Splunk-Based SIEM For Real-Time Threat Detection

Syed Omair Ahmed[1], Subramanian K.M[2], Md. Ateeq Ur Rahman[3]
[1]*PG Scholar, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086*
[2,3]*Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086*

***Abstract*—The rapid increase in cyber threats has highlighted the need for effective Security Information and Event Management (SIEM) solutions capable of detecting and responding to security incidents in real time. Traditional security monitoring methods often struggle to analyze large volumes of log data generated by enterprise systems, resulting in delayed threat identification and increased security risks. This paper presents a Splunk-Based SIEM for Real-Time Threat Detection, designed to provide centralized log collection, real-time event correlation, and automated alert generation in a Windows Server environment. The proposed framework utilizes Splunk Enterprise 10.0 to collect and analyze Sysmon logs from multiple virtual machines, enabling comprehensive monitoring of authentication events and system activities. Custom Search Processing Language (SPL) correlation rules are implemented to identify brute-force authentication attacks by detecting repeated failed login attempts and suspicious user behavior. Upon detecting malicious activity, the system generates real-time alerts and interactive dashboards to support rapid investigation and incident response by Security Operations Center (SOC) analysts.**

The framework is further enhanced by mapping detected attack techniques to the MITRE ATT&CK framework, providing standardized threat classification and improving security analysis. Experimental evaluation demonstrates efficient log ingestion, fast search execution, and timely alert generation, confirming the effectiveness of the proposed approach for enterprise security monitoring. The results show that the developed SIEM framework enhances threat visibility, reduces incident response time, and provides a scalable solution for real-time cybersecurity operations.

Index Terms—**Security Information and Event Management (SIEM), Splunk Enterprise 10.0, Sysmon, Windows Server, Threat Detection, Security Monitoring, Search Processing Language (SPL), Brute-Force Attack, Authentication Monitoring, MITRE ATT&CK**

I. INTRODUCTION

The rapid growth of digital technologies and interconnected enterprise networks has significantly increased the volume and complexity of cybersecurity threats. Organizations across various sectors rely on information systems to manage critical business operations, making them attractive targets for cyberattacks such as brute-force login attempts, unauthorized access, malware infections, ransomware, and insider threats. As enterprise infrastructures continue to expand, security teams face the challenge of monitoring millions of security events generated daily by servers, endpoints, network devices, and applications. Traditional security monitoring methods, which often depend on manual log analysis or isolated security tools, are no longer sufficient to detect sophisticated attacks in a timely manner.

Security Information and Event Management (SIEM) systems have emerged as an effective solution for centralized security monitoring by collecting, correlating, and analyzing security logs from multiple sources. A SIEM platform provides real-time visibility into organizational security events by aggregating logs from operating systems, network devices, firewalls, applications, and endpoint monitoring tools. Through event correlation and automated alert generation, SIEM solutions help Security Operations Center (SOC) analysts identify suspicious activities, investigate security incidents, and respond to threats more efficiently.

Among the available SIEM platforms, Splunk Enterprise has gained widespread adoption because of its scalability, powerful indexing capabilities, flexible Search Processing Language (SPL), and advanced dashboard visualization features. Splunk enables organizations to ingest large volumes of structured and

unstructured machine data, perform real-time searches, create correlation rules, and generate actionable alerts for security incidents. These capabilities make Splunk a suitable platform for enterprise security monitoring and incident response.

Authentication-related attacks, particularly brute-force attacks, remain one of the most common techniques used by attackers to gain unauthorized access to enterprise systems. Attackers repeatedly attempt different username and password combinations until valid credentials are identified, potentially compromising sensitive organizational resources. Detecting such attacks requires continuous monitoring of authentication events, rapid correlation of failed login attempts, and immediate notification to security administrators. Without automated detection mechanisms, brute-force attacks may remain unnoticed until significant damage has occurred.

This research presents a Splunk-based SIEM framework for real-time threat detection using Splunk Enterprise 10.0 in a Windows Server environment. The proposed framework collects Sysmon logs from multiple virtual machines, centralizes security event data, and applies custom SPL correlation rules to detect brute-force authentication attacks. When suspicious login patterns are identified, the framework generates real-time alerts and visual dashboards that assist SOC analysts in monitoring and investigating security incidents. The solution is designed to improve visibility into authentication-related threats while reducing the time required to detect and respond to potential attacks.

