iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79884

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

A Portable Offline Log Analysis and Security Monitoring System for Air Gapped Networks Using Syslog and MITRE ATT&CK Mapping

Ashithosh Nair, Ashutosh Dhiwar, Dr.Sandeep Kulkarni
School of Engineering Ajeenkya Dy Patil University

Abstract: ***Air-gapped networks, also known as isolated networks, are commonly deployed in highly sensitive environments such as defense infrastructures, industrial control systems, research laboratories, and government facilities where external connectivity is intentionally restricted to reduce exposure to cyber threats. While such isolation strengthens security boundaries, it also creates significant challenges for the continuous monitoring because most modern Security Information and Event Management (SIEM) platforms depend on a centralized infrastructure and internet connectivity. As a result, organizations operating in the isolated environments often rely on manual log inspection or fragmented monitoring mechanisms, which reduces visibility into system activity and increases the possibility of undetected attacks.***

This paper presents PORTSOC, a portable offline log analysis and security monitoring system designed specifically for air-gapped environments. The proposed system collects logs from multiple endpoints using a Syslog-based ingestion mechanism and converts heterogeneous log formats into structured records through parsing and normalization. These events are stored locally in a lightweight SQLite database and analyzed using a rule-based detection engine capable of identifying common adversarial behaviors such as brute-force authentication attempts, credential misuse, suspicious privileged command execution, and security control tampering. Detected events are mapped to MITRE ATT&CK techniques to provide standardized threat classification and improved contextual understanding of security incidents. Experimental evaluation conducted in a controlled environment demonstrates that the system can efficiently process large volumes of log data while maintaining low resource consumption. The results indicate that PORTSOC provides a practical and deployable solution for implementing SOC-style monitoring capabilities in isolated environments where traditional SIEM systems cannot be deployed.

Index Terms: ***Air gapped networks, SIEM, Syslog, SQLite, MITRE ATT&CK, security monitoring, offline analysis, intrusion detection***

I. INTRODUCTION

In recent years, cyberattacks have increased in both frequency and complexity, affecting organizations across multiple domains such as IT enterprises, government institutions, industrial systems, and defense infrastructures. Modern digital environments generate massive volumes of logs from servers, endpoints, network devices, and applications. These logs contain valuable evidence of system activities including user authentication events, network connections, configuration changes, system errors, and suspicious behaviors. Because many cyberattacks leave identifiable traces in system logs, the continuous monitoring and analysis of these records has become one of the most important components of modern cybersecurity operations [1].

Continuous log monitoring plays a crucial role in modern security operations centers (SOCs). Logs generated by operating systems, network devices, and applications provide detailed insights into system activities and user behavior. Security analysts rely on these logs to detect anomalies, investigate security incidents, and identify potential attack patterns. In many cases, early indicators of cyber intrusions such as repeated authentication failures, unauthorized privilege escalation attempts, or abnormal command execution patterns can be observed through log analysis [1]. Therefore, effective log collection and analysis mechanisms are essential for maintaining visibility into system activities and detecting malicious behavior in enterprise environments.

However, implementing such monitoring mechanisms becomes significantly more challenging in environments where external connectivity is restricted. Traditional enterprise monitoring systems are typically designed to operate within connected infrastructures where centralized logging servers and cloud-based analytics platforms can be deployed. Security Information and Event Management (SIEM) systems aggregate logs from multiple sources and perform real-time analysis to detect suspicious activities and potential security incidents [2].

These systems rely on centralized storage and often integrate with external threat intelligence feeds to enhance detection capabilities.

In enterprise networks, SIEM platforms such as Splunk and Elastic Security are commonly used to collect and correlate logs from different systems and network devices in order to detect brute-force attempts, malware activity, policy violations, and unauthorized access events in near real time [3], [4]. However, this centralized approach is not always feasible in highly restricted environments. Many critical infrastructures operate on isolated or air-gapped networks where systems are intentionally separated from the internet and public networks to reduce exposure to external threats. Such environments are commonly found in defense networks, industrial control systems such as ICS and SCADA environments, government facilities, and sensitive research laboratories [9].

Although air-gapped environments improve network isolation and reduce exposure to external cyber threats, they introduce significant challenges for continuous cybersecurity monitoring. Most modern SIEM platforms rely on centralized infrastructure and continuous connectivity for log aggregation, analytics, and threat intelligence updates. In air-gapped environments where internet connectivity is strictly restricted, deploying such systems becomes difficult or impractical. As a result, administrators and security teams often rely on manual log inspection or limited standalone tools, which reduces monitoring visibility and increases the risk of undetected security incidents.

