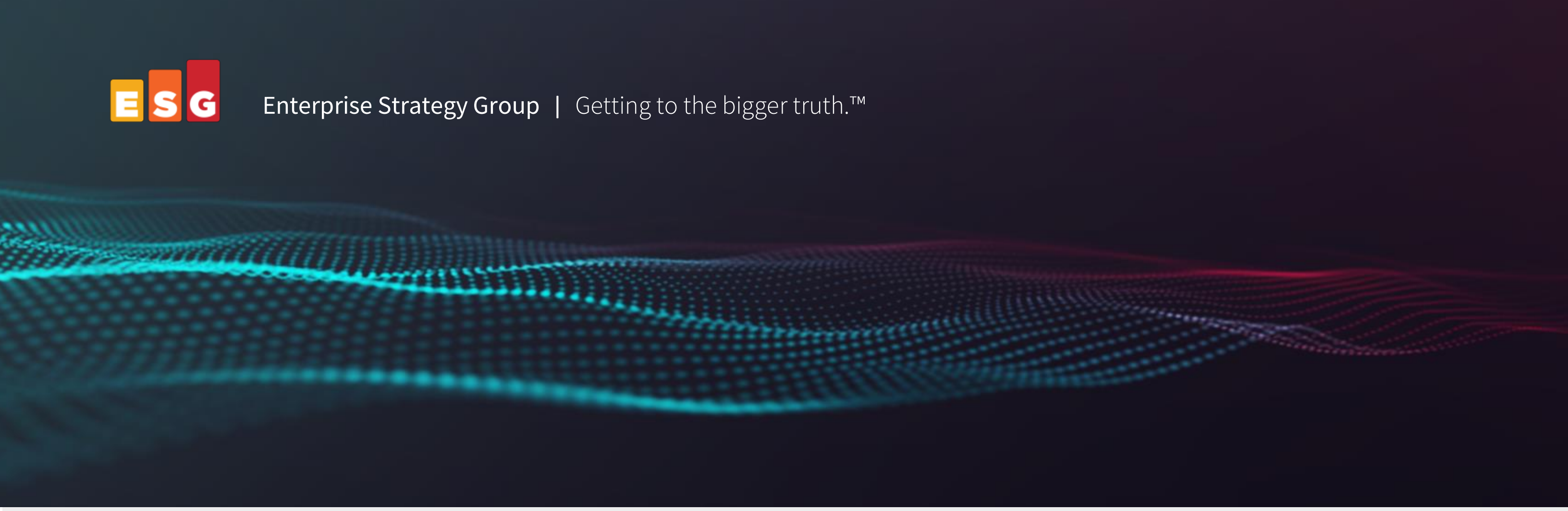


Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH INSIGHTS PAPER

The Benefits of Security Operations Consolidation and Integration through a Common UI/UX

By Jon Oltsik, Senior Principal Analyst and Fellow

July 2020

This ESG Research Insights Paper was commissioned by Splunk
and is distributed under license from ESG.

Contents

Executive Summary

In February and March 2020, the Enterprise Strategy Group (ESG) completed a research survey of 300 cybersecurity and IT professionals who are directly involved with their organization's cybersecurity management and operations. Further description of the research methodology and survey demographics are displayed in the appendix section of this report.

Based upon the research presented in this research insights paper, ESG concludes:

- **Security teams have numerous security operations objectives.** The security operations center (SOC) acts as a backbone for organizations, with security analysts tasked with mitigating cyber-risks, preventing/detecting cyber-attacks, and responding to security incidents when they occur. To accomplish these goals, organizations have several security operations objectives for the next 12 to 18 months, including refining cyber-risk identification, improving threat intelligence operationalization, and enhancing security data enrichment/contextualization. All these objectives are ultimately intended to protect critical business assets and enable business processes.

- **Most organizations manage security operations with too many tools and not enough security staff.** Achieving security operations goals may be difficult for several reasons. Most organizations have more than 25 security operations tools, making security operations complex and time consuming. Furthermore, four out of five organizations surveyed have been impacted by the global cybersecurity skills shortage, leaving them short-staffed and lacking in advanced security operations skills. CISOs understand these issues and are responsible for improving security operations as soon as possible. This may be why improving security operations is a top priority.

- **CISOs believe that improvement depends upon security operations technology consolidation and integration.** Given current security operations issues, it will be difficult if not impossible for organizations to meet their security objectives. Many security leaders believe that improving this situation depends upon security operations technology consolidation and integration. This means fewer vendors and tools, and tight technology interoperability from the data pipeline, through security analytics, to security operations process management. Technology consolidation and integration should simplify security operations, helping to improve process efficiency and SOC productivity.

- **Security professionals see potential benefits in a common security operations UI/UX.** Many firms are already integrating security operations technologies at the data, application, and process layers, but what about the user level? In other words, could there be benefits to a common security operations user interface/user experience (UI/UX)? This research specifies that the majority of security professionals believe a common security operations UI/UX could be valuable in areas like SOC staff training, incident detection/response acceleration, and SOC communications improvement. Given these advances, common security operations UI/UX projects may be worthwhile undertakings in the near future.

Security Operations Today

Cybersecurity centers on minimizing cyber-risks, protecting critical digital assets, and detecting/responding to incidents when they occur. Accomplishing these tasks requires situational awareness, keen data analysis, and the ability to take the right actions at the right time.

According to the research, 87% of organizations say that improving security operations is one of their top priorities relative to other technology initiatives. What are the primary objectives for security operations in the immediate future? Survey respondents identified goals like (see Figure 1):

- Improving risk identification. This is especially difficult due to an expanding attack surface driven by cloud computing proliferation, IoT device deployment, and work-from-home (WFH) initiatives resulting from COVID-19. To manage security, CISOs need a real-time view of dynamic cyber-risks.

- Improving the operationalization of threat intelligence. Cyber threat intelligence (CTI) can alert organizations to nefarious activities happening “in the wild,” like identifying malicious IP addresses, domains, and files. Security teams can then operationalize this intelligence by using it to modify security controls and block indicators of compromise (IoCs). The ESG data indicates that many organizations are seeking to improve this process soon.

- Security data enrichment and contextualization. Detecting cyber-attacks requires analysis of multiple data elements—a resource-intensive methodology that can require advanced skills. To streamline this process, organizations want to view related data elements like anomalous user activity, rogue endpoint processes, and suspicious network traffic in the context of a cyber-attack kill chain or within a taxonomy like the MITRE ATT&CK framework. SOC teams have set objectives for data enrichment and contextualization to make this happen.

