SANS

Analyst Program

Custom Survey

Modernizing Security Operations

Written by **TJ Banasik**

January 2022

ExtraHop

Abstract

Security operations are the epicenter of the cybersecurity industry. SecOps is where the metaphorical rubber meets the road for organizations defending their enterprises. Security governance, risk, and compliance (SGRC), security application development, security engineering, and all respective cybersecurity functions overlap to enable security operations centers (SOCs) to respond to threats. These teams sit the line 24/7, through nights, weekends, and holidays, to defend today's enterprises. Yesterday's SecOps was grounded in perimeter-based approaches to secure data inside an organization. The pandemic has created a technological revolution driving businesses to the cloud and evolving IT policies to support globally distributed and remote workforces. The threat has capitalized on this growth and change in business, which drives our need to mature SecOps programs. A mature SecOps team operates with measurable service level agreements, constantly learning from adversaries and proactively mitigating threats. Growing SecOps doesn't just mean getting better at defending; it means modernizing with evolving people, processes, and technologies.

Executive Summary

The pandemic has created a technological revolution driving businesses to the cloud and evolving IT policies to support globally distributed and remote workforces. Cyber attackers have capitalized on this growth and change in business, which drives our need to mature SecOps programs. This survey's primary goal is to better understand how customers think about modernizing security operations—not just getting better at defending. Survey collection of customer data included three generalized areas (demographics, SecOps architecture, and SecOps priorities) and was designed to understand dynamics including:

- Fundamental dynamics (people, processes, technologies) for SecOps
- Key investments in maturing SecOps
- Tradeoffs in augmenting the workforce with security orchestration, automation, and response (SOAR)
- Most effective measures for defending against cyber threats
- Security tools for validation of organizational security posture
- Threat detection/response integration with SecOps workflows

Key Findings

- **Cyber staffing shortages are the overarching challenge evident in almost all survey responses.**
- **Respondents report a disconnect between stakeholder understanding of breach impacts and desired response/resolution timeframes, meaning that resourcing doesn't align with expectations and that impacts become more significant.**
- **The SecOps industry cannot secure data with the available workforce, and SOAR, while complementary to SecOps functions, isn't effective in augmenting cyber staffing shortages.**
- **Because SecOps demands strain retention rates, most of the cybersecurity workforce is mid-junior level.**
- **SecOps modernization shows a pattern of migrating toward emergent capabilities such as network detection and response (NDR) and cloud workload protection platforms (CWWPs), and technological integration is key to these strategies.**
- **Organizations often identify compliance as a secondary SecOps concern, but it's a primary driver for requirements.**

Respondents and Their Environments

The SANS 2021 survey gathered responses from 142 respondents, with the demographics shown in Figure 1.

Top 4 Industries Represented

- Technology
- Banking and finance
- Healthcare
- Government

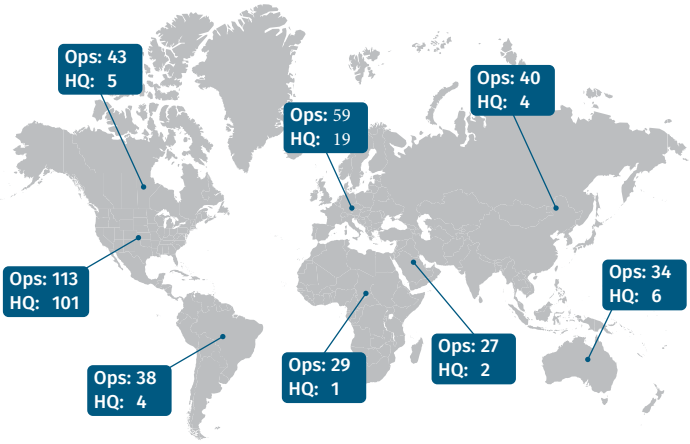
Each gear represents 5 respondents.

Organizational Size

- **Small** (Up to 1,000)
- **Small/Medium** (1,001–5,000)
- **Medium** (5,001–15,000)
- **Medium/Large** (15,001–50,000)
- **Large** (More than 50,000)

Each building represents 5 respondents.

Operations and Headquarters



Top 4 Roles Represented

- **Security administrator/ Security analyst**
- **Security manager or director**
- **Security architect**
- **System administrator/ System analyst**

Each person represents 5 respondents.

Figure 1. Key Demographic Information

State of Security Operations

SecOps leverages personnel, processes, and tools to promote measurable results in securing infrastructure and business processes.[1] SOCs provide 24x7x365 monitoring of security events and alerting. Running of security operations programs includes using and maturing fundamental dynamics, including people, processes, and technologies. Respondents noted cybersecurity workforce shortage, strict industry compliance regulations, and evolving technology as prevalent challenges. Maturing SecOps requires a detailed understanding of quantifying metrics, including performance SLAs such as mean time to respond and mean time to recover from security incidents. These performance evaluations align with the key dynamics of people, processes, and technology, so the maturity of these processes is often more of an art than a

[1] "MGT551: Building and Leading Security Operations Centers," www.sans.org/cyber-security-courses/building-and-leading-security-operations-centers/

science. The rapid evolution of technology produces more signals for a cyber analyst to evaluate, driving requirements for automation. SOAR leverages respective automation for the machine-driven performance of manual tasks such as creating a ticket for a commodity malware incident. Can automation replace and augment shortages in the cybersecurity workforce? Because various employments of security operations models exist, understanding the dominant trends helps security analysts design SecOps programs. SOCs support organizations across multiple support models depending on organizational policy, resourcing, and business requirements:

- **Onsite staff—**Information technology professionals support cross-functional security requirements without a dedicated security team (common in smaller organizations without stringent security compliance requirements).
- **Local SOC—**A single organization-hosted SOC supports all security-monitoring functions for an organization (often aligned with 24x7 shift-work configurations).
- **Global SOC (GSOC)—**A combination of multiple regional-based SOCs often align to geographic distribution in follow-the-sun models.
- **Managed security service provider (MSSP)—**Provides security monitoring as a service remotely. Many MSSPs are moving toward coupling security services with respective security product offerings.

