The State of Security Automation

This report is based on a survey of security professionals that covers the state of security automation. Findings include the revelations that incident response teams remain relatively small and tend to handle a sizable share of incident response processes in-house. Automation is taking place, but it appears to lag behind the volume of incidents. Many teams plan to automate more but are facing delays caused by a lack of skills and confusion about where to begin.

Executive Summary

This latest Palo Alto Networks study of the state of security automation analyzes the views and experiences of 266 IT and security professionals. Located primarily in North America, respondents work in organizations that span multiple industries and range in size from 1,000 employees to over 20,000. The research is timely, as security teams face increasing pressure to mitigate an ever-growing array of cyberthreats.

Highlights:

- **Most incident responses are taking place in-house**—90% of respondents either perform incident response completely in-house or "primarily in-house, or augment by consultants as needed."
- **Incident response teams are small**—56% of respondents work at organizations with incident response teams with five or fewer members. One in six organizations with 10,000+ employees field teams consisting of just one-to-three people.
- **Incident response teams have to coordinate with other areas**, e.g., 69% of respondents have to interact with network/firewall admins to resolve incidents.
- **Half of threat management is manual**—this seemingly high rate of manual processes for such a critical workload could contribute to overloading limited staff resources.
- **Phishing, malware and endpoints are the highest volume incidents**—the three highest volume incident types included phishing alerts, named by 74% of respondents, malware alerts (56%) and endpoint security alerts (53%).
- **Incident response times threaten to swamp under-sized teams**—while most incidents can be resolved within an hour, a surprisingly high number take days to sort out, potentially overloading response team members who can only work so many hours a day.
- **Organizations are automating security processes**—top priorities for automation have been phishing response (37% of respondents) and vulnerability management (29%).
- **A variety of factors are holding security automation back**—50% of respondents cited "Not sure where to start" as the biggest barrier to automation. Respondents expressed a strong interest in playbooks and integrations that would facilitate the implementation of automation.

Contents

Introduction

Palo Alto Networks recently conducted a survey of security professionals that examines the current state of security automation. The results reveal a group under pressure to cope with incident response. A large proportion of incident response is still handled in-house by relatively small teams. For certain workloads, such as threat management, half of the respondents report they are using manual processes. Response processes require coordination across multiple departments, some of which are outside of IT or security operations. While these teams are automating their incident response processes, the automation effort lags behind the volume of incidents. Reasons for delaying automation include a lack of skills and confusion about where to begin.

Survey Overview

The survey respondents comprise a diverse group. Of the 266 who shared their insights, 25% serve in the role of Security Engineer, 18% in network security operations and 15% in VP/CISO or CIO roles. The respondent group also represents a variety of organization sizes and industries. Twenty-two percent have over 20,000 employees. Twenty-one percent have between 2,500 and 4,999 employees, and 19% have between 5,000 and 9,999. The appendix provides the full details of the survey demographics.

Why Security Automation Matters Today

The backdrop for this series of surveys on the state of security automation is a world where cyberthreats are on the rise, while the pool of available talent remains stagnant. As the potential for attacks becomes more probable, and the outcomes more serious, there are fewer people on hand to manage security incidents. This is not a sustainable or healthy situation for businesses and government organizations around the world.

Security automation is a viable response to this dilemma. By automating some or all of the steps in security operations, organizations can make optimal use of the staff they have—without having to worry so much about team members getting burned out by the stress of it all. Security automation is a rather broad area, covering simple in-tool capabilities as well as comprehensive security orchestration, automation, and response (SOAR) solutions and the like. Most of the organizations covered by this survey are figuring it out as they make their way toward a higher level of security automation.

Survey Findings

The survey offers a view into security departments that depend on small teams to handle incident response in-house, with many processes still being performed manually. SOAR use, which signifies automation, is increasing, but still has room to grow. A variety of factors, such as a lack of skills and budget, are holding back the move to greater security automation, however.

Incident Response Is Mostly Performed In-House

How are survey respondents' organizations handling incident response? It seems to be a mostly in-house affair, with 90% of respondents either performing incident response completely in-house or "primarily in-house, or augment by consultants as needed." Figure 1 summarizes the findings. Nearly half (49%) handle incident response in-house. Just 1% have it fully outsourced. Companies are relying on themselves to handle security incidents, for the most part.

One interesting finding has to do with the consistent split between in-house and outsourced incident response for organizations of different sizes. Figure 2 shows the percentage of in-house vs. outsourced incident response, by organization size. The results for each organization size grouping are nearly identical to the whole. Organizations with 1,000–2,499 employees have 52% in-house, versus 45% for organizations of 2,500–4,999, 52% for 10,000+ and 49% in aggregate. The proportions for in-house augmented by consultants, partially outsourced and fully outsourced are also comparable in each organizational size grouping.

