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

ESG Research Insights Paper

Automation and Analytics versus the Chaos of Cybersecurity Operations

By Jon Oltsik, ESG Senior Principal Analyst; and Jack Poller, ESG Analyst

September 2017

This ESG Study was commissioned by McAfee
and is distributed under license from ESG.

Contents

Executive Summary

ESG recently surveyed 412 IT and information security professionals representing large midmarket (500 to 999 employees) and enterprise-class (more than 1,000 employees) organizations based in North America and Western Europe.

The survey included representation from multiple industry verticals including manufacturing, financial, retail/wholesale, business services, government (federal/national and state/local), and healthcare, among others. All respondents were involved in the planning, implementation, and/or daily operations of their organization's security analytics and operations.

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

- **Cybersecurity analytics and operations are getting more difficult.** Seventy-two percent of those surveyed believe that cybersecurity analytics and operations are more difficult today than they were two years ago for several reasons. Survey respondents say it is difficult to keep up with the evolving threat landscape, they lack adequate cybersecurity skills or the appropriately sized security staff, and they have too many tools. That last response—too many tools—is a new challenge, while the others are perennial. Alarmingly, more than one-quarter (27%) say they spend most of their time responding to high-priority or emergency issues. It seems that security analytics and operations scaling needs may be overwhelming many organizations.

- **Organizations are consolidating their security operations.** To accommodate data growth while enriching, contextualizing, and acting upon security intelligence in real time, CISOs realize that they need a tightly integrated security operations and analytics platform architecture (SOAPA). This trend is early but gaining momentum as 15% of organizations have actively moved toward a more consolidated operations model, while another 66% are moving toward a more consolidated and integrated approach today. Additionally, 21% of organizations say consolidating their security operations technologies is one of their highest priorities.

- **Operationalizing security analytics is a primary objective.** The time and effort organizations expend to acquire and deploy each new point tool takes a toll. Implementing new tools distracts the infosec team from addressing tactical issues, and they can't reap the benefits until they both tune the tool to their specific environment and obtain tool mastery. Twenty-nine percent of those surveyed want to improve the operationalization of behavioral intelligence and 25% want to integrate disparate tools into a more efficient and effective architecture.

- **Security operations automation and orchestration is a high priority.** Two-thirds of respondents' organizations consider automation of security analytics and operations to be a high priority. Technology initiatives are rampant, with 19% already adopting extensively, 39% adopting on a limited basis, and 26% engaged in a project to deploy technology for security analytics and operations automation and orchestration.

- **Machine learning (ML) for security operations and analytics is gaining interest.** The future appears bright for cybersecurity technologies based upon machine learning as 12% of survey respondents say that their organization has deployed machine learning technologies for security analytics and operations extensively, while another 27% have deployed machine learning for security analytics and operations on a limited basis. Despite less than a third of respondents declaring themselves very knowledgeable about these technologies, the data indicates that organizations hope to use these nascent advances to improve the productivity, efficiency, and efficacy of their security analysts.

The Chaotic State of Security Operations and Analytics Today

Cybersecurity operations and analytics is made up of a complex set of processes, tools, and personnel focused on cyber threat prevention, detection, and response. Organizations must block known malicious behavior, as well as collect, process, and analyze internal and external data, identify and investigate suspicious activities, and remediate problems quickly before minor issues become major data breaches.