Selection and employment of cybersecurity tooling arguably represents the most critical element to maturing SecOps programs. Exploration of industry trends in tooling and processes provides additional perspectives for evaluating the efficiency of capabilities. In addition, various types of security products align with security functions and requirements. This list focuses on the most general categories, without being all-encompassing because of the numerous specialized security products. Many product types include a combination of functions such as network detection and response (NDR), which both complements and goes beyond the capabilities of security information and event management (SIEM) and endpoint detection and response (EDR) for extended detection and response (XDR):[2]

- **NDR—**A category of security solution that monitors and analyzes network traffic in the cloud and on-premises, detects threats using AI/ML, and provides investigative and response capabilities. NDR products deliver visibility and coverage into areas of the attack surface invisible to SIEM and EDR tools.
- **EDR—**An endpoint security solution combining anti-malware with response-driven capabilities supporting proactive response.
- **SIEM—**Solutions that aggregate security log collection across multiple sources for security analysis and visualization, including incident management, dashboards, and reporting. SIEM technology supports threat detection, compliance, and security incident management through collection and analysis capabilities.[3]

---

[2] "Network Detection and Response (NDR) Vs. Extended Detection & Response (XDR)," August 7, 2020, www.extrahop.com/company/blog/2020/ndr-vs-xdr/

[3] "Security Information and Event Management (SIEM)," Gartner, www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

- **CWPP—**Provides visibility, hardening, and vulnerability management for cloud-based workloads.
- **Cloud security posture management (CSPM)—**Automates cloud security posture in a risk-based approach while identifying and remediating cloud-based vulnerabilities.
- **Vulnerability management—**A security control designed to identify security vulnerabilities and misconfigurations while driving remediations to reduce the attack surface.
- **Cloud access security broker (CASB)—**Consolidates security logging for correlations and insights across numerous cloud-delivered applications.
- **Data loss prevention (DLP)—**Encompasses a multitude of technologies designed to identify, monitor, and secure data content via detection and policy-based controls.
- **Secure web gateway (SWG)—**Technologies designed to secure web traffic and user browsing and to mitigate malware callbacks.
- **Unified threat management (UTM)—**A network-based control category including firewall, intrusion prevention, and various threat-detection capabilities.

SecOps Challenges

The SANS 2021 Modernizing Security Operations survey's first focus area involves understanding SecOps challenges. Questions include understanding top challenges, the average experience of SecOps personnel, incident response/recovery timeframes, and the most significant SecOps concerns. The results demonstrate that 62% of organizations struggle with staffing cyber roles, 57% cite challenges in cybersecurity complexity, and slightly more than 50% of respondents reported difficulties in cost. Cyber talent acquisition is the primary challenge driving respondents toward outsourcing cyber functions with MSSPs. Data growth, technological changes, and compliance requirements make it challenging to maintain adequate cyber talent/resourcing due to both complexity and cost of maintaining these capabilities (see Figure 2).

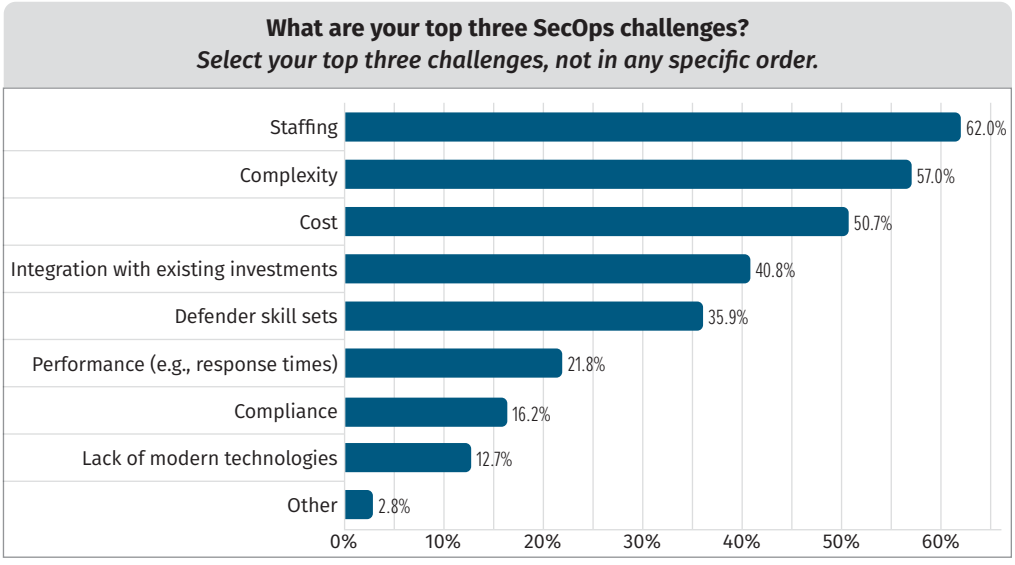


Figure 2. Top 3 SecOps Challenges

To better understand the challenges with staffing the cybersecurity workforce, we asked our survey respondents the average experience level of SecOps team members. Sixty-four percent of the respondents report SecOps personnel are professionals with 5 years or less of experience and with just slightly under half being mid-level professionals with between 3 and 5 years of experience (refer to Figure 3). The cybersecurity discipline and organizational needs have outgrown the talent market. Retention of cyber personnel complicates this dynamic as SecOps personnel are often required to work extended shifts across nights, weekends, and holidays while performing complex tasks under stressful circumstances. Cyber professionals will often endure the strain of SecOps work at the start of their careers, but most do not want that to define their career long term. Our survey results support this fact, showing that 9% or less of SecOps professionals have 10+ years in the field. Many SecOps professionals move on to other cyber disciplines, such as engineering, architecture, compliance, etc.

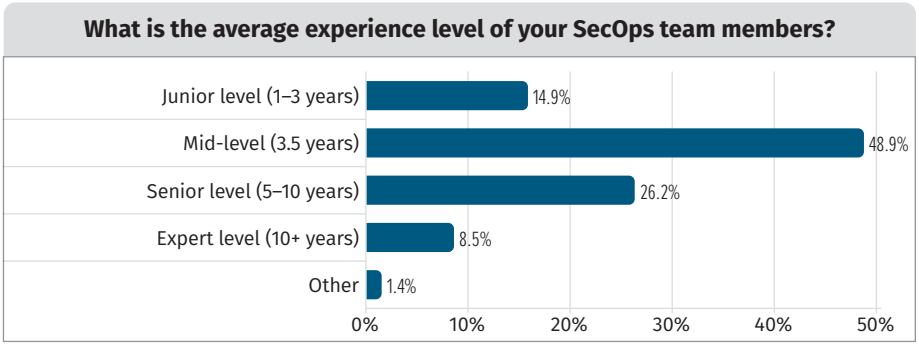


Figure 3. Average SecOps Analyst Experience

What is the average response time for a high severity incident, and what are the biggest challenges in this response? Over 67% of our survey respondents reported response times of 1 hour or less. Interestingly, over 80% of respondents noted the average resolution/remediation time to recover from high severity incidents is 3 days or less (see Figure 4).

