



Digital Forensic Readiness to Mitigate Insider Threats in the SaaS Cloud Environment

Gabriel O. Shoderu¹, Stacey O. Baror², Sheunesu Makura³, Abiodun Modupe⁴

u16186258@tuks.co.za¹

^{1,2,3,4}Department of Computer Science, University of Pretoria, Pretoria, 0002, South Africa

Article Information

Received : 5 Dec 2025

Revised : 28 Dec 2025

Accepted : 30 Dec 2025

Keywords

Digital Forensic Readiness; Insider Threat Detection; Cloud Security; SaaS Environments; Anomaly Detection; Behavioral Analytics; ISO 27043; Forensic Investigation

Abstract

Cloud environments are now central to organizational operations and hold sensitive information and essential business processes that depend on trust between users and the systems they access. Insider threats present a significant challenge in this setting because individuals with legitimate access understand how these environments operate and can misuse their privileges. Traditional insider threat mitigation approaches are mostly reactive. They often rely on delayed evidence collection and post-incident investigation, which results in incomplete records, late detection, and increased organizational harm. This highlights the need for proactive strategies that identify suspicious behavior early and support reliable forensic investigation.

This study addresses the lack of a clear Digital Forensic Readiness (DFR) framework that can manage insider threats in cloud environments. It introduces a readiness framework that integrates forensic principles with intelligent behavioral analytics to detect, interpret, and preserve indicators of insider activity in Software as a Service environments. The research includes a detailed review of existing literature, identifies gaps in insider threat mitigation, and presents a practical scenario that illustrates how the framework supports investigation. In addition, the study proposes a structured approach for extracting and preparing data to improve anomaly detection and timely threat recognition. The framework aligns with ISO/IEC 27043 standards by promoting modularity, scalability, and evidential reliability. This work contributes a proactive and forensically sound approach to insider threat detection and establishes a foundation for future validation and adoption across organizations.

A. Introduction

Insider threats remain one of the most persistent and damaging challenges in modern cloud based environments. Organizations rely on cloud services to store sensitive information, deliver business applications, and support distributed workforces, which increases the volume and complexity of digital activity that must be monitored for security and forensic purposes. Unlike external attackers, insiders possess legitimate credentials and an understanding of internal systems, which allows them to bypass traditional perimeter defenses and conceal malicious behavior until significant harm has occurred. Prior studies report that insider incidents often go undetected for extended periods due to insufficient evidence collection, limited visibility across cloud platforms, and reactive forensic processes that begin only after a compromise has been identified [1, 2]. As cloud adoption continues to expand, these challenges place critical pressure on organizations to adopt proactive strategies that improve evidence availability and investigative readiness.

DFR has emerged as a strategic approach that enables organizations to anticipate incidents and prepare the data, processes, and structures needed to support efficient forensic investigations. Research in this area highlights the value of evidence planning, predefined response procedures, and consistent logging practices to improve the accuracy and reliability of forensic outcomes [3, 4]. However, many existing readiness frameworks were designed for traditional on-premise infrastructures and do not address the distributed, multi-tenant nature of cloud environments. The absence of standardized evidence preparation processes, combined with inconsistent log formats and varying provider controls, limits the ability of investigators to reconstruct events and identify insider activity in Software as a Service settings.

This study introduces a DFR framework designed specifically to support insider threat mitigation in cloud environments. The framework integrates DFR principles with behavioral analytics to identify unusual user activity, preserve relevant evidence, and strengthen investigative processes. By aligning with ISO 27043 guidance and incorporating a scenario-based proof of concept, the research demonstrates how structured evidence preparation and anomaly focused analysis can enhance the early detection of insider behavior while supporting forensic soundness [5]. The proposed framework contributes a practical foundation for organizations seeking to improve their readiness for insider incidents and offers a path toward more reliable and scalable forensic practices in cloud-based systems.

The remainder of this paper is structured as follows. Section 2 presents the research background and related work that motivate the need for a DFR framework in SaaS environments. Section 3 describes the materials and methods used to develop the proposed framework and demonstrate it through a scenario-based proof of concept. Section 4 reports the results obtained from the proof of concept. Section 5 discusses the findings, implications, and limitations of the study. Section 6 concludes the paper by summarizing the contribution and outlining directions for future work.

