WHITE PAPER

THE EVOLUTION TOWARDS AI-DRIVEN SECURITY OPERATIONS CENTERS

Abstract:

Security Operations Center (SOC) teams encounter an increasing array of challenges: highly skilled threat actors, an overwhelming volume of alerts that far exceeds available time, and the burnout of SOC analysts striving to keep up with demand. These impediments, along with the surge in organizational data that must be safeguarded, call for a new approach to the SOC.

paloalto® NETWORKS

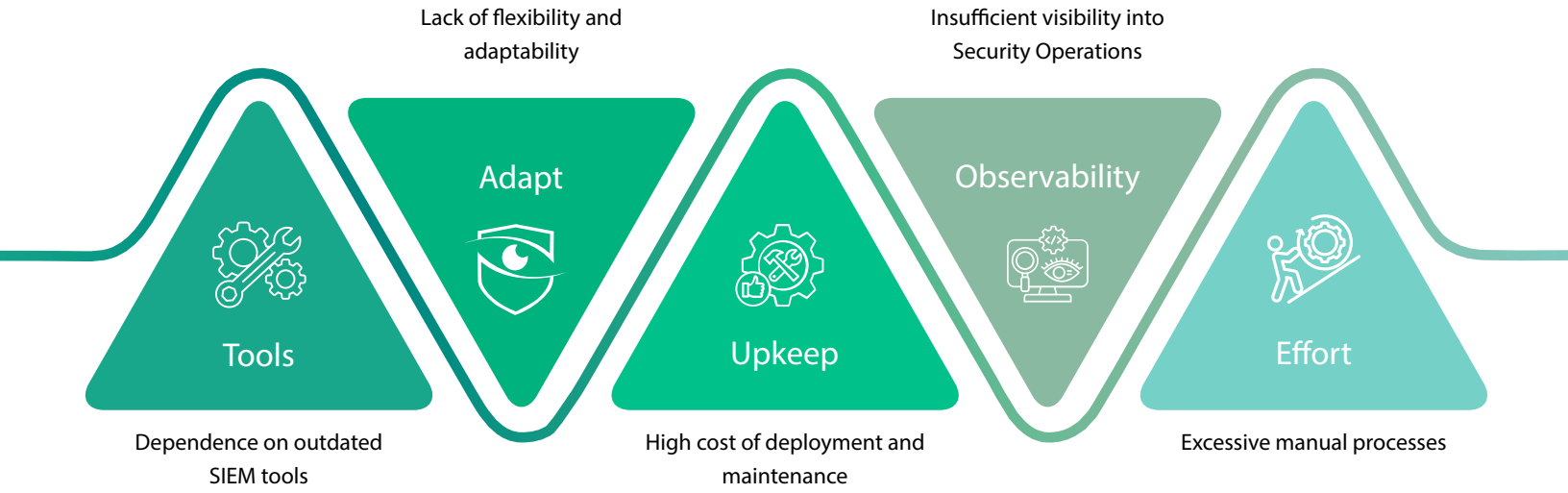
Infosys® Navigate your next

Introduction

Although Security Operations Center (SOC) teams are essential in safeguarding organizations' IT infrastructures and data from cyber threats, these challenges continue to evolve alongside advancements in cyber threats and technology. The intricacies of cyber threats are growing, and the volume of data is soaring, making security increasingly challenging and overwhelming.

In response, traditional Security Operations Centers are undergoing a major transformation. Security Operations Centers (SOCs) are now serving as a vanguard of advanced defense against the unyielding flood of cyber threats. The analysts in the SOC are constantly working to detect, analyze, and address potential breaches as threat landscapes grow more intricate. New SOC tools, powered by intelligent value realization, have emerged with the advent of AI, ML, and natural language processing technologies, bringing a modern approach to cybersecurity and delivering measurable outcomes. These tools have the potential to increase efficiency and improve incident response automation, which will speed up response times and reduce security issues significantly.