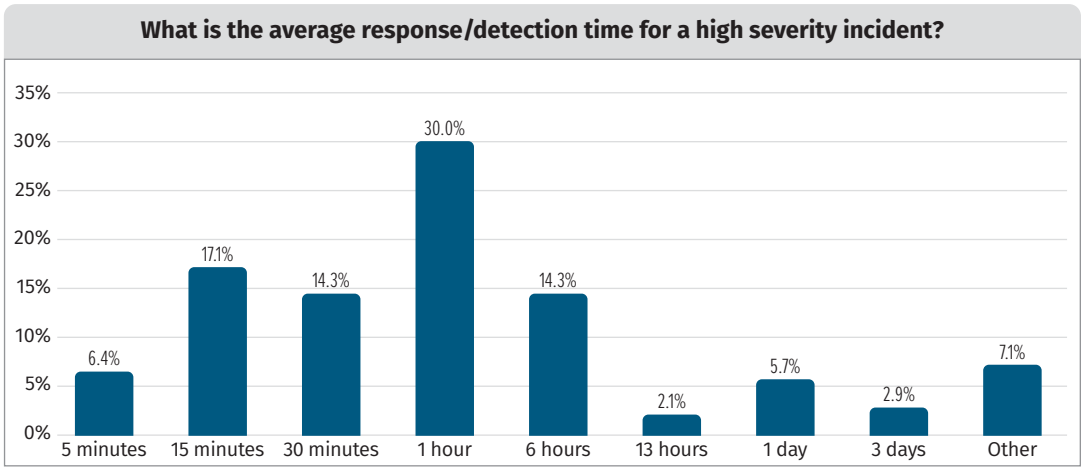


Figure 4. Average Response Time (High Severity Incident)

The comparison of these two data points highlights the noted SecOps challenges in both personnel shortages and complexity. A SecOps analyst is required to detect and respond to a high severity incident within an hour. The respective workflow involves an average of 3 days to investigate, remediate, and report (see Figure 5).

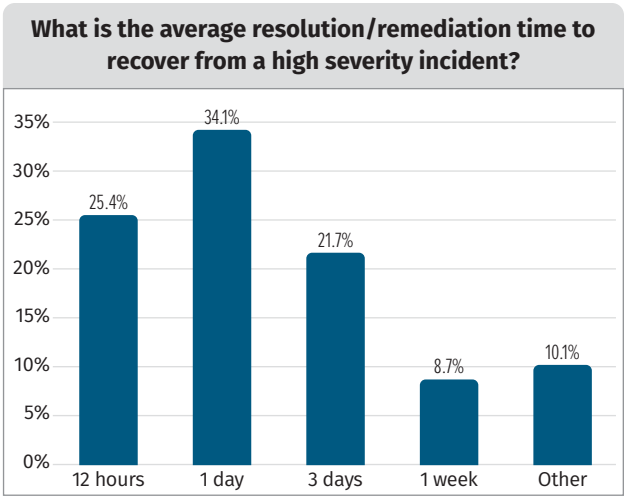


Figure 5. Average Resolution Time (High Severity Incident)

What are the significant SecOps issues or concerns? Our respondents reported that staffing and workforce (61%), visibility and control over sensitive data (49%), and phishing/commodity malware (49%) are the most significant areas of concern (see Figure 6). These findings again highlight a common pattern with concerns of staffing shortages in the cybersecurity workforce. High-volume phishing and commodity malware challenge these dynamics because they're often some of the most common security incidents observed in SOCs. An interesting observation is that compliance and performance are secondary in concerns, but later questions highlight these areas as primary SecOps drivers.

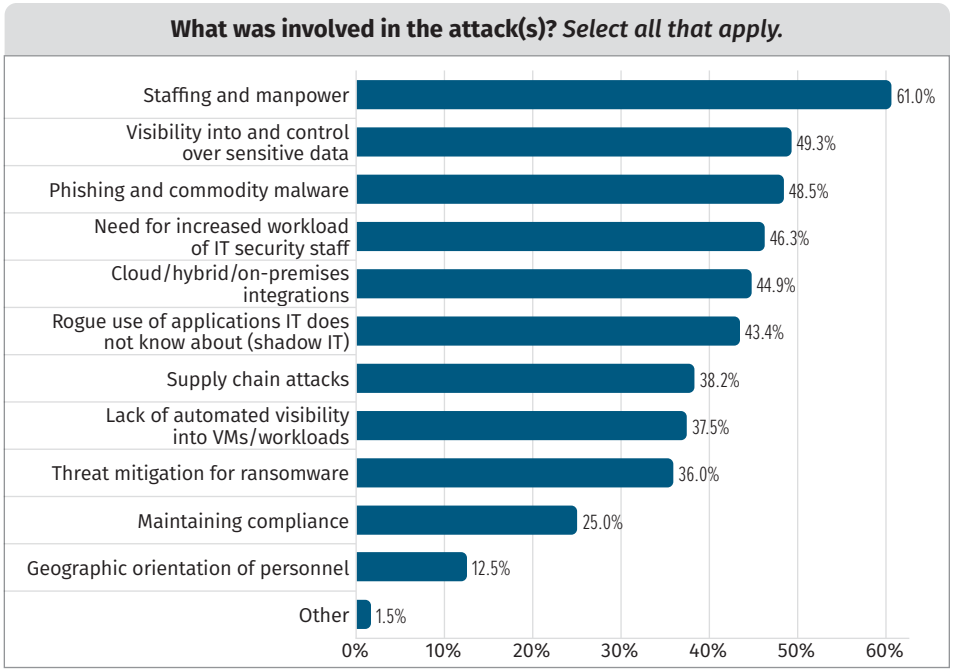


Figure 6. Biggest SecOps Model Concerns

Requirements, Drivers, and Assessment

The SANS 2021 Modernizing Security Operations survey's second focus area involves understanding SecOps requirements, drivers, and assessment. Questions include SecOps risk-mitigation perspectives, SecOps strengths/weaknesses, breach preparedness, and incident recovery timeframes. The results demonstrate that incident response (34%) and automation (15%) are listed as the greatest SecOps strengths, although 30% of respondents also noted automation as one of their SecOps program's most significant weaknesses (see Figure 7). These findings indicate that SOAR can increase the efficacy of existing staff but can't replace staffing entirely.

