Enterprise Strategy Group | **Getting to the bigger truth.™**

An ESG Research Insights Report

2017: Security Operations Challenges, Priorities, and Strategies

By Jon Oltsik, Senior Principal Analyst

March 2017

This ESG Research Insights Report was commissioned by Siemplify and is distributed under license from ESG.

Contents

Executive Summary

In early 2017, the Enterprise Strategy Group (ESG) completed a research survey of 150 IT and cybersecurity professionals with knowledge of, or responsibility for security operations at their organizations. Survey respondents were in North America and came from organizations ranging in size: 7% of survey respondents worked at organizations with 500 to 999 employees, 21% of survey respondents worked at organizations with 1,00 to 2,499 employees, 21% worked at organizations with 2,500 to 4,999 employees, 23% worked at organizations with 5,000 to 9,999 employees, 9% worked at organizations with 10,000 to 19,999 employees, and 22% worked at organizations with more than 20,000 employees. Respondents represented numerous industry and government segments, with the largest participation coming from manufacturing (23%), financial (i.e., banking, securities, insurance, 19%), retail/wholesale (11%), health care (11%), information technology (10%), and government (i.e., federal, state, local, 6%).

Based upon the data collected as part of this research project, ESG concludes:

- **Security operations is fraught with people, process, and technology challenges.** Security operations teams are engaged in a constant struggle to keep up with the volume of security alerts, maintain the right skills, and manage manual IR processes. Furthermore, organizations and the industry are chronically understaffed in cybersecurity or lack the advanced skills necessary for security operations. These factors limit security operations effectiveness and increase business and IT risk. Security operations have become a cybersecurity bottleneck. **Security operations improvement is a high priority**. Security operations weaknesses make organizations extremely vulnerable to targeted attacks by sophisticated cyber-adversaries. CISOs seem to recognize this risk gap and are ramping up security investments accordingly—nearly three-quarters of organizations plan to increase spending on security operations this year. CISOs plan to add new threat detection tools, integrate security point tools together into a common architecture, and improve processes and technologies used for security investigations.

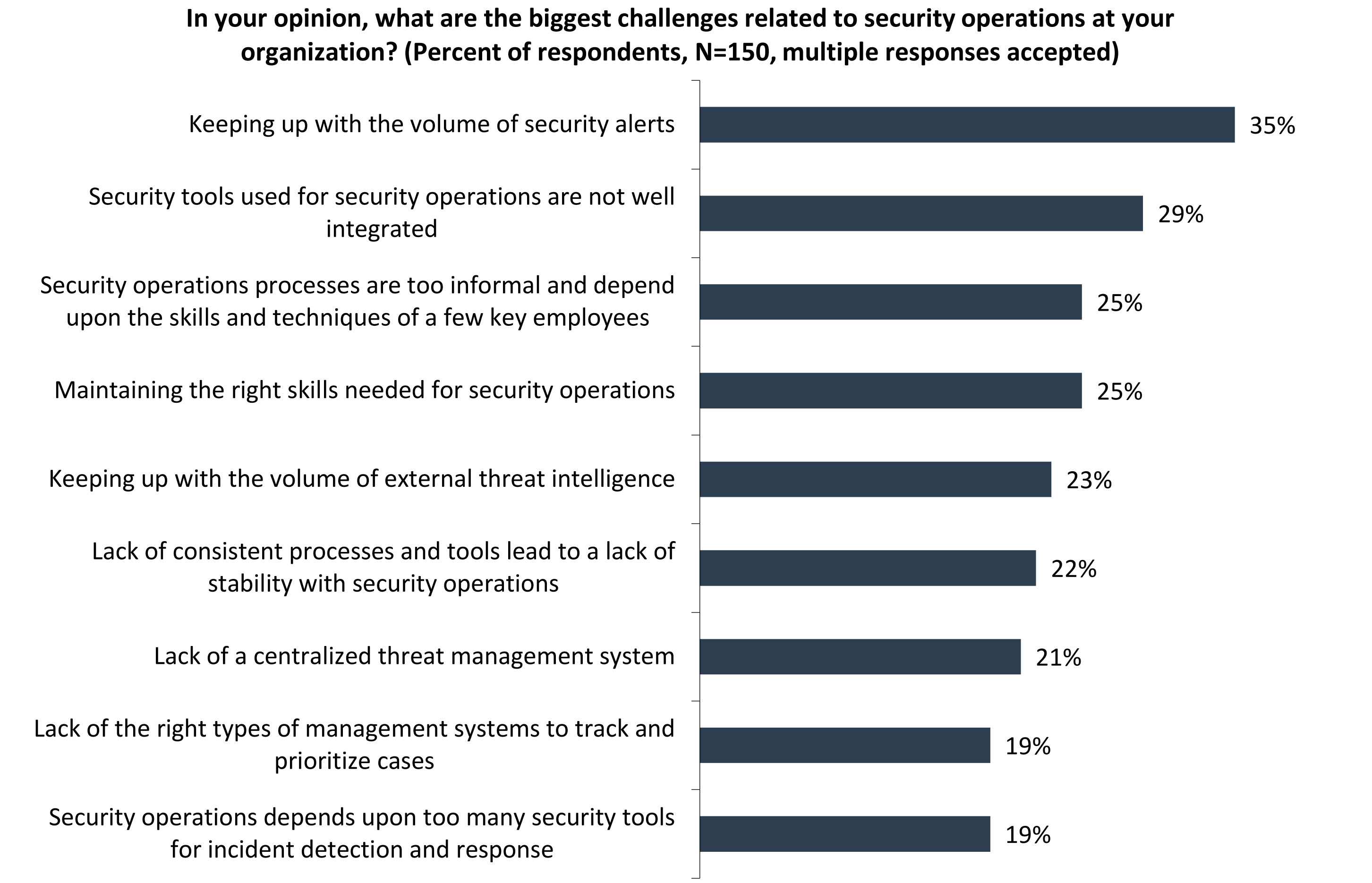
- **Organizations are embracing security orchestration.** Many firms are adopting tools and techniques for security operations orchestration in response to today's skills deficits and reliance on manual processes and dispersed tools. Fully 96% of respondents have security orchestration projects underway, are planning to launch, or are contemplating launching such initiatives.

