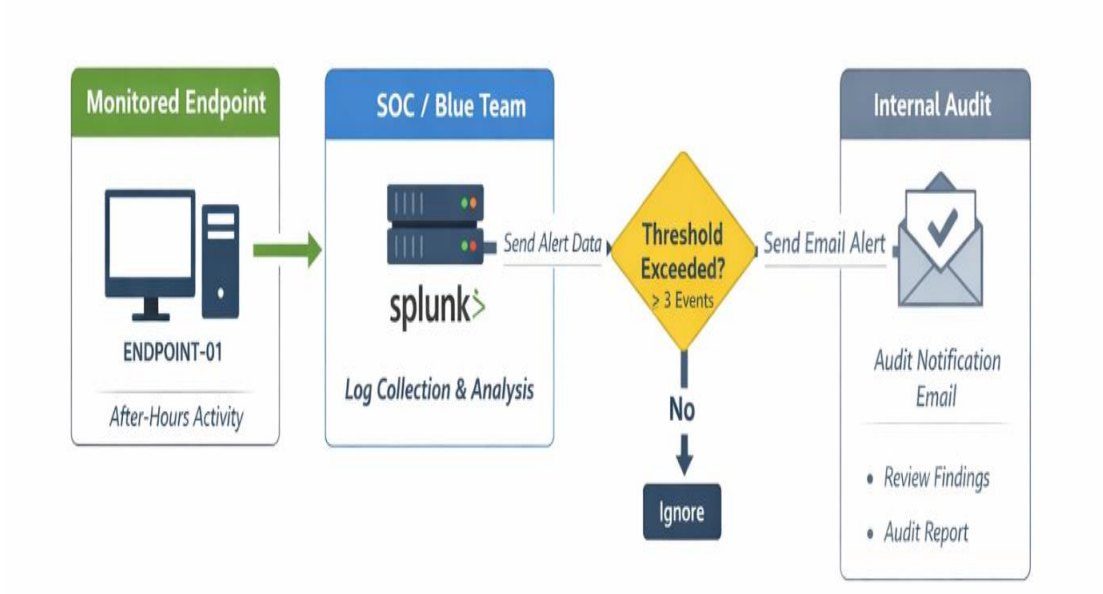


Figure 2.

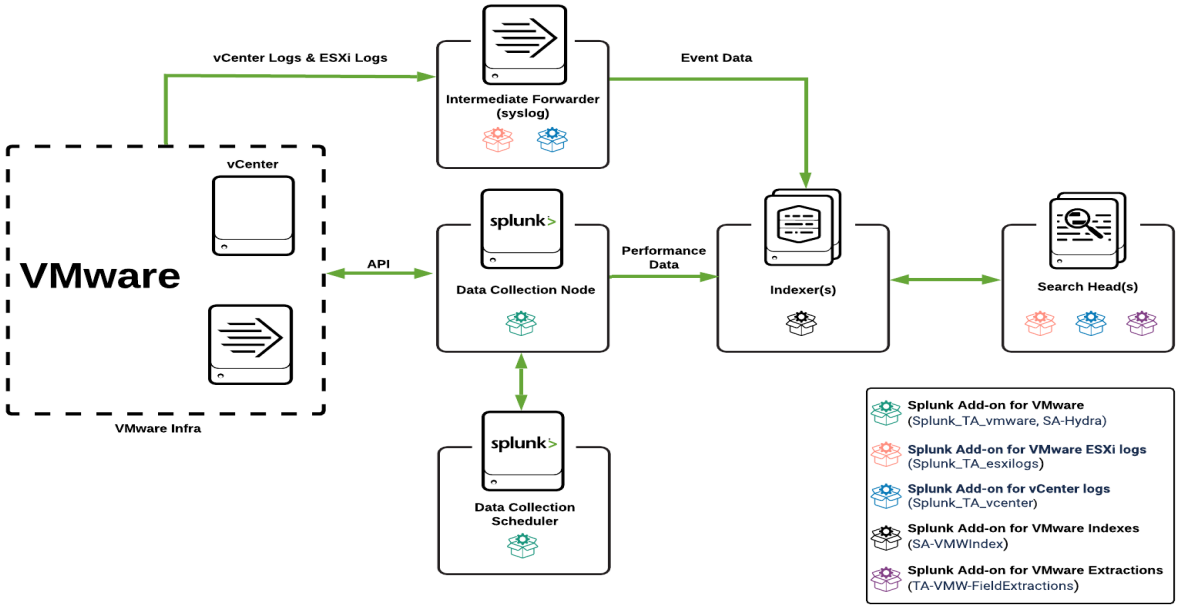
Study Summary Diagram

5.1. Virtualized SOC Environment and Splunk Configuration

The proposed model is constructed on a VMware-based virtualization infrastructure. The virtualization approach reflects the SOC architecture commonly used in corporate environments by ensuring that different security and audit roles are executed on isolated virtual machines (Behl & Behl, 2017).

