ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

REAL-TIME MONITORING AND ALERTING ON APPLICATION USING A SPLUNK

Jatavath Dileep Kumar

21N81A6221

Computer Science and Engineering (Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

dileepkumarjatavath2004@gmail.com

Nakka Murali

21N81A6223

Computer Science and Engineering (Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

nakkamuralimuralitej@gmail.com

Syed Saifullah

21N81A6222

Computer Science and Engineering (Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

syedsaifullah3794@gmail.com

Kompoju Akash

21N81A6242

Computer Science and Engineering (Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

akashkompoju@gmail.com

Mr. J. Naresh Kumar

Assistant Professor

Computer Science and Engineering (Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

Abstract: Cybersecurity is a critical concern for organizations as cyber threats grow increasingly frequent and sophisticated.

Real-time detection and response to these threats are essential for safeguarding data and maintaining operational continuity. Splunk Enterprise Security (ES), a robust Security Information and Event Management (SIEM) platform, offers advanced tools for identifying and mitigating cyber threats. This paper explores the possibilities of using Splunk ES to enhance advanced cyber threat detection, focusing on its features, capabilities, and real-world applications. Splunk ES collects, indexes, and analyzes extensive machine data from diverse sources, including system logs, network traffic, and security devices. With real-time monitoring and comprehensive visibility into an organization's IT ecosystem, Splunk ES enables early detection of suspicious activities. It offers pre-

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

configured security content, such as correlation searches, dashboards, and reports, to streamline threat identification and incident response. A notable strength of Splunk ES lies in its flexibility, allowing users to customize detection rules and dashboards to meet specific organizational needs. The platform's adaptive response features support automated actions based on predefined criteria, significantly reducing the time from threat detection to mitigation. Furthermore, the integration of machine learning enhances its ability to detect patterns and anomalies, including those that might bypass traditional signature-based detection methods. In practice, Splunk ES has demonstrated its efficacy in addressing diverse cyber threats, including advanced persistent threats (APTs), insider threats, and zero-day vulnerabilities. By offering scalable and powerful tools, Splunk ES enables organizations to detect, analyze, and respond to security risks efficiently, paving the way for more robust cybersecurity strategies. This study examines the potential of Splunk ES as a vital asset in the fight against advanced cyber threats.

Keyword(s): Cybersecurity, Cyber threat detection, Splunk, Splunk Enterprise Security (ES), SIEM (security information and event management), Real-Time monitoring

1. Introduction

The rapid evolution of cyber threats has made real-time detection and response essential for maintaining organizational security and operational continuity. Security Information and Event Management (SIEM) systems address this need by combining Security Information Management (SIM) for log management and compliance reporting with Security Event Management (SEM) for real-time monitoring and event correlation. SIEM systems collect, normalize, and analyze log data from diverse sources, such as endpoint devices, servers, firewalls, and intrusion detection and prevention systems (IDPS), to provide a centralized view of system activity. According to the Information Technology Infrastructure Library (ITIL), an event is defined as any significant occurrence within an IT environment that requires attention or action [9]. SIEM systems rely on event correlation to analyze log data in near real-time and identify patterns or anomalies indicative of potential attacks [3][7][27]. Despite their effectiveness, traditional SIEM systems face challenges such as performance bottlenecks and query prioritization issues when handling large volumes of raw log data [4]. Modern platforms like Splunk Enterprise Security (ES) overcome these limitations by integrating advanced tools for real-time threat detection, response, and analytics. Splunk ES collects and indexes machine data from multiple sources, offering comprehensive visibility into IT environments. Its pre-configured security content, customizable detection rules, and machine learning capabilities enable organizations to proactively identify and mitigate sophisticated threats, including advanced persistent threats (APTs), insider threats, and zero-day vulnerabilities. This paper explores how Splunk ES enhances cybersecurity strategies by leveraging its advanced features. The discussion begins with an overview of SIEM systems, their evolution, and their dual SIM and SEM functionalities. It then delves into the architecture and key capabilities of Splunk ES, including its data collection, indexing, and adaptive response mechanisms. Additionally, the role of machine learning in anomaly detection is examined, focusing on its ability to uncover patterns that traditional methods may overlook. Finally, the paper

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

presents a design for implementing Splunk ES, demonstrating its practical applications and effectiveness in mitigating diverse cyber threats.