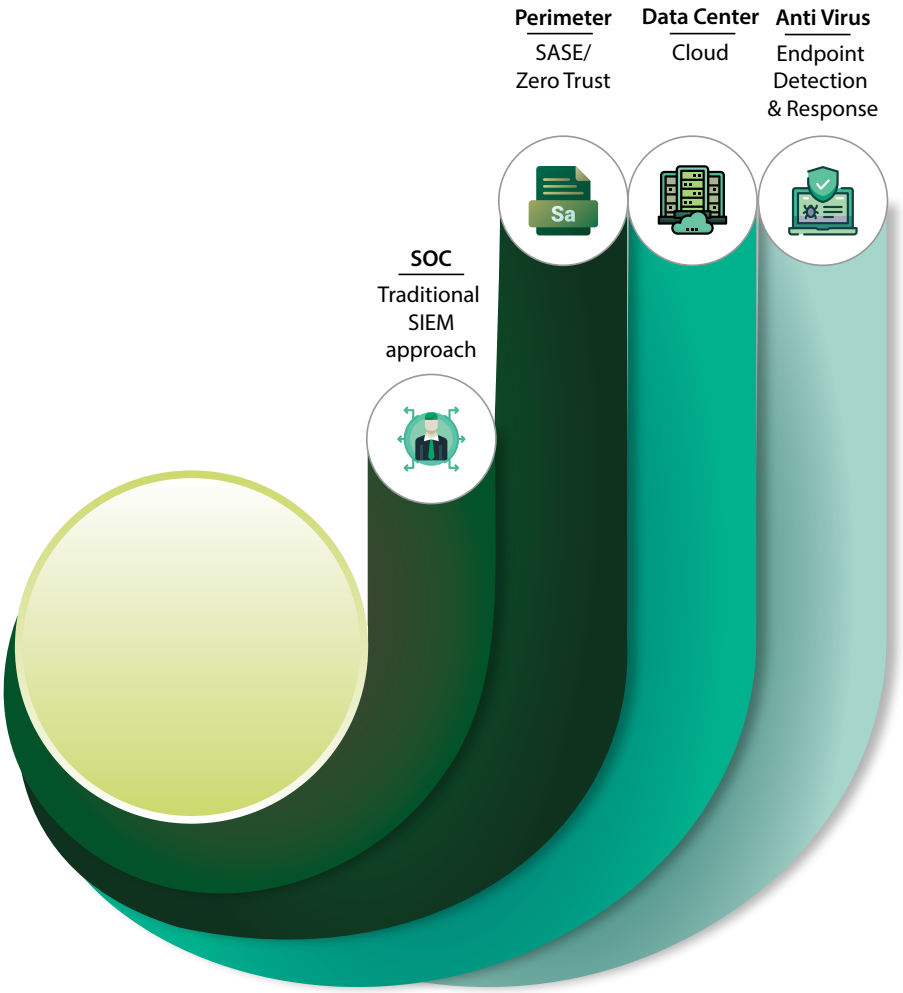
Challenges with Traditional SOC



1. Conventional Security Operations Centers (SOCs) frequently rely on numerous diverse tools, data sources, logs, feeds, and alerts. However, these do not provide a comprehensive and cohesive view of the organization's security posture and threat environment. Moreover, they fail to offer sufficient context and correlation for SOC analysts to understand the root cause, impact, and scope of an incident.
2. The lack of automation and orchestration, dependency on manual efforts, adapting to changing business and compliance requirements, newer tools and technologies, and the increasing volume of threats are some of the key challenges that conventional SOCs struggle to keep up with. As a result, SOC analysts must contend with a significant amount of complexity, redundancy, and inconsistency, all of which can impair their performance and productivity.
3. The cost of deploying and maintaining cybersecurity tools can be substantial, often including the initial purchase price of the software, ongoing subscription fees, hardware upgrades, staff training, and expert maintenance services. This makes it a significant expense for businesses of all sizes.
4. Traditional security operation centers (SOCs) often operate in isolation, lacking a comprehensive understanding of the organization's business objectives, risks, and priorities. Furthermore, they do not communicate and collaborate effectively with other key stakeholders. Consequently, SOC analysts have a limited and narrow perspective on the organization's security requirements and obstacles. These challenges can weaken the effectiveness and value of a traditional SOC, leaving the organization vulnerable to increased risks. Therefore, we must reimagine and update the SOC model to effectively address these challenges and achieve meaningful, business-focused results.
5. SOC analysts must invest significant time and resources in manual investigations, data gathering across multiple systems, triage, and remediation. This can result in alert fatigue, overlooked incidents, and false positives. This can be significantly improved by utilizing AI-powered SOC solutions that automate these tasks, allowing analysts to focus on more strategic and complex threat investigations instead.