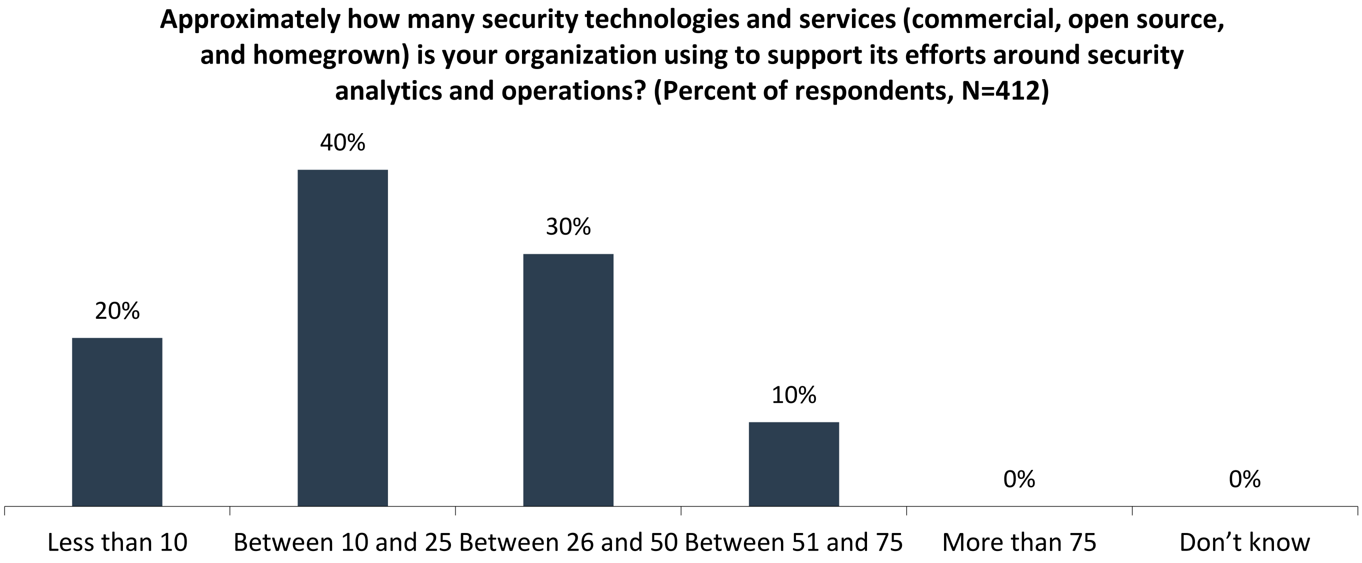
These standard requirements have become more sophisticated and complicated, according to nearly three-quarters (72%) of survey respondents. The research points to several issues including:

- **The evolving threat landscape.** Twenty-six percent of survey respondents said that the threat landscape is evolving and changing rapidly, making it difficult to keep up. Operational and analytics tasks and workloads have changed as threats have done a better job of penetrating countermeasures and establishing persistence within an organization. Attackers are leveraging hundreds of anti-security, anti-sandbox, and anti-analyst evasion techniques that make their activities look benign and their software look innocent, so analysts are seeing more demand for subtle data assessments of more context-sensitive incidents.

- **Too many tools**. The survey revealed that 40% of organizations use ten to 25 tools while 30% use 26 to 50 tools (see Figure 1). Cybersecurity operations and analytics toolsets have grown organically as security professionals deploy new tools to address specific issues. This army of point tools presents a problem because organizations require more resources as they deploy more tools. For example, each tool comes with its own installation, configuration, maintenance, compute, storage, and networking requirements, and generates data that must be managed and assimilated. Since no single member of the security team can develop expertise with every tool, organizations must hire and train more staff as the pool of tools expands.

  Unfortunately, the plethora of point tools seldom comes with ways to integrate each data set into analysis processes and dashboards. They can't provide a holistic view of the organization's security status, forcing cybersecurity professionals to manage security operations on a tool-by-tool basis. This doesn't scale or provide real-time visibility to existing threats or compromises.

Figure 1. Number of Security Technologies and Services in Use



Source: Enterprise Strategy Group, 2017

- **A lack of adequate skills or adequately sized staff**. More than half (54%) of respondents indicated that their organization lacks the appropriate level of cybersecurity skills for security operations, and 56% said they don't have appropriate staffing levels for the size of their organization. This reinforces prior ESG research, which revealed that 45% of organizations claim to have a problematic shortage of cybersecurity skills—the biggest skills gap of all types of IT skills.[1]

  Cybersecurity teams need appropriate levels of skilled staff to manage their operations and analytics, and these skills and staffing gaps are not minor problems. While many organizations are trying to add cybersecurity personnel, 81% of hiring organizations said it is difficult or extremely difficult to recruit and hire additional staff. This indicates that CISOs will not be able to hire their way out of today's cybersecurity analytics and operations challenges, rather they will need to be more creative when addressing and attempting to solve security operations problems.

- **An overwhelming time commitment for emergency response.** These issues contribute to the "whack a mole" reactive situation: Twenty-seven percent of those surveyed believe that their organization's security team spends **most** of its time addressing high-priority/emergency issues and not enough time on strategy or process improvement. This type of environment is highly stressful for the cybersecurity professional, and can lead to employee burnout and attrition. Additionally, when organizations are constantly firefighting emergency issues, they are not investing in the remedies that would rescue them: strategy and process improvements to address the growing cybersecurity workload or the increasingly dangerous threat landscape.

In aggregate, the research data indicates that current security operations and analytics strategies are not working. CISOs must implement changes soon, or their organizations will face increased risk and/or damaging security incidents.

