Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Meta-Analysis of Incident Response Failures Due to Telemetry Misconfigurations in SME Networks

Dr Kazi Abdul Mannan

drkaziabdulmannan@gmail.com

Center for Academic & Professional Career Development and Research (CAPCDR)
https://orcid.org/0000-0002-7123-132X

Nusrat Jahan Mim

Shanto-Mariam University of Creative Technology https://orcid.org/0009-0000-5898-0986

Research Article

Keywords: Incident Response, Telemetry Misconfiguration, SME Networks, AAA, NTP, Syslog, SOC Failure, Virtual Sandbox

Posted Date: August 5th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10592797/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Abstract

Incident response effectiveness in Small-to-Medium Enterprise (SME) networks depends critically on the integrity of foundational telemetry services-Authentication, Authorization, and Accounting (AAA), Network Time Protocol (NTP), and Syslog. When these services are misconfigured, Security Operations Centers (SOCs) lose the ability to attribute actions, reconstruct timelines, and detect ongoing activity, resulting in systematic incident-response failures. This meta-analysis synthesizes secondary evidence from simulation-based studies and peer-reviewed literature (2015–2026) that examine the operational consequences of telemetry degradation within realistic SME topologies. Drawing principally on a documented Cisco Packet Tracer sandbox that implements a four-floor multi-VLAN architecture, the analysis contrasts a verified “Good State” baseline against a deliberately induced “Chaos State.” Findings demonstrate three recurring failure modes: forensic timeline collapse following NTP desynchronization, loss of non-repudiation after AAA disablement, and total visibility blindness after Syslog interruption. These failures translate directly into delayed detection, incomplete containment, and compromised recovery. The meta-analysis concludes that unverified assumptions about telemetry integrity constitute a latent systemic risk and that risk-free virtual sandboxes offer a practical mechanism for pre-emptively identifying and mitigating such misconfigurations before they precipitate incident-response collapse in production environments.

1. Introduction

Security Operations Centers (SOCs) function as the nerve centre of enterprise cyber defence, responsible for continuous monitoring, detection, analysis, and response to security incidents [11]. Their effectiveness rests on three interdependent telemetry services that answer the fundamental questions of incident investigation: who performed an action (AAA), when the action occurred (NTP), and what the action entailed (Syslog) [10]-[13]. AAA provides identity and non-repudiation; NTP supplies the temporal scaffolding required for causal reconstruction; and Syslog furnishes the persistent event record that enables both real-time detection and post-incident forensics [3], [9], [10], [12]. Collectively these services form the telemetry substrate upon which SIEM correlation, playbook execution, and forensic analysis depend.

In Small-to-Medium Enterprise (SME) environments the same dependencies hold, yet resource constraints often lead to incomplete verification of telemetry integrity. Secondary literature repeatedly documents that organisations treat the correct functioning of AAA, NTP, and Syslog as an implicit assumption rather than a continuously validated control [11]. When that assumption proves false-whether through configuration drift, hardware failure, or human error-incident response processes degrade in predictable and severe ways. The resulting failures are not merely technical; they translate into delayed containment, incomplete attribution, and elevated residual risk.

The core problem addressed by this meta-analysis is the systematic failure of incident-response processes that arises when foundational telemetry is misconfigured. SOC analysts must frequently

adjust or validate security configurations and response playbooks. Performing these activities on live production networks exposes the organisation to downtime, policy violations, and service disruption [1], [15]. Simultaneously, the absence of a verified telemetry baseline means that even routine incident handling can collapse when timestamps diverge, identities become unattributable, or event streams cease. Secondary sources confirm that alert fatigue further compounds the problem by reducing analyst capacity for thorough investigation [6]. Without a risk-free method of exposing and quantifying these failure modes, SMEs remain vulnerable to latent telemetry-induced response breakdowns.