To address these challenges, this paper proposes **PORTSOC**, a portable offline log analysis and security monitoring system specifically designed for isolated environments. The primary objective of PORTSOC is to provide essential Security Operations Center (SOC)-like monitoring capabilities in a lightweight and easily deployable architecture that does not require internet connectivity or large-scale enterprise infrastructure. The proposed system collects logs from multiple endpoints using the Syslog protocol (UDP), which is a widely adopted standard for system log transmission in networked environments [5]. The collected logs are stored locally and processed through parsing and normalization mechanisms that convert heterogeneous log formats into structured records. These normalized events are then stored in a lightweight SQLite database, enabling efficient querying, indexing, and analysis of log data [6].

The system incorporates a rule-based detection engine that analyzes normalized log entries to identify common security events such as authentication failures, repeated login attempts, brute-force attacks, and suspicious command execution patterns. Detected events are further mapped to the MITRE ATT&CK framework in order to provide standardized threat classification and improve the contextual understanding of adversarial behavior [7], [8]. In addition, the system integrates incident correlation mechanisms, offline threat intelligence enrichment, and automated report generation capabilities to assist security analysts in investigating and responding to potential security incidents.

The overall architecture of PORTSOC emphasizes portability, offline functionality, and ease of deployment. The system operates entirely offline and provides a local dashboard for log visualization and alert monitoring. This design allows the monitoring solution to function effectively in restricted environments where external connectivity is unavailable. Through this approach, the proposed system demonstrates that practical security monitoring capabilities can be implemented in air-gapped environments without relying on cloud-based services or large-scale SIEM infrastructures.

II. PROBLEM STATEMENT

In this modern world , SIEM tools which are centralized for monitoring are widely used in most of the traditional enterprise settings which helps in gathering , storing and correlating security logs from various different sources. These systems help track in real time and then notify the SOC teams to identify the risks like malware attacks , privilege abuse or any type of bruteforce attack . To reduce the exposure to this cyber threats, most of the time the networks are kept cut off from the internet in real life environments especially where high security and critical systems are kept. They are also called as air gapped or isolated networks. This air gapped system are quite well in lowering this cyber threats but it has its own operational issues like lack of ongoing, centralized feeds or real time updates. Majority of the SIEM tools in market require internet to run. In this air gapped networks where internet is strictly prohibited due to security reasons , installing and running this SIEM tools are quite impossible. Due to this lack of tools , the security teams often rely on manually reading the logs , which are time consuming and also have high chances of not detecting many attacks at a time

Also as we talk about isolated network, they are not immune to attacks . Threats such as USB based attacks , insider threats , lateral movement within the network , misconfigurations and credential abuse still poses a large amount of possible attacks. Without a efficient log collection and analysis system, these kind of attacks can happen and will cause a significant amount of damage to the company. This is why there is a need of portable and self contained log monitoring system which collects it from different sources, analyse it and provide all the important alerts without any internet connectivity.

This system will fill up the remaining gap in the isolated environments for security purposes. The solution aims to provide a SOC capability tool for this environment which is lightweight, deployable with minimal infrastructure , less complex and does not rely on cloud like other enterprise grade SIEM systems.

III. LITERATURE REVIEW

The field of log analysis and security monitoring has long emphasized the need for structured collection, normalization, and correlation of logs to enable effective detection of malicious activity. Traditional Security Information and Event Management (SIEM) systems centralize logs from disparate sources and provide real time analysis and alerting [1], [2] . However, such systems are typically dependent on substantial infrastructure, centralized storage, and persistent connectivity, making them less suitable for environments with restricted or no internet access [3], [4].

Several studies have explored offline log analysis frameworks capable of extracting meaningful insights from stored datasets, demonstrating that syslog based collection and asynchronous ingestion can support forensic workflows when real time connectivity is unavailable [5]. Other research highlights the challenges posed by heterogeneous log formats and emphasizes the value of robust parsing and normalization techniques to transform raw records into structured events usable for downstream security analytics [1], [6]. In parallel, detection methodologies aligned with structured threat frameworks such as MITRE ATT&CK have been shown to enhance contextual interpretation of adversary behaviour by mapping observable events to known tactics and techniques [7], [8]. This approach improves the relevance and interpretability of alerts generated from log streams. Additionally, research on air gapped systems has demonstrated that isolated networks are not immune to advanced threats and require specialized monitoring approaches [9]. Despite this progress, most existing approaches assume availability of online services, continuous integration with cloud based threat intelligence, or heavyweight processing capabilities [3], [4]. This creates a gap in portable, lightweight, and offline ready solutions for air gapped networks where log data must remain local and security operations must function independently of external dependencies. The proposed Portable Offline Log Analysis and Security Monitoring System addresses this gap by combining multisource syslog ingestion, offline file imports, structured normalization, MITRE ATT&CKaligned rule and heuristic detection, incident correlation, and integrity verification within a locally hosted architecture designed specifically for air gapped operation.