In the VMware-based virtualized environment, Splunk Enterprise is deployed on a separate virtual machine and functions as the centralized SIEM platform representing the SOC/Blue Team layer. As illustrated in Figure 3, Splunk Universal Forwarder components installed on monitored endpoint systems collect operating system and application logs locally and transmit them to the central Splunk server through a secure channel. Splunk then centrally collects, indexes, normalizes, and analyzes endpoint logs, enabling the production of traceable and consistent audit evidence from an auditing perspective (NIST SP 800-92). The VMware infrastructure further supports scalability, segregation of duties (SoD), and resource management by allowing components such as Data Collection Nodes, Indexers, and Search Heads to operate on isolated virtual machines.

Figure 3. How Splunk Works On VMware



The Splunk Universal Forwarder components installed on endpoint systems exclusively undertake the task of log collection and transmission, without incorporating any analysis or decision-making mechanisms. This approach ensures that raw log data is transferred to the centralized SOC environment without modification, thereby enhancing the reliability of audit evidence (Kent & Souppaya, 2006).

5.2. Three-Host Architectural Structure

5.2.1 Host 1: Log-Generating Endpoint System

The first host functions as the endpoint system where user interactions and system-level operations occur. Security-critical events such as process creation, command execution, and authentication are logged on this host.

For this implementation, process creation events (Event ID 4688) generated on Windows operating systems serve as the primary data source. Specifically, the execution of a manually initiated process outside of business hours (after 17:00) is modeled as an indicator of potential privilege abuse, policy violation, or ineffective control operation.

The “privileged access outside of business hours” scenario was selected deliberately because it is relevant to both security monitoring and internal auditing. From a SOC perspective, privileged activities occurring outside predefined

working hours are widely recognized as high-risk events because they may indicate unauthorized access, insider threats, misuse of administrative privileges, or attempts to bypass established controls. From an internal audit perspective, such activities structured and automated transfer to governance, segregation of duties, access management, and control effectiveness assessments. Therefore, this scenario provides a common risk domain that can be simultaneously interpreted by both SOC analysts and internal auditors.

Its applicability across different sectors and organizational environments also supports its selection as a proof-of-concept case. Regardless of industry type, institutions generally define authorized working hours and privileged account management policies. Consequently, deviations from these predefined behavioral baselines constitute a universally understandable control exception. This characteristic makes the scenario particularly suitable for demonstrating the integration model.

Furthermore, the operation of local security authentication servers, such as lsass.exe, which indicates the initiation of the operating system, has enabled the recording of suspicious logins after-hours as they fall within the scope of Event ID 4688. Evaluating time-based deviations as anomaly indicators is consistent with behavior-based anomaly detection approaches in the literature (Chandola et al., 2009). This proof-of-concept provides a controlled case for observing the proposed integration mechanism. The same architecture can be extended to various other security events, including failed login attempts, unauthorized privilege escalations, critical configuration changes, data exfiltration indicators, suspicious PowerShell executions, or segregation-of-duty violations

5.2.2. Host 2: SOC / Blue Team Log Analysis System

The second host is the centralized log analysis environment representing the SOC and Blue Team functions. Splunk Enterprise running on this host centrally indexes all logs originating from endpoints and performs behavior-based analyses.

The analytical logic focuses on recurring behavioral patterns over time rather than isolated incidents. The execution of three or more commands/processes outside of business hours within a specific timeframe is evaluated as a significant deviation from an auditing perspective. This logic reduces false positives while allowing audit findings to be interpreted contextually (Alles & Vasarhelyi, 2004). The analysis outputs generated at this layer qualify as potential security incidents for the SOC, whereas for internal audit, they are evaluated as evidence regarding control design and operational effectiveness.

The threshold-based logic distinguishes isolated events from recurring deviations that may require audit attention. While a single event may represent an isolated anomaly, repeated occurrences indicate a potentially systematic weakness in access governance, monitoring controls, or policy enforcement mechanisms. Such repetitive deviations are more meaningful for internal audit assessments because they provide measurable evidence regarding the effectiveness of organizational controls.

The detection logic implemented in Splunk is deliberately modular. Although the model is evaluated through the “privileged access outside of business hours” scenario, the same analytical workflow can operate on any SIEM correlation rule or behavioral analytics output. Thus, the model depends not on the specific content of an alert, but on the automated transfer of high-risk SOC findings into the internal audit workflow.

Figures 4 and 5 illustrate the SPL (Search Processing Language) query developed on Splunk to identify suspicious commands executed on a designated endpoint after-hours (post-17:00) and the resulting log outputs.