- **Orchestration is becoming a centralized platform.** Ultimately what is being demanded is a centralized "workbench" for security analysts to drive efficiency: a platform that provides the full scope of threat response to unify people, process, and technology, and not just automation of selective tasks. Organizations really want the ability to consolidate, enrich, and contextualize cases to provide the needed visibility to triage the high volume of alerts.

Security Operations Situational Analysis

Security operations processes can be complex, requiring multiple tools, highly skilled security technicians, cooperation between security and IT operations groups, and an assortment of manual processes. Little wonder then why survey respondents point to a long list of security operations challenges. More than one-third (35%) of organizations find it challenging to keep up with the volume of security alerts, 29% are challenged because security tools used for security operations are not well integrated, 25% claim security operations is challenging because processes are too informal and depend upon the skills and techniques of a few key employees, and 25% say that it can be challenging to maintain the right skills for security operations (see Figure 1).

Figure 1. Top Security Operations Challenges Reported by Respondents

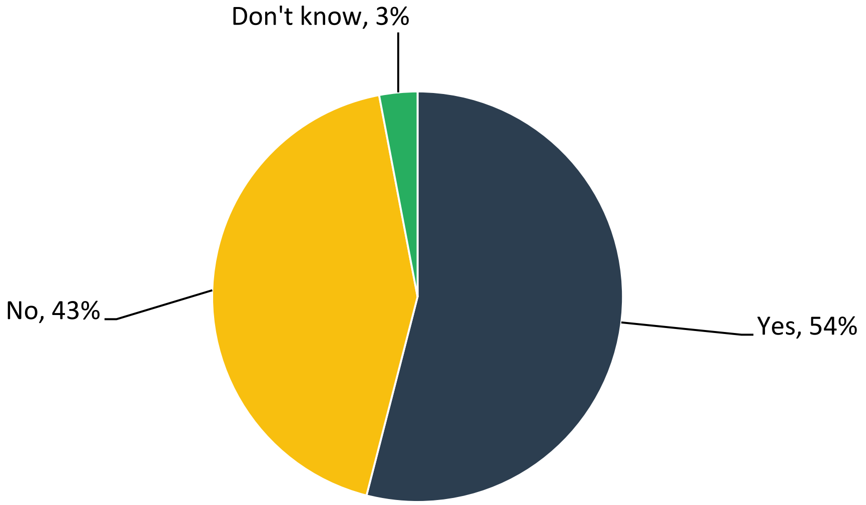


Source: Enterprise Strategy Group, 2017

What happens when security operations can't keep up with the volume of security alerts? The ESG data reveals that more than half (54%) of organizations are forced to ignore some security alerts and/or events that they believe should really be investigated (see Figure 2).

Figure 2. Propensity of Respondents to Ignore Events/Alerts Due to Volume

Does your organization ever have to ignore some security events/alerts that you believe should be investigated further but can't because it can't keep up with the overall volume? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, 2017

Just how many security alerts and events are ignored in order to keep up with overall volume? A substantial amount—43% of the cybersecurity professionals surveyed say that their organization ignores more than 25% of security events/alerts that should be investigated but aren't due to the overall volume of security alerts/events.