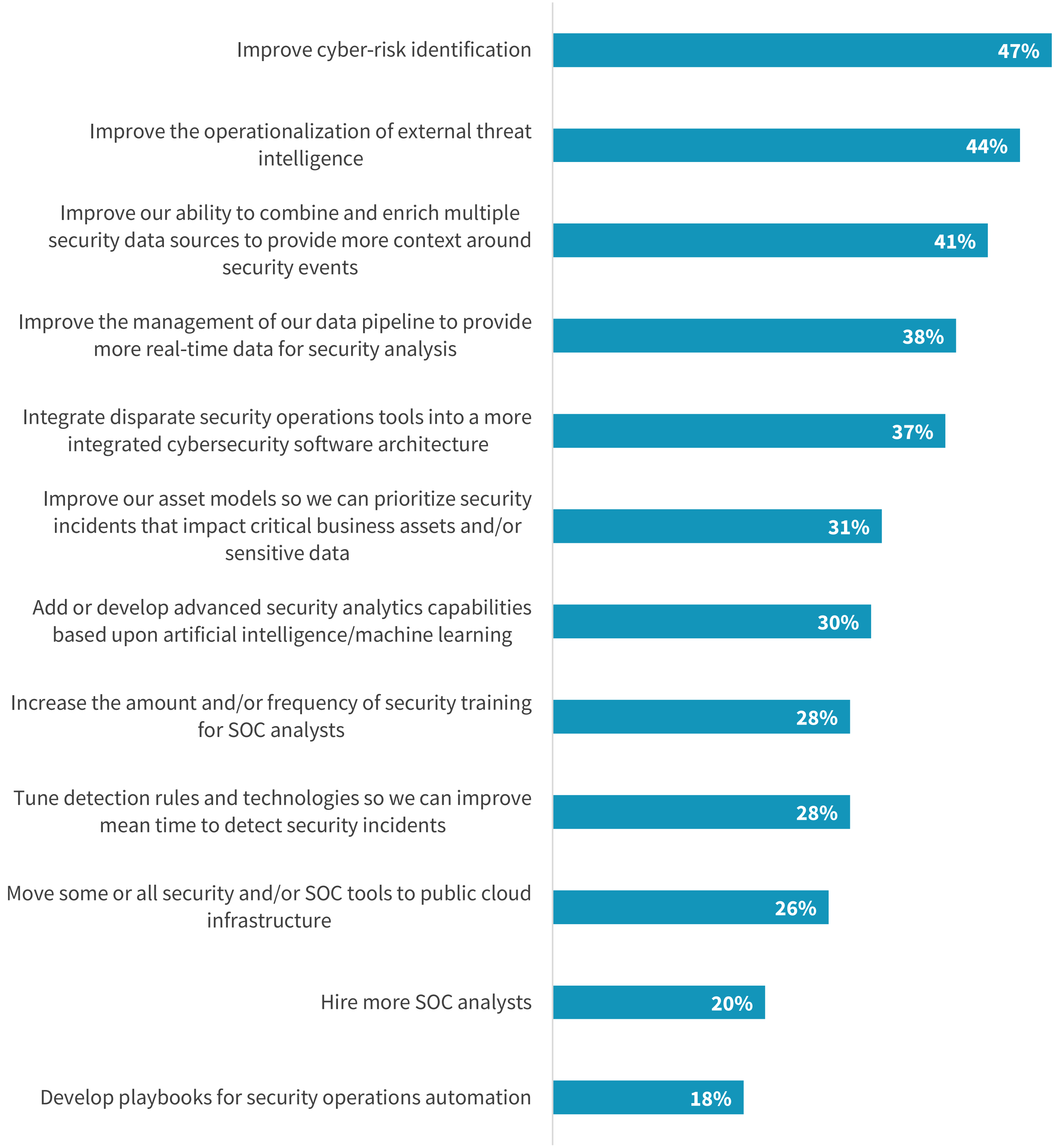
Top 5 Security Operations Objectives

1. Improve cyber-risk identification.
2. Improve the operationalization of external threat intelligence.
3. Improve our ability to combine and enrich multiple security data sources to provide more context around security events.
4. Improve the management of our data pipeline to provide more real-time data for security analysis.
5. Integrate disparate security operations tools into a more integrated cybersecurity software architecture.

- Security data pipeline enhancement. Security operations can require GBs and even TBs of real-time and batch data collection, processing, and analysis. Many organizations are reengineering their security data pipelines to address scaling and performance requirements.

Figure 1. Primary Security Operations Objectives

Over the next 12-18 months, which of the following would you say are your organization's primary objectives regarding security operations? (Percent of respondents, N=300, five responses accepted)



Source: Enterprise Strategy Group

Too Many Tools, Not Enough People

While organizations have aggressive security operations plans, they still face a few fundamental problems. First, the research indicates that 81% of organizations have been impacted by the cybersecurity skills shortage, and 39% of those organizations believe the skills shortage has gotten worse over the past few years. What is the specific impact of the cybersecurity skills shortage?

- 48% of respondents say it has increased the cybersecurity staff's workload. So, organizations are piling more work on an already overwhelmed cybersecurity staff.
- 38% of respondents say security teams are often too busy managing their workload to keep up with training. This is a concern because threat actors continually change the tactics, techniques, and procedures (TTPs) they use in cyber-attacks. Without continuous training, cyber-risk always increases.
- 36% of respondents say the cybersecurity staff is unable to focus on anything but high-priority issues and incidents. In this scenario, the cybersecurity team puts out fires as they arise but never gets around to working with the business to build a comprehensive security strategy.

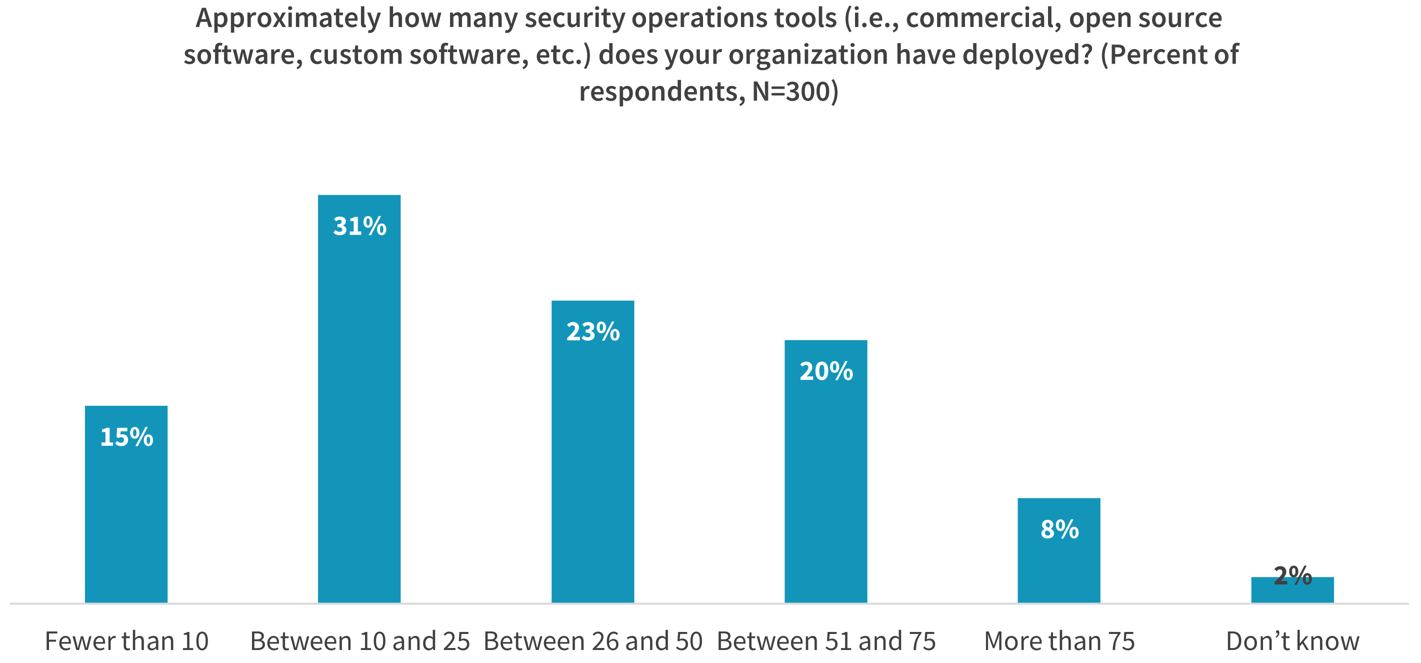
Top 5 Implications of the Cybersecurity Skills Shortage

1. Increasing workload on existing staff.
2. Security team is often too busy managing their workload to keep up with training.
3. Cybersecurity staff is unable to focus on anything but high-priority issues and incidents.
4. High "burn out" and/or attrition rate among the cybersecurity staff.
5. Inability to fully learn or utilize some security technologies to their full potential.

Addressing security operations difficulty is critical—58% of survey respondents believe their organization experienced a security incident (e.g., compromised system, malware instance, data breach, or compliance violation) in the past 12 months that could have been prevented or minimized if their team's security operations skills were improved.

Adding to cybersecurity skills shortage issues, many organizations still rely on an army of disparate security analytics and operations point tools. For example, the research indicates that 51% of organizations surveyed use more than 25 security operations tools today, and 28% use more than 50 tools (see Figure 2).