2. Literature Review

Security Information and Event Management (SIEM) systems have evolved into indispensable tools for modern cybersecurity practices, combining log management, threat detection, and incident response. This literature review critically examines foundational and recent advancements in SIEM research, highlighting their contributions, limitations, and implications describing SIEM capabilities with Splunk Enterprise Security (ES). Bryant Blake [1] introduced a novel threat ontology model to improve the detection and response capabilities of SIEM systems. His framework, which integrates a kill-chain model into SIEM processes, enhanced the contextual understanding of security incidents by normalizing log data and linking events across multiple stages of an attack lifecycle. This work was pivotal in reducing false positives, a persistent challenge in SIEM systems. However, while Blake's model demonstrated improved detection accuracy, its reliance on predefined ontologies left room for exploration in dynamic and adaptive threat detection, which forms a key focus of more recent studies. Privacy and compliance have become critical considerations in SIEM deployments, as explored by Menges et al. [2]. Their research addressed the integration of General Data Protection Regulation (GDPR) principles into modern SIEM systems. By incorporating pseudonymization and granular access controls, the authors demonstrated a framework that ensures both robust security monitoring and compliance with privacy laws. This dual focus on security and compliance underscores a growing trend in SIEM research, where tools must cater to regulatory requirements without compromising operational efficiency. This study's emphasis on Splunk ES reflects a similar consideration, as Splunk provides extensive tools for regulatory reporting and data protection. The historical progression of SIEM systems was analyzed by Inns [3], who traced their evolution from basic log management tools to sophisticated platforms incorporating real-time analytics and automated response. Inns highlighted early SIEM systems' inability to correlate multi-source events effectively, a limitation that spurred the development of advanced correlation engines. His work serves as a backdrop for understanding the advancements in modern systems like Splunk ES, which address these limitations through machine learning and customizable correlation rules. Expanding the scope of SIEM functionality, Detken et al. [5] explored the integration of Network Access Control (NAC) with SIEM systems, demonstrating the potential for combining access management with real-time monitoring. By leveraging open-source SIEM tools, their study provided a cost-effective solution for small and medium-sized enterprises (SMEs). Although open-source tools offer flexibility, the study acknowledged their limitations in scalability and pre-built functionality, which commercial systems like Splunk ES effectively address through robust analytics and enterprise-grade scalability. Bezas et al. [6] conducted a comparative analysis of open-source and commercial SIEM systems, identifying critical

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

differences in performance, customization, and cost. Their findings highlighted Splunk's superiority in handling large-scale data, offering intuitive dashboards, and supporting diverse use cases. However, they also pointed to challenges such as Splunk's high cost and steep learning curve, raising questions about balancing enterprise-level functionality with accessibility, an area this study explores further by examining Splunk's usability enhancements and training resources. Hristov et al. [8] and Kamal et al. [10] investigated the application of Splunk ES in detecting complex threat vectors, including Distributed Denial of Service (DDoS) attacks and anomalies in IoT environments. Hristov's work emphasized the importance of real-time data visualization and advanced alerting mechanisms in mitigating DDoS attacks, while Kamal's study demonstrated Splunk's adaptability in academic network monitoring. Together, these studies highlight the versatility of Splunk ES in addressing diverse cybersecurity challenges, emphasizing its role in this study as a tool for enhancing threat detection in multi-vector environments. Bruzzese [14] extended Splunk's application by developing a custom app for synthesizing and analyzing application logs. His work illustrated the potential for tailoring SIEM platforms to meet specific organizational needs, a flexibility that underscores the adaptability of commercial systems like Splunk. Similarly, Raja and Vasudevan [9] tackled specific attack patterns by proposing rule-generation techniques for TCP SYN flood detection, highlighting the critical role of customizable correlation rules; a feature extensively leveraged in Splunk ES. Sornalakshmi [17] explored zero-day threat detection using SIEM systems, demon54strating the effectiveness of continuous monitoring and heuristic-based alerting. This study, alongside that of Di Mauro and Di Sarno [7], who addressed encrypted traffic detection, underscores the need for innovative approaches to emerging threats.

