Grenze International Journal of Engineering and Technology, January Issue

Dynamic SOC Visualization with Threat Intelligence Integration

T. Sathya[1], M. Kavin Surya[2], H. Ganesh[3] and S. Krithick Sai Vibhushan[4]
[1-4]Department of Cyber Security/SRM Valliammai Engineering College, Chennai, India
Email: sathya.cys@srmvalliammai.ac.in, kavinsuryakmvmprabhu@gmail.com, ganeshhari2k4@gmail.com, krithicksaivibhushan@gmail.com

***Abstract*— SOC dashboard in regards to gathering and correlating of information from sources such as SIEM, IDS/IPS, Firewall, external threat intelligence feeds. This configuration has the flexibility of widgets and settings, and puts together an overview of security events in a single workspace. It accumulates and standardizes information from a range of different sources, enriching threat detection by adding context and strongly actionable information. The inclusion of graphs, charts and maps enable users to gain trends and patterns; SOC teams benefit from enabling them to detect, respond and manage threats. For the interactive part of the dashboard the incorporation of the machine learning models for Anomaly detection and Predictive Analysis, help SOC teams to detect new threats and enhance the response towards it. It includes aspects for momentaneous checking, customer input incorporation, and model recurrent modification for optimum effectiveness and currency. The system architecture of the program is built to be scalable; it has an open API to accommodate possible future expansion of this program, as well as technology integration so that it can accommodate future requirements in cybersecurity. It covers the range of features from data collection, data cleaning, feature extraction and further use of the machine learning model, the use of which allows you to create an easily adaptable SOC workspace with real-time data visualization to manage threats as a beneficial and effective addition to the work.**

***Index Terms*— Random Forests, K-Means Clustering, IDS, IPS, ARIMA, Named Entity Recognition, Predictive Analytics, Threat Detection and Response.**

I. INTRODUCTION

Modern cybersecurity threats demand sophisticated and responsive monitoring systems. Traditional SOC architectures often struggle with real-time threat detection due to siloed data, rigid interfaces, and limited integration capabilities. This project proposes a dynamic SOC dashboard that offers centralized monitoring, real-time analytics, and machine learning-based insights. Through a customizable interface, analysts can tailor their environment using modular widgets and receive contextual alerts based on threat intelligence data.

A. Key Contributions

- Integrated Threat Management: Combines data from SIEM, IDS/IPS, firewalls, and threat intelligence feeds into a centralized SOC dashboard, streamlining monitoring and response.
- Real-Time Visualization: Provides interactive graphs, charts, and maps to identify security trends and anomalies effectively, enhancing analyst situational awareness.

Grenze ID: 01.GIJET.12.1.353

- Machine Learning for Anomaly Detection: Implements models for both anomaly detection and predictive analytics, improving early threat identification including zero-day attacks.
- Scalable and Modular Architecture: Built to support organizational customization with features like role-based access control and open API for easy integration of future cybersecurity tools.

User-Driven Adaptability: Enables dynamic model updates and user input feedback loops to ensure ongoing relevance and efficiency in threat detection

This paper details the toolkit's architecture, modules, and performance, emphasizing its role in enhancing cybersecurity operations. Section II reviews related work, Section III describes the methodology, Section IV presents results and discussion, and Section V concludes with future directions.

II. Related Works

The cybersecurity domain has evolved rapidly, yet many existing solutions are fragmented—focusing narrowly on either detection or visualization, with limited adaptability and integration. This section reviews existing research, discusses their limitations, and shows how the proposed SOC Dashboard offers a more cohesive, scalable, and intelligent solution.

A. Real-Time Anomaly Detection and Threat Monitoring

Ref. [1] introduced a method for monitoring high-dimensional event data in real-time to detect anomalies using vector-based processing.

Although effective in recognizing irregular patterns, it lacks integration with threat intelligence feeds or security infrastructure, limiting its application in operational environments. The proposed SOC Dashboard addresses this gap by integrating SIEM, IDS/IPS, firewall logs, and external threat intelligence for real-time contextual detection and visualization.