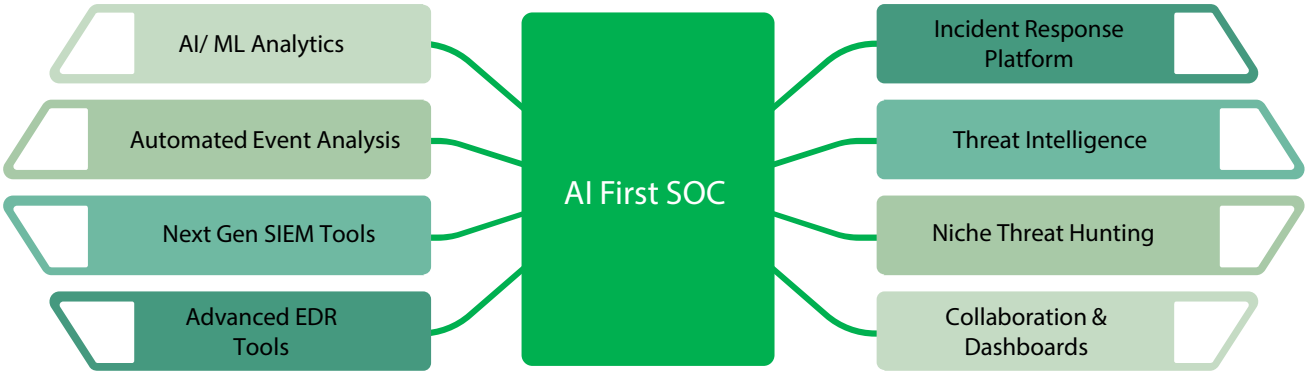
Evolution of SOC

The requirements of Security Operations Centers (SOCs) have evolved, yet the configurations of Security Information and Event Management (SIEM) systems and SOCs remain unchanged. Many fundamental components of security architecture have seen advancements. The focus on networks has shifted from a traditional "hard shell" perimeter approach to embracing a Zero Trust and SASE framework. Additionally, focus on endpoints has transitioned from antivirus solutions to Endpoint Detection and Response (EDR), while runtimes are also undergoing changes as data centers move to the cloud. However, in many organizations, the Security Operations Center continues to operate based on a SIEM model established two decades ago.