Figure 7. SecOps Strengths and Weaknesses

Do you believe that your organization's SecOps effectively mitigates organizational risk? Sixty-one percent of respondents agree, while the other 39% disagree, are unsure, or decline to answer (see Figure 8). A disconnect seems to exist between suitable risk mitigation and desired state. Most respondents think they've effectively mitigated risk, but as for the SecOps functions central to strategy question comments, few respondents communicated satisfaction with their SecOps maturity.

Next, we asked to what extent respondents feel comfortable with their organization's ability to withstand a major breach? While 80% answered favorably (i.e., comfortable or above), these findings indicate an observed mismatch between risk mitigation, desired state, and program maturity questions because responses to questions regarding SecOps functions aligned with strategy (current, 12 months, 3 years) didn't align with this perspective (see Figure 9).

To further understand perspectives in SecOps risk mitigation and compliance alignment, we asked respondents to what extent their business understands the impact of a major breach. The findings demonstrate that 7 out 10 is the most common score, indicating that most organizations have a well-developed understanding, but not perfect, of the impact of a major breach (see Figure 10). Respondents reported several interesting perspectives as influencing this score, including a lack of understanding of risk due to intangible elements, lack of user awareness, and lack of breach reducing the priority of organizational resourcing.

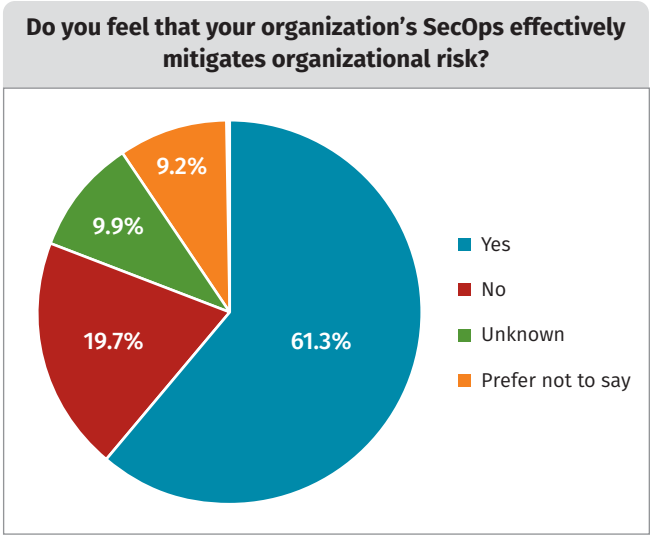


