SPOTLIGHT

Sponsored by: Tata Communications

By reimagining the security operations center as a dynamic, intelligence-driven nerve center, organizations can improve their security posture and align their cybersecurity efforts more closely with broader business objectives.

Review and Modernize the Security Operations Center

October 2024

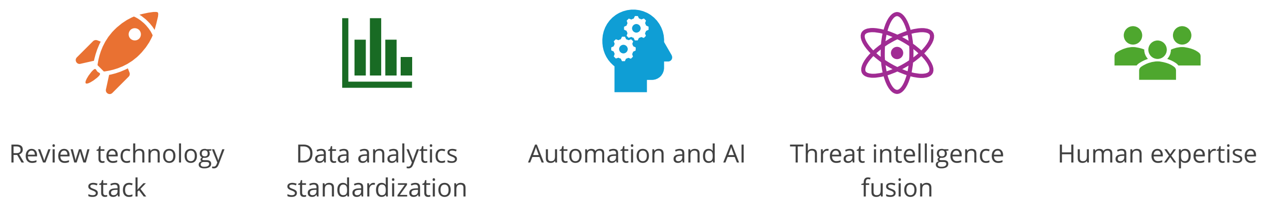
Written by: Cathy Huang, Research Director, Security and Trust, and Craig Robinson, Research Vice President, Security and Trust, IDC

Introduction

In an era of rapidly evolving cyberthreats, the security operations center (SOC) stands as a critical bulwark in an organization's defense strategy. However, as the digital landscape transforms, many SOCs struggle to keep pace with sophisticated adversaries, exponential data growth, and an expanding attack surface. The traditional SOC model, often characterized by siloed tools, manual processes, and reactive approaches, is increasingly inadequate in the face of today's complex threat environment.

This IDC Spotlight discusses crucial components, including data, platforms, threat intelligence, automation, AI for future proofing SOCs (see Figure 1), which have revolutionized how organizations detect, analyze, and respond to cyberthreats. This shift addresses several key challenges faced by traditional SOC setups, offering significant improvements in efficiency, effectiveness, and scalability. This paper also discusses key metrics to define a modern SOC.

Figure 1: ***Components for Future Proofing SOCs***



Source: IDC, 2024

By reimagining the SOC as a dynamic, intelligence-driven nerve center, organizations can improve their security posture and align their cybersecurity efforts more closely with broader business objectives. Modernization is not just about adopting new tools; it involves fostering a culture of continuous adaptation and improvement in response to an ever-changing threat landscape.

Crucial Components for Future Proofing SOCs — Data, Data, Data

Data, whether through analytics or a data lake, is a crucial component in future proofing SOCs. It is an asset worthy of protection and the fuel for analytics that helps organizations detect and respond to attacks.

An effective data strategy within the SOC addresses the growing volume, variety, and velocity of security data, enabling organizations to maintain effective threat detection and response capabilities in an evolving cyberlandscape. Some actionable steps are:

- **Standardize data formats for logs, alerts, and other security data.** Data format standardization is a foundational element. By defining common formats for logs, alerts, and other security data, organizations can streamline their data integration and analysis processes. This standardization may involve adopting widely used formats such as Common Event Format or Structured Threat Information eXpression for threat intelligence. The benefits are substantial: Analysts can more easily correlate events across different systems, automation becomes simpler, and new data sources integrate more quickly.
- **Establish uniform data collection protocols.** Uniform data collection protocols are equally important, ensuring that data from various sources is complete, accurate, and consistent. Protocols should specify the frequency of data collection, the specific data points to capture, and the handling of edge cases or errors. By establishing these protocols, SOCs can minimize data gaps and inconsistencies that might lead to missed threats or false positives. For example, a standardized protocol for collecting endpoint data ensures that critical information such as process creation events or network connections consistently appears across all systems, regardless of operating system or hardware differences.
- **Govern the data lake.** Data lakes serve as a vast, centralized repository for all security-relevant data. Like a library's extensive archives, they store raw information from various sources, allowing for deep historical analysis and the discovery of patterns. Unlike traditional databases with rigid schemas, data lakes can ingest and store data in its raw format, whether structured log files, unstructured text from threat intelligence feeds, or semi-structured JSON data from cloud services. This flexibility is crucial in the rapidly evolving security landscape, where new data types and sources constantly emerge. A well-implemented data lake strategy enables SOCs to future proof their data architecture, accommodating new data sources without major infrastructure changes.

As the saying goes, "a data lake can quickly become a data swamp" without proper governance. Developing processes to validate and clean data is essential for maintaining high data quality standards. This may involve automated checks for data completeness and consistency, deduplication processes, and mechanisms for handling and flagging data quality issues. Regular data quality audits and cleansing routines ensure the data lake remains a reliable source of information for security analysis.

Data residency is another critical consideration given the increasing importance of data privacy regulations and regional compliance requirements. It is vital to design the SOC architecture with data residency in mind from the outset and implement geofencing technologies to ensure data remains within specified boundaries. Organizations should only collect and transfer data that is necessary for SOC operations. If organizations decide to go with a federated SOC model (i.e., regional SOCs that handle local data processing and analysis with a central SOC for global threat intelligence and coordination), they should implement secure data sharing protocols between regional and central SOCs.

The Rise of Platforms in a Modern SOC

In a modern SOC, platforms act as the central nervous system, integrating diverse security tools and data sources into a cohesive ecosystem. These platforms often include security information and event management (SIEM) or security orchestration, automation, and response (SOAR) solutions, providing a unified interface for monitoring, analysis, and response activities. They aggregate and correlate data from various sources, including network devices, endpoints, and cloud services, enabling a holistic view of the organization's security posture. Key benefits include:

- **Holistic visibility:** By centralizing data from various sources — including network logs, endpoint telemetry, and threat intelligence feeds — a platform provides security analysts with a comprehensive view of the organization's security posture. This consolidated approach enables the identification of complex attack patterns that might go unnoticed when analyzing data in isolation. For instance, a seemingly benign event in network logs may gain significance when analysts correlate it with unusual endpoint behavior, allowing them to quickly piece together the full scope of an ongoing attack.
- **Simplified management:** Instead of juggling multiple tools and interfaces, security teams can operate with streamlined workflows, reduced training overhead, and minimized configuration errors from managing disparate systems. IDC's December 2023 *North American Tools and Vendors Consolidation Survey* found that on average, organizations have nearly 50 security tools in their environments, with some exceeding 140. Encouragingly, some 60% of organizations began consolidation efforts in 2023, according to the survey:
  - One of the most effective ways to consolidate tools is by adopting a platform approach that standardizes security tools across fewer vendors. Moreover, updates and security patches apply more efficiently across the entire platform, ensuring all components remain current and secure against the latest threats.
  - The soft costs of moving from a best-of-breed tool strategy to a platform model are also notable. A similar look and feel across every component inherently help cybersecurity practitioners — especially in smaller organizations where one person may shift between the SIEM, CASB, and EDR during an investigation. With fewer vendors and tools, organizations benefit from simpler upgrades, fewer relationships to manage, and the potential to bundle savings.
- **Single source of truth:** This concept is valuable in the collaborative environment of a SOC. With all team members working from the same data set and within the same platform, there's less risk of miscommunication or conflicting analyses. This shared context facilitates faster incident response, more accurate threat assessments, and improved team performance.

- **Scalability:** Scalability is crucial, as organizations face growing data volumes and an expanding array of sources. Platform-centric SOCs accommodate this growth, allowing for the seamless integration of new data types and resource scaling as necessary. This flexibility ensures the SOC evolves alongside the organization, maintaining effectiveness even as the threat landscape and business requirements change.

- **Advanced capabilities:** Advanced platforms incorporate machine learning for enhanced threat detection and automated response workflows. They facilitate collaboration among team members, ensuring consistent processes and knowledge sharing. By centralizing operations, these platforms improve efficiency, reduce response times, and enhance SOC effectiveness. Moreover, they provide scalability and flexibility, allowing the SOC to adapt to evolving threats and changing organizational needs while maintaining comprehensive visibility and control over the security environment.

Threat Intelligence, Automation, and AI — Empowering a Modern SOC

Threat intelligence is pivotal for empowering a modern SOC with contextual, actionable information about potential and existing threats. It goes beyond raw data, providing analyzed insights into adversaries' tactics, techniques, and procedures. In a SOC, threat intelligence feeds inform detection rules, guide incident response strategies, and enhance proactive threat hunting. It enables the SOC to stay ahead of emerging threats, understand attack motivations, and effectively prioritize defensive efforts. Furthermore, threat intelligence aids in risk assessment and strategic decision-making, helping organizations allocate resources efficiently and adapt their security posture to address relevant threats.

Similarly, automation is crucial for enhancing the efficiency and consistency of a modern SOC. It streamlines repetitive, rule-based tasks, allowing human analysts to focus on more complex issues. In a SOC, automation is typically applied to alert triage, ticket creation, and routine data collection. For instance, automation can filter out false positives based on predefined rules, automatically escalate high-priority alerts, or initiate standard incident response procedures.

The use of AI is not new; AI with machine learning has been prevalent for years. For example, user and entity behavior analytics establishes baseline behavior for devices or personas, and it will look for abnormalities or deviations from expected behavior. Integrating generative AI (GenAI) into the SOC can significantly enhance the efficiency, accuracy, and scalability of security operations. Figure 2 shows a functional road map of GenAI use cases in security operations and related functions that are currently being piloted or rolled out, along with potential future use cases. Some primary GenAI use cases in the SOC are:

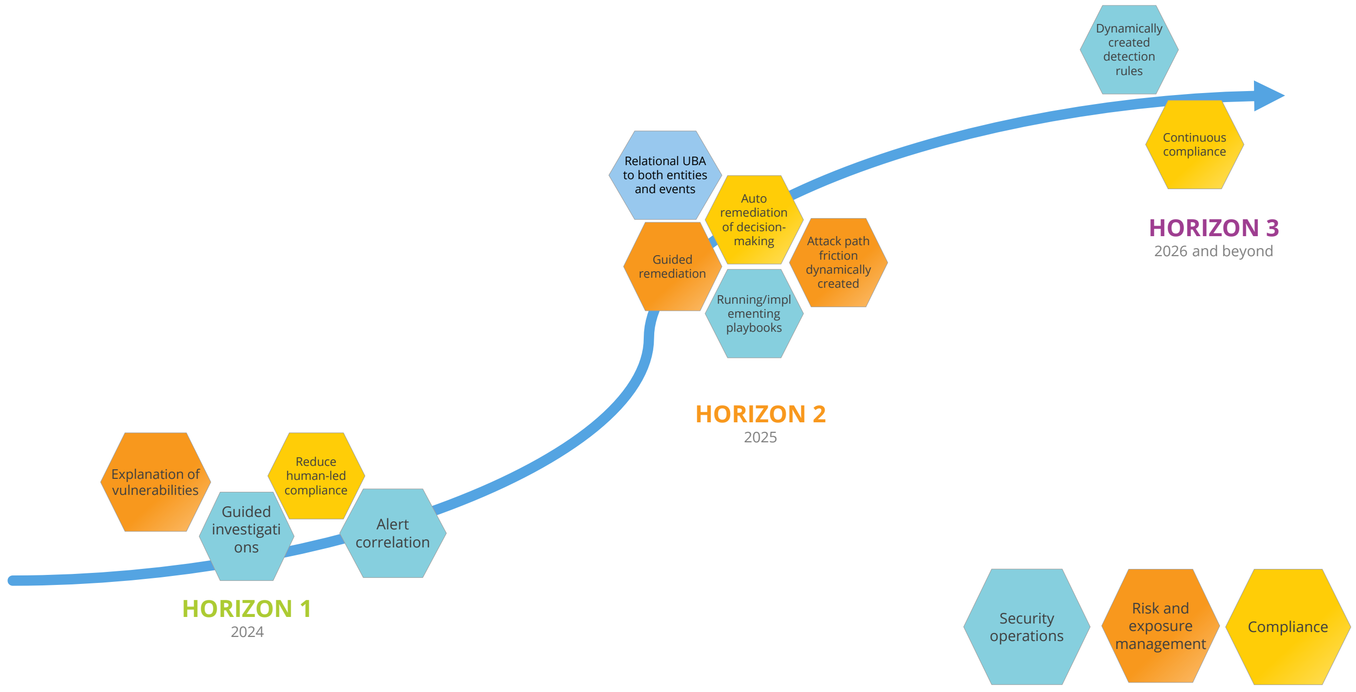
- **Alert correlation:** Adding GenAI capabilities allows for determining if an alert is a false positive and correlating attack path movements with specific threat actor groups.

- **Writing detection rules:** Detection rules encompass behaviors that fall outside baseline expectations or violations concerning access or application use. These rules usually take the form of filters.

- **Guided investigations:** This capability was among the first GenAI applications in cybersecurity. GenAI serves two purposes. The first is the automatic collection of artifacts and metadata, which becomes useful in the case write-up that documents the steps and associated data collected and used during the investigation. The second is the use of natural language processing (NLP) to guide analysts through the investigation process.

- **Running and implementing playbooks:** A playbook is the logical next step after guided investigations. Playbooks are specific to use cases depending on the type of attack (e.g., ransomware, SQL injection). GenAI can be leveraged for threat detection and response to help analysts create response playbooks on data learning models.

FIGURE 2: ***GenAI Adoption in Future Proofing SOCs***


Dynamically created detection rules
Continuous compliance
HORIZON 3
2026 and beyond
Relational UBA to both entities and events
Auto remediation of decision-making
Guided remediation
Attack path friction dynamically created
Running/implementing playbooks
HORIZON 2
2025
Explanation of vulnerabilities
Reduce human-led compliance
Guided investigations
Alert correlation
HORIZON 1
2024
Security operations
Risk and exposure management
Compliance

Source: IDC, 2024

Human Element

While technology is important in modern SOCs, the human element remains critical. As the threat landscape evolves, SOC skills and roles must adapt. Table 1 illustrates key human skills in modern SOCs, emphasizing the need for continuous learning and adaptation in the cybersecurity workforce.

Table 1: ***Most Important Human Skills for a Modern SOC***

Important Human Skills	**Descriptions**
Critical thinking and context	Humans excel at understanding context, making nuanced decisions, and thinking creatively — skills that AI has not fully replicated.
Incident response coordination and leadership	Complex incidents often require human leadership to coordinate responses across multiple teams and stakeholders.

Threat hunting	While AI can assist, skilled analysts are crucial for proactive threat hunting, especially against novel or sophisticated threats.
Stakeholder communication	Explaining complex security issues to nontechnical stakeholders requires human soft skills and judgment.
Strategic thinking	Strategic thinking can help anticipate future threats and technology trends so multiyear road maps for SOC capabilities and maturity can be developed.

Source: IDC, 2024

In addition, soft skills such as teamwork, problem-solving, and continuous learning are crucial across all roles in a modern SOC. The key is finding the right balance of technology and human expertise — whether through insourcing, co-sourcing, or outsourcing — that best fits the organization's needs, resources, and risk profile.

Metrics of Success

Defining the success of a SOC modernization initiative requires comprehensive metrics that extend beyond traditional measures. These metrics should reflect the SOC's efficiency in detecting, responding to, and mitigating threats while aligning with broader organizational and business goals. Key metrics to consider:

- **Operational metrics** measure the SOC's efficiency and effectiveness in identifying threats and limiting potential damage:
  - Mean time to detect measures the average time between the onset of a security incident and the discovery by the SOC.
  - Mean time to respond measures the average time from detection to initial response.
  - Mean time to contain measures the average time from detection to containment of a threat.
  - False positive rate measures the accuracy in threat detection systems (for both known and unknown threats) by tracking the percentage of alerts that turn out to be false alarms.
- **Governance metrics** measure the SOC's efficacy in delivering security outcomes:
  - Automated response rate tracks the percentage of incidents SOC analysts resolve with automated responses, indicating the SOC's maturity in analytics and automation.
  - Incidents handled per analyst measures SOC analysts' efficiency by tracking how many incidents each can address effectively, reflecting the SOC's efficacy in using analytics, AI/GenAI, and automation.
  - Incident recovery time measures how quickly the SOC restores systems to normal operations following an incident.
- **Overall management metrics** measure the integration and results of SOC activities to the overall security posture:
  - Compliance with service-level agreements (SLAs) tracks how often the SOC meets its defined service-level agreements for various incident types.

- System uptime measures the percentage of time the information system is fully operational, related to business continuity and risk management.
- Risk reduction measures the decrease in organizational risk due to SOC activities.

A modern SOC should regularly review and adjust these metrics to ensure they align with evolving threats, technologies, and business objectives.

Considering Tata Communications' Cybersecurity Offerings

Tata Communications is a global provider of communications, connectivity, and security services headquartered in India. It owns one of the largest subsea fiber networks, supporting the internet backbone and carrying about 30% of global internet routes. Tata Communications aims to be a leading provider of cybersecurity services and a one-stop partner for managing cyber-risks globally.

The company's Managed Detection and Response (MDR) provides automated threat detection and response to identify and isolate cyberthreats across the IT, OT, and IoT infrastructure. With a foundation built on proprietary intellectual property, technology partnerships, and over a decade of experience protecting global clients, Tata Communications' Anticipate, Defend, Respond (ADR) methodology enables proactive security measures and supports business continuity in the event of a cyberattack. The platform leverages correlation rules and behavior pattern analysis to analyze network, endpoint, user, and other security logs. The ingested telemetry data, combined with context from the security infrastructure and enriched with commercial and proprietary threat intelligence and research, helps prevent zero-day threats and improves the MTTD and MTTR. Tata's cybersecurity portfolio comprises three pillars of advisory, transform, and manage, including capabilities across endpoints to the cloud, namely:

- Advanced network security including security service edge, DDoS protection services, and perimeter edge security
- Cloud security including cloud-native security and third-party cloud security controls, including data loss prevention, IAM, and CNAPP
- Cyberthreat detection and response including managed and captive security operations center, managed detection and response, threat hunting, managed SIEM, EDR, and NDR services
- Security assessment and consulting services including vulnerability assessment, data discovery and classification, cybersecurity maturity assessment, phishing simulation, and security awareness services
- On-demand premium services like UEBA, attack surface management, breach attack simulation, red teaming, and brand protection to further support the growing security needs of agile businesses

Tata Communications MDR has helped organizations with activities such as:

- Automation of incident response processes for unified visibility against an evolving threat landscape
- Real-time threat detection with indicators of attack that analyze code execution, command and control communications, and lateral movement

- Integrated log monitoring, security analytics, and native SOAR to improve operational effectiveness and efficiency of SOC operations and lower total cost of ownership
- Meeting compliance requirements and carrying out historical log analysis for one year
- Reduction in detection and response time for critical assets to help ensure business continuity
- Stronger security posture with comprehensive visibility and greater experience

Challenges

Stricter security measures mandated by emerging regulatory frameworks continue to shape the cybersecurity field and push vendors to address the challenges organizations face. Tata Communications can push its global ambition and brand recognition more aggressively. Building more successful customer cases or showcasing its compliance readiness services with its MDR solution can be a good starting point.

Conclusion

Modernizing a SOC is not a one-time endeavor, but an ongoing journey. The future success of SOC depends on its ability to evolve continuously, leveraging cutting-edge technologies while nurturing human expertise. By adopting a proactive, intelligence-driven approach, organizations can transform their SOC from a reactive cost center into a strategic asset that contributes to business resilience and growth.

About the Analysts

Cathy Huang, *Research Director, Security and Trust*

Cathy Huang is the research director for IDC's Security and Trust research practice. In her role, she collaborates with other worldwide and regional analysts to develop a set of thought leadership and actionable research for IT buyers and suppliers. Specifically, she develops core research around security consulting, professional security services, and cloud security services within the program. She brings a wealth of security and services expertise and knowledge to the position. She draws on her deep domain expertise across a broad range of ICT segments to support any custom or advisory work with regard to security services.

Craig Robinson, *Research Vice President, Security and Trust*

Craig Robinson is a research vice president within IDC's Security and Trust research practice, focusing on managed security services and integration. Coverage areas include Managed Detection and Response services, Cyber-Resilience, and Incident Readiness and Response services. Craig delivers unparalleled insight and analysis, leveraging his unique practitioner experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

MESSAGE FROM THE SPONSOR

Future-Proof Your SOC: Embrace Modernization

Tata Communications is empowering organizations to modernize their Security Operations Centers (SOCs) with advanced technologies. By leveraging automation, generative artificial intelligence, and real-time threat intelligence, we're helping businesses detect and respond to cyber threats more effectively.

Our threat detection and response platform optimize processes, enhance visibility across security infrastructure, and provide the tools needed to address today's complex cyber threats. This modernization enables organizations to protect critical assets, improve response times, and utilize resources more efficiently. Tata Communications is helping businesses become more resilient in the face of evolving cyber threats.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com