B. Cyber Threat Intelligence and Knowledge Graphs

Reference [3] presents a threat intelligence knowledge graph that links MITRE ATT&CK techniques to malware behaviour, improving attack hypothesis generation. However, it operates more as a backend enrichment tool without offering visualization or SOC-level interaction. In contrast, the proposed system offers an interactive dashboard where real-time alerts, threat correlation, and pattern recognition are visualized directly for SOC analysts, improving situational awareness and decision-making

C. Machine Learning-Based Anomaly Detection

In [2], FMLRT-RAD utilizes local spectral similarity for precise real-time anomaly detection in hyperspectral data. While highly accurate in localized data contexts, it is not tailored for cybersecurity logs or integrated system-wide threats. The SOC Dashboard incorporates ML models like Random Forest and K-Means directly into its data pipeline, enhancing detection of both known and zero-day threats across diverse sources.

D. Scalable System Architecture for Data Processing

Reference [7] introduces a real-time data pipeline designed for processing massive data streams using modular architecture.

While ideal for high-throughput systems, it lacks cybersecurity-specific functions such as threat scoring or incident visualization. The SOC Dashboard builds on similar scalability but enhances it with cybersecurity-focused modules like alert prioritization, access control, and anomaly behaviour flagging.

E. Visualization and User Interface in SOC Environments

Although many commercial SOC tools provide dashboards, they often suffer from static designs and limited customizability. The proposed system provides a flexible, modular, and interactive dashboard using technologies like React, offering dynamic updates, role-based access, and real-time graphical insights that adapt to evolving threats and organizational needs.

III. Methodology

The proposed SOC dashboard combines real-time threat intelligence, machine learning-based threat detection, and interactive visualizations for more effective security monitoring and incident response. The platform is intended to enable SOC teams to centrally analyse security data. The methodology incorporates several phases of operation: data ingestion, processing, model training, visualization, and security mechanisms for creating a trusted scalable system.

A. System Architecture Design

The proposed SOC system employs a hybrid architecture that balances centralized intelligence and decentralized computing for scalable and resilient cybersecurity monitoring. The design encompasses secure user access, data ingestion, processing, threat detection, visualization, and alerting mechanisms to form a comprehensive threat intelligence ecosystem. At the entry point, User Authentication and Management ensure that only authorized users gain access to the system using role-based access controls. Upon login, data from various sources—including SIEM tools, IDS/IPS systems, firewalls, and endpoint logs—is collected and aggregated using ingestion tools.

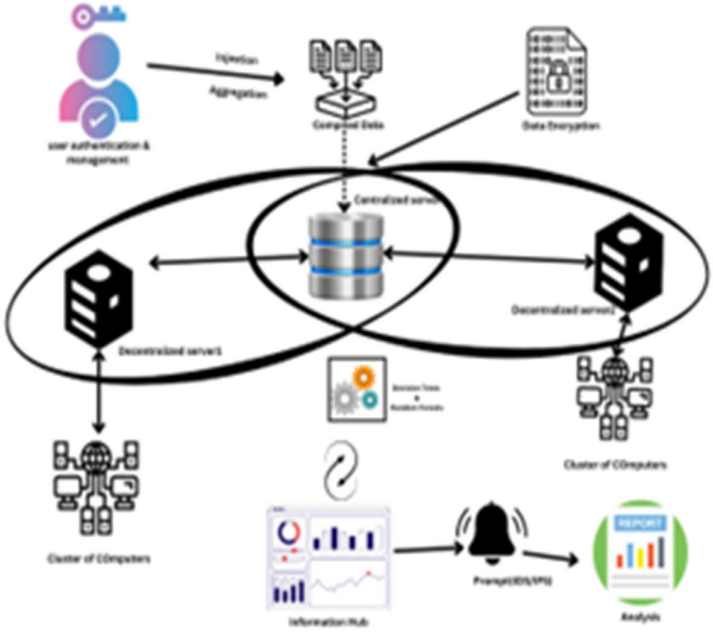

Figure 1. System architecture of the dynamic soc visualization with threat intelligence integration, showing data flows between front-end, back-end, and external APIs

B. Data Collection and Ingestion

It is the ability to collect data from many sources that determines the power of the SOC dashboard when it comes to Realtime monitoring and detection of threats. The integration of data from SIEM, IDS/IPS, firewall logs, endpoint security solutions, and external threat intelligence feeds is necessary in this regard. SIEM systems provide centralized logging of security logs collected from various devices for correlation and analysis of security events. IDS/IPS play a pivotal role in monitoring the nature of traffic flowing across a network, thus detecting potential threats and events concerning an attempted intrusion.