Figure 8. SecOps Risk Mitigation

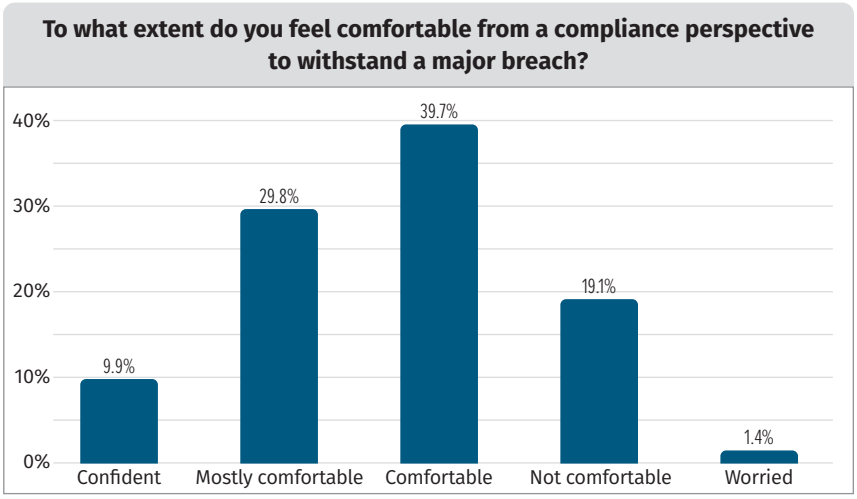


Figure 9. Breach Resilience from Compliance Perspective

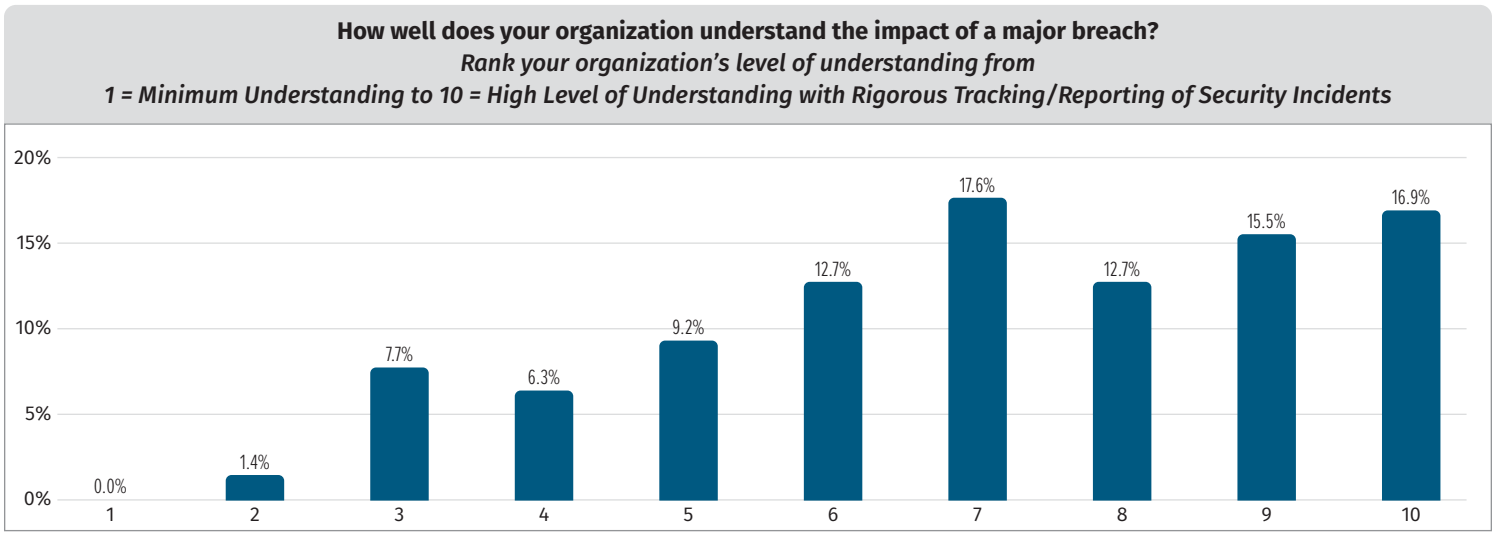


Figure 10. Breach Impact Understanding

We followed this question with another to understand the average mean downtime a business is willing to accept during a high severity incident, such as a ransomware attack. Twenty-four percent of the respondents reported 6 hours, 20% reported 24 hours, and 13% reported 1 hour as the most common acceptable downtimes (see Figure 11). The SecOps functions central to strategy question comments showed multiple respondents listing resourcing/budgetary concerns as factors influencing SecOps maturity roadmaps. The findings highlight that stakeholder expectations of downtime don't align with understanding the threat of budgetary/resourcing commitments.

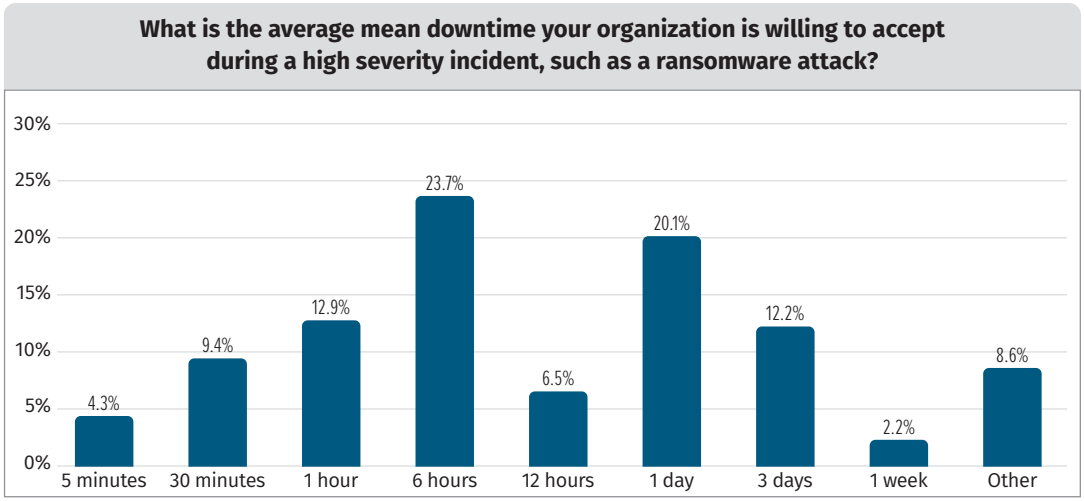


Figure 11. Average Acceptable Downtime from Security Incident

While the threat landscape is vast and complex, our respondents strongly agreed that ransomware and phishing are the biggest threats to organizations (see Figure 12). These perspectives highlight that victim-oriented threats, lack of end-user training, and disclosable breach events raise the biggest organizational concerns.

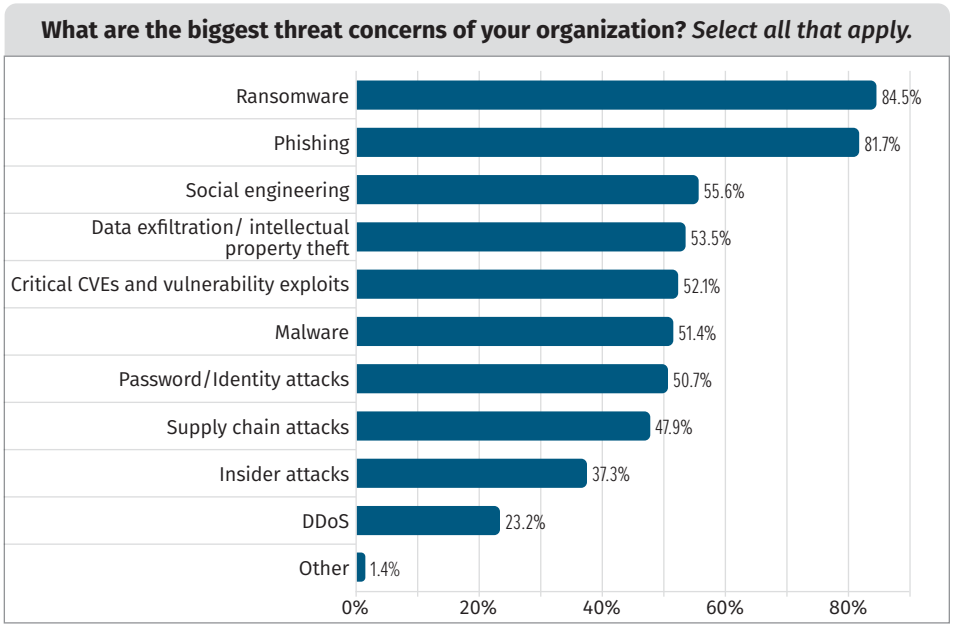


Figure 12. Greatest Threat Concerns

The SANS 2021 Modernizing Security Operations survey's third focus area involves incident response and compliance frameworks. Over 82% of respondents report using the NIST model for incident response, demonstrating an industry trend in the selection/efficiency of incident response models (see Figure 13).

