Enterprise Strategy Group™ by TechTarget

SOC Market Trends Report:

Skills Shortages, Growing Complexity, and the Need for Greater Analyst Efficiency All Support the Case for a Shift Toward Unified Security Operations

Jon Oltsik, *Distinguished Analyst & ESG Fellow*
ENTERPRISE STRATEGY GROUP

OCTOBER 2023

This Enterprise Strategy Group eBook was commissioned by Splunk and is distributed under license from TechTarget, Inc.

CONTENTS

CLICK TO FOLLOW

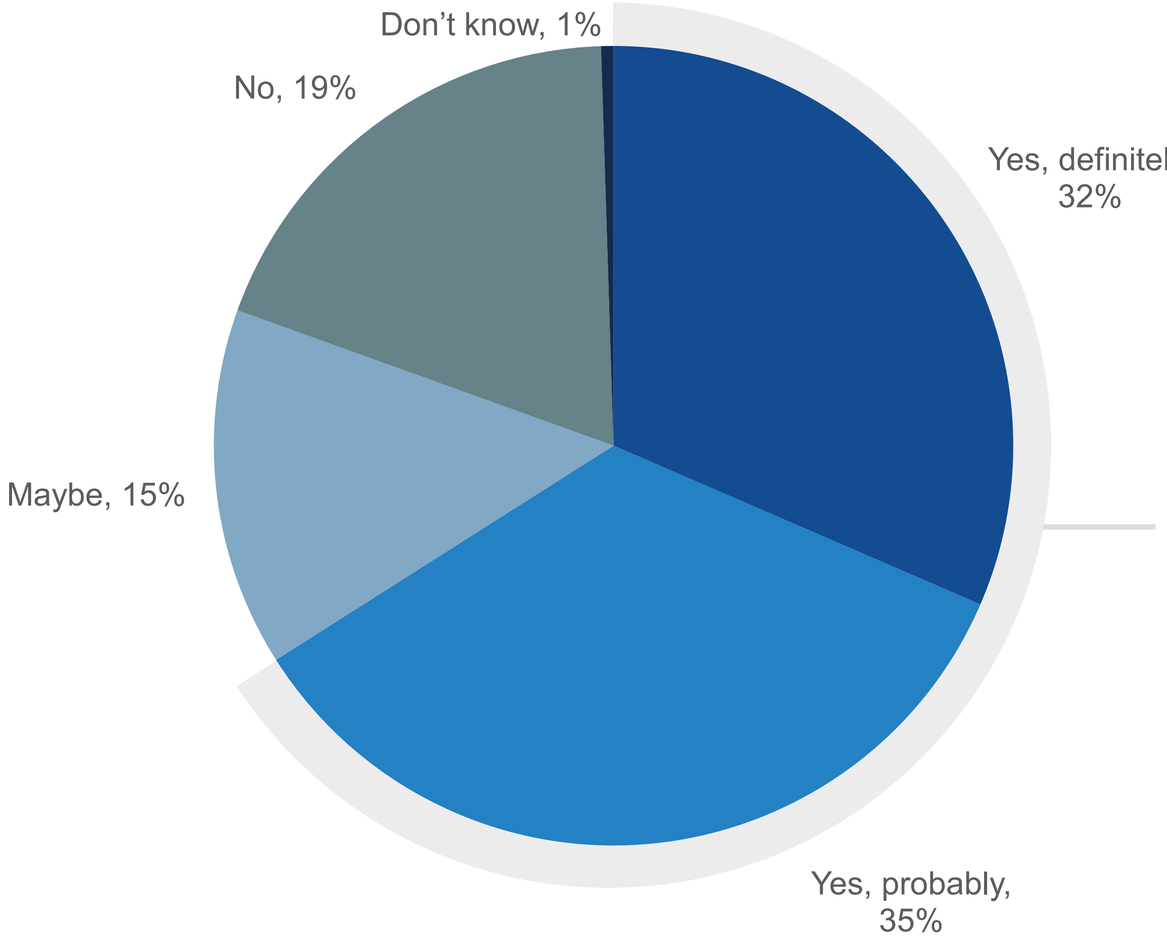
The State of the SOC

The Problematic Frequency of Incidents

CISOs have good reason to invest in security operations: They are experiencing security incidents that could have been prevented if their security operations were improved. In fact, when looking back over the past 12 months, two-thirds of surveyed security leaders said they've experienced an incident that could have been prevented if their team were more capable.

Of course, these security incidents lead to consequences, like business operations disruptions, sensitive data theft, and regulatory compliance violations.

The Perception That Preventable Security Incidents Are Occurring Within Organizations



Two-thirds

of surveyed security leaders said they've experienced an incident **that could have been prevented if their team were more capable.**

BACK TO CONTENTS

Top Security Operations Objectives

Given the security incident frequency, it is not surprising that organizations have numerous security operations objectives, such as improving cyber-risk identification, enhancing cyber resilience, and better operationalizing threat intelligence.

