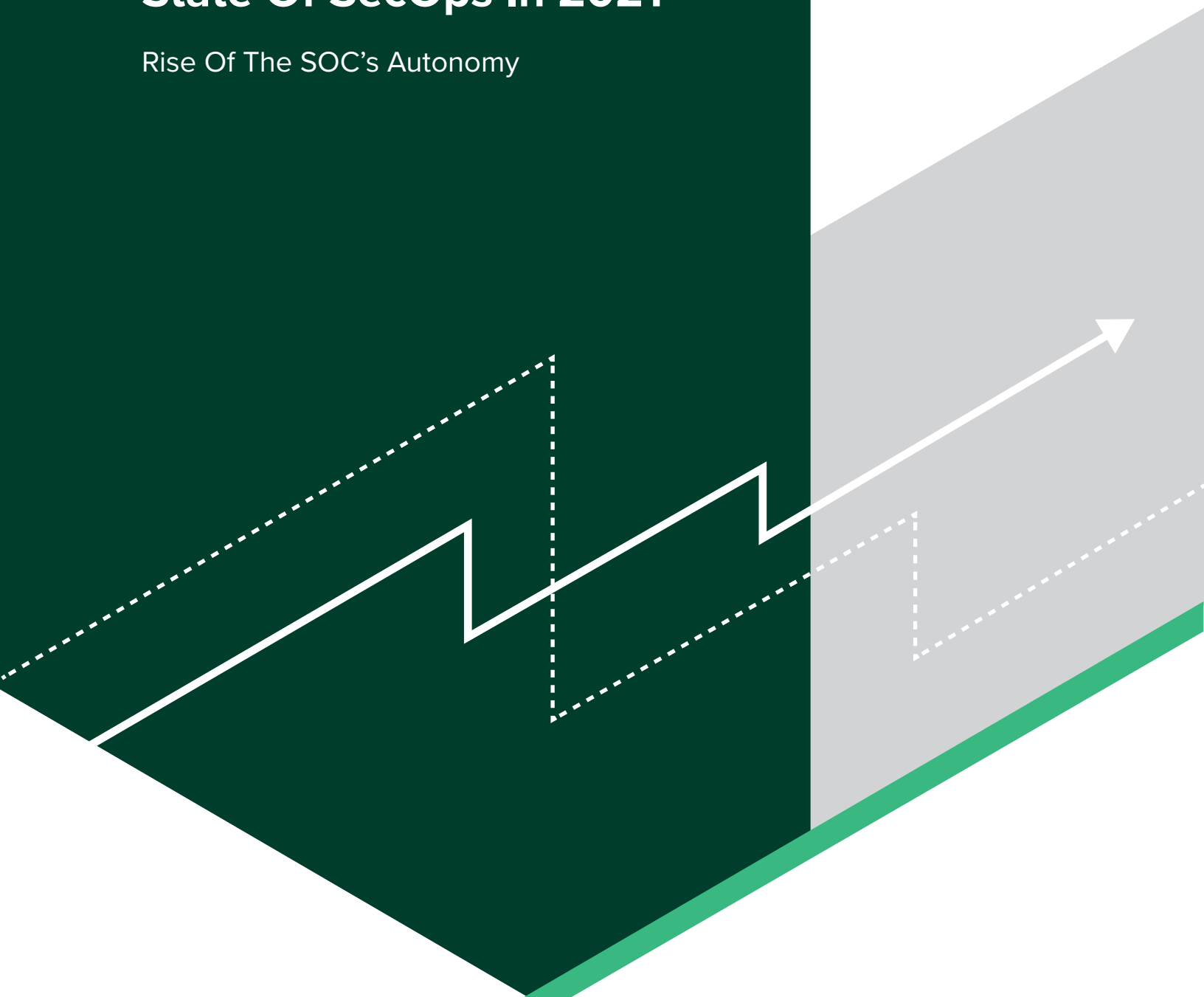
A Forrester Consulting
Thought Leadership Paper
Commissioned By Palo Alto Networks