A meta-analytic synthesis of secondary evidence drawn from controlled simulation studies offers a practical path forward. Cisco Packet Tracer environments that replicate authentic four-floor SME topologies with departmental VLANs and dedicated server rooms allow researchers to induce controlled telemetry failures and observe their precise impact on incident-response capability [1], [5]. By aggregating findings across such studies and the broader literature on AAA, NTP, and Syslog, the present analysis identifies recurring failure patterns and evaluates the protective value of virtual sandbox validation. The rationale is therefore both diagnostic-revealing how telemetry misconfigurations produce response failures-and prescriptive-demonstrating how risk-free environments can prevent those failures.

The objectives of this meta-analysis are:

- To synthesise secondary evidence on the operational consequences of AAA, NTP, and Syslog misconfigurations in SME-scale networks.
- To identify the characteristic incident-response failure modes produced by each form of telemetry degradation.
- To evaluate the protective contribution of virtual sandbox frameworks in preventing telemetry-induced response failures.
- To derive practical recommendations for continuous verification of telemetry integrity within SME SOCs.

This meta-analysis contributes to both research and practice. It consolidates fragmented secondary findings into a coherent account of how telemetry misconfigurations precipitate incident-response collapse. For practitioners, it underscores that investment in advanced SIEM and SOAR platforms is undermined if the underlying telemetry substrate is unverified. For researchers, it highlights the methodological value of dual-state (Good State / Chaos State) simulation designs and points toward future primary studies that can quantify the economic cost of telemetry-induced failures. Ultimately, the work supports a shift from assumed telemetry health to continuously validated observability as a foundational control for SME cyber defence [1], [5], [11].

2. Literature Review

The secondary literature establishes that accurate time synchronisation, attributable identity, and continuous event logging are prerequisites for effective incident response. NTP, formalised by Mills [12],

remains the dominant mechanism for distributing coherent time across packet-switched networks. Subsequent studies confirm that clock divergence directly impairs forensic reconstruction and industrial monitoring applications [3], [4]. When device clocks drift, the temporal ordering required by digital forensics becomes unreliable, producing what secondary sources term forensic failure [3], [12].

Syslog has evolved from a debugging facility into a primary data source for anomaly detection, failure prediction, and root-cause analysis [9], [13]. Contemporary research employs statistical models, deep-learning architectures such as DeepLog, and scalable platforms such as LogLens to extract sequential and quantitative features from log streams [9]. When remote Syslog forwarding is interrupted, the SOC loses its primary sensory input, resulting in total visibility blindness regardless of the health of other services [5], [9], [13].

AAA frameworks supply the identity and authorisation substrate that renders logged events attributable. Authentication confirms identity, authorisation enforces policy, and accounting records activity [10], [14]. Simulation studies demonstrate that TACACS+-based AAA policies improve campus-network security by centralising credential verification [1], [10]. When the AAA server is disabled, non-repudiation collapses and internal actions become unattributable [5], [10], [14].

SOC literature further emphasises that alert fatigue and incomplete telemetry interact to degrade response quality [6], [11]. Automation and AI-supported triage systems presuppose complete, correctly timestamped, and attributable event data; when that precondition fails, even sophisticated analytics cannot compensate [7].

The analytical framework organises secondary evidence around three linked constructs: the structural fidelity of the simulated SME topology, the dual-state integrity of the telemetry triad, and the resulting incident-response outcomes.

Structural fidelity is established by four-floor topologies that allocate VLANs 10–80 to departmental traffic and VLAN 100 to servers, thereby approximating realistic SME segmentation [5]. Core routers (F1, F2, F3) and associated switches form the forwarding plane upon which AAA, NTP, and Syslog services are overlaid. Secondary Packet Tracer studies confirm that such designs support realistic evaluation of routing, access control, and security policies without physical infrastructure [1], [2], [15].

Dual-state integrity is examined by comparing a verified Good State against a deliberately induced Chaos State. In the Good State, TACACS+ authentication records identities, NTP maintains synchronisation across core routers, and Syslog events from all subnets converge on a central collector [5]. In the Chaos State, each service is independently degraded: NTP synchronisation is broken, the TACACS+ server is disabled, and Syslog forwarding is interrupted. Secondary observation shows that these degradations produce three characteristic failure modes-forensic timeline collapse, loss of accountability, and total visibility blindness-that map directly onto incident-response process breakdowns [5].

