ESG SHOWCASE

What Security Pros Want for Threat Detection and Response

Date: October 2022 **Author:** Jon Oltsik, Senior Principal Analyst and Fellow

ABSTRACT: Security operations are challenging and getting harder all the time, but when security pros seek help from the security technology industry, they often get confusing messages and false promises. ESG research reveals what SOC teams want in a threat detection and response platform. Vendors like Stellar Cyber provide solutions that truly align with these requirements.

Organizations Face an Assortment of Security Operations Challenges

Security operations are vital for protecting critical assets, detecting/responding to threats, and managing cyber-risks. Yet, security operations don't come easily. According to recently published ESG research, many organizations face a multitude of common security operations challenges, such as (see Figure 1):[1]

- Constant firefighting. Just over one-third of security professionals admit that their security operations team spends most of its time addressing emergencies, leaving little time for strategy or process improvement. This type of constant firefighting cannot scale, while a high-stress work environment tends to burn out the SOC team. Nothing good can come of this situation.

- An expanding attack surface. One-third of security pros say that their security operations team is challenged to manage and monitor security across a growing attack surface. This is a real problem—previous ESG research reveals that 67% of organizations claim that their attack surface has grown over the past few years, driven by third-party IT connections, the need to support remote workers, cloud-native application deployment, and SaaS implementation.[2] For security operations, a growing attack surface means more assets, vulnerabilities, alerts, and work. Thus, the inability to monitor and manage a growing attack surface increases cyber-risk.

- Operationalizing threat intelligence. This involves using raw threat information for blocking indicators of compromise (IoCs), uncovering gaps in security defenses, monitoring adversary behavior, and aligning threat feeds with the MITRE ATT&CK framework. Regrettably, operationalizing threat intelligence requires advanced skills, formal workflows, and technology integration. Many security teams lack the appropriate budgets, staff, and skills to accomplish these goals.

- Too many manual processes. Security operations often depend upon individual skills or tribal knowledge rather than formal automated processes. Manual processes don't scale, however, limiting the speed and scale of the SOC.

[1] Source: ESG Complete Survey Results, *SOC Modernization and the Role of XDR*, September 2022.

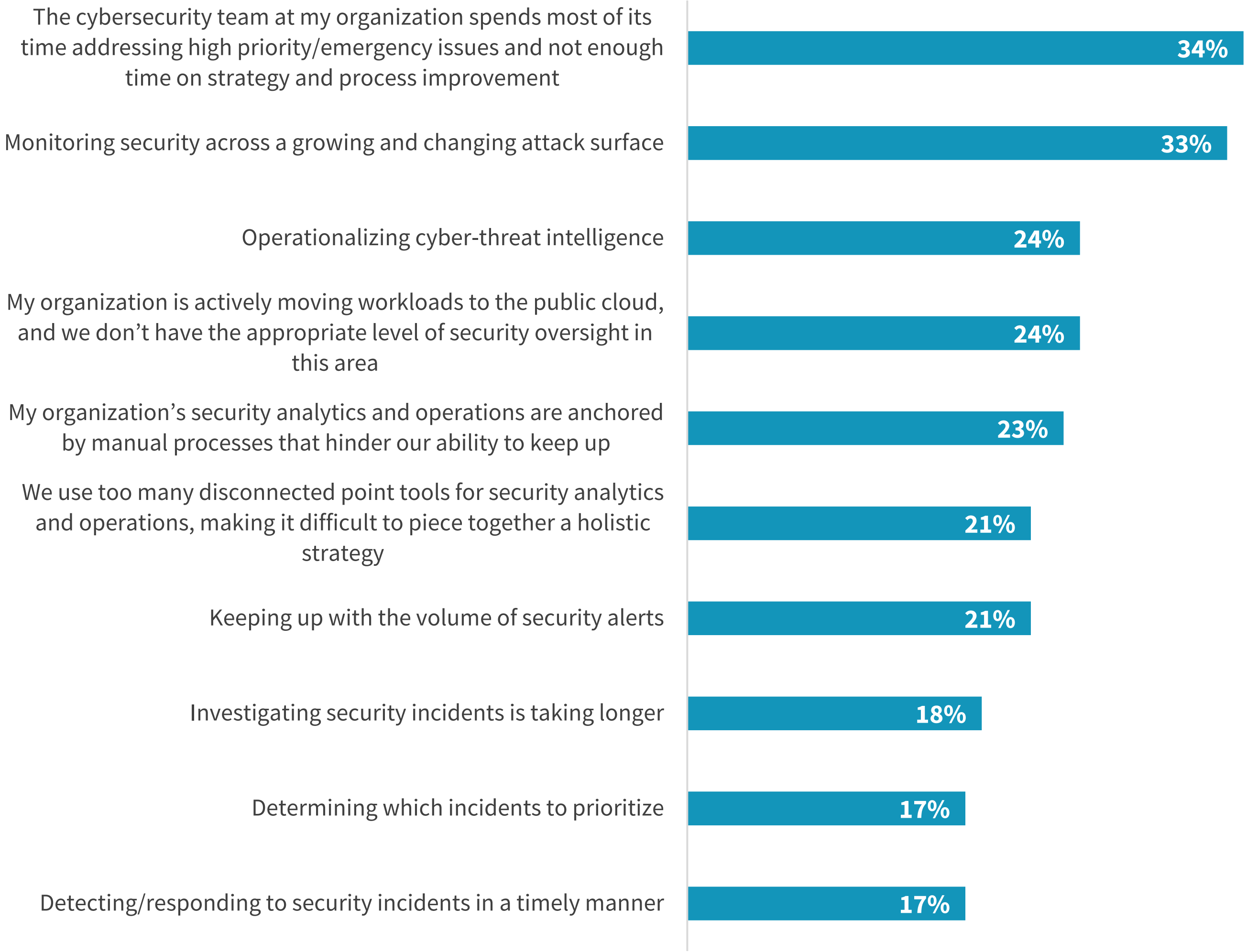
[2] Source: ESG Research Report, *Security Hygiene and Posture Management*, January 2022.

