ESG SHOWCASE

AWS, Recorded Future, and Splunk: Better Security Operations Together

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

ABSTRACT: Enterprise security operations can be hamstrung by an army of point tools, chaotic threat intelligence management, and an immature adoption of the cloud security shared responsibility model. Unfortunately, this can lead to security operations complexity, inefficiency, and overhead. CISOs can improve this situation by adopting a security operations and analytics platform architecture (SOAPA) for technology integration and interoperability. Recorded Future and Splunk, in collaboration with AWS, are working to provide a collective SOAPA, helping organizations to mitigate risk and improve security operations efficacy and efficiency.

Overview

Organizations face an increasingly dangerous threat landscape from global adversaries and cyber-criminals. At the same time, security operations teams must defend their digital assets across a growing attack surface amplified by more remote workers, cloud-based workloads, and SaaS applications. Addressing these requirements demands a detailed enterprise security program anchored by a strong security operations practice. Unfortunately, many organizations continue to struggle because security operations teams are burdened by:

- Too many disconnected point tools. Organizations often use dozens of disparate tools and technologies for security operations. Enterprise Strategy Group (ESG) research indicates that this can lead to security "silos," requiring organizations to train the staff on multiple technologies, figure out how to piece together different tools to get a full security perspective, and aggregate security technologies. These and other issues create bottlenecks, adding time and complexity to security operations processes (see Figure 1).[1]

- Adoption of a shared responsibility model. Cloud security is based on a well-defined shared responsibility model, so organizations need to incorporate the right policies, procedures, and monitoring in place to address cloud and traditional security requirements simultaneously. This requires the right KPIs, metrics, and reviews for continuous improvement. Many organizations are learning how to manage a shared responsibility model while cloud application development accelerates—a difficult balancing act.

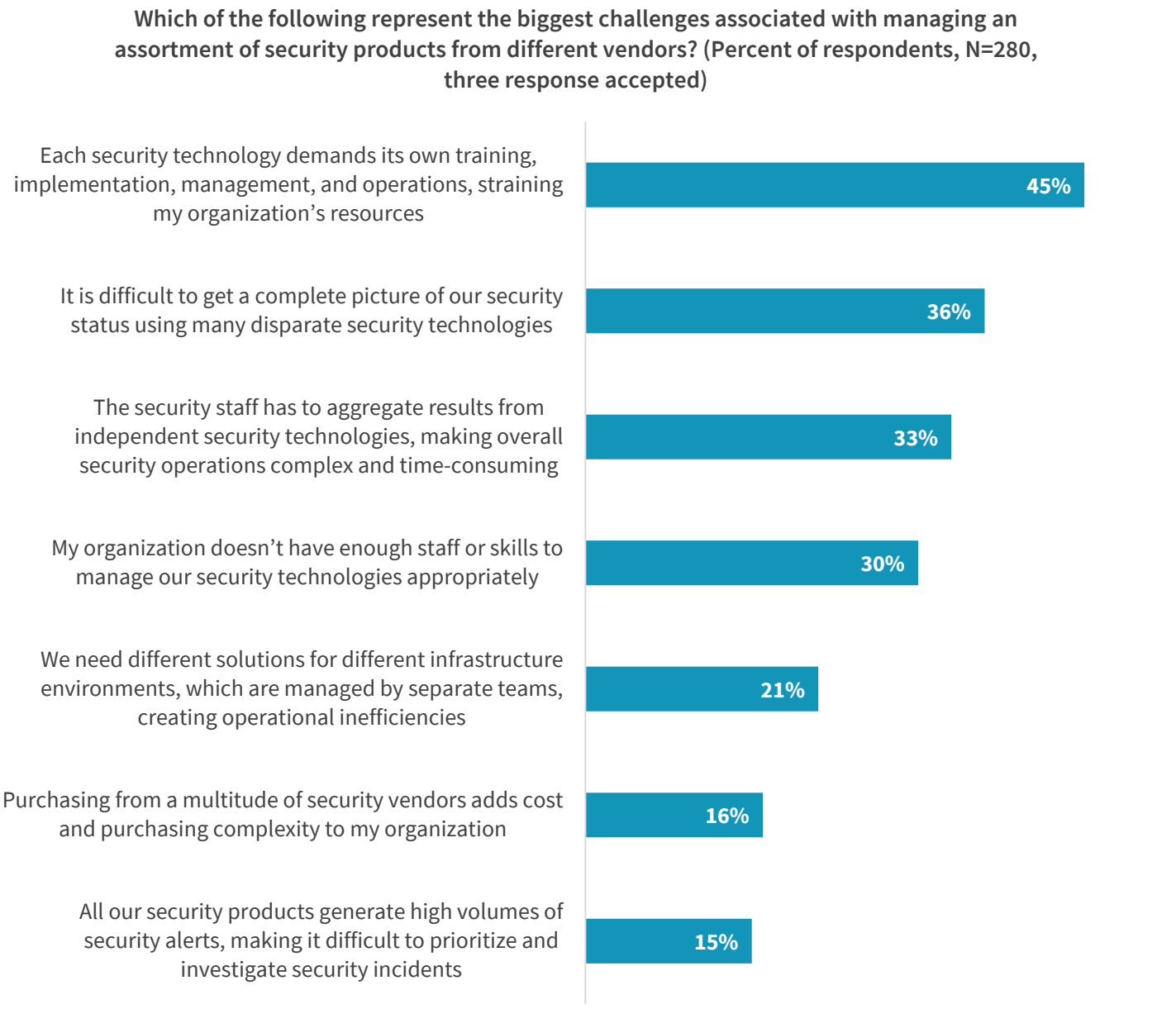
- Haphazard threat intelligence management. SOC teams often try to piece the threat landscape together through open source and commercial feeds, static content (i.e., blogs, threat reports, articles, etc.), manual processes, and limited integration into their security stack. What's missing? A focused effort on defining and tracking real and relevant

