Volume 9, Issue 12, December – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

An Integrated Soc Tool

[1]Archana PS
Department. of Cse Sree Narayana Gurukulam
College of Engineering Ernakulam, India

[2]Christan Jose
Department. of Cse Sree Narayana Gurukulam
College of Engineering Ernakulam, India

[3]Albin Biju
Department. of Cse Sree Narayana Gurukulam
College of Engineering Ernakulam, India

[4]Aromal Dileep
Department. of Cse Sree Narayana Gurukulam
College of Engineering Ernakulam, India

[5]Aswanth G Pillai
Department. of Cse Sree Narayana Gurukulam
College of Engineering Ernakulam, India

Abstract:- This paper reviews current SOC tools to identify the deficiencies encountered as well as analyses the emerging requirements of modern SOC environments. It means the use of automation, machine learning and visualization in SOC environ- ments is very important in order to increase speed and efficiency. This survey compiles the recent advances in SOC architecture, automation interfaces and real-time data processing. After going through the paper, the following significant observations can be made: Firstly, there is a lack of coordination in linking numerous tools collectively; secondly, when it comes to the enhancement of the detection rate , the engagement of the machine learning algorithm; and thirdly, rising automation trends that help to minimize a huge amount of manual work. Challenges that have kept SOC from gaining widespread acceptance are discussed including cost, technical expertise, and privacy issues, followed by strategies of how an improved SOC tool can be created to overcome the drawbacks of existing solutions.

I. INTRODUCTION

The Security Operations Center (SOC) has a vital role to play keeping an organization secure, with the evolving threat landscape it is imperative that security operations staff are always one step ahead and ready for whatever attack comes their way. Summary, Networks are monitored for suspicious activity and detection should respond to incidents when they arise; Security Operation Center (SOCs) that view all the outputs of these detections on network activities. Yet the sophistication of cyberattacks and sheer amount of data from different sources has increasingly exposed traditional SOC tools as fundamentally inadequate. Typically each of these tools work in general-purpose silos, and yet what is really needed for effective security are specialized best-of-breed solutions.

Many of the current SOC tools such as Security Information and Event Management (SIEM) systems, as well as newly introduced to market solutions like Security Orchestration Automation Response (SOAR) platforms lack scalability, are slow when it comes down for the response time they offer/they take in detecting threats or fall under heavy manual interven- tion. The relate to data subjectedSplitOptions.minimum with the smallest value divided then replicated.

As cyber threats become more sophisticated, there is an increasing need for SOC tools that can seamlessly integrate multiple security functions into a unified platform, automating routine tasks and providing real-time visualization of data. This paper surveys the current state of SOC tools, highlights the challenges faced by modern SOCs, and explores how emerging technologies such as machine learning, automation, and advanced analytics can address these challenges.

➢ *In Particular, the Paper will focus on the Following:*

- The integration of disparate SOC tools to enhance threat detection and response capabilities.
- The role of machine learning in improving anomaly detection and reducing false positives.
- The importance of automation in streamlining SOC op- erations and alleviating the burden on security personnel.
- The use of real-time dashboards and visualization tools to improve situational awareness for SOC analysts.
- The goal is to propose an integrated SOC tool that addresses the limitations of existing solutions while meeting the evolving needs of modern cybersecurity operations.

II. METHODOLOGY

A. Conceptual Model for Security in Next Generation Network

The proposed network security tool utilizes a comprehensive methodology combining several industry-standard frameworks and practices. Risk assessment is performed using the STRIDE and PASTA models to identify threats and simulate attack vectors. In the Secure Development Lifecycle (SDLC), both static and dynamic code analysis are employed alongside secure coding practices to ensure code integrity. Application security is enhanced with Role-Based Access Control (RBAC) for authorization and Advanced Encryption Standard (AES) for

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

data encryption. The Intrusion Detection and Prevention System (IDPS) integrates signature-based and anomaly-based detection to monitor for known and emerging threats. A layered security approach includes Multi-Factor Authentica- tion (MFA) and Data Loss Prevention (DLP) mechanisms to safeguard access and prevent data exfiltration. The tool is built upon Zero Trust architecture principles, assuming no entity is trusted by default, and incorporates Privacy by Design through Privacy Enhancing Technologies (PETs) and OAuth 2.0 for secure, token-based authorization.