B. Background and Related Work

The complexity of insider threats has grown alongside the widespread adoption of cloud services. Insiders operate with legitimate access and awareness of internal processes, which makes their actions difficult to detect and even more difficult to investigate when cloud infrastructure is involved. Understanding this problem requires an examination of insider threat behavior, cloud computing characteristics, forensic requirements, and prior approaches to both detection and readiness. This section outlines the relevant background and reviews the literature that informs the need for a forensic readiness framework tailored to Software as a Service environments.

B.1 Background

Insider threats arise when individuals with authorized access misuse their privileges for malicious, negligent, or unintended actions. Studies describe insider behavior as a blend of technical activity and human intention, influenced by workplace stressors, opportunity, or intentionally harmful motives [6]. Cloud environments increase this risk because user activity is distributed, logs are fragmented across platforms, and evidence is not always preserved by default. SaaS systems introduce further constraints since customers have limited visibility into the provider's infrastructure and depend on the provider for log generation, retention, and access. This creates challenges for forensic investigations and demands clearer processes for planning, collecting, and preserving evidence.

Cloud forensics extends traditional forensic practices to virtualized and remote infrastructures. Prior work highlights that evidence in cloud systems is volatile, multi-tenant, and often outside the direct control of an investigator [19]. The shared responsibility model applied by cloud providers means that customers must prepare their own investigative processes even when they do not control the underlying hardware. These constraints motivate organizations to adopt a readiness approach that ensures evidence will be available when an insider incident occurs.

B.2 ISO/IEC 27043 and its Relation to DFR-BUST

ISO/IEC 27043 is an international standard that provides structured guidelines for conducting digital investigations in a consistent and repeatable manner. It defines principles and process classes that support the identification, collection, preservation, analysis, and interpretation of digital evidence across investigative scenarios [5]. The standard emphasizes clarity, transparency, and documented procedures to ensure evidence reliability and admissibility when challenged [5]. The need for structured investigation processes is also reflected in established digital forensic frameworks and guidelines that organise investigations into phases covering evidence handling and reporting [14, 18, 20]. ISO/IEC 27043 harmonises these activities into a generic process model that can be applied across environments and case types [5]. Recent work further shows that ISO/IEC 27043 can guide security monitoring and digital forensic readiness activities in operational cloud settings [21]. In this study, DFR-BUST relates to ISO/IEC 27043 by anchoring its readiness activities in the standard's process class taxonomy, with particular emphasis on readiness processes and concurrent processes that support

proactive evidence preparation, integrity, documentation, and chain of custody [5]. This alignment provides a standards-based foundation for the DFR-BUST design choices in SaaS environments, rather than relying on ad hoc readiness practices.

B.3 Existing Insider Threat Approaches

Insider threat research reflects two major detection approaches: misuse-based detection and anomaly based detection. Misuse based techniques rely on predefined rules or signatures but fail when insiders behave in unexpected ways. Anomaly based techniques model normal user behavior and identify deviations that may signal harmful intent. Several studies apply machine learning to this problem, including behavioral modeling, feature extraction, deep learning, and optimization methods [1, 7]. While these methods improve detection capabilities, most are designed for controlled environments and assume access to complete datasets, consistent logging, and stable system behavior. They rarely address the operational realities of SaaS platforms, where investigators must work with partial visibility and provider dependent data. This gap influences the reliability of insider threat response.

B.4 Digital Forensic Readiness

DFR is the proactive capability to collect, preserve, and structure digital evidence before an incident occurs. Research emphasizes the importance of logging strategies, predefined procedures, and structured event documentation to reduce investigative effort and cost [3]. Cloud specific readiness frameworks have been proposed, such as frameworks for organizing forensic evidence or preparing virtual environments for investigation [4]. Although valuable, these models often generalize cloud environments and do not address the operational characteristics that differentiate SaaS from other service models. There is limited research that combines readiness with systematic behavioral monitoring to support both detection and investigation.

B.5 Cloud Forensics and SaaS Evidence Preparation

Cloud forensics literature frequently outlines challenges related to distributed architectures, hypervisor abstraction, and limited access to provider systems. SaaS introduces additional restrictions because customers depend on the provider to generate logs and retain evidence. Studies point out that investigative reliability depends on timestamp alignment, complete activity traces, and preservation of user interactions across multiple services [8, 9]. Without a predefined plan to manage these elements, organizations struggle to reconstruct incidents involving insider activity. SaaS platforms therefore require tailored readiness processes that focus on consistent evidence preparation, structured logging, and clarity in how investigative data is produced and retained.