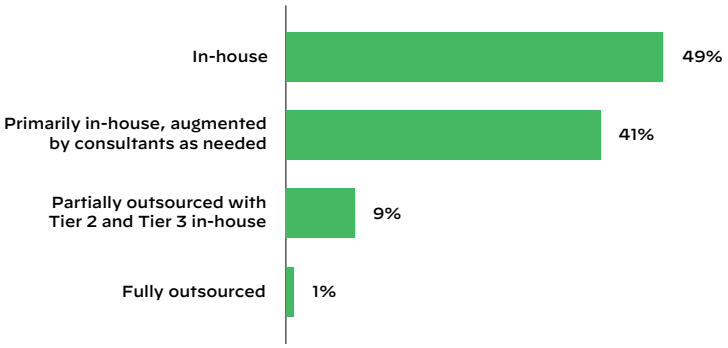

Figure 1: Responses to question "Our incident response is:"

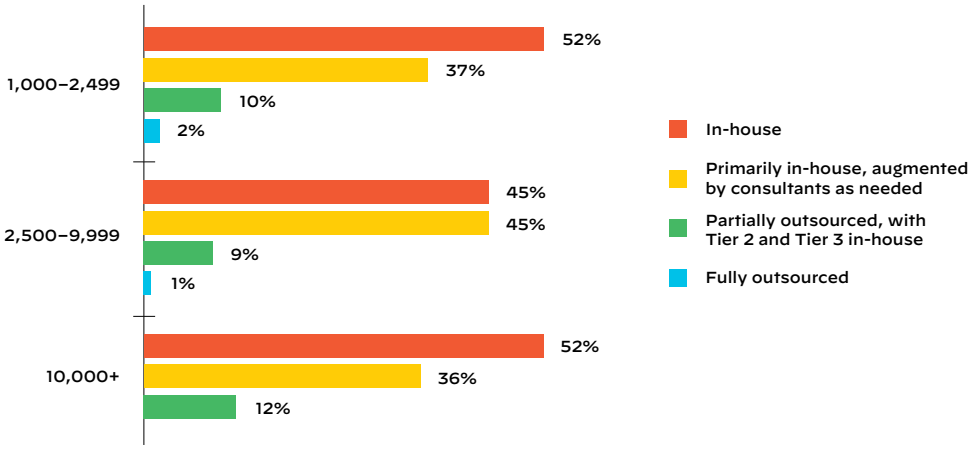

Figure 2: How incident response is handled, by organization size

Incident Response Teams Tend to Be Small

Incident response teams are smaller than one might guess, with over 50% of respondents reporting that their teams had fewer than 5 people, as shown in Figure 3. Twelve percent had between 11 and 25 members, and just 8% had over 25. Considering how many organizations are handling incident response wholly or partly in-house, these small team sizes may translate into a relatively high stress level: a few people bear complete responsibility for handling security incidents.

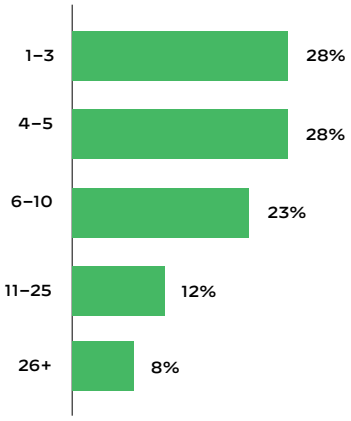

Figure 3: Responses to question "How many people on your security team are dedicated to incident response?"

Even big companies employ small incident response teams. Figure 4 captures this breakdown. It's not too surprising that 35% of organizations with between 1,000 and 2,499 employees would have teams of one-to-three people. What is striking is that 15% of organizations with over 10,000 employees also have teams of one-to-three people. Twenty-three percent of this large organizational cohort has teams of four-to-five people. That is not a lot of people to cope with a major enterprise's incident response workloads.

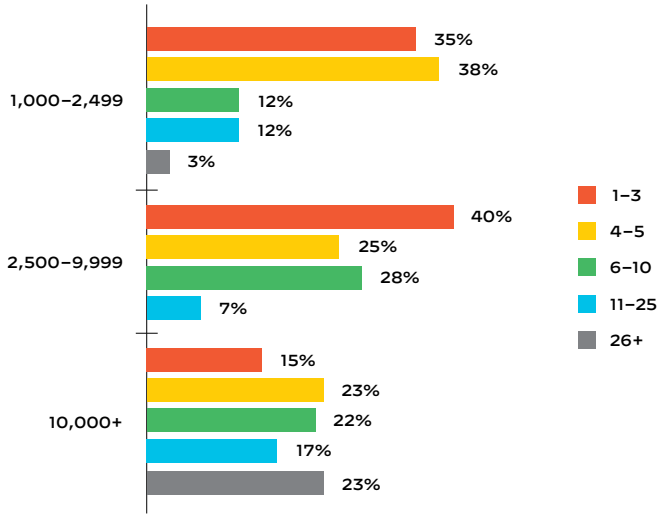

Figure 4: Responses to question "How many people on your security team are dedicated to incident response?"

Incident Response Teams Must Collaborate Broadly

Incident response is a multi-team sport, with the survey revealing that incident response teams must collaborate broadly across the organization as they deal with security events. Some of the teams they have to engage with are outside of security. For example, 32% of respondents who work in Cloud Security Operations (Cloud SecOps) collaborate with security department peers in Cloud DevOps in incident

