

SIEM Logs as Digital Evidence: Reliability, Integrity, and Challenges in Cybercrime Investigations

 **Ernest Kobbie Doe**

School of Computing, University of Portsmouth, Portsmouth, United Kingdom

Received: 06 Sep 2026
Revised: 27 Sep 2026
Accepted: 01 Oct 2026
Published: 12 Oct 2026

Volume 03 **Issue** 10, 2026
Page No - 09-16
DOI: - 10.64917/fecsit/Vol3Iss10-02

Article Citation: Doe, E. K. (2026). SIEM Logs as Digital Evidence: Reliability, Integrity, and Challenges in Cybercrime Investigations. *Frontiers in Emerging Computer Science and Information Technology*, 3(10), 09–16.
<https://doi.org/10.64917/fecsit/Vol3Iss10-02>

Copyright: © 2026 The Authors. Published by FECSIT under the Creative Commons CC BY License

Abstract

Security Information and Event Management (SIEM) systems are widely used to collect, correlate, and analyse logs for cybersecurity monitoring and incident response. However, the growing reliance on SIEM data during digital forensic and cybercrime investigations raises important questions about whether such logs can be treated as reliable digital evidence. This paper examines the factors that influence the evidential value of SIEM logs through a conceptual research design supported by a structured integrative review of literature from cybersecurity, digital forensics, log management, incident response, and digital evidence preservation. The analysis develops four propositions relating to source-log quality, preservation and chain of custody, transparency of SIEM processing, and the effects of timestamp inconsistencies, weak access controls, incomplete logging, and deliberate manipulation. The findings show that SIEM evidential reliability depends on the entire logging lifecycle and not just on the kind of SIEM platform used. High-quality source logs, strong integrity controls, clear chain of custody procedures, and transparent correlation and normalisation processes strengthen evidential value, while incomplete records, weak preservation practices, and manipulation reduce confidence in forensic conclusions. The paper argues that SIEM platforms should be treated as part of a wider digital evidence ecosystem. Organisations should therefore incorporate forensic requirements into logging, preservation, and security-monitoring practices before incidents occur. Future empirical research should test the proposed relationships across different SIEM platforms and investigative environments.

Keywords: Security Information and Event Management, Digital evidence, Digital forensics, log integrity, Chain of custody, Cybercrime investigation

1. Introduction and Background

Digital systems continuously generate logs that record activities across operating systems, applications, networks, security devices, and cloud environments. These records have become important to cybersecurity because they can help organisations identify suspicious behaviour, investigate security incidents, and reconstruct events after an attack (Khan et al., 2023; Nelson et al., 2025; Scarfone & Souppaya, 2023). As information technology environments continue to expand, the amount of log data generated has also increased, making manual analysis increasingly difficult. Security Information and Event Management (SIEM) systems help address this problem by collecting, centralising, correlating, and analysing logs from different sources to improve

security monitoring and threat detection (Măcăneață, 2024; Scarfone & Souppaya, 2023). SIEM platforms are mainly designed to support security monitoring and incident response. They help security teams identify unusual activities, correlate events, generate alerts, and investigate patterns that may indicate malicious behaviour (Măcăneață, 2024; Nelson et al., 2025). However, the same logs collected for operational security may later become important during digital forensic and cybercrime investigations. Event logs can provide information about authentication attempts, user activities, system changes, network connections, and other events that help investigators reconstruct what happened during an incident (Azahari & Balzarotti, 2024; Khan et al., 2023). They can therefore become an important source of digital evidence where an investigation depends on establishing a sequence of activities across different systems.