This pattern of ignoring security alerts represents a cybersecurity Faustian compromise where security teams knowingly disregard suspicious activities to dedicate scarce resources to those alerts deemed higher priorities. It is worth noting that the Target breach of 2013 may have been prevented if the security operations staff had investigated rather than ignored several key security alerts.

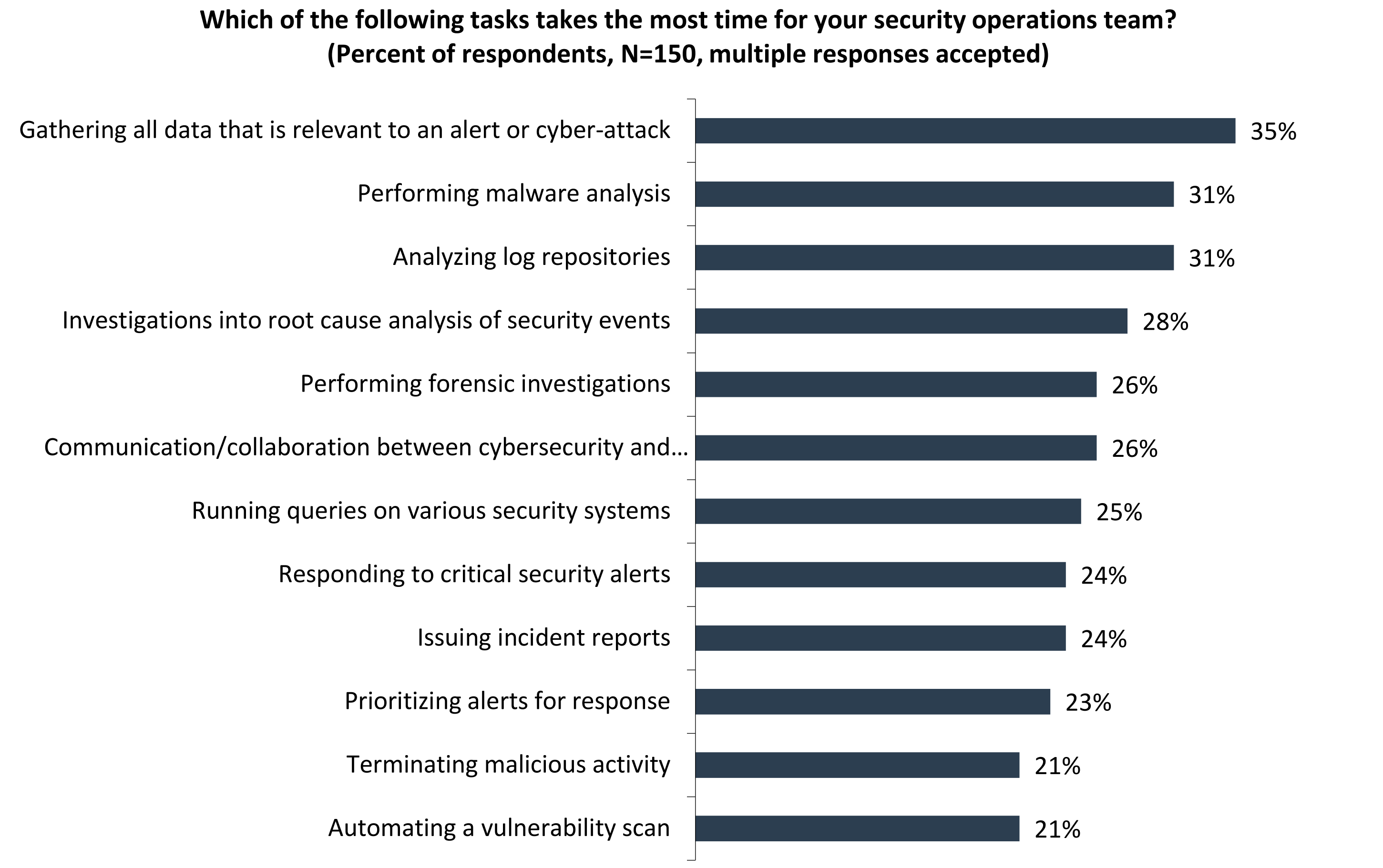
Aside from the crushing volume of security alerts, it's likely that many organizations simply don't have the skills or appropriate security staff size to keep up with security investigations. ESG's 2017 IT spending intentions research report indicates that 45% of organizations report having a "problematic shortage" of cybersecurity skills today.[1] Often times, security skills deficits are most acute in advanced areas like security analytics, forensic investigations, and incident responders—the very skills needed for security operations.

Based upon the research data associated with this project, it appears that the organizations interviewed suffer from similar skills shortages. Only 17% of organizations say that the size of their security operations staff is always adequate while 18% claim that the skill set of their security operations staff is always adequate. This means that the majority of organizations suffer from some level of security operations skills or staffing shortage.

