PROJECT REPORT

ON

SIEM FOR ANALYSIS & THREAT DETECTION

Submitted By

Seema Kanwar (2301410020)

Payal Rathore (2301410022)

Adhvay Banerjee (2301410002)

Amitabh Srivastava (2301410016)

Under the guidance of

University Guide
Ms. Ruchika Bhakhar
Ms. Archna Goyal
(Assistant professor)
School of Engineering and Technology

Industry Guide

Mr. Harsh Goyal
Founder, (Suvikson Technologies Pvt. Ltd.)



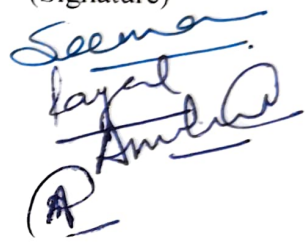
Department of Computer Science and Engineering

School of Engineering and Technology

K. R. Mangalam University, Gurugram – 122003

DECLARATION

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have not been properly cited or from whom proper permission has not been obtained when needed.

Student Name	(Roll No.)	(Signature)
Seema Kanwar	2301410020	
Payal Rathore	2301410022	
Adhvay Banerjee	2301410002	
Amitabh Srivastava	2301410016	

Place: K.R. Mangalam University

Date: 5th December 2024

CERTIFICATE

This is to certify that

S No.	Roll Number	Name	Place of Work	Duration of Project
1	2301410020	Seema Kanwar	KR Mangalam University, Gurugram	15th OCT, 2024 – 5th DEC, 2024
2	2301410022	Payal Rathore	KR Mangalam University, Gurugram	15th OCT, 2024 – 5th DEC, 2024
3	2301410002	Adhvay Banerjee	KR Mangalam University, Gurugram	15th OCT, 2024 – 5th DEC, 2024
4	2301410016	Amitabh Srivastava	KR Mangalam University, Gurugram	15th OCT, 2024 – 5th DEC, 2024

enrolled in B.Tech CSE (cybersecurity) program have satisfactorily completed the project SIEM FOR ANALYSIS & THREAT DETECTION under the guidance of *Mr. Harsh* and *Ms. Ruchika Bhakhar, Ms. Archna Goyal* of School of Engineering and Technology.

This project work represents their original work and the references given in the present report are authentic.

Industry Mentor:

Mr. Harsh Goyal

Designation: Founder

Suvikson Technologies Pvt. Ltd.

Faculty In charge:

Ms. Ruchika Bhakhar

Ms. Archna Goyal

Dean Name:

Prof.Pankaj Agrawal

School Name: SOET

SR. NO- SUVIKSAN/24-25/KRPC112

K.R. MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

SEEMA SEKHAWAT

(Roll no -2301410020, B. Tech CSE (Cyber Security),3rd Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
KR MANGALAM UNIVERSITY, GURUGRAM

has successfully completed the project on

SIEM FOR ANALISIS & THREAT DETECTION

OCTOBER 15, 2024 - DECEMBER 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.

SR. NO- SUVIKSAN/24-25/KRPC113

K.R. MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

PAYAL RATHORE

(Roll no -2301410022, B. Tech CSE (Cyber Security),3rd Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
KR MANGALAM UNIVERSITY, GURUGRAM

has successfully completed the project on

SIEM FOR ANALISIS & THREAT DETECTION

OCTOBER 15, 2024 - DECEMBER 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.



SR. NO- SUVIKSAN/24-25/KRPC110

K.R. MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

ADHVAY BANERJEE

(Roll no -2301410002, B. Tech CSE (Cyber Security),3rd Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
KR MANGALAM UNIVERSITY, GURUGRAM

has successfully completed the project on

SIEM FOR ANALISIS & THREAT DETECTION

OCTOBER 15, 2024 - DECEMBER 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.



SR. NO- SUVIKSAN/24-25/KRPC111

K.R. MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

AMITABH SRIVASTAVA

(Roll no -2301410016, B. Tech CSE (Cyber Security),3rd Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
KR MANGALAM UNIVERSITY, GURUGRAM

has successfully completed the project on

SIEM FOR ANALISIS & THREAT DETECTION

OCTOBER 15, 2024 - DECEMBER 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.

ACKNOWLEDGEMENT

We extend our sincere gratitude to our faculty guide, Ms. Ruchika Bhakhar and Ms. Archna Goyal for her insightful guidance, constructive criticism, and unwavering support throughout the entire project. We are especially grateful for her expertise in project and her encouragement that pushed us to excel. We would also like to express our sincere appreciation to our industry mentor, Mr. Harsh Gupta, for their invaluable industry insights, practical advice, and for providing us with real-world perspectives. We are deeply grateful for their time, patience, and for sharing their valuable experience in the field. Finally, we would like to thank our peers and colleagues for their insightful discussions and helpful feedback during our brainstorming sessions. Their support has been invaluable in shaping this report.