Figure 2. Number of Security Operations Tools Deployed



Source: Enterprise Strategy Group

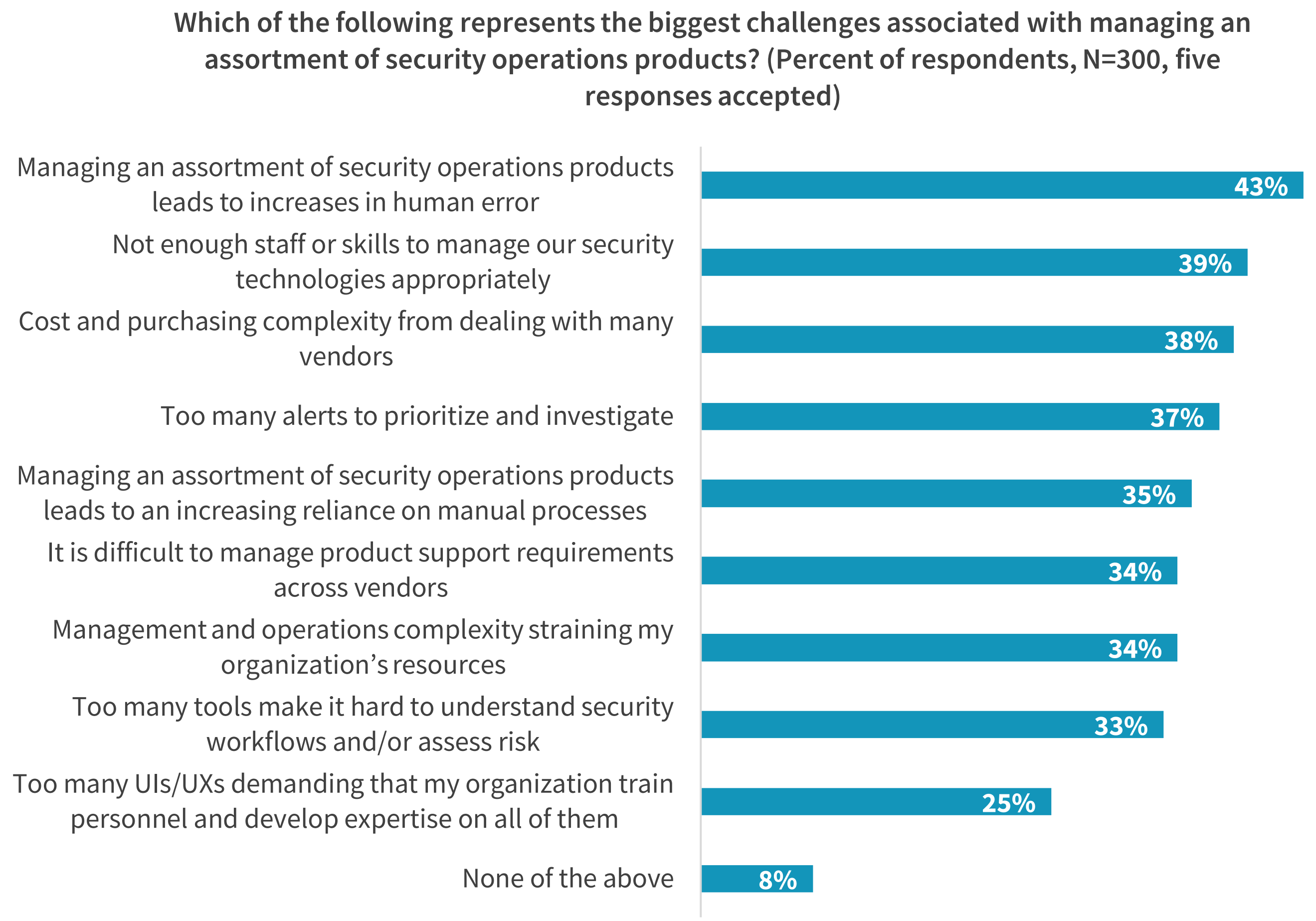
So, what's the problem here? Each of these tools must be deployed, configured, managed, and operated, requiring lots of resources and personnel. This operational overhead can then lead to numerous other issues (see Figure 3). Survey respondents point to challenges around managing an assortment of security operations point tools, such as:

- 43% of respondents say that managing an assortment of security operations products leads to an increase in human error as the cybersecurity staff scrambles to keep up with a growing security operations workload.
- 39% don't have enough staff or skills to manage their security technologies appropriately. This is consistent with the data presented regarding the global cybersecurity skills shortage.
- 38% point to high costs and purchasing complexity. This is understandable as cybersecurity teams and purchasing managers juggle contracts, sales cycles, and payments.
- 37% are challenged by too many alerts to prioritize and investigate. This type of "alert fatigue" forces SOC teams into dead-end investigations while ignoring critical alerts they should be pursuing.

Top 5 Challenges with Managing Assorted Security Operations Products

1. Managing an assortment of security operations products leads to increases in human error.
2. Not enough staff or skills to manage security technologies appropriately.
3. Cost and purchasing complexity from dealing with many vendors.
4. Too many alerts to prioritize and investigate.
5. Managing an assortment of security operations products leads to an increasing reliance on manual processes.

Figure 3. Challenges Associated with Managing Assorted Security Operations Products



Source: Enterprise Strategy Group

The data indicates that many organizations are at a crossroads. Security operations is critical, so much so that 82% of organizations plan on increasing security operations spending in pursuit of aggressive security operations objectives. Nevertheless, many organizations remain hamstrung as they try to manage and improve security operations incrementally on a tool-by-tool basis with an under-staffed and under-skilled cybersecurity team. This is a recipe for failure.

Security Operations Consolidation and Integration

Given the dangerous threat landscape and growing attack surface, relying on disconnected security operations point tools seems like a fool's errand. CISOs need to bolster security operations efficacy and efficiency any way they can.

The quest to improve security operations is driving changes. For example, 37% of organizations (see Figure 1) say that creating an integrated cybersecurity software architecture is one of their biggest security operations objectives in the next 12 to 18 months. The thought here is that technology integration can help organizations better manage and operate their security operations technology.

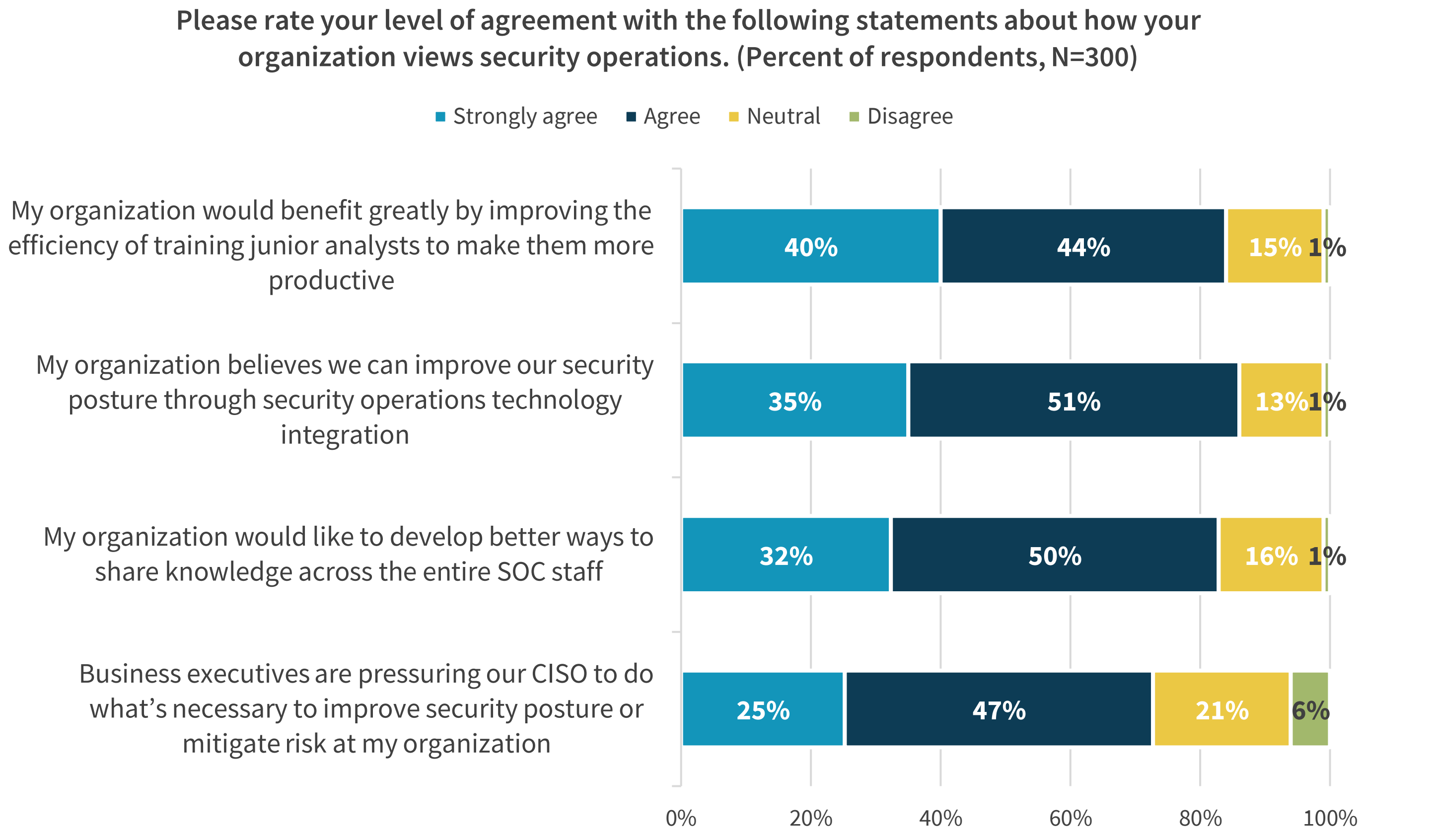
This point was reinforced through a series of opinion questions posed to survey respondents. Most (86%) strongly agree or agree that their organization believes it can improve security posture through security operations technology integration (see Figure 4). Technology integration here may include aggregating security telemetry into a common security data pipeline, integrating analytics applications for alert triaging and investigations, and connecting security analytics and operations technologies to security controls for process automation and orchestration.