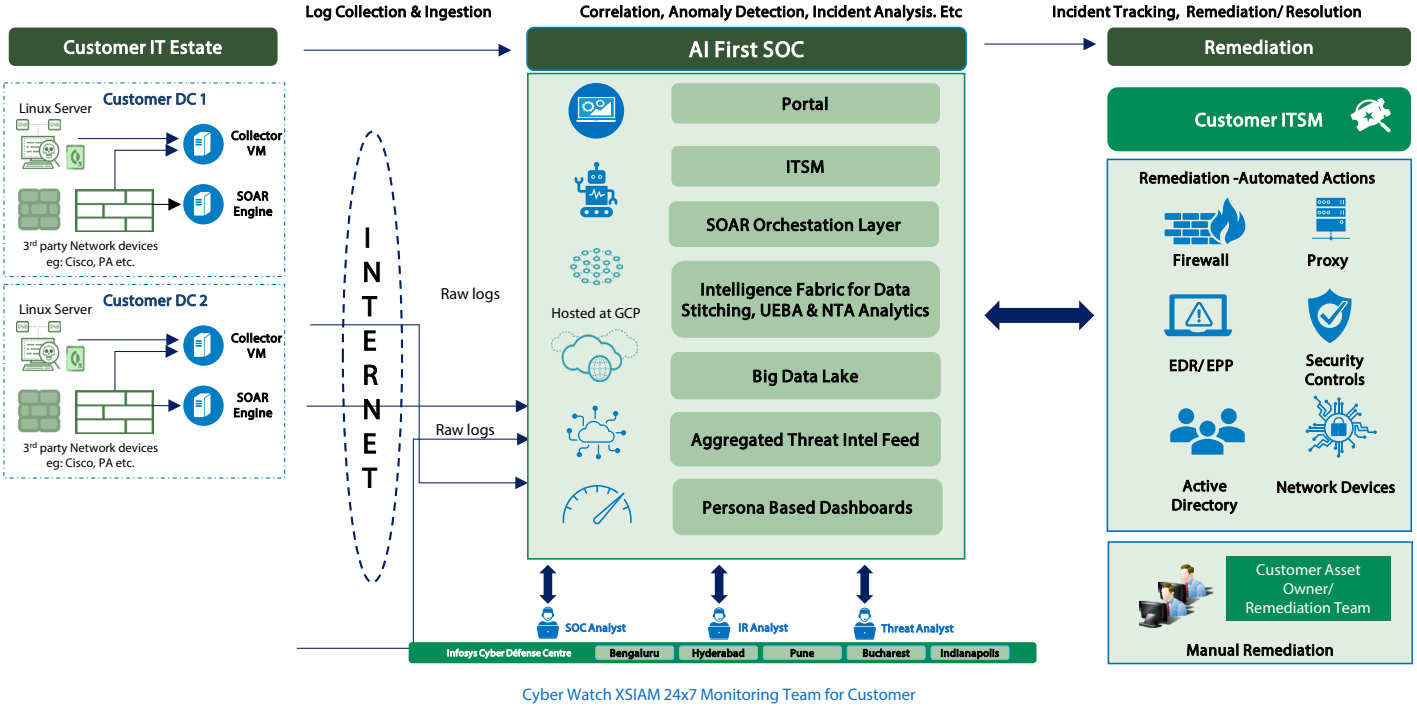


What is AI-First SOC?

AI-First SOC (Security Operations Center) is a newer approach to cybersecurity that utilizes AI (Artificial Intelligence) and ML (Machine Learning) to automate and augment security operations. The AI-First SOC aims to transform cybersecurity by facilitating quicker threat identification, proactive defense mechanisms, and improved operational efficiency.



The AI-First SOC will enhance and amplify the effectiveness of security analysts by enabling scalable data collection and robust analytics through a unified dataset, free of silos and data replication. By employing AI and ML, the administrative and investigative functions and processes of security analysts can be simulated. Steps in the security incident lifecycle, such as response, triaging, analysis, and collaboration, will be automated, thereby enriching the alert and incident data. This allows security analysts to focus on genuine incidents, eliminating alert fatigue and increasing efficiency. The high-level reference architecture of the AI-First SOC is shown below:



High-Level Reference Architecture of AI First SOC

Key functions of AI-First SOC

SOCs are not exempt from the rule that all technologies must adapt to changing user needs and environments. Successfully implementing automation powered by artificial intelligence (AI) and machine learning (ML) is essential. This helps streamline and manage the tedious process of analyzing alerts and identifying which ones require action.

The main purpose of the AI-First SOC is to enhance the capabilities of security teams and increase the effectiveness of human SOC analysts. The AI-First SOC can quickly sort through massive datasets, effectively differentiating between benign alerts and real threats. By simulating sophisticated investigative techniques, the integration of Gen-AI significantly expands the capabilities of the AI-First SOC. It will provide prompt and efficient incident response and detection to address threats in expansive, cloud-first infrastructures.