These goals indicate an effort to better align security with the business. For example, improving cyber resilience can help organizations recover from cyber attacks while maintaining business operations. In support of this, organizations also want to concentrate their efforts on business-critical systems and data.

Of course, these security operations objectives depend upon more efficient and effective data collection, processing, and analysis to guide real-time risk mitigation and incident response decisions.

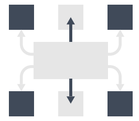
Organizations' Top 5 SecOps Objectives for the Next 12-18 Months

46%
Improve cyber-risk identification

43%
Improve cybersecurity/digital resilience

36%
Improve the operationalization of external threat intelligence

34%
Prioritize security incidents that impact critical business assets and/or sensitive data



34%
Improve our ability to combine and enrich multiple security data sources to provide more context around security events

BACK TO CONTENTS

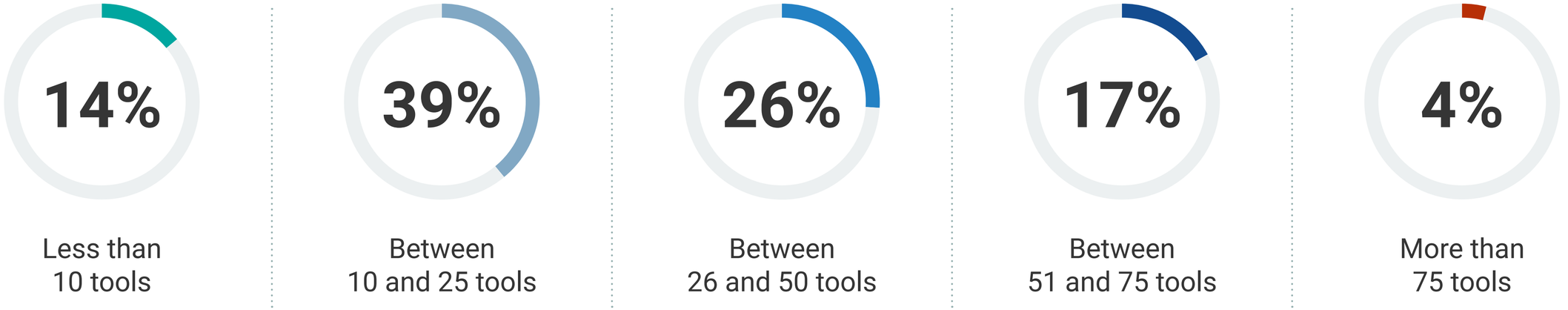
Security Operations Tool Sprawl Hinders Effectiveness

Security operations is built on a foundation of assorted tools for cyber-risk management, threat intelligence analysis, threat detection and response, and process automation.

Nearly two out of five organizations (39%) use between 10 and 25 disparate security tools for security operations, while nearly half (47%) use more than 25 incongruent security operations tools.

Since each tool requires user training, deployment, configuration, tuning, and ongoing administration, organizations risk additional operational overhead as the SOC team scrambles from tool to tool to maintain threat prevention, detection, and response.