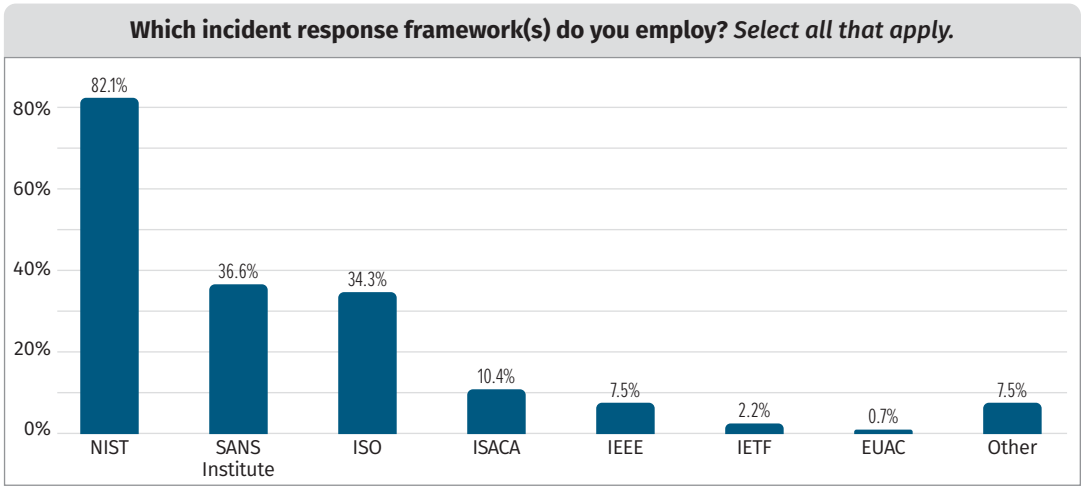


Figure 13. Incident Response Frameworks

Next, we asked which compliance regulations and standards are driving their

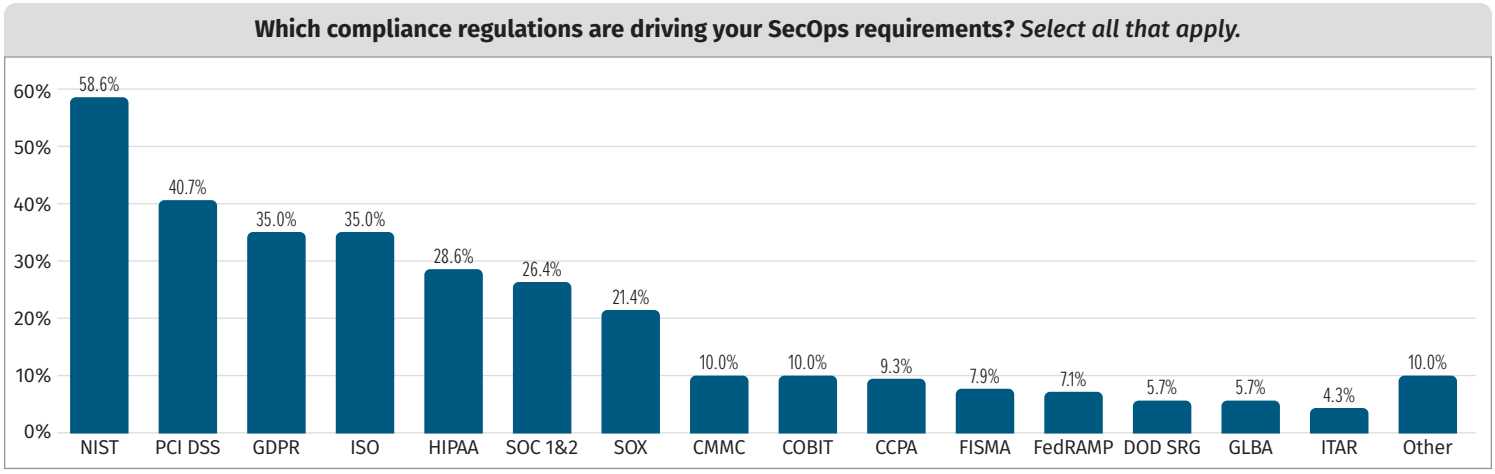


Figure 14. Compliance Drivers

organizational SecOps requirements. Again, as shown in Figure 14, respondents report NIST (59%) as the dominant driver, followed by PCI DSS (41%), and GDPR (35%). Our findings indicate that cybersecurity compliance enforced with potential financial penalties is one of the most influential drivers. GDPR and PCI DSS have some of the strictest consequences for noncompliance.

Threat modeling was another area of focus in this category. Sixty-six percent of respondents report they are either not using threat modeling or are unsure.

As shown in Figure 15, of the remaining 47% using threat modeling, 88% reported using MITRE ATT&CK® as the dominant framework over the Lockheed Martin Cyber Kill Chain® (29%) and STRIDE (19%).

The SANS 2021 Modernizing Security Operations survey's fourth focus area involves SecOps tooling and technologies (see Figure 16). When asked about the strongest/weakest tools for SecOps, respondents reported EDR (44%) and SIEM (19%) as the strongest tools. Respondents reported forensics (24%) and CWWPs (19%) as the weakest tools."The dominant trends indicate trending toward EDR, NDR, and SIEM. Respondents seem to find emergent tools such as CWWPs or more complex tools such as forensics offerings as less effective. The findings indicate a migration from traditional to more cloud-based/integrated tooling suites. Respondents noted budget shortages, digital

