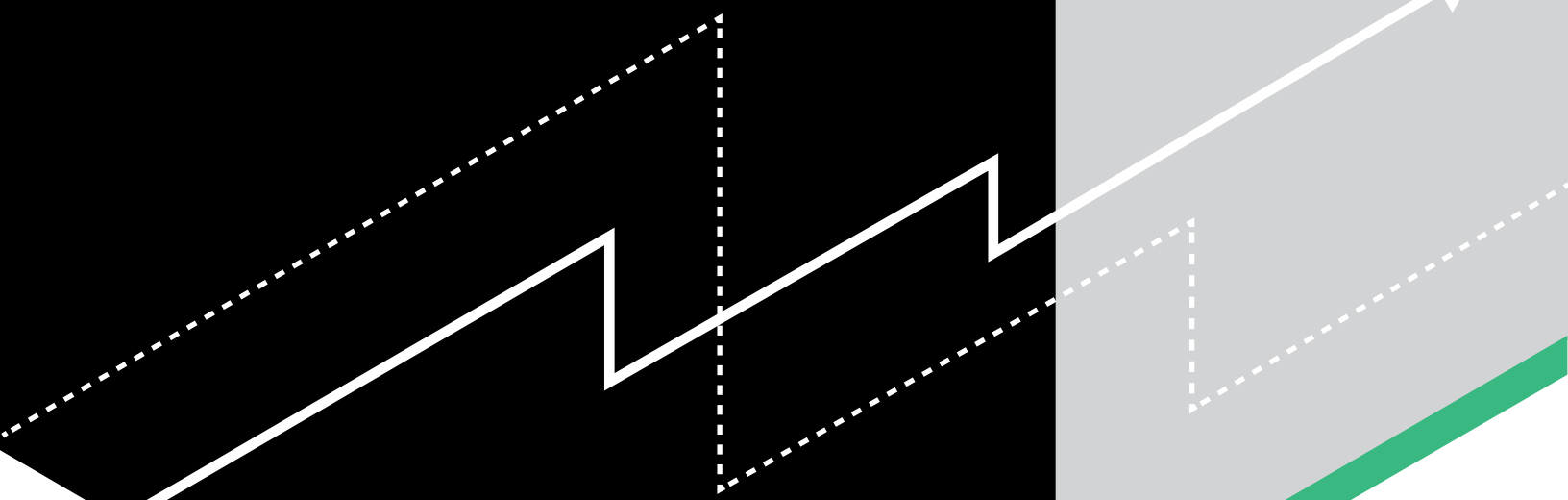
A Forrester Consulting
Thought Leadership Paper
Commissioned By Palo Alto Networks

The State Of Security Operations

SecOps Teams Struggle To Hit Key Metrics In Quest To Keep Up With The Growing Volume Of Security Alerts



FORRESTER®

Table Of Contents

Project Director:
Ana Brzezinska,
Market Impact Consultant

Contributing Research:
Forrester's security and risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

79% of businesses have experienced a breach within the past year.

Executive Summary

Data breaches continue to grow in velocity and sophistication, threatening businesses small and large. More than three-quarters of businesses have experienced a breach in the past year. Breaches have significant business impact — from loss of data to loss of customer trust and potential litigation — but they also have significant impact on security operations teams.

Security operations teams are often the frontline defense against breaches, and analysts are feeling the added pressure in today's security-focused world. Alarmingly, only 46% of security operations decision makers are satisfied with their current ability to detect threats. They point to wasted time chasing false leads, poorly integrated security tools, and a large learning curve for effectively using those tools. This leads to low visibility and inefficient workstreams. Many security operations decision makers are looking for a solution that can help weave together disparate tools and data sources to help analysts identify true alerts more quickly and increase productivity and visibility.