A. Limitations of Existing SIEM Solutions in Air-Gapped Environments

Another important aspect highlighted in existing research is the growing need for the lightweight and portable monitoring solutions in restricted environments. Traditional SIEM platforms such as Splunk and Elastic Security are designed for enterprise-scale deployments and typically depend on centralized log storage, high computational resources, and continuous network connectivity for real-time analysis and threat detection [2], [3], [4]. While these platforms offer the powerful analytics capabilities, they are often unsuitable for air-gapped environments where the centralized infrastructure and external connectivity are not available.

Recent research has therefore explored monitoring approaches that emphasize the localized data processing and lightweight detection mechanisms. These systems focus on portability, reduced infrastructure requirements, and the ability to operate independently within the isolated environments while still providing a meaningful security insights [5], [7], [8]. The PORTSOC system proposed in this research follows a similar direction by combining offline log ingestion, structured normalization, rule-based detection, and incident correlation into a single portable monitoring framework specifically designed for air-gapped networks.

Despite these advancements, many existing monitoring solutions still rely on the centralized infrastructures or assume the availability of continuous network connectivity for data aggregation and threat intelligence updates. Such assumptions limit their applicability in air-gapped environments where strict isolation policies prevent external communication. Therefore, there is a clear need for monitoring architectures that can operate completely offline while still providing effective log analysis, threat detection, and incident correlation capabilities. The PORTSOC system proposed in this research aims to address this gap by providing a lightweight, portable, and fully offline monitoring solution specifically designed for isolated network environments.

IV. METHODOLOGY

The design of the PORTSOC monitoring architecture focuses on three primary goals: portability, offline functionality, and operational simplicity. Since air-gapped environments cannot rely on external services or centralized cloud infrastructure, the system must be capable of performing all monitoring operations locally. This includes log collection, parsing, threat detection, and incident correlation. Additionally, the architecture is designed to operate efficiently on systems with limited computational resources while still providing meaningful threat visibility. To achieve this, the system uses lightweight components and modular processing stages that allow each part of the monitoring pipeline to operate independently.

PORTSOC is designed as an offline first security monitoring pipeline that performs log ingestion, parsing, normalization, detection, and alert correlation entirely inside an isolated environment. The system is built specifically for air gapped networks where cloud based SIEM platforms and real time threat intelligence lookups are unavailable. The architecture follows a modular design to ensure portability, ease of deployment, and maintainability across both Windows and Linux environments. The overall workflow is structured as a staged pipeline: log collection, raw evidence preservation, parsing and normalization, offline enrichment, rule based detection with MITRE ATT&CK mapping, correlation into incidents, risk scoring, visualization, reporting, and integrity verification.

The complete pipeline design is shown in Fig. 1.3, while the detailed modular architecture is illustrated in Fig. 1,1. The database level workflow from raw logs to incidents is summarized in Fig. 1.2.

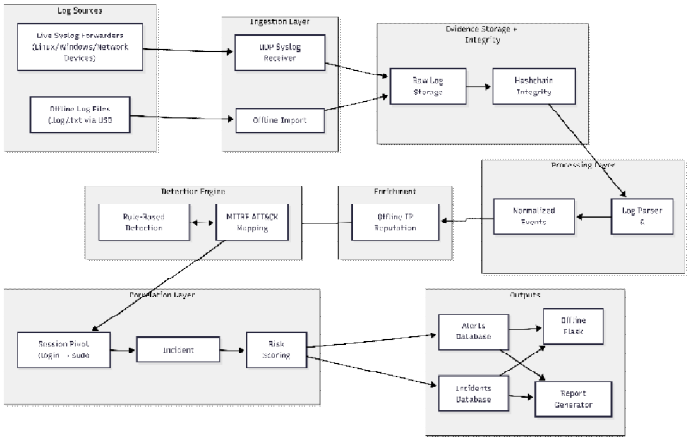


Figure 1.1 Model Architecture Diagram

A. Log Collection (Dual Mode Ingestion)

PORTSOC supports two ingestion modes to ensure compatibility with both live monitoring and post incident forensic analysis. In the first mode, the system runs a lightweight UDP syslog receiver on port 5514 to collect real time logs forwarded from hosts and network devices. This enables continuous monitoring for Linux servers, Windows systems (via syslog agents), routers, and other infrastructure components capable of syslog forwarding. Incoming syslog messages are immediately written into raw log storage to preserve the original evidence exactly as received.