B. Computer Network Security Evaluation Method Based on GABP Model

The GABP model combines a Genetic Algorithm (GA) with a Bayesian Network (BN) to enhance computer network security. The GA optimizes network security parameters, such as firewall settings and access controls, by iteratively evolving solutions that improve security effectiveness. Simultaneously, the BN assesses the probabilistic dependencies between net- work components, allowing for the prediction of vulnerabil- ities and potential threats. By integrating GA's optimization with BN's probabilistic analysis, the GABP model provides a comprehensive approach to dynamically optimizing network defenses and proactively identifying emerging security risks.

C. New Network Security Architecture Based on SDN/NFV Technology

The integration of Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) creates a flexible and programmable security architecture. SDN offers centralized control and dynamic policy enforcement, allowing for real- time management of network traffic and security policies. In parallel, NFV virtualizes key network functions such as firewalls and intrusion detection systems, enabling scalable, on-demand deployment of security solutions. Together, SDN and NFV provide an agile and adaptable security framework, capable of addressing evolving network security challenges with enhanced flexibility and scalability.

D. Security Operations Center: A Systematic Study and Open Challenges

This study examines the structure, functions, and processes of Security Operations Centers (SOCs) through a compre- hensive literature review and analysis of case studies. Itaims to identify key components essential for effective SOC operations, focusing on threat detection methodologies and tools, incident response processes, and continuous monitoring strategies. By integrating insights from both literature and case studies, this research provides a comprehensive understanding of SOC capabilities and their critical role in enhancing orga- nizational security.

E. Security Issues and Challenges on Wireless Sensor Net- works

This study conducts a comprehensive literature review to identify and analyze security threats, vulnerabilities, and chal- lenges in Wireless Sensor Networks (WSNs). A systematic search of academic databases, including IEEE Xplore and Google Scholar, was performed using keywords related to WSN security. Peer-reviewed articles published in the last decade were selected to ensure relevance. Key information on data confidentiality, integrity, authentication, and attack mitigation was extracted from the literature. A qualitative analysis was then conducted to identify common themes and evaluate the effectiveness of proposed security measures. The synthesis of findings highlights existing research gaps and suggests directions for future work in WSN security.

F. Next-Generation SIEM: From Monitoring to Detection and Response

This study focuses on the integration of Machine Learn- ing techniques to enhance network security through anomaly detection. Artificial Intelligence (AI) is employed to analyze network behaviors, utilizing various algorithms to process and evaluate extensive data generated by network activities in real time. Behavioral Analysis involves monitoring deviations from established patterns of normal network behavior, allowing the system to flag anomalies that may indicate potential threats. By employing statistical analysis and pattern recognition techniques, the accuracy of threat detection is significantly improved.

G. RESTful Web Services: Principles and Best Practices

This study implements a stateless architecture where each API call is independent, simplifying scaling and improving fault tolerance by allowing services to handle requests in parallel without relying on server-side sessions. Scalability is achieved through horizontal scaling, adding more instances to manage higher volumes of API requests. Load balancing techniques are employed to evenly distribute traffic across servers, ensuring optimal resource utilization and preventing performance degradation during peak loads.

H. Building a SOAR Platform: Design Considerations and Technical Challenges

This study utilizes a modular architecture, enabling flexibil- ity and easier scaling by designing the system with discrete, independent components that can be updated or scaled individ- ually. Additionally, AI and Machine Learning techniques are integrated to automate complex incident responses, allowing the system to analyze data in real-time, detect security threats, assess their severity, and trigger appropriate responses with minimal human intervention, thereby improving efficiency and reducing response times.

I. Microservices: A Flexible Model for SOC Tool Development

This methodology focuses on implementing a Microser- vices Architecture by creating small, independent services that can be updated and deployed separately. It begins with the identification of distinct services based on business ca- pabilities, ensuring that each service encapsulates a specific functionality. Services are designed to be loosely coupled, communicating through well-defined APIs using standard pro- tocols such as HTTP/REST. Containerization technologies, such as Docker, facilitate independent deployment, while Con- tinuous

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

Integration/Continuous Deployment (CI/CD) pipelines automate testing and updates. Each service manages its own database, promoting autonomy and reducing dependencies. Finally, monitoring tools are integrated to track performance and health, with protocols established for scaling services to handle varying workloads effectively.