However, the presence of information within a SIEM platform does not automatically make that information reliable digital evidence. Digital evidence must be identified, collected, acquired, and preserved in a manner that protects its evidential value (Azam et al., 2023; Guttman et al., 2022; International Organisation for Standardisation (ISO), 2012; Ismail & Akram Zainol Ariffin, 2025). Investigators must also be able to understand where the evidence originated, how it was handled, and whether its integrity has been maintained. This becomes more complex in SIEM environments because log data may pass through several processes before it reaches an investigator. These processes can include collection, parsing, normalisation, enrichment, correlation, filtering, storage, and retrieval. Although such processing can make security information easier to analyse, it may also create questions about provenance and the relationship between the original record and the information eventually presented during an investigation (ISO, 2012; Olegård et al., 2025).

The quality of the original logs is another important consideration. Azahari & Balzarotti (2024) examined logging practices across 60 open-source applications and found that many logs lacked information needed for effective security and forensic analysis. Some applications did not record timestamps, while others lacked identifiers needed to correlate related events. Olegård et al. (2025) similarly found that conventional logs may contain too much or too little information and often lack the causal information needed to establish relationships between events across different systems. These findings show that centralising information in a SIEM cannot completely correct weaknesses that already exist at the source. If important events were never recorded, timestamps are missing, or contextual information is incomplete, later correlation may still produce an incomplete reconstruction

of the incident (Azahari & Balzarotti, 2024; Olegård et al., 2025).

The volume of log data creates an additional challenge. Event-log analysis can be difficult and time-consuming because potentially relevant events may be hidden among large quantities of normal system events (Khan et al., 2023; Măcăneață, 2024). SIEM systems reduce some of this burden through automated correlation, filtering, and alert generation. However, operational usefulness and evidential reliability are not necessarily the same. An alert may be sufficient to direct a security analyst towards suspicious activity, while a forensic investigation requires stronger assurance about the origin, completeness, integrity, and interpretation of the underlying records (Khan et al., 2023; Olegård et al., 2025).

This creates an important gap between security monitoring and digital evidence. Existing literature has examined log management, SIEM-based monitoring, event analysis, and digital forensic readiness, but the conditions under which SIEM logs can be considered dependable evidence require further conceptual examination. This paper therefore examines the reliability, integrity, and challenges associated with using SIEM logs as digital evidence in cybercrime investigations. It brings together literature from cybersecurity, digital forensics, log management, and incident response to examine how source-log quality, preservation, processing, chain of custody, and resistance to manipulation influence evidential value. These relationships are subsequently developed into propositions to provide a structured explanation of when SIEM logs can support reliable digital forensic conclusions.

2. Literature Review and Proposition Development

2.1 SIEM Systems and the Forensic Value of Logs

SIEM systems were developed to improve visibility across complex information technology environments. They collect logs from different sources, centralise them, and support correlation, alerting, investigation, and incident response (Măcăneață, 2024; Scarfone & Souppaya, 2023). This centralised view can also assist post-incident investigations because investigators may need to reconstruct timelines across endpoints, applications, network devices, and cloud services. Logs therefore sit between operational cybersecurity and digital forensics. They are generated mainly for monitoring and administration, but they may later provide information about who performed an action, when it occurred, and how events developed across a system (Khan et al., 2023; Olegård et al., 2025).

The forensic value of a log, however, depends on more than its availability. A SIEM may contain millions of logs, but the presence of a log does not by itself establish that it is complete, accurate, authentic, or sufficient for evidential purposes. Digital evidence must be preserved and examined in a manner that maintains confidence in its integrity and origin (Azam et al., 2023; Guttman et al., 2022; ISO, 2012; Ismail & Akram Zainol Ariffin, 2025). This is important because SIEM systems are designed primarily for security monitoring, while forensic investigations also require reliable reconstruction and clear evidence handling.

2.2 Source-Log Quality, Completeness, and Contextual Value

The reliability of SIEM evidence therefore depends not only on the collection and correlation capabilities of the platform, but also on the integrity and completeness of the information available to it at the point of generation. SIEM systems cannot compensate for gaps in the evidential record once data enters the centralised environment (Azahari & Balzarotti, 2024). In forensic contexts, missing context, inconsistent event recording, or insufficient detail at the source can limit the ability to reconstruct an incident accurately, even when the available data is successfully aggregated and correlated (Azahari & Balzarotti, 2024; Olegård et al., 2025). This highlights the importance of treating logging practices as part of the wider forensic readiness of an organisation rather than as a separate technical function (Olegård et al., 2025).