Number of SecOps Tools Deployed Within Organizations Today

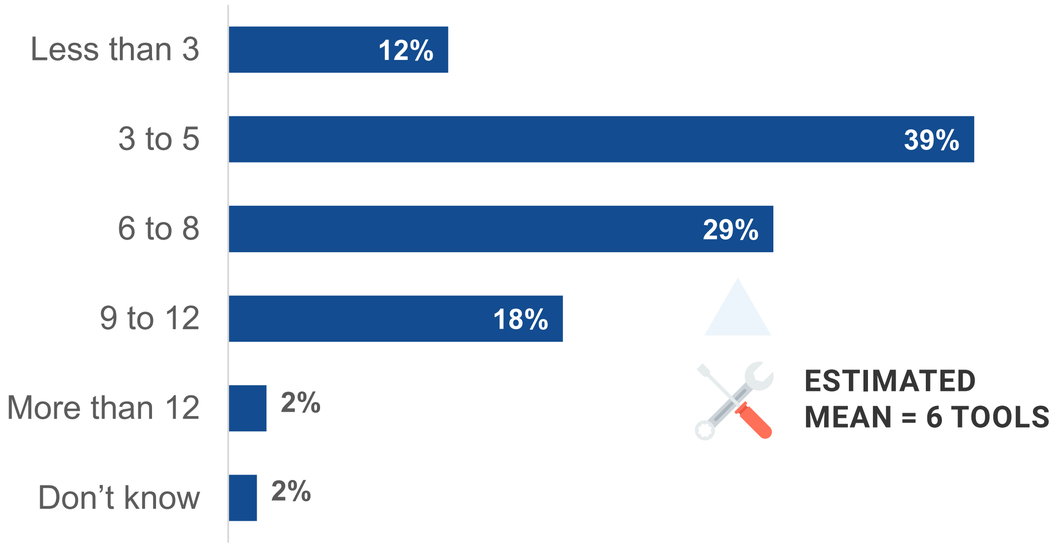


BACK TO CONTENTS

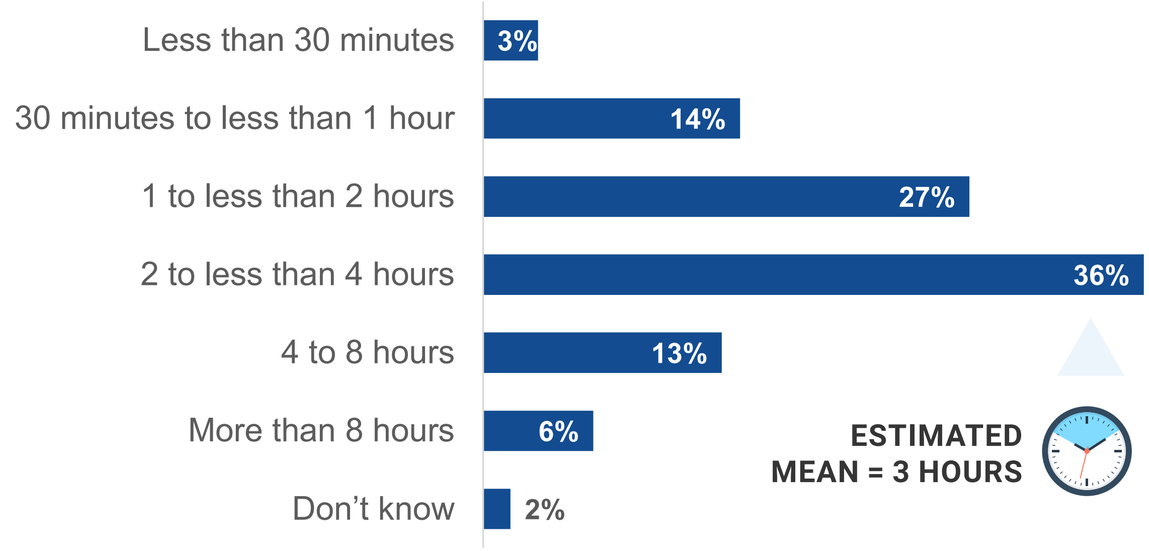
Investigating Alerts Today Requires Many Tools and Takes Significant Time

On average, analysts interact with 6 tools to investigate an alert, requiring an average of 3 hours dedicated to resolving investigations. Unfortunately, that's far from the entire picture. Security analysts often have dozens of open investigations based on critical alerts. Analysts must know what information they need, where it is located, and how to get it in a timely manner. Cloud computing proliferation has driven an expanding attack surface, generating more alerts and investigations.

Number of SecOps Tools an Analyst Uses to Investigate, Triage, and Remediate Alerts



Person-hours Analysts Allocate to the Typical Incident



On average, analysts interact with
6 tools to investigate an alert, requiring an average of 3 hours
dedicated to resolving investigations.

BACK TO CONTENTS

Challenges Managing Multiple SecOps Tools

Respondents almost ubiquitously (93%) report one or more issues directly tied to managing numerous SecOps tools, including high costs, a reliance on manual processes, and dawdling threat detection and response.

Furthermore, managing cyber-risks or coordinating workflows across an army of point tools can be difficult. This situation should trigger alarm bells in the CISO's office.

93%

of organizations report one or more issues **directly tied to managing numerous SecOps tools**.

Top 5 Challenges Related to SecOps Tool Sprawl

Cost and purchasing complexity from dealing with many vendors

Managing more security products increases reliance on manual processes

Managing too many tools leads to slower investigation and response times

Too many tools make it hard to assess security risk

Too many tools make it hard to coordinate security workflows

BACK TO CONTENTS

Skills Shortage Realities

While managing a multitude of security operations tools, alerts, and investigations is difficult on its own, many organizations are forced to do so while short-staffed or lacking the necessary security operations skills.

Alarmingly, 89% organizations are being impacted by a security skills shortage in the labor market, and 73% of cybersecurity professionals believe this skills shortage has been affecting their organization for multiple years with no improvement.

Acute skills shortages in areas like data science skills, knowledge sharing, and process automation make it difficult to achieve security operations objectives like improving cyber-risk identification, cyber resilience, or the ability to operationalize threat intelligence.

89%

of organizations are being impacted by a security skills shortage in the labor market.

7 Weakest Skills Areas for Security Operations Teams

BACK TO CONTENTS

Impact of the Cybersecurity Skills Shortage

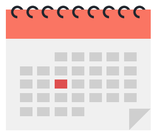
Too many tools, not enough people, and a lack of the right skills constitute a recipe for security operations failure. Additionally, security pros point to explicit implications tied to skills shortages, like an increasing workload (49%), a lack of time for training (38%), open jobs (33%), and staff burnout (33%).