In the second mode, PORTSOC supports offline import of prerecorded log files. Log files in .log or .txt format can be placed inside a predefined directory (storage/import/), allowing the tool to analyze historical logs even if it is deployed after an incident has already occurred. This dual mode design ensures that PORTSOC remains useful for both proactive monitoring and reactive forensic reconstruction. Both ingestion methods are unified into the same downstream processing pipeline as shown in Fig. 1.3.

B. Raw Log Storage and Evidence Preservation

A key objective of PORTSOC is to maintain forensic traceability. This is why the raw logs are treated as a immutable evidence and are stored before any parsing or transforming process. This raw log storage layer keeps the log in its original forma without altering any important objects like syslog headers, timestamps and the message payloads. Thus ensuring that system can handle the raw logs that are kept in the storage even if there are changes been made in the parsing logic or if any events that cannot be normalized. Storing this raw log also helps the security team in auditing and compliance the logs for its authenticity.

C. Parsing and Normalization into Structured Events

Since syslog and system logs are inherently unstructured, PORTSOC applies a parsing layer that extracts structured fields from raw text. This stage converts log entries into normalized records stored in SQLite, enabling consistent querying and correlation across log sources. Each record contains core attributes such as timestamp, source IP, event type, username, and the full raw message. The normalized event schema stored in SQLite is shown in Table 1.1.

Field Name	Type	Description
timestamp	DATETIME	Extracted time of event (syslog

		timestamp if present, else system time)
source_ip	TEXT	Source IP extracted from log line (or LOCAL_HOST if not present)
username	TEXT	Username extracted from authentication or sudo log
event_type	TEXT	Normalized category (AUTH_FAIL, AUTH_FAIL_INVALID_USER, AUTH_SUCCESS, PRIV_ACCESS, SEC_TAMPER, OTHER)
raw_log	TEXT	Full original raw log line preserved for forensic traceability

Table 1.1 Normalized Event Schema Stored in SQLite

The parser is designed to manage realistic Linux authentication and privilege logs, including SSH failures, successful logins, invalid user attempts, and sudo execution traces. In order to avoid evidence loss, logs that do not match predefined patterns are still stored with an OTHER category. This ensures that all collected data remains available for analysis and that the database contains a complete record of the ingested logs. The database transformation workflow from raw logs to events, alerts, and incidents is illustrated in Fig. 1.2.

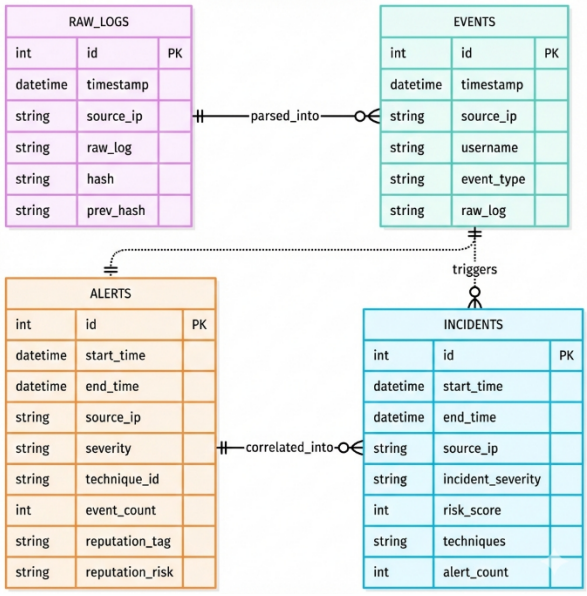


Figure 1.2 Database level workflow

D. Offline Threat Intelligence Enrichment

Improve alert confidence in air gapped environments, PORTSOC implements offline threat intelligence enrichment using a locally stored IP reputation feed. The feed is stored as a CSV file (feeds/ip_reputation.csv) containing IP addresses mapped to a tag (e.g., scanner, botnet, suspicious) and a risk level (high, medium, low). During analysis, extracted source IP addresses are checked against this offline feed. Alerts triggered by high risk IPs are automatically assigned higher severity and stronger evidence weighting. This enrichment layer provides a lightweight approximation of external threat intelligence while remaining fully deployable without internet connectivity, as shown in the enrichment stage of Fig. 1.1.

E. Rule Based Detection Engine with MITRE ATT&CK Mapping

PORTSOC uses a rule based detection engine designed to detect common adversarial behaviors visible in authentication and privilege logs. Each detection module focuses on a specific attack pattern and produces alerts containing severity, technique ID, time window, event count, and enrichment metadata. The detection rules are mapped to MITRE ATT&CK techniques to provide standardized classification and SOCaligned reporting.