- Too many tools. ESG research indicates that 54% of organizations use 26 or more tools for security operations.[3] This creates operational overhead and complexity, demanding that SOC personnel pivot from tool to tool to get their jobs done.

- Too many alerts. SOC teams often describe things like “alert storms” and “alert fatigue” because of the growing volume of security alerts. Hamstrung by manual processes and too many tools, SOC teams simply cannot keep up with alert volume, leading to uncomfortable tradeoffs between investigating or ignoring suspicious or anomalous behaviors.

Figure 1. Top Ten Security Operations Challenges

Which of the following would you say are your organization’s current, primary security operations challenges? (Percent of respondents, N=376, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

Security Pros Need Technology Solutions, Not Industry Hyperbole

Facing numerous challenges, CISOs need help from their security technology vendors, but many claim that the industry responds to their needs with soundbites and spin. In fact, new research from ESG and ISSA indicates that 73% of security

[3] Source: ESG Complete Survey Results, SOC Modernization and the Role of XDR, September 2022.

professionals agree that security vendors tend to engage in too much hype and not enough substance.[4] This is certainly true regarding security operations, with its abundance of acronyms (i.e., EDR, NDR, SIEM, SOAR, UEBA, XDR, etc.), conflicting product definitions, and inflated efficacy claims. Security professionals often tell ESG that they know their current security strategies are inadequate, but they don't know what actions they should prioritize to break this ineffective cycle.

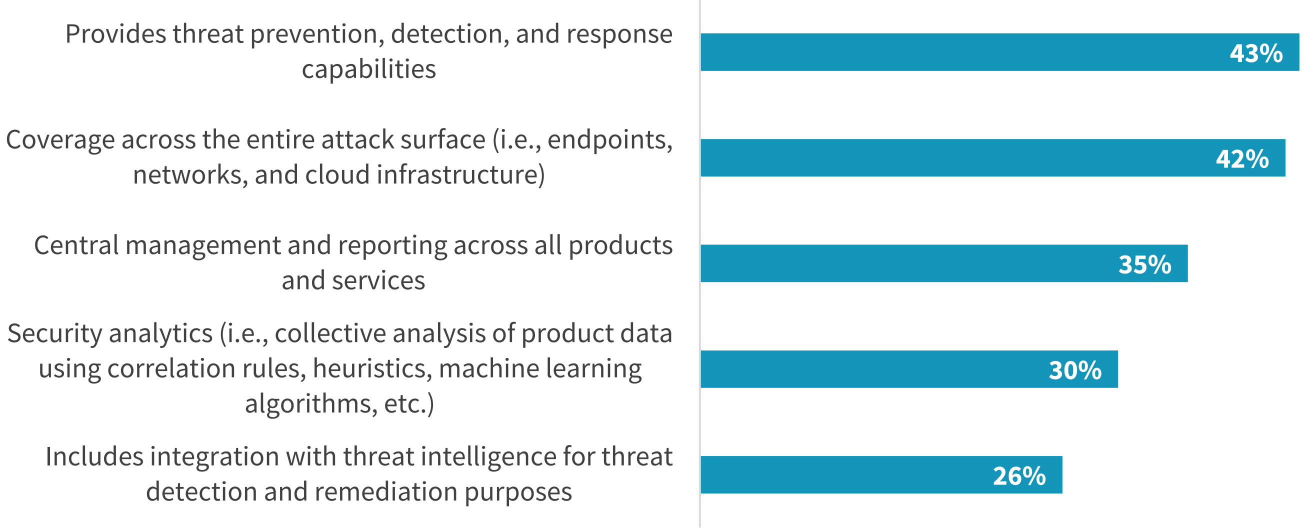
While industry hyperbole and confusion persist, security professionals have strong opinions about what is most important for threat detection and response technologies (see Figure 2).[5] They want platforms that deliver:

- **A complete solution for threat prevention, detection, and response.** In other words, they want solutions that can integrate with security controls, update prevention rules, and reinforce defenses in addition to monitoring and detection.
- **Security monitoring across the entire attack surface (aka Lateral Movement).** Sophisticated cyber-attacks can progress across endpoints, networks, data centers, cloud-based workloads, and SaaS applications. Rather than look at each domain individually, SOC teams want solutions that can monitor behavior, protect assets, and detect suspicious/malicious activities across all components of hybrid IT.
- **Central management.** To ease operations, SOC teams want one place from which to monitor security status, triage alerts, escalate investigations, and take remediation actions. This includes support for junior and senior analysts with custom dashboards supported by role-based access controls.
- **Security analytics for more timely and accurate threat detection.** Security operations tools should provide layers of defense by providing static detection rules, behavior-based heuristics, and advanced analytics using nested machine learning algorithms. The goal? Weed out pedestrian threats while providing accurate analytics for more sophisticated low-and-slow attacks that follow a cyber kill chain pattern.
- **Integration with threat intelligence.** SOC teams want to utilize threat intelligence for activities like alert enrichment, security investigations, threat hunting, and operationalizing the MITRE ATT&CK framework.

[4] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.
[5] Ibid.

Figure 2. Top 5 Most Important Attributes for Threat Detection and Response Platforms

Which of the following would you consider the most important attributes of a cybersecurity "platform" for threat detection and response? (Percent of respondents, N=280, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

How Stellar Cyber Aligns with these Requirements

While the threat detection and response solution attributes illustrated in Figure 2 are most important, it's also worth noting that SOC teams have no appetite for "ripping and replacing" existing security technologies and starting from scratch. They want to implement new technologies that unify existing tools, provide incremental benefits for security efficacy and operational efficiency, *and* help them achieve the attributes listed above.

What's needed to build such a SOC solution? An open security operations and analytics platform architecture (SOAPA) that can integrate existing tools while adding incremental functionality. Stellar Cyber can help here with its Open XDR. Stellar Cyber aligns well with the threat detection and response priorities described above, as its technology can:

- Protect the attack surface. Stellar Cyber comes with out-of-the-box integrations with market leading EDRs, cloud infrastructure monitoring, SaaS applications, identity services, and email security products. Working with third-party tools, Stellar Cyber's platform can protect the entire attack surface. Stellar Cyber also comes with native NDR for detecting lateral movement and suspicious/malicious network connections.

- Centralize management and reporting. Stellar Cyber provides central management, enabling SOC teams to conduct operations tasks through a single console. This can help with analyst training and overall SOC productivity.

- Add advanced analytics models. Stellar Cyber can integrate with data sources, creating a normalized and enriched data model for AI modeling. Stellar Cyber's AI engine generates contextualized, correlated alerts and outputs for security teams, providing depth and a holistic view for triage, investigations, and remediation decisions.

- Offer response capability. Stellar Cyber integrates with security, IT, and productivity tools to allow security analysts to automatically or manually address cyber-attacks with immediate actions, such as blocking offenders at the firewall, containing a host, or disabling a user or an account in the same platform.

- **Integrate with other threat Intelligence technologies.** Stellar Cyber's platform integrates with various threat intelligence technologies and allows customers to bring their own threat intelligence tools. The threat intelligence is centrally managed and automatically applied to the telemetry collected to detect known threats.

Stellar Cyber can provide the technology underpinning for SOC modernization with its next-generation SIEM and NDR and a "bring your own EDR" model that adds XDR integration and analytics capabilities on top of leading EDR tools. To work with existing security and IT technologies, Stellar Cyber interoperates with the market-leading IT and security tools, collects telemetry, creates analytics models, and generates response actions directly through tools and controls. In aggregate, Stellar Cyber can unify currently disjointed security tools and data sources to visualize; correlate through AI; and automatically detect, investigate, and respond to all attack activities—exactly the type of functionality that security professionals are looking for.

The Bigger Truth

SOC teams need help modernizing security operations in areas like integrating technologies, automating processes, and creating advanced analytics for threat detection. When security pros reach out to security technology vendors, they hear conflicting messages leading to confusion and project delays.

ESG sought to cut through this confusion by asking security professionals what they need from a threat detection and response platform. The results paint a picture of clarity: Security pros need solutions that provide threat prevention, detection and response, coverage across the entire attack surface, and central management/reporting. Furthermore, SOC teams want platforms that provide incremental value on top of their existing security technology stack.

Stellar Cyber may not be a household name, but it does align well with these requirements. In this way, Stellar Cyber provides a pragmatic threat detection and response solution rather than more confusion and hyperbole.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188