These contributions align closely with the adaptive response mechanisms in Splunk ES, which enhance detection and response capabilities for sophisticated attack patterns. Despite the significant advancements in SIEM systems, challenges remain. Bhatt et al. [15] identified issues such as data overload and the complexity of rule creation, which hinder effective decision-making. These limitations emphasize the importance of user-friendly interfaces and automated tools, areas where Splunk ES excels with its machine learning toolkit and pre-built content for common use cases. These studies collectively highlight the evolution of SIEM systems and their trajectory toward greater intelligence, automation, and adaptability. However, they also reveal persistent gaps, such as the need for enhanced automation, privacy-preserving mechanisms, and advanced detection capabilities. This study builds on these insights by exploring how Splunk Enterprise Security addresses these challenges, particularly through its pre-built analytics, machine learning capabilities, and integration with diverse threat detection frameworks. By evaluating Splunk ES in the context of these advancements, this paper contributes a comprehensive analysis of its role in advancing the SIEM landscape.

3. **Security Information and Event Management (SIEM)** Using Splunk Enterprise Security (ES)

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

3.1 Foundational Principles of SIEM Systems

Security Information and Event Management (SIEM) systems form the backbone of modern cybersecurity operations, integrating various processes to detect, analyze, and respond to potential threats. Key functions of SIEM include:

- **Log Collection:** SIEM systems gather logs from a wide variety of monitoring tools and devices, including firewalls, servers, network equipment, and applications. This comprehensive log collection forms the foundation for effective threat detection [15].
- **Log Aggregation:** Once collected, logs are aggregated. This process involves grouping similar log entries to reduce redundancies and avoid overwhelming the security team with excessive data [2].
- **Log Standardization:** Since logs come from various devices and tools with different formats, standardization normalizes this data. This ensures all log data adheres to a common structure, making it easier to analyze and correlate [19].
- **Event Correlation:** Event correlation is the process of connecting different logs and events that may appear unrelated at first glance but are indicative of a potential security threat when combined. This step is crucial for identifying patterns of suspicious behavior and is often powered by rules, machine learning, or artificial intelligence [3].
- **Log Storage:** SIEM systems ensure that logs are stored securely for future reference and for compliance with regulations. Effective log storage solutions protect against tampering, ensuring the integrity of logs for audits, forensic analysis, and long-term retention [19].

Figure 1: Splunk Enterprise SIEM Overview [16]

Splunk Enterprise SIEM platform (Figure 1) is a powerful and versatile platform designed to provide advanced capabilities for log and event management. It delivers seamless log collection, normalization, and correlation, offering users a centralized and cohesive view of their critical IT services. Powered by machine learning, Splunk's analytics capabilities help detect anomalies, uncover root causes, and assess the impact of issues with remarkable efficiency [8].

This research chooses Splunk Enterprise SIEM as the preferred platform due to its numerous advantages. Its instant trial and seamless transition from proof of concept to production make it highly accessible and practical for testing and deployment [14]. Additionally, the platform ensures reliability by offering a dedicated and secure environment for each customer. One of its standout features is the ability to configure custom alert triggers, which enable users to monitor data in real time and identify potential anomalies swiftly [19].

Splunk Enterprise also excels in providing a single, unified view of all machine-generated data, streamlining data management and analysis [10]. This centralized approach not only

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

simplifies monitoring but also enhances the flexibility and adaptability required for businesses to operate at their desired pace. These features make Splunk a reliable and effective choice for experimental and operational purposes, aligning with the dynamic needs of enterprises [16].