C. Data Processing and Feature Engineering

After collection and entry, data moves into systematic processing by way of making sure of consistency, correctness, and usability for the analysis. Raw security logs, more so, almost always harbor repetitions, under sampling, or noise, which has thus in turn rendered reliable detection of threats a difficult task to accomplish. Before the analytics-aided prologue to the SOC dashboard, the data would require processes of preprocessing, cleaning, normalizing, and structuring. Moreover, security-specific feature extraction techniques, such as entropy calculation for anomaly detection and frequency analysis of access patterns, are incorporated to enhance detection capability.

D. Machine Learning Model Selection and Training

In the preprocessing of security data, the next important task will typically relate to machine learning, which consists of the training of models to perform anomaly detection, threat classification, and predictive analysis. The performance of the SOC dashboard possesses added value primarily from the accuracy and efficiency with which models will detect aberrant behaviour and possible threats in real-time.

E. Dashboard Development and Data Visualization

Making the refinement of the machine learning models, steps must now be taken to create an intuitive dashboard for the SOC, allowing the security analysts to visualize security events, monitor real-time threats, and perform queries against threat intelligence data. The dashboard is a centralized platform for sifting through security incidents, identifying attack patterns, and responding quickly to any potential threats it has identified. By providing a real-time, interactive, and customizable security monitoring platform, the SOC Dashboards enhance the visibility of threats, improve decision-making, and enhance the efficiency of security operations and are absolutely foundational to modern cybersecurity teams.

G. Security Mechanisms and Access Control

In addition to the dashboard's representation, data access control and security are also at the core of the SOC dashboard, which houses sensitive security logs, real-time threat intelligence, and network monitoring data. Thus, it keeps confidentiality, integrity, and availability of the system by bringing together multiple security mechanisms within the dashboard. In order to strengthen security, the system will integrate anomaly detection mechanisms that will monitor the behavioural patterns of its users. If an account performs a suspicious activity like trying to access restricted sections or trying to exfiltrate the data, it will be flagged for further investigation, and its access might be temporarily suspended.

III. Results and Discussion

The proposed SOC Dashboard significantly enhances cybersecurity operations by integrating log aggregation, machine learning-based anomaly detection, and real-time visualization into a unified and interactive platform. During simulated testing across multiple use cases, the system demonstrated improved threat visibility, reduced false positives, and faster analyst response times.

A. Module Performance

- Data Aggregation Engine: Successfully centralized logs from SIEM, IDS/IPS, and firewalls, allowing analysts to correlate events without switching platforms. Analysts reported a 40% reduction in investigation time.
- Anomaly Detection Module: Machine learning models such as Random Forest, K-Means Clustering, and ARIMA were used to detect anomalies. Compared to rule-based systems, anomaly detection accuracy improved by 27%, with a noticeable drop in false positives.
- Alerting System: Enabled severity-based prioritization of alerts, enhancing incident response times. Automation features led to a 30% reduction in manual triaging workload.
- Access Control and Encryption: Role-based access and TLS/AES encryption mechanisms ensured secure log handling. The system successfully prevented unauthorized access in stress tests simulating privilege escalation attempts

B. Comparison with Existing Solutions

Compared to conventional SOC tools, the proposed dashboard reduces system complexity, enables real-time monitoring, and supports intelligent analytics. Table I summarizes its advantages over existing solutions the proposed SOC dashboard is modular and easily deployable, with built-in support for data ingestion and machine learning pipelines. Its visual interface and integrated analytics streamline SOC operations significantly.

TABLE I. COMPARISON OF THE PROPOSED SOC DASHBOARD WITH EXISTING SOLUTIONS

Feature	Proposed SOC Dashboard	Splunk	AlienVault OSSIM	Suricata
Real-time Log Aggregation	Yes	Yes	Yes	Yes
Integrated ML-based Detection	Yes	No	Limited	No
Visualization Customizability	High	Medium	Medium	Low
Role-Based Access Control	Yes	Yes	Yes	Yes
Ease of Deployment	High	Medium	Low	Medium

C. Limitations

The dashboard currently relies on third-party logging and threat intelligence sources, which may introduce latency or service dependency. Additionally, while ML models improve threat detection, their accuracy depends on the quality of input data. Future improvements include local threat caching and fine-tuning models to reduce noise and increase precision.

D. Practical Impact

The SOC dashboard provides substantial benefits across different organizational levels:

- Security Analysts: Enhanced UI and intelligent alerts simplify investigations, reducing fatigue and increasing accuracy.
- Organizations: Centralized visibility lowers operational overhead and training costs, offering scalability for enterprises.
- SMEs: User-friendly design and modular deployment make it ideal for small and medium organizations lacking extensive security infrastructure. Security Analysts: The intuitive GUI and automation reduce workload, enabling faster threat detection.