Completeness also affects event correlation. Investigators frequently depend on relationships between records. User identifiers, process information, network addresses, session identifiers, and timestamps can provide the context needed to connect related events. Where these elements are absent, investigators may identify suspicious activity but still struggle to establish how one event relates to another (Azahari & Balzarotti, 2024; Olegård et al., 2025). Khan et al. (2023) further demonstrate the value of contextual analysis in detecting irregular activities in event logs. Therefore, the following proposition is made:

Proposition 1: *The quality, completeness, and contextual richness of source logs are positively related to the reliability of SIEM logs as digital evidence.*

2.3 Integrity, Preservation, and Chain of Custody

Digital evidence can be copied, transferred, modified, or deleted. Preservation is therefore critical to maintaining its evidential value. The National Institute of Standards and Technology (NIST) identifies particular preservation challenges for digital evidence and emphasises appropriate controls throughout its lifecycle (Guttman et al., 2022). Log-management guidance likewise stresses preservation

while logs are stored at the source, transferred to the logging infrastructure, and retained within that infrastructure (Scarfone & Souppaya, 2023).

Chain of custody (CoC) provides a documented history of how evidence was collected, handled, transferred, stored, and accessed (Jansen & Ayers, 2004; Kruse II & Heiser, 2001). Recent digital-forensic literature continues to identify CoC as important for demonstrating trustworthiness, traceability, and evidential integrity (Nath et al., 2024; Patil et al., 2024). In a SIEM environment, investigators may need to show how an event reached the platform, who had access to it, whether it was altered, and how the evidence used in the investigation was extracted. Weak documentation or uncontrolled access can create uncertainty even where the underlying event occurred. Therefore, the following proposition is made:

Proposition 2: *Strong preservation controls and a demonstrable chain of custody are positively related to the evidential value of SIEM logs in cybercrime investigations.*

2.4 Correlation, Normalisation, and Transformation of Log Data

One of the main strengths of SIEM technology is its ability to combine logs from different sources. Correlation can reveal relationships that would be difficult to identify manually, while normalisation allows different log formats to be represented more consistently (Măcăneală, 2024; Olegård et al., 2025). These processes can reduce fragmentation and help analysts follow activity across systems. However, the logs displayed by a SIEM may not be identical in form to the original because fields may have been parsed, reformatted, enriched, or mapped into a common schema. For forensic purposes, such transformation should be transparent and reproducible. Investigators should be able to distinguish original data from information added or interpreted by the SIEM. This is particularly important where automated processing may affect timestamps, field names, event categories, or relationships between logs. Research on forensic tool validation also shows that reliable conclusions depend on processes that can be tested and reproduced (Ismail & Akram Zainol Ariffin, 2025). Therefore, the following proposition is made:

Proposition 3: *SIEM correlation, normalisation, and contextual enrichment enhance the interpretation of log evidence when transformations are transparent, traceable, and reproducible.*

2.5 Timestamp Reliability and Log Manipulation

Timestamps are fundamental to timeline reconstruction because investigators use timestamps to establish the order and relationship of events. However, timestamps can be

affected by incorrect system clocks, clock drift, system malfunction, or deliberate tampering. Recent research shows that relying on timestamps without validation can create inaccurate forensic timelines (Dreier et al., 2024). Source-log studies also show that, in some cases, timestamps may be absent altogether, further limiting timeline reconstruction (Azahari & Balzarotti, 2024).