J. Data Fusion in Cybersecurity: Techniques, Tools, and Applications

This study employs a multi-faceted approach to anomaly detection, incorporating rule-based systems, machine learning algorithms, and statistical models. Rule-based systems use predefined rules to correlate data points and identify anomalies based on established conditions. Machine learning algorithms are applied to automatically learn patterns from historical data, enabling the detection of complex or previously unknown threats. Additionally, statistical models are used to predict and detect abnormal behaviors by identifying deviations from expected norms, enhancing the overall accuracy of anomaly detection.

K. Designing Scalable APIs for Real-Time Data Processing in SOC Tools

This study employs an event-driven architecture where APIs respond to specific events in real-time, improving system responsiveness and reducing latency by processing requests as they occur. Additionally, load balancing techniques are imple- mented to evenly distribute requests across multiple servers, ensuring smooth performance, preventing server overload, and optimizing resource utilization during periods of high traffic.

L. Machine Learning for Security Incident Detection

This study utilizes two machine learning approaches—Supervised Learning and Unsupervised Learning—to enhance threat detection capabilities. Supervised Learning involves training models on labeled datasets, where each instance corresponds to a known threat, allowing for the identification of such threats based on features associated with the labels. Performance metrics, including accuracy and precision, are used to evaluate the models. In contrast, Unsupervised Learning employs unlabeled data, enablingmodels to detect unknown anomalies by identifying patterns and relationships within the data through techniques such as clustering. The effectiveness of these models is assessed using metrics like silhouette scores and the Davies–Bouldin index to gauge clustering quality.

III. EXISTING SOC TOOLS

Traditional SOC tools are the cornerstone of cybersecurity operations within organizations, enabling them to monitor, detect, and respond to security incidents in real time. However, these tools often work in silos, leading to inefficiencies in data correlation and incident response. The most common SOC tools include Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Re- sponse (SOAR) platforms, Endpoint Detection and Response (EDR) solutions, and threat intelligence platforms [?].

- *SIEM Systems*

SIEM tools such as Splunk and IBM QRadar are widely used to aggregate logs and correlate security events across an organization's infrastructure. These tools provide centralized monitoring of security data from various sources, including firewalls, intrusion detection systems (IDS), and network de- vices. Despite their effectiveness, SIEM systems face several limitations:

- Alert Overload: SIEM systems generate vast numbers of alerts, many of which are false positives, contributing to alert fatigue among SOC analysts.
- Scalability Issues: As organizations grow, SIEM tools often struggle to scale efficiently, resulting in delayed incident detection and response.
- Manual Incident Response: SIEM systems primarily alert analysts but do not automate the response process, increasing the workload on SOC teams [?].

- *SOAR Platforms*

SOAR platforms such as Demisto and TheHive automate incident response workflows and help SOC teams manage and respond to security alerts more efficiently. Key features of SOAR platforms include:

- Automation of Routine Tasks: SOAR platforms auto- mate repetitive tasks such as alert triaging, log analysis, and threat intelligence correlation, allowing analysts to focus on higher-priority activities [?].
- Playbooks for Incident Response: SOAR tools often feature predefined playbooks that automate the response to common security incidents, helping reduce response times.
- However, the implementation of SOAR platforms can be complex and requires significant customization to fit an or- ganization's specific workflows.

- *EDR Tools*

Endpoint Detection and Response (EDR) tools, such as CrowdStrike Falcon and Carbon Black, provide real-time monitoring and response at the endpoint level. These tools offer:

- Behavioral Analysis: EDR systems monitor endpoint activities for abnormal behaviors that may indicate a security threat.
- Rapid Containment: EDR tools can isolate compro- mised endpoints to prevent the spread of attacks across the network [?].
- Despite these capabilities, EDR tools focus primarily on endpoints and may lack the broader network-wide visibility that SOC teams require for comprehensive threat detection.

- *Threat Intelligence Platforms*

Threat intelligence platforms, such as Recorded Future, aggregate external threat intelligence data, providing SOC teams with up-to-date information on emerging threats. These platforms enhance the decision-making process by correlating internal security events with known external threats. Chal- lenges with threat intelligence platforms

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

include:

- Data Overload: Similar to SIEM systems, threat intelligence platforms can overwhelm SOC analysts with excessive data, making it difficult to prioritize relevant information.
- Integration Issues: Many threat intelligence platforms face integration challenges with other SOC tools, complicating efforts to streamline data correlation [?].

IV. SURVEY FINDINGS

The survey results provide insights into the current chal- lenges facing SOC operations, integration needs, automation in SOC tools, the role of machine learning, and visualization preferences for SOC analysts. These findings highlight the gaps in existing SOC tools and underscore the need for more advanced and integrated solutions.