The ability of SIEM systems to centralize data and provide actionable insights is critical for maintaining security and operational continuity [2].

3.2 Splunk ES Architecture and Data Management

Splunk Enterprise Security (ES) is built on a robust and scalable architecture (Figure 2), designed to efficiently process, analyze, and manage vast amounts of machine data generated by IT infrastructure and applications [24]. This architecture supports real-time security monitoring and comprehensive data analysis, enabling organizations to proactively detect and respond to threats. Below is a detailed explanation of the key components in the Splunk ES architecture:

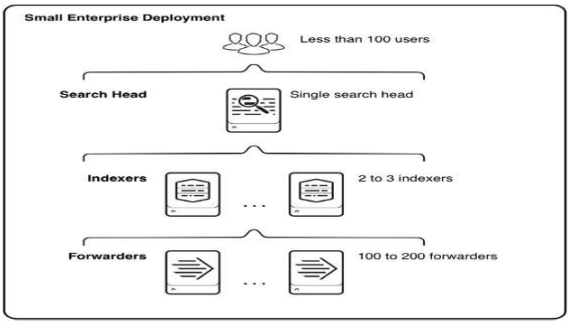

Figure 2: Small Enterprise Deployment [31]

Splunk Forwarders: Splunk Forwarders are lightweight software agents installed on endpoint devices, such as servers, workstations, and network devices, to collect log data. These agents are responsible for:

• **Log Collection:** Capturing logs, metrics, and other machine-generated data from diverse sources, including system logs, application logs, and network traffic [21].

• **Data Preprocessing:** Filtering unnecessary data and performing basic transformations to reduce the volume of data transmitted [2].

• **Data Transmission:** Securely forwarding the pre-processed logs to Indexers in real time using protocols such as TCP or HTTP [21].

• **Splunk Forwarders:** ensure that data collection is decentralized and efficient, reducing the load on central servers [8].

Splunk Indexers: Indexers are the backbone of Splunk's architecture, responsible for:

• **Data Ingestion:** Receiving raw data from Splunk Forwarders and preparing it for indexing [20].

• **Data Parsing and Indexing:** Splitting raw data into searchable events and creating an index for fast retrieval [20].

• **Storage Management:** Storing indexed data in a highly optimized format to ensure quick access while maintaining scalability [14].

• **Search Optimization:** Enabling fast query execution by creating metadata and leveraging indexing algorithms [5].

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

• The distributed nature of Indexers allows Splunk to scale horizontally, accommodating growing data volumes seamlessly [20].

Splunk Search Head: The Search Head serves as the primary user interface for analysts, providing tools for querying, visualizing, and managing data. Its functionalities include:

• **Search Execution:** Allowing users to perform ad-hoc or scheduled searches on indexed data using Splunk's Search Processing Language (SPL) [23].

• **Data Visualization:** Generating dashboards, charts, and graphs to represent trends and anomalies in a user-friendly format [10].

• **Collaboration and Reporting:** Enabling teams to share insights and generate comprehensive reports for stakeholders [22].

• The Search Head ensures that complex data queries are executed efficiently, providing actionable insights in real-time [6].

Splunk Enterprise Security Application: The Splunk Enterprise Security (ES) Application is a specialized module designed specifically for cybersecurity use cases. It includes:

• **Security-Specific Dashboards:** Prebuilt and customizable dashboards to monitor key security metrics and threat landscapes [25].

• **Correlation Rules:** Advanced rule-based logic to correlate multiple events and identify potential security incidents or anomalies [9].

• **Incident Review and Investigation:** Tools for triaging, investigating, and responding to detected threats [16]. • Pre-Built Content: Including use case templates, correlation searches, and security-specific workflows to accelerate deployment and efficiency [18].

• By leveraging the capabilities of the ES application, organizations can enhance threat detection and incident response, tailoring solutions to their specific security needs [17].