CISOs can't hire their way out of this predicament. Rather, they need a security operations strategy that includes process automation, advanced analytics, and managed services to help alleviate the burden on the existing SOC team.

Top Impacts of the Cybersecurity Skills Shortage

49%
Increasing workload on existing cybersecurity staff

38%
Security team is often too busy managing their workload to keep up with training



33%
New security jobs remain open for weeks or months

33%
High "burn out" and/or attrition rate amongst the cybersecurity staff

32%
My organization has had to delegate some security tasks to IT that it would normally do itself

BACK TO CONTENTS

Security Operations Challenges

General SecOps Challenges

> With the state of security operations, CISOs should expect an assortment of challenges. Indeed, **96% of organizations experience one or several security operations challenges across people, processes, and technologies.**

Jon Oltsik, Distinguished Analyst & ESG Fellow
ENTERPRISE STRATEGY GROUP

Top SecOps Challenges Organizations Face Today

Detecting, escalating, and responding to security incidents

Monitoring security across a growing attack surface

Better prioritizing incidents for investigation and response

Keeping pace with compliance mandates/ requirements

Keeping up with the volume of security alerts

BACK TO CONTENTS

SecOps Workflow Challenges

Clearly, CISOs face a toxic mix of too many security operations tools and increasing volumes of security alerts and investigations. This is exemplified by the top SecOps workflow challenges reported by respondents and the fact that 94% of organizations had one or several of these.

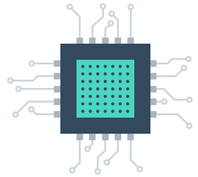
Organizations struggle to collect, process, and analyze the right data in a timely manner. Many firms also face organizational issues in trying to coordinate security operations across multiple teams using multiple tools. Finally, process automation remains immature at many organizations.

Top SecOps Workflow Challenges Organizations Face Today

Network security monitoring needs improvement

Use of too many tools makes it hard to understand what's really going on in our environment