A. *Current Challenges in SOC Operations*

SOC teams face numerous operational challenges that hin- der their ability to detect and respond to threats effectively. Key challenges include:

- Alert Overload: SOCs generate thousands of security alerts daily, many of which are false positives or low-priority notifications. This ”alert fatigue” often leads to missed or delayed responses to critical incidents. Vielberth et al. (2020) noted that automation in alert prioritization is essential to mitigate this problem [?].
- Lack of Skilled Personnel: The shortage of skilled cybersecurity professionals is a global issue. Automating routine tasks through SOAR platforms and machine learning can reduce the reliance on human analysts for manual operations [?].
- Disjointed Tools: SOCs typically use multiple, unintegrated tools for security monitoring, which complicates incident response. Moustafa and Anjum (2020) emphasize the need for improved data fusion techniques to unify disparate data sources [?].

B. *Integration Needs*

The need for seamless integration across various SOC tools is critical for improving operational efficiency. SOC environments often involve multiple security systems, includ- ing SIEM, EDR, and threat intelligence platforms, which do not always communicate effectively with each other. Key integration needs include:

- Unified Architecture: SOC tools should provide a unified architecture that integrates data from different systems to ensure a holistic view of security events [?].
- Cross-Platform Compatibility: SOC tools must work across on-premise and cloud environments, ensuring comprehensive coverage and threat detection in modern hybrid environments [?].
- API-Driven Integration: Open APIs allow SOC tools to integrate with third-party security solutions, improving flexibility and extending SOC capabilities [?].

C. *Automation in SOC Tools*

Automation plays a critical role in reducing the manual workload on SOC teams and improving the speed and efficiency of incident response. Key findings on automation include:

- Automated Incident Response: SOAR platforms can automate repetitive tasks such as triaging alerts, isolating compromised endpoints, and blocking malicious IPs. Automation helps to streamline response workflows, reducing human error [?].
- Caution in Automation: While automation offers significant benefits, it must be implemented carefully to avoid improper handling of critical incidents or excessive reliance on automation without human oversight [?].

D. *Use of Machine Learning in SOC Tools*

Machine learning (ML) is increasingly integrated into SOC tools to enhance threat detection and reduce false positives. Key findings include:

- Anomaly Detection: ML models can identify abnormal behaviors in network traffic and system activity that may signal security threats, even those not detected by traditional rules-based systems [?].
- Reducing False Positives: ML algorithms can learn from historical data to distinguish between benign and malicious activities, significantly reducing false positives and allowing SOC analysts to focus on real threats [?].

E. *Visualization and Dashboard Preferences*

Visualization tools are essential for SOC analysts to inter- pret and act upon security data. Key findings on visualization include:

- Real-Time Data Visualization: SOC tools must provide real-time visualizations of security events to enable prompt detection and response. Laska et al. (2021) stress the importance of customizable dashboards that enable analysts to tailor their views to their specific needs [?].
- Actionable Insights: Dashboards should provide actionable insights, allowing analysts to quickly assess the severity of an incident and respond accordingly [?].

V. DESIRED FEATURES FOR AN INTEGRATED SOC TOOL

To address the challenges and limitations of traditional SOC tools, an integrated SOC tool should possess several key features. These features are aimed at enhancing operational efficiency, improving threat detection and response, and en- abling seamless integration of various security technologies.

➢ *Automated Threat Detection and Response*

An essential feature of an integrated SOC tool is the automa- tion of threat detection and response processes. Automation significantly reduces the workload on SOC

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

teams by managing repetitive tasks and allowing analysts to focus on critical incidents.

- SOAR Integration: Security Orchestration, Automation, and Response (SOAR) platforms should be integrated to automate routine tasks such as alert triaging and incident response. SOAR platforms streamline workflows and reduce the time to respond to security incidents [?].
- Behavior-Based Detection: The SOC tool should use behavior-based detection models powered by machine learning to identify anomalies in network traffic and user behavior. This approach allows for more accurate detection of threats, including those not recognized by signature-based systems [?].