Logs may also be modified, deleted, or selectively disabled to conceal activity. These risks make integrity preservation, restricted access, secure transfer, and independent corroboration critical when SIEM data is used as evidence (Guttman et al., 2022; Scarfone & Souppaya, 2023). A SIEM can centralise evidence and make later manipulation more difficult, but it cannot automatically guarantee that every source data is genuine or complete. Therefore, the following proposition is made:

Proposition 4: *Timestamp inconsistencies, weak access controls, incomplete logging, and deliberate log manipulation are negatively related to the reliability of SIEM logs as digital evidence.*

These four propositions suggest that SIEM evidential value is not determined by the platform alone. It develops from the interaction between source-log quality, evidence preservation, processing transparency, and resistance to manipulation. These relationships provide the conceptual basis for the methodological approach and subsequent discussion. The framework captured in Figure 1 shows that the reliability and evidential value of SIEM logs is the central outcome of the paper. This outcome is strengthened by three positive drivers and weakened by one negative driver. It further suggests that where evidential reliability is strong, SIEM logs are more likely to support credible forensic reconstruction and stronger cybercrime investigations.

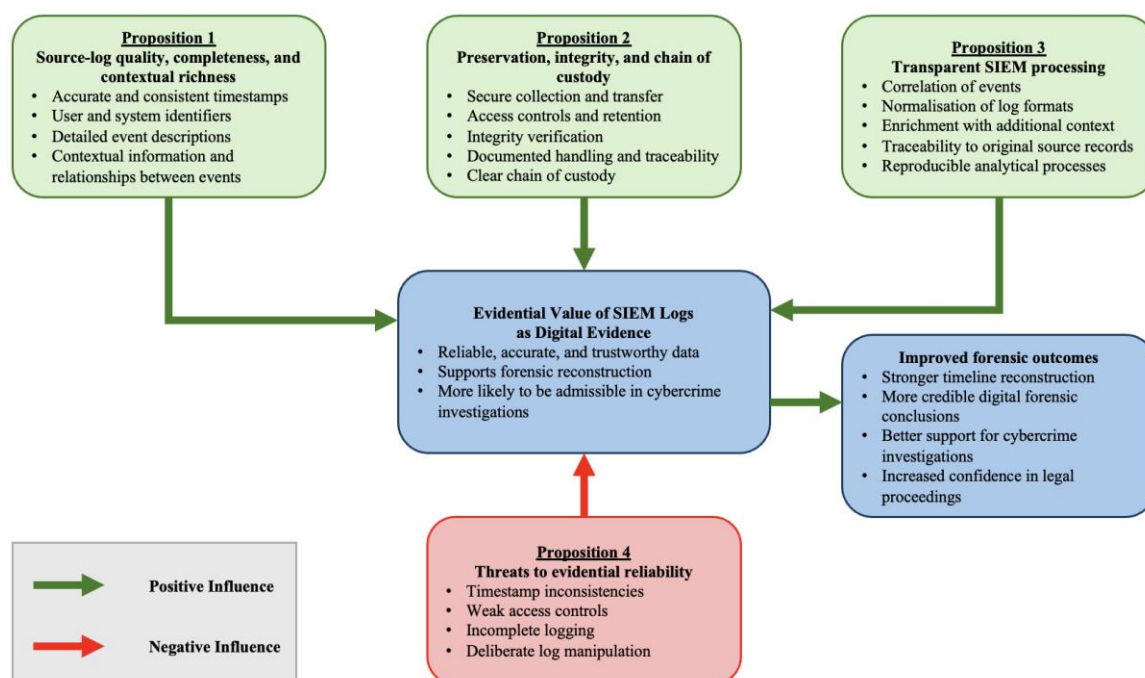


Figure 1: Conceptual framework of the factors that influence the evidential value of SIEM logs in cybercrime investigations

3. Methodological Approach

3.1 Research Design

This paper adopts a conceptual research design supported by a structured integrative review of existing literature. A conceptual approach is appropriate where the purpose is to bring together knowledge from different research areas and develop clearer relationships between concepts (Jaakkola, 2020; Snyder, 2019). Integrative reviews are particularly useful where a topic is fragmented across different disciplines because they allow existing evidence to be compared, combined, and interpreted to generate new conceptual understanding (Snyder, 2019;

Torraco, 2016). This approach fits the present study because research relevant to SIEM logs as digital evidence is distributed across cybersecurity, digital forensics, log management, incident response, and evidential integrity.