Integrating with disparate and/or siloed systems creates gaps and inefficiencies



Complexity experienced as result of multiple teams and technologies

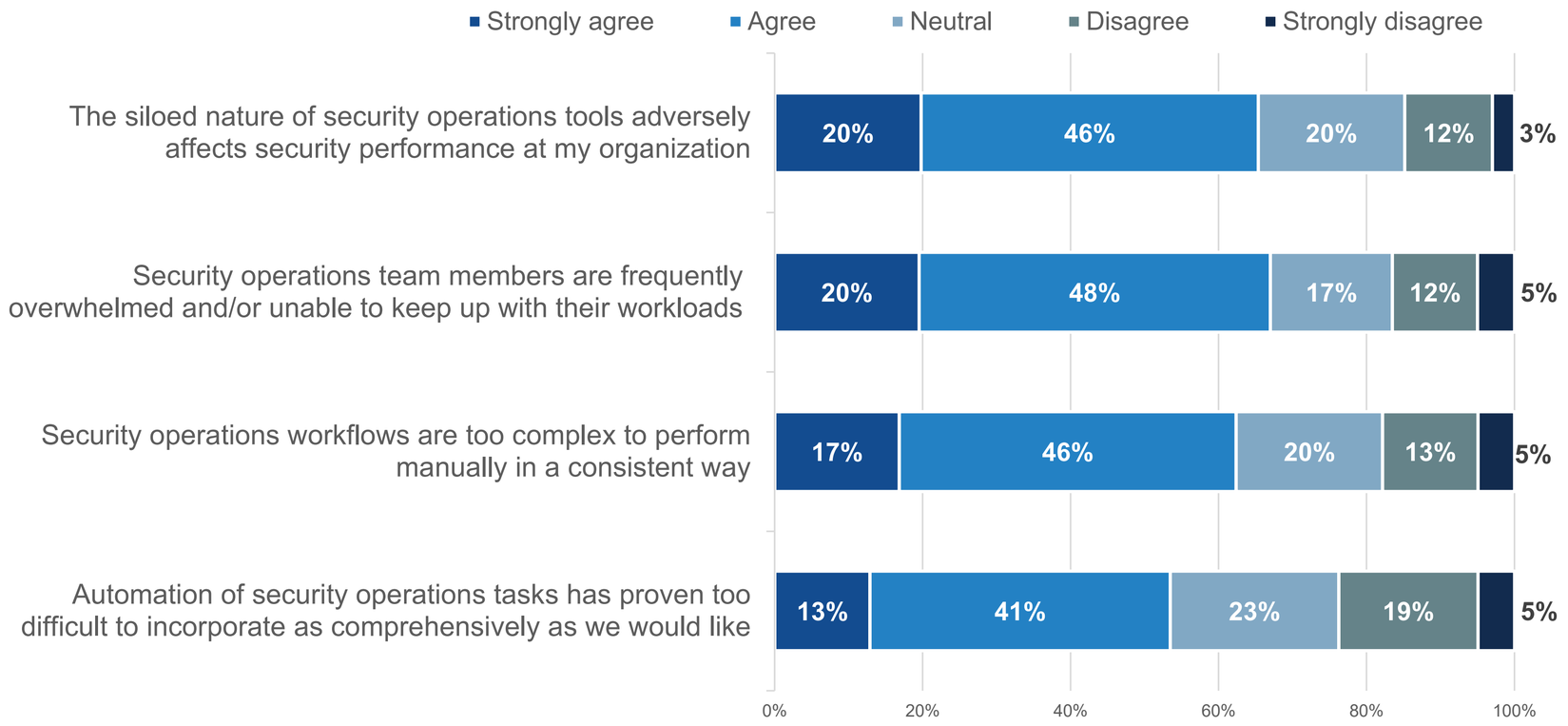
Too much of the work is still manual

BACK TO CONTENTS

Security Operations Opinions

Facing all these challenges, survey respondents had strong opinions about the state of security operations at their organizations. Roughly two-thirds agree both that security operations silos negatively impact performance and that workloads are complex and overwhelming.

Sentiment Related to Various Aspects of Security Operations Teams and Tasks



Roughly two-thirds agree both that security operations silos negatively impact performance and that workloads are complex and overwhelming.

BACK TO CONTENTS

Drivers for Change in the SOC

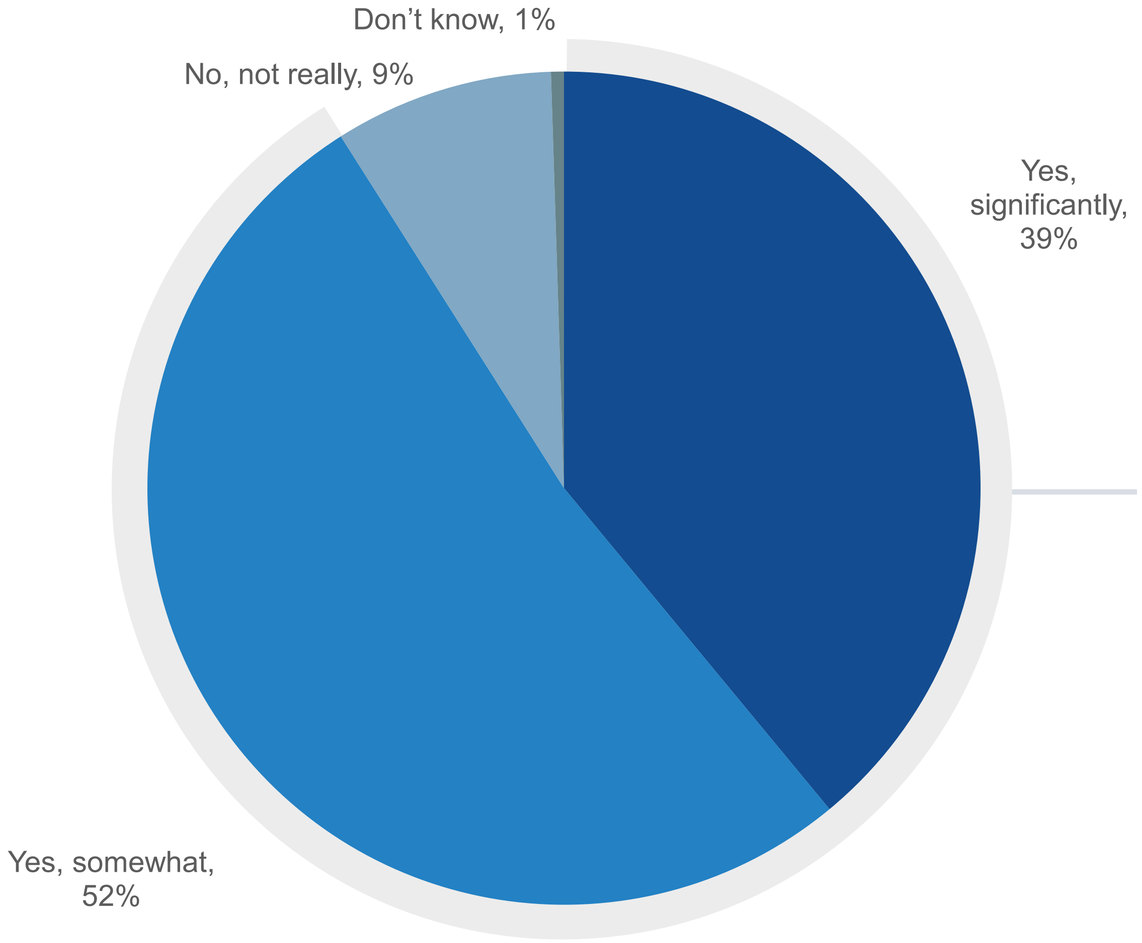
Digital Resilience Is Top of Mind

The top areas where organizations struggle with digital resilience include recovering from a security incident, prioritizing vulnerabilities to remediate, managing security controls, hardening critical business systems, and implementing threat detection rules.