➢ *Machine Learning Integration*

Machine learning (ML) should be a core component of the integrated SOC tool. ML can enhance the capabilities of SOCs in several ways:

- Anomaly Detection: Machine learning algorithms should be used to identify deviations from normal activity pat- terns that may indicate a security breach. This allows SOC teams to detect unknown threats, including zero- day vulnerabilities [?].
- Reducing False Positives: By learning from historical data, ML models can reduce the number of false positives generated by traditional security systems. This ensures that analysts spend their time responding to real threats rather than sorting through non-critical alerts [?].

➢ *Customizable Dashboards and Visualization*

SOC analysts rely on dashboards to gain a real-time view of their security posture. An integrated SOC tool should offer:

- Real-Time Data Visualization: Dashboards should display real-time data on network traffic, security events, and system health, enabling SOC analysts to respond quickly to emerging threats [?].
- Customizable Views: Different SOC roles (e.g., incident responders, SOC managers) require different types of data. Dashboards should be customizable, allowing users to focus on the most relevant information for their tasks [?].

➢ *Seamless Integration with Existing Infrastructure*

An integrated SOC tool must be able to work seamlessly with the organization's existing infrastructure. This includes integration with:

- SIEM, EDR, and Threat Intelligence Platforms: The tool should integrate with existing SIEM systems, Endpoint Detection and Response (EDR) tools, and external threat intelligence platforms to provide a unified view of security data [?].
- Cloud and On-Premise Systems: As organizations increasingly adopt cloud services, the SOC tool must be capable of monitoring both on-premise and cloud-based environments, providing complete visibility across the entire infrastructure [?].

➢ *Scalability and Flexibility*

SOC tools must be scalable to accommodate the growing volume of security data. This can be achieved through:

- Microservices Architecture: The SOC tool should be built on a microservices architecture, allowing individual components to be scaled independently based on demand. This ensures that the SOC tool can adapt to changes in workload without sacrificing performance [?].
- Cloud-Native Capabilities: SOC tools should be capable of scaling dynamically in cloud environments, enabling them to handle spikes in traffic or increased logging from cloud-native applications [?].

➢ *Compliance and Reporting Capabilities*

For organizations in regulated industries, compliance is a major concern. An integrated SOC tool should include:

- Automated Compliance Reporting: The SOC tool should automatically generate reports that meet the requirements of regulations such as GDPR, HIPAA, and PCI-DSS, ensuring that the organization remains compli- ant [?].
- Detailed Audit Trails: The tool should maintain compre- hensive audit logs of all security incidents and responses, enabling organizations to demonstrate compliance during audits and reviews [?].

VI. CHALLENGES TO ADOPTION OF INTEGRATED SOC TOOLS

Despite the clear advantages that integrated SOC tools offer, several barriers prevent their widespread adoption. These bar- riers include financial, technical, and organizational challenges that organizations must overcome to implement advanced SOC solutions effectively.

➢ *High Costs*

One of the primary barriers to adopting integrated SOC tools is the significant cost involved. Building a fully integrated SOC tool that incorporates automation, machine learning, and real- time data processing requires a substantial investment in both infrastructure and personnel.

- Initial Investment: Developing or acquiring an integrated SOC tool often demands a large upfront cost, particularly for small to medium-sized enterprises (SMEs). Purchas- ing commercial SOC tools and hiring skilled profession- als to deploy and maintain them can be prohibitively expensive [?].
- Operational Costs: In addition to the initial setup, maintaining and operating integrated SOC tools requires significant ongoing costs, including cloud storage, computa- tional resources, and license fees for third-party software [?].

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

➢ *Technical Complexity*

The technical complexity of deploying and managing an integrated SOC tool poses another major barrier. Organiza- tions without a mature IT or cybersecurity infrastructure may struggle to implement these systems effectively.

- Integration with Existing Systems: Most organizations already have a variety of security tools in place, such as SIEM, EDR, and firewalls. Integrating these existing tools with a new, centralized SOC system can be technically challenging and time-consuming [?].
- Configuration and Maintenance: Configuring an integrated SOC tool to work optimally in an organization's specific environment requires expertise. This includes tuning machine learning models, configuring automation workflows, and continuously monitoring system perfor- mance [?].

➢ *Security and Privacy Concerns*

The introduction of advanced features such as automation and machine learning introduces new risks related to security and privacy.

