Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Integrated SOC Framework for Real Time Threat Monitoring

Arya Sanju
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Diya R
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Keerthana B K
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Ms. Aswathi V
Assistant Professor
Department of Computer Science
Vimal Jyothi Engineering College
Chemperi, Kannur

***Abstract*—The project titledIntegrated Security Operations Center Framework for Real-Time Cyber Threat Monitoring proposes a centralized cybersecurity monitoring system designed to detect, analyze, and respond to network-based threats in real time. As cyber attacks targeting personal and organizational systems continue to increase, traditional security mechanisms often fail to provide continuous monitoring and timely response. The proposed framework addresses this limitation by integrating real-time monitoring, behavioral analysis, rule-based threat detection, and centralized logging within a unified system. The system continuously monitors network activities and collects telemetry data from endpoint systems, including running processes and active network connections. This data is analyzed using behavior-based and rule-based detection techniques to identify anomalies such as unusual connection patterns, port scanning attempts, and suspicious process activities. Upon detecting potential threats, the system generates alerts and records events in a centralized database. These logs support The cloud-based SOC server processes data and provides a real- time dashboard for monitoring security events and alerts. This centralized system enhances threat visibility, improves incident response, and supports efficient analysis, offering a scalable and user-friendly solution for cybersecurity monitoring.auditing, incident analysis, and investigation, enabling administrators to trace malicious activities and respond effectively. The cloud-based SOC server processes data and provides real-time monitoring, improving threat detection and response in a scalable and efficient manner.**

***Index Terms*—Operating System Security, Behavioral Analysis, Zero-Day Defense, Local AI, Privacy-Preserving Computing, Malware Detection, Proactive Defense**

I. INTRODUCTION

The rapid expansion of digital infrastructures and online services has significantly transformed the cybersecurity landscape, necessitating advanced approaches to monitoring and threat management. Modern organizations increasingly rely on interconnected systems and cloud-based platforms, which, while enhancing operational efficiency, also expose them to a wide range of sophisticated cyber threats. Attacks such as malware infections, unauthorized access, and data breaches have evolved in complexity, often bypassing traditional security mechanisms. Conventional security monitoring solutions, which primarily depend on static rules and signature-based detection, are often insufficient to identify and mitigate advanced, evolving threats in real time.

To address these challenges, the project titled “Integrated Security Operations Center (SOC) Framework” proposes a comprehensive cybersecurity monitoring and incident response system aimed at strengthening organizational security infrastructure. The framework is designed to provide continuous monitoring of system and network activities, enabling the timely detection of suspicious behavior and efficient response to potential security incidents.

The proposed system incorporates behavioral analysis and machine learning techniques to enhance threat detection capabilities. By analyzing system logs and user behavior patterns, the framework can identify anomalies that may indicate malicious activities. Unlike traditional approaches, this method enables the detection of previously unknown threats by focusing on deviations from normal behavior. The system is implemented using Python for automation and threat analysis, while SQL-based databases are utilized to store logs, alerts, and system data for further analysis and reporting.

The architecture of the framework integrates both hardware and software components to simulate a real-world SOC environment. Continuous collection and processing of system and network logs allow for real-time analysis and incident identification. Upon detecting suspicious activity, the system automatically generates alerts and initiates preliminary response actions to minimize potential damage and contain threats at an early stage.

Furthermore, the framework includes a real-time monitor-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

ing dashboard that provides security administrators with a comprehensive view of system status, detected alerts, and ongoing threat activities. This visualization enables efficient tracking of incidents, supports informed decision-making, and enhances the overall incident response process. The integration of automated alerting and response mechanisms significantly improves the efficiency and accuracy of threat detection and management.

Through systematic testing and evaluation, the proposed SOC framework demonstrates its effectiveness in identifying anomalies, generating timely alerts, and supporting proactive incident response. The system offers a scalable, efficient, and cost-effective solution for modern cybersecurity monitoring, addressing the limitations of traditional approaches and contributing to improved security management in organizational environments.