What else could be done to improve security operations?

- 84% of respondents strongly agree or agree that their organization would benefit by improving the efficiency of training junior analysts to make them more productive. In this way, junior analysts could triage greater volumes of security alerts, freeing experienced SOC personnel to work on the most vexing problems. Additionally, junior analysts could gain experience and become more productive sooner.
- 82% of respondents strongly agree or agree that their organization would like to develop better ways for SOC knowledge sharing. This could help establish best practices among the team and serve as the foundation of a mentoring program where experienced analysts work directly with more junior staffers.

Note too that 72% of respondents strongly agree or agree that business executives are pressuring their CISO to improve security posture or mitigate risk—evidence that security operations improvement is a business, not just a technical, goal.

Figure 4. Security Operations Opinions



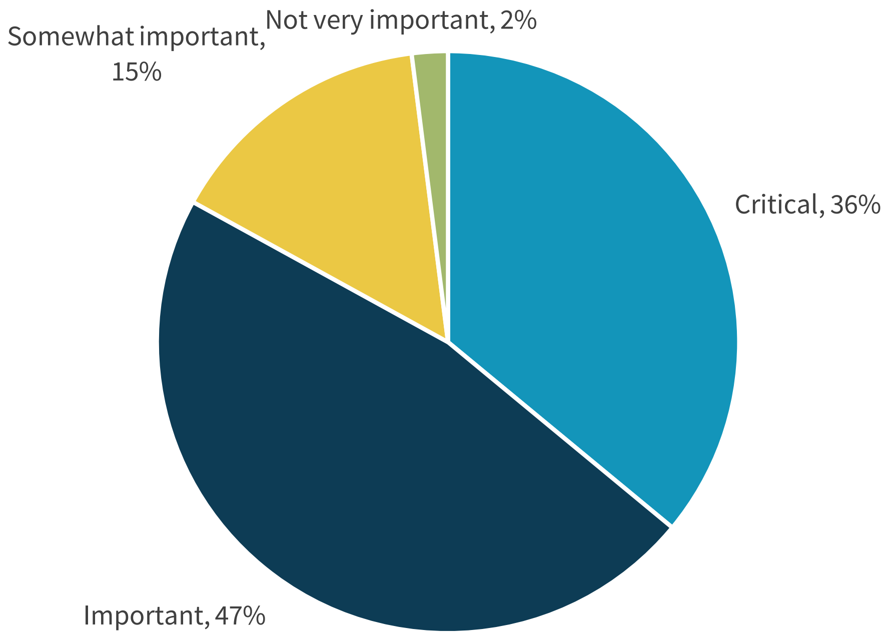
Source: Enterprise Strategy Group

As organizations consolidate security technologies, they may turn to leading vendors offering integrated security operations product suites. However, security operations will likely remain a heterogeneous technology endeavor for the foreseeable future.

Recognizing this situation, 83% of security professionals believe it is critical or very important for single-vendors' security operations solutions to provide integration with other tools in use (see Figure 5). Leading security operations technology vendors must be responsive to this requirement with open APIs, standards support, partner ecosystems, and strong go-to-market programs with software developers and key channel and technology partners.

Figure 5. Importance of Security Operations Technology Integration

If your organization purchased multiple security operations technologies from a single vendor, how important would it be for those technologies to be able to be integrated with other tools in use? (Percent of respondents, N=300)



Source: Enterprise Strategy Group

Toward a Common Security Operations UI/UX

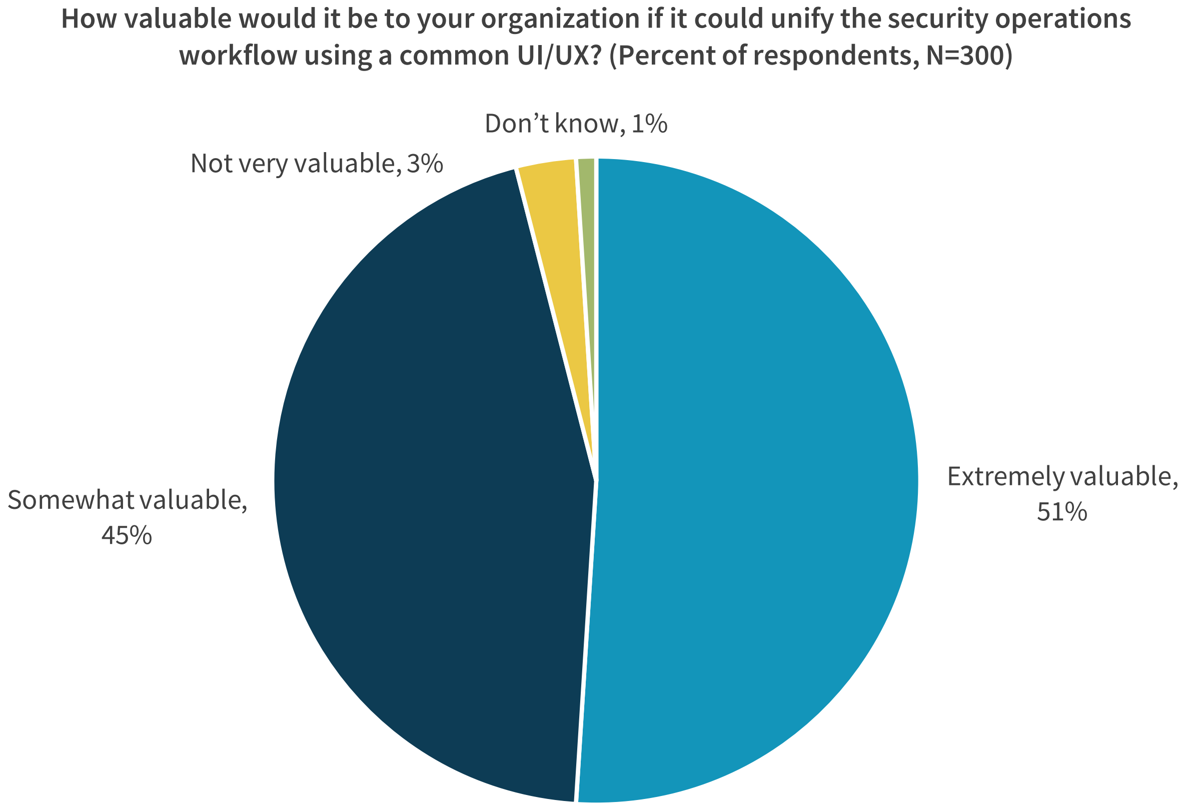
Over the past few years, many organizations have started the process of security operations technology integration. For example, organizations have consolidated their security data pipeline using Apache Kafka, an event streaming platform capable of handling trillions of events per day. SOC teams are also combining security analytics by purchasing multifunction analytics combinations (e.g., common SIEM and UEBA systems) or integrating disparate tools through APIs. ESG has also seen organizations create security operations runbooks that aggregate various technologies at a process level.