B.6 Related Work on Machine Learning for Insider Threat Detection

Machine learning has strengthened insider threat detection by enabling automated modeling of user behavior. Researchers have explored a range of algorithms such as One Class Support Vector Machines, Isolation Forest, Local Outlier Factor, and neural networks [10, 11, 12]. These studies demonstrate

improvements in anomaly detection but do not incorporate forensic requirements such as evidential integrity, log completeness, or ISO 27043 compliance. Most machine learning approaches focus on accuracy rather than explainability or the evidential value needed in forensic contexts. As a result, they offer detection capability but do not support the investigative needs of organizations facing insider incidents.

B.7 Synthesis and Gap

Across the literature, several observations emerge. Insider threat detection research advances behavioral and anomaly based methods, but these approaches do not address the forensic constraints that affect evidence availability in SaaS environments. DFR research provides processes for planning and preserving evidence but does not directly integrate intelligent behavioral analysis for proactive detection. Cloud forensic studies identify structural limitations in evidence generation and retention but stop short of offering a readiness framework that combines detection, interpretation, and preservation. The gap lies in the absence of a unified framework that prepares SaaS environments for insider investigation while supporting early detection through behavioral analytics. No existing work aligns forensic readiness with anomaly based monitoring under ISO 27043 principles. This study addresses this gap by proposing a readiness framework that integrates structured evidence preparation with analytic support to improve investigative reliability and enable earlier recognition of insider activity in cloud based systems.

C. Material and Methods

This section describes the approach used to develop the proposed DFR framework, including the study design, the literature review method, the conceptual framework definition, the software requirements specification, the scenario-based proof of concept, and the evaluation and validity considerations.

C.1 Study Design

This study follows a conceptual forensic research design that builds on established readiness principles and cloud forensic constraints described in prior work [3, 4, 5]. It focuses on developing and explaining a readiness framework rather than conducting controlled experiments.

The aim is to investigate how proactive forensic preparation can support insider threat mitigation in Software as a Service environments. The design integrates forensic principles, cloud computing constraints, behavioral monitoring, and investigative needs. A scenario based approach is used to demonstrate how the framework functions during insider activity, which is appropriate for forensic readiness research where the emphasis is on investigative reliability rather than statistical performance. Machine learning is included as a supportive analytic element that enhances early recognition of unusual user behavior but does not drive the core methodology. The study aligns with ISO 27043 readiness guidance by emphasizing preparation, structure, and evidential reliability.

B.2 Literature Review Method

The literature review used a structured thematic approach to identify relevant work in insider threat detection, cloud forensics, and DFR. Key surveys and foundational studies guided this process, including comprehensive reviews of insider threat methods [1, 6, 13] and cloud forensic challenges [19].

Sources were collected from Google Scholar, IEEE Xplore, ACM Digital Library, SpringerLink, and Wiley Online Library. Searches included terms such as "insider threat detection," "cloud forensics," "digital forensic readiness," "SaaS logging," and "behavioral analytics." Inclusion criteria focused on peer reviewed studies that examined insider behavior, anomaly detection methods, cloud forensic challenges, or forensic readiness frameworks. Exclusion criteria removed studies limited to external attacks or unrelated security domains. The review emphasized forensic relevance, evidence preparation, and the operational characteristics of SaaS environments. Insights from this process informed the design of the readiness framework and highlighted gaps in existing research.

B.3 Conceptual Framework

The proposed DFR to Bust Insider Threats (DFR-BUST) framework integrates evidence preparation processes with analytic support to improve investigative outcomes in SaaS environments. It builds on cloud forensic principles that highlight the need for structured logging, evidence preservation, and investigative clarity [19, 14]. The framework consists of five components (as shown in Figure 1): SaaS Evidence Preparation (SEP), Detection Engine Process (DEP), Evidence Archival and Preservation (EAP), Analyst and Forensic Review Process (AFR), and Audit and Documentation Process (ADP).

DFR-BUST defines a structured readiness pipeline that supports proactive evidence preparation, behavioral analytic support, evidence archival and preservation, and analyst-driven forensic review within SaaS environments. Figure 1 presents a high-level view of the DFR-BUST readiness pipeline and the core components that operationalize these functions.