3.2 Literature Identification and Selection

The literature base was developed through structured searches focused on peer-reviewed journal articles, conference papers, standards, and authoritative technical guidance. Searches targeted terms including “SIEM,” “security information and event management,” “logs as digital evidence,” “event logs,” “log integrity,” “forensic logging,” “chain of custody,” “log correlation,”

“timestamp reliability,” and *“digital evidence preservation.”* Priority was given to recent literature to reflect current SIEM and digital-forensic environments, while older foundational standards and methodological sources were retained where they remained relevant.

Sources were selected according to their direct relevance to the research problem and their ability to explain one or more of the concepts under examination. Literature was excluded where it discussed general cybersecurity monitoring without meaningful relevance to logging, digital evidence, forensic investigation, or evidential reliability. Unlike a systematic review, the purpose was not to identify and count every publication on SIEM technology. The aim was to obtain a sufficiently broad and credible body of literature from which relationships between key concepts could be developed. This is consistent with conceptual research, where source selection should be guided by the theoretical purpose of the paper and clearly explained (Jaakkola, 2020; Snyder, 2019).

3.3 Analysis and Proposition Development

The selected literature was analysed through thematic synthesis. Findings were grouped around four recurring areas: source-log quality and completeness; integrity, preservation, and chain of custody; correlation and normalisation; and timestamp reliability and log manipulation. Studies within each area were compared to identify points of agreement, limitations, and relationships relevant to evidential value.

These relationships informed the development of the propositions presented in Section 2. The analysis subsequently uses theory synthesis to integrate previously separated streams of research and develop a conceptual explanation of the conditions under which SIEM logs may be considered reliable digital evidence (Jaakkola, 2020; Torracco, 2016). The propositions therefore provide an analytical framework for interpreting and discussing the findings that follow.

4. Findings and Discussion

4.1 Evidential Reliability Begins at the Source

The conceptual synthesis shows that the evidential value of SIEM logs begins before the data enters the SIEM platform. A SIEM can centralise, correlate, and analyse records, but it remains dependent on what the original systems record. Where source logs contain sufficient timestamps, user identifiers, event descriptions, session information, and other contextual details, investigators are in a stronger position to reconstruct a timeline of events. Where these elements are missing, later analysis may remain incomplete regardless of the capabilities of the

SIEM platform (Azahari & Balzarotti, 2024; Khan et al., 2023; Olegård et al., 2025).

This finding supports Proposition 1, which states that the quality, completeness, and contextual richness of source logs positively influence the reliability of SIEM logs as digital evidence. Azahari & Balzarotti (2024) found important weaknesses in application logging, including missing timestamps and insufficient information for connecting related events. Olegård et al. (2025) similarly show that conventional logging often provides insufficient causal information for understanding how events relate across applications. This suggests that evidence quality cannot be created entirely through centralisation. SIEM technology may make existing records easier to search and connect, but it cannot reliably reproduce an event that was never logged in the first place.

Completeness should therefore be understood in relation to the investigative question. A large quantity of logs may provide little forensic value if they do not capture the activities required to reconstruct a timeline of events. In contrast, carefully selected logs that show relationships between users, processes, systems, and network activity may provide stronger evidential context. This is particularly important where investigators must move beyond showing that an alert occurred to explaining how an incident developed over time (Khan et al., 2023; Olegård et al., 2025).

4.2 Integrity, Preservation, and Chain of Custody

Investigators must demonstrate that the logs used in an investigation have been appropriately preserved. Digital evidence can be copied, transferred, modified, or deleted with relative ease, creating specific challenges for preservation and long-term evidential reliability (Guttman et al., 2022). For SIEM data, these concerns apply throughout the log lifecycle, including generation, transmission, storage, access, extraction, and eventual presentation during an investigation (Guttman et al., 2022; Scarfone & Souppaya, 2023).