To enhance threat analysis, the detected attack patterns are aligned with the MITRE ATT&CK framework, enabling standardized classification of adversarial techniques and supporting more effective incident investigation. The framework combines centralized log management, automated event correlation, and interactive dashboards to provide a practical and scalable solution for enterprise security operations.

The major contributions of this work are summarized as follows:

- Design and implementation of a centralized SIEM framework using Splunk Enterprise 10.0 for enterprise security monitoring.
- Collection and analysis of Sysmon logs from multiple Windows Server virtual machines.
- Development of custom SPL correlation rules for real-time detection of brute-force authentication attacks.
- Integration of automated alert generation and interactive dashboards to improve SOC monitoring capabilities.
- Mapping of detected attack techniques to the MITRE ATT&CK framework for standardized threat classification.
- Performance evaluation of the proposed framework based on log ingestion, search execution, and alert response efficiency.

The remainder of this paper is organized as follows. Section II reviews related research on SIEM technologies and threat detection approaches. Section III describes the proposed SIEM framework and system architecture. Section IV explains the implementation and experimental setup. Section V presents the experimental results and performance evaluation. Section VI discusses the MITRE ATT&CK mapping and comparative analysis. Finally, Section VII concludes the paper and outlines future research directions.

II. RELATED WORK

Security Information and Event Management (SIEM) systems have become a fundamental component of modern cybersecurity operations by providing centralized log collection, event correlation, threat detection, and incident response capabilities. As cyberattacks continue to evolve in complexity, researchers have proposed various SIEM architectures and detection techniques to improve security monitoring and reduce response time. Recent studies have focused on enhancing SIEM platforms through real-time analytics, machine learning, threat intelligence integration, and behavior-based anomaly detection.

Several researchers have investigated the use of Splunk Enterprise as a SIEM platform for enterprise security monitoring. Splunk provides scalable log collection, efficient indexing, powerful Search Processing Language (SPL) capabilities, and customizable dashboards that enable security analysts to monitor heterogeneous environments. Previous studies have demonstrated the effectiveness of Splunk in collecting logs from Windows systems, Linux

servers, firewalls, web servers, and network devices to improve centralized visibility into security events. However, many of these implementations primarily focus on log management and dashboard visualization without providing comprehensive evaluations of detection performance or standardized threat classification.

Other studies have explored open-source SIEM solutions such as the Elastic Stack (ELK) and Wazuh. These platforms offer centralized logging and event analysis while reducing deployment costs. Wazuh extends ELK with host-based intrusion detection, file integrity monitoring, and vulnerability assessment. Although these solutions provide flexible monitoring capabilities, they often require significant manual configuration and tuning to achieve enterprise-level detection accuracy. In contrast, Splunk Enterprise offers mature indexing, optimized search performance, and advanced correlation capabilities suitable for large-scale security operations.

Machine learning techniques have also been integrated into SIEM systems to identify unknown attacks and anomalous user behavior. Researchers have proposed supervised and unsupervised learning models for detecting insider threats, abnormal authentication activities, and malware infections. While machine learning improves the ability to detect previously unseen attacks, its effectiveness depends heavily on high-quality training datasets, computational resources, and continuous model updates. Many organizations therefore continue to rely on rule-based detection for operational reliability, regulatory compliance, and explainable security investigations.

Authentication attacks, particularly brute-force attacks, remain among the most common threats targeting enterprise environments. Previous research has proposed detection methods based on repeated failed login attempts, authentication event correlation, user behavior analysis, and login frequency monitoring. However, many existing approaches analyze authentication events in isolation and do not integrate centralized log management, automated alert generation, interactive dashboards, and standardized threat mapping within a unified SIEM framework.

Recent cybersecurity research has increasingly adopted the MITRE ATT&CK framework to classify attacker techniques and improve threat intelligence. Mapping security detections to ATT&CK techniques provides a standardized method for understanding adversary behavior, identifying coverage gaps, and supporting Security Operations Center (SOC) investigations. Nevertheless, many SIEM implementations still lack direct integration with ATT&CK, reducing the contextual information available during incident analysis.