4. Core Features of Splunk ES

Splunk Enterprise Security (ES) is an advanced platform designed to enhance an organization's cybersecurity posture. By offering tools for rapid detection, analysis, and mitigation of cyber threats, Splunk ES plays a critical role in modern IT security operations. One of the core strengths of Splunk ES is its pre-built security content, which includes a library of resources that address common cybersecurity scenarios. This content features correlation searches, which are pre-configured queries that help identify patterns of behavior, such as brute-force login attempts or lateral movements within a network. These searches simplify the process of detecting potential threats. Additionally, dashboards in Splunk ES provide visual representations of security data, enabling users to monitor real-time threat status and trends over time. Reports are automatically generated for compliance purposes or to share insights with stakeholders, streamlining the security monitoring process [1] [2].

In terms of real-time monitoring, Splunk ES offers comprehensive visibility into an organization's IT infrastructure. The platform continuously aggregates and normalizes data from diverse sources, such as firewalls, endpoint devices, and cloud environments. This ensures a unified view of all operations, which is

essential for early threat detection. Real-time alerts immediately notify analysts of suspicious activities, allowing for a swift response to mitigate potential risks [19].

Another powerful feature of Splunk ES is its customization options. Users can tailor security rules, dashboards, and alerts to meet the specific needs of their organization. Analysts have the flexibility to define custom correlation rules to detect unique threats that are relevant to their environment. Furthermore, custom dashboards can be designed for specific teams or use cases, providing tailored insights and metrics. Alerts can also be configured to trigger notifications for critical events, ensuring the right teams are informed in real time [14] [19].

Finally, adaptive response in Splunk ES automates predefined actions in response to detected threats. This feature is particularly useful for reducing the time between threat detection and mitigation. Automated actions such as blocking an IP address, isolating a compromised endpoint, or generating service tickets are available. Additionally, Splunk ES integrates seamlessly with incident response systems to streamline workflows, reducing the need for manual interventions and improving response efficiency [5] [19].

5. Machine Learning Workflow in Splunk ES

The machine learning process within Splunk ES is streamlined into distinct phases, each contributing to its ability to detect and analyze threats effectively.

In the raw data collection phase, Splunk ES collects vast amounts of machine data, including system logs, network traffic, and application metrics, from multiple endpoints and sources. This diverse collection of data forms the foundation of Splunk ES's analytical capabilities and ensures that it has access to a comprehensive view of an organization's network and systems [26].

The next phase, feature extraction, involves identifying and extracting relevant features from the raw data that can aid in anomaly detection. These features highlight critical attributes such as login frequency, data transfer rates, and geographical access locations, which are indicative of normal or anomalous behavior. This step is crucial for narrowing down the large volumes of raw data into manageable, meaningful patterns [1].

Once the features have been extracted, the next step is model training. During this phase, machine learning models are trained using historical datasets to learn typical patterns of behavior and establish a baseline for normal activities. Both supervised and unsupervised learning techniques are applied depending on the type of threat being addressed, with supervised learning leveraging labeled datasets to predict specific outcomes, while unsupervised learning focuses on identifying patterns or anomalies without prior labelling [2]. This dual approach enhances the model's ability to detect known and unknown threats.

After the model has been trained, the prediction phase begins. The trained models continuously analyze incoming data in real-time, comparing it to the baseline established during training. Any anomalies or deviations from expected behavior are flagged for further investigation, ensuring that potential threats are detected promptly. This real-time analysis enables immediate responses to unusual activities, such as

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

unauthorized access attempts or suspicious network flows [4].

In the anomaly detection phase, detected anomalies are categorized based on their severity. This classification helps security teams prioritize their response efforts, addressing the most critical threats first. For example, unauthorized login attempts from unusual locations or sudden spikes in network traffic can be flagged as high- severity anomalies requiring immediate attention, while less critical anomalies may be flagged for later review. This tiered approach helps optimize the incident response process [16].