II. Overview of SOC

The Integrated Security Operations Center (SOC) Framework is a proactive cybersecurity solution designed to strengthen threat detection and incident response in modern digital environments. Unlike traditional security systems that rely on reactive and signature-based methods, this framework utilizes **behavioral analysis and machine learning** to identify anomalies and detect potential cyber threats in real time.

The system continuously monitors system and network activities, collecting and analyzing logs to detect suspicious behavior. It is implemented using Python for automation and threat analysis, while SQL databases are used for storing logs, alerts, and system data for further investigation. Upon identifying a threat, the framework generates alerts and performs preliminary response actions to reduce potential impact.

Additionally, a real-time monitoring dashboard provides security administrators with a clear visualization of alerts, system status, and ongoing threat activity, enabling efficient tracking and informed decision-making. Overall, the framework offers a scalable, efficient, and cost-effective solution for proactive cybersecurity monitoring and improved incident management.

A. *KEY FEATURES*

1) **Automated Log Monitoring and Analysis:**
   - Continuously collects and analyzes system and network logs to identify suspicious activities in real time.
   - Reduces dependency on manual log inspection by automating threat detection using predefined rules and analysis techniques.
2) **Real-Time Threat Detection Engine:**
   - Detects abnormal patterns in user behavior and network activity that may indicate potential cyber threats.
   - Enables early identification of attacks such as unauthorized access, brute-force attempts, and malware activity.
3) **Proactive Alert and Response System:**
   - Automatically generates alerts when suspicious activities are detected.
   - Initiates preliminary response actions to minimize the impact of potential threats and support faster incident handling.
4) **Centralized Log Management (SQL Database):**
   - Stores logs, alerts, and system data in a structured SQL database for easy access and analysis.
   - Supports historical data tracking, reporting, and forensic investigation.
5) **Real-Time Monitoring Dashboard:**
   - Provides a web-based interface for visualizing system status, alerts, and network activities.
   - Enables security administrators to monitor events, track incidents, and make informed decisions efficiently.
6) **Scalable and Modular Architecture:**
   - Designed to support multiple systems, virtual machines, and network environments.
   - Allows easy integration of additional security modules and future enhancements such as machine learning-based detection.

The proposed Integrated Security Operations Center (SOC) Framework incorporates several core modules to ensure effective threat detection, real-time monitoring, and efficient incident response.

III. PROPOSED SYSTEM AND DESIGN

The proposed system, Integrated Security Operations Center Framework provides continu- ous monitoring of network activities and detects cyber threats in real time. Due to the increasing number of cyber attacks and security breaches, organizations require an efficient system to monitor logs, identify suspicious activities, and respond quickly to security incidents. Unlike traditional security methods that rely on manual log inspection, the system automates log collection, threat detection, and alert generation. It collects security logs from servers and network devices and analyzes them to detect abnormal or malicious activities. When a threat is detected, the system generates alerts and notifies administrators through a monitoring dashboard. The system architecture includes advanced features across six major functional domains:

- **Log Collection Module:**Collects logs and security-related data from servers and network devices.
- **Threat Detection Module:** Analyzes collected logs to identify suspicious behavior,malware activity, or unauthorized access attempts.
- **Alert Generation Module:** Generates alerts when abnormal activities or security threats are detected.
- **Monitoring Dashboard:** A web-based dashboard that allows administrators to view system status, alerts, and log information in real time.

monitoring interface is provided through a web dashboard. The collected data and alerts are stored in an