In an effort to further explore the key challenges in enterprise security operations today, Palo Alto Networks commissioned Forrester Consulting to evaluate current approaches to security operations for the enterprise and how today's security operations teams are managing alerts. In April 2020, Forrester conducted an online survey with 315 respondents with responsibility over security operations and/or incident response at their organizations across the US, the UK, Germany, France, Australia, New Zealand, and Canada.

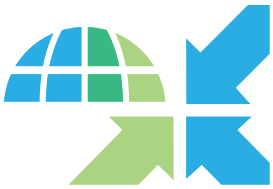
KEY FINDINGS

- **A data breach is around the corner for any business.** Data breaches are a persistent concern for all businesses, and they can happen to any business at any time. Nearly 50% of surveyed businesses have experienced a cyberbreach within the past six months and 79% have experienced a breach within the past year.
- **Security teams face significant technology challenges.** Security operations teams have many complicated and siloed tools, leading to inefficiencies and subpar security outcomes as analysts work to integrate tools and struggle with large learning curves. Issues such as a lack of visibility into what endpoint process resulted in a network alert cause analysts to waste time chasing false positives.
- **Investing in a solution that can increase visibility and efficiency will bring many benefits.** Less than 20% of teams have a solution in place that can effectively provide visibility across networks, applications, and endpoints — leaving them with unanticipated blind spots. However, those who are able to improve their detection and response technologies expect increased productivity, better visibility, and a reduction in false positives as the key benefits.

FORRESTER®

Challenges Of The Modern SOC

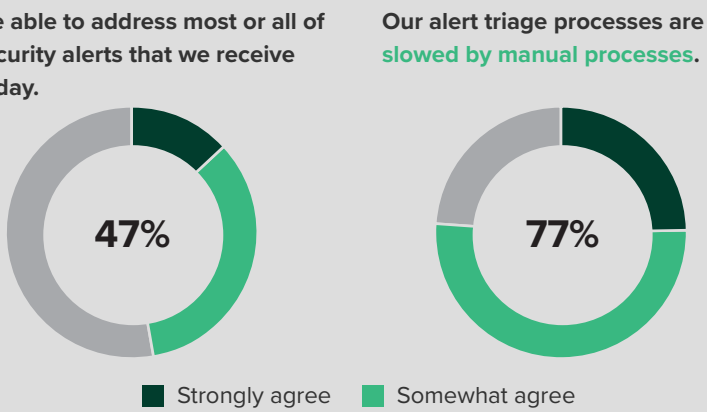
In surveying 315 businesses about their security operations challenges, we found some common themes defining today's security operations center (SOC). While the overwhelming majority — 94% — of organizations that have an internal SOC and also outsource some aspects of their security have a multitier approach, the organizations that do not have an internal SOC, instead have a dedicated in-house security operations team that is more divided in their approach to hierarchy. And although 83% of businesses have some form of 24x7 coverage, many security operations teams lack the right combination of people and technology to keep up with the evolving volume and complexity of cyberattacks, and often struggle to keep up with the high volume of alerts they see every day.



- **Businesses today recognize the threat of cyberattacks.** Eighty-seven percent of decision makers are primarily concerned with an external attack targeting their organization. Nearly 80% of surveyed businesses have experienced a breach within the past year, leading to loss of customer data, loss of sensitive corporate data, and importantly, financial loss. According to Forrester Research, the average data breach costs as much as $7 million per incident, from the response and notification, lost productivity, potential legal actions, regulatory fines, and other liabilities.[1] And the number of breaches is increasing. From 2016 to 2017, Forrester noted an increase of 5 percentage points in global enterprise decision makers who experienced a breach compared to the previous year.[2]
- **Analyst time is often spent inefficiently chasing alerts.** The average security operations team receives over 11,000 alerts per day, and the vast majority of these alerts must be manually processed. Seventy-seven percent of decision makers agree that their alert triage processes are slowed down by manual processes (see Figure 1).

Figure 1: Alerts Are Slowed By Manual Processes and SecOps Teams Are Unable To Keep Up With Volume

"To what extent do you agree with the following statements?"