Benefits of Machine Learning in Splunk ES

• Proactive Threat Identification: ML algorithms enable Splunk ES to detect threats before they escalate, minimizing potential damage [14].

• Reduced False Positives: By continuously learning and refining its models, Splunk ES reduces the number of false positives, ensuring analysts focus on genuine threats.

• Enhanced Scalability: Machine learning models can process and analyze large-scale datasets, making Splunk ES suitable for enterprises with extensive IT infrastructures [8] [9].

6. Splunk Enterprise Security Application Implementation Design:

We are ensuring high availability by creating distributed Splunk cluster architecture (as shown in Figure 3) which has Splunk servers in 2 different zones. The following are the major components that are installed and configured as part of the Splunk Security Information and Event Management (SIEM) solution:

• Indexers: An indexer is the Splunk Enterprise instance that indexes data. The indexer processes raw data by converting it into structured events, which are then systematically stored within an index for efficient retrieval and analysis. The indexer also searches the indexed data in response to the search requests.

• Search head: In a distributed search environment, the search head is the Splunk Enterprise instance that handles search management functions, directing search requests to a set of search peers and subsequently consolidates the results to present them back to the user. If this instance does only search and not indexing, it is usually referred to as a dedicated search head. It is the major front-end, generally assessed through Splunk web interface.

• Deployment Server: It manages configuration, apps and content updates across all Splunk components. Deployment server communicates with Heavy Forwarder and Universal Forwarder over port 8089.

• License Master: A License Master in Splunk is a specialized instance responsible for managing and controlling multiple license slaves. It oversees tasks such as defining license stacks, configuring pools, adding licensing capacity, and efficiently managing connected license slaves.

• Universal Forwarders: A lightweight Splunk Enterprise instance that obtains and streams data to the indexers. Currently all the Windows and UNIX servers are installed with Universal Forwarders.

• Heavy Forwarder: HF can be used to decrease parsing load to Indexers and work as log aggregators, also some of the add-ons required for parsing are better suitable on HF.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

• Cluster Master Node: Regulate the functioning of an index cluster; controls and manages index replication.

• Syslog Server: Syslog provides a standardized method for network devices to transmit event messages to a centralized logging server, commonly referred to as a Syslog server. Widely supported by various devices, the Syslog protocol enables logging of diverse event types. Many networking components, including routers and switches, can generate and sending Syslog messages.

• Splunk Apps: They are pre-built collections of dashboards, panels and UI elements that are driven by pre-configured searches and packaged for a specific technology or use case.

• Splunk Web: It is an interactive graphical user interface in Splunk that remote users can connect to over a web browser for administration, problem investigation and reporting on results.

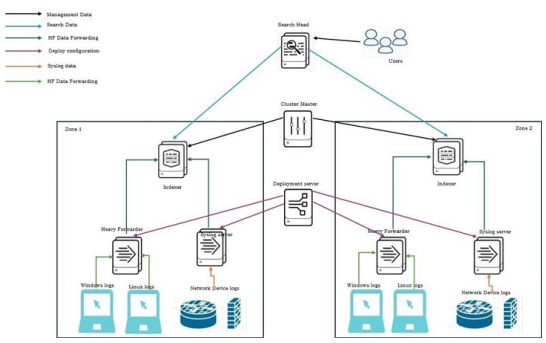

Figure 3: Splunk ES Application Architecture Design

The Universal Forwarders will be installed on Windows and Linux machines and these logs will be forwarded to the Heavy Forwarder where we can filter logs and send it further to the Indexer for data parsing and indexing. Network device logs are sent to the Syslog server which has a Splunk Universal Forwarder installed on it already, will further send these logs to the Splunk Indexer within the same zone. The Heavy Forwarder and Syslog server in both the zones is managed by the Deployment server and the Cluster Master manages the Indexers in the two zones. The Search head is used by the SOC analyst to view and analyse event data, thus working on the cyber threats detected. This Search head can view and searches data from both the indexers in our Splunk architecture and has the Splunk ES application installed on it. In our Splunk architecture, we are considering Cluster Master to act also as the License Master (hence not shown in diagram).