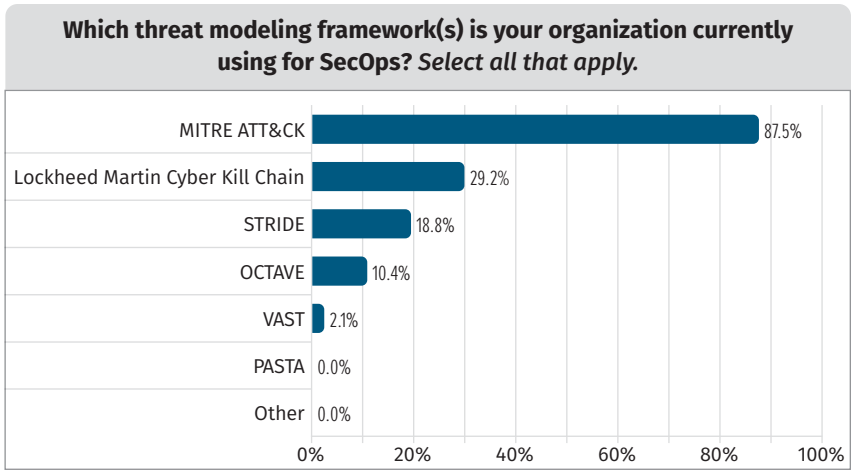


Figure 15. Threat Modeling Frameworks

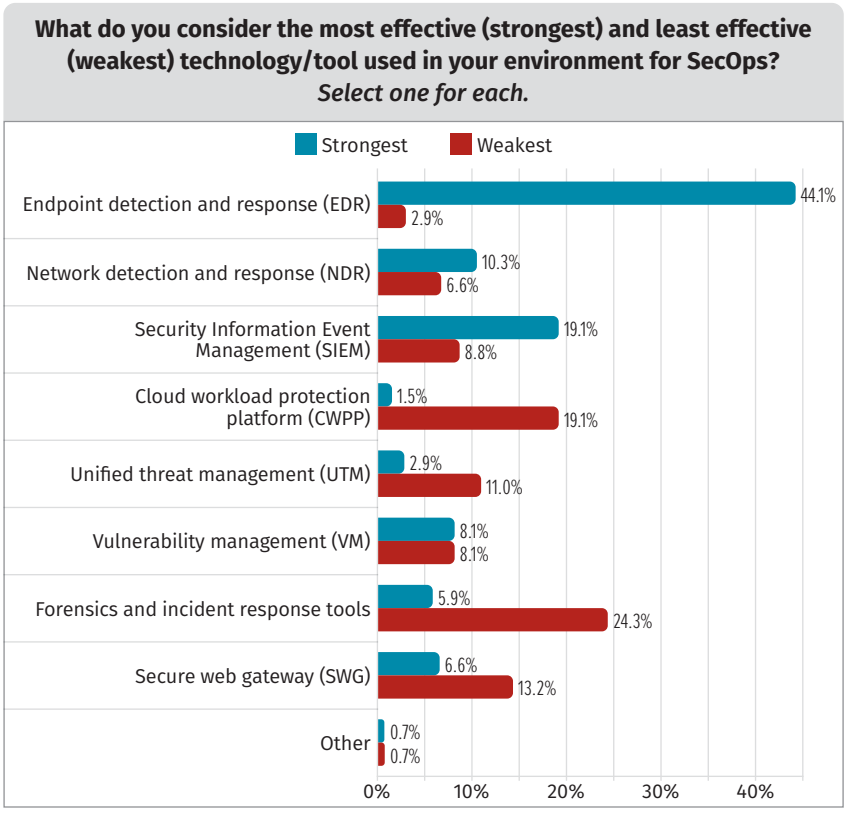


Figure 16. Most/Least Effective Security Tools

transformation to cloud, remote-work cultural changes, and the need to mature programs/technologies as the dominant driving factors.

The SANS 2021 Modernizing Security Operations survey's final focus area addresses the future state of SecOps. Questions include technologies and functions key to modernizing SecOps. We asked: *Which SecOps technologies are currently central to your SecOps strategy? What do you envision as your desired state of technologies over the next 12 months? Next 3 years?* As shown in Figure 17, respondents reported EDR (84%), SIEM (75%), vulnerability management (72%), and NDR (57%) as the most central to current SecOps. Responses for 3-year plans highlighted data loss prevention (30%), CWWPs (29%), and NDR (30%). Respondents noted budgetary constraints, compliance requirements, and immature SecOps programs as the primary drivers. Interestingly, NDR scored the highest in strategy for both current and future roadmaps, indicating customer satisfaction in the capability as a future state.

To better understand these dynamics, we asked respondents: *Which SecOps functions are most central to your SecOps strategy? What do you envision your desired state of functions over the next 12 months? Next 3 years?* Respondents report security incident response (82%), vulnerability management (73%), and intake and monitoring (70%) as the most central current functions (see Figure 18). Respondents' future states lean toward cloud security, threat intelligence, and security application development as the dominant trends.