This supports Proposition 2. Strong preservation controls and a demonstrable CoC increase confidence that the evidence being examined is the same information that was originally collected. Recent studies continue to identify traceability, integrity, and accountability as important elements of digital evidence management (Nath et al., 2024; Patil et al., 2024).

In a SIEM environment, CoC extends beyond documenting possession of a physical device. Organisations may need to document the source of a log, the system used to collect it, how long it was retained, who had administrative access, and how relevant records were exported for forensic analysis. Hashing and other integrity-

verification mechanisms can further support the detection of unauthorised modification, in addition to proper documentation and evidence-handling procedures (Guttman et al., 2022; Nath et al., 2024; Patil et al., 2024).

4.3 The Benefits and Risks of SIEM Processing

The analysis also shows that SIEM processing creates both forensic benefits and evidential risks. Correlation can help investigators connect events that would otherwise remain separated across different systems. Normalisation can make different log formats easier to compare, while enrichment can add useful context to an event. These functions are particularly valuable where an investigation involves several hosts, applications, or network components and requires reconstruction of related activities (Olegård et al., 2025; Scarfone & Souppaya, 2023).

However, processing also creates a distinction between the source log and the representation produced by the SIEM. Fields may be renamed, converted, filtered, enriched, or classified before they are presented to an analyst. An automatically generated alert may therefore contain an interpretation of several underlying logs. For evidential purposes, investigators should be able to move from the SIEM output back to the underlying logs and explain how they were produced. This reflects broader forensic requirements for transparent and reproducible analytical processes (Ismail & Akram Zainol Ariffin, 2025).

The synthesis therefore supports Proposition 3, but with an important condition. Correlation, normalisation, and enrichment improve evidential interpretation only when the processing is transparent, traceable, and reproducible. A correlated SIEM event may provide an effective starting point for an investigation, but confidence becomes stronger where investigators can identify the sources and reproduce the analytical relationship between them. This distinction is important for operational accuracy and evidential reliability.

4.4 Timestamp Reliability and Resistance to Manipulation

Time is another central issue. Digital forensic investigations frequently rely on timestamps to determine the timeline of events. However, a timestamp should not automatically be treated as an unquestionable representation of when an event occurred. Incorrect system clocks, differences between systems, missing timestamps, and deliberate manipulation can create inconsistencies in event reconstruction (Azahari & Balzarotti, 2024; Dreier et al., 2024).

Dreier et al. (2024) demonstrate that other forms of timing information, including sequence and positional

information, can assist investigators in identifying timestamp inconsistencies and ordering events even when conventional timestamps are unreliable. This indicates that SIEM timelines should ideally be corroborated using multiple artefacts and not just depend on a single time field. Such corroboration becomes particularly important where there is a possibility of tampering.

These findings support Proposition 4. Weak access controls, incomplete logging, timestamp inconsistencies, and deliberate log manipulation reduce confidence in SIEM evidence. Centralised logging may improve preservation and visibility, but it does not make the data automatically immune to manipulation. Secure transmission, restricted administrative access, appropriate retention, integrity checking, and comparison with independent sources can reduce this risk (Guttman et al., 2022; Scarfone & Souppaya, 2023).

4.5 An Integrated View of SIEM Evidential Value

The four propositions altogether suggest that SIEM evidential reliability should be viewed as the outcome of several connected factors and not just a property of the SIEM product itself. Source-log quality provides the initial evidential foundation. Preservation and CoC protect that information as it moves through the investigative process. Transparent correlation and normalisation help investigators interpret events without losing sight of their sources. Finally, resistance to manipulation and reliable temporal information reduce uncertainty when reconstructing timelines.

The conceptual relationship can therefore be expressed as follows: source-log quality, preservation and CoC, and transparent SIEM processing strengthen evidential reliability, while incomplete logging, timestamp uncertainty, weak controls, and manipulation weaken it. These factors are also interdependent. Strong preservation cannot compensate for an important event that was never recorded, while detailed logs may still have limited evidential value if their integrity cannot be ascertained. SIEM logs are therefore most useful as digital evidence when forensic requirements are considered throughout the logging lifecycle and not just after a cybersecurity incident has occurred. This position is consistent with recent work on forensic readiness, preservation, and CoC, which emphasises that reliable evidence depends on preparation before an investigation begins (Guttman et al., 2022; Nath et al., 2024; Olegård et al., 2025).

5. Implications for Digital Forensic and Cybercrime Practice

The findings have important implications for organisations that rely on SIEM during cybersecurity incidents and subsequent investigations. First, forensic

considerations should be incorporated into logging strategies before an incident occurs. Organisations should identify which systems generate evidentially important logs and ensure that logs contain sufficient timestamps, identifiers, event descriptions, and contextual information to support later reconstruction (Azahari & Balzarotti, 2024; Olegård et al., 2025). Collecting large quantities of data without considering forensic relevance may increase storage and analysis burdens without necessarily improving evidential value.

Second, organisations should treat log preservation as part of digital forensic readiness. SIEM logs should be preserved through appropriate access controls, retention policies, secure transmission, and integrity-verification procedures. Evidence handling should also be documented so that investigators can establish where relevant logs originated, how they were collected, who accessed them, and whether they were altered during storage or analysis (Guttman et al., 2022; Nath et al., 2024; Patil et al., 2024). These measures can strengthen confidence in the evidence if findings are later challenged.

Third, investigators should avoid treating SIEM alerts as complete forensic conclusions. Alerts are often produced through automated correlation, normalisation, enrichment, or predefined detection rules. They can therefore provide useful investigative leads but should be supported by examination of the underlying logs and, where possible, independent artefacts from endpoints, network devices, applications, or other systems (Khan et al., 2023; Olegård et al., 2025). This allows investigators to distinguish observed events from interpretations generated by the SIEM.

The findings also have implications for security operations centres (SOCs). Analysts responsible for detection engineering should consider how logging and correlation decisions may affect future investigations. Detection rules should therefore not only identify suspicious behaviour but also preserve sufficient context for explaining why an alert was generated. Collaboration between security analysts, incident responders, and digital forensic practitioners can help ensure that monitoring practices support both immediate threat detection and later evidential requirements.

Overall, organisations should view SIEM as part of a wider evidence ecosystem, though their forensic value depends on how logs are generated, protected, processed, documented, and corroborated throughout the evidence lifecycle.

6. Suggestions for Future Research

Although this paper develops a conceptual explanation of the factors that influence the evidential value of SIEM

logs, further empirical research is needed to test these relationships. Future studies could examine whether the four propositions developed in this paper hold across different SIEM platforms, operating environments, and types of cybercrime investigation. Controlled experiments could be used to compare how platforms such as Splunk, Microsoft Sentinel, IBM QRadar, and Wazuh preserve, normalise, correlate, and export log data for forensic purposes.

More research is also required on source-log quality. Existing studies show that many applications do not generate logs with sufficient contextual information for forensic reconstruction (Azahari & Balzarotti, 2024; Olegård et al., 2025). Future work could therefore develop measurable criteria for determining whether a log source is forensically sufficient before it is integrated into a SIEM environment. Such research could examine minimum requirements for timestamps, identifiers, event relationships, and contextual information.

Another important area is the evidential effect of automated processing. Modern SIEM platforms use machine learning, behavioural analytics, and automated correlation to identify suspicious activity. Future studies should examine whether these processes introduce changes that affect traceability, reproducibility, or interpretation when SIEM outputs are later presented as evidence. Particular attention should be given to distinguishing original log records from derived alerts and analytical outputs.