Figure 4. Querying Suspicious Commands After Business Hours Using Search Processing Language (SPL)

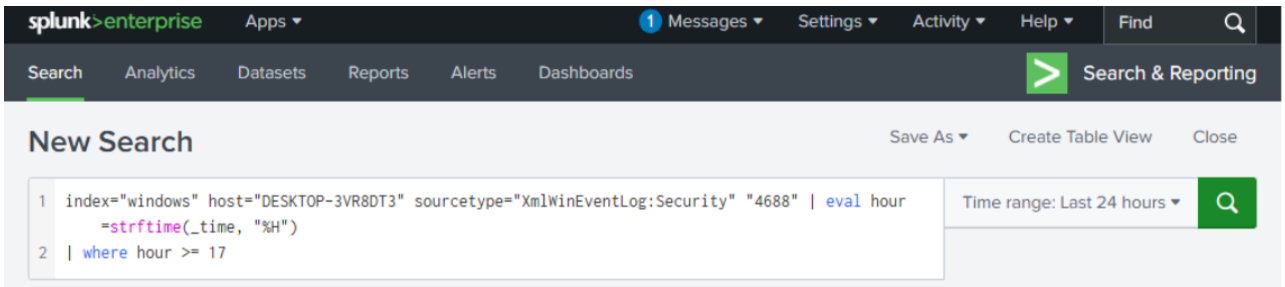


Figure 5. Log Record Of The Suspicious Command Execution

The active observation of the lsass.exe process within the relevant logs confirms that the target host's operating system is functional and that security subsystems have been successfully initialized. Therefore, this log demonstrates that the host was indeed active and in use during after-hours periods.

Respectively, the contribution of the proposed model should not be interpreted as the detection of a particular security violation, but rather as the establishment of an automated governance mechanism that bridges SOC operations and continuous auditing activities through real-time security telemetry.

5.2.3. Host 3: Internal Audit and Notification System

The third host functions as the independent evaluation, governance, and notification layer corresponding to the internal audit function. Unlike the SOC environment, which focuses primarily on threat detection and operational response, this layer evaluates security events from the perspective of risk management, internal control effectiveness, compliance, and organizational governance.

A core objective of the model is to reduce the traditional separation between security monitoring activities and internal audit processes. In conventional environments, security incidents identified by SOC teams are typically documented through periodic reports and later communicated to audit functions.

Such a reporting structure often causes delays, information loss, and reduced audit responsiveness. The proposed architecture addresses this gap by enabling the direct and automated transfer of security-relevant findings into the internal audit workflow.

Due to the limitations on native alerting and email notification features within the Splunk Free license used in this study, the audit notification mechanism was implemented through external automation tools. For this reason, the analysis outputs generated on the SOC host were exported and processed through a custom script structure running on the internal audit host. The PowerShell script, detailed in Figure 6, continuously scans the exported data to verify whether predefined thresholds (three repetitions) have been exceeded. When the specified criteria are met, the script automatically initiates an email notification to the internal audit unit.

The custom-developed script dynamically generates HTML-based reports containing sender information, recipient details, event summaries, timestamps, and specific audit findings. This automation demonstrates that continuous auditing mechanisms can be established independently of the built-in capabilities of a particular SIEM platform. Consequently, the proposed approach remains adaptable to different SIEM technologies and organizational infrastructures. In a production environment, such notifications should be limited to the minimum audit-relevant information and transmitted through secure channels, while detailed or sensitive log records should remain within access-controlled evidence repositories.

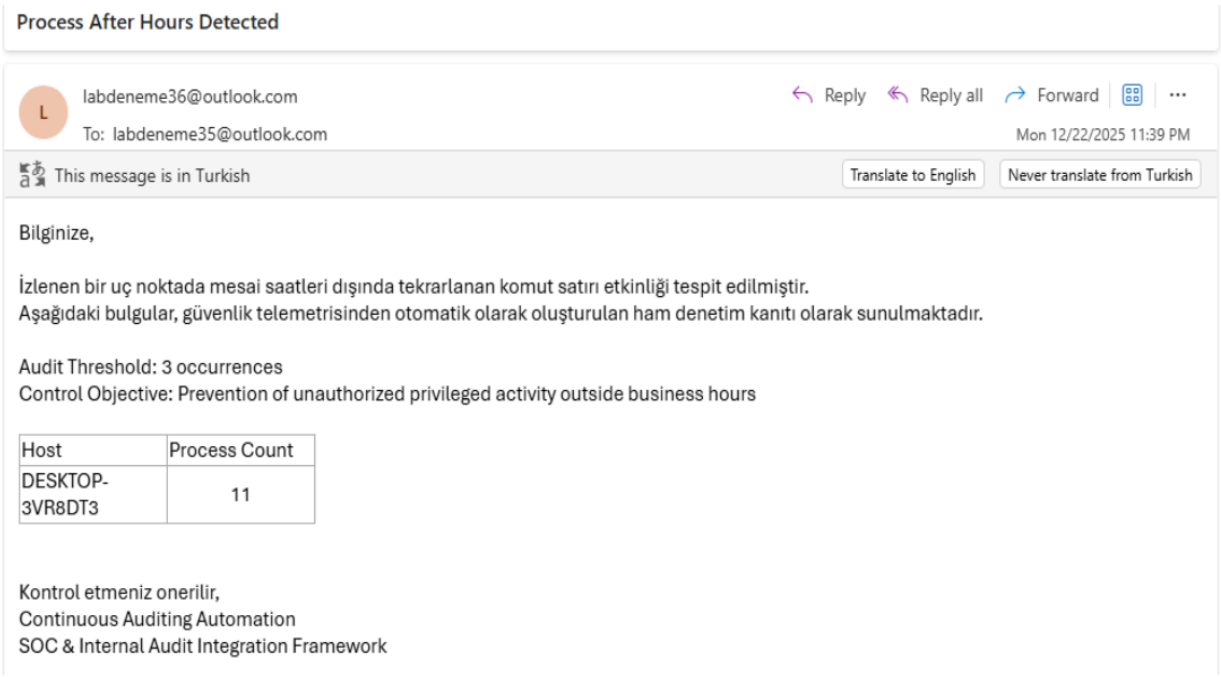
Methodologically, the notification mechanism is designed to remain independent of any specific security scenario. Although the proof-of-concept implementation focuses on privileged access activities occurring outside business hours, the same workflow can process any high-risk event generated by a SOC environment, including unauthorized privilege