Implemented detections include brute force attacks (T1110), password spraying, lowandslow credential guessing, suspicious privileged command execution, identity misuse (T1078), and security control tampering indicators. The detection engine operates as a pipeline, processing normalized logs in time windows and applying thresholdbased and heuristic checks. The complete mapping of detection modules to log sources, rule summaries, MITRE technique IDs, and severity levels is shown in Table 1.2. This design ensures that alerts remain interpretable and aligned with widely accepted adversary behaviour taxonomy.

Detection Name	Log Source (Current)	Rule Logic (Summary)	MITRE ID	Severity
Brute Force Login Attempts	SSH auth logs (syslog / auth.log style)	≥ THRESHOLD failures from same IP in a short window	T1110	High
Identity Abuse / Password Spraying	SSH auth logs	Failures across multiple distinct usernames from one IP within a window	T1110	High
Low & Slow Password Spray	SSH auth logs	Repeated failures from same IP over a long time window (behavioural)	T1110	Medium
Privileged Account Access Attempt	sudo logs	sudo used with USER=root or privilege access pattern detected	T1078	Medium
Suspicious Privileged Command Execution	sudo logs	sudo commands matching high riskpost exploitation patterns (shell spawn, shadow access, SUID search, etc.)	T1548	High
Security Control Tampering	system logs (raw syslog text / imported logs)	keyword based tampering indicators (firewall disabled, logging stopped, audit cleared, defender disabled, etc.)	T1562	High
Policy Violation	system logs / sudo logs	keyword based risky activity violating security policy	T1484 *(or generic policy category)*	Medium
Anomalous Activity (Log Volume Spike)	any ingested logs	log volume from an IP exceeds threshold within brief time	T1499	Medium

Table 1.2 PORTSOC Detection Modules and MITRE ATT&CK Mapping

F. Session Pivoting and Contextual Enrichment

Reduce false fragmentation of attacker activity, PORTSOC implements a simplified session pivot mechanism. Instead of treating events as isolated entries, the system attempts to associate successful authentication events with subsequent privileged actions originating from the same source IP or user account. This supports the reconstruction of attacker progression into a more meaningful sequence such as login → privilege escalation → suspicious command execution.

Session pivoting also improves investigation usability by providing context across multiple event types, which is particularly important in offline environments where analysts cannot rely on cloudbased correlation services. The pivoting and contextual workflow is represented in the correlation layer of Fig. 1.3.

G. Incident Correlation and Risk Scoring

Rather than displaying alerts as isolated detections, PORTSOC groups related alerts into incidents. Incidents are correlated using attributes such as source IP, time proximity, and overlapping MITRE techniques. Each incident contains a list of techniques involved, number of correlated alerts, and a computed risk score in the range of 0 to 100. This correlation layer reduces alert overload and improves situational awareness by presenting higherlevel summaries of suspicious activity.

Risk scoring is derived from multiple weighted factors including alert severity, event volume, technique criticality, and IP reputation risk. The scoring model is intentionally designed to be interpretable and tunable, allowing analysts to understand why an incident was prioritized. The factors and weights used in the incident risk scoring model are summarized in Table 1.3. This correlation and scoring mechanism makes the tool closer to practical SOC workflows by enabling prioritization of incidents instead of raw alerts.

H. Offline Dashboard and Report Generation

PORTSOC includes a local Flaskbased web dashboard that runs fully offline. The dashboard provides tables for alerts and incidents with sorting and filtering support. It displays key fields such as timestamp, source IP, severity, technique mapping, event counts, reputation tags, and incident risk scores. Since the system is designed for isolated networks, all visualization and interaction occurs locally without any dependency on external services. In addition, PORTSOC supports automated report generation for audit documentation and forensic reporting. Reports can be exported in PDF and CSV formats, enabling investigators to preserve evidence summaries and incident timelines for documentation and review.

I. Log Integrity Verification (Hashchain)

To support forensic credibility, PORTSOC implements an integrity verification mechanism for raw logs using a chained hashing approach. Each collected raw log line contributes to a chained hash value, forming a tamper evident sequence. Any deletion, insertion, or modification of a raw log entry breaks the chain and can be detected during verification. This strengthens the reliability of stored logs in offline environments where centralized integrity services such as remote logging servers or cloud immutability controls are unavailable. The raw log integrity mechanism is reflected in the evidence storage and integrity component shown in Fig. 1.2.

