iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: III Month of publication: March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67835

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Cyber Security SOC Analyst

Vandan Beladiya, MihirSontakke
ParulInstituteofEngineering&Technology,Vadodara,Gujarat

Abstract:In today's rapidly evolving digital landscape, organizations face an increasing number of cyber threats that jeopardize their sensitive data, operations, and reputation. A Cyber Security Security Operations Center (SOC) Analyst plays a critical role in detecting, analyzing, and mitigating cyber threats in real-time. This role involves continuous monitoring of security alerts, incident response, threat intelligence analysis, and ensuring compliance with security policies and frameworks. SOC Analysts leverage advanced security tools such as SIEM (Security Information and Event Management) systems, IDS/IPS, firewalls, and endpoint protection solutions to safeguard organizational assets. Their expertise in log analysis, network traffic monitoring, and threat hunting helps in identifying vulnerabilities and minimizing the risk of cyberattacks. As cyber threats become more sophisticated, the role of a SOC Analyst remains pivotal in strengthening an organization's cybersecurity posture and resilience.

I. INTRODUCTION

A Security Operations Center (SOC) Analyst is a cybersecurity professional responsible for monitoring, detecting, and responding to security threats within an organization's IT infrastructure. SOC Analysts play a crucial role in protecting sensitive data, preventing cyberattacks, and ensuring compliance with security policies.

Their primary tasks include analyzing security alerts, investigating potential threats, and coordinating incident response efforts. Using advanced security tools such as SIEM (Security Information and Event Management) systems, firewalls, intrusion detection systems (IDS/IPS), and endpoint protection solutions, SOC Analysts help identify and mitigate cyber risks in real-time.

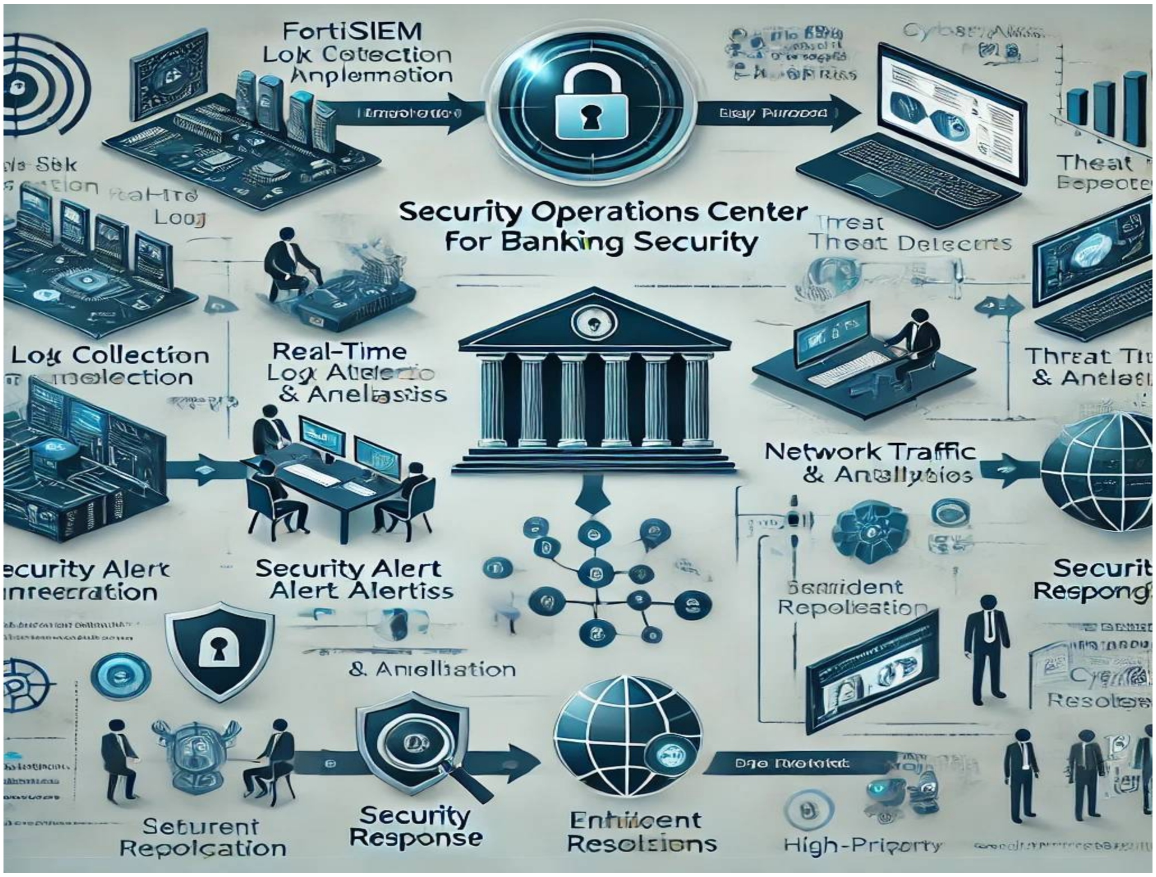
II. RELATEDWORK

In the banking sector, cybersecurity is a critical component of operational integrity, as financial institutions are prime targets for cyber threats, including fraud, data breaches, and ransomware attacks. A Security Operations Center (SOC) serves as the backbone of a bank's cybersecurity infrastructure, providing continuous monitoring, threat detection, and incident response.Related work in SOC-based banking security primarily focuses on threat intelligence, anomaly detection, risk management, and regulatory compliance. Researchers and industry experts have explored the integration of AI-driven threat detection, behavioral analytics, and real-time monitoring to enhance security operations. Studies highlight the importance of Security Information and Event Management (SIEM) systems, Intrusion Detection/Prevention Systems (IDS/IPS), and endpoint security solutions in proactively identifying and mitigating cyber threats.Additionally, literature on SOC frameworks emphasizes the role of automation, threat hunting, and machine learning in improving response time and reducing false positives. Compliance with banking regulations such as PCI DSS, GDPR, and FFIEC guidelines is another key area of SOC research, ensuring that security measures align with industry standards.This study examines existing SOC methodologies and technologies applied in banking security, identifying challenges such as advanced persistent threats (APTs), insider threats, and evolving attack vectors. By analyzing current approaches and innovations, this research aims to contribute to the development of a more resilient, adaptive, and intelligent SOC framework for banking institutions

II. METHODOLOGY

1) This study employs a Security Operations Center (SOC) methodology that integrates FortiSIEM, email communication, and direct calling to ensure a robust security monitoring and incident response framework for banking security. FortiSIEM, a powerful Security Information and Event Management (SIEM) tool, is used for real-time log collection, correlation, and threat detection across the bank's IT infrastructure. By analyzing network traffic, system logs, and endpoint activities, FortiSIEM helps detect anomalies, unauthorized access, and potential cyber threats.
2) When security alerts are generated, analysts assess the severity of the incidents through log analysis, threat intelligence feeds, and behavioral analytics. Based on the criticality of the event, SOC analysts initiate response procedures using email notifications and direct calls to the relevant stakeholders. Low-priority alerts are addressed via email for documentation and further investigation, whereas high-priority threats, such as ransomware attacks or unauthorized financial transactions, trigger immediate phone calls to security teams and bank executives for swift action.

3) The methodology also includes incident validation, threat containment, and resolution tracking. All incidents are documented in a centralized incident management system, ensuring compliance with regulatory frameworks such as PCI DSS and GDPR. This integrated approach enhances the bank's cyber resilience, minimizes response time, and improves coordination among SOC teams and banking officials.



III. IMPLEMENTATION

To build an effective Security Operations Center (SOC), analysts rely on a combination of tools, methodologies, and best practices to detect, analyze, and mitigate cybersecurity threats. Below is a structured approach to implementing SOC analyst tools and processes in a banking environment.

1. Security Information and Event Management (SIEM) – FortiSIEM Implementation

☑ Tool Used:FortiSIEM (or alternatives like Splunk, IBM QRadar, ArcSight)

☑Implementation Steps:

- Deploy FortiSIEM to collect and correlate logs from firewalls, servers, and network devices.
- Configure custom rule sets to detect anomalies and potential cyber threats.
- Integrate with threat intelligence feeds for real-time detection of malicious activities.
- Automate alerts and categorization based on criticality levels (low, medium, high).

2. Intrusion Detection & Prevention Systems (IDS/IPS)

☑ Tools Used: Snort, Suricata, Palo Alto Threat Prevention

☑Implementation Steps:

- Deploy IDS/IPS sensors at network entry points to monitor inbound and outbound traffic.
- Configure signature-based and behavioral anomaly detection techniques.
- Set up alert forwarding to the SIEM for real-time analysis and response.

3. Endpoint Detection and Response (EDR/XDR)
☑ Tools Used: CrowdStrike Falcon, Microsoft Defender, SentinelOne
☑Implementation Steps:

- Install EDR agents on all critical banking infrastructure endpoints.
- Enable automated threat detection and response for malware, ransomware, and unauthorized access.
- Integrate with SIEM to correlate endpoint activity with network logs.

4. Threat Intelligence & Hunting
☑ Tools Used:MISP, Recorded Future, ThreatConnect
☑Implementation Steps:

- Implement threat intelligence feeds to receive up-to-date threat actor information.
- Automate IOC (Indicators of Compromise) correlation within SIEM.
- Conduct proactive threat hunting using YARA rules and Sigma rules.

5. Incident Response & Communication
☑Tools Used:TheHive, Cortex, Email & Phone Alerting Systems
☑mplementation Steps:

- Set up automated incident response workflows with case management tools.
- Establish email notification and direct calling procedures for high-priority threats.
- Maintain an incident tracking system to document response actions and resolutions.

6. Compliance & Reporting (PCI DSS, GDPR, NIST Frameworks)
☑Tools Used: Nessus, OpenVAS, Splunk Compliance Dashboard
☑Implementation Steps:

- Conduct regular vulnerability assessments and penetration testing.
- Automate compliance reporting dashboards in SIEM for auditing purposes.
- Ensure log retention policies meet regulatory requirements.

A. KeyFeatures

1) Real-Time Threat Monitoring
2) Incident Detection and Response
3) Security Information and Event Management (SIEM) Expertise
4) Threat Intelligence & Hunting
5) Intrusion Detection & Prevention (IDS/IPS) Management
6) Endpoint Security & Malware Analysis
7) Security Compliance & Risk Management
8) Automation & Security Orchestration
9) Communication & Collaboration
10) Continuous Learning & Cybersecurity Awareness

IV. EVALUATION

Evaluating the effectiveness of a Security Operations Center (SOC) is essential to ensure it meets organizational security needs, detects threats efficiently, and responds to incidents effectively. The evaluation process involves various metrics, methodologies, and frameworks.

1) MTTD (Mean Time to Detect) – How fast threats are identified.
2) MTTR (Mean Time to Respond) – Speed of incident response.
3) False Positive Rate – Number of unnecessary alerts.
4) Threat Containment Rate – How well threats are neutralized.
5) SOC Coverage & Visibility – Ensuring complete system monitoring.

SOC
A SECURITY OPERATIONS CENTER ANALYST
SOC
RECAL-TIME THEIATREAIT
REAL-TIME MONTORING
INTIENT DETRACT AND RESPONSE
MASTIIIONS
EXPERESS
DETECTION & RESPONSE EXPERIENSE
INTURENT INTIINRANT EXFELIGENCE
SECURITY SECURITY
ECURITY INTERIGTION EVENT MARAGEMST
ENDELIRITE & SECURITE ENTORNRE
ECURITY SECURITY LURITY
INTUPOTE SECURITY & PERVENTMION
INTHPONT SECURITY
COMMUNICAT & SECURIDIRATION
COMMNUNIN & CYBERGIA

V.CONCLUSION&FUTUREWORK

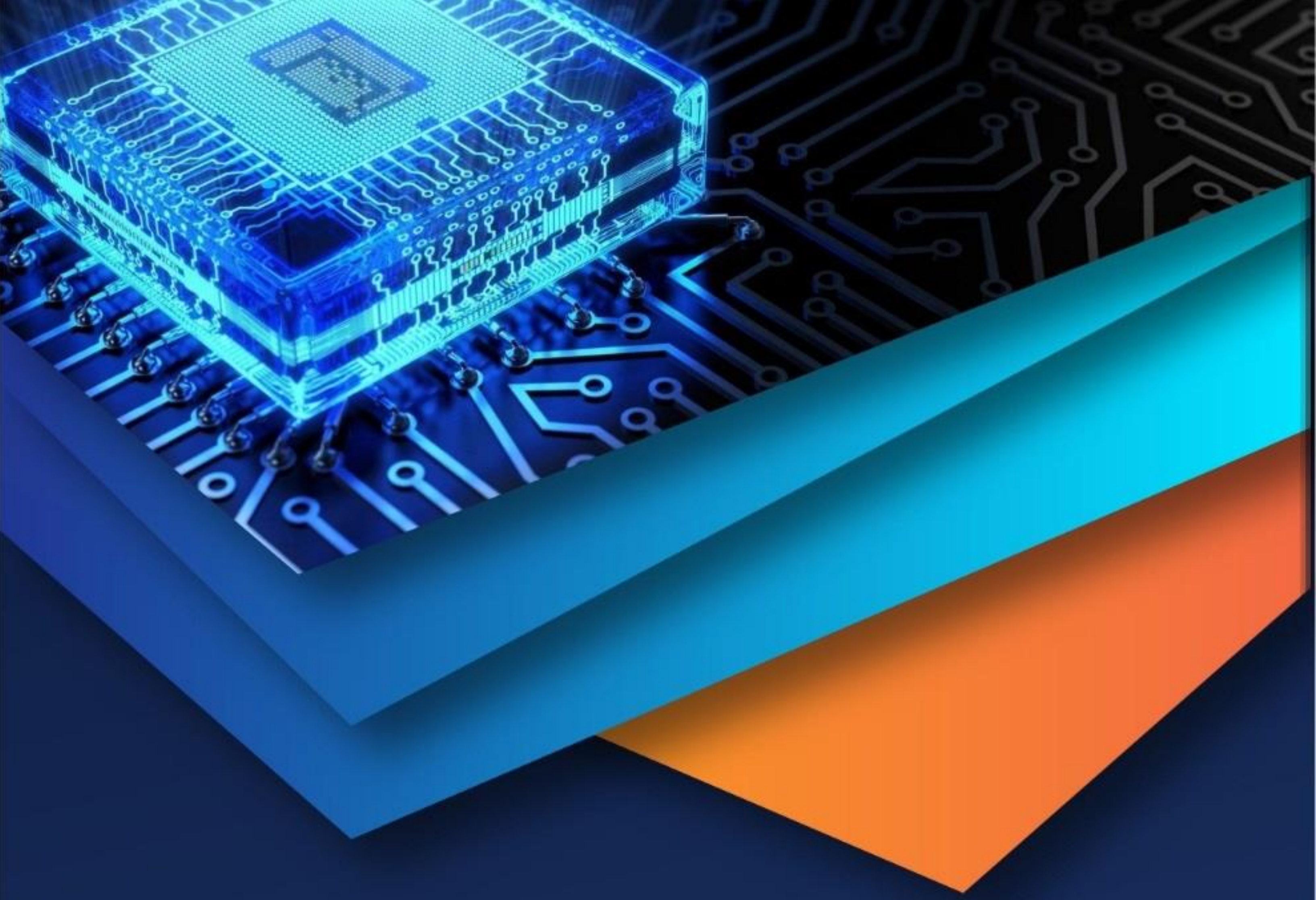
A well-structured Security Operations Center (SOC) is essential for detecting, analyzing, and responding to cyber threats in real-time. By integrating SIEM tools like FortiSIEM, IDS/IPS, threat intelligence, and incident response protocols, SOC analysts can effectively mitigate risks and enhance an organization's security posture. Regular evaluation through KPIs, maturity models, and red/blue team exercises ensures continuous improvement. With cyber threats evolving rapidly, maintaining a proactive SOC is critical to safeguarding banking and financial institutions from potential cyberattacks..

Futureimprovementswillfocuson:

1) AI and Machine Learning Integration – Enhancing threat detection through automated anomaly detection and predictive analytics.
2) Zero Trust Architecture – Implementing stricter access controls to minimize insider threats and unauthorized access.
3) Cloud Security Expansion – Strengthening SOC capabilities for multi-cloud environments as financial institutions adopt cloud technologies.
4) Automation with SOAR – Increasing the use of Security Orchestration, Automation, and Response (SOAR) to reduce manual efforts and improve response times.
5) Improved Threat Hunting – Advancing proactive security strategies to detect hidden threats before they cause harm.
6) Compliance Adaptation – Keeping up with evolving regulatory requirements such as GDPR, PCI DSS, and upcoming global cybersecurity standards.

REFERENCES

[1] Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.Covers fundamental security concepts, including SOC operations, SIEM, and threat intelligence.
[2] NIST (2020). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.Provides guidelines on cybersecurity frameworks used in SOC evaluations.
[3] MITRE ATT&CK Framework. (https://attack.mitre.org/)A widely used knowledge base of adversary tactics and techniques for SOC analysts.
[4] Fortinet (2022). FortiSIEM: Next-Gen Security Information and Event Management. Fortinet Whitepaper.Explains how FortiSIEM helps in log management, real-time threat detection, and SOC operations.
[5] Gartner (2021). Market Guide for Security Information and Event Management (SIEM).
[6] Provides insights into the latest SIEM trends, including tools used in modern SOCs.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429