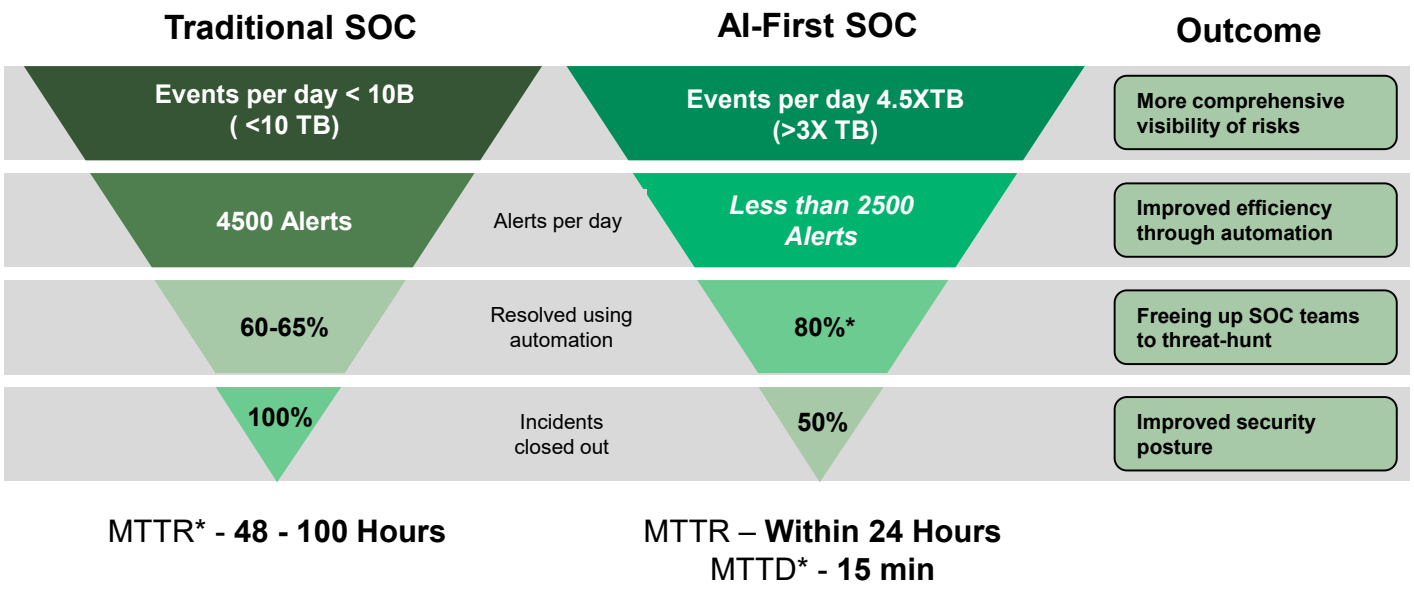
The SOC operations are enhanced by Gen-AI's contextual understanding and decision-making capabilities. This amalgamation enables the system to offer more insightful security analysis and respond more intelligently to new threats. For enterprises looking to maintain strong, flexible, and efficient cybersecurity defenses, deploying AI-First SOC technologies becomes not only advantageous but also necessary as cyber threats become more frequent and sophisticated.

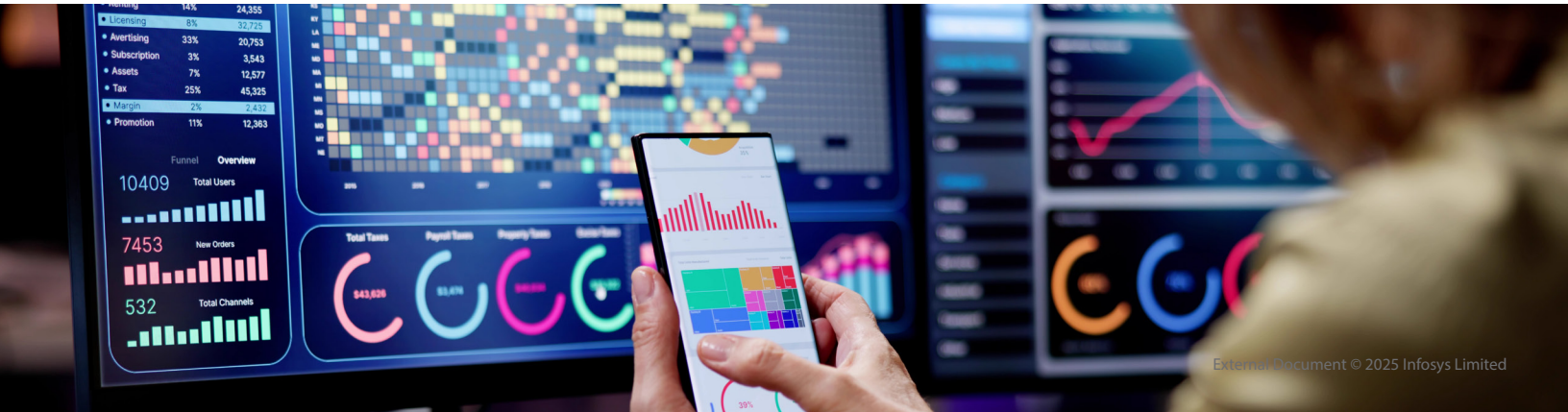
This represents a turning point in how we approach cybersecurity and the use of AI in fields where tools are designed to be more efficient than humans. It is the culmination of a goal to develop the autonomous security platform of the future, which will enable significantly improved security with detection and response in almost real-time.