Incident-response outcomes are evaluated against the classic phases of detection, analysis, containment, eradication, and recovery. Secondary evidence indicates that forensic failure (NTP) primarily impairs analysis and recovery; loss of accountability (AAA) undermines attribution during containment and post-incident review; and visibility blindness (Syslog) disables detection itself, rendering subsequent phases moot [5], [9]-[13]. The framework therefore links specific telemetry misconfigurations to discrete stages of response failure.

Cross-study comparison further reveals that while individual protocols have been examined extensively, their joint degradation within a single realistic SME topology remains underexplored. The integrated dual-state design synthesised in this meta-analysis therefore supplies both explanatory power and practical diagnostic value.

Despite extensive literature on individual telemetry protocols and on campus-network simulation, secondary sources contain few systematic examinations of how concurrent or sequential misconfigurations of AAA, NTP, and Syslog produce cascading incident-response failures in SME environments. Existing work tends either to treat each protocol in isolation or to focus on higher-layer analytics while assuming telemetry integrity. Consequently, practitioners lack an aggregated evidence base that maps specific misconfigurations to discrete response failures and that evaluates the protective role of virtual validation. This gap motivates the present meta-analysis.

The reviewed secondary literature establishes three conclusions relevant to the meta-analysis. First, AAA, NTP, and Syslog form an interdependent telemetry triad whose integrity is a precondition for effective incident response. Second, misconfiguration of any element produces a characteristic and severe response failure mode. Third, virtual sandboxes that support controlled dual-state experimentation offer a practical means of exposing these failure modes before they occur in production. These conclusions provide the empirical and conceptual foundation for the theoretical and methodological sections that follow.

3. Theoretical and Conceptual Framework

The theoretical foundation rests on the proposition that incident-response capability is an emergent property of continuous, attributable, and temporally coherent observability. Drawing on SOC theory and classical security principles [11], the framework posits that detection, analysis, containment, and recovery cannot succeed if the telemetry substrate is compromised. AAA supplies non-repudiation; NTP supplies temporal coherence; Syslog supplies the event stream. Disruption of any single element cascades into systemic response failure, independent of the sophistication of higher-layer tools. This stance aligns with socio-technical perspectives that recognise technological controls as only as effective as the human and procedural processes that depend upon them [6], [11].

Alert fatigue literature further supports the theory: when analysts cannot trust timestamps or attribute actions, verification effort increases and response is delayed [6]. Thus telemetry integrity is not merely a technical prerequisite but a precondition for effective human-machine collaboration within the SOC.

Conceptually the problem space is organised into three layers: topological representation of an authentic SME network, dual-state configuration of the telemetry triad, and mapping of observed degradations onto incident-response phases. The first layer ensures ecological validity; the second operationalises the independent variable (telemetry integrity); the third measures the dependent variables that matter to practitioners-detection latency, attribution completeness, and recovery fidelity. An integrated workflow follows: construct the multi-floor topology → establish Good State baselines → induce controlled Chaos State misconfigurations → record response-relevant impacts → restore baseline and document lessons for playbook design. The workflow is fully reversible, reflecting the risk-free character of the virtual sandbox.

The integrated workflow comprises four sequential phases synthesised from secondary evidence: topology construction inside Cisco Packet Tracer using VLAN segmentation and multi-router design; baseline service deployment (TACACS+, NTP hierarchy, centralised Syslog); controlled degradation of each telemetry service; and comparative evaluation against incident-response impact criteria. Because each phase can be snapshotted and restored, the workflow supports both single-protocol and multi-protocol interaction studies without cumulative state pollution.

4. Methodology

This meta-analysis employs a qualitative, secondary-data methodology. Primary empirical material is drawn from a documented Packet Tracer-based SME sandbox that implements and degrades AAA, NTP, and Syslog services [5]. Supporting literature spanning 2015–2026 supplies theoretical context, comparative findings, and validation of individual protocol behaviours [1]-[15].