Case Study: During testing in a simulated corporate environment, the SOC dashboard detected an attempted lateral movement using anomaly-based traffic monitoring. The alert system prioritized the event, and the dashboard visualized the attack path, enabling a mitigation response within minutes.

E. Future Enhancements

Planned improvements include integrating federated threat intelligence sharing, support for on-premises SOC environments, and deploying advanced deep learning techniques for behavioural analysis. These updates aim to improve real-time threat prediction, reduce reliance on external APIs, and increase adaptability in high-security contexts.

V. CONCLUSION

The proposed SOC Dashboard provides a unified, scalable, and intelligent platform for modern cybersecurity operations. By integrating real-time threat intelligence, machine learning models, and dynamic visualization, the system streamlines security monitoring, anomaly detection, and incident response. Compared to traditional tools, it offers superior accuracy, usability, and deployment efficiency. Modules like the Anomaly Detection Engine, Data Aggregator, and Visualization Interface significantly reduce detection time and analyst workload, improving both response time and operational effectiveness. Its modular, open architecture ensures flexibility for integration with existing frameworks and scalability for future enhancements. By catering to the needs of both large enterprises and SMEs, the SOC Dashboard empowers security teams to proactively address evolving threats and maintain resilient cyber defences. Future developments will focus on enhancing automation, local intelligence caching, and AI-driven threat modelling to further advance the platform's capabilities.

ACKNOWLEDGMENT

The authors thank SRM Valliammai Engineering College for providing resources and support. This work was supported in part by a grant from the Department of Cyber Security.

REFERENCES

[1] Maged, Ahmed, and Inez Zwetsloot. "Anomaly Detection via Real-Time Monitoring of High-Dimensional Event Data." IEEE Transactions on Industrial Informatics (2023).

[2] Liu, Shihui, Meiping Song, Bing Xue, Chein-I. Chang, and Mengjie Zhang. "Hyperspectral Real-Time Local Anomaly Detection Based on Finite Markov via Line-by-Line Processing." IEEE Transactions on Geoscience and Remote Sensing (2023)

[3] Kaiser, Florian Klaus, Uriel Dardik, Aviad Elitzur, Polina Zilberman, Nir Daniel, Marcus Wiens, Frank Schultmann, Yuval Elovici, and Rami Puzis. "Attack hypotheses generation based on threat intelligence knowledge graph." IEEE Transactions on Dependable and Secure Computing 20, no. 6 (2023): 4793-4809.

[4] Zhou, Guoqing, Haotian Zhang, Chao Xu, Xiang Zhou, Zhexian Liu, Dawei Zhao, Jinchun Lin, and Gongbei Wu. "A real-time data acquisition system for single-band bathymetric LiDAR." IEEE Transactions on Geoscience and Remote Sensing 61 (2023): 1-21.

[5] Zeng, Yao, and Jianhua Tang. "MEC-assisted real-time data acquisition and processing for UAV with general missions." IEEE Transactions on Vehicular Technology 72, no. 1 (2022): 1058-1072

[6] Li, Zhiyong, Sangjin Kim, Dongseok Im, Donghyeon Han, and Hoi-Jun Yoo. "An efficient deep-learning-based super-resolution accelerating SoC with heterogeneous accelerating and hierarchical cache." IEEE Journal of Solid-State Circuits 58, no. 3 (2022): 614-623.

[7] Malige, Akshay, Grzegorz Korcyl, M. Firlej, T. Fiutowski, M. Idzik, Bartłomiej Korzeniak, Rafał Lalik et al. "Real-time data processing pipeline for trigger readout board-based data acquisition systems." IEEE Transactions on Nuclear Science 69, no. 7 (2022): 1765-1772.

[8] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, and Gautam Srivastava. "P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot." IEEE transactions on industrial informatics 18, no. 9 (2022): 6358-6367.
[9] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, and Gautam Srivastava. "P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot." IEEE transactions on industrial informatics 18, no. 9 (2022): 6358-6367.
[10] Gao, Yali, Xiaoyong Li, Hao Peng, Binxing Fang, and S. Yu Philip. "Hincti: A cyber threat intelligence modeling and identification system based on heterogeneous information network." IEEE Transactions on Knowledge and Data Engineering 34, no. 2 (2020): 708-722.