Further research should also investigate CoC in cloud-based and distributed SIEM environments. As organisations increasingly rely on managed and cloud-hosted security platforms, evidence may pass through multiple systems, service providers, and jurisdictions. This can create additional questions about control, preservation, and evidential accountability (Guttman et al., 2022; Nath et al., 2024). Empirical studies involving investigators, security analysts, and legal professionals could therefore help establish practical standards for using SIEM logs in real-world cybercrime investigations.

7. Conclusion

SIEM platforms have become important to cybersecurity monitoring and incident response because they centralise large volumes of log data and support correlation across different systems. Their growing use also means that SIEM logs are more likely to be relied upon during digital forensic and cybercrime investigations. However, this paper shows that the presence of data within a SIEM platform does not automatically make it reliable digital evidence.

The conceptual analysis identified four main factors that influence evidential value. First, SIEM evidence depends on the quality, completeness, and contextual richness of the source logs. Missing timestamps, weak identifiers, or incomplete event recording can limit later reconstruction, even where sophisticated correlation tools are available (Azahari & Balzarotti, 2024; Olegård et al., 2025). Second, integrity protection, preservation, and a clear CoC are important for demonstrating that records have not been improperly altered during collection, storage, or analysis (Guttman et al., 2022; Nath et al., 2024). Third, correlation, normalisation, and enrichment can improve interpretation, but their evidential value depends on whether the transformations are transparent and reproducible. Finally, timestamp inconsistencies, weak access controls, incomplete logging, and deliberate manipulation can reduce confidence in the resulting evidence.

This paper therefore argues that SIEM evidential reliability should be understood as the outcome of the entire logging lifecycle and not just as a property of the SIEM platform used. Reliable use requires attention to how logs are generated, transmitted, preserved, processed, accessed, and corroborated. Organisations that incorporate these requirements into their logging and security-monitoring practices are better positioned to use SIEM logs not only for detecting threats, but also for ensuring credible digital forensic conclusions. Future empirical research should test the propositions developed in this paper across different SIEM technologies and investigative environments.

References

1. Azahari, A., & Balzarotti, D. (2024). On the inadequacy of open-source application logs for digital forensics. *Forensic Science International: Digital Investigation*, 49, 301750.
2. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, 2(1).
3. Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy*, 15(6), 12–17.
4. Dreier, L. M., Vanini, C., Hargreaves, C. J., Breiting, F., & Freiling, F. (2024). Beyond timestamps: Integrating implicit timing information into digital forensic timelines. *Forensic Science International: Digital Investigation*, 49, 301755.
5. Guttman, B., White, D. R., Williams, S., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers*.
6. International Organization for Standardization (ISO). (2012). *ISO/IEC 27037:2012 Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*.
7. Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, 20(9), e0331683.
8. Jaakkola, E. (2020). Designing conceptual articles: four approaches. *AMS Review*, 10(1), 18–26.
9. Jansen, W., & Ayers, R. P. (2004). *SP 800-72. Guidelines on PDA Forensics*. National Institute of Standards & Technology.
10. Khan, S., Parkinson, S., & Murphy, C. (2023). Context-based irregular activity detection in event logs for forensic investigations: An itemset mining approach. *Expert Systems with Applications*, 233, 120991.
11. Kruse II, W. G., & Heiser, J. G. (2001). *Computer forensics: incident response essentials*. Pearson Education.
12. Măcăneafă, C. (2024). Overview of security information and event management systems. *Informatica Economica*, 28(1), 15–24.
13. Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 11–20.
14. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management. *NIST Special Publication*, 800.
15. Olegård, J., Axelsson, S., & Li, Y. (2025). When is logging sufficient?—Tracking event causality for improved forensic analysis and correlation. *Forensic Science International: Digital Investigation*, 52, 301877.
16. Patil, H., Kohli, R. K., Puri, S., & Puri, P. (2024). Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egyptian Journal of Forensic Sciences*, 14(1), 12.
17. Scarfone, K., & Souppaya, M. (2023). *Cybersecurity log management planning guide*.
18. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.
19. Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review*, 15(4), 404–428.