Real-World Applications and Case Studies

Splunk ES has been successfully deployed across various industries to mitigate cyber threats. Some Real-world examples include:

• • Advanced Persistent Threats (APTs): Detecting and responding to prolonged, targeted attacks.

• • Insider Threats: Identifying malicious or accidental activities by employees.

• • Zero-Day Attacks: Spotting unknown vulnerabilities through anomaly detection.

7. Conclusions and Future Research

Splunk Enterprise Security has proven to be a valuable tool in the fight against modern cybersecurity challenges. Its ability to integrate advanced analytics with traditional SIEM functionalities offers organizations a scalable and effective solution for threat management. The platform's centralized data management, real-time alerting, and customizable dashboards help streamline security operations, improve threat detection, and

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

enable rapid response. Furthermore, Splunk ES is well-suited to meet compliance requirements, making it an essential component of a robust enterprise cybersecurity strategy [20].

In this study, Splunk Enterprise Security seemed to promise its capability to provide insights that enable timely identification and mitigation of threats. The use of machine learning and adaptive response mechanisms can enhance the efficiency and precision of threat analysis, reducing response times and minimizing the potential impact of security incidents. These features make Splunk ES a versatile and reliable tool for securing enterprise environments in an ever-changing threat landscape [26].

While Splunk Enterprise Security offers significant advantages, further research could explore additional enhancements and applications to address emerging cybersecurity challenges. Some potential areas for future work include:

• **AI-Powered Threat Intelligence:** Integrating more advanced AI models into Splunk ES could improve predictive threat analysis, allowing organizations to anticipate and prepare for potential attacks before they occur [2].

• **Integration with IoT and OT Security:** As the Internet of Things (IoT) and Operational Technology (OT) environments grow, research could focus on how Splunk ES can be adapted to monitor and secure these domains effectively [8].

• **Behavioral Analysis and Insider Threat Detection:** Developing enhanced behavioral analytics capabilities within Splunk ES could improve the detection of insider threats and anomalous activity that traditional methods might overlook [9].

• **Automated Incident Response:** Future studies could explore integrating Splunk ES with more sophisticated SOAR (Security Orchestration, Automation, and Response) capabilities to automate complex incident response workflows further [20]. These research directions would not only extend the capabilities of Splunk Enterprise Security but also strengthen its role as a critical tool in the ever-evolving cybersecurity landscape. By addressing these areas, future advancements can ensure that Splunk ES remains at the forefront of enterprise security solutions [14].

Acknowledgements

The author would like to thank Business Finland (BF) within the EUREKA CELTIC-NEXT project CISSAN (www.celticnext.eu.) for supporting this work.

References

Bryant Blake (2016) "Hacking SIEMS to Catch Hackers: Decreasing the Mean Time to Respond to Security Incidents with a Novel Threat Ontology in SIEM Software", Master's Thesis, University of Kansas Florian Menges et al (2021) "Towards GDPR-compliant data processing in modern SIEM systems", Computers & Security, Volume 103, April 2021, 102165, https://doi.org/10.1016/j.cose.2020.102165 https://www.splunk.com/content/dam/splunk2/en_us/gated/ebooks/top-5-use-cases-for-splunk-security-analytics.pdf J. Inns, "The evolution and application of SIEM systems," Netw. Secur., vol. 2014, no. 5, pp. 16–17, May 2014 J. Kaskade, "Magic Quadrant for Security Information and Event Management," p. 32