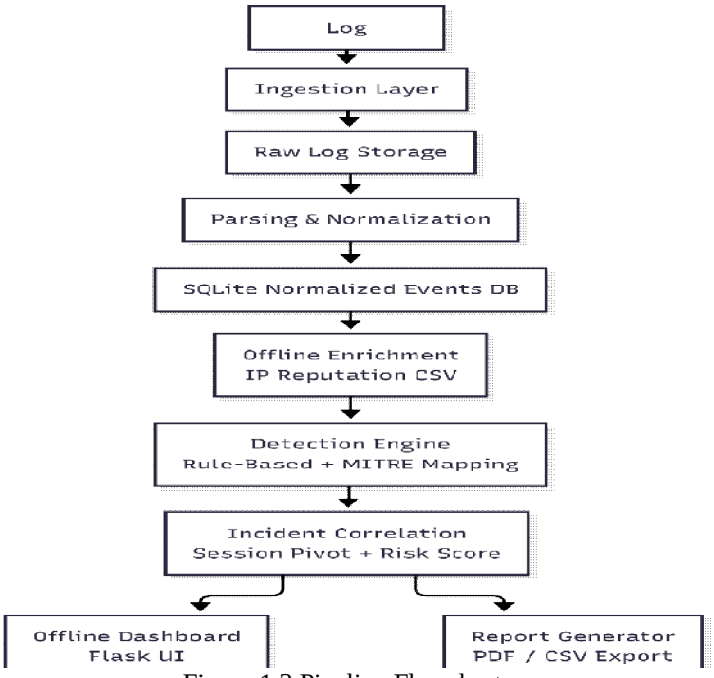


Figure 1.3 Pipeline Flowchart

Factor	Weight	Example Contribution
Alert Severity	0.40	High/Critical detections raise score significantly
IP Reputation Risk (Offline Feed)	0.30	Known scanner/botnet/suspicious IP increases incident priority
Event Count / Volume	0.20	Large bursts of failures or high event count increases score
MITRE Technique Weight	0.10	Higher impact techniques (e.g., brute force + privilege escalation) increase score

Table 1.3 Incident Risk Scoring Factors

V. RESULTS

A. *Detection Accuracy Analysis*

The detection accuracy of the PORTSOC system was evaluated using the several simulated attack scenarios in a controlled testing environment. These scenarios included brute-force authentication attempts, suspicious sudo command executions, credential misuse patterns, and system policy violation events. The rule-based detection engine is analyzed authentication logs and command execution traces to identify abnormal patterns that indicate a potential malicious activity. During the evaluation process, the detection engine successfully identified most of the simulated attack scenarios by correlating repeated authentication failures, abnormal command executions, and suspicious system behaviour observed within the collected logs.

The experimental results showed that the overall detection accuracy of the monitoring system was approximately 99%. A small number of false alerts were observed during anomaly detection experiments when sudden spikes in legitimate system activity triggered threshold-based detection rules. However, these alerts were easily distinguishable from a genuine attack pattern because the system provided contextual information through the incident correlation mechanism and MITRE ATT&CK mapping. This capability allowed the analysts to quickly differentiate between legitimate system behaviour and potentially malicious activity.

B. *Incident Correlation Effectiveness*

The incident correlation mechanism plays a significant role in reducing alert noise by grouping related security events into a single incident for easier analysis. Instead of displaying each alert independently, the system analyzesthe temporal relationships, source IP addresses, and overlapping MITRE ATT&CK techniques to determine whether multiple alerts belong to the same attack sequence.

During the experimental evaluation, several alerts generated from related attack activities were successfully combined into a single correlated incident. For example, in one of the simulated scenarios, three brute-force authentication alerts, one suspicious sudo command execution alert, and one policy violation alert were automatically correlated into a single high-risk security incident. The calculated risk score for this incident was 82 out of 100, and the system assigned it the highest severity level. This correlation capability significantly reduces alert fragmentation and enables security analysts to focus on the meaningful attack sequences rather than investigating multiple isolated alerts.

C. *Security Impact and Practical Applicability*

Beyond the detection accuracy and incident correlation capabilities, it is important to evaluate the practical security impact of the proposed monitoring system in real operational environments. Air-gapped networks are commonly deployed in critical infrastructures where the system visibility is limited and conventional cloud-based monitoring solutions cannot be used. In such environments, the ability to continuously monitor logs, detect suspicious behavior, and generate meaningful alerts locally becomes essential for maintaining situational awareness and responding to potential security incidents.