- Automation Risks: Automated responses, if improperly configured, can result in unintended actions, such as shutting down critical systems or blocking legitimate traffic. Ensuring that automated responses are carefully managed is critical to prevent potential disruptions [?].
- Machine Learning Vulnerabilities: Machine learning models used in SOC tools are vulnerable to adversarial attacks, such as model poisoning, where attackers manipulate the training data to compromise the model's integrity [?].
- Data Privacy Regulations: Organizations that handle sensitive data must comply with strict data privacy regu- lations (e.g., GDPR, HIPAA). Deploying SOC tools that aggregate and analyze large amounts of security data must ensure compliance with these regulations to avoid penalties [?].

➢ *Organizational Resistance to Change*

Even when technical and financial barriers are addressed, organizational resistance can prevent the successful implemen- tation of integrated SOC tools.

- Cultural Resistance: In many organizations, security teams are accustomed to using specific tools and processes. Introducing a new, integrated SOC tool often requires a cultural shift that may be met with resistance from staff [?].
- Training and Adoption Curve: SOC tools often come with steep learning curves. Training SOC analysts to use new tools effectively can take time and resources, and there may be initial resistance to adopting the new system [?].

➢ *Vendor Lock-in*

Many commercial SOC solutions are proprietary, leading to the risk of vendor lock-in. Once an organization commits to a particular vendor's SOC tool, they may become dependent on the vendor for updates, support, and future scalability, which can limit flexibility and increase costs over time [?].

VII. RECOMMENDATIONS FOR DEVELOPING AN

➢ *Integrated Soc Tool*

To overcome the challenges and barriers highlighted in the survey, this section provides recommendations for developing an integrated Security Operations Center (SOC) tool. These recommendations focus on ensuring that the SOC tool is scal- able, user-friendly, secure, and adaptable to evolving security threats.

➢ *Modular Design for Flexibility*

An integrated SOC tool should be built using a modular design to ensure flexibility and adaptability. By breaking the SOC tool into smaller, self-contained modules, organizations can update or replace specific components without impacting the entire system.

- Modularity for Easy Updates: Each module should handle a distinct function (e.g., log aggregation, threat intelligence, or incident response), allowing organizations to independently update or scale these components based on their needs [?].
- Third-Party Integration: Modular designs with open APIs enable seamless integration with third-party tools and services, ensuring that the SOC tool can evolve with emerging technologies [?].

➢ *Microservices Architecture for Scalability*

A microservices architecture is recommended to enhance the scalability of the SOC tool. By implementing microser- vices, each service operates independently and can be scaled based on demand, ensuring efficient resource utilization during periods of high traffic.

- Independent Scaling: Services like log management and real-time analytics can be scaled separately without af- fecting other parts of the SOC tool, allowing for dynamic resource management [?].
- Improved Fault Tolerance: With microservices, if one service fails, the rest of the system remains operational, reducing downtime and improving system reliability [?].

➢ *Incorporating Machine Learning and Automation Thought- fully*

While automation and machine learning (ML) are essential for enhancing SOC capabilities, their implementation must be done thoughtfully to avoid potential pitfalls such as false positives or unintended automation consequences.

- Anomaly Detection Models: The SOC tool should incor- porate ML models capable of detecting abnormal network activity in real time. These models should be trained continuously to adapt to evolving threat patterns [?].

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

- Human-in-the-Loop Automation: While automation can handle repetitive tasks, critical incidents should involve human oversight to ensure appropriate response actions. SOC tools should strike a balance between automation and human judgment [?].

➢ *User-Centric Design*

A successful SOC tool must focus on user experience (UX) to ensure that SOC analysts can quickly and efficiently interpret data and respond to incidents.

- Customizable Dashboards: The SOC tool should provide customizable dashboards that allow users to tailor their views based on their roles and responsibilities. For example, SOC managers may prioritize system health and performance, while incident responders focus on real- time security alerts [?].
- Actionable Insights: Visualization tools should provide actionable insights that enable SOC analysts to quickly assess the severity of incidents and respond accordingly. Clear, intuitive visualizations reduce cognitive load and improve decision-making [?].

➢ *Compliance and Regulatory Features*

Given the importance of regulatory compliance in industries such as healthcare, finance, and government, SOC tools must offer built-in compliance features.

- Automated Reporting: The SOC tool should automatically generate compliance reports based on predefined templates for regulations like GDPR, HIPAA, and PCI-DSS. This reduces manual effort and ensures that organizations stay compliant [?].
- Audit Logs and Traceability: The SOC tool should maintain comprehensive audit logs of all security events and responses, allowing organizations to demonstrate compliance and trace incidents for regulatory audits [?].