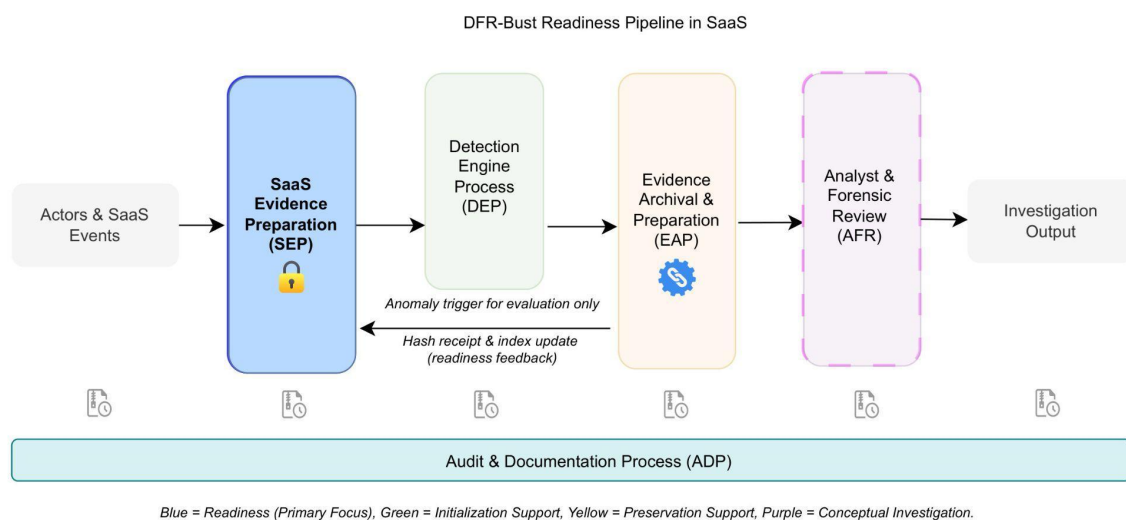


Figure 1. High-level view of the DFR-BUST readiness pipeline in a SaaS environment

SaaS Evidence Preparation identifies essential logs and ensures consistency across SaaS applications. Data Extraction and Processing normalizes events for investigative use. Behavioral Analytics Support provides anomaly focused insights using machine learning as a supportive mechanism [11, 10]. Evidence Preservation and Interpretation follows ISO 27043 guidance on maintaining forensic soundness [5].

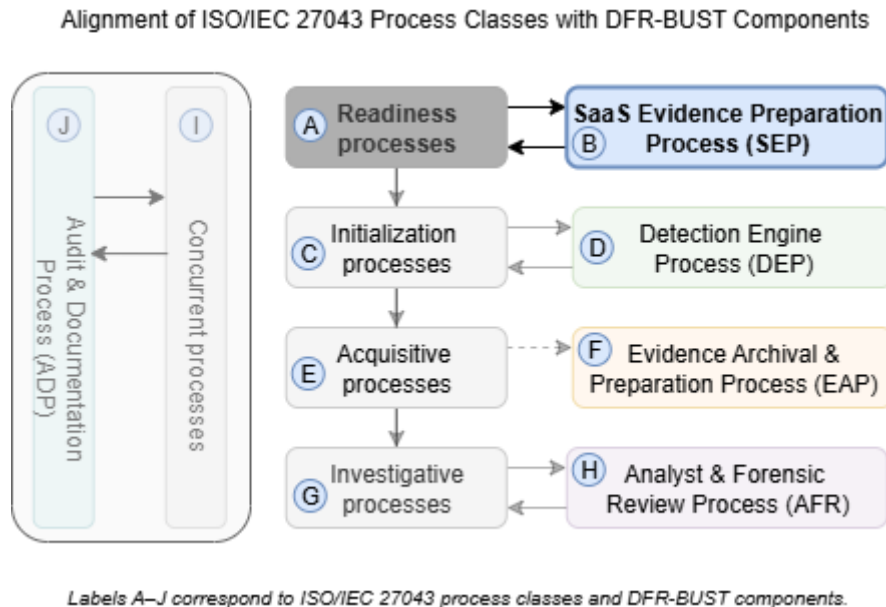


Figure 2. Alignment of ISO/IEC 27043 process classes with DFR-BUST components

To demonstrate this alignment, Figure 2 maps the DFR-BUST components to the ISO/IEC 27043 process classes, highlighting how the readiness architecture supports standardized investigative phases.

SaaS Evidence Preparation (SEP) establishes the foundation by identifying essential logs and ensuring that evidence is generated in a consistent and reliable manner across SaaS applications. Detection Engine Process (DEP) analyzes normalized activity data to identify deviations from normal behavior and provide early analytic indicators of suspicious activity. Evidence Archival and Preservation (EAP) secures collected artifacts through integrity preservation and structured storage to support later reconstruction. Analyst and Forensic Review Process (AFR) enables human investigators to interpret analytic outputs, correlate events, and derive investigative meaning from preserved evidence. Audit and Documentation Process (ADP) captures the procedural, contextual, and chain of custody information required to maintain investigative reliability and compliance.