Lastly, we asked our respondents about their

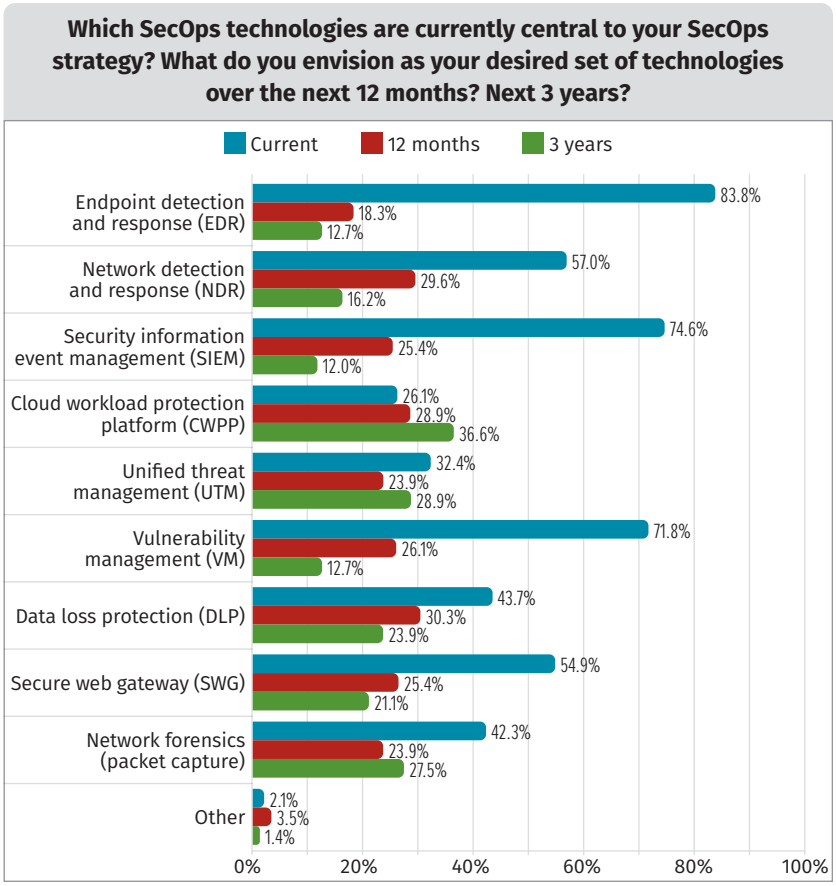


Figure 17. Central SecOps Tooling

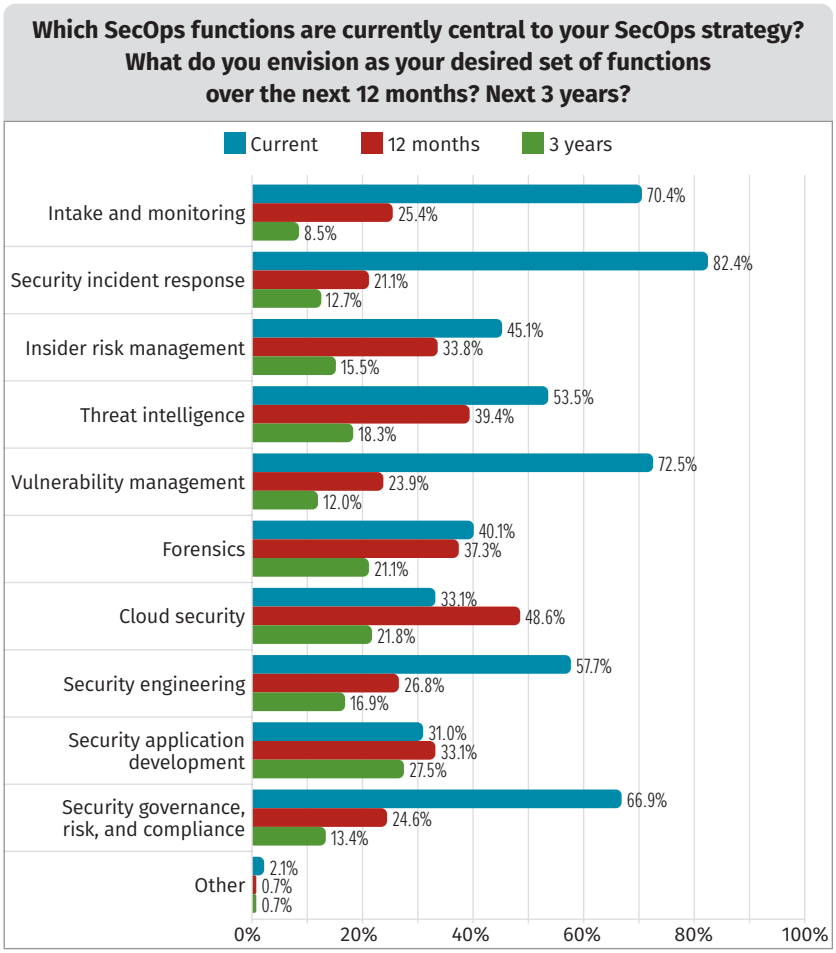


Figure 18. Primary SecOps Functions

current and future states for SecOps management and monitoring. Local onsite staff (84%) and localized SOC (53%) were the most prevalent current states, while global SOCs and MSSPs were the most prevalent in the 1- and 3-year strategies (see Figure 19). The movement from onsite staff to distributed global and managed security service providers reinforces respondents' biggest cybersecurity challenge of staff shortages. Findings and driving factors indicate that cyber talent acquisition, training, and retention approaches are driving respondents toward consolidated/outsourced SecOps approaches.

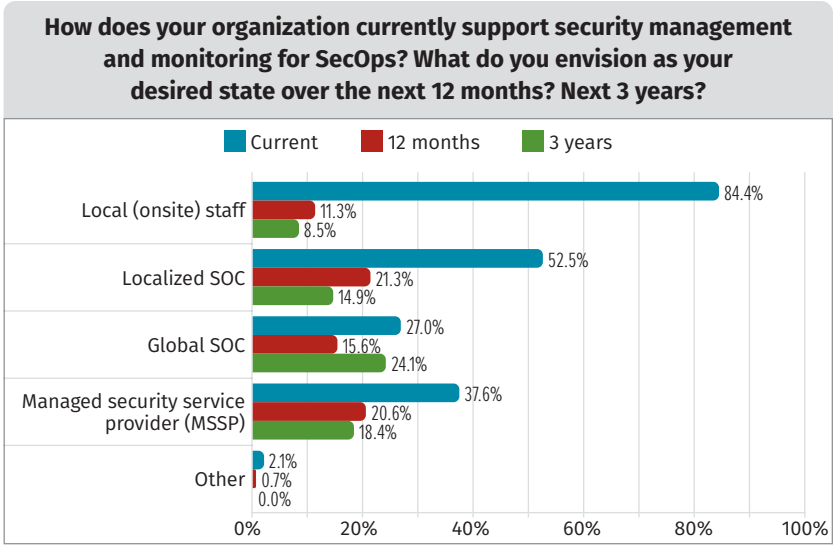


Figure 19. SecOps Management and Monitoring Models

Conclusion

The pandemic has created a technological revolution driving businesses to the cloud and evolving IT policies to support globally distributed and remote workforces. The threat has capitalized on this growth and change in business, which drives our need to mature SecOps programs. Cyber staffing shortages are the overarching challenge evident in almost all survey responses. The SecOps industry cannot secure data with the available workforce, and SOAR, while complementary to SecOps functions, isn't effective in augmenting cyber staffing shortages. A driving need exists for artificial intelligence and machine learning to boost analytical procedures and help humans scale their analytical functions better. Because SecOps demands strain retention rates, most of the cybersecurity workforce is mid-junior level. SecOps modernization shows a pattern of migrating toward emergent capabilities such as NDR and CWWPs, and technological integration is key to these strategies. Respondents report a disconnect between stakeholder understanding of breach impacts and desired response/resolution timeframes, meaning that resourcing doesn't align with expectations and that impacts become more significant. SecOps risk mitigation is acceptable, although all but MSSPs describe not being in the desired state with needs for both growth and maturity. Victim-initiated threats demonstrate a lack of end-user awareness, and fears of disclosure breaches prioritize concerns. Respondents indicated compliance as a secondary SecOps concern, but it's a primary driver for requirements. Industries must direct strict non-compliance penalties to ensure cybersecurity posture because these consequences drive better stakeholder understanding of impacts and commitment of resources.

Sponsor

SANS would like to thank this paper's sponsor: