

Organizations are reimagining security operations by embracing unified SNOC approaches, leveraging GenAI capabilities, and adopting integrated platforms that build on existing IT/network expertise while enabling effective security operations despite resource constraints.

How Organizations Are Reimagining Security Operations with Limited Resources

March 2025

Questions posed by: Cisco

Answers by: Cathy Huang, Research Director, Security Services Worldwide

Q. What challenges do organizations with limited dedicated security expertise face?

A. In today's environment, cybersecurity has become increasingly critical to organizational success. However, a significant challenge emerges in how organizations approach this vital function, particularly when they lack dedicated security teams and leadership positions or struggle with staffing key security roles.

The reality for many organizations is that cybersecurity responsibilities often fall to IT or network leaders, who must manage security alongside their primary operational duties. Although these professionals excel in maintaining system availability and network performance, security requires a fundamentally different mindset — one focused on threat anticipation, risk management, and constant vigilance against evolving threats. Moreover, security operations demand constant attention across multiple time-intensive activities: 24 x 7 alert monitoring and response, extensive documentation, regular tool maintenance and updates, and stakeholder communication.

On top of that, the security field's rapid evolution demands constant learning about new threats, compliance requirements, and security tools, adding another layer of complexity to leaders' already full plates. IT and network professionals must shift from a service enablement perspective to one that sometimes requires restricting access or implementing controls that may impact user experience. This shift can be particularly challenging for teams historically focused on optimizing system performance and user accessibility.

A noteworthy nuance in this scenario is the emergence of "solo security practitioners" — individuals or small teams dedicated to security but lacking dedicated security leadership. These practitioners face the unique challenge of effectively communicating upward to non-security leadership and across various organizational functions. Their success often hinges on their ability to translate complex security concepts and requirements into languages that resonate with business leaders and other stakeholders.

Q. How are modern platforms bridging the security expertise gap?

A. The cybersecurity landscape presents significant challenges for organizations lacking dedicated security expertise. These organizations often struggle to effectively combat sophisticated cyberthreats, having response mechanisms that tend to be more reactive than proactive. This reactive posture can lead to missed early warning signs that security specialists would typically identify and address. Today's adversaries are also leveraging AI to enhance their attack capabilities. These AI-powered attacks can learn from defense responses and modify their techniques in real time, creating a new class of intelligent, persistent threats that traditional security measures find difficult to counter.

Modern solutions, such as extended detection and response (XDR) solutions, have emerged as a transformative force in this context. As the central nervous system of security operations, these platforms integrate diverse security tools and data sources into a coherent ecosystem. This integration is crucial for organizations with limited security expertise, as it provides a unified interface that simplifies complex security operations.

The power of these security tools lies in their ability to aggregate and correlate data from multiple sources, from network devices, user identities, applications, and endpoints to email systems and cloud services. This comprehensive data collection and correlation enables organizations to maintain a holistic view of their security posture even without deep security expertise on staff. Instead of juggling multiple security tools and interfaces, teams with security responsibilities — think dedicated security or IT/network teams — can operate with streamlined workflows, reduced training overheads, and minimized configuration errors from managing disparate systems.

Most importantly, the industry is witnessing the emergence of unified platforms that align with existing team strengths while serving multiple operational needs. This evolution is particularly valuable for organizations with limited dedicated security resources, as it allows them to leverage their existing operational expertise while enhancing their security capabilities. These platforms effectively bridge the gap between traditional IT operations and security requirements, enabling more efficient and effective security management.

Q. How is generative AI (GenAI) transforming security operations for different organizational personas?

A. The integration of GenAI into security operations represents a significant evolution in how organizations approach cybersecurity challenges. GenAI is playing a crucial role in bridging expertise gaps, automating routine tasks, and facilitating collaboration among team members — enhancing security operations' efficiency, accuracy, and scalability.

According to IDC's August 2024 *Future Enterprise Resiliency and Spending Survey, Wave 8*, cybersecurity professionals have identified clear priorities for GenAI use cases in security. The top-ranked use cases include (in order of importance):

- » Summarizing security incidents
- » Writing detection rules for security operations
- » Running and implementing playbooks

What makes this data particularly fascinating is how different organizational personas prioritize these GenAI use cases. Perhaps the most revealing insight from the survey is the stark contrast in the ways different teams prioritize security impact analysis. IT management and infrastructure professionals place a significantly higher emphasis on security impact analysis, ranking it a top priority (20% and 21% of respondents, respectively). In contrast, cybersecurity professionals ranked it as their second-lowest priority (11%).