The research framework follows a structured four-phase sequence synthesised from secondary sources. Phase 1 constructs an authentic four-floor SME topology containing three departmental floors and a dedicated server room. VLANs 10–80 segment departmental traffic; VLAN 100 isolates servers. Three core routers (F1-router, F2-router, F3-router) provide Layer-3 connectivity. Phase 2 deploys the Good State: TACACS + AAA is configured on all routers, NTP clients synchronise to a central server, and Syslog messages from every subnet are forwarded to a centralised collector. Phase 3 induces the Chaos State by selectively disabling or misconfiguring each service while preserving the underlying topology. Phase 4 records the observable impact on identity attribution, temporal coherence, and event visibility, thereby quantifying incident-response degradation [5]. Secondary sources are integrated at each phase to corroborate observed behaviours: NTP literature confirms forensic timeline collapse [3], [12]; AAA literature confirms loss of non-repudiation [10], [14]; and Syslog literature confirms total visibility blindness [9], [13].

4.1 Variable Selection

Independent variables comprise the operational status of each telemetry service (enabled/synchronised versus disabled/misconfigured). Dependent variables are the three incident-response outcomes:

forensic timeline integrity, user accountability (non-repudiation), and overall network visibility. Control variables include topology, VLAN design, and traffic patterns, which remain constant across Good State and Chaos State observations.

4.2 Cross Validation

Cross validation is achieved by comparing simulation outcomes against independent secondary sources. The observation that NTP failure destroys temporal ordering is corroborated by Mills [12] and subsequent synchronisation studies [3], [4]. The observation that TACACS+ disablement eliminates identity attribution aligns with AAA literature [10], [14]. Consistency between simulated behaviour and published theory strengthens internal validity of the meta-analytic synthesis.

4.4 Model Evaluation

Model evaluation proceeds through qualitative comparative analysis. Side-by-side examination of Good State and Chaos State logs, authentication records, and time-synchronisation status yields a structured impact matrix (Telemetry Element × State × Incident-Response Impact). The matrix is further interpreted against SOC operational requirements reported in the secondary literature [6], [11], ensuring that evaluation criteria remain practitioner-relevant.

4.5 Software

All primary simulation evidence was generated using Cisco Packet Tracer, a widely adopted network-simulation platform that supports configuration of routing, switching, AAA, NTP, and Syslog services without physical hardware [1], [2], [15]. Secondary literature was managed and synthesised using standard academic databases and citation-management tools.

4.6 Ethical Issues

Because the entire study relies on secondary data and virtual simulation, no human subjects, live production systems, or sensitive organisational data were involved. Ethical considerations are limited to accurate representation of published sources and transparent acknowledgement of the secondary character of the evidence base.

5. Results

Meta-analytic synthesis of the Packet Tracer sandbox and supporting literature yields a consistent pattern of incident-response failure modes across the telemetry triad. In the Good State, centralised TACACS+ authentication successfully records user identities and attributes administrative actions; NTP maintains synchronised time across core routers F1, F2, and F3; and Syslog events from VLANs 10–80 converge cleanly on the fourth-floor collector [5]. The resulting telemetry stream supplies the SOC with complete identity, temporal, and content information, satisfying the prerequisites for detection, analysis, containment, and recovery.

In the Chaos State, three independent failure modes appear. When NTP synchronisation is broken, edge-node timestamps diverge from the logging infrastructure; the SOC can no longer reconstruct accurate attack sequences, producing forensic failure that impairs analysis and recovery phases [3], [5], [12]. When the TACACS+ server is disabled, access tracking ceases; internal actions become unattributable and threat actors can operate without non-repudiation, undermining containment and post-incident attribution [5], [10], [14]. When Syslog forwarding is interrupted, remote event generation stops entirely; the SOC loses all capability to detect configuration changes or policy violations, resulting in total visibility blindness that disables detection itself [5], [9], [13].

These outcomes are summarised in the comparative impact matrix derived from secondary evidence:

Table 1
Meta-analytic mapping of telemetry misconfigurations to incident-response failure modes (synthesised from secondary sources).