➢ *Support for Multi-Cloud and Hybrid Environments*

With the growing adoption of cloud services, SOC tools must be capable of providing visibility and security across both on-premise and cloud-based infrastructures.

- Cloud-Native Monitoring: SOC tools should integrate with cloud platforms such as AWS, Azure, and Google Cloud to collect and analyze security data from cloud environments [?].
- Cross-Platform Compatibility: The SOC tool should be designed to work seamlessly in hybrid environments, combining cloud-native and on-premise security data for comprehensive monitoring [?].

VIII. CONCLUSION

The development of an integrated Security Operations Center (SOC) tool is essential for addressing the growing challenges of modern cybersecurity. This paper has surveyed the existing SOC tools, highlighted their limitations, and dis- cussed the need for enhanced integration, automation, machine learning, and real-time visualization in SOC environments.

➢ *Key Takeaways from this Survey Include the Necessity of:*

- Seamless integration across various security tools to enable effective data correlation and a unified view of security events.
- Automating routine tasks and incorporating machine learning to improve the accuracy of threat detection and reduce false positives, while ensuring that human over- sight remains a critical component in handling complex incidents.
- Adopting modular and microservices architectures to allow for scalability, flexibility, and ease of maintenance, particularly in cloud-native and hybrid environments.
- Designing user-centric dashboards that provide customiz- able, real-time insights to SOC analysts, improving their ability to respond to incidents efficiently.
- Ensuring built-in compliance features that simplify regulatory reporting and audit processes, particularly in industries with stringent privacy requirements.

While the benefits of an integrated SOC tool are clear, organizations face barriers to adoption, such as high costs, technical complexity, and organizational resistance to change. Overcoming these challenges requires a thoughtful approach that balances advanced technology with usability and cost- effectiveness.

Future SOC tools must focus on continuous improvement, incorporating the latest advancements in machine learning and automation while remaining flexible enough to adapt to new threats. By addressing the current limitations and implementing the recommendations discussed in this paper, organizations can significantly improve their security posture and enhance their ability to detect and respond to cyber threats in real time.

REFERENCES

[1] Hayeri Khyavi and M. Rahimi, “Conceptual Model for Security in Next Generation Network,” in Proceedings of the 2021 IEEE Interna- tional Conference on Computer and Communication Systems (ICCCS), 2021, pp. 123-128.

[2] Q. Yang, “Computer Network Security Evaluation Method Based on GABP Model,” Journal of Computer Networks and Communications, vol. 2020, pp. 1-9, 2020.

[3] Z. Lina and Z. Dongzhao, “A New Network Security Architecture Based on SDN/NFV Technology,” in Proceedings of the 2021 IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2021, pp. 98-103.

[4] Vielberth, F. Bo¨hm, I. Fichtinger, and G. Pernu, “Security Operations Center: A Systematic Study and Open Challenges,” IEEE Access, vol. 8, pp. 211407-211420, 2020.

[5] Elsadig, A. Altigani, and M. A. A. Baraka,

ISSN No:-2456-2165 https://doi.org/ 10.5281/zenodo. 14557505

"Security Issues and Challenges on Wireless Sensor Networks," International Journal of Information Security, vol. 18, no. 4, pp. 305-319, 2019.

[6] Pautasso, "RESTful Web Services: Principles and Best Practices," IEEE Internet Computing, vol. 17, no. 4, pp. 79-82, 2013.

[7] Islam, M. A. Babar, and S. Nepal, "Building a SOAR Platform: Design Considerations and Technical Challenges," in Proceedings of the 2021 IEEE International Conference on Cybersecurity and Privacy (ICCP), 2021, pp. 50-55.

[8] Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Microservices: A Flexible Model for SOC Tool Development," in Proceedings of the 2021 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2021, pp. 209-216.

[9] Gonza´lez-Granadillo and S. Gonza´lez-Zarzosa, "Next-Generation SIEM: From Monitoring to Detection and Response," Journal of Cybersecurity and Privacy, vol. 1, no. 3, pp. 322-339, 2021.

[10] Moustafa and A. Anjum, "Data Fusion in Cybersecurity: Techniques, Tools, and Applications," IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2345-2372, 2019.

[11] Laska, S. Herle, R. Klamma, and J. Blankenbach, "Designing Scal- able APIs for Real-Time Data Processing in SOC Tools," in Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1-6.

[12] Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Machine Learn- ing for Security Incident Detection: A Survey," Journal of Information Security and Applications, vol. 58, 2021.