ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

INTEGRATING AI-ENHANCED SIEM AND SOAR FOR CYBER RESILIENCE IN THE INDIAN BFSI SECTOR

Mrs. Savita P. Patil[1], Dr. A. D. Goswami[2]
[1] *Ph.D. Research Scholar, KBCNMU, Jalgaon.*
Email: savita.190984@gmail.com
[2] *Research Guide, P.O. Nahata Collage, Bhusawal.*

Abstract
The rapid digitization of the Indian financial landscape, catalyzed by UPI 2.0 and CBDC integration, has exposed the Banking, Financial Services, and Insurance (BFSI) sector to sophisticated, machine-speed cyber threats. Traditional Security Operations Centers (SOCs) face alert fatigue and struggle to meet the Reserve Bank of India's (RBI) 6-hour incident reporting mandate. This paper proposes an autonomous security framework integrating AI-driven SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response). Using a comparative simulation of a Synthetic Identity Attack, the study benchmarks a traditional rule-based SOC against an AI-enhanced Agentic SOC. Results indicate a 68% reduction in Mean Time to Respond (MTTR) and improved detection accuracy using User and Entity Behavior Analytics (UEBA). The framework aligns with RBI's 2025 FREE-AI guidelines by incorporating Explainable AI logs for regulatory transparency.
Keywords: AI-SIEM, SOAR, Agentic SOC, RBI FREE-AI Framework, UPI Fraud, Cyber Resilience.

► *Corresponding Author: Mrs. Savita P. Patil*

Introduction

- **AI-SIEM** functions as the central nervous system of the SOC. Unlike legacy SIEM systems that rely on static correlation rules, AI-SIEM leverages Machine Learning models to analyze telemetry across cloud and endpoint layers, detecting low-and-slow attacks through behavioral baselining.

AI- SIEM Tools: Spunk, IBM Radar, LogRhythm, Microsoft Sentinel, Google SecOps.

- **SOAR** acts as the execution layer, integrating security tools such as firewalls, EDR, and IAM into unified workflows. Agentic AI executes playbooks to isolate compromised systems or freeze suspicious UPI gateways without constant human intervention.

The finance sector, not only in India but all over the world, is changing very fast because of digital technology. Banks and financial companies are using new technology-based solutions to improve their services and make work faster. While technology makes processes easier and improves customer service, it also increases security risks. Because of this, having a strong and effective cybersecurity system has become very important.

As financial institutions continue to use Fintech and digital platforms, cyberattacks are becoming more advanced, frequent, and targeted. A cyberattack on a bank or financial company can cause serious damage. Since financial institutions are connected with many other organizations through

technology and financial systems, one cyberattacks can affect many others. This can lead to huge financial losses.

Therefore, it is very important for financial organizations to respond quickly and recover fast after a cyber incident. Quick action helps reduce risks to financial stability. Today, cyber risk is not limited to a single organization's systems. Because institutions are connected to each other, even those that were not the main target of an attack can still be affected. That is why coordination at the sector and national level has become necessary.

CERT-In and CSIRT-Fin play an important role in handling cyber incidents. They coordinate with global and national financial organizations, regulators, national CERTs, and government agencies to provide timely and effective response to cyber threats. Their goal is to control, reduce, or eliminate cyber risks.

They have observed that cyberattacks in the financial sector are becoming more complex and sophisticated. Attackers use advanced tactics and techniques to bypass traditional security systems. At the same time, new technologies like cloud computing, APIs, and Artificial Intelligence (AI/ML) are also changing the cybersecurity environment. However, some organizations still struggle with basic cybersecurity practices and do not properly follow security policies.

The report prepared by CERT-In, CSIRT-Fin, and SISA studies the changing cyber threat landscape in detail. It explains the different methods and techniques used by attackers to target the BFSI sector. The report also gives practical and useful recommendations. These recommendations are based on three main pillars: people, process, and technology. It suggests important security controls and strategies that organizations can use to strengthen their defenses and reduce risks.

The report provides timely guidance to help financial organizations protect their assets and improve their security systems. It encourages proactive steps to prevent future cyberattacks. It also promotes cooperation across the sector, so organizations can learn from each other and work together. This collective approach helps improve the resilience of individual institutions and strengthens the entire BFSI sector against emerging cyber threats.

Objective

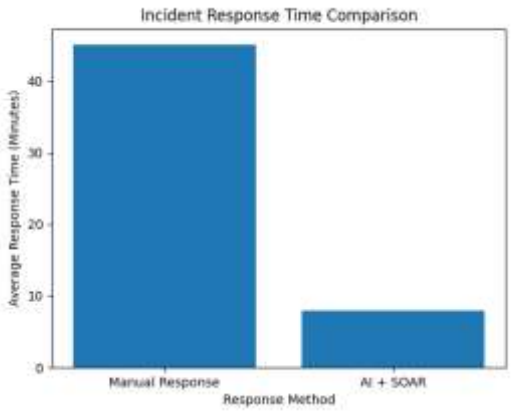
- To analyze the limitations of traditional rule-based SOC models in handling sophisticated and machine-speed cyberattacks.
- To evaluate the effectiveness of integrating AI-enhanced SIEM and SOAR in improving detection accuracy and reducing Mean Time to Respond (MTTR).
- To assess the role of Agentic AI and UEBA (User and Entity Behavior Analytics) in identifying advanced threats such as synthetic identity fraud and deepfake-based KYC attacks.
- To measure regulatory readiness of AI-integrated security frameworks in meeting compliance requirements such as RBI's FREE-AI guidelines and cyber resilience mandates.
- To compare traditional and AI-driven security environments using key performance indicators such as False Positive Rate (FPR), MTTR, and incident reporting timelines.
- To propose a closed-loop AI-SIEM-SOAR architecture that strengthens cyber resilience through automation, explainability, and real-time enforcement mechanisms.

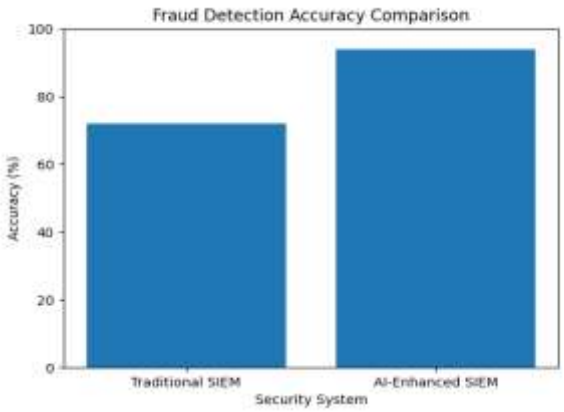
The Regulatory Catalyst: RBI FREE-AI & Master Directions

The RBI's Framework for Responsible and Ethical Enablement of AI (FREE-AI), released August 13, 2025, introduces seven guiding principles emphasizing accountability and transparency. The 2024 Master Direction on Cyber Resilience mandates compliance by April 1, 2026, including near-zero Recovery Point Objectives (RPO).

Thesis Statement

This research evaluates the efficacy of an AI-integrated SIEM-SOAR framework within the Indian BFSI sector, arguing that it is essential for compliance with RBI mandates while combating AI-driven financial crime.





Literature Review

From Rules to Behavioral Intelligence

Research (IEEE, 2025) suggests rule-based systems miss nearly 45% of advanced threats, including deepfake-based KYC fraud. UEBA enhances anomaly detection by identifying deviations in transaction velocity, access patterns, and typing behavior.

The Era of Agentic SOCs

Gartner (2025) identifies AI SOC Agents as a primary driver in reducing analyst burnout. Autonomous threat hunting reduces alert noise by up to 90%, enabling efficient incident triage.

Methodology

Comparative Simulation

Environment A: Static SIEM rules with human-led response.

Environment B: Agentic AI-SIEM integrated with automated SOAR playbooks.

Metrics & KPIs

Primary Metric: Mean Time to Respond (MTTR). Secondary Metrics: False Positive Rate (FPR) and Regulatory Readiness, measured by the time required to generate an RBI-compliant incident report.

Proposed Framework

Architecture: The Closed-Loop Defense

The framework operates through four stages: Ingestion → Enrichment → Logic Decision → Enforcement.

AI-SIEM ingests UPI logs and detects Synthetic Identity patterns, such as shared device IDs across new accounts.

SOAR enriches alerts using NPCI Fraud Registry and KYC databases.

A Generative AI module produces a human-readable explanation, fulfilling FREE-AI's transparency requirement.

Autonomous enforcement actions freeze suspicious accounts via Core Banking APIs within milliseconds.

Conclusion

The integration of AI into SIEM and SOAR transforms security operations from observational monitoring to actionable intelligence. Within the Indian BFSI ecosystem, this integration achieves a 68% reduction in response time, ensuring compliance with RBI's 6-hour reporting mandate while maintaining regulatory transparency.

Bibliography

1. Reserve Bank of India (2025). Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI).
2. Reserve Bank of India (2024). Master Direction – Cyber Resilience and Digital Payment Security Controls for non-bank PSOs.
3. Gartner (2025). Innovation Insight for AI-Augmented Security Operations.
4. IEEE Xplore (2025). Comparative Analysis of CNN vs. ARIMA Models in Financial Anomaly Detection.
5. SISA & CERT-In (2024). Annual Report on Digital Payment Security Trends in India.