escalations, repeated authentication failures, suspicious administrative actions, configuration changes, data exfiltration indicators, or policy violations. This design allows the notification workflow to remain adaptable to different SOC-generated high-risk events.

Figure 6. Powershell Script Created For Sending Emails

```
$csvPath = "C:\Users\labde\Desktop\alert.csv

if (Test-Path $csvPath) {

    $data = Import-Csv $csvPath

    if ($data.Count -ge 3) {

        $htmlTable = $data | ConvertTo-Html -Fragment -PreContent "<h3>After-Hours CMD Execution Audit
Finding</h3>"

        $htmlBody = @"

<p>Bilginize,</p>

<p>
İzlenen bir uç noktada mesai saatleri dışında tekrarlanan komut satırı etkinliği tespit edilmiştir.
Aşağıdaki bulgular, güvenlik telemetrisinden otomatik olarak oluşturulan ham denetim kanıtı olarak
sunulmaktadır.
</p>

$htmlTable

<p>
<b>Audit Threshold:</b> 3 occurrences<br/>
<b>Control Objective:</b> Prevention of unauthorized privileged activity outside business hours
</p>

<p>
Kontrol etmeniz onerilir<br/>
<b>Continuous Auditing Automation</b><br/>
SOC & Internal Audit Integration Framework
</p>
"@

        $cred = Get-Credential

        Send-MailMessage `
            -From "labdeneme36@outlook.com" `
            -To "labdeneme35@outlook.com" `
            -Subject "Continuous Audit Alert – After-Hours CMD Activity" `
            -Body $htmlBody `
            -BodyAsHtml `
            -SmtpServer "smtp.office365.com" `
            -Port 587 `
            -UseSsl `
            -Credential $cred
    }
}
```

Figure 7. Example Of An Email Sent To The Internal Audit Unit



As illustrated in the sample notification email presented in Figure 7, the relevant alert is delivered explicitly linked to the internal audit department. This automated communication provides structured information, including the affected endpoint (Host), the number of detected incidents (Process Count), the timestamp of occurrence, and the associated Control Objective. Such information enables auditors to immediately assess whether the identified activity represents an isolated event, a recurring control weakness, or a potential governance issue requiring further investigation.

Importantly, the generated notification should not be viewed merely as a technical security alert. Within the proposed approach, it serves as raw audit evidence produced generated from security telemetry in near real-time. By transforming operational security data into auditable evidence without requiring manual intervention, the model supports continuous auditing principles and significantly reduces the delay between control deviation occurrence and audit awareness. As a result, internal auditors gain the ability to monitor control exceptions continuously, prioritize investigations based on risk, and perform more proactive assurance activities.

5.3. Continuous Auditing Flow

In the proposed framework, the continuous auditing process consists of the following steps:

- Logging of security events occurring on the endpoint system,
- Transmission of logs to the SOC environment via Splunk Universal Forwarder,
- Application of behavior-based analysis and threshold controls on the SOC host,
- Triggering of the internal audit host when designated audit thresholds are exceeded,
- Reporting of audit findings via email and recording them as audit evidence.

This process ensures that security incidents are treated not only as technical threats but also as a continuous feedback tool regarding the effectiveness of internal control mechanisms.

5.4. Contribution of the Framework

The contribution of the framework lies in the establishment of a structured evidence-sharing mechanism between SOC operations and internal audit rather than in the detection of a specific alert type. By separating the endpoint, SOC/SIEM, and internal audit layers, the architecture preserves functional independence while enabling selected SOC outputs to be transferred into audit workflows as structured evidence. This design supports near real-time visibility into control

deviations, reduces the delay between security event detection and audit awareness, and provides a reusable integration logic that can be extended to different SIEM rules, log sources, and high-risk security scenarios.

6. FINDINGS

This section presents the findings obtained from implementation of the proposed audit-driven threat monitoring framework in a virtualized SOC environment are evaluated. The results are organized under log visibility, control effectiveness, audit evidence generation, and the operational implications of internal audit and SOC collaboration.