Based on the reviewed literature, several research gaps remain. First, many SIEM implementations emphasize log collection and visualization without evaluating operational performance under realistic enterprise conditions. Second, limited attention has been given to integrating Sysmon-based endpoint monitoring with centralized authentication analysis in Windows Server environments. Third, relatively few studies combine custom SPL correlation rules, automated brute-force detection, interactive dashboards, and MITRE ATT&CK mapping within a single framework. Finally, comprehensive evaluations of detection efficiency, search performance, and alert response time are often absent from existing implementations.

To address these limitations, this research proposes a Splunk-Based SIEM for Real-Time Threat Detection using Splunk Enterprise 10.0. The proposed framework centralizes Sysmon log collection from multiple Windows Server virtual machines, applies custom SPL correlation rules to detect brute-force authentication attacks, generates real-time alerts and dashboards, and maps detected techniques to the MITRE ATT&CK framework. In addition, the framework includes a practical performance evaluation based on real implementation results, providing a comprehensive assessment of its effectiveness in supporting enterprise security monitoring and incident response.

III. PROPOSED METHODOLOGY

A. System Overview

The proposed framework is designed to provide centralized security monitoring and real-time threat detection using Splunk Enterprise 10.0. The architecture collects security logs from multiple Windows Server virtual machines and processes them through a centralized SIEM platform. The collected logs are indexed, correlated, and analyzed using custom Search Processing Language (SPL) queries to identify suspicious authentication activities. When malicious behavior is detected, the system automatically generates alerts and updates security

dashboards to assist Security Operations Center (SOC) analysts in incident investigation and response.
The framework follows a layered architecture consisting of log generation, log collection, centralized processing, threat detection, alert generation, visualization, and threat classification. This design enables efficient monitoring of enterprise environments while maintaining scalability and fast search performance.

B. System Architecture
The proposed SIEM architecture consists of the following components:

1) Windows Server Virtual Machines
Multiple Windows Server virtual machines are deployed to simulate an enterprise environment. Each virtual machine generates security events including authentication logs, process creation events, account activities, and system-level events.

2) Sysmon
Sysmon (System Monitor) is installed on each Windows Server virtual machine to capture detailed endpoint activities.

It records information such as:
- Process creation
- Network connections
- File creation events
- Driver loading
- Authentication-related activities

These detailed logs improve endpoint visibility beyond standard Windows Event Logs and provide valuable data for security monitoring.

3) Splunk Universal Forwarder
The Splunk Universal Forwarder is configured on each monitored system to securely transmit Sysmon logs to the centralized Splunk Enterprise server. The forwarder continuously monitors the configured log sources and forwards new events with minimal impact on system performance.

4) Splunk Enterprise 10.0
Splunk Enterprise acts as the central SIEM platform responsible for:
- Collecting logs
- Parsing incoming events
- Creating indexes
- Executing SPL searches
- Correlating security events
- Generating alerts
- Displaying dashboards

The centralized architecture enables efficient management of security data collected from multiple endpoints.

C. Log Collection and Indexing
Security logs generated by Sysmon are continuously collected through the Universal Forwarder and transmitted to the Splunk Enterprise server. Incoming events are parsed and stored in dedicated indexes to improve search efficiency and simplify event management.

The indexing process provides several advantages:
- Faster search execution
- Efficient storage management
- Organized event classification
- Improved scalability for enterprise deployments

D. Threat Detection Using SPL
Threat detection is performed using custom Search Processing Language (SPL) correlation rules. The framework focuses on identifying brute-force authentication attacks by analyzing repeated failed login attempts occurring within a defined time interval.

The detection process includes:
- Monitoring authentication events
- Counting repeated failed login attempts
- Identifying suspicious user accounts
- Detecting abnormal login behavior
- Triggering automated alerts when predefined thresholds are exceeded

This rule-based approach enables rapid identification of authentication attacks while minimizing manual analysis by security analysts.

E. Alert Generation
When suspicious authentication behavior is detected, Splunk automatically generates real-time alerts. Alerts are classified according to severity levels to support effective incident prioritization.

The framework supports:

- Informational alerts
- Warning alerts
- High-severity alerts
- Critical alerts

Alert notifications are displayed on the Splunk dashboard and can also be delivered through email notifications to SOC personnel for immediate response.

F. Dashboard Visualization

Interactive dashboards are developed to provide real-time visibility into enterprise security events. The dashboards summarize authentication activities, detected threats, and system status using graphical visualizations and statistical summaries.