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

threats to business operations. Regrettably, current slapdash threat intelligence management is inefficient and incomplete and leaves organizations in a state of perpetual catchup mode.

These challenges are exacerbated by the global cybersecurity skills shortage. According to research from ESG and the information systems security association (ISSA), 57% of organizations claim they've been impacted by the skills shortage, resulting in increasing workloads on existing staff, unfilled job openings, high staff burn out, and an inability to use security technologies to their full potential.[2]

Figure 1. Security Technology Management Challenges



Source: ESG, a division of TechTarget, Inc.

[2] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.

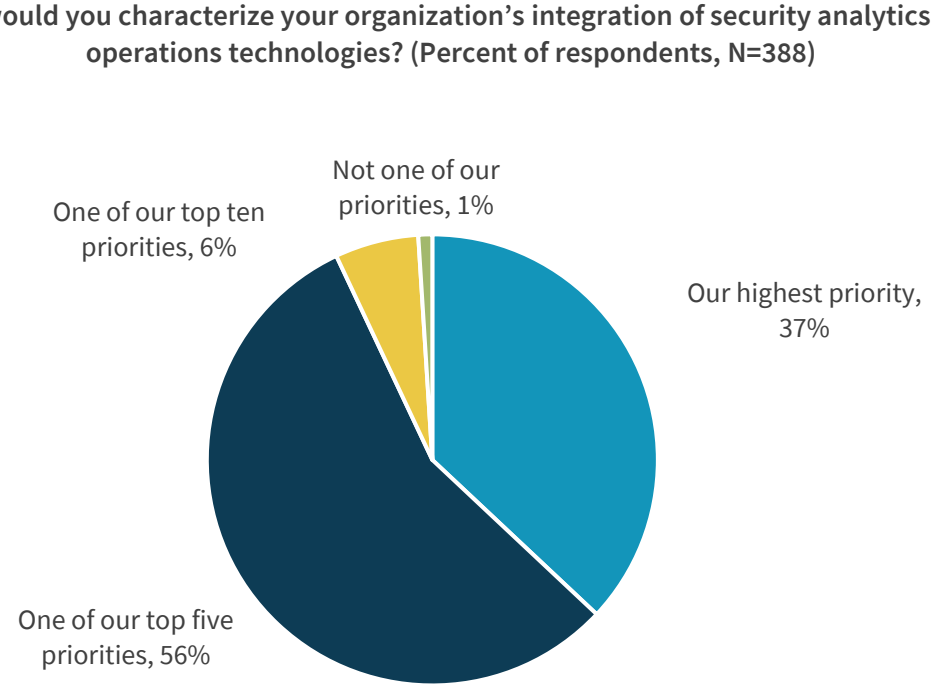
What's Needed?

Security operations issues like those described above should set off alarm bells for CISOs and business executives. To protect business-critical assets deployed across hybrid IT infrastructure, security teams must address these challenges by adopting:

- A single source of security operations truth for hybrid IT visibility. Establishing end-to-end visibility requires the collection, processing, and analysis of security data from endpoints, networks, data centers, and public clouds within a single data repository. While many organizations have established this model for internal systems, integrated cloud visibility is increasingly important as workloads migrate from internal data centers to the public cloud. According to ESG research, 18% of organizations claim that more than 40% of their business applications are cloud-resident today. This percentage will increase substantially: 44% of organizations forecast that more than 40% of their business applications will be cloud-resident within the next 36 months.[3]

- An architecture for security technology interoperability. To enable security operations teams to collect, process, analyze, and act upon security data in a timely manner, security operations tools must interoperate seamlessly. This requires an integrated security operations and analytics platform architecture (SOAPA) with coverage across hybrid IT infrastructure. Clearly, organizations realize the need for SOAPA and are rapidly moving in this direction. This is evidenced in recent ESG research, which indicates that security analytics and operations technology consolidation is a top priority for nearly every organization (see Figure 2).[4]

Figure 2. Prioritization of Integrating Security Operations Technologies



Source: ESG, a division of TechTarget, Inc.