6.1. Log Visibility and Anomaly Detection

Process creation logs (Event ID 4688) generated on the endpoint system used in the study provided enhanced visibility for detecting manual process initiations occurring after business hours. Specifically, the after-hours triggering of lsass.exe and similar system components was successfully modeled as an indicator of potential privilege abuse or control violations.

In queries conducted via SPL (Search Processing Language), repeated process initiations within specific timeframes were classified as behavioral anomalies, creating log patterns with auditing significance. This method reduced false positives and enabled context-based detection.

6.2. Mapping SOC Alerts with Control Indicators

SOC alerts mapped with MITRE ATT&CK techniques were reclassified as audit indicators within the scope of the COSO internal control model. For example, log data regarding brute force attempts were evaluated both as attack behaviors and as "unauthorized access control violations." Through this mapping, security incidents become interpretable not only as technical threats but also as control failures or design weaknesses from an internal audit perspective.

6.3. Automation-Based Audit Evidence Generation

When behavior-based thresholds defined at the SOC layer (e.g., executing more than three commands after-hours) were exceeded, an automated notification was sent to the internal audit system. This process was automated via PowerShell scripts, and the relevant findings were reported as audit evidence. Although the audit unit classifies this data manually, the automated threshold controls and notification flow provided by the system demonstrate that the concept of continuous auditing has become functional at a technical level.

6.4. Operational Data Flow in SOC-Audit Collaboration

The three-host architecture has maintained functional independence while ensuring technical data flow between the internal audit and SOC units. Consequently, SOC outputs were evaluated within the structure of control design and operational effectiveness, rather than being converted structured and automated transfer into operational interventions by the internal audit unit.

Through this structure:

- Internal Audit gained direct access to technical details,
- SOC received feedback on control weaknesses through evaluations provided by the audit unit.

6.5. Framework Outcomes of Continuous Auditing

The model's outputs increase the visibility of the corporate control model, offer real-time triggering mechanisms in place of manual testing processes, and closely involve internal audit in the threat detection process, especially in areas requiring high security (e.g., the defense industry).

Overall, the implementation shows that continuous auditing increases risk visibility, grounds audit findings in technical evidence, and strengthens the synergy between audit and cybersecurity.

7. GOVERNANCE AND ACCESS CONTROL CONSIDERATIONS

Although the approach demonstrates the feasibility of integrating real-time SOC outputs into continuous auditing processes, its implementation also raises governance, privacy, and access-control issues that require careful management.

A central concern is the direct exposure of internal audit personnel to operational security data. SOC environments often contain highly sensitive information, including authentication records, privileged account activities, user behavior data, system configurations, network communications, and incident investigation details. Granting unrestricted access to such information may create data privacy concerns, particularly when logs contain personally identifiable information (PII), employee activity records, or confidential operational details. Consequently, organizations must establish clear data governance policies defining which categories of security telemetry can be accessed by auditors and under what conditions.

Preserving internal audit independence is equally important. According to established governance frameworks such as the Three Lines Model and the Institute of Internal Auditors (IIA) guidance, internal audit functions are expected to maintain an independent assurance role rather than participate specifically in operational activities. Excessive involvement of auditors in daily SOC operations may create role ambiguity and potentially compromise the objectivity of audit assessments. Consequently, the proposed model should not be interpreted as integrating auditors into operational threat detection or incident response activities. Instead, internal audit should draw on selected security outputs as audit evidence while maintaining its independent evaluation and assurance responsibilities.

Operational challenges may also arise when SOC outputs are integrated into audit workflows. Large-scale SOC environments generate substantial volumes of alerts, anomalies, and correlation findings on a daily basis. If all detected events are automatically transferred to internal audit units, auditors may experience alert fatigue similar to that observed among SOC analysts. Excessive notification volumes may reduce the effectiveness of continuous auditing processes and divert attention away from genuinely critical control deficiencies. For this reason, risk-based prioritization mechanisms, severity classifications, and threshold-based filtering procedures should be implemented before security findings are forwarded to audit functions.

Segregation-of-duties risks may also emerge if access models are not properly designed. Inappropriately designed access models may allow auditors to obtain permissions that exceed their assurance responsibilities or enable them to influence operational security decisions. Such situations may weaken accountability structures and blur the distinction between control ownership and control evaluation. To mitigate this risk, organizations should implement role-based access control (RBAC) mechanisms, ensuring that internal audit personnel receive read-only access to predefined audit-relevant datasets without obtaining operational administration privileges.

As a mitigation measure, organizations may adopt an audit-specific access model in which auditors receive filtered and contextualized security information through dedicated dashboards, reports, or automated evidence-sharing mechanisms rather than unrestricted access to the entire SIEM environment. This model preserves audit independence, protects sensitive operational information, and maintains the principle of least privilege while still enabling continuous assurance activities.