The developed dashboards include:

- Security Overview Dashboard
- Authentication Dashboard
- Threat Monitoring Dashboard
- Alert Summary Dashboard

These dashboards enable analysts to quickly identify suspicious activities, monitor attack trends, and investigate security incidents.

G. MITRE ATT&CK Mapping

To improve threat intelligence and incident analysis, detected authentication attacks are mapped to the MITRE ATT&CK framework. Brute-force login attempts are associated with the Brute Force (T1110) technique, while successful authentication following repeated failures can be correlated with Valid Accounts (T1078) where appropriate.

This mapping provides standardized threat classification, improves analyst understanding of attacker behavior, and helps evaluate detection coverage against widely recognized adversarial techniques.

H. Methodology Workflow

The overall workflow of the proposed framework consists of the following sequential stages:

1. Security events are generated on Windows Server virtual machines.
2. Sysmon records endpoint activities and authentication events.
3. Splunk Universal Forwarder collects and forwards logs.
4. Splunk Enterprise receives and indexes the incoming data.
5. Custom SPL correlation rules analyze authentication events.
6. Brute-force attacks are identified based on repeated failed login attempts.
7. Real-time alerts are generated for detected threats.
8. Security dashboards are updated to provide continuous monitoring.
9. Detected techniques are mapped to the MITRE ATT&CK framework for standardized threat analysis.

The proposed methodology provides a scalable and efficient approach for centralized log management, automated threat detection, and real-time security monitoring in enterprise environments.

IV. EXPERIMENTAL SETUP

A. Experimental Environment

The proposed SIEM framework was implemented in a controlled laboratory environment to evaluate its effectiveness in detecting authentication-related threats. A virtualized infrastructure was created using multiple Windows Server virtual machines to simulate an enterprise network. This environment enabled the generation of realistic security events while maintaining isolation and repeatability for testing purposes.

The SIEM platform was deployed using Splunk Enterprise 10.0, which served as the centralized server for log collection, indexing, event correlation, and security monitoring. Each virtual machine was configured with Sysmon to capture detailed endpoint activities and the Splunk Universal Forwarder to securely transmit log data to the central Splunk server.

B. Hardware Configuration

The experimental environment was deployed on a host system with the following minimum configuration:

Component	Specification
Processor	Intel Core i5/i7 or equivalent
Memory	16 GB RAM
Storage	512 GB SSD
Virtualization Platform	VMware Workstation / VirtualBox
Network	Virtual NAT/Host-Only Network

The hardware configuration was sufficient to run multiple virtual machines simultaneously while maintaining stable SIEM performance.

C. Software Configuration

The software components used during implementation are summarized in Table 1.

Table 1. Software Environment

Software	Version	Purpose
Windows Server	2022	Log source
Splunk Enterprise	10.0	SIEM Platform
Sysmon	Latest Stable Release	Endpoint Monitoring
Splunk Universal Forwarder	Compatible with Splunk 10.0	Log Collection
PowerShell	Default	Administrative Configuration

D. Log Collection Process

Sysmon was installed on each Windows Server virtual machine to collect detailed endpoint telemetry. The configuration captured process creation, authentication events, network connections, and other security-relevant activities. The Splunk Universal Forwarder continuously monitored the generated logs and securely forwarded them to the centralized Splunk Enterprise server.

Within Splunk, the incoming events were parsed and indexed to enable efficient searching and correlation. Dedicated indexes were configured to organize authentication and security events, improving query performance and simplifying security investigations.

E. Brute-Force Attack Simulation

To evaluate the detection capability of the proposed framework, a controlled brute-force authentication scenario was performed within the laboratory environment. Multiple failed login attempts were intentionally generated against user accounts hosted on the Windows Server virtual machines. These authentication events produced corresponding Sysmon and Windows security logs, which were forwarded to Splunk Enterprise for analysis.

Custom Search Processing Language (SPL) correlation rules monitored authentication events in real time. When the number of failed login attempts exceeded the predefined threshold within a specified time interval, the framework classified the activity as a potential brute-force attack and generated a high-severity alert.

F. Dashboard Configuration

Several dashboards were created to provide continuous visibility into the monitored environment.

The primary dashboards included:

- Security Overview Dashboard
- Authentication Dashboard
- Threat Monitoring Dashboard
- Alert Summary Dashboard

These dashboards displayed authentication statistics, failed login trends, active alerts, and security events using tables, charts, and graphical visualizations. The dashboard interface enabled SOC analysts to quickly identify suspicious activities and investigate potential threats.