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

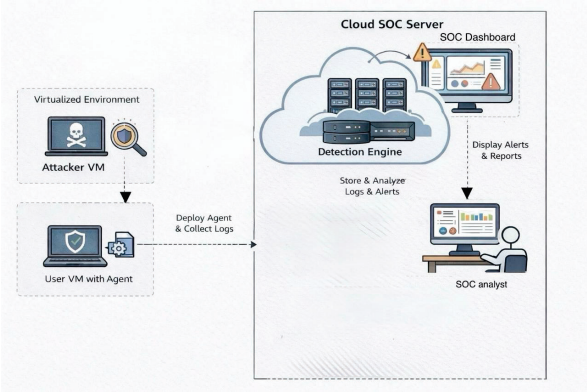

Fig. 1. SOC Server Workflow

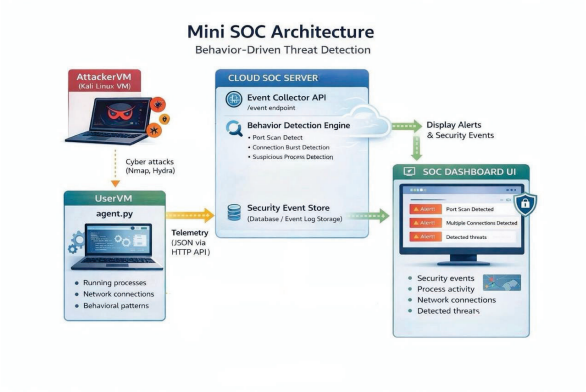

Fig. 2. Architecture Diagram

SQL database to allow easy retrieval and analysis. The architecture follows a modular design that includes log collection, threat detection, alert management, and monitoring modules. This modular structure allows easier system maintenance, testing, and future scalability. The automated workflow enables continuous monitoring of network activities and ensures that administrators are informed about security threats without delay.

A. *SYSTEM ARCHITECTURE*

The Integrated SOC Framework follows a layered architecture designed for real-time monitoring and efficient threat detection.The data collection layer continuously gathers system and network logs from servers and virtual machines. This data is forwarded to the analysis layer, where logs are processed in real time to detect anomalies, suspicious behavior, and potential cyber threats. When an issue is detected, the system generates alerts and initiates basic response actions.

All logs and alerts are stored in a centralized SQL database, which supports analysis and reporting. The presentation layer consists of a web-based SOC dashboard that provides real-time visualization of alerts, system status, and network activity for security administrators.Overall, this architecture ensures continuous monitoring, fast threat detection, and effective incident response in a scalable and efficient manner.

B. *SYSTEM DESIGN*

The system design of the Integrated SOC Framework is illustrated using Use Case and Data Flow Diagrams to represent system interactions and data movement.

The Use Case Diagram describes the interaction between the SOC Analyst (User) and the SOC system. The user performs actions such as monitoring alerts, viewing system logs, and analyzing network activity through the SOC dashboard. The system processes these requests and provides real-time security insights while ensuring continuous monitoring and automated threat detection.

The Data Flow Diagram (DFD) represents the flow of security data within the system. At the highest level, the main components include the User, SOC System, and Data Storage (SQL Database).

- Input:System and network logs are collected from servers and virtual machines.
- Process: The SOC system analyzes logs in real time to detect anomalies and suspicious activities.
- Output: Detected threats and system alerts are displayed on the dashboard and stored in the database for further analysis.

The Level 0 DFD shows the SOC system as the central processing unit that manages data collection, analysis, and response generation. It ensures continuous monitoring by processing incoming log data and providing real-time alerts to the user interface.

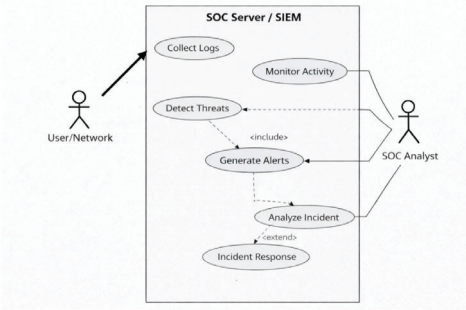

Fig. 3. Use Case Diagram

The Level 0 Data Flow Diagram shows the overall flow of data in the Integrated Custom SOC System, highlighting the interaction between the SOC Analyst, Client Systems, and Management.