Together, these components create a readiness structure that enables investigation across all phases of insider activity (before, during, and after an insider incident).

B.4 Software Requirements Specification

Requirements specification incorporated forensic soundness requirements including evidential integrity and chain of custody practices informed by

established forensic literature [15, 16]. Functional requirements included consistent log generation, normalization, anomaly alerting, investigative review and ISO 27043 readiness alignment [5]. Non-functional requirements focused on scalability, modularity, and SaaS compatibility. These requirements guided the structure of the framework and informed decisions about the type of data to collect, how to process it, and how to ensure that analytic outputs could support forensic interpretation.

B.5 High-Fidelity Prototype and Scenario-Based Proof of Concept

Figure 3 provides a high-level timeline of the insider incident as represented in the adapted scenario. The emphasis of the timeline is on how user behaviour changes over time rather than on specific calendar dates. In narrative terms, the scenario unfolds across four phases as labelled in the figure.

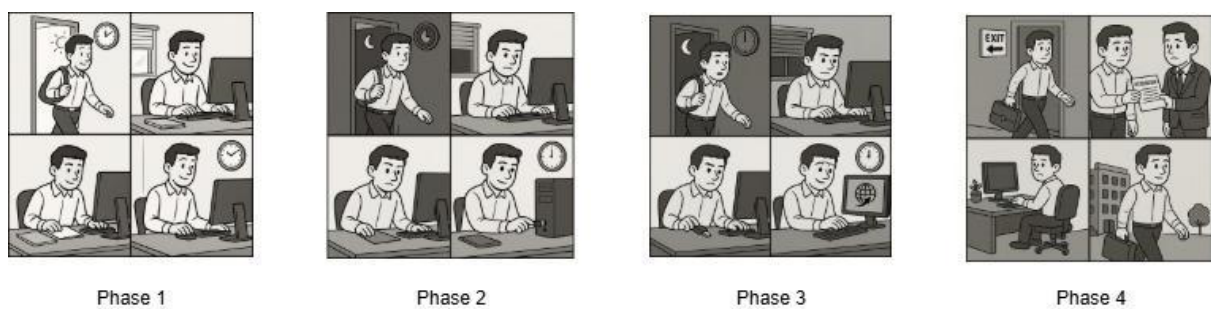


Figure 3. High level timeline of the Adapted Insider Scenario

Phase 1 (baseline behaviour) represents an initial period where the employee works strictly within office hours, accesses routine business files, and shows no abnormal web or removable-device activity. This period is modelled by the Detection Engine as representative of normal departmental behaviour. Phase 2 (emerging deviation) reflects a shift where the user begins logging in after hours, accessing a broader range of files than usual, and intermittently connecting a removable drive. At this stage, the behaviour is unusual but not yet overtly malicious. Phase 3 (escalation and exfiltration) is characterised by frequent after-hours logins, increased removable-device usage, and outbound data transfers to an external site, during which multiple anomalous user-days are flagged by the DFR-BUST framework. Phase 4 (departure) occurs shortly after the exfiltration activity, where the employee resigns from the organization. The preserved logs and analytical outputs across all phases form the basis for retrospective investigation and potential legal or disciplinary processes. This phased timeline provides the backbone for the proof-of-concept demonstration, with subsequent sections illustrating how forensic artefacts are captured and processed as the scenario progresses.

A high fidelity prototype was created to demonstrate how the readiness framework operates during an insider threat scenario. Scenario based demonstrations are commonly used in insider threat research to validate analytic and investigative processes [17]. The prototype simulated a SaaS environment in which a user transitions from normal behavior to suspicious activity. The scenario included four phases illustrated in Figure 3: Phase 1 (baseline behavior), Phase 2

(early deviation), Phase 3 (escalation and exfiltration), and Phase 4 (departure). Logs such as logon events, file activity, and device interactions were collected and processed with timestamp alignment for forensic reliability. Behavioral analytics leveraged insights from unsupervised anomaly detection studies [11, 10, 12]. The prototype illustrated how evidence flows through the readiness framework and how alerts support early recognition.