In practice, access to audit-relevant SOC data should be supported by additional privacy and security safeguards. Where logs contain personal data, employee activity records, or confidential operational information, data minimization, masking, or pseudonymization should be applied before the information is transferred to the internal audit function. Auditor access to SOC-derived evidence should itself be logged, periodically reviewed, and restricted in accordance with predefined purposes, retention periods, and authorization rules. The confidentiality and integrity of transferred audit evidence should also be protected through encryption, controlled repositories, and tamper-evident mechanisms. In particular, automated email notifications should contain only the minimum information necessary for audit assessment and should not expose raw logs, sensitive identifiers, or confidential incident details. Responsibilities for approving access, reviewing permissions, and escalating unauthorized or inappropriate use should be clearly assigned among data owners, SOC management, and the internal audit function.

Taken together, successful SOC–audit integration depends not only on technical feasibility but also on appropriate governance structures, privacy safeguards, access-control mechanisms, and clearly defined organizational responsibilities. These governance considerations constitute essential design requirements for any practical implementation of the proposed model.

8. DISCUSSION

This section discusses the positioning and contributions of the audit-driven threat monitoring approach, which is designed to integrate real-time log analytics into continuous auditing processes, in relation to the existing literature. Subsequently, the discussion compares the findings with current literature and explains the necessity of the proposed integration.

A significant portion of the literature focusing on SOC operations concentrates on developing threat detection, technical visibility, and MITRE ATT&CK-based classification mechanisms (Chamkar et al., 2024; Le et al., 2025). While these studies enhance the effectiveness of security operations, they do not provide guidance on how the resulting technical outputs can be utilized in internal audit processes. The implementation results show that correlation outputs produced by the SOC can be reinterpreted as indicators of control violations and as audit evidence from an internal audit perspective. In this respect, the structure assigns an "auditable meaning" to outputs that are predominantly treated at the operational level in SOC literature.

Research on continuous auditing has primarily focused on automated control testing, policy compliance, and configuration monitoring (Torkura et al., 2021; Kestane, 2021). These studies emphasize the inadequacy of document-based auditing approaches and point toward the necessity of integrating technology into audit processes. However, this literature does not explicitly address how real-time SOC log streams can be technically connected to continuous auditing mechanisms.

These results respond to this gap by showing that behavior-based log thresholds can function as audit triggers and that continuous auditing can be supported by operational data.

Technical studies on log analytics and anomaly detection aim to detect threats at an early stage through big data infrastructures and machine learning models (Reddy, 2024; Danish, 2025; Huang et al., 2024). The implementation supports the technical validity of the behavior-based analysis approach used in the model. Nevertheless, analytical outputs in the relevant literature are mostly limited to operational decision-support mechanisms; they are not treated as audit evidence or indicators of control effectiveness. The interdisciplinary contribution lies in repositioning log analytics outputs within an audit-oriented assurance logic.

In the internal audit literature, criticisms regarding the effectiveness of periodic audit approaches based on document reviews are increasing, and interest in the use of technical data is rising (Islam et al., 2018; Tharwat et al., 2025). The results support this trend by showing that the internal audit function can be informed by real-time data produced in SOC environments. Thus, internal audit evolves from being a structure that only provides retrospective assurance into a continuous and technically grounded evaluation mechanism regarding control operations.

Against this background, the audit-driven threat monitoring approach brings together SOC operations, continuous auditing, and log analytics, which are typically addressed separately in the literature, around a common objective. The main contribution is not merely the presentation of a new model, but the demonstration of why such a model is needed for internal audit by connecting the potential of real-time technical data with the limitations of document-based auditing highlighted in the literature.

Nevertheless, this integration should not be assessed solely in terms of its potential benefits. Bringing SOC operations and continuous internal auditing into a closer technical relationship may also introduce organizational, methodological, and operational risks. A critical evaluation of these risks is necessary to clarify the conditions under which the architecture may generate assurance value without weakening the established responsibilities of the participating functions.

Role confusion between the SOC and internal audit constitutes a potential concern. SOC teams perform operational responsibilities related to monitoring, detection, investigation, and incident response, whereas internal audit is expected to provide independent assurance regarding governance, risk management, and control effectiveness. If internal auditors participate directly in defining operational detection rules, investigating incidents, or determining response actions, the distinction between control ownership and independent evaluation may become blurred. This may also create a conflict

in which auditors subsequently assess controls or processes that they have helped design or operate. For this reason, the model should be understood as a governed evidence-sharing mechanism rather than as the incorporation of internal audit into routine SOC operations.

SOC alert fatigue may also be transferred to, or compounded within, the internal audit function. Large-scale SOC environments produce substantial volumes of repetitive, context-dependent, low-severity, or false-positive alerts. Automatically forwarding excessive numbers of these outputs to internal audit may create additional audit noise, divert attention from material control deficiencies, and reduce the practical value of continuous assurance. The effectiveness of the model therefore depends on risk-based thresholds, severity classifications, aggregation procedures, and clearly defined criteria determining which SOC outputs are relevant to internal audit.

Closer integration may also result in scope creep and mission drift. Continuous access to operational security information could gradually create an expectation that internal audit should monitor daily events, follow individual incidents, or provide real-time operational recommendations. Such an expansion may consume limited audit resources, interfere with approved audit plans, and transform internal audit into a parallel monitoring function. This risk should be controlled through clearly defined audit charters, responsibility matrices, escalation criteria, and explicit limitations on the categories of security information transferred to the audit function.