Kai-Oliver Detken et al (2017) "Combining Network Access Control (NAC) and SIEM functionality based

on open source", 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), DOI: 10.1109/IDAACS.2017.8095094 Konstantinos Bezas et al (2023) "Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)", Indonesian Journal of Computer Science, ISSN 2549-7286, DOI: 10.33022/ijcs.v12i2.3182 M. Di Mauro and C. Di Sarno, "Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection," J. Inf. Secur. Appl., vol. 38, pp. 85–95, Feb. 2018 Marian Hristov et al (2021) "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT", IEEE 20th International Symposium on Network Computing and Applications (NCA), DOI: 10.1109/NCA53618.2021.9685977 M. Siva Niranjan Raja, A.R. Vasudevan (2017) "Rule Generation for TCP SYN Flood attack in SIEM Environment", 7th International Conference on Advances in Computing & Communications, ICACC-2017, Cochin, India, https://doi.org/10.1016/j.procs.2017.09.117 Muhammad Rijal Kamal et al (2021) "Anomaly Detection with Splunk Security Information and Event Management (SIEM) on UII Network", AUTOMATA Journal, https://journal.uii.ac.id/AUTOMATA/issue/view/1482 NIST. (2022). Guidelines for Automated Threat Response in SIEM Systems. Retrieved from https://www.nist.gov Official Manual of Splunk®, Enterprise - Alerting Manual, version 8.2.2, Copyright © 2021 Splunk Inc Official Manual of Splunk®, Enterprise - Getting Data In, version 8.2.2, Copyright © 2021 Splunk Inc Roberto Bruzzese, (2019) "An Analysis of Application Logs with Splunk: Developing an App for the Synthetic Analysis of Data and Security Incidents", https://doi.org/10.48550/arXiv.1912.11283 Sandeep Bhatt et al (2014) "The Operational Role of Security Information and Event Management Systems", IEEE Security & Privacy (Volume: 12, Issue: 5, Sept.-Oct. 2014), DOI: 10.1109/MSP.2014.103 Seyed Morteza Zeinali, (2016) "Analysis of Security Information and Event Management (SIEM) Evasion and Detection Methods", Master's Thesis available at: https://mendillo.info/seguridad/tesis/Morteza.pdf Sornalakshmi.K (2017) "Detection of DoS attack and Zero Day Threat with SIEM", International Conference on Intelligent Computing and Control Systems (ICICCS) 2017 Splunk Documentation. (2024). Use Cases for Pre-Built Content in Splunk ES. Retrieved from https://docs.splunk.com Splunk Inc. (2024). How Adaptive Response Enhances Incident Management. Retrieved from https://docs.splunk.com Splunk Inc. (2024). How Indexing Works in Splunk Enterprise. Retrieved from https://docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresdata Splunk Inc. (2024). Introduction to Forwarding and Receiving. Retrieved from https://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Aboutforwardingandreceiving Splunk Inc. (2024). Real-Time Monitoring and Threat Detection in Splunk. Retrieved from https://www.splunk.com Splunk Inc. (2024). Search Head Overview. Retrieved from https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/AboutSH Splunk Inc. (2024). Splunk Architecture: Data-to-Everything Platform. Retrieved from https://www.splunk.com/en_us/resources.html Splunk Inc. (2024). Splunk Enterprise Security Overview. Retrieved from https://docs.splunk.com/Documentation/ES/latest/Ov

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

erview/IntroductiontoES Splunk, “Splunk® Machine Learning Toolkit User Guide 5.2.0,” Splunk Inc, 2020. https://docs.splunk.com/Documentation/MLApp/5.2.0/User/WelcometoMLTK (accessed Sep. 10, 2020) S. S. Sekharan and K. Kandasamy, “Profiling SIEM tools and correlation engines for security analytics,” in 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017, pp. 717–721 Stallings, W., & Brown, L. (2021). Computer Security: Principles and Practice. Pearson Wahluf Abidian et al. (2021) "Implementing Splunk in Building SIEM Based on Firewall Logs: A Case Study of UII Network", AUTOMATA Journal, https://journal.uii.ac.id/AUTOMATA/issue/view/1390 Splunk Inc. (2021). Splunk Enterprise Overview. Retrieved from