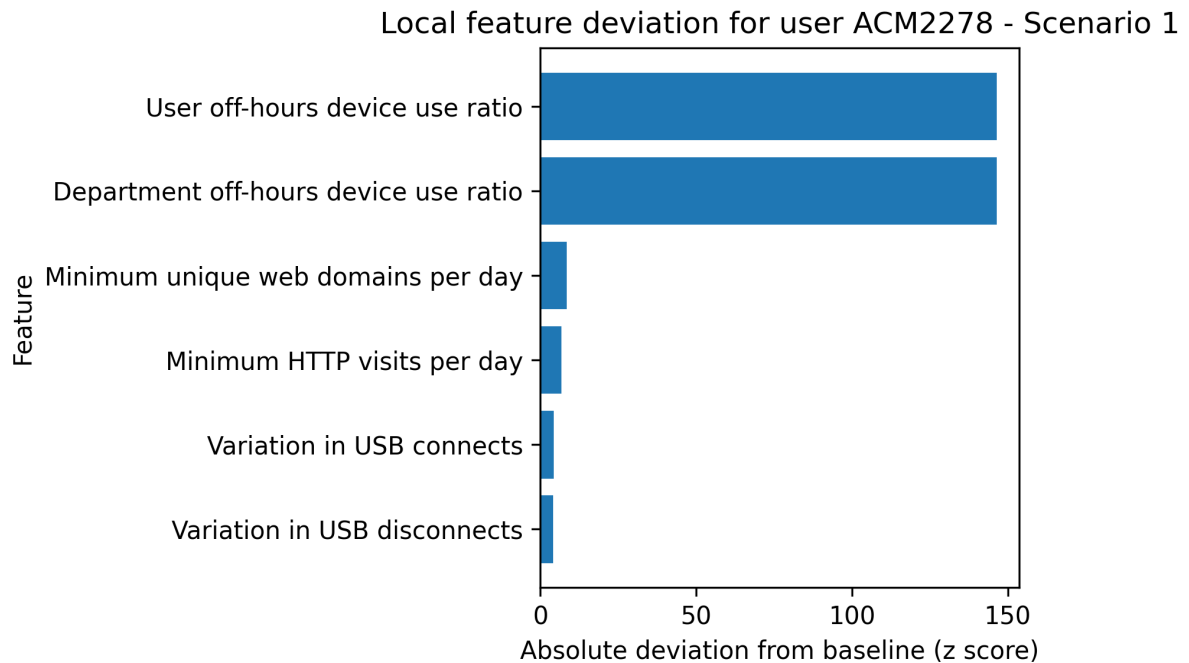


Figure 4. Local Feature deviation for User

Figure 4 presents the local feature deviation analysis, illustrating which behavioural attributes diverged most significantly from the user’s baseline and contributed to the anomaly signal.

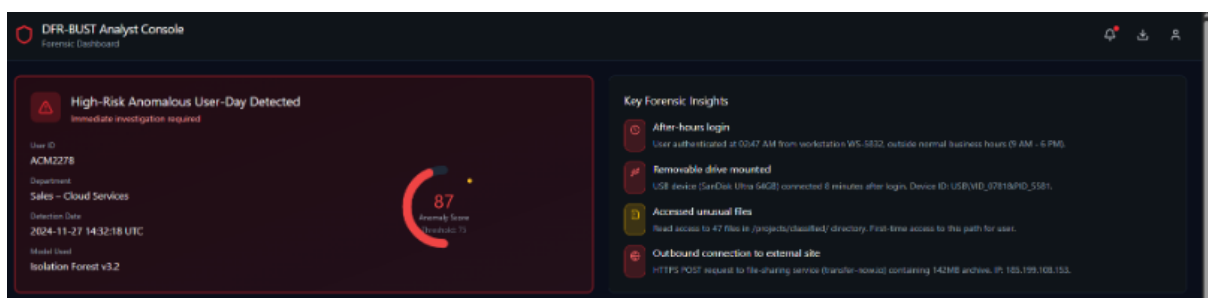


Figure 5. DFR-BUST Analyst Console showing anomaly alert for a user.

Figure 5 further visualizes the temporal escalation of anomaly intensity across scenario phases. Machine learning served as a supportive mechanism that improves situational awareness rather than replacing investigative judgment.

C.6 Evaluation and Validity

Evaluation considered evidence completeness, log consistency, and alignment with forensic readiness principles defined in ISO 27043 [5]. Forensic evaluation approaches often prioritize investigative usefulness rather than statistical performance [3, 4, 18]. Scenario based reasoning assessed whether the framework supported timely detection and reliable reconstruction. Expert insights from prior readiness and cloud forensic research informed the evaluation logic. Machine learning outputs were interpreted according to forensic expectations rather than predictive accuracy, consistent with findings in anomaly detection research [11].