The need to improve digital resilience is a catalyst for security operations changes, with 9 out of 10 respondents saying it factors into their organization's SecOps strategies more than it did 12 months ago.

Executives and board members understand that modern businesses run on the back of technology. Therefore, digital resilience must be a high priority.

Is digital resilience more important now vs. 12 months ago?



9 OUT OF 10

respondents say the need to improve digital resilience factors into their organization's SecOps strategies **more than it did 12 months ago.**

BACK TO CONTENTS

Opinions About Security Operations Improvement

Based on the challenges described previously, CISOs know they must improve the efficacy and efficiency of their security operations. Indeed, 84% of organizations claim it is among their top 5 technology priorities.

Surveyed security professionals offered many opinions for security operations improvement, with the vast majority agreeing they can improve security by integrating technologies, that they see a lot of potential to improve the productivity of junior analysts, and that they want to develop better ways for knowledge sharing across the SOC.

It's worth noting that business executives are participating in the security operations process by pressuring CISOs to improve security posture and cyber-risk mitigation.

84%

of organizations claim improving the efficacy and efficiency of their security operations **is among their top 5 technology priorities.**

Organization Sentiment Related to Security Operations

BACK TO CONTENTS

Top Priorities for Security Operations Investments

A vast majority (88%) of organizations plan to increase spending on security operations over the next 12 to 18 months, illustrating the urgency of efficacy and efficiency improvements.

Security operations training is a high priority, along with moving security operations technologies to the cloud and actively developing an integrated security operations software architecture.

Note, too, that CISOs plan to invest in tools for process automation. This can help them bolster productivity and address the impact of the cybersecurity skills shortage.

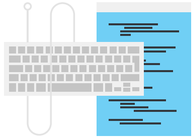
88%

of organizations plan to increase spending on security operations over the next 12 to 18 months.

Organizations' Top Priorities for Security Operations Investment Over the Next 24 Months

31%
Provide security operations training for cybersecurity and IT operations staff

25%
Move security analytics/ operations technologies from on-premises to the cloud



24%
Actively develop and build an integrated software architecture for security analytics and operations tools

23%
Hire more security operations personnel

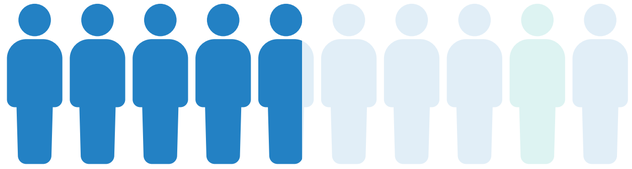
22%
Purchase security operations tools designed to help an organization automate and orchestrate security operations processes

BACK TO CONTENTS

The Case for a Shift Toward Unified Security Operations

Steps for Change

Security professionals offered their suggestions for improving security operations workflows. Aside from automating SOC processes and reducing the number of SOC tools, nearly half (49%) of security professionals recommend implementing a common work surface for all SOC workflow activities.



Nearly half

of security professionals recommend **implementing a common work surface for all SOC workflow activities.**

Steps to Take That Could Most Improve SecOps Workflows

55%
Automating SOC workflow tasks and processes

51%
Reducing the number of tools used as part of SOC workflows

49%
Implement a common interface or work surface for all SOC workflow activities

47%
More training for SOC personnel

46%
Adopting and formalizing more SOC workflow best practices

BACK TO CONTENTS

Value of a Common SecOps Work Surface

Many security professionals believe it would be valuable to unify security operations workflows using a single work surface: 97% report this shift would deliver material value.

Why? A common SecOps work surface could help accelerate threat detection, investigation, and response; alleviate the need to train security analysts on multiple tools; and improve communications within the SOC.

This could go a long way toward improving the productivity of SOC teams impacted by the cybersecurity skills shortage while minimizing the operational issues around managing various security operations technologies.

97%

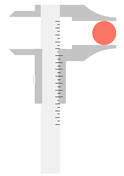
report the shift to unifying security operations **would deliver material value.**

Top Reasons SecOps Workflow Unification via a Single Work Surface Is Seen as Valuable

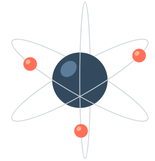
48%
Accelerating the time needed for incident detection, investigation, and response

43%
Easing the burden of training the SOC staff on multiple security tools

43%
Improving communications within the SOC



40%
Helping my organization use more of the functionality of individual security tools