April 2021

State Of SecOps In 2021

Rise Of The SOC's Autonomy



FORRESTER®

Table Of Contents

Project Director:
Ana Brzezinska,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security & 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®

Executive Summary

To stop modern attacks, organizations need more integration, more visibility and more automation — analysts are struggling underwater trying to keep up with the immense volume of alerts that they receive every day. Today, analysts note that they struggle to triage and investigate threats quickly, with manual processes slowing down alert triage for a striking 74% of the survey participants. Because teams face a deluge of security alerts — 11,047 alerts a day on average — many teams ignore low-priority alerts, leaving over a quarter of alerts completely untouched.

Worse yet, almost two-thirds of security teams still rely on legacy endpoint security solutions, like antivirus tools and endpoint protection platforms, which limit their ability to gather rich endpoint data for detection, investigation, and response. Security operations decision-makers recognize that they must further embrace automation to relieve their analysts and allow for more strategic work to be focused on, rather than the day-to-day tactical management. Many organizations have begun to enlist automation to assist with pieces of the security workflow, and are working to increase their level of automation over the next two years.

Palo Alto Networks commissioned Forrester Consulting to explore today's cybersecurity challenges and opportunities. Forrester conducted an online survey with 418 global security operations decision-makers who have responsibility over detection and response purchasing to understand the state of current security operations. We found that while few organizations have reached SOC maturity, 70% of respondents have begun their automation journey and 44% expect to use more automation in the next one to two years.

KEY FINDINGS

- **Security operations teams are still struggling to address the high volume of alerts.** Less than half of decision-makers note that their organization is able to address most or all of the alerts they receive in a day. Teams struggle to quickly triage and investigate threats; and because they face a deluge of security alerts, many teams are forced to ignore low-priority alerts, leaving organizations vulnerable.
- **Almost half of all firms report struggling to hire and retain qualified staff.** Because so much of threat detection, investigation, and response is still done manually, security operations teams are dealing with high rates of analyst burnout. Many teams are beginning to automate pieces of their workflows to alleviate this.
- **Nearly three-quarters of decision-makers have begun their SOC automation journey.** With full SOC automation being a long-term goal, 70% of surveyed organizations have begun their automation journey, and 44% expect to be using more automation in the next one to two years. Those who have adopted more automation report having a happier security operations team and a lower likelihood of technical challenges, such as poor visibility into security tools and a lack of tool integration.

Security Operations Teams Are Unable To Address Today's Volume Of Alerts

Today's security operations teams are struggling. Analysts are faced with over 10,000 alerts a day and most security operations teams largely rely on manual review, which takes far too long. Security professionals are bogged down by false positives and are unable to perform threat hunting.

- **Few organizations are confident in their ability to protect against today's attacks.** Crucially, only 51% of interviewees are confident that they have the right skills to secure their organization. Most organizations are spending their time triaging and investigating alerts, rather than responding to or hunting for threats and improving processes. Less than half are satisfied with their ability to detect threats, and only 28% of decision-makers are satisfied with their ability to proactively hunt threats.
- **SecOps teams face over 10,000 alerts a day.** Today's teams face, on average,11,047 alerts a day, a minor — 0.8% — decrease from 2019. Importantly, there was a 6% *increase* in the number of firms that report 25,000 to 50,000 alerts a day. Over a quarter of all alerts are untouched or ignored and while automation is increasing slowly — 18% of alerts are touched by automation in 2020, compared to 17% in 2019 — progress is slow (see Figure 1).

Figure 1

"Which of the following best describes how your security operations team is structured?"

19% A single tier: All analysts are roughly on the same level and have the same responsibilities.

81% Multitier: Analysts are at different levels with different responsibilities.

"On average, how many alerts does your internal security operations team receive per day?"

Average — 11,047.0

10% 25,001 to 50,000

26% 10,001 to 25,000

23% 5,001 to 10,000

27% 1,000 to 5,000

13% Less than 1,000

"In an average week, what percentage of hours are spent by your internal security operations resources performing the following tasks?"