Place: - K.R. Mangalam University

Date: -

Name of Students:
Seema Kanwar
Payal Rathore
Adhvay Banerjee
Amitabh Srivastava

ABSTRACT

This project report explores the implementation and application of Security Information and Event Management (SIEM) solutions for real-time analysis and threat detection. SIEM systems aggregate and analyze log data from diverse sources to provide actionable insights, enabling organizations to detect, investigate, and respond to security incidents efficiently. The project emphasizes the integration of advanced analytics, threat intelligence, and automation to improve the effectiveness of SIEM solutions. The report also details challenges in traditional SIEM systems, such as handling large-scale data and managing false positives, and proposes methods to overcome these issues.

Key Words: SIEM, Threat Detection, Real-Time Monitoring, Incident Response, Security Analytics

TABLE OF CONTENTS

Content	Page no.
Declaration	2
Certificate	3
Acknowledgement	6
Abstract	7
Introduction	9
Literature Review	10
Problem Formulation and Objectives	11
Methodology	12
Implementation	13
Results and Discussion	14
Conclusion and Future Scope	15
References	16

1. INTRODUCTION:

The evolving cybersecurity landscape has made it critical for organizations to adopt robust threat detection and response systems. Security Information and Event Management (SIEM) systems provide a centralized platform for log collection, real-time monitoring, and threat analysis. By aggregating data from multiple sources, such as firewalls, servers, and endpoint devices, SIEM systems enable security teams to identify anomalies, detect intrusions, and respond to threats effectively.

This project focuses on leveraging SIEM systems to enhance security monitoring and threat detection capabilities, ensuring organizations are better equipped to prevent and mitigate cyberattacks.

1.1 Technological Context

SIEM systems combine data aggregation, analytics, and threat intelligence to provide actionable insights. These systems utilize machine learning and rule-based logic to analyze log data for identifying suspicious activities. Modern SIEM solutions also integrate automation for streamlined incident response, reducing the time required to address security events.

1.2 Significance in Modern Cybersecurity

The increasing frequency and complexity of cyber threats necessitate proactive security measures. SIEM systems play a pivotal role in modern cybersecurity frameworks by enabling organizations to identify potential vulnerabilities and mitigate risks before they escalate into significant incidents. This report highlights the transformative impact of SIEM solutions in improving organizational resilience against cyberattacks.

2. LITERATURE REVIEW:

Existing SIEM Solutions Prominent SIEM tools such as Splunk, IBM QRadar, and ArcSight have transformed how organizations manage cybersecurity threats. Each solution provides unique features, from real-time monitoring to integration with third-party threat intelligence platforms. Despite their capabilities, challenges such as high operational costs, complexity, and data overload persist.

Splunk, known for its powerful search and analytics capabilities, excels in processing and visualizing large volumes of data. IBM QRadar leverages built-in intelligence to prioritize threats, reducing the burden on security teams. ArcSight focuses on scalability, making it suitable for large enterprises with diverse security needs. However, the operational complexity and steep learning curve associated with these tools often act as barriers to their widespread adoption.

Advances in Threat Detection Recent advancements in AI and machine learning have significantly improved SIEM capabilities. These technologies enable systems to detect advanced persistent threats (APTs), insider threats, and zero-day attacks with greater accuracy. Integrating threat intelligence feeds enhances the detection of known threats by leveraging global attack data.

Research indicates that machine learning models, such as anomaly detection and clustering algorithms, are highly effective in identifying deviations from normal behavior patterns. For instance, unsupervised learning techniques help detect unknown threats by analyzing historical data and identifying outliers.

Challenges in Traditional SIEM Systems Despite technological advancements, traditional SIEM systems face significant challenges. The high volume of false positives generated by these systems often leads to alert fatigue among security analysts. Additionally, the lack of standardization in log formats complicates data integration from diverse sources. Addressing these challenges requires a combination of advanced analytics, streamlined workflows, and user-friendly interfaces.

3. PROBLEM FORMULATION AND OBJECTIVES

3.1 Problem Formulation

Traditional SIEM systems face limitations, such as:

- High false positive rates leading to alert fatigue.
- Difficulty in processing and analyzing large volumes of log data.
- Limited automation capabilities, increasing response times.

Organizations struggle to achieve comprehensive visibility into their network activities, leaving critical vulnerabilities unaddressed. Furthermore, the manual intervention required for threat investigation and response delays mitigation efforts, increasing the risk of data breaches.

3.2 Objectives

- To enhance threat detection accuracy by integrating machine learning models.
- To streamline incident response through automation.
- To improve scalability and reduce operational complexity.
- To enable real-time monitoring and predictive analytics for proactive threat management.