D. Results

The readiness framework demonstrated clear support for insider threat mitigation during the scenario based proof of concept. Results reflect how each phase of user activity was captured, analyzed, and preserved in a structured and forensically reliable manner. During the baseline phase, routine logon activity, file access, and browsing patterns were consistently collected and stored. No alerts were generated, which confirmed that the system established a stable representation of normal behavior. This baseline served as the reference for later forensic comparison.

Early deviation was recognized when the user began accessing files outside their usual working pattern. The framework captured these deviations and behavioral analytics highlighted the unusual activity. Although the anomaly signals were low, they provided early awareness and allowed investigators to monitor the user more closely. As deviations continued, the framework recorded recurring patterns that differed from the user's baseline. Structured logs preserved each event, allowing investigators to reconstruct the timeline accurately.

The escalation and exfiltration phase included sudden increases in file access frequency, removable device interaction, and attempts to transfer information outside the environment. These actions produced stronger anomaly signals that aligned with typical indicators of insider misuse. The readiness components ensured that all events were preserved with synchronized timestamps. Figure 4 highlights the most significant local feature deviations contributing to the anomaly signal, while Figure 5 shows how these anomaly scores escalate across the scenario phases, supporting investigative interpretation.

Following the escalation, the user resigned from the organization. The framework preserved all relevant artifacts, which enabled retrospective investigation and supported potential legal or disciplinary action. The structured and consistent logs allowed investigators to connect the sequence of events from baseline to departure, providing a complete and coherent narrative of the incident in line with ISO 27043 readiness expectations.

Overall, the results show that the readiness framework improves early recognition of insider activity, strengthens evidence preservation, and supports investigative interpretation. The scenario demonstrates how structured evidence preparation and analytic support can enhance forensic readiness in cloud-based environments.

E. Discussion

The findings demonstrate that proactive evidence preparation combined with behavioral analytics can strengthen insider threat investigations in cloud environments. The readiness framework enabled the consistent capture and preservation of activity across all scenario phases, which improved investigative clarity and supported earlier recognition of suspicious behavior. These outcomes align with DFR principles described in prior work and reinforce the value of structured evidence management in Software as a Service settings.

A key implication of this study is the improvement in investigative visibility. Traditional insider threat investigations often suffer from incomplete activity traces due to inconsistent logging practices, distributed cloud architecture, or reactive approaches that begin only after harm has occurred. By generating structured logs from the beginning of the user lifecycle, the readiness framework reduced evidential gaps and improved the ability to reconstruct events. This supports the emphasis in ISO 27043 on preparedness and reliability of evidence, and aligns with findings from Reddy and Venter [3] that highlight the importance of consistent organizational readiness.

The integration of behavioral analytics provided additional investigative support. While machine learning was not the focus of the study, anomaly signals helped identify deviations early enough to guide investigative attention. These findings complement previous research showing that behavioral modeling improves insider detection while also addressing one of the limitations in detection focused studies. Most anomaly detection research prioritizes accuracy but does not account for evidential integrity or forensic usability. The results here show that when analytics are embedded into a readiness structure, they can support forensic interpretation without replacing investigative judgment.

Despite these strengths, several limitations must be acknowledged. The prototype scenario was simulated, and real-world cloud environments may introduce variability in log availability, provider constraints, and event granularity. Machine learning outputs were used to support forensic reasoning rather than predict malicious behavior, which means that the framework does not replace full detection systems. The scenario did not test multiple user profiles, large scale datasets, or adversarial attempts to evade detection. These factors limit the generalizability of the results and present opportunities for future validation.

The study contributes to forensic science by demonstrating how readiness principles can be operationalized in SaaS environments, which have historically lacked clear guidance for evidence preparation. It also bridges the gap identified in the literature between detection oriented techniques and forensic readiness frameworks. By showing how structured evidence flows support both early recognition and post incident investigation, the study positions forensic readiness as a practical and necessary component of insider threat mitigation in cloud based systems.

F. Conclusion

This section concludes the paper by summarizing the main findings and contributions of the proposed DFR-BUST framework. It highlights how the framework supports proactive evidence preparation and forensic investigation in

SaaS environments, and it outlines practical implications and future research directions.