This disparity illuminates fundamental differences in operational priorities: IT management/infrastructure teams aim to understand the operational impact before acting, while security teams are trained to respond first through established incident response protocols and playbooks.

These findings have important implications for modern XDR solutions, particularly in how they approach incident prioritization scoring and blast radius assessment. The varying priorities across organizational roles underscore the need for security solutions that can accommodate multiple operational perspectives while maintaining effective security measures. As GenAI evolves, its ability to support these diverse operational needs while facilitating collaboration between different teams becomes increasingly vital.

Q. Why is the combined security and network operations center (SNOC) approach relevant?

A. The emergence of the security and network operations center represents a strategic evolution in how organizations manage and secure their IT operations. This unified operational model merges traditional network operations with security functions, offering a practical approach to common challenges such as limited cybersecurity expertise and suboptimal visibility across systems.

The SNOC approach is particularly valuable in resource-constrained environments in which organizations operate with minimal dedicated security staff or limited security expertise. By combining network operations with security functions, organizations can maximize their limited resources while maintaining comprehensive coverage of both operational and security needs. This integration proves especially beneficial for organizations where IT teams must handle networking and security responsibilities.

This model's effectiveness stems from its ability to leverage existing strengths. IT teams can build on their established IT/network expertise while gradually expanding their security capabilities. This natural progression allows organizations to enhance their security posture without requiring a complete operational overhaul or significant additional resources.

The practical benefits of the SNOC approach manifest in several ways. For example, when investigating a potential security incident, teams can immediately correlate security alerts with network performance data, leading to faster and more accurate incident triage. The SNOC model delivers greater efficiencies through integrated tools and workflows. Instead of switching between multiple systems and dashboards, teams can monitor and manage network and security events from a unified interface. This integration improves operational efficiency and enhances the team's ability to detect and respond to threats that might otherwise go unnoticed when viewing network and security data in isolation.

Q. What does the future hold for security operations?

A. As traditional boundaries between IT, network, and security operations continue to blur, this convergence trend is reshaping the threat detection and response market, driving new requirements for solution design and functionality. Future XDR solutions must evolve to meet several critical requirements:

- » First, they must offer seamless integration with existing tools, regardless of vendor, eliminating the complexity that often hampers adoption and effectiveness.
- » Second, these solutions must provide enhanced operational visibility, giving teams a comprehensive view of their environment.
- » Third, and perhaps most important, they should enable teams to leverage their current skills for security purposes, reducing the learning curve and maximizing resource utilization.

A key aspect of future solutions will be their ability to provide guidance that fills capability gaps while delivering secure outcomes. This becomes particularly crucial as organizations continue to operate with limited dedicated security expertise.

These future-focused characteristics align naturally with broader industry trends, such as the rise of zero trust architectures and universal zero trust network access (ZTNA). The growing importance of identity context and the strategic use of AI and automation are central to the evolution of security and network operations. Organizations that successfully embrace this evolution will not only enhance their security posture but also create more resilient and adaptive operational models.

The future of security operations lies not just in new technologies but in the seamless fusion of people, processes, and technology — where AI augments human expertise, automation enhances efficiency, and integrated platforms enable diversified teams to stay ahead of the evolving threats.

In summary, key areas for reimagining security operations are the following:

- » Developing integrated training programs that blend network and security skills
- » Establishing shared KPIs across network and security operations
- » Creating unified workflows across network and security tasks
- » Focusing on unified platforms with operational and security visibility
- » Automating routine tasks to maximize limited resources and speed responses
- » Leveraging GenAI for guidance, decision-making, and communication support

About the Analyst



Cathy Huang, Research Director, Security Services Worldwide

Cathy Huang is the research director for IDC's Security Services Worldwide research practice. In her role, Cathy 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 managed security services, security consulting, and integration services within the program. She also incorporates IDC's Future of Trust and other FoX agenda to drive new research such as cloud security services and secure edge services for the program.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)