- Input: The process starts with Client Systems sending Raw Log Data / Authentication Logs to the SOC system for monitoring.
- Process: The Integrated Custom SOC System analyzes the incoming data, detects incidents, and manages security events. The SOC Analyst can send Incident Review Requests to further investigate issues.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- Feedback: The system generates Alerts, Incident Summaries, and Severity Reports for the SOC Analyst, and provides High-Level Incident Reports to Management for decision-making.

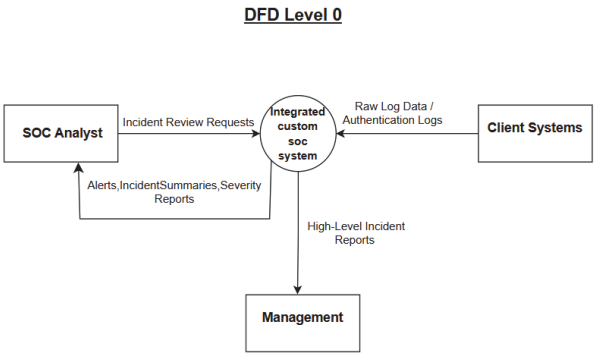

Fig. 4. Data Flow Diagram (Level 0)

The Level 1 Data Flow Diagram provides a detailed view of the Integrated Custom SOC System, showing how internal processes and data stores interact with external entities.

- Log Management: The process begins with Client Systems sending Raw Authentication Logs to Log Collection Ingestion, where data is normalized and stored in Log Storage.
- Threat Detection: The normalized logs are forwarded to Threat Detection Correlation, which analyzes structured log events and generates Detection Results and Security Alerts, stored in the Incident Database.
- Incident Handling: The SOC Analyst interacts with Incident Analysis Response by sending Incident Review Requests. The system processes alerts and provides Incident Summaries Severity back to the analyst.
- SThreat Intelligence: Confirmed incident data is passed to Threat Intelligence Knowledge Mapping, which updates the Threat Knowledge Base.
- Management Reporting: The system generates High-Level Incident Reports from the threat intelligence module and sends them to Management for strategic decisions.

IV. IMPLEMENTATION

The development of the Cloud-Based SOC Monitoring System was carried out in a structured approach to ensure efficient log collection, threat detection, and real-time security monitoring.

A. *MODULES*

Phase 1: System Design and Architecture This phase focused on designing the overall architecture, including the Virtualized Environment and the Cloud SOC Server. It defined how attacker simulations, user systems, and cloud-based detection components interact. ***Phase 2: Data Collection and Agent Deployment*** In this phase, agents were deployed on the

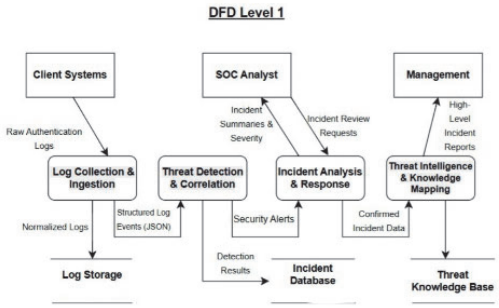

Fig. 5. .Data Flow Diagram (Level 1)

User VM to collect system logs and activity data. The system ensures continuous monitoring by forwarding collected logs from the virtual environment to the cloud server.

Phase 3:Detection Engine Implementation The Detection Engine was developed within the cloud SOC server to store and analyze logs and alerts. It processes incoming data to identify suspicious activities and generate security alerts.

Phase 4:Monitoring and Reporting The final phase focused on the SOC Dashboard, where alerts and reports are displayed to the SOC Analyst. This enables real-time monitoring, incident analysis, and informed decision-making based on detected threats.

B. *TOOLS AND TECHNIQUES*

The development of the Cloud-Based SOC Monitoring System utilizes a combination of efficient programming tools and data analysis technologies to ensure reliable log monitoring, threat detection, and reporting.