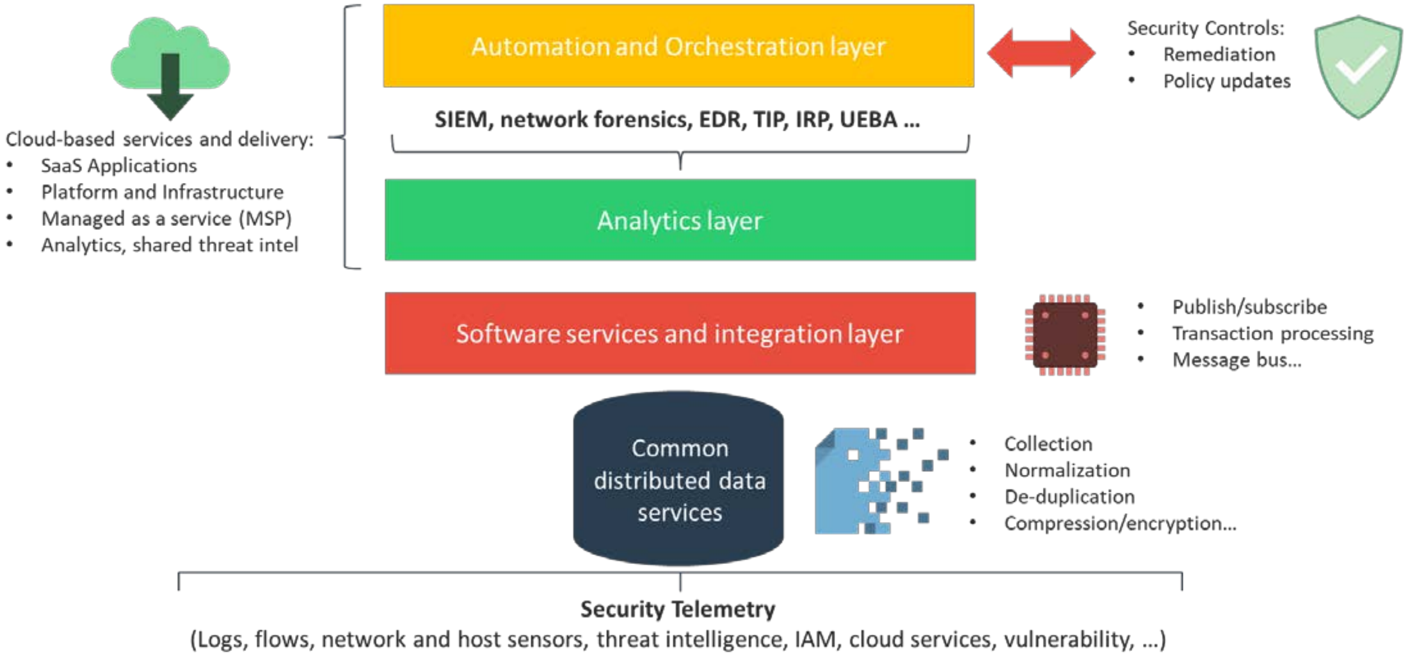
Moving Toward a Security Operations and Analytics Platform Architecture (SOAPA)

Security operations and analytics platform architecture (SOAPA) is a new model for security operations that knits cybersecurity tools into a loosely coupled software system that meets the challenges of increasing efficacy and efficiency.

SOAPA is designed to integrate, orchestrate, and automate endpoint protection platforms (EPP), endpoint detection/response tools (EDR), incident response platforms (IRPs), network security analytics, user and entity behavior analytics (UEBA), vulnerability scanners and security asset managers, anti-malware sandboxes, and threat intelligence. As a dynamic environment, new data sources, applications, and technologies can be added incrementally over time for additional utility. Beyond data exchange between security tools, SOAPA provides centralized command and control for analytics and management of the security infrastructure. Using SOAPA, security analysts can quickly pivot across tools to find data and take action as they need to in real time.

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

Figure 2. Security Operations and Analytics Platform Architecture (SOAPA)


Automation and Orchestration layer
Security Controls:
• Remediation
• Policy updates
SIEM, network forensics, EDR, TIP, IRP, UEBA …
Cloud-based services and delivery:
• SaaS Applications
• Platform and Infrastructure
• Managed as a service (MSP)
• Analytics, shared threat intel
Analytics layer
Software services and integration layer
• Publish/subscribe
• Transaction processing
• Message bus…
Common distributed data services
• Collection
• Normalization
• De-duplication
• Compression/encryption…
Security Telemetry
(Logs, flows, network and host sensors, threat intelligence, IAM, cloud services, vulnerability, …)

Source: Enterprise Strategy Group, 2017

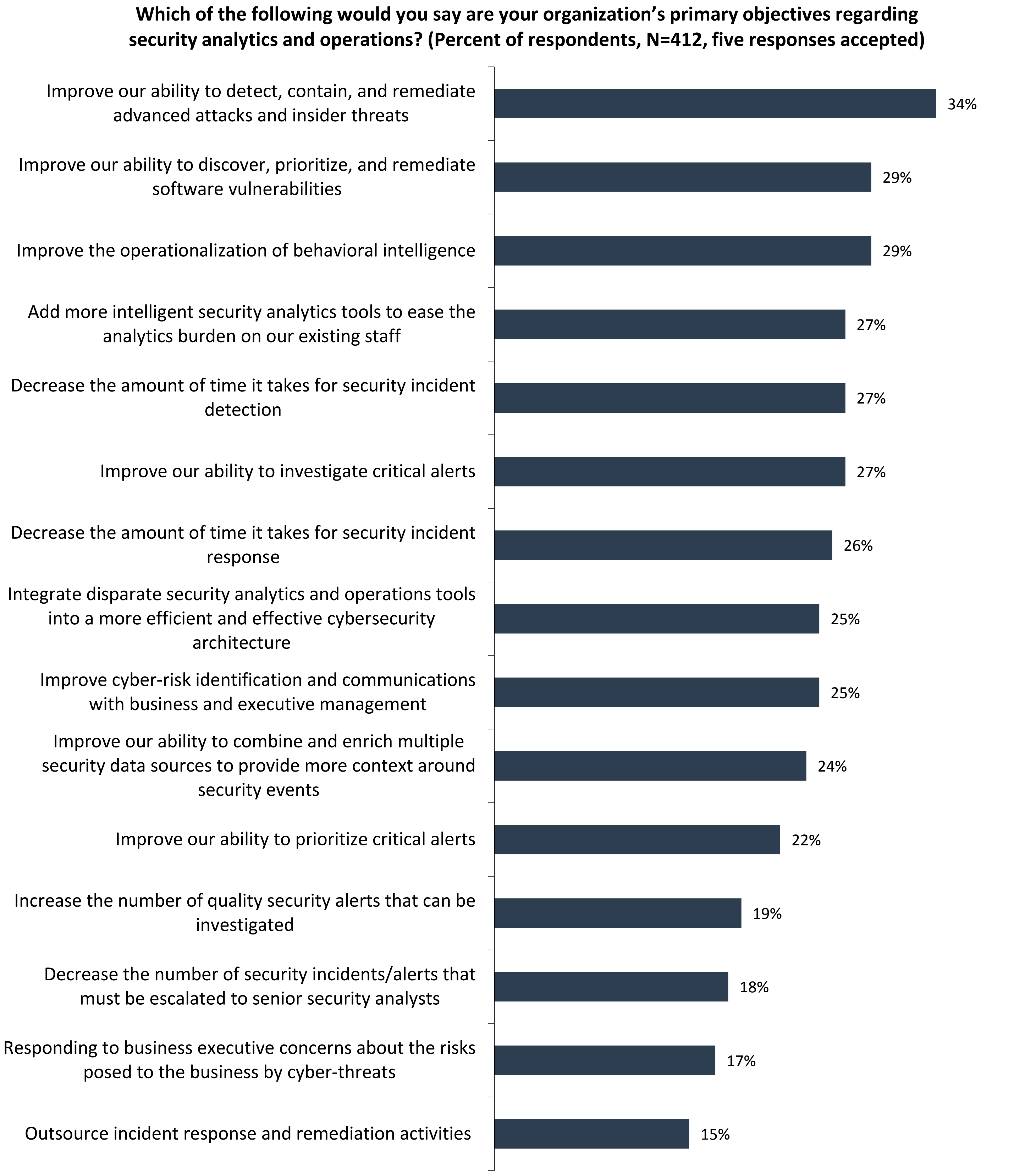
SOAPA provides a structure that can help guide the goals, strategies, and architectural choices organizations are already making. It will help more enterprises achieve the goals that this research showed represent the plans of leading organizations committed to this path, including (see Figure 3):

- Improving threat detection and response. One-third (34%) of those surveyed want to improve their ability to detect, contain, and remediate advanced attacks and insider threats, and 29% want to improve their ability to discover, prioritize, and remediate software vulnerabilities. Malicious actors, both inside and outside of the organization, are growing in sophistication, and continue to develop advanced capabilities to obfuscate and target their attacks. Integrating and analyzing data across multiple security tools can transform seemingly unrelated events into a set of related incidents, unmasking threats and attacks in progress.

- Increasing staff productivity. Due to the global cybersecurity skills shortage, worker productivity figures prominently in security analytics and operations objectives: Respondents indicated that they want to add more intelligent security analytics tools to ease the analytics burden on existing staff (27%), improve their ability to investigate critical alerts (27%), decrease the amount of time for incident detection (27%) and response (26%), and improve their ability to prioritize critical alerts (22%).

- Operationalizing security analytics more efficiently. Integrating new tools and technology can enhance an organization’s ability to detect and respond to threats, and improve the efficiency of the security operations and analytics efforts, reducing the burden on staff. In addition to adding more intelligent security analytics tools, 29% of those surveyed want to improve the operationalization of behavioral intelligence, and 25% want to integrate disparate tools into a more efficient and effective architecture.

Figure 3. Primary Objectives for Security Analytics and Operations



Source: Enterprise Strategy Group, 2017

Consolidation and Integration

Many organizations are reducing the number of tools used, and integrating those they still use into a comprehensive cybersecurity architecture. Almost three-quarters (71%) of those surveyed are actively integrating their toolsets, and 21% said integration is one of their highest priorities. Why? Respondents point to several goals, including:

- **Improving data analysis**. Consolidation and integration of tools can provide data contextualization and enrichment, chaining of individual events, and cross correlation. The ability to pivot across technologies (i.e., threat intelligence, endpoint and security analytics, user and entity behavior analytics, etc.) can enable a better and more thorough data analysis, with the ability to identify threats across a broader swath of the organization's attack surface. Along these lines, one quarter (25%) of respondents have a goal of establishing a proactive threat hunting practice, 25% want to integrate external threat intelligence to improve data contextualization, and 23% want to synthesize and contextualize data related to security incidents and cyber-attacks.

- **Accelerating incident remediation**. Consolidation and integration can facilitate and expedite operations, enabling more value from existing tools, people, and programs through greater emphasis on simplicity and efficiency. Thirty percent of respondents want their integration and consolidation efforts to accelerate incident detection, and 27% want to accelerate incident response. With incident detection time currently averaging 191 days and incident response time averaging 66 days,[2] it's not surprising that 23% of respondents believe it takes too long for their organizations to remediate security incidents. During this time, malicious actors can cause damage, penetrating many areas of the organization, compromising identities, and exfiltrating data.

- **Proactively identifying and mitigating risk.** Thirty-one percent of respondents have a goal of improving identification and communication of risks to the business when they consolidate and integrate security tools, and 29% want to improve collaboration among the security and IT operations teams. Businesses that understand the specific cyber threats they face can work to actively thwart the threat, and push their employees to reduce the amount of potentially compromising activities such as responding to phishing attacks or clicking on malicious URLs.

- **Automating manual processes.** Thirty percent of respondents believe that consolidation and integration will help them automate the many manual processes in their security analytics and operations. Automating low-value repetitive manual tasks can enable scarce resources to focus on high-value activities including threat hunting, incident remediation, and behavioral analyses.

With the excess of tools and technologies in use, there are plenty of opportunities for consolidation and integration. Approaches under consideration by respondents include:

- **Integrating and correlating disparate tools and data sets**. Thirty-seven percent are potentially pursuing integration of network and endpoint security analytics, and 30% are considering the integration of security analytics and identity management. Cross correlation of network and endpoint data can give an organization insight into infections that are attempting communication with command and control servers, exfiltrating data, or expanding their footprint within the organization. Integrating security analytics with identity information can pinpoint malicious or spoofed insiders and their potentially harmful activities.

- **Managing security data.** It should be noted that 77% of those surveyed collect more than 1 TB of security data every month, and that volume keeps growing, both as the organization scales, and as more and different types of data are collected to generate higher fidelity incident detection. This makes security data management a challenge for many

[2] Source: Ponemon Institute, *2017 Cost of Data Breach Study,* June 2017.

organizations. Thus, 28% of respondents are considering implementing a common security data management platform, 27% are contemplating integrating multiple data sources into a common SIEM, and 23% are considering moving large amounts of security data into big data technologies.

Automation and Orchestration

Automation and orchestration technologies for security operations can help an organization accelerate workflows, automate manual processes, and free up cybersecurity staff to become more productive. These technologies are increasingly popular: Thirty percent of respondents indicate that they will leverage automation and orchestration capabilities built into their SIEM, 27% will use a threat intelligence platform (TIP), and 22% will use a commercial incident response platform.

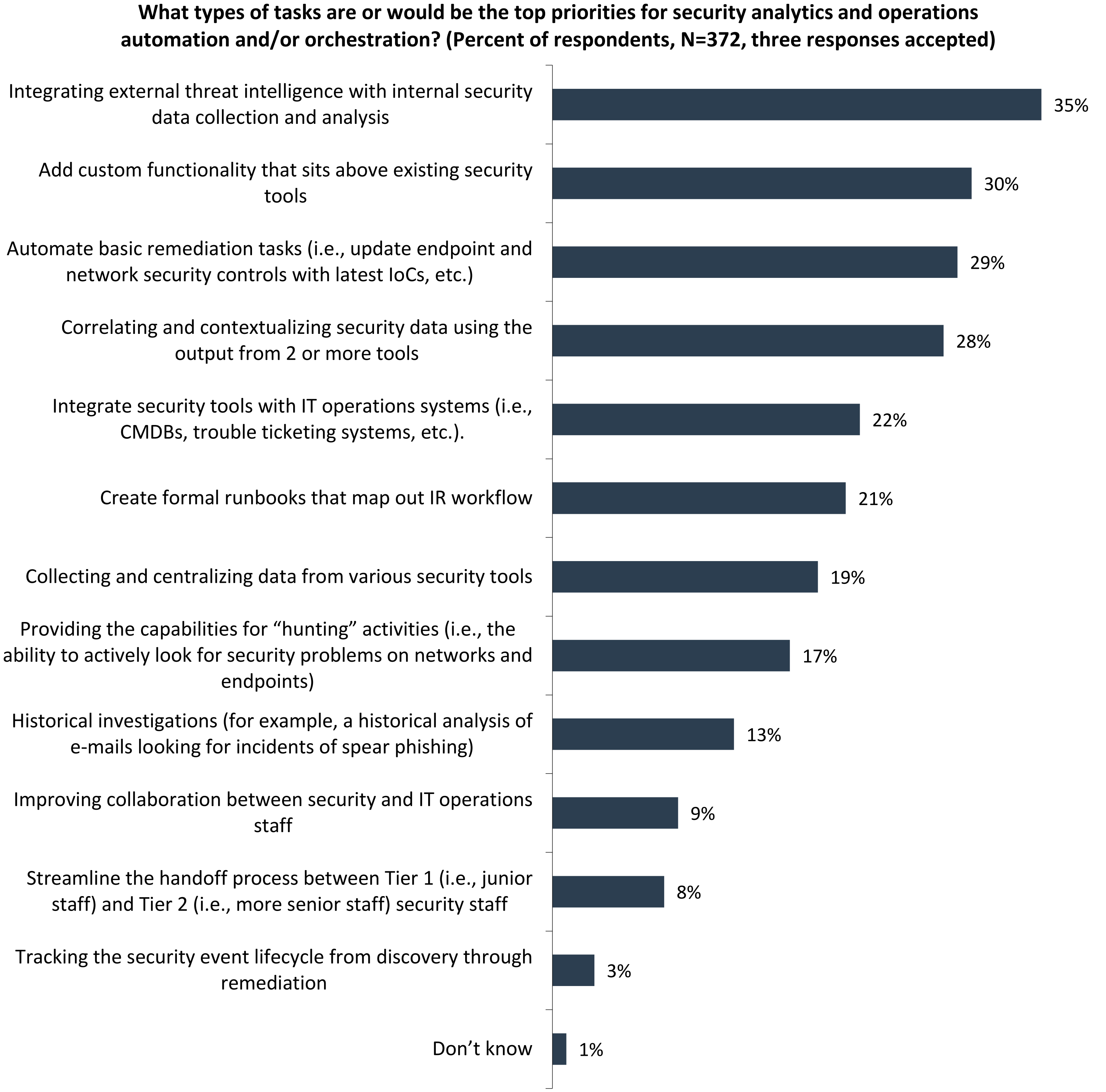
What are the top priorities for operations and analytics automation and orchestration? The research reveals that organizations want to use these technologies for (see Figure 4):

- **Operationalization of threat intelligence**. It should be noted that 39% of organizations still rely on individuals to manually collect, process, and analyze data from disparate external threat intelligence sources. Cyber threat intelligence (CTI) automation and orchestration can be used to improve analytics and accelerate remediation tasks like blocking IP addresses or patching software vulnerabilities. Thus, more than two-thirds (35%) of survey respondents are prioritizing integrating external threat intelligence with internal security data collection and analysis.

- **Customization**. Organizations see automation as a key to freeing up talent to create custom tools, scripts, and processes dedicated to their specific environment, which in turn can be automated. Since attackers have access to off-the-shelf tools and a vibrant dark web marketplace churning out new threats, 30% of organizations want to add custom functionality that sits above their existing tools. This ensures their analysts have time and scope to develop new and specialized approaches to threat detection and prioritization.

- **Automation of analytics workflows and basic remediation**. Current cybersecurity operations and analytics often depend upon the cybersecurity professional manually analyzing multiple reports and mentally correlating data to form an internal understanding of the cybersecurity status. This is difficult to do accurately, time-consuming, and operationally inefficient. The opportunity for human error is great, leading to inaccuracies, or worse, missing a threat altogether. Thus 28% of respondents want to correlate and contextualize security data using the output from two or more tools. Further, 29% want to take these findings from analysis and use them to automate basic remediation tasks such as policy and indicator of compromise (IOC) updates. The acceptance of automation is rising throughout the threat management lifecycle.

Figure 4. Top Priorities for Security Analytics and Operations Automation and/or Orchestration



Source: Enterprise Strategy Group, 2017

Machine Learning and Artificial Intelligence

Applying machine learning to cybersecurity tools is a relatively new and evolving use, and has the potential for major impacts in the future as the nascent technology is developed into standard practice. ML has gained traction in cybersecurity analytics and operations over the past few years in areas such as behavioral analysis and incident response, and the ESG research indicates organizations will continue to build on this momentum as 12% of survey respondents say that their organization has extensively deployed ML technologies for security analytics and operations, while another 27% have deployed ML technologies for security analytics and operations on a limited basis.

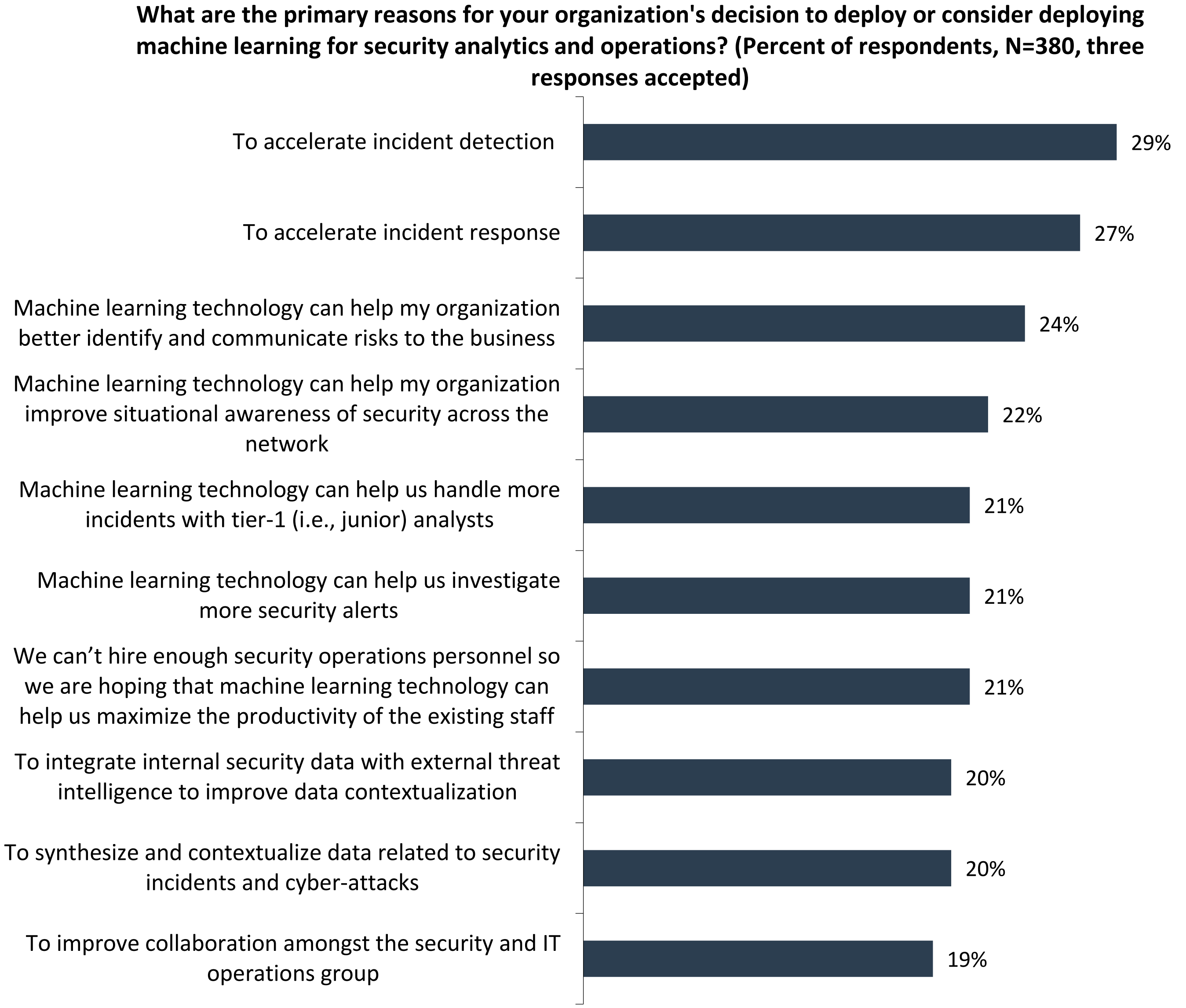
What is motivating the interest in machine learning for security analytics and operations? The data from this research indicates that ML is primarily seen as a method to enhance and support the cybersecurity team by improving the productivity, efficiency, and efficacy of security analysts (see Figure 5):

- Twenty-nine percent of respondents say they want to deploy ML to accelerate incident detection. ML provides the ability to evaluate larger volumes of data, and apply more refined and sophisticated models. As a result, incident detection tools can utilize a wider set of telemetry, correlating data across longer time horizons to identify hidden threats, obscure patterns, and indicators of compromise. This can reduce the time to detect an incident and minimize the potential for extensive damage or costs.

- Twenty-seven percent of respondents say they want to deploy ML to accelerate incident response. ML can help infosec professionals to identify repeated and effective incident response processes and patterns. This in turn can enable automation of incident triage, containment, mitigation, and remediation tasks, and free up valuable resources for other critical tasks.

- Twenty-four percent of respondents say that ML can help their organization better identify and communicate risk to the business. For example, threat intelligence tools incorporate ML to help identify emerging threats that may target specific industries or organizations. ML is also being applied to organizational strategic risk identification and prioritization, analyzing corporate data associated with cybersecurity best practices such as the NIST cybersecurity framework (CSF).

Figure 5. Reasons for Deploying or Considering Deploying Machine Learning for Security Analytics and Operations



Source: Enterprise Strategy Group, 2017

ML can be used to detect suspicious behaviors, patterns, and combinations of events that indicate with high probability that an activity is malicious. It can add value to and interact with countermeasures, inline inspection, and SOC analytics to implement updated detection rules and concepts quickly and automatically. Thirty-five percent of those surveyed said ML will be added as a separate big data security analytics solution built on top of a big data framework, and 27% of respondents plan to add ML to endpoint security software.

Other areas where respondents plan to deploy ML include adding an ML module to the SIEM (26%), adding an ML module to an identity and access management solution (22%), or adding a separate machine learning user behavior analytics solution.

The Bigger Truth

Cybersecurity operations and analytics is a chaotic environment plagued by too many tools and a lack of the right amount of adequately skilled staff who face complex, often manual processes while tackling high-priority tactical activities that take too much time. The report provides a wakeup call and specific benchmarks to CISOs responsible for the protection of critical IT assets, valuable data, and business processes.

What can organizations do to make measurable improvements in their cybersecurity analytics and operations? ESG recommends that CISOs:

1. **Evaluate their current infrastructure**. Cybersecurity analytics and operations is chaotic because infrastructure, skills, and tools were developed tactically over time as new types of threats arose, resulting in silos of operation rather than a cohesive and comprehensive strategy. CISOs should structure their assessment to reveal their most pressing cybersecurity operations problems; their staffing resources, skills, and capabilities; their security process maturity; and their current cybersecurity toolset and technology.

2. **Build on best practices**. CISOs should use their assessment as a guide while they develop a pragmatic long-term cybersecurity analytics and operations strategy. While some aspects of business are unique, many cybersecurity operations and analytics attributes are shared across organizations and industries. CISOs need to be open to learning from others and adopting and building upon industry best practices, including:

    - **Outsourcing**. Managed security service providers (MSSPs) can take over some or all security operations to alleviate the burden and enhance security, especially in areas such as threat intelligence analysis or routine monitoring.

    - **Vendor and expert best practices**. CISOs should challenge vendors and security experts to provide best practices for key use cases in easy-to-implement formats such as automatable runbooks and consumable threat intelligence.

    - **Implementing SOAPA**. CISOs should designate an architect to lead a team of security engineers, SOC personnel, and security analysts with a goal of adopting SOAPA principles and creating a SOAPA implementation plan. This plan may take several years to execute through a phased approach, but the goal should be to increase security efficacy and improve operational efficiency incrementally through each phase.

3. **Invest in human-machine teaming**. CISOs need to invest in tools and methodologies that enable their infosec professionals to become more efficient. Automation, orchestration, machine learning, and artificial intelligence can enable machines to perform most of the routine, repetitive, “grunt” work. This can free highly trained personnel to focus on anomalies or discrepancies surfaced by ML, along with providing more time for critical decision making and strategic planning.

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