3.3 Scope of the Project

This project focuses on developing a scalable and efficient SIEM framework that addresses the limitations of traditional systems. Key areas of focus include data ingestion, correlation rule creation, and the implementation of automated response mechanisms. The project also explores the integration of external threat intelligence feeds to enhance detection capabilities.

4. METHODOLOGY

4.1 Data Collection

Logs from firewalls, intrusion detection systems (IDS), and servers are collected and centralized within the SIEM platform. These logs are pre-processed to ensure consistency in format and eliminate redundant data. Data enrichment techniques, such as geolocation tagging and threat intelligence integration, are applied to provide additional context for analysis.

4.2 Analysis Techniques

Machine learning algorithms and predefined correlation rules are applied to analyze logs for identifying potential threats. Supervised learning models are trained using labeled datasets to detect known attack patterns, while unsupervised models identify anomalies indicative of emerging threats. Additionally, rule-based logic ensures compliance with regulatory standards and organizational policies.

4.3 Incident Response

Automated workflows are developed to respond to detected incidents, reducing response times and improving efficiency. These workflows include actions such as isolating affected systems, notifying stakeholders, and generating detailed incident reports. Integration with Security Orchestration, Automation, and Response (SOAR) platforms further enhances the incident response process.

4.4 Performance Metrics Key

performance metrics, such as detection accuracy, false positive rate, and mean time to detect (MTTD), are monitored to evaluate the system's effectiveness. These metrics are analyzed to identify areas for improvement and ensure the SIEM system meets organizational requirements.

5. IMPLEMENTATION

This section details the integration of a SIEM platform, including data ingestion, analytics configuration, and automation. Specific use cases, such as detecting brute force attacks or anomalous user behavior, are implemented to demonstrate system capabilities.

5.1 Data Ingestion and Normalization

The implementation process begins with data ingestion from diverse sources, including network devices, servers, and cloud platforms. Data normalization ensures consistency in log formats, enabling seamless analysis across different data types.

5.2 Rule-Based Correlation

Correlation rules are defined to identify relationships between events and detect complex attack scenarios. For example, a rule might trigger an alert when multiple failed login attempts are followed by a successful login from the same IP address.

5.3 Integration with Threat Intelligence

External threat intelligence feeds are integrated to enhance the system's ability to detect known threats. These feeds provide information on indicators of compromise (IOCs), such as malicious IP addresses and domains, enabling the SIEM system to identify and block threats proactively.

5.4 Automation and Orchestration Automated workflows

are implemented to streamline incident response. These workflows include actions such as isolating affected systems, notifying stakeholders, and generating detailed incident reports. Integration with SOAR platforms further enhances the automation capabilities, enabling coordinated responses across multiple security tools.

6. RESULTS AND DISCUSSION

The implemented SIEM system successfully detected and responded to simulated cyberattacks in a controlled environment. Key performance metrics, such as detection accuracy and response time, are discussed. The system's ability to process large volumes of data and generate actionable insights was evaluated, demonstrating its effectiveness in improving threat detection and response capabilities.

6.1 Use Case:

Brute Force Attack Detection A use case involving brute force attack detection was implemented to test the system's capabilities. The SIEM system successfully identified multiple failed login attempts from a single IP address, triggering an automated response to block the IP and notify the security team.

6.2 Performance Evaluation

Performance metrics, including MTTD and false positive rate, were monitored to evaluate the system's effectiveness. The results indicate significant improvements in detection accuracy and response times compared to traditional systems.

7. CONCLUSION AND FUTURE SCOPE

This project underscores the importance of SIEM systems in modern cybersecurity. The implementation of advanced analytics, machine learning, and automation significantly enhances threat detection and response capabilities. Future work could involve enhancing scalability through cloud-based SIEM solutions and exploring advanced AI techniques for improved threat detection. Additional research could focus on integrating predictive analytics to anticipate and mitigate potential threats proactively.

REFERENCES

1. Splunk Documentation: https://www.splunk.com/
2. IBM QRadar Technical Papers: https://www.ibm.com/products/qradar-siem
3. ArcSight User Guides: https://www.microfocus.com/en-us/cyberres/arcsight
4. Research articles on AI and cybersecurity
5. Threat Intelligence Data from Recorded Future: https://www.recordedfuture.com/
6. MITRE ATT&CK Framework: https://attack.mitre.org/
7. Elastic SIEM Overview: https://www.elastic.co/siem
8. Palo Alto Networks Threat Intelligence: https://www.paloaltonetworks.com/cyberpedia/what-is-threat-intelligence
9. NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
10. CIS Critical Security Controls: https://www.cisecurity.org/controls