Possible overreliance on automated audit evidence represents another limitation. SIEM alerts and log-based indicators depend on the completeness of the underlying logs, the accuracy of timestamps, the quality of correlation rules, the appropriateness of thresholds, and the availability of contextual information. Incomplete logging or poorly calibrated rules may generate misleading findings, while the absence of an alert cannot by itself demonstrate that a control is operating effectively. SOC-derived outputs should therefore be treated as one component of the audit evidence set and, where necessary, corroborated through configuration reviews, inquiries, substantive testing, and other audit procedures.

The model also requires auditors to possess sufficient cybersecurity and log-analytics competence and may create uncertainty regarding responsibility for incorrect, delayed, or undetected alerts. Continuous monitoring may further produce an unjustified perception that comprehensive assurance has been achieved. Taken together, these concerns indicate that technical integration alone is insufficient; periodic validation of detection rules, data-quality controls, formal accountability arrangements, and regular assessment of the continuing relevance of transferred information are also required. Future research should examine how different governance models, organizational structures, prioritization mechanisms, and assurance boundaries affect audit independence, role clarity, resource requirements, and the overall effectiveness of SOC–audit integration.

The use of a single proof-of-concept scenario should also be interpreted in relation to the design-oriented purpose of the research. The research did not aim to compare the model's performance across multiple cybersecurity scenarios or to establish empirical generalizability on the basis of different attack patterns. Instead, the "privileged access outside of business hours" scenario was selected as a representative and readily interpretable case through which the technical and organizational feasibility of transforming SOC-generated telemetry into continuous audit evidence could be demonstrated. This scenario enables the complete evidence flow to be observed, from log generation and SIEM-based analysis to threshold evaluation and automated notification of the internal audit function. Thus, the scenario functions as a validation instrument for the integration mechanism rather than as the substantive focus or sole intended use case of the model.

Although the modular architecture and evidence-sharing workflow are not technically dependent on this specific alert type, the present findings demonstrate feasibility only within the implemented scenario and controlled laboratory environment. Therefore, the results should not be interpreted as empirical confirmation that the structure will perform identically across all threat categories, organizational structures, or operational settings. Validation through additional scenarios, including repeated authentication failures, unauthorized privilege escalation, critical configuration changes, suspicious administrative actions, and data exfiltration indicators, is required to assess the model's broader applicability, scalability, and generalizability.

Overall, the discussion shows that the model is aligned with theoretical trends in the literature while offering a distinctive contribution by integrating these trends at both technical and auditing levels. In this respect, the study provides the literature with an explanatory and applicable perspective on how the internal audit function can be repositioned in a digitalized security environment.

9. CONCLUSION

This study proposes an integrated framework that incorporates real-time log analytics-based continuous auditing approach into continuous auditing within Security Operations Center (SOC) environments from governance, technical, and strategic perspectives. Through an interdisciplinary approach, cybersecurity monitoring, internal audit, and control systems, which are generally addressed separately in the literature, are unified within an applicable framework.

Technically, the Splunk-based three-host virtual environment enabled the analysis of process logs through SPL queries, the definition of behavior-based thresholds, and the automated notification of control deviations to the audit unit.

Specifically, using critical logs such as Event ID 4688, recurring manual operations after business hours were detected and transformed into audit triggers. Aligning the model with MITRE ATT&CK techniques enabled incidents to be evaluated from both technical and auditing perspectives.

In terms of corporate governance, the model supports the transition from traditional document-based approaches to data-driven continuous monitoring by enabling the internal audit function to access operational-level security data. As a result, the internal audit unit becomes a strategic actor that contributes to the real-time evaluation of both control design and control operation. This transformation enhances the practical integrated applicability of governance frameworks such as COSO and COBIT.

Strategically, the model indicates that internal audit units should be integrated more systematically into security infrastructures, especially in sectors with high security sensitivity (defense industry, public sector, finance, etc.). Correspondingly, organizations are recommended to implement the following policy steps:

- Granting internal audit units role-based and read-only access to predefined audit-relevant datasets, dashboards, or reports,
- Providing auditors with training on cybersecurity log analytics,
- Integrating continuous auditing infrastructures with manual audit plans,
- Updating log management policies to meet audit requirements.

In conclusion, the proposed framework extends beyond a technical solution by providing a governance-oriented approach that supports the evolving role of the internal audit profession in digitally enabled organizations. The approach presented in this study strengthens audit-cybersecurity collaboration, supports proactive risk management, and positions the audit function as a more effective component of corporate decision-making processes.

10. FUTURE WORK

The research has demonstrated the feasibility of conceptualizing and implementing a continuous auditing framework based on real-time log analytics. Further research opportunities remain for developing, scaling, and enhancing the sectoral adaptability of the model.

First, testing the approach on different SIEM platforms(e.g., QRadar, Elastic, ArcSight) will be important for assessing its technical robustness and generalizability. The integration of diverse log sources, such as database and network traffic logs, would also expand the model's scope and enhance its incident correlation capabilities.