G. Evaluation Metrics

The effectiveness of the proposed framework was evaluated using operational performance metrics commonly applied in SIEM environments.

The evaluation focused on:

- Log ingestion performance
- Search execution time
- Alert generation time
- Dashboard refresh performance
- Detection of brute-force authentication attacks

These metrics were selected to assess the framework's ability to provide efficient log processing and timely threat detection in a multi-virtual-machine environment.

H. Experimental Workflow

The experimental procedure consisted of the following steps:

1. Deploy multiple Windows Server virtual machines.
2. Install and configure Sysmon on each virtual machine.
3. Configure Splunk Universal Forwarder to transmit Sysmon logs.
4. Deploy Splunk Enterprise 10.0 as the centralized SIEM platform.

5. Create indexes and configure data inputs.
6. Develop custom SPL correlation rules for authentication monitoring.
7. Simulate brute-force authentication attacks.
8. Generate real-time alerts and visualize results through dashboards.
9. Evaluate system performance using predefined metrics.

The experimental setup demonstrates that the proposed framework can effectively collect, process, and analyze security events from multiple endpoints while providing centralized monitoring and automated threat detection in real time.

V. RESULTS AND DISCUSSION

A. Log Collection Results

The proposed SIEM framework successfully collected and centralized security logs from multiple Windows Server virtual machines using Splunk Enterprise. Sysmon continuously monitored endpoint activities, while the Splunk Universal Forwarder transmitted security events to the centralized SIEM server. The indexed logs included authentication events, process creation records, and system activities, enabling comprehensive monitoring of the enterprise environment.

The successful ingestion of security events confirmed that the framework could reliably collect and process endpoint telemetry from multiple sources without interrupting normal system operation.

B. Brute-Force Attack Detection

A controlled brute-force authentication attack was conducted within the experimental environment to evaluate the effectiveness of the proposed framework. Multiple failed login attempts were generated against Windows Server user accounts. The custom SPL correlation rule continuously analyzed authentication events and detected repeated failed login attempts occurring within the predefined threshold.

Once the threshold was exceeded, Splunk Enterprise generated a high-severity alert and displayed the event on the authentication dashboard. This enabled rapid identification of suspicious login activity and demonstrated the effectiveness of the proposed detection mechanism.

C. Dashboard Analysis

The developed dashboards provided real-time visibility into security events and authentication activities. The Authentication Dashboard displayed failed login attempts, successful logins, and user activity trends, allowing security analysts to identify suspicious behavior quickly.

The Search and Reporting interface enabled analysts to execute SPL queries, filter authentication events, and investigate potential security incidents. Saved searches and automated alerts further enhanced operational efficiency by reducing the need for continuous manual monitoring.

D. Discussion

The experimental results demonstrate that the proposed Splunk-based SIEM framework effectively supports centralized log management and real-time threat detection. The integration of Sysmon with Splunk Enterprise provided detailed endpoint visibility, while custom SPL correlation rules enabled accurate identification of brute-force authentication attacks.

The framework offers several practical advantages:

- Centralized monitoring of multiple Windows Server virtual machines.
- Automated detection of suspicious authentication activities.
- Reduced manual effort through real-time alerts and dashboards.
- Improved visibility into enterprise security events.
- Standardized threat analysis through MITRE ATT&CK mapping.

Although the current implementation focuses on brute-force authentication attacks, the framework can be extended to detect additional threats such as privilege escalation, ransomware activity, lateral movement, and insider threats by implementing additional correlation rules and integrating external threat intelligence sources.

VI. PERFORMANCE EVALUATION

A. Evaluation Metrics

The performance of the proposed Splunk-based SIEM framework was evaluated using operational metrics that reflect its effectiveness in enterprise security

monitoring. The evaluation focused on log collection efficiency, search execution, alert generation, dashboard responsiveness, and threat detection capability.

The primary evaluation metrics include:

- Log ingestion capability
- Search execution efficiency
- Alert generation time
- Dashboard responsiveness
- Brute-force attack detection

These metrics were selected because they directly influence the ability of a Security Information and Event Management (SIEM) system to provide timely and accurate threat detection.

B. Log Collection Performance

The proposed framework successfully centralized security logs generated from multiple Windows Server virtual machines. Sysmon continuously captured endpoint events, and the Splunk Universal Forwarder transmitted these events to the centralized Splunk Enterprise server.