39%
Increasing utilization of security telemetry

BACK TO CONTENTS

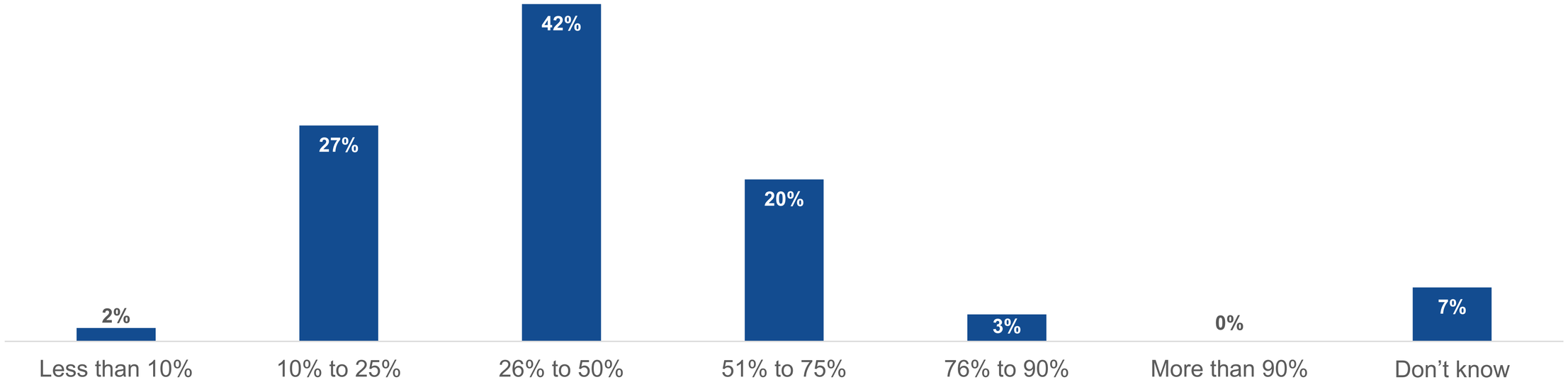
Expected Efficiencies From a Pivot to a Single Work Surface

Recall that CISOs are motivated to improve security operations' efficacy and efficiency. Survey respondents believe that a common SecOps work surface could greatly help organizations achieve this goal.

How? By accelerating detection/response time, easing the training burden, and improving communications. In fact, 42% of security professionals believe that investigation efficiency could be improved by 26% to 50%, while 23% believe investigation efficacy could improve by more than 50%.

This would help organizations enhance analyst productivity in the face of acute and persistent skills shortages, a growing attack surface, and increasing volumes of security alerts.

Investigation Efficiency Increases Expected if Security Analysts Could Conduct Investigations Using a Single Work Surface