Palo Alto Cortex XSIAM integrates vast volumes of security data using an ML-led design, built on a security-specific data model that is continuously updated with Palo Alto Networks threat information collected globally across tens of thousands of clients. To respond to most events automatically and allow analysts to concentrate on fewer threats that require human involvement, it collects alerts into incidents for automated analysis and triage.

New-generation products featuring AI-powered detections and automations, such as EDR, SOAR, ASM, UEBA, TIP, and SIEM, are among the best-in-class functions integrated into Palo Alto Cortex XSIAM. These components will assist an enterprise in implementing an AI-powered SOC. The value proposition of the AI-First SOC, based on a benchmark, is shown below:

Value Proposition of AI-First SOC based on a benchmark





Key Benefits of AI-First SOC

1. Better Incident Response

By containing threats and isolating compromised systems, AI-First SOCs can mitigate the impact of security incidents on business operations.

2. Eliminate Security Silos

A variety of screens are used by the analysts in a typical SOC. With the same workflows and fully integrated data, AI-First SOC can provide all functionality in a single console.

3. Obliterate repetitive tasks

By eliminating repetitive tasks and processes, response times will be accelerated, improving operational efficiency and empowering analysts to provide faster threat mitigation.

4. Minimal Human Errors

The AI-First SOC reduces the possibility of human error by automating repetitive processes and providing insightful information through the use of AI and ML. This increases the precision of security operations and strengthens the organization's defenses against online attacks.

5. Integrated Actions

Security teams will be able to react to threats more swiftly and convincingly once there is integration of detection, investigation, hunting, automation, and forensic analysis into a single user-friendly platform.

6. Enhanced Threat Analysis

AI-First SOCs use advanced threat intelligence to analyze threats in detail. This thorough comprehension aids SOC analysts in creating focused responses, guaranteeing prompt risk mitigation.

7. Improved Security Posture

By analyzing past data, patterns and trends, AI-First SOCs will be able to anticipate threats. This makes it possible to put preventative measures in place before any incidents arise.

8. Reduce Risk

Minimize risk by thoroughly investigating and promptly prioritizing every piece of information and alert received from integrated sources.

9. Scalability

The scalability will be increased by bringing in automations resulting in enterprises spending less to get the same level of protection and security.

Factors to consider before investing in an AI-First SOC

The AI-First SOC is the future direction our industry is moving towards. It is expected that most major enterprises are considering transitioning to an AI-First SOC in the next few years. Unfortunately, many leaders incorrectly perceive the SOC as a cost center and underestimate its contribution to generating revenue for the organization.

Transitioning to an AI-First SOC might appear challenging or unfeasible, but the primary goal of an AI-First SOC is to maximize the value derived from the tools and workflows available to the SOC, ultimately resulting in less burnout for SOC analysts, higher engagement levels, and a more manageable work environment.