Given the security operations skills shortage, the security team's time is a precious resource. What are the most time-consuming security operations tasks? The research points out areas like gathering relevant cyber-attack data, analyzing log repositories, and investigating the root cause of security events (see Figure 3).

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, to be published.

Figure 3. Time-consuming Security Operations Tasks

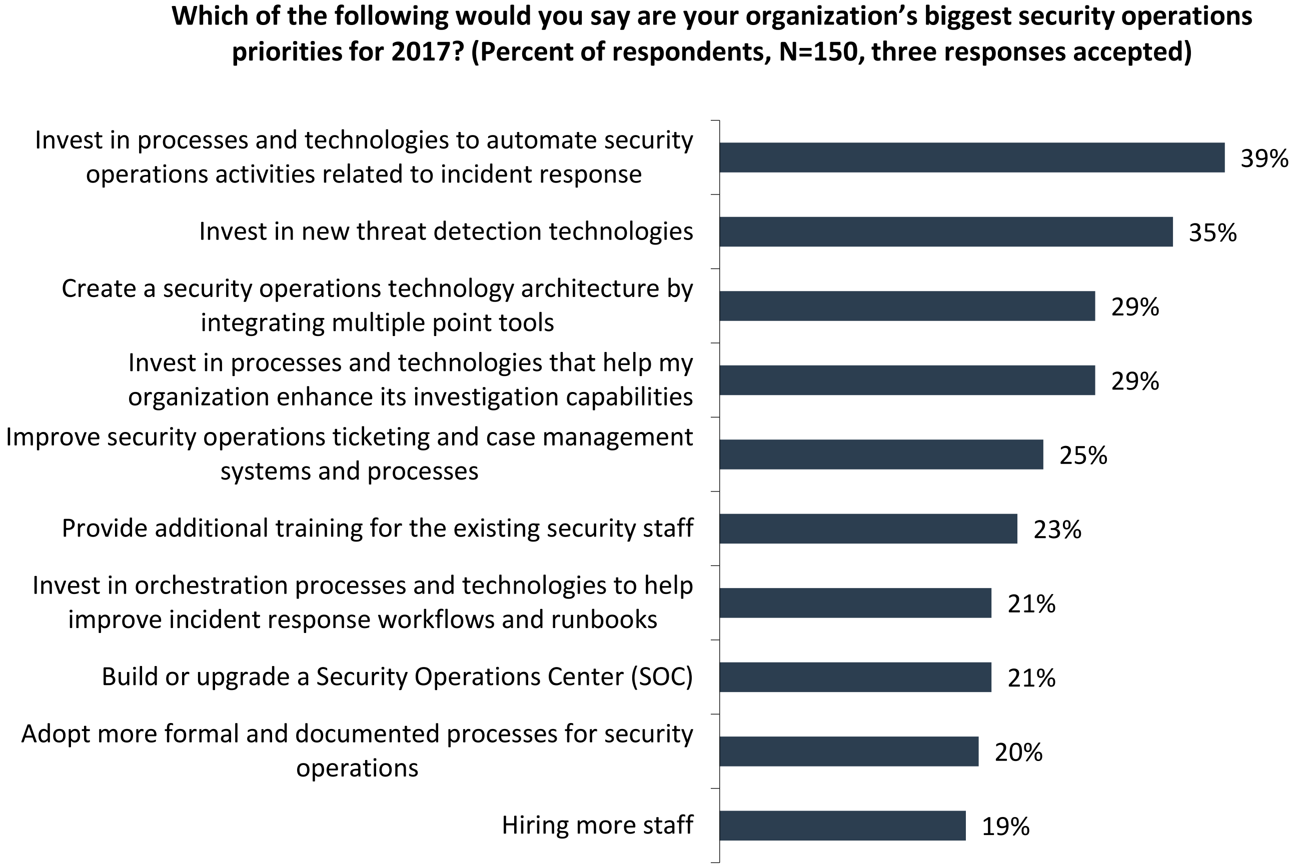


Source: Enterprise Strategy Group, 2017

Security Operations Priorities and Initiatives

Many organizations find themselves understaffed, under-skilled, and buried in a continuous avalanche of security alerts. How do they suggest getting out of this untenable situation? Survey respondents propose several security operations priorities, including investing in processes and technologies for security operations automation (39%), creating an integrated security operations architecture (29%), and investing in processes and technologies that enhance investigation capabilities (see Figure 4).