Telemetry Element	Good State	Chaos State	IR Failure Mode
NTP	Centralised time synchronisation maintained across F1-F3	Time synchronisation between edge nodes and logging infrastructure lost	Forensic Failure → Analysis & Recovery collapse
AAA (TACACS+)	Centralised authentication records user identities and actions	TACACS+ server disabled; access tracking eliminated	Loss of Accountability → Containment & Attribution fail
Syslog	Events from VLANs 10–80 centralise on fourth-floor server	Syslog configurations broken; remote event generation stops	Total Visibility Blindness → Detection disabled

6. Discussion

The meta-analytic evidence demonstrates that the telemetry triad is both necessary and fragile. Each protocol contributes a non-substitutable dimension of observability; the failure of any single dimension produces a distinct and severe incident-response impairment. Forensic failure arising from NTP desynchronisation is particularly consequential because modern playbooks and digital-forensic procedures presuppose accurate temporal ordering [3], [12]. Without synchronised clocks, even complete Syslog records become chronologically ambiguous, undermining root-cause analysis and legal evidentiary value.

Loss of AAA accountability is equally critical. In the absence of centralised authentication records, internal threat actors or compromised credentials can effect configuration changes without leaving an attributable trail [10], [14]. This condition directly violates the non-repudiation principle that underpins both security policy and regulatory compliance. The Chaos State experiments confirm that the mere presence of logging infrastructure is insufficient; identity must be bound to each logged action.

Total visibility blindness resulting from Syslog failure represents the most complete form of response impairment. When remote event generation ceases, the SOC loses situational awareness regardless of the health of AAA and NTP. Secondary literature on log analytics [9], [13] underscores that advanced detection algorithms-DeepLog, LogAnomaly, or SIEM correlation rules-are powerless without a continuous event stream. Consequently, organisations that invest heavily in higher-layer analytics while neglecting foundational telemetry risk a false sense of security.

The virtual sandbox approach mitigates these risks by allowing controlled, reversible experimentation. Because Packet Tracer supports instantaneous state restoration, analysts can explore the boundary between functional and failed telemetry without residual impact on production systems [1], [5], [15]. This capability transforms playbook validation from a high-stakes production activity into a routine, low-cost exercise. The secondary literature further indicates that such sandboxes also serve pedagogical purposes, enabling students and junior analysts to internalise the dependencies among AAA, NTP, and Syslog before encountering them in live environments [1], [15].

A notable limitation of the secondary evidence base is the relative scarcity of large-scale, multi-protocol empirical studies. Most published work examines individual protocols or higher-layer security mechanisms. The integrated treatment of the telemetry triad within a realistic SME topology therefore remains an emerging rather than mature research theme. Future primary studies could usefully extend the Chaos State methodology to additional protocols and to hybrid physical-virtual testbeds, and could quantify the economic impact of telemetry-induced response failures.

7. Conclusion

This meta-analysis has synthesised secondary literature on the operational consequences of AAA, NTP, and Syslog misconfigurations, demonstrating how telemetry degradation systematically precipitates incident-response failures in SME networks. The analysis successfully addressed its objectives by consolidating evidence on failure modes, mapping those modes onto incident-response phases, and evaluating the protective contribution of virtual sandbox frameworks.

Key findings confirm that synchronised time, centralised authentication, and remote event logging form an interdependent telemetry triad. Disruption of any element produces a characteristic incident-response failure: forensic collapse (NTP), loss of accountability (AAA), or total visibility blindness (Syslog). Virtual sandboxes realised in Cisco Packet Tracer provide a safe, reversible platform for exposing these failures before they occur in production.

The meta-analysis contributes a coherent mapping of telemetry misconfigurations to discrete incident-response failure modes and consolidates previously fragmented secondary evidence into a single practitioner-relevant narrative focused on SME environments.

Organisations should treat continuous verification of AAA, NTP, and Syslog integrity as a mandatory operational control rather than an implicit assumption. Investment in higher-layer SIEM and SOAR

platforms should be preceded by documented assurance that the underlying telemetry substrate is sound. Virtual sandbox environments offer a practical means of achieving this assurance at minimal cost and risk.

Future research should extend the Chaos State methodology to additional telemetry protocols, explore hybrid physical-virtual testbeds, quantify the economic cost of telemetry-induced response failures, and conduct longitudinal studies of sandbox adoption within operational SME SOCs.

References

1. Swapna K, Nandeeshwar B, Gagan B, Aravind A, Ravi B Campus Network Design Using Cisco Packet Tracer, 2025 10th International Conference on Signal Processing and Communication (ICSC), Noida, India, 2025, pp. 45–50. 10.1109/ICSC64553.2025.10968176
2. Stănescu C, Georgian A, Predusca G, Carciumarescu D, Angelescu N, Puchianu C (2023) IoE Simulation with Cisco Packet Tracer, 2023 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 01–06. 10.1109/ECAI58194.2023.10194081
3. Kawamura T, Fukushi M, Hirano Y, Fujita Y, Hamamoto Y (2018) A Network-Based Event Detection Module Using NTP for Cyber Attacks on IoT, 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), Takayama, Japan, pp. 86–91. 10.1109/CANDARW.2018.00025
4. Agarwal FFAA, Sharma D, Yadav DS (2025) and S. M. R., Time Synchronization Performance Analysis Based on NTP Data Captured from Two Distant Locations, International Conference on Innovation in Computing and Engineering (ICE), Greater Noida, India, 2025, pp. 1–6. 10.1109/ICE63309.2025.10984309
5. Ahsan M, Mim NJ, Khan MAH (2026) Building a Risk-Free SOC Sandbox: A Packet Tracer Framework for Validating AAA, NTP, and Syslog Telemetry Integrity
6. Goud KN, Jain K, Krishnan P, 9th International Conference on Intelligent Computing and, Systems C (2026) A Semi-Supervised and Evasion-Aware Framework for Reducing Alert Fatigue in Security Operations Centers (SoC), (ICICCS), Erode, India, 2026, pp. 2007–2013. 10.1109/ICICCS67901.2026.11502746
7. Özgözler E, Varol A, Tanrıverdi İ, ASOC) (2026) Event-Driven Agentic SOC (ED-: Supervisor-Based LLM Framework for Dynamic Incident Response and SOAR Orchestration, 2026 14th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA, pp. 1–5. 10.1109/ISDFS69419.2026.11458922
8. Yang G, Lei Z, Wang H, Dou Y, Xie Y (2014) Analysis of the RADIUS Signalling Based on CDMA Mobile Network, Sixth International Conference on Intelligent Human-Machine Systems and Cybernetics, Hangzhou, China, 2014, pp. 270–274. 10.1109/IHMSC.2014.167
9. Chovanec M, Havrilla M, Chovancová E (2020) Analysis of Logs in the Environment of Email Services, 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia, 2020, pp. 74–79. 10.1109/ICETA51985.2020.9379260

10. Paolini A, Scardaci D, Liampotis N, Spinoso V, Grenier B, Chen Y (2020) Authentication, Authorization, and Accounting. in Towards Interoperable Research Infrastructures for Environmental and Earth Sciences. Springer, Cham, Switzerland, pp 247–271
11. Vielberth M, Böhm F, Fichtinger I, Pernul G (2020) Security Operations Center: A Systematic Study and Open Challenges. IEEE Access 8:227756–227779. 10.1109/ACCESS.2020.3045514
12. Mills DL (1991) Internet Time Synchronization: The Network Time Protocol, IEEE Transactions on Communications, vol. 39, no. 10, pp. 1482–1493, Oct
13. Anton AA, Csereoka P, Capota EA, Cioargă RD (2024) Enhancing Syslog Message Security and Reliability over Unidirectional Fiber Optics, Sensors, vol. 24, no. 20, Art. no. 6537. 10.3390/s24206537
14. Paolini A, Scardaci D, Liampotis N, Spinoso V, Grenier B, Chen Y (2020) Authentication, Authorization, and Accounting. Towards Interoperable Research Infrastructures for Environmental and Earth Sciences. Lecture Notes in Computer Science, vol 12003. Springer, Cham
15. Rashid NA, Othman Z, Johan R, Sidek SBH Cisco Packet Tracer Simulation as Effective Pedagogy in Computer Networking Course, Proceedings of International Conference on Electrical, Electronics and System Engineering