The indexing mechanism enabled efficient storage and rapid retrieval of security events, ensuring that authentication logs were available for real-time analysis.

The experiment demonstrated that centralized log collection improved security visibility and simplified the monitoring of distributed systems.

C. Search Performance

Search Processing Language (SPL) queries were used to retrieve authentication events and identify suspicious login behavior.

The indexed data structure provided efficient search performance, allowing analysts to locate authentication events quickly and investigate potential attacks with minimal delay.

The Search & Reporting interface also enabled filtering based on source type, host, event ID, and user activity, supporting rapid forensic analysis.

D. Alert Generation Performance

Custom SPL correlation rules continuously monitored authentication events.

When repeated failed login attempts exceeded the configured threshold, Splunk Enterprise generated real-time alerts.

The alerting mechanism reduced the need for manual log review and enabled faster response to potential brute-force attacks.

Automated alerts were displayed through the Authentication Dashboard, allowing SOC analysts to prioritize investigations based on event severity.

E. Dashboard Performance

Interactive dashboards provided continuous visualization of authentication events and detected threats.

The dashboards displayed:

- Failed login attempts
- Successful logins
- Alert statistics
- Authentication trends
- Event distribution

The graphical representation of security events improved situational awareness and reduced the time required to identify suspicious activities.

F. Comparative Analysis

The proposed framework was compared with commonly used SIEM platforms based on key operational characteristics.

Feature	Proposed Framework	ELK Stack	Wazuh	IBM QRadar
Real-Time Log Collection	✓	✓	✓	✓
Centralized Monitoring	✓	✓	✓	✓
Sysmon Integration	✓	✓	✓	✓
Custom SPL Detection Rules	✓	✗	✗	Limited
Interactive Dashboards	✓	✓	✓	✓
Automated Alerts	✓	✓	✓	✓
MITRE ATT&CK Mapping	✓	Partial	Partial	✓

The comparison indicates that the proposed framework provides comprehensive security monitoring while leveraging Splunk's powerful search and visualization capabilities.

G. Discussion

The experimental evaluation confirms that the proposed SIEM framework effectively supports centralized log collection, real-time authentication monitoring, and automated brute-force attack detection.

The integration of Splunk Enterprise with Sysmon enables rapid analysis of security events while providing intuitive dashboards and automated alerting mechanisms.

The framework is scalable and can be extended to monitor additional attack techniques, including privilege escalation, malware execution, lateral movement, and ransomware activity.

VII. LIMITATIONS

Although the proposed framework demonstrates effective real-time threat detection, several limitations should be considered.

- The current implementation focuses primarily on brute-force authentication attacks.
- The experimental environment is based on a laboratory deployment using multiple virtual machines rather than a large-scale production network.
- Detection is based on rule-based SPL correlation and does not currently include machine learning or behavioral analytics.
- The framework relies on Windows Server and Sysmon logs, while additional data sources such as firewalls, IDS/IPS systems, cloud services, and endpoint detection platforms could further enhance visibility.

Future work will address these limitations by integrating advanced analytics, additional log sources, and automated response capabilities.

VIII. CONCLUSION AND FUTURE WORK

A. Conclusion

This paper presented a Splunk-Based SIEM for Real-Time Threat Detection designed to improve enterprise security monitoring through centralized log management, automated event correlation, and real-time alert generation. The proposed framework utilized Splunk Enterprise, Sysmon, and multiple Windows Server virtual machines to collect, process, and analyze security events from distributed endpoints. A centralized SIEM architecture was implemented to aggregate security logs and provide comprehensive visibility into authentication activities across the monitored environment. Custom Search Processing Language (SPL) correlation rules were developed to identify brute-force authentication attacks by detecting repeated failed login attempts within a specified time interval. Upon detecting suspicious behavior, the framework generated real-time alerts and updated interactive dashboards to assist Security Operations Center (SOC) analysts in investigating and responding to potential threats.

The experimental results demonstrated that the proposed framework effectively supports centralized security monitoring, rapid event analysis, and automated threat detection. The integration of Sysmon with Splunk provided detailed endpoint visibility, while dashboard visualizations improved situational awareness and reduced the effort required for manual log analysis. Furthermore, the mapping of detected attack techniques to the MITRE ATT&CK framework enhanced threat classification and supported a standardized approach to security investigations.