[3] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

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

- An outside-in perspective. Security teams must be able to correlate internal security behavior with adversary behavior happening "in the wild." This requires a thorough understanding of threat intelligence, contextualized and customized for individual organizations. In this way, security teams can gain an understanding of adversary campaigns and TTPs (tactics, techniques, and procedures) and relate them to observable behaviors across their endpoints, networks, data centers, and cloud-resident workloads. An outside-in perspective can help accelerate threat detection while enabling ongoing threat hunting activities.

- A common security operations workbench. Rather than pivot between tools, security analysts need a primary interface for dashboards, notable events, analytics, and data queries. This can help improve threat management accuracy and efficacy while increasing the efficiency and productivity of the security operations center (SOC) staff. A common workbench can also help organizations monitor and manage the shared responsibility model continuously.

Recorded Future and Splunk, in Collaboration with AWS, Can Help Modernize Security Operations

Organizations need to aggregate all security data to streamline processing, analysis, and decision making. While this equates to SOAPA, many organizations don't have the engineering resources or experience needed for custom integration. Fortunately, some vendors recognize these needs and are working together to provide heterogeneous integrated security operations solutions.

For example, AWS, Recorded Future, and Splunk offer product integration for mutual customers. In this relationship, the three vendors facilitate SOAPA, with:

- Splunk acting as a common data service. Splunk Enterprise and Enterprise Security can anchor security operations for collecting, processing, and analyzing all security data. In this way, Splunk breaks down traditional data silos by providing an open and scalable data platform for structured and unstructured data from any source across the hybrid infrastructure. To meet today's deployment demands, Splunk Enterprise and Enterprise Security can be deployed on-premises, in the public cloud, or as a hybrid model. Once deployed, SOC teams can use Splunk for processes such as threat detection/hunting, risk mitigation, and incident response.

- Splunk working with AWS for comprehensive cloud security monitoring. To provide security oversight over cloud-based workloads, Splunk Enterprise and Enterprise Security can consume all types of AWS logs like AWS Config, AWS CloudTrail, Amazon Inspector, Amazon CloudWatch, and Amazon Kinesis Data Firehose. Once ingested, Splunk then presents this data in pre-built dashboards and templates. Additionally, the Splunk threat research team provides AWS-specific detections to help identify threats and risks out-of-the-box. Splunk can also help SOC teams get to the root cause of security issues using Splunk's search capabilities and Investigation Workbench—a central interface for user and system behavior investigations. Splunk also supports the MITRE ATT&CK framework for mapping adversary TTPs and risk scoring across AWS and hybrid IT infrastructure. Taken together, Recorded Future and Splunk integrate with AWS to help organizations mature their shared responsibility model management.

- Recorded Future providing an outside-in perspective. Through API integration into Splunk, Recorded Future provides broad cyber-threat intelligence (CTI) that can enrich alerts with risk scores, indicators of compromise (IOCs), and detailed information on adversary groups, TTPs used, and attack campaigns. In this way, Recorded Future adds an outside-in perspective, enabling analysts to enrich events that they are seeing within Splunk Enterprise and Enterprise Security and showing them trends for malware families, threat actors, and critical vulnerabilities across hybrid IT

infrastructure. Armed with this intelligence, security teams can improve cyber-risk mitigation, fine-tune security controls, and effectively reduce their attack surface.

The Bigger Truth

In a recent ESG research survey, security professionals were asked to identify the benefits of security technology vendor consolidation (i.e., purchasing security products from fewer vendors). The research revealed that:[5]

- 65% of security professionals believe that security vendor consolidation could lead to greater operational efficiencies with IT and security teams.
- 60% of security professionals believe that security vendor consolidation could lead to tighter integration between disparate security controls.
- 51% of security professionals believe that security vendor consolidation could lead to greater threat detection efficacy.

These benefits can be seen as synonymous with security technology integration and SOAPA. AWS, Recorded Future, and Splunk understand security operations needs and typical challenges around scalability, integration, hybrid IT visibility, and threat intelligence integration and are working together to address enterprise requirements. In this way, the three vendors can help organizations mitigate cyber-risks, improve security efficacy, increase operational efficiency, and enable business processes.

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

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