Task	Average % of hours spent by internal sec ops resources on task	Hours a week
Triaging alerts	**19.1%**	38.2 hours
Investigating alerts	**31.1%**	62.2 hours
Mitigating/ responding to alerts	**14.4%**	28.8 hours
Threat hunting	**15%**	30 hours
Process improvements	**10%**	20 hours
Compliance reporting	**8%**	16 hours

"Of the alerts that your internal security operations team received per week, what percent are..."

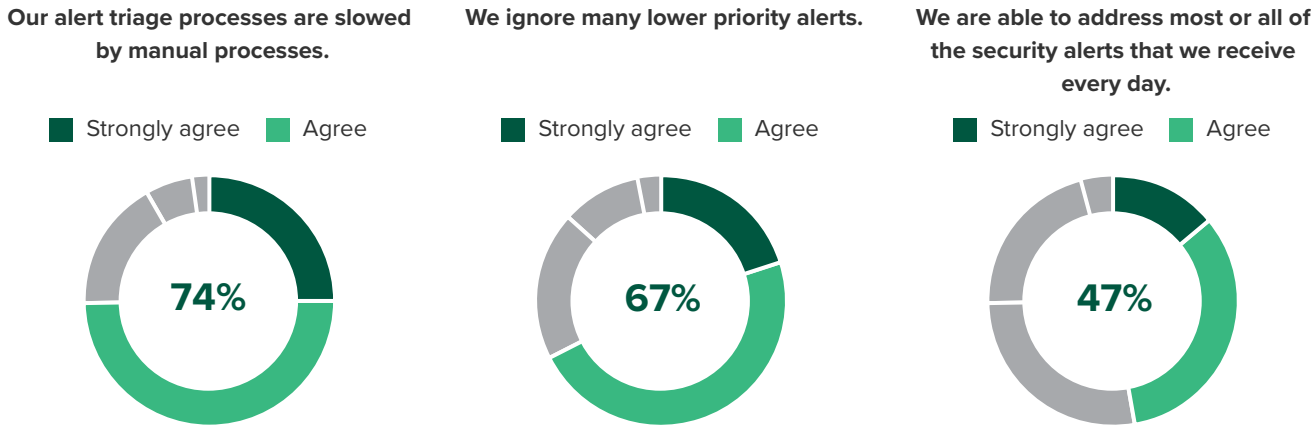
Task	Average % per week
Manually reviewed/triaged	**20.7%**
False positives	**30%**
Touched by automation	**18.1%**
Untouched	**26.1%**

Base: 418 global security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, December 2020

- **Almost two-thirds of security teams rely on legacy antivirus, next-generation antivirus, or endpoint protection products.** Sixty-one percent of decision-makers noted that their organization's *primary* endpoint security tool was either a traditional or next-generation antivirus tool or an endpoint protection platform. Relying on legacy tools without endpoint detection and response (EDR) limits their ability to gather rich endpoint data for investigation and response.
- **Organizations recognize that they are vulnerable today.** Nearly three-quarters believe that their triage processes are slowed by manual efforts; 67% ignore low-priority requests. Further underscoring this is the fact that less than half of surveyed decision-makers note that they are able to address most of the security alerts they receive in a day (see Figure 2). The volume of alerts they have to contend with is untenable.

Figure 2

Please indicate your agreement to the following statements.



Base: 418 global security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, December 2020

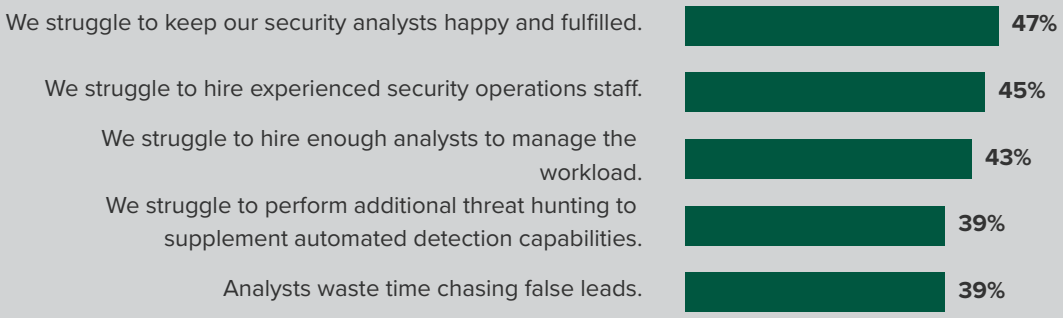
Lacking Automation, Many Organizations Struggle To Hire And Retain Qualified Staff