While many organizations now share data between tools, they continue to do their daily security operations tasks by accessing multiple user interfaces. For example, an incident investigation may force an analyst to pivot across SIEM to endpoint detection and response (EDR), network traffic analysis (NTA), and threat intelligence platform (TIP) UI/UXs. This type of “swivel chair” management requires training and experience across multiple tools and can lead to process overhead and human error.

The inefficiencies associated with “swivel chair” SOC management lead to an obvious question: Why not develop a common interface across tools that can act as a workbench for all SOC activity? Could this be beneficial?

Cybersecurity professionals seem to like this idea: 96% of survey respondents believe a common UI/UX that unifies security operations workflow would be extremely or somewhat valuable (see Figure 6). CISOs should take note: Since nearly all security professionals perceive value in a common security operations UI/UX, this is an initiative worth pursuing.

Figure 6. Value of a Common Security Operations UI/UX



Source: Enterprise Strategy Group

Respondents who believe a common UI/UX would be useful were then asked to identify how it would add value (see Figure 7). The research indicates:

- 43% see value in easing the burden of training the SOC staff on multiple security tools. This is especially important because most organizations are short-staffed in cybersecurity and may have acute shortages of security analysts. A common security operations UI/UX could reduce security analyst training from many to one, which should help analysts increase productivity in shorter timeframes.
- 41% say the value of a common UI/UX is accelerating the time needed for incident detection and response. This is critical as it often takes hundreds of days to detect a sophisticated targeted attack. By that time, cyber-adversaries may have already mapped out networks, harvested credentials, and stolen valuable data.
- 39% believe a common UI/UX could improve communications within the SOC. Enhancing SOC communications could help in areas like employee training, runbook creation, and continuous process improvement.

- 38% claim that a common UI/UX could help their organization use more of the functionality of individual security tools. This is a hidden benefit as ESG finds that many security professionals are often too busy with day-to-day tasks to learn or use all the functionality available in their security tools. Better utilization of security controls could mean the difference between blocking malware and a devastating cyber-attack.

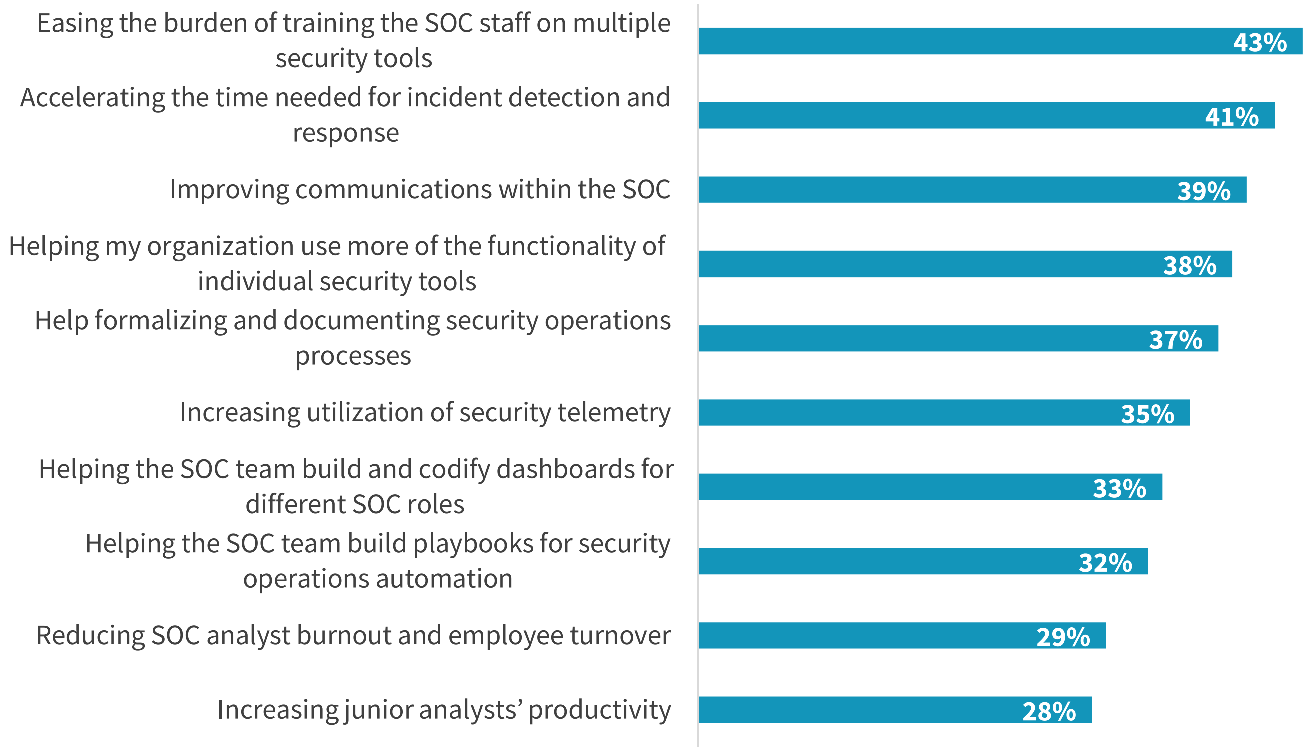
Taken together, these are significant results. SOC analysts could come up to speed quicker, gain deeper experience, and develop better skills by replacing multiple UI/UXs with a common UI/UX. Thus, a common UI/UX could act as a "force multiplier" making the SOC team more efficient, effective, and productive. These are substantial benefits.

Top 5 Most Valuable Aspects of a Common Security Operations UI/UX

1. Easing the burden of training the SOC staff on multiple security tools.
2. Accelerating the time needed for incident detection and response.
3. Improving communications within the SOC.
4. Helping the organization use more of the functionality of individual security tools.
5. Helping formalize and document security operations processes.

Figure 7. Most Valuable Aspects of a Common Security Operations UI/UX

You indicated that it would be valuable to your organization to unify security operations workflow using a common UI/UX. What do you think would be most valuable? (Percent of respondents, N=287, five responses accepted)



Source: Enterprise Strategy Group

Survey respondents were also asked to identify the most important attributes of a common UI/UX for security operations (see Figure 8). Security professionals pointed toward:

- Minimizing or eliminating the need for product UI/UXs. As previously described, 38% of security professionals want a common SOC UI/UX that acts as a workbench for junior and experienced analysts. The SOC team may then spend the majority of their time within the common SOC UI/UX and only pivot to other analytics tools on an as-needed basis.

- The ability to track and manage the security event lifecycle. 36% of survey respondents believe it's important for a common SOC UI/UX to span the entire security event lifecycle from threat detection, through investigation, to remediation. This would demand functionality for alerting, case management, query, and integration with security controls for process automation/orchestration.

- Federated search capabilities. Security operations technologies are quickly evolving into a hybrid architecture with substantial data repositories on-premises and in the public cloud. Rather than aggregate that data in one location, 36% of security professionals want a common SOC UI/UX with the ability to search data wherever it resides.