Figure 4. Top Security Operations Priorities for 2017 Reported by Respondents



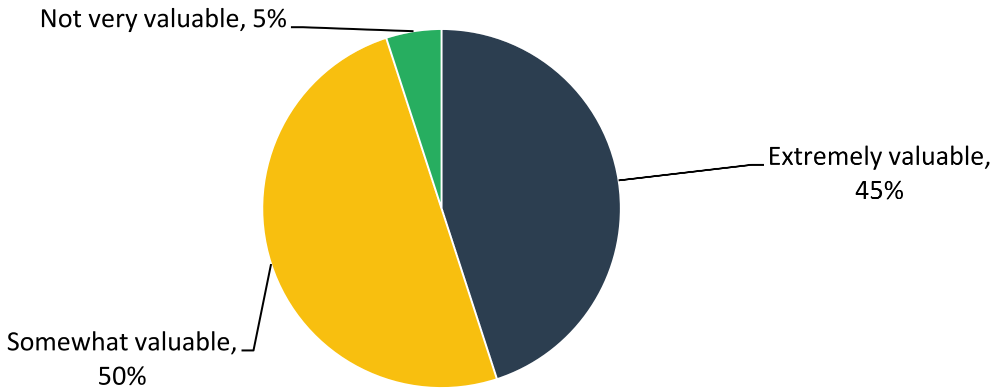
Source: Enterprise Strategy Group, 2017

Security alerts can be viewed as single data elements that could be pointing to some type of suspicious or malicious activity in progress. Unfortunately, each security alert only hints at more global security attacks from its own limited purview. This forces security analysts to piece together the threat storyline by manually ploughing through individual security alerts, tools, and reports. Without the necessary context, basic triage becomes extremely difficult, as analysts try to assess whether all of these discrete hints add up to an actual attack or data breach in progress.

Recently, new types of security analytics tools have been introduced that consolidate, enrich, and contextualize security alerts to help analysts understand the full threat storyline and accelerate triage and investigation of threats. Could this be a valuable service for the SOC team? Yes. In fact, 45% of survey respondents would find security alert consolidation and contextualization extremely valuable, while another 50% say it would be somewhat valuable (see Figure 5).

Figure 5. Value Respondents Ascribe to Security Alert Consolidation and Contextualization

How valuable would it be to your organization if you could consolidate and contextualize all security alerts (i.e., group separate alerts that are related to the same incident, cluster alerts across timeframes and events, etc.)? (Percent of respondents, N=150)

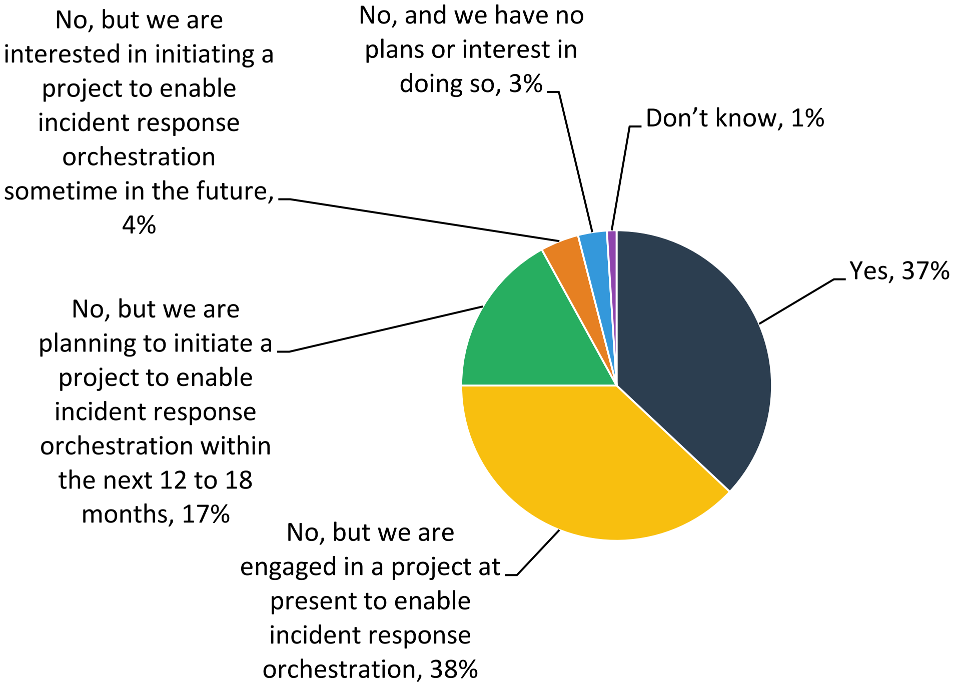


Source: Enterprise Strategy Group, 2017

The research also indicates that many organizations have initiated or completed projects to orchestrate incident response (IR) processes—37% are already orchestrating IR to drive process consistency today, 38% are currently engaged in an IR orchestration project, and 17% plan to begin an IR orchestration project over the next 12 to 18 months (see Figure 6). Taken together nearly 96% of organizations are engaged in or contemplating security orchestration initiatives.