Today's security operations organizations are beginning to dip their toe into the world of automation; however, many are unprepared to harness the full power of SOC automation. Two-thirds of interviewees are only using automation for specific steps of the incident response cycle, and almost 20% aren't even using automation. This means that each alert must be manually processed, which unsurprisingly results in an overtaxed security operations team and high turnover rates for dissatisfied analysts.

- **Most organizations see the value in automation, and they are beginning to automate pieces of their incident response processes.** While full automation is a long-term goal, 70% of decision-makers report they have built automation into a few of their common security workflows. Automating specific actions inside of workflows has the benefit of accelerating response without the risk of full automation without human interaction.
- **Organizations struggle to hire and retain staff.** The top people-related challenges that organizations report when preventing data breaches is keeping their analysts happy and fulfilled. On top of that, nearly 50% report struggling to hire and retain the right staff to manage workloads (see Figure 3). Alert fatigue, too much focus on manual alert triage, and limited time to spend on high-level strategic work all contribute to analyst frustrations.
- **Those with higher SOC automation readiness are less likely to struggle with staff and tools.** Organizations that have embraced automation are less likely to struggle with keeping their analysts happy — 56% of organizations with low readiness struggle, as compared to 36% of organizations with high readiness. And those firms that have embraced automation are 13 points less likely to struggle when hiring experienced security operations staff. Additionally, less than a third of high readiness firms currently struggle with their tools, as compared to nearly 50% of low readiness firms.

Figure 3

What are the biggest people-related challenges your organization faces in preventing data breaches? (Select all that apply.)



Base: 418 security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February and December 2020

FORRESTER®

Increasing Automation Results In A Happier Team And Fewer Struggles

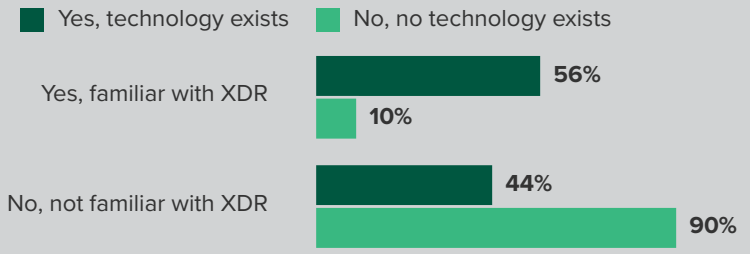
Decision-makers recognize that their current approaches are woefully inadequate, and as such, they are looking toward product advancements and the adoption of new technologies that will improve their efficiency. And while few organizations have reached SOC automation maturity, 70% have begun their automation journey and 44% expect to use more automation in the next 1-2 years. The organizations that have adopted automation report having happier staff and lower likelihood to struggle with their security tools.

- **Security operations professionals look to increase visibility and productivity.** Nearly 50% of decision-makers expect improved detection and response technologies to increase their visibility to find threats faster; 47% anticipate increased productivity for their less experienced analysts; and 46% anticipate an increased return on security investment. By investing in the right tools and technologies, these firms expect to alleviate their staffing issues and allow their security operations teams to focus on strategic work, rather than on the tactical day-to-day minutiae.
- **Decision-makers who have heard of XDR are five times more likely to believe a technology exists in the market that meets their security operations' needs.** XDR, or the extended set of detection and response capabilities which aggregate data from various sources such as the network, endpoint, and application stacks to improve detection and response, is a relatively new class of security technology. However, in the two short years that XDR has emerged as a security tool category, 15% of organizations have already adopted it. On top of that, when asked if there is a technology that currently exists in the market that meets their security operations' needs, respondents who were familiar with XDR were five times more likely to agree than those who had not heard of XDR (see Figure 4).