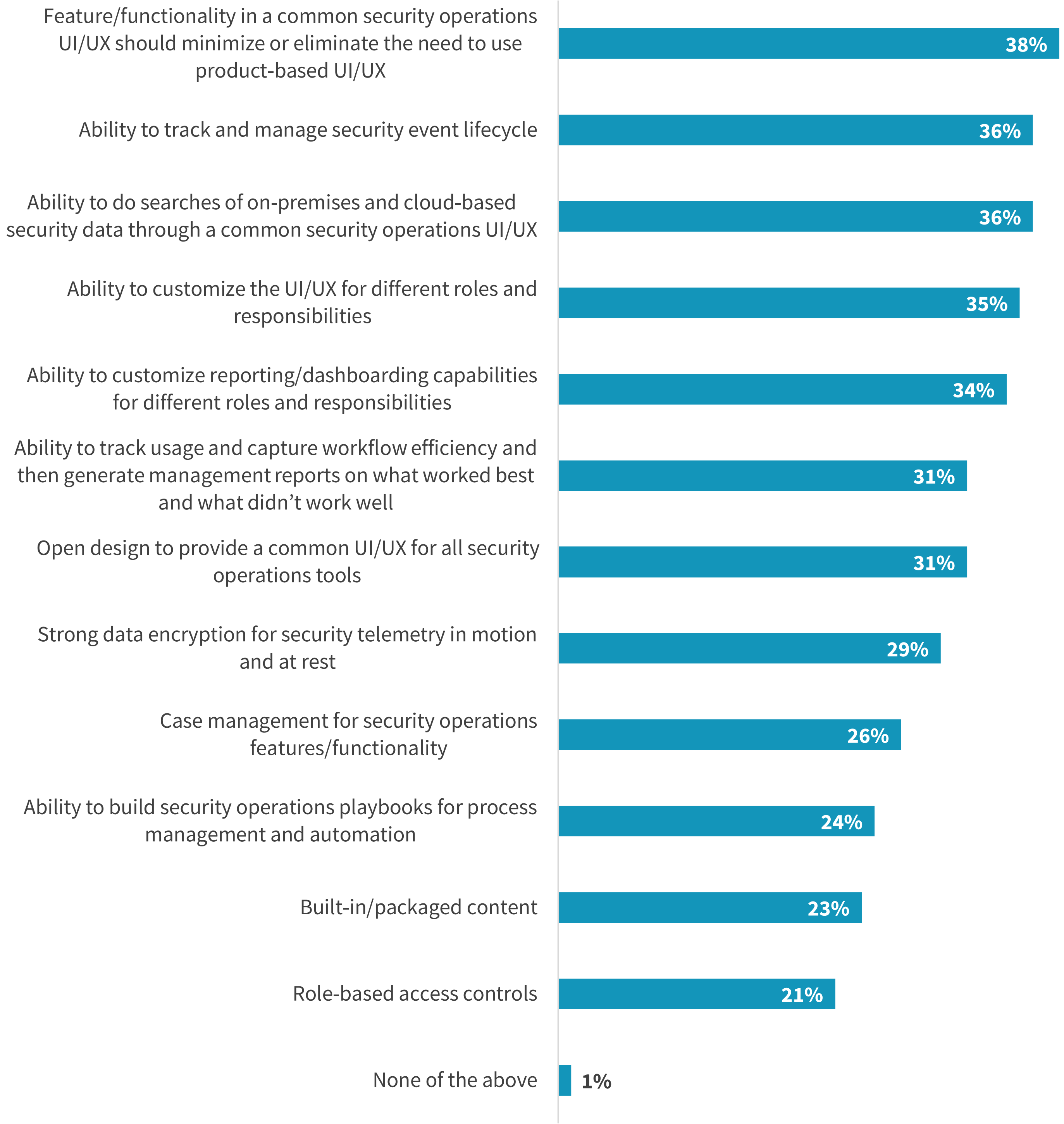
- UI/UX customization. More than one-third (35%) of respondents want a common SOC UI/UX that can be customized for different roles and responsibilities, while 34% believe it's important for a common SOC UI/UX to offer customized reporting/dashboards for different roles and responsibilities. In this way, a common UI/UX could support the needs, roles, responsibilities, and nuances from junior to the most experienced analysts.

Top 5 Most Important Attributes of a Common Security Operations UI/UX

1. Minimizes or eliminates the need to use product-based UI/UX.
2. Tracks and manages security event lifecycle.
3. Searches on-premises and cloud-based security data.
4. Customizable UI/UX for different roles and responsibilities.
5. Customizable reporting/dashboarding capabilities for different roles and responsibilities.

Figure 8. Most Important Attributes of a Common Security Operations UI/UX

In your opinion, what would be the most important attributes of a common UI/UX for security operations? (Percent of respondents, N=300, five responses accepted)



Source: Enterprise Strategy Group

Tracking and managing security events across the entire lifecycle goes beyond the UI/UX alone, requiring coordination of a multitude of tasks across numerous processes and projects. This makes security operations extremely complex and difficult to scale.

To address this problem, many organizations have documented processes, developed process templates, created runbooks, and leveraged technology for process automation and orchestration.

Security operations process automation has become a requirement for most organizations: 31% of organizations have deployed technologies designed for process automation extensively, while another 36% have done so on a limited basis.

Which security operations process will be automated? Survey respondents were asked to identify their organization's top priorities (see Figure 9). The research reveals that:

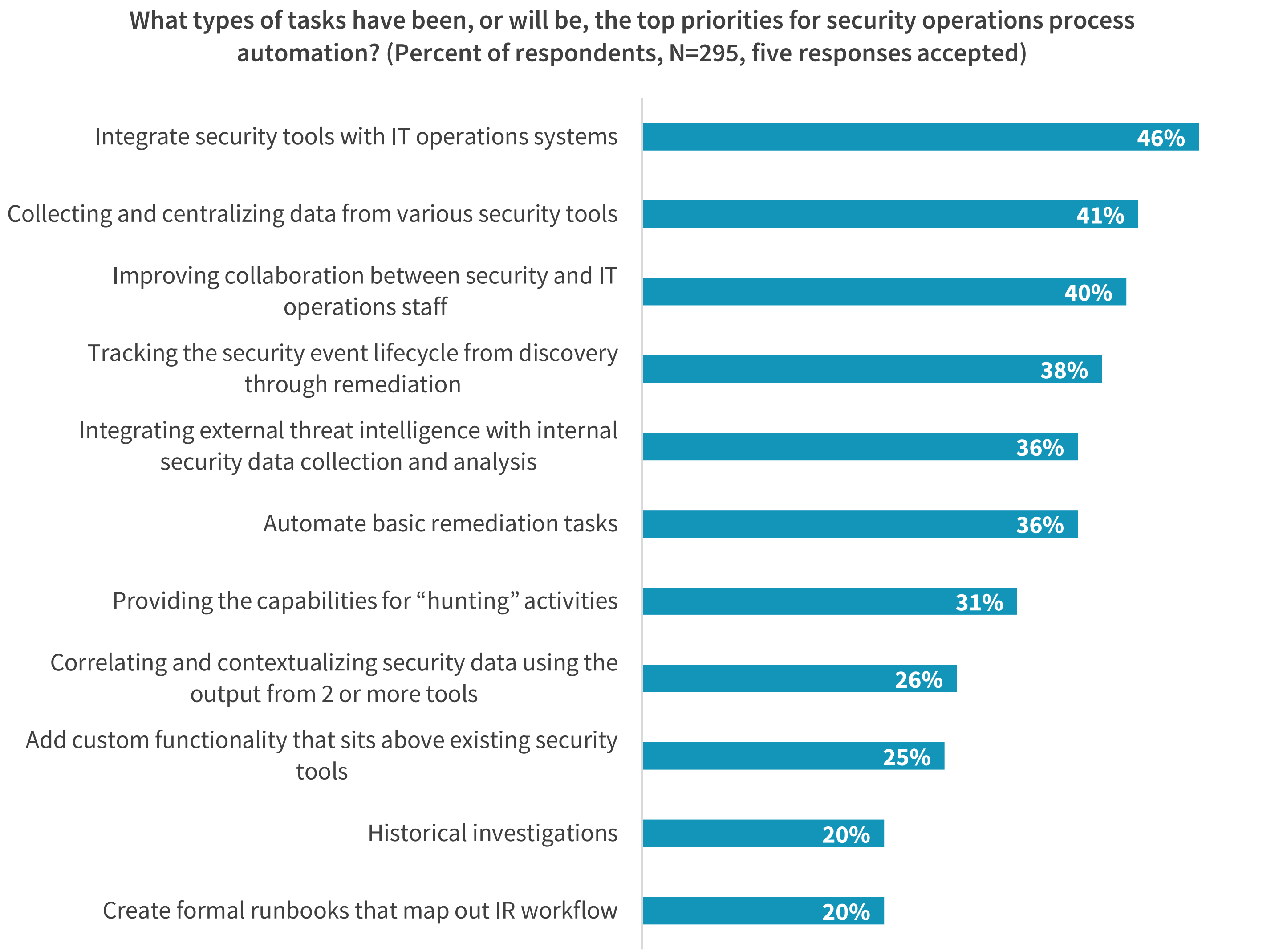
- Nearly half (46%) want to automate processes that cross between security and IT operations. Additionally, 40% want to improve collaboration between security and IT staff. Why? When security teams detect a problem, they often turn to IT operations teams to take an action like quarantining a system, segmenting a network, or patching software. Automating these cross-department processes could accelerate risk mitigation or incident response, helping to safeguard the organization.
- 41% want to automate data collection from various security tools. Security investigations require data analysis across areas like endpoints, identity repositories, networks, cloud workloads, and threat intelligence telemetry. Simply fetching this data can be time consuming, so security professionals would like to automate as many of these tedious tasks as possible.
- 38% want to track the security event lifecycle. Just as organizations want one UI/UX to view events, they also want tools to automate all security processes from event detection through response and recovery. This would be another important attribute for a security operations UI/UX.