Figure 6. Frequency of Actions Organizations Have Taken to Orchestrate Incident Response Processes

Has your organization taken any actions to orchestrate its incident response processes (i.e., connect and centralize disparate security operations tools, centralize management, investigation, and automation under one umbrella, to drive consistency through the response process, etc.)? (Percent of respondents, N=150)

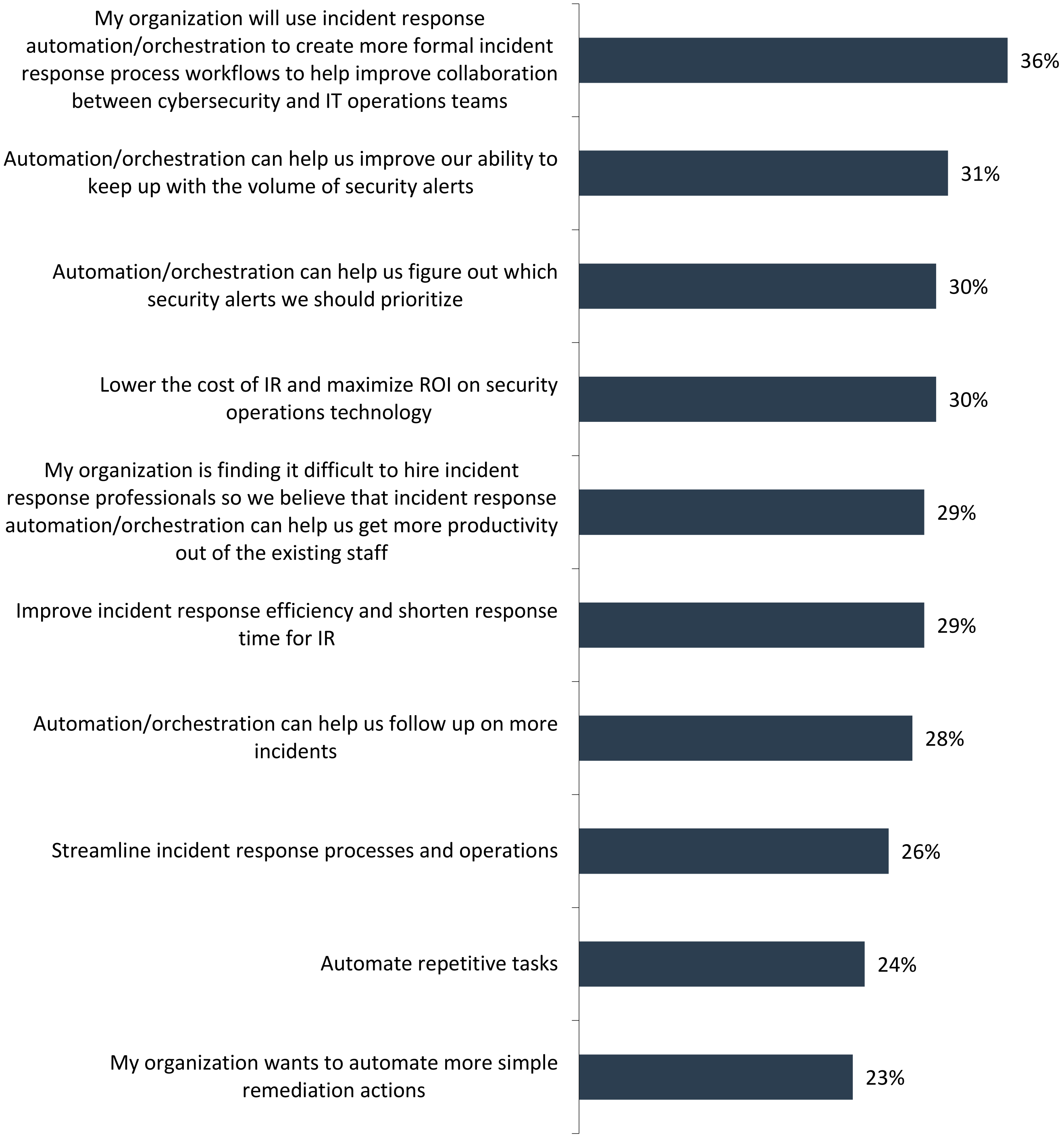


Source: Enterprise Strategy Group, 2017

Why do organizations want to automate and orchestrate security operations tasks? There are numerous reasons, including moving toward more formal incident response workflows (36%), increasing the number of security alerts for investigation (31%), and helping the cybersecurity staff determine which alerts to prioritize (30%, see Figure 7).

Figure 7. Reasons for Automating/Orchestrating Incident Response

You indicated that your organization has taken actions to automate and/or orchestrate incident response processes or is planning to do so or interested in doing so in the future. Why has or will your organization do this? (Percent of respondents, N=145, multiple responses accepted)

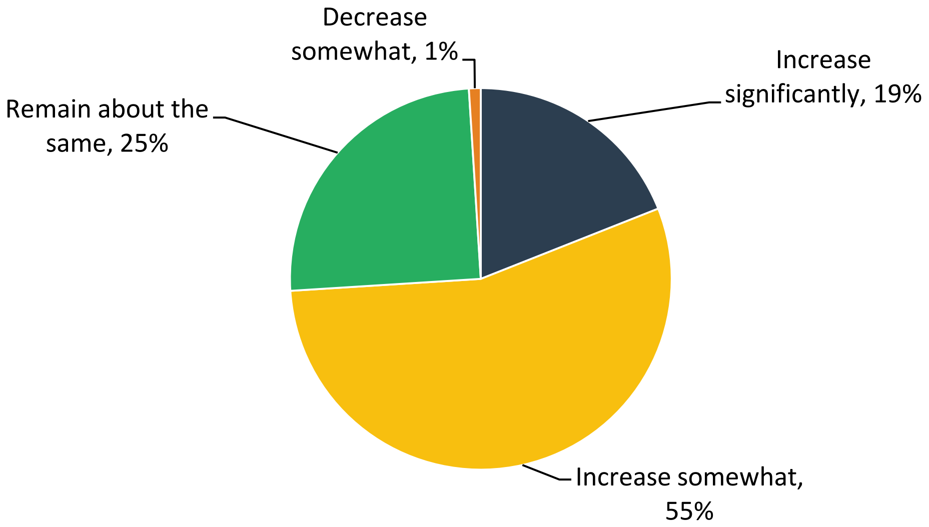


Source: Enterprise Strategy Group, 2017

IR automation and orchestration projects represent a bigger trend—a comprehensive effort to improve security operations. For example, the research also reveals that nearly one in five (19%) of organizations will increase security operations spending significantly while more than half say that security operations spending will increase somewhat (see Figure 8). Taken together, nearly three-quarters (74%) of organizations will bolster security operations spending in 2017.

Figure 8. Change in Security Operations Spending Anticipated by Respondents

Over the next two years, how will your organization's spending on security operations change, if at all? (Percent of respondents, N=150)

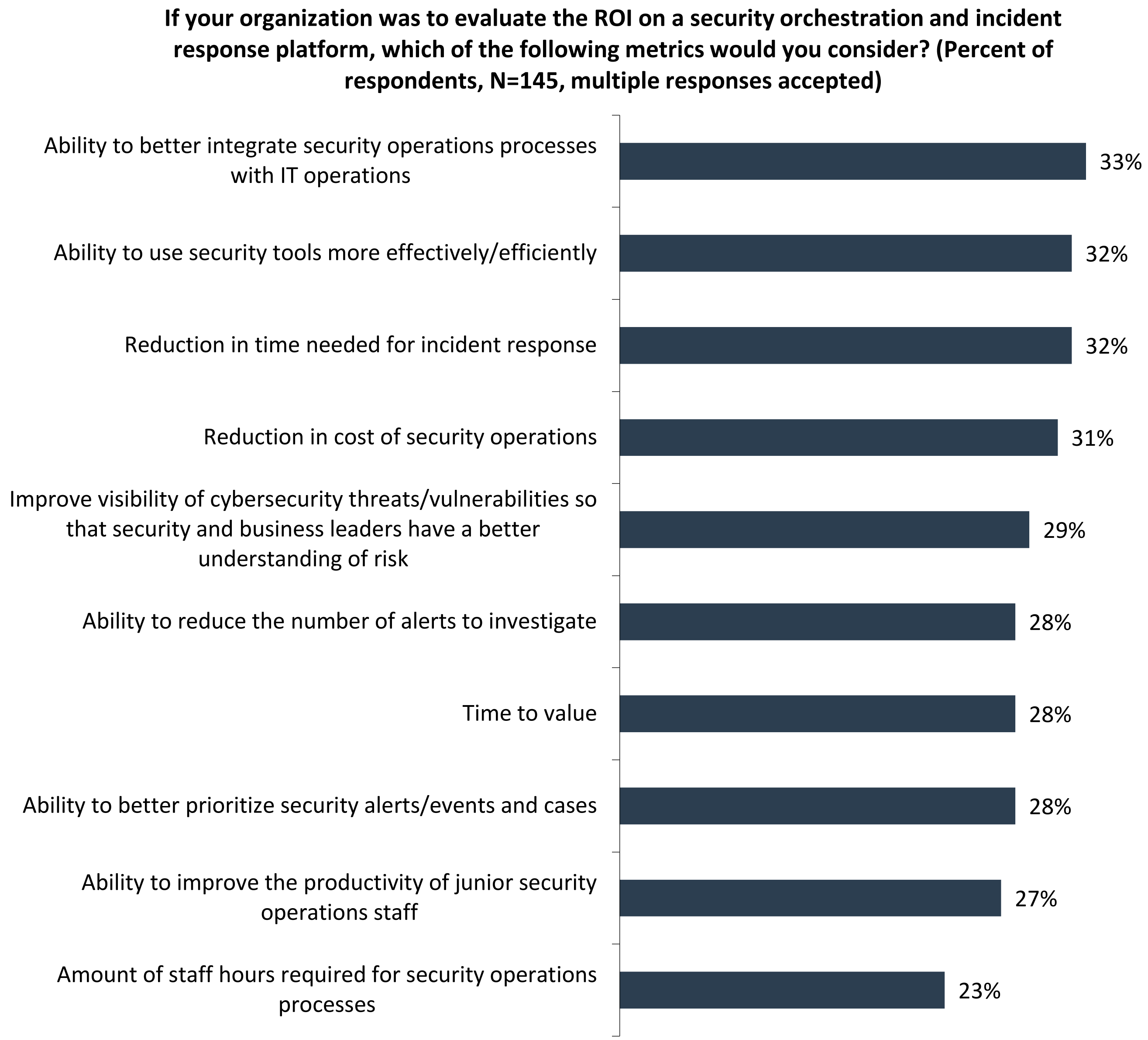


Source: Enterprise Strategy Group, 2017

In the past, security automation and orchestration projects were homegrown and depended upon things like Python scripts, open source software, API integration, and custom applications. Over the past few years, however, new innovative security vendors have introduced software products designed as command-and-control integration hubs for IR automation and orchestration. Which attributes are most important for these incident response platforms (IRPs)? Survey respondents point to characteristics like platform flexibility for customization (36%), vendors with security operations knowledge and experience (32%), ease-of-implementation (31%), and (closely related) a generally easy-to-use security operations platform (28%). We can infer from the collective responses that many organizations want a centralized "workbench" for security analysts to drive efficiency—in other words, a centralized platform that provides the full scope of threat response, not just automation of selective tasks.

Security professionals also identified a number of ROI metrics they consider when evaluating security orchestration and incident response platforms in this survey (see Figure 9). The most frequently cited responses include things like an increase in the efficiency/effectiveness of current security tools (32%), a reduction in the time needed for incident response (32%), and a reduction in security operations costs (31%). Clearly, security operations professionals see a central security orchestration platform as a way to maximize their existing security investments.

Figure 9. ROI Metrics for a Security Operations Platform



Source: Enterprise Strategy Group, 2017

The Bigger Truth

CISOs should review the data presented in this report as it provides an overview of security operations issues and offers suggestions to address these problems from cybersecurity professionals themselves. As part of this process, ESG suggests that organizations:

- **Assess security operations processes, skills, workloads, and relationships.** The research presented in this report demonstrates that security teams are overwhelmed, lack the right tools, and are highly reliant on manual processes to do their job. CISOs should start by digging deep to unearth people and process problems that hinder the productivity, efficacy, and efficiency of security operations teams. Armed with this list, cybersecurity managers should prioritize and initiate projects to solve the most pressing problems.

- **Investigate what's really needed for security operations technologies.** When faced with the security operations challenges outlined in this report, many cybersecurity professionals instinctively evaluate and even purchase the latest and greatest point tool designed to detect some type of new cyber-threat. The research indicates that this may actually be counterproductive as cybersecurity professionals already complain about too many point tools and simply don't have adequate time to configure, deploy, and operate new tools to achieve their full potential. Rather than finding the next cybersecurity silver bullet, CISOs should look for technologies that unify and enrich existing security technology investments. In other words, the goal should be adding security operations value, increasing productivity, and improving ROI rather than increasing the already untenable security operations workload.

- **Look for quick wins with security operations automation and orchestration.** Since it's difficult to hire cybersecurity professionals, CISOs must look to new technology to help the existing infosec team work smarter, not harder. This means more investment and focus on security operations automation and operations—a trend that is clearly well underway per this research. ESG suggests that CISOs look for quick wins by pointing these projects at complex, multi-stepped tasks like phishing investigations. Orchestrate these processes, gain a near-term payback, learn from these projects, and apply lessons learned to future SOC automation and orchestration initiatives.

- **Realize that context is king.** When considering orchestration solutions, CISOs should realize that the biggest issues tend to center around tier-1 analysts coping with basic triage amidst a sea of alerts. Providing solutions that integrate the many existing security tools and data to provide context to the complete threat storyline is key to accelerating tier-1 decision making and driving efficiency throughout security operations.

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

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