Figure 4

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

"Are you familiar with what XDR technology is?" By XDR, we mean: an extended set of detection and response capabilities which aggregate data from various sources such as the network, endpoint, and application stacks to improve detection and response.



Base: 418 security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February and December 2020

› **High SOC automation readiness firms are more likely to be able to address alerts.** While today's organizations are still in the early stages of building a strong foundation for future SOC automation readiness, those who are high on the readiness scale are more likely to be able to address most or all security alerts (53%, compared to 45% of low readiness) and are more likely to have a built a tech stack that meets their needs (72%, compared to 55% of low readiness) (see Figure 5). Firms have created a stronger security operations team for today's demands by focusing on aligning their data, threat detection capabilities, and automated processes to begin their journey to a fully automated SOC — where automation assists in all workflows.

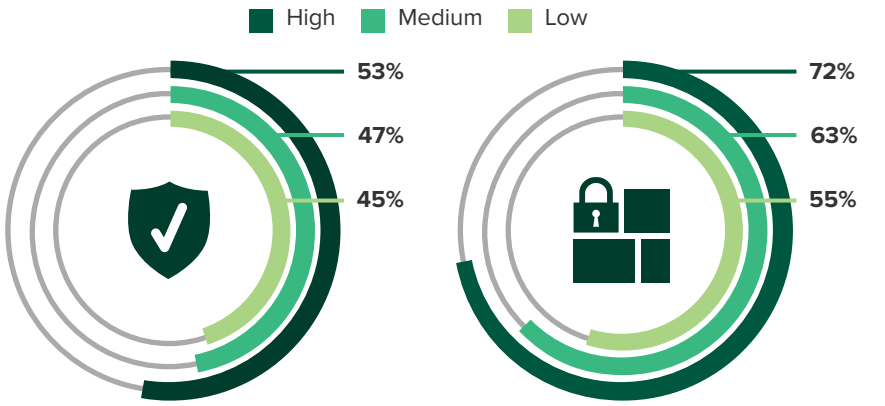
› **Over the next 1 to 2 years, decision makers expect to increase their use of threat intelligence and increase their use of automation.** Building upon the foundation of data, capabilities, and processes, over half of all security operations professionals surveyed expect to increase the use of threat intelligence for incident enrichment and response over the next 12 to 24 months (see Figure 6). Additionally, 44% of decision makers plan to increase their use of automation for incident response over the same timeframe. Taking immediate steps towards automation, organizations can make to help alleviate the challenges they face today.

Figure 5

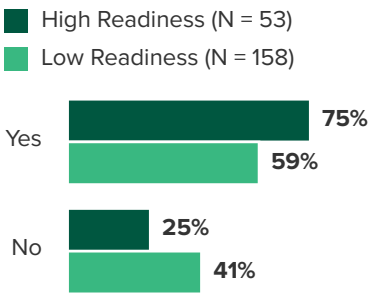
Please indicate your agreement to the following statements.

We are able to address most or all of the security alerts that we receive every day.

Our current security operations technology stack meets our needs.



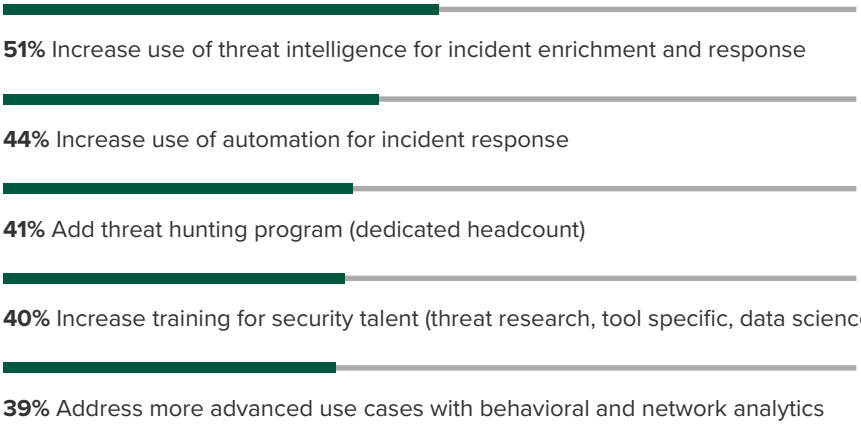
"Do you feel that technology currently exists in the market which meets your security operations' needs?"