- *Programming Languages*: A multi-language approach was used to handle different system components. Python was primarily used for implementing log processing, threat detection logic, and backend services due to its strong support for data analysis and automation. Shell Scripting was used for agent deployment and log collection tasks within virtual machines. Additionally, JavaScript (or similar) can be used for developing interactive SOC dashboards.
- *Frameworks and Libraries*: The system leverages log analysis and detection techniques within the Detection Engine to process incoming data and identify threats. Visualization tools and web technologies are used to build the SOC Dashboard, enabling real-time monitoring of alerts and reports. Virtualization technologies are used to simulate attacker and user environments for testing and analysis.
- *Database and Storage*: A centralized database system (such as MongoDB or similar) is used to store logs, alerts, and incident data. This ensures efficient retrieval, analysis, and long-term storage of security events.
- *Development and Monitoring Tools*: Development was carried out using standard IDEs such as Visual Studio

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Code and Python-based environments. Virtual machines (VMs) were used to simulate attacker and user systems. The system was tested across environments like Windows and Linux (Ubuntu) to ensure compatibility. Monitoring is performed through the SOC dashboard, where analysts can view alerts, analyze incidents, and generate reports in real time.

V. Results and Discussion

The implementation of the Integrated SOC Framework for Real-Time Monitoring successfully achieved its primary objectives of improving threat detection speed, accuracy, and overall security monitoring through automation. The system was validated through performance comparisons and functional testing against traditional manual monitoring approaches.

Functional Testing and Threat Detection

The system demonstrated high efficiency in detecting threats using automated log analysis. In the testing environment, the SOC framework successfully performed the following:

- Faster Detection: The system reduced threat detection time from 60 seconds (manual monitoring) to 20 seconds, enabling quicker identification of potential attacks.
- Improved Accuracy: Detection accuracy increased from 82
- Real-Time Alert Generation: The system generated instant alerts based on log analysis, ensuring timely response to security incidents.

System Performance and Monitoring Efficiency

Performance evaluation confirmed that the system significantly improves monitoring efficiency compared to traditional methods:

- Automated log collection replaces manual inspection, reducing workload.
- Continuous monitoring ensures no security events are missed.
- Centralized data storage enables faster retrieval and analysis of logs.
- Dashboard-based visualization improves system visibility and simplifies incident analysis.

Security Analysis

The proposed SOC framework enhances overall security by:

- Enabling real-time threat detection instead of delayed manual processes
- Providing instant alert generation for quick response
- Supporting centralized log management for better control
- Reducing time required for incident investigation through automation

The proposed SOC framework significantly improves overall security by enabling continuous monitoring and automated threat detection, which strengthens the system's ability to identify and respond to cyber threats effectively. It also enhances performance by reducing detection delays through real-time log analysis, allowing faster identification of potential attacks. The integration of a centralized dashboard provides real-time monitoring, offering instant visibility into system activities and alerts, which supports quick decision-making. Additionally, the framework is scalable and can be extended to monitor multiple systems and network environments as needed. Future enhancements may further improve the system by incorporating machine learning techniques for advanced threat detection and predictive analysis, making the solution more intelligent and adaptive to evolving cybersecurity challenges.