F.1 Summary

This study presented a DFR framework that prepares SaaS environments for insider threat investigation. The framework integrates structured evidence preparation, data processing, behavioral analytics, and forensic interpretation processes that align with ISO 27043 [5]. Through a scenario based demonstration, the framework showed that proactive readiness improves investigative visibility, supports early recognition of suspicious behavior, and strengthens the preservation of evidential artifacts. The structured flow of information from baseline behavior through deviation, escalation, and eventual departure provided investigators with a complete view of the incident and improved the reliability of forensic reconstruction.

F.2 Contribution

The main contribution of this work is the development of a readiness framework designed specifically for SaaS environments, where evidence is fragmented, provider dependent, and sometimes incomplete. Unlike traditional insider threat detection methods that focus solely on accuracy, the proposed framework embeds analytic outputs within a forensic readiness structure that prioritizes evidential integrity and investigative clarity. This approach brings together areas that are often treated separately: anomaly based behavioral monitoring and DFR. The framework offers a practical foundation for organizations seeking a forensic aware method for insider threat mitigation.

F.3 Future Directions

Several directions can extend this research. Future work should validate the framework in real world SaaS environments that include diverse user populations, multiple departments, and varying log granularities. Additional studies can incorporate adversarial behavior to evaluate resistance to evasion. The analytic components can be expanded to include explainable machine learning or hybrid models that combine supervised and unsupervised methods. There is also room to explore automated chain of custody tooling, enhanced timestamp synchronization techniques, and organization wide readiness policies. Collaboration with cloud providers may enable improved log access and standardized evidence formats.

F.4 Closing Statements

DFR is essential for modern organizations that depend on cloud services and face increasing risks from insider activity. This study offers a structured and practical approach that improves preparedness, enhances investigative reliability, and supports earlier recognition of potential misuse. By integrating analytic support within a readiness framework and aligning with international forensic standards, the work contributes to more resilient and accountable cloud based environments.

G. References

- [1] L. Liu, O. De Vel, Q. L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1397–1417, 2018.
- [2] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," *Electronics*, vol. 9, no. 9, Art. no. 1460, 2020.
- [3] K. Reddy and H. S. Venter, "The architecture of a digital forensic readiness management system," *Computers & Security*, vol. 32, pp. 73–89, 2013.
- [4] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," *Australian Journal of Forensic Sciences*, vol. 50, no. 5, pp. 552–591, 2018.
- [5] International Organization for Standardization, *ISO/IEC 27043:2015 Incident investigation principles and processes*, Geneva, Switzerland, 2015.
- [6] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–40, 2019.
- [7] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Computers & Security*, vol. 104, Art. no. 102221, 2021.
- [8] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," in *Proceedings of the 2013 Information Security for South Africa (ISSA)*, 2013, pp. 1–5.
- [9] A. Singh, R. A. Ikuesan, and H. S. Venter, "Secure storage model for digital forensic readiness," *IEEE Access*, vol. 10, pp. 19469–19480, 2022.
- [10] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, "Insider threat detection based on user behavior modeling and anomaly detection algorithms," *Applied Sciences*, vol. 9, no. 19, Art. no. 4018, 2019.
- [11] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," in *Proceedings of the AAAI Workshops*, 2017, pp. 224–231.
- [12] D. C. Le and N. Zincir-Heywood, "Anomaly detection for insider threats using unsupervised ensembles," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 30–44, 2020.
- [13] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis," *Big Data Analytics*, vol. 1, no. 1, Art. no. 6, 2016.
- [14] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Computers & Security*, vol. 38, pp. 103–115, 2013.
- [15] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Amsterdam, The Netherlands: Elsevier Academic Press, 2011.
- [16] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: The diagnostic work of IT security incident response," *Information Management & Computer Security*, vol. 18, no. 1, pp. 26–42, 2010.

- [17] J. Glasser and B. Lindauer, "Bridging the gap: A pragmatic approach to generating insider threat data," in Proceedings of the 2013 IEEE Security and Privacy Workshops, 2013, pp. 98–104.
- [18] K. Kent, S. Chevalier, and T. Grance, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86, 2006.
- [19] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," Digital Investigation, vol. 10, no. 1, pp. 34–43, 2013.
- [20] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, vol. 9, no. 2, pp. 71–80, 2012.
- [21] S. Makura, H. Venter, V. R. KEBANDE, N. M. Karie, R. A. Ikuesan, and S. Alawadi, "Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring," Security and Privacy, vol. 4, no. 3, e149, 2021.