Base: 315 global decision makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

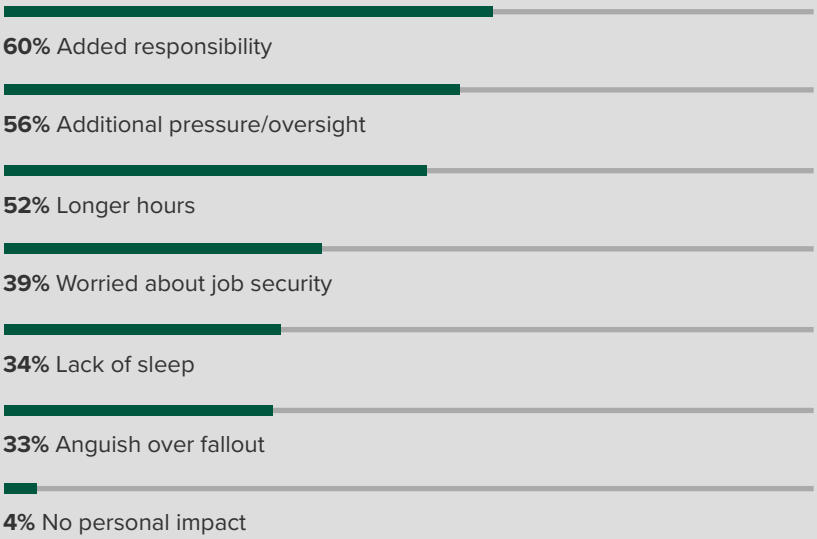
On average, internal security operations teams receive over **11,000** alerts per day.

FORRESTER®

- **Security operations teams are unable to keep up with the volume of alerts they see.** Only 47% of organizations noted that they are able to address most or all of the security alerts they receive in a single day. Nearly 20% of alerts are manually reviewed/triaged by an analyst; almost a third are false positives; and 28% are outright ignored by analysts struggling to keep up with the workload.
- **Analysts are feeling the pinch.** The effects of cyberattacks extend beyond business losses — 96% of analysts are feeling significant personal impacts after cybersecurity breaches. Most analysts report longer hours, additional pressure/overnights, and added responsibility after an attack (see Figure 2). VPs and C-level executives were particularly worried about their job security after a breach.
- **All of this leaves decision makers frustrated and unsatisfied.** Only 46% of decision makers agreed that they are satisfied with their organization's ability to detect threats. In particular, many decision makers pointed to their reactive security approaches as key problems. Eighty-two percent of IT decision makers agreed that their responses to threats are mostly or completely reactive, but they'd like to be more proactive; only 50% agreed that they have the right resources to proactively hunt for threats.

Figure 2: Cyberattacks Affect Both Coffers And Personnel

"What personal impact did your company's most recent cybersecurity breach have on you?"

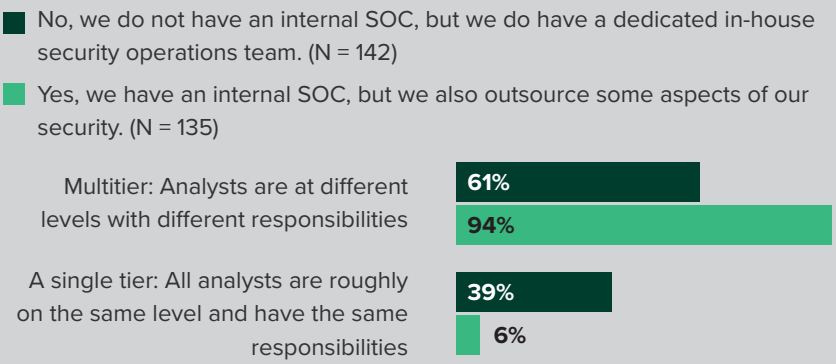


Base: 313 global security operation decision makers that have experienced a security breach
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

While the business impacts of a cyberattack are significant, personal impact on analysts must be understood as well. **96%** of analysts felt a personal impact after their organization's most recent breach.