Investing in cybersecurity is crucial to safeguard assets, reputation, and operations, ultimately reducing costs. With the continually evolving landscape of cyber threats and changing tactics employed by cybercriminals, it is essential for businesses of every scale to implement robust cybersecurity measures to protect against attacks and adhere to regulatory requirements.

Another crucial factor to consider is timing, specifically whether your organization is prepared for this transition or not. Evaluate the level of maturity within the Security Operations Center (SOC) through a discussion involving SOC analysts, architects, and leaders. It is worth mentioning that transitioning to an AI-First SOC does not have to be a complete shift, but rather a gradual process, as it is a journey. While enterprises need to carefully evaluate multiple options, tools like Palo Alto Cortex XSIAM can help amplify their ability to augment their SOC journey. Cortex XSIAM offers a platform with sophisticated AI and automation capabilities, allowing security analysts to practice real-world scenarios, gain knowledge from machine-driven insights, and hone their threat detection and response skills with minimal manual intervention. This effectively simulates a contemporary SOC environment and accelerates their learning curve.

While enterprises must be cautious when evaluating multiple options, tools like Palo Alto Cortex XSIAM can significantly enhance their Security Operations Center (SOC) journey. Cortex XSIAM provides a platform with advanced AI and automation capabilities, allowing security analysts to engage in real-world scenarios, derive insights from machine-driven data, and refine their threat detection and response skills with minimal manual intervention. This effectively simulates a modern SOC environment and accelerates their learning curve.

Role of SOC Analysts in AI-First SOC

One question that comes to mind is: once the AI-First SOC is implemented, what will be the role of SOC analysts in an AI-First SOC? Even though processes around security operations are automated, the human element remains essential for activities such as system monitoring, recognizing threats, validating critical attack scenarios, decision-making, creating dashboards, and deploying and maintaining tools and technologies. Furthermore, cybersecurity teams are consistently involved in collaborating with other teams to enhance infrastructure security measures, including network device segmentation, addressing and mitigating vulnerabilities, and managing identities and access. The analysts who are freed up due to automation could be reallocated to handle these tasks.

Automation doesn't eliminate the need for SOC analysts; rather, it reduces the manual efforts and tools required for streamlining the security incident lifecycle.

By shifting some responsibilities from human analysts to automated systems, SOC automation increases the overall scalability factor. For example, compared to manual processes, automated playbooks are far more scalable. They not only improve response speed but also ensure that the responses are consistent, thereby reducing the likelihood of manual errors during the process.

Conclusion

AI-First SOCs represent a progressive advancement in the evolution of cybersecurity operations. Security teams are making strides in enhancing their organizations' security posture by moving toward a more comprehensive and resilient approach as they transition to an AI-First SOC.

This new iteration of the SOC aims to address numerous issues faced by traditional SOCs. With the rising complexity and frequency of cyber threats, the collaboration of human skills and AI-powered automation in AI-First SOCs will play a vital role in maintaining strong, flexible, and efficient cybersecurity defenses.

References

https://www.paloaltonetworks.com/cyberpedia/revolutionizing-soc-operations-with-ai-soc-solutions

https://www.darkreading.com/vulnerabilities-threats/5-tips-for-modernizing-your-security-operations-center-strategy

https://www.forbes.com/sites/tonybradley/2024/10/25/accelerating-and-improving-cyber-defense-with-an-autonomous-soc/

https://solutionsreview.com/security-information-event-management/what-to-consider-when-building-an-autonomous-soc/

https://www.paloaltonetworks.com/blog/2024/03/ai-in-the-modern-soc/

About the Author

Prassanna Rao Rajgopal

Industry Principal

Prassanna has 20+ years of IT experience specializing in cybersecurity. As the North America offering leader for Infosys' strategic partnership with Palo Alto Networks, he manages joint go-to-market cybersecurity offerings. He has managed security portfolios for Fortune 500 clients, program-managed critical engagements, and led global 24/7 security operations and risk management teams. Prassanna has developed cybersecurity roadmaps with CISOs and collaborated on building a Cybersecurity Operations Center. His experience also includes transformation, outsourcing, and service delivery within cybersecurity.

For more information, contact askus@infosys.com

Infosys®
Navigate your next