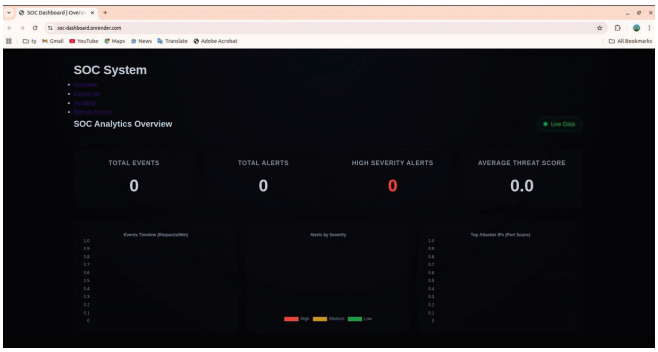

Fig. 6. SOC Dashboard

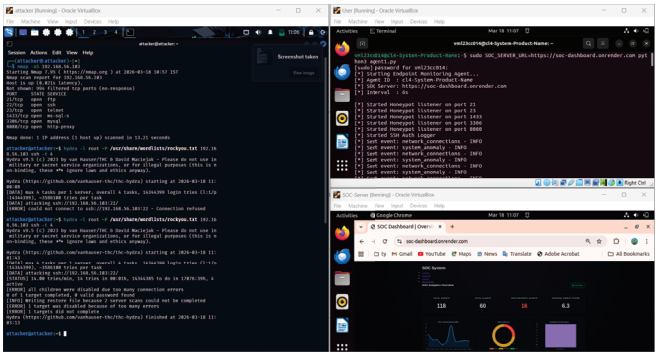

Fig. 7. Working

VI. Conclusion and Future Work

A. *Conclusion*

The Integrated SOC Framework for Real-Time Monitoring provides an effective solution to modern cybersecurity challenges, by replacing traditional manual log monitoring with automated analysis, improving threat detection speed through real-time processing, enhancing detection accuracy using automated techniques, ensuring efficient data handling through centralized log storage, enabling instant alert generation for faster incident response, providing continuous monitoring of system activities, improving visibility through a real-time SOC dashboard, reducing the workload on security analysts, minimizing human errors in monitoring processes, supporting scalability across multiple systems and networks, simplifying incident investigation through dashboard-based analysis, ensuring reliability through the use of standard technologies, strengthening overall cybersecurity through automation and efficiency, and serving as a robust and practical solution for real-time security monitoring.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

B. *Future Work*

Future enhancements will focus on improving the system's intelligence and performance by integrating advanced machine learning techniques for predictive threat detection and anomaly analysis. The framework can also be extended to support cloud-based and distributed environments for monitoring large-scale networks. Additionally, incorporating advanced visualization tools and automated response mechanisms can further reduce incident response time. Future iterations may also explore integration with external threat intelligence platforms and security tools to enhance detection capabilities and provide a more comprehensive cybersecurity solution.

REFERENCES

[1] U. N. A. Perera, S. Rathnayaka, N. Perera, W. Madushanka, and A. N. Senarathne, "The next gen security operation center," in *2021 6th International Conference for Convergence in Technology (I2CT)*. IEEE, 2021, pp. 1–9.

[2] J. Zhang, C. Chen, T. Liu, and H. Chen, "Research on integrated network security operation system for large central enterprises," in *2025 7th International Conference on Natural Language Processing (ICNLP)*. IEEE, 2025, pp. 556–559.

[3] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *Ieee Access*, vol. 8, pp. 227 756–227 779, 2020.

[4] D. Shahjee and N. Ware, "Designing a framework of an integrated network and security operation center: A convergence approach," in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*. IEEE, 2022, pp. 1–4.

[5] D. Shahje and N. Ware, "Integrated network and security operation center: A systematic analysis," *IEEE Access*, vol. 10, pp. 27 881–27 898, 2022.

[6] P. Jacobs, A. Arnab, and B. Irwin, "Classification of security operation centers," in *2013 Information Security for South Africa*. IEEE, 2013, pp. 1–7.

[7] C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy," in *2015 international conference on cyber situational awareness, data analytics and assessment (cybersa)*. IEEE, 2015, pp. 1–10.

[8] S. Schinagl, K. Schoon, and R. Paans, "A framework for designing a security operations centre (soc)," in *2015 48th Hawaii International Conference on System Sciences*. IEEE, 2015, pp. 2253–2262.

[9] M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and H. M. Khater, "Empowering security operation center with artificial intelligence and machine learning—a systematic literature review," *IEEE Access*, vol. 13, pp. 19 162–19 197, 2025.

[10] F. D. János and N. H. P. Dai, "Security concerns towards security operations centers," in *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 2018, pp. 000 273–000 278.