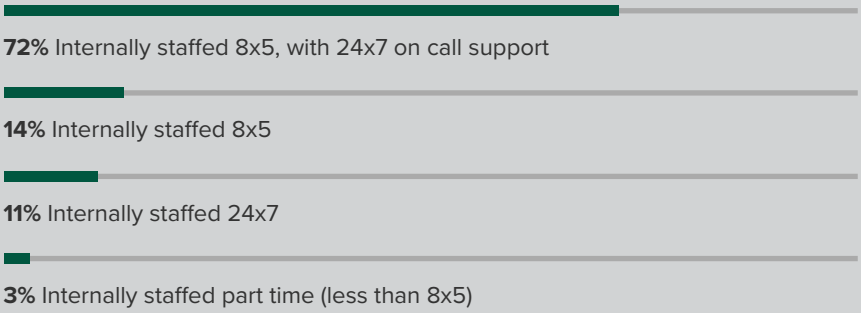
FORRESTER®

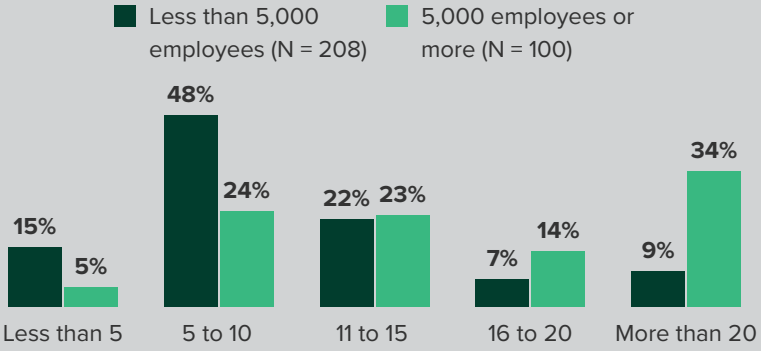
Figure 3: A Snapshot Of Enterprise Security



Most security operations teams are multi-tier. And most security operations managers report directly to the CIO or CISO.

83% of businesses have some form of 24x7 coverage, either through full-time staffing or an on-call support system.





Businesses have on average 14 full-time security analysts; smaller orgs have 11 and larger orgs have 20.

Investigating alerts takes the most of an analyst's time, followed by triaging and threat hunting. Only 10.9% of time is spent on process improvements.

Task	Average percentage of hours spent by internal SecOps resources on task
Triaging alerts	**21.8%**
Investigating alerts	**31.3%**
Mitigating/responding to alerts	**14.8%**
Threat hunting	**17.6%**
Process improvements	**10.9%**

Base: 315 global decision makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of SheerID, March 2020

FORRESTER®

The Impact Of Security Complexity On Business Outcomes

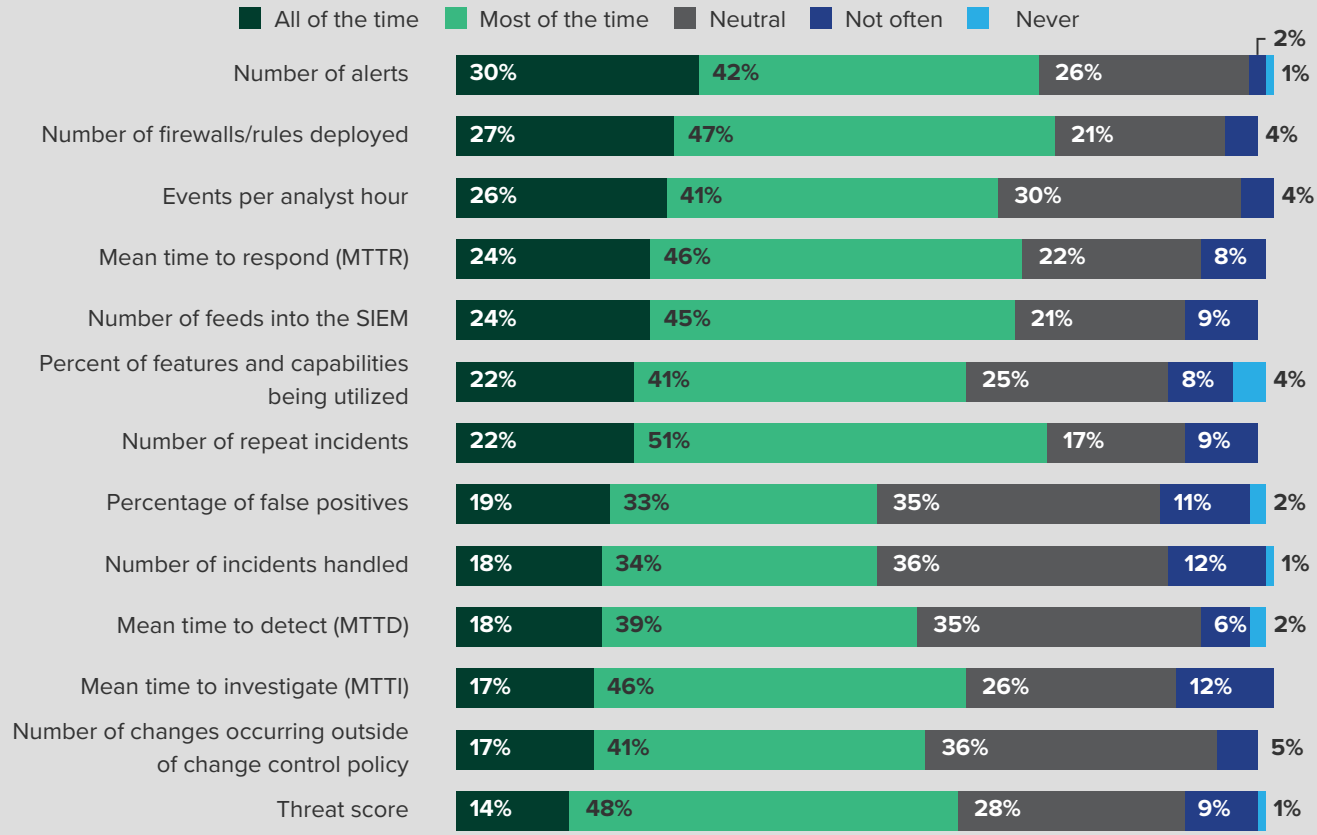
The status quo cannot hold. Analysts feel overworked, companies are experiencing breaches more frequently, and business leaders are frustrated. Nearly 50% of survey respondents noted that they struggle to perform additional threat hunting to supplement automated detection capabilities. They are working reactively, rather than proactively, in large part due to their struggle to maintain a robust security operations team. And their analysts' time is wasted on chasing false leads and performing highly manual processes.

All of this negatively impacts organizations' security postures, with teams rarely meeting success metrics. Security operations teams are evaluated across five key metrics, on average, with the most popular metrics being: mean time to investigate, number of incidents handled, mean time to respond, threat score, and number of alerts. However, less than half of teams are able to meet these metrics most of the time and even fewer are able to hit their key metrics all of the time (see Figure 4).

Less than half of teams are able to meet their key metrics most of the time, and even fewer are able to hit their key metrics all of the time.

Figure 4: Security Operations Teams Are Unable To Hit Key Metrics

"Thinking about the last year, how frequently is your internal security operations team able to hit your goals for the following key metrics?"



Base: 83-156 global security operation decision makers who use formal metrics to evaluate the success of their security operations team
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

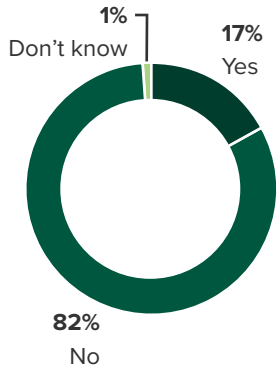
FORRESTER®

- **Businesses struggle to attract and retain experienced analysts.** Over 40% of IT decision makers noted that they struggle to hire experienced security operations staff and hire enough analysts to manage the workload. At the same time, over a third indicated that as an organization, they struggle to retain good talent.
- **Teams are using siloed and poorly integrated tools to investigate and remediate alerts.** The top technology-related challenges that inhibit the ability of security operations decision makers to prevent data breaches are the steep learning curve of their existing toolset and a lack of integration between security tools. Only 17% of alerts are touched by automation, leaving security teams to rely on an average of 10 different categories of security tools when managing alerts. In fact, only a quarter are using behavioral analytics, indicating that teams are unable to detect threats without a known malware signature. Only 49% agree that the data and information from their various security tools are well integrated, and over a third indicate that their staff wastes significant time chasing false leads.
- **Few organizations have a solution to address the security operations challenges they face.** Only 17% of organizations have a solution that provides effective visibility across networks, applications, and endpoints; these solutions are aimed at applying analytics and automation to help address threats (see Figure 5). Most organizations are left to piece together a solution through existing tools, creating a patchwork of manual processes for analysts.

Only 17% of alerts are touched by automation.

Figure 5: Current Solutions

"Does your organization currently have a solution that provides effective visibility across networks, applications, and endpoints, applying analytics and automation to help you address threats?"



Base: 315 global decision makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

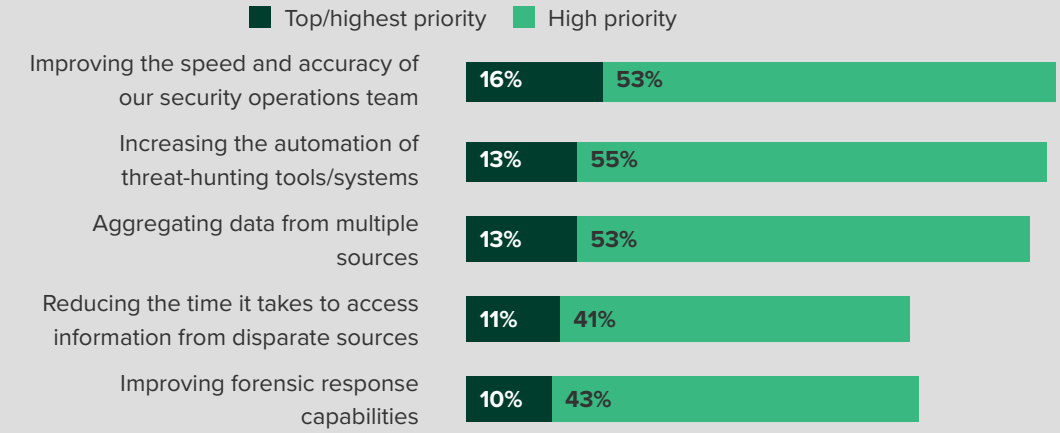
Opportunities For Improving Security Operations

Most security operations decision makers recognize that their current approaches to threat detection, investigation, and remediation are fatally flawed. They realize that to meet their top priorities for 2020 — improving the speed and accuracy of their team and increasing the automation of threat-hunting tools/systems — leaders must focus on solving for both short- and long-term issues (see Figure 6). It's a virtuous cycle. Improving efficiency and visibility creates happier, more productive analysts, who in turn improve their organization's security outcomes and are therefore able to work more efficiently.

- **Most teams are not tapping into the full potential of automation.** Only 13% of organizations are using automation/machine learning (ML) for the full lifecycle of an alert – triage, analysis, and response. Seventeen percent are not using automation/ML at all.
- **Extended detection and response (XDR) is seen as a solution that can help with analyst fatigue, tool inefficiency, and overall security outcomes.** XDR is a set of capabilities that aggregates data from various sources such as the network, endpoints, and application stacks to improve detection and response. XDR, as a category, aims to solve many of the top challenges that analysts and security operations teams are facing. XDR integrates data sources and capabilities of siloed tools so that companies can execute threat detection and response on all devices — managed and unmanaged — and data sources. This gives security teams better visibility and improves analysts' efficiency, ultimately leading to happier, more productive analysts and more secure environments for organizations.

Figure 6: Increasing Speed And Automation Are Top Priorities For The Next 12 Months

"Which of the following security operations improvements is your organization prioritizing for the next 12 months?"



Base: 315 global decision makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

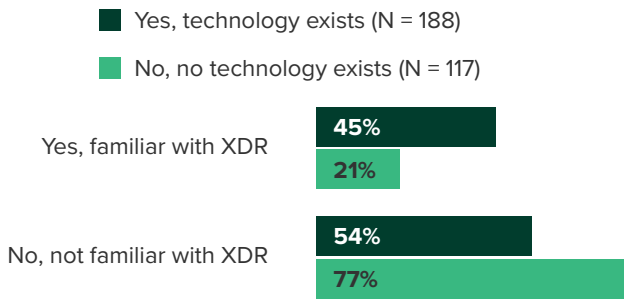
FORRESTER®

- **Decision makers who are familiar with XDR are more than twice as likely to feel that there is a security technology that will meet their needs.** Of those who are familiar with XDR, 45% believe that there is a currently existing technology in the market that would meet their security operations' needs, compared to 21% who don't believe such a technology solution exists (see Figure 7).
- **Those who invest in improving their detection and response technologies expect a myriad of benefits.** Respondents expect that improving detection and response capabilities will increase the productivity of their less-experienced analysts, increase visibility across multiple sources to find threats faster, and reduce the number of false positives that analysts waste time chasing.

Figure 7: Familiary With XDR Breeds Confidence In Technology Solutions

"Are you familiar with what XDR technology is?"

"Do you feel that technology currently exists in the market which meets your security operations' needs?"



Base: 305 global decision makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

Those who are familiar with XDR technology are more than 2 times as likely to feel that there is a technology that currently exists that can meet their security operations teams' needs.

Key Recommendations

Security teams require a unified view of their organization's threat mitigation technologies to align the people, processes, and technology within the organization toward the singular mission of defending that organization. Organizations familiar with the concept of XDR are shown to have confidence that this is the right solution for solving their top challenges.

Forrester's in-depth survey of 315 global IT decision makers about security operations teams yielded several important recommendations:

Improve visibility with unifying technology that seamlessly integrates telemetry from multiple sources. Organizations need to ensure they are able to aggregate data across networks, applications, and endpoints in a single, scalable data lake for more effective hunting and detection.

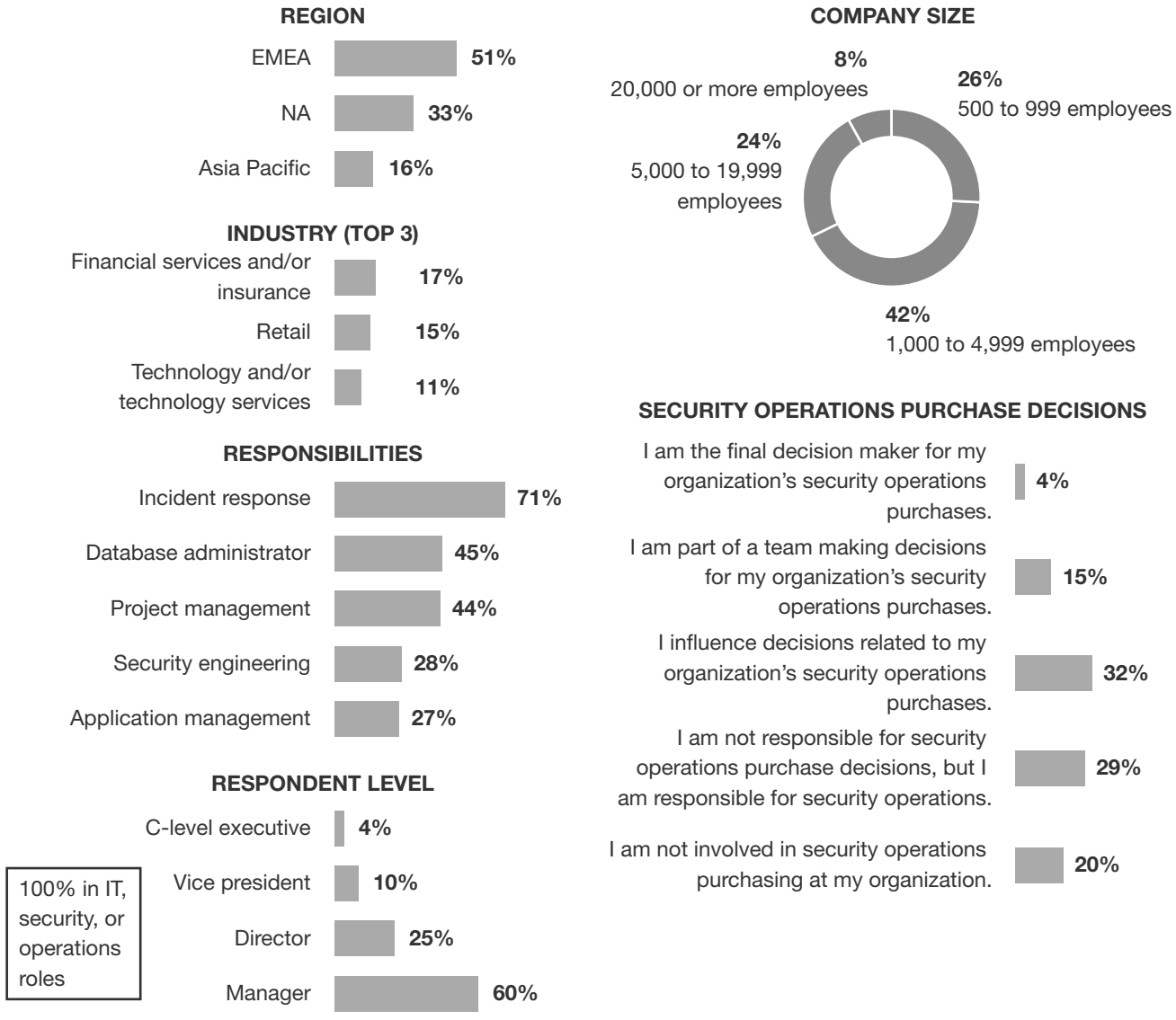
Leverage security analytics capabilities such as machine learning to surface indictable patterns for detection. Many SOCs are alert driven. By improving the quality of alerts, organizations can start to reduce alert fatigue and get more proactive with security.

Invest in capabilities that automate root cause analysis. Reduce SOC triage time with mature analytic capabilities that will surface related events and automate investigation. The correlation of these events provides the opportunity to have a second or third chance at an earlier, lower confidence alert which may have been ignored or overlooked.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 315 IT decision makers to evaluate their current approaches in managing security operations at their organization. Survey participants included decision makers in IT, security, or operations roles who are directly involved in security operations and/or incident response. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in February 2020 and was completed in March 2020.

Appendix B: Demographics/Data



Base: 315 global decision makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

Appendix C: Endnotes

[1] Source: "Your Guide To Cyberinsurance," Forrester Research, Inc., June 6, 2018.

[2] Source: "Planning For Failure: How To Survive A Breach," Forrester Research, Inc., July 6, 2018.

FORRESTER®