Top 5 Priorities for Security Operations Automation

1. Integrate security tools with IT operations systems.
2. Collect and centralize data from various security tools.
3. Improve collaboration between security and IT operations staff.
4. Track the security event lifecycle from discovery through remediation.
5. Integrate external threat intelligence with internal security data collection and analysis, and automate basic remediation tasks.

Aside from these three, security professionals have a long list of other process automation priorities. To improve the chances for success here, SOC analysts would benefit from a common UI/UX capable of acting as a workbench for monitoring and managing process automation.

Figure 9. Top Priorities for Security Operations Process Automation



Source: Enterprise Strategy Group

The Bigger Truth

Security operations technology grew organically over the past 20 years as SOC teams added new tools incrementally over time. This drove the need to add security professionals and skills for day-to-day management and administration. Meanwhile, the volume and sophistication of cyber threats increased while the IT attack surface expanded to mobile applications, IoT devices, and cloud-based workloads.

Unfortunately, these trends have led to a security operations mismatch where SOCs have become too complex and labor-intensive to keep up with the scale and erudition of modern cyber threats. This may be one of the main reasons why there continue to be so many devastating cyber-attacks and data breaches.

CISOs seem to recognize this imbalance and are responding by consolidating and integrating security operations technology. The goal? Build a tightly coupled security operations and analytics platform architecture (SOAPA) that includes security data pipelining services, multidimensional analytics, and security operations process management.

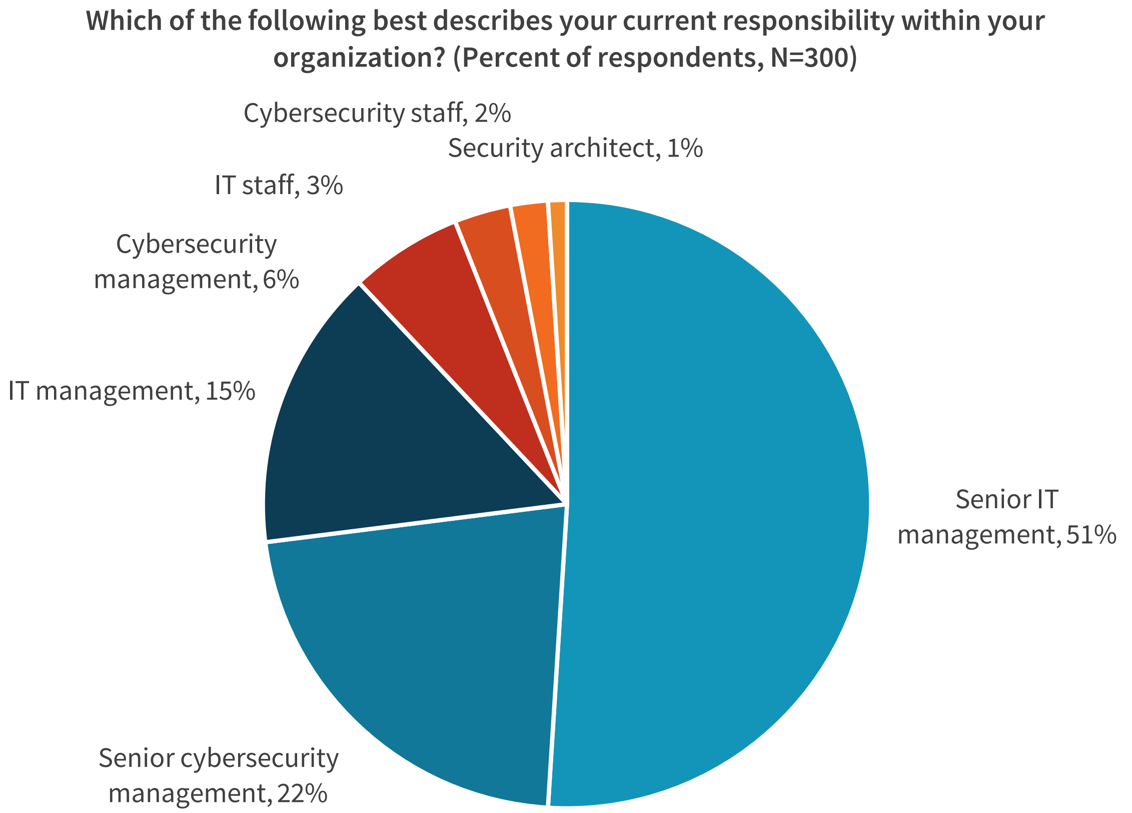
ESG research indicates that many organizations have achieved numerous benefits from security operations technology consolidation and integration. This project explored whether these benefits could be accentuated through a common security operations UI/UX, something that has been missing to date. Based upon this research project, it is safe to conclude that most security professionals believe a common security operations UI/UX could improve SOC efficacy and efficiency.

Appendix: Research Methodology and Demographics

To gather data for this report, ESG conducted a comprehensive survey of cybersecurity and IT professionals with knowledge of and participation in their organization's security operations. All respondents were located in North America and employed at organizations with at least 1,000 employees. The survey was fielded between February 25, 2020 and March 18, 2020. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 300 respondents remained. Figures 10-14 detail the demographics of the respondent base, including their role and responsibility areas. Firmographics include organizations' total number of employees, primary industry, and annual revenues. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