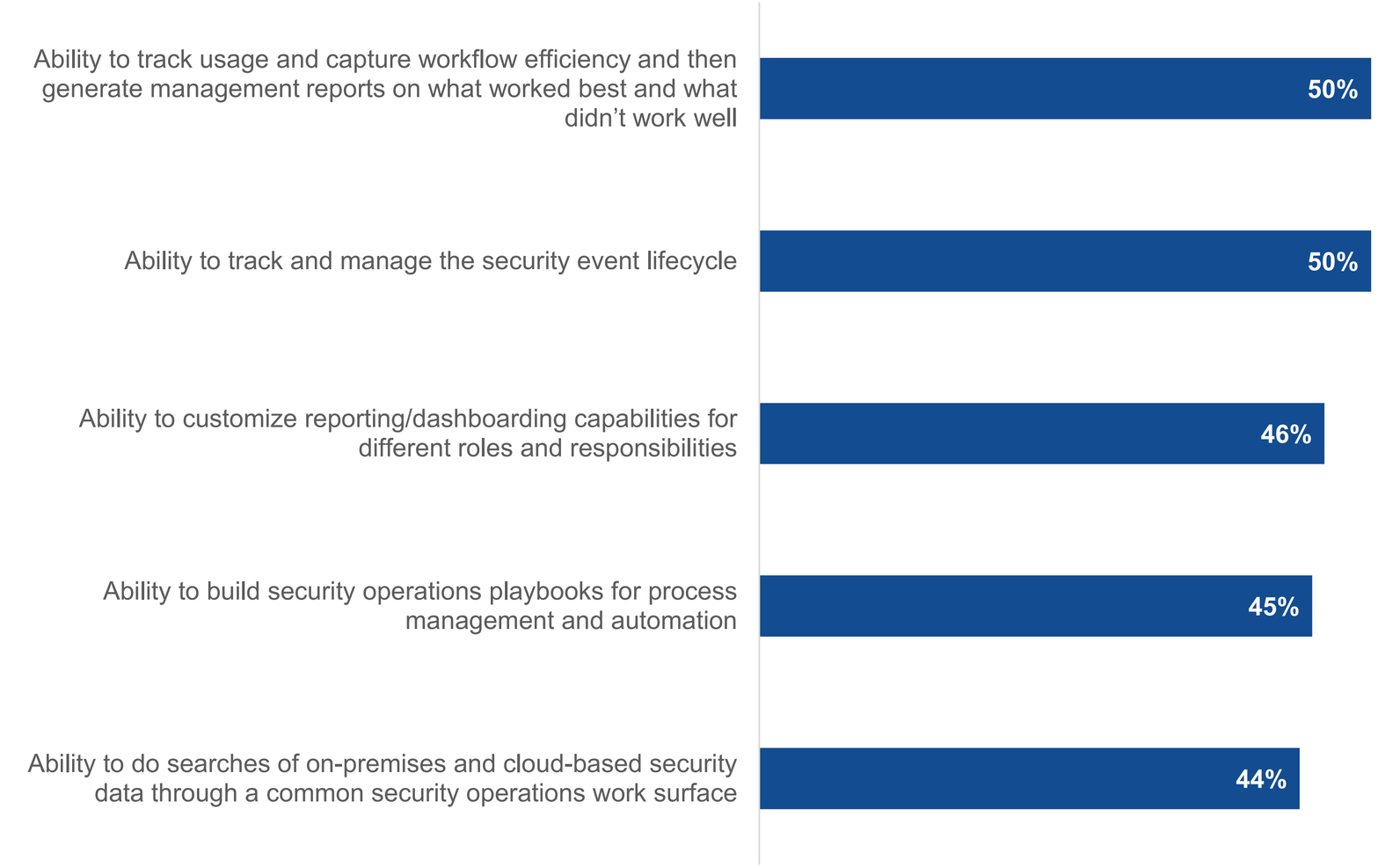
BACK TO CONTENTS

Important Attributes of a Common SecOps Work Surface

Security professionals also have a vision of what a common SecOps work surface should look like. They want the ability to track and capture workflows, generate reports, track and manage security event lifecycles, and customize dashboards for different roles.

In other words, they want a powerful UI/UX for all SOC tasks and personnel needs across cyber-risk management, threat detection, forensic investigations, and incident response.

Most Important Attributes of a Solution That Provides a Common Work Surface for Security Operations



BACK TO CONTENTS

splunk>®

Splunk Security provides a unified, simplified and modernized security operations experience for your SOC.

Learn More

Research Methodology and Demographics

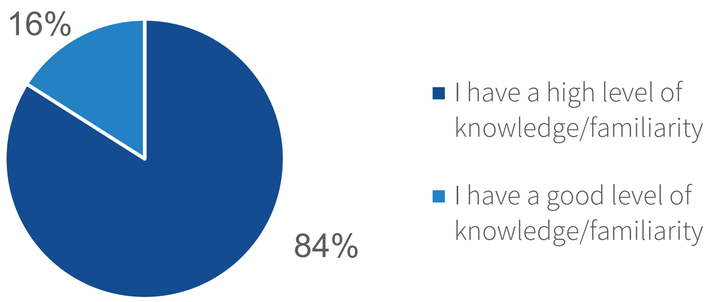
To gather data for this eBook, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of 200 security decision-makers and influencers with intimate knowledge of the organization's security operations/alerting/event detection technologies and performance.

All respondents were employed at enterprise organizations and were based in the U.S. (63%) and Canada (37%). The survey was fielded in May 2023.

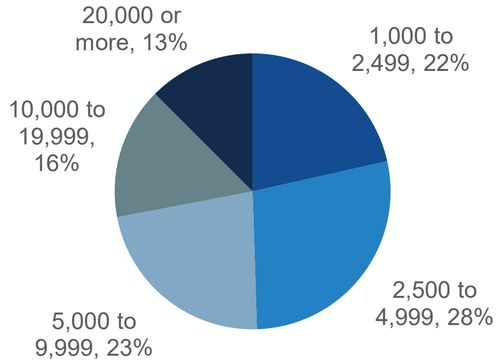
The margin of error at the 95% confidence level for this sample size is + or – 7 percentage points. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding.

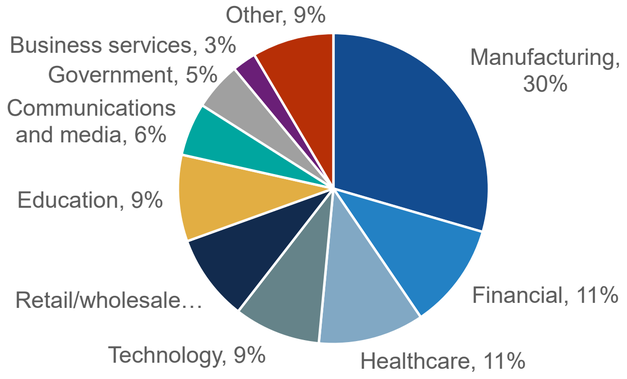
Respondents' knowledge of their organizations security strategies (i.e., risk management, incident detection, security investigations/forensics, etc.), N=200)



Respondents, by company size (N=200)



Respondents, by industry (N=200)



BACK TO CONTENTS

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