Overall, the developed SIEM framework provides a practical, scalable, and cost-effective solution for real-time threat detection and enterprise security operations.

B. Future Work

Although the proposed framework successfully detects brute-force authentication attacks, several opportunities exist for future enhancement.

Future work may include:

1. Machine Learning-Based Threat Detection

Integrating machine learning algorithms to identify anomalous user behavior and previously unknown attack patterns.

2. Threat Intelligence Integration

Incorporating external threat intelligence feeds to detect malicious IP addresses, domains, and indicators of compromise (IOCs).

3. SOAR Integration

Combining the SIEM framework with Security Orchestration, Automation, and Response (SOAR) platforms to automate incident response actions.

4. Cloud Security Monitoring
Extending the framework to collect and analyze logs from cloud platforms such as AWS, Microsoft Azure, and Google Cloud.

5. Advanced Attack Detection
Implementing additional SPL correlation rules to detect ransomware activity, privilege escalation, lateral movement, insider threats, and malware execution.

6. Large-Scale Enterprise Deployment
Evaluating the framework in a production-scale environment with a greater number of endpoints and diverse log sources. By incorporating these enhancements, the proposed framework can evolve into a more intelligent and comprehensive cybersecurity monitoring solution capable of addressing modern enterprise security challenges.

Research Gap
Existing SIEM implementations primarily focus on centralized log collection and event visualization. However, many studies provide limited evaluation of real-time authentication threat detection using Sysmon-generated logs in Windows Server environments. Additionally, the integration of custom SPL correlation rules, automated alert generation, dashboard-based monitoring, and MITRE ATT&CK mapping within a unified framework remains insufficiently explored. This research addresses these gaps by developing and evaluating a Splunk-based SIEM framework capable of detecting brute-force authentication attacks in real time while providing centralized monitoring and standardized threat classification.

REFERENCES

[1] M. Chuvakin, K. Schmidt, and C. Phillips, *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*, Waltham, MA, USA: Syngress, 2013.

[2] Splunk Inc., "Splunk Enterprise Documentation," 2025. [Online]. Available: https://docs.splunk.com/

[3] Microsoft, "Sysmon - System Monitor," Microsoft Learn, 2025. [Online]. Available: https://learn.microsoft.com/sysinternals/downloads/sysmon

[4] MITRE Corporation, "MITRE ATT&CK Framework," 2025. [Online]. Available: https://attack.mitre.org/

[5] National Institute of Standards and Technology, Computer Security Incident Handling Guide (SP 800-61 Rev. 2).

[6] National Institute of Standards and Technology, Guide to Computer Security Log Management (SP 800-92).

[7] B. B. Gupta, D. P. Agrawal, and others, Handbook of Computer Networks and Cyber Security, Springer, 2021.

[8] S. Mansfield-Devine, "Security Information and Event Management," Network Security, vol. 2021.

[9] R. Bejtlich, The Practice of Network Security Monitoring, San Francisco, CA, USA: No Starch Press.

[10] M. Collins, Network Security Through Data Analysis, Sebastopol, CA, USA: O'Reilly Media.

[11] Microsoft, "Windows Security Auditing," Microsoft Learn, 2025.

[12] Splunk Inc., "Search Processing Language (SPL) Search Reference," 2025.

[13] Splunk Inc., "Universal Forwarder Administration Manual," 2025.

[14] Elastic, "Elastic Security Documentation," 2025.

[15] Wazuh, "Wazuh Documentation," 2025.

[16] IBM, "IBM QRadar Documentation," 2025.

[17] Microsoft, "Microsoft Sentinel Documentation," 2025.

[18] MITRE Engenuity, "ATT&CK Evaluations," 2024.

[19] National Institute of Standards and Technology, Cybersecurity Framework (CSF) 2.0, 2024.

[20] R. Shackleford, State of Cybersecurity Report, SANS Institute, 2024.

[21] Splunk Inc., "Security Use Cases," 2025.

[22] Microsoft, "Windows Event Log Reference," Microsoft Learn, 2025.

[23] A. Oltsik, "Security Analytics Research," Enterprise Strategy Group.

[24] Gartner, "Market Guide for Security Information and Event Management," 2024.

[25] European Union Agency for Cybersecurity (ENISA), Threat Landscape Report, 2024.