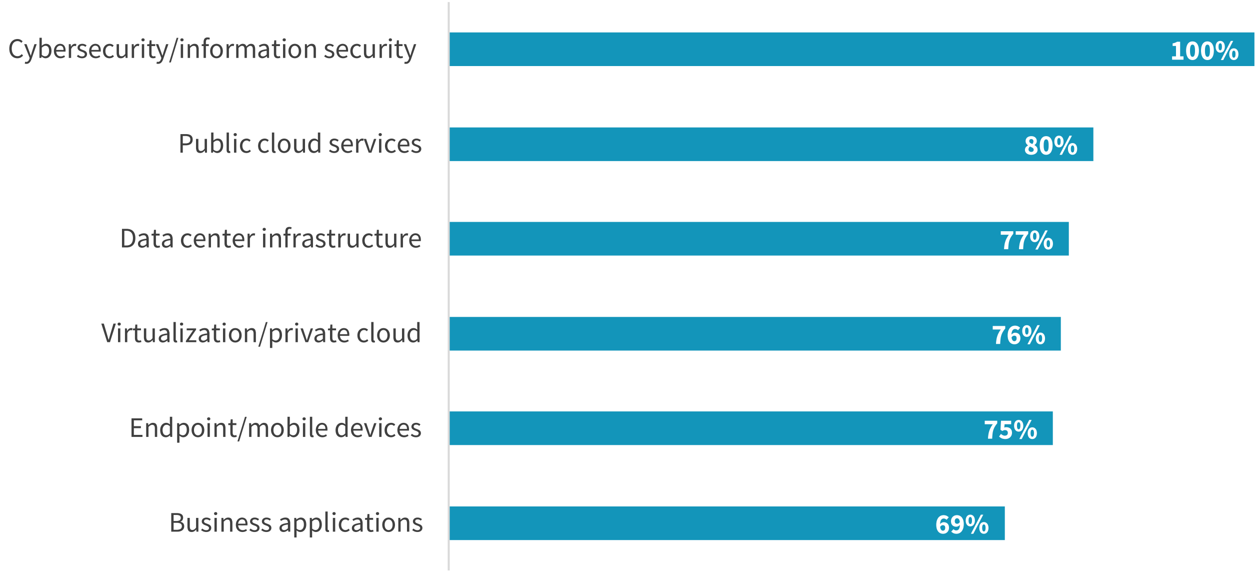
Figure 10. Survey Respondents by Role



Source: Enterprise Strategy Group

Figure 11. Survey Respondents by Areas of Responsibility

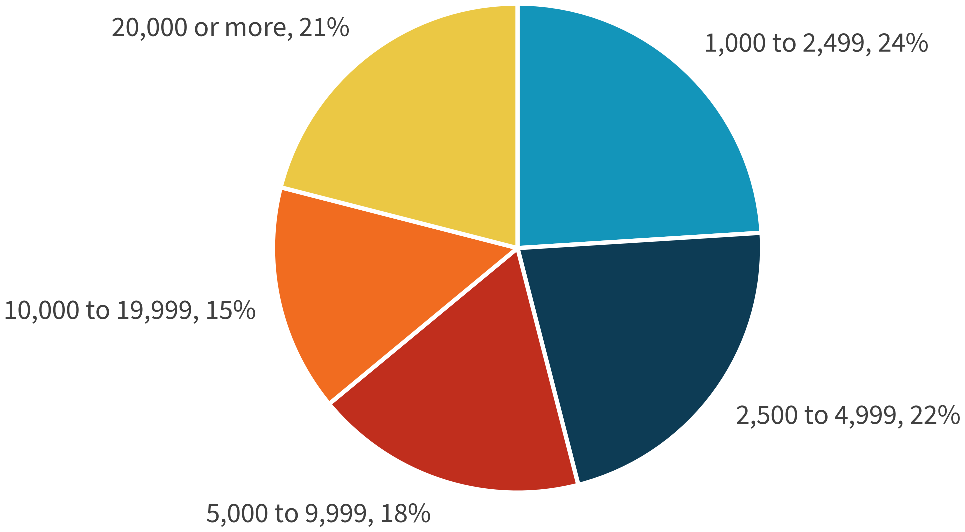
In which of the following areas do you have significant involvement in the planning, implementation, and/or operations of technology for your company? (Percent of respondents, N=300, multiple responses accepted)



Source: Enterprise Strategy Group

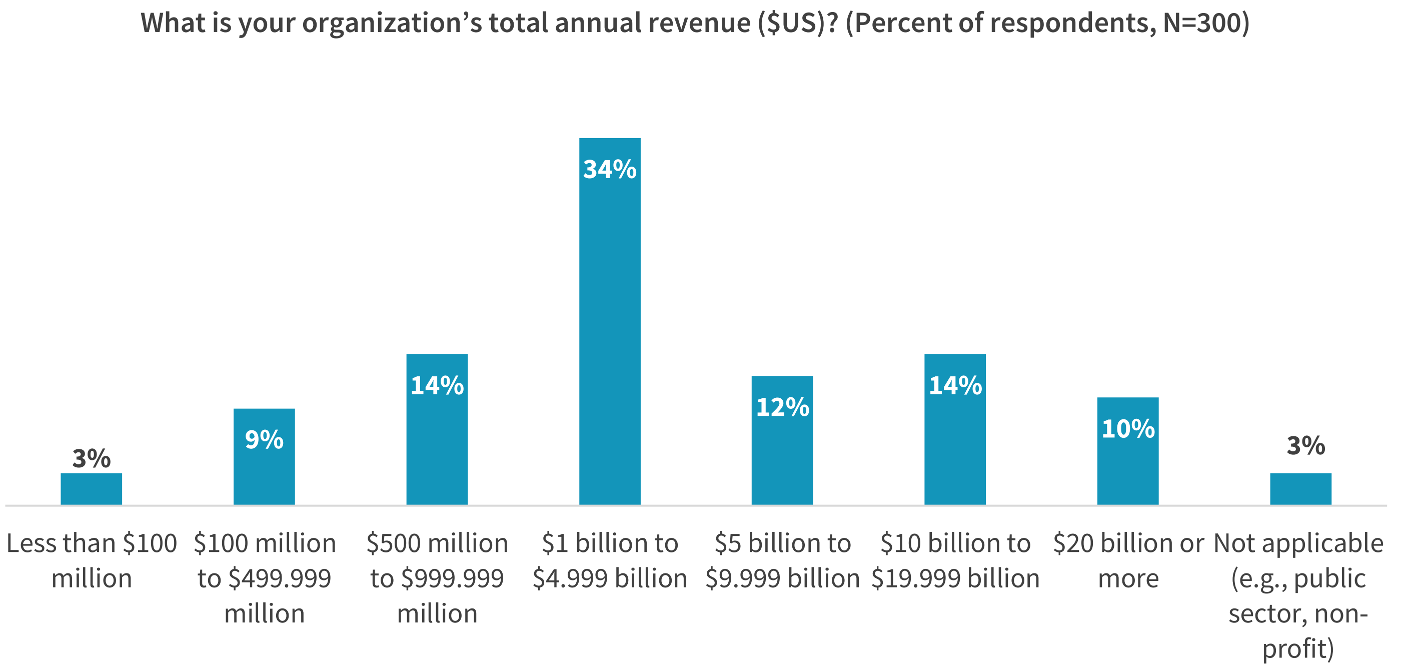
Figure 12. Respondents by Number of Employees at Their Organization

How many total employees does your organization have worldwide? (Percent of respondents, N=300)



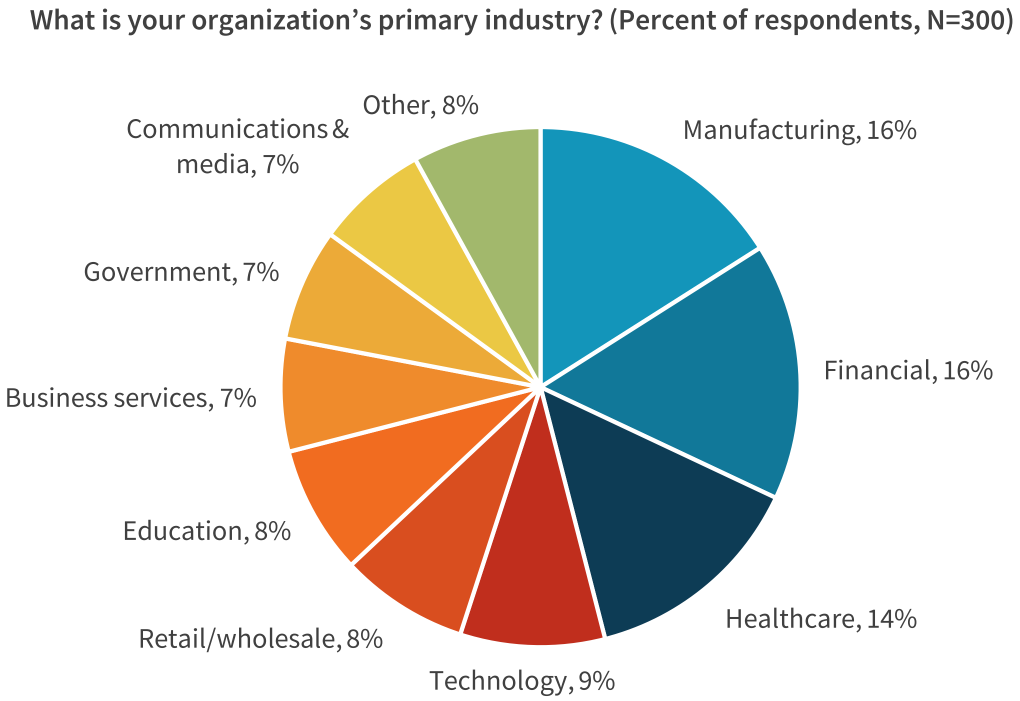
Source: Enterprise Strategy Group

Figure 13. Respondents by Revenue at Their Organization



Source: Enterprise Strategy Group

Figure 14. Respondents by Industry



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188