The PORTSOC monitoring architecture demonstrates that lightweight monitoring mechanisms can still provide a valuable security insights without relying on centralized SIEM infrastructure. By integrating rule-based detection, incident correlation, and MITRE ATT&CK mapping, the system provides analysts with contextualized alerts that describe not only the detected activity but also its relation to known adversarial tactics and techniques. This mapping significantly improves the interpretability of alerts and assists security teams in understanding potential attack progression within the monitored environment.

Another important advantage of the proposed system is its portability and minimal infrastructure requirements. Since all components of the monitoring pipeline operate locally, the system can be deployed in restricted environments where external connectivity is prohibited. The use of lightweight storage mechanisms such as SQLite, combined with modular detection components, allows the system to function efficiently even on systems with limited computational resources.

Furthermore, the implementation of log integrity verification through the hash-chain mechanism contributes to the forensic reliability of the monitoring system. In many security investigations, maintaining the integrity of log data is critical for reconstructing attack timelines and validating digital evidence. By ensuring that any modification to stored logs can be detected, the system enhances the trustworthiness of collected monitoring data and supports forensic analysis in the high-security environments.

Overall, the evaluation results indicate that portable monitoring architectures such as PORTSOC can provide practical SOC-style monitoring capabilities for isolated infrastructures. Although the system is intentionally lightweight compared to enterprise-scale SIEM platforms, it still offers essential security monitoring features that assist organizations in detecting suspicious activities, investigating incidents, and maintaining visibility over critical systems operating in air-gapped environments.

After conducting trials with the tool, we produced the results that detection accuracies for all the incidents were around 99\%, where there were some false alerts due to the anomaly detection module. The test was done using more than 2000 logs at once from a system, and it performed smoothly without any issues.The incident correlation results also showed how multiple alerts became a single incident, where 3 brute force alerts, 1 suspicious sudo alert, and 1 policy violation alert were all correlated into 1 incident. This incident had a high risk score of 82/100, and the severity was ranked as highest. All the MITRE mappings were combined for easier understanding. This demonstrated that the tool has a strong and effective correlation logic.

The dynamic thresholds and scoring were also accurate, where normal IPs had a risk score of 35, whereas malicious IPs had a score of 60, and multialert attacks had the highest risk score of 85. For performance testing, we ran the tool on an Ubuntu VM with 5GB of RAM, and it processed 2400 logs in 2 seconds. The testing was conducted in an isolated environment to depict the real working condition of the tool.Also, keeping security in mind, we implemented a hash chain mechanism for the raw logs stored inside the tool. Any modification of the logs will break the chain and throw an integrity error.

VI. CONCLUSION

This paper presented PORTSOC, a portable offline log analysis and security monitoring system designed specifically for air gapped and isolated network environments where conventional cloud based SIEM solutions cannot be deployed due to connectivity and security restrictions. The proposed system demonstrates that essential SOClevel monitoring capabilities can be effectively implemented in a lightweight and fully offline architecture without dependence on centralized infrastructure or external threat intelligence services.

By utilizing Syslog based log ingestion, PORTSOC enables the collection of real time security logs from multiple endpoints and servers within an isolated network. The incorporation of a structured parsing and normalization layer allows heterogeneous and unstructured logs to be transformed into consistent event records, which are then stored locally using a portable SQLite database. The rule based detection engine implemented in the system successfully identifies common adversarial behaviours such as repeated authentication failures, bruteforce attempts, credential misuse, and suspicious privilege escalation activities.