Second, automated finding classification and risk-scoring algorithms could help audit units produce faster and more effective results with minimal manual intervention. In this regard, studies can be conducted on integrating artificial intelligence and machine learning-based recommandation systems with audit decision-support mechanisms.

Third, assessing the governance challenges that may arise during the integration of this model into corporate audit processes, such as data privacy, conflicts of roles, and audit independence, and developing governance mechanisms to address these challenges.

Furthermore, conducting sector-specific case studies in high-risk industries like energy, finance, and defense would help demonstrate how the approach can be tailored to varying sectoral risk profiles. In this context, integrating the model with regulatory frameworks such as (KVKK, GDPR, ISO 27001, NIST 800-53) can be considered a distinct area of research.

Finally, the development of organizational structures and governance models that increase the level of collaboration between internal audit and information security units will further reinforce the role of the audit function within the cybersecurity ecosystem.

In these respects, taken together these research directions provide opportunities to extend the proposed model across different technological, organizational, and regulatory contexts, thereby contributing to the continued development of continuous auditing research.

References

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. Journal of Information Systems, 22(2), 195–214. https://doi.org/10.2308/jis.2008.22.2.195

Alles, M., & Vasarhelyi, M. A. (2004). Continuous assurance and auditing: A prototype implementation. International Journal of Accounting Information Systems, 5(2), 143–168.

Antunes, M. G., Maximiano, M., & Gomes, D. (2022). A client-centered information security and cybersecurity auditing framework. Applied Sciences, 12(9), 4102.

Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security and what to do about it. Oxford University Press.

Behloul, A., Ait Chellouche, M., & Lakhoua, N. (2015). Audit policy compliance and log analysis for information systems security. In Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW) (pp. 183–188). IEEE. https://ieeexplore.ieee.org/document/7166125

Briliyant, A. S., Ramadhani, N., & Nugraha, A. A. (2025). Beyond automation gap: A survey on continuous compliance audit for IoT security. SSRN. https://doi.org/10.2139/ssrn.xxxxx

Chamkar, A., Maleh, Y., & Gherabi, N. (2024). Security operations centers: Use case best practices, coverage, and gap analysis based on MITRE ATT&CK. Journal of Cybersecurity and Privacy, 4(4), 36–52.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3).

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control-Integrated framework.

Danish, S. (2025). Enhancing cyber security through predictive analytics: Real-time threat detection and response. International Journal of Advanced Computer Science and Applications, 16(8), 25–37.

Fort Worth Internal Audit Department. (2021). Cybersecurity audit report.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS Quarterly, 37(2), 337–355.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly.

Huang, M., et al. (2024). SAGA: A synthetic audit log generator for anomaly detection in cybersecurity. arXiv. https://arxiv.org/abs/2411.13138

Institute of Internal Auditors (IIA). (2017). Global technology audit guide (GTAG) 4: Management of IT auditing.

Institute of Internal Auditors. (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense. Institute of Internal Auditors.

Islam, M. A., et al. (2018). Factors associated with cybersecurity audit by internal audit function: An international study. SSRN. https://doi.org/10.2139/ssrn.xxxxx

Kent, K., & Souppaya, M. (2006). Guide to computer security log management (NIST SP 800-92). National Institute of Standards and Technology.

Kestane, A. (2021). Siber güvenliğin etkinleştirilmesinde sürekli süreç denetimi modeli. Yönetim Bilimleri Dergisi, 19(40), 245–263.

Kuzu, A. (2013). Tasarım tabanlı araştırma yaklaşımı ve eğitim alanındaki uygulamaları. Akademik Bilişim, Eğitim ve Sosyal Bilimler Dergisi. https://dergipark.org.tr/tr/pub/ajesi/article/18728

Le, T., et al. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. Electronics, 14(11), 2252.

MITRE Corporation. (2023). MITRE ATT&CK framework: Techniques, tactics, and adversary behaviors. https://attack.mitre.org

Moeller, R. R. (2016). Executive's guide to IT governance. John Wiley & Sons.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity. https://www.nist.gov

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Reddy, K. (2024). Real-time predictive log analytics: A scalable Java-driven pipeline for dynamic insights in modern data environments. JNAO Journal.

Tharwat, H., Hafez, S. T., Elgohary, I. E., & Hassanein, A. (2025). A decade of cybersecurity research in internal auditing: Bibliometric mapping and future research agenda.

Torkura, K. A., et al. (2021). Continuous auditing and threat detection in multi-cloud infrastructure. Computers & Security.

Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. Auditing: A Journal of Practice & Theory, 10(1), 110–125.

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting, 1(1), 1–21. https://doi.org/10.2308/jeta.2004.1.1.1

Vasarhelyi, M. A., Alles, M., & Williams, K. T. (2010). Continuous assurance for the now economy. The Institute of Chartered Accountants in Australia.

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2010). Continuous auditing: Theory and application. Emerald Group Publishing.