Base: 418 global security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, December 2020

Figure 6

"How do you expect your security processes to change in the next 1-2 years?" (Select all that apply.)



Base: 418 global security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, December 2020

Key Recommendations

Security leaders must embrace automation to keep up with the pace of threats, improve response times, and empower their security operations teams. Security leaders can take steps now to build a foundation for an ML-driven, automated future. To get started, security leaders should:

Start by automating aspects of incident response to reduce MTTR. Analysts struggle to triage and investigate alerts fast enough, leading to missed lower priority alerts. Take this opportunity to automate the most time-consuming, manual, and cumbersome parts of the investigation and response process.

Increase automation of repetitive, manual tasks to attract and retain talent. Analysts struggle with tactical, monotonous activities — constant triage and alert response leading to burnout. Automate manual work to give analysts time to focus on strategic initiatives.

Most security teams have begun their automation journey; now it's time to ramp it up through integration. Integrate security tooling into a unified platform for centralized logging, alert correlation, and orchestrated response.

Appendix A: Methodology

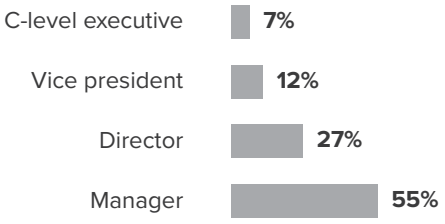
In this study, Forrester conducted an online survey of 418 global security operations decision-makers with influence over detection and response purchase decisions in EMEA, North America, and ANZ. Survey respondents were managers or above and worked at organizations with 500 or more employees. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in December 2020 and was completed in January 2021.

Appendix B: Demographics

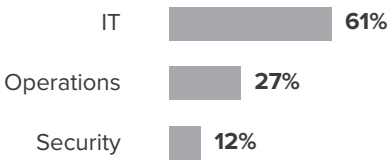
REGION/COUNTRY

50% North America | **38%** EMEA | **13%** ANZ

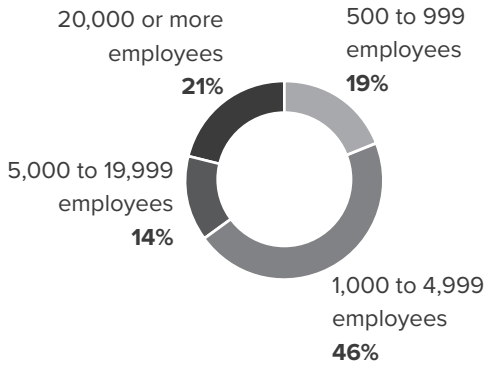
POSITION



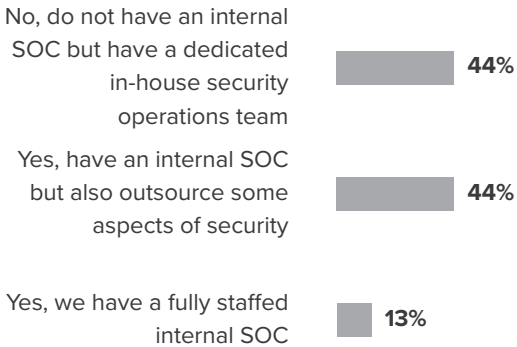
DEPARTMENT



COMPANY SIZE



SECURITY OPERATIONS CENTER



Base: 418 global security operations decision-makers with influence over detection and response purchase decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, December 2020

FORRESTER®