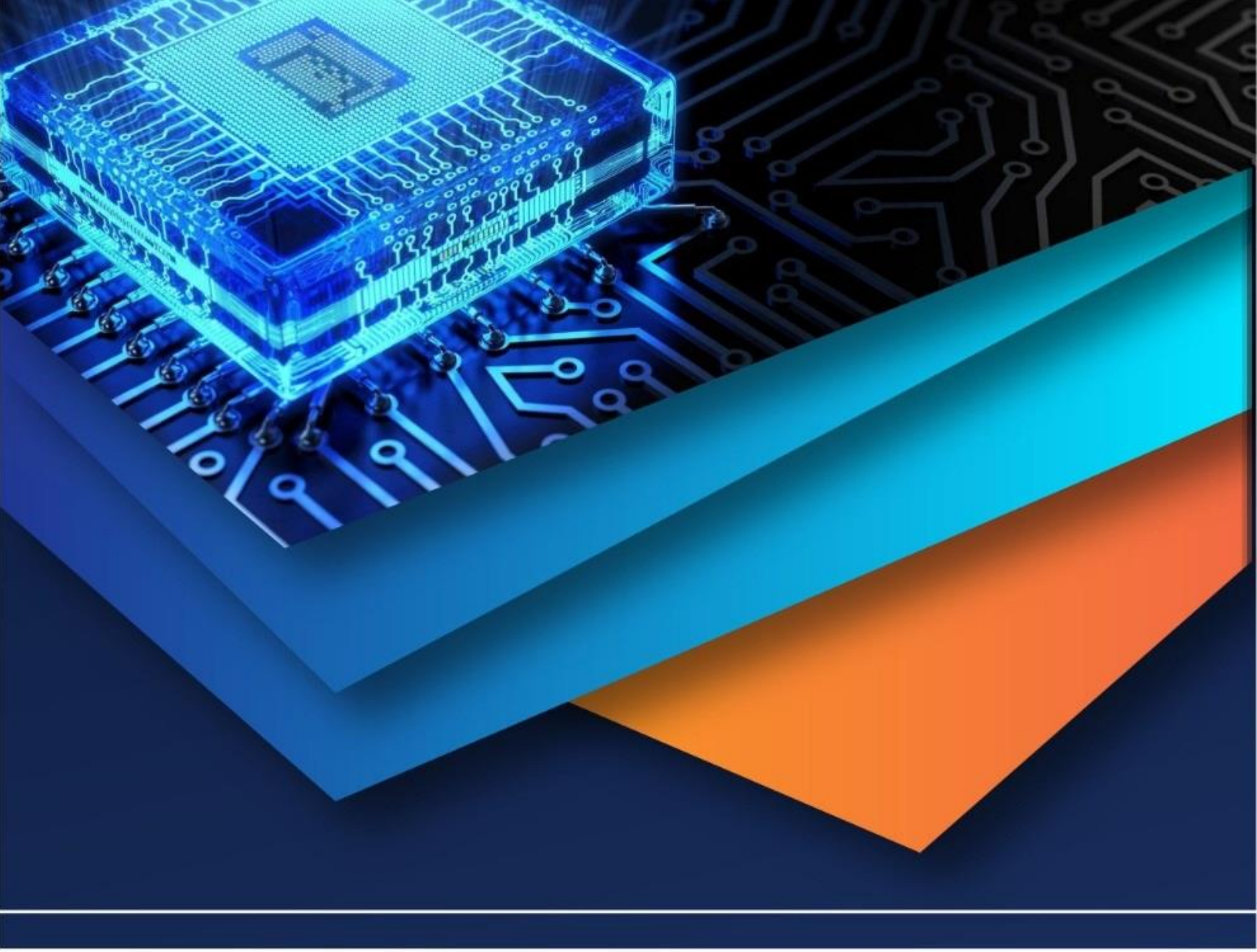
Furthermore, mapping detected security events to MITRE ATT&CK techniques provides standardized threat classification and improves the contextual understanding of adversary behaviour even in offline environments. The integration of offline threat intelligence enrichment and incident correlation mechanisms enhances detection confidence while minimizing alert fragmentation.

PORTSOC also incorporates an offline dashboard for alert visualization and automated report generation to support audit documentation and forensic analysis. Additionally, the implementation of a chained hash based integrity verification mechanism strengthens the evidentiary reliability of collected logs by enabling tamper detection in the absence of centralized logging infrastructure.Experimental evaluation in a controlled lab setup indicates that the system can efficiently process large volumes of log data while maintaining low resource utilization, making it suitable for deployment in constrained environments such as critical infrastructure networks, defence systems, and regulated industrial environments.

In conclusion, the proposed system addresses a significant gap in cybersecurity monitoring for isolated networks by providing a practical, portable, and offline first solution capable of delivering meaningful threat visibility without enterprise scale SIEM complexity.

REFERENCES

[1] K. Kent and M. Souppaya, "Guide to computer security log management," National Institute of Standards and Technology (NIST), Tech. Rep. NIST SP 80092, 2006.
[2] A. Behl, "Security information and event management (siem): Implementationchallenges," International Journal of Computer Applications, 2017.
[3] Splunk Inc., "Security information and event management (siem)," https://www.splunk.com/en_us/solutions/siem.html, 2024.
[4] Elastic N.V., "Elastic security overview," https://www.elastic.co/security,2024.
[5] R. Gerhards, "The syslog protocol," IETF, Tech. Rep. RFC 5424, 2009.
[6] SQLite Development Team, "SQLite documentation," https://www.sqlite.org/docs.html, 2024.
[7] B. E. Strom et al., "Mitre attack: Design and philosophy," MITRE TechnicalReport, 2018.
[8] MITRE Corporation, "Mitre attack framework," https://attack.mitre.org,2024, accessed: 20260215.
[9] M. e. a. Guri, "Airgap computer security: Threats and countermeasures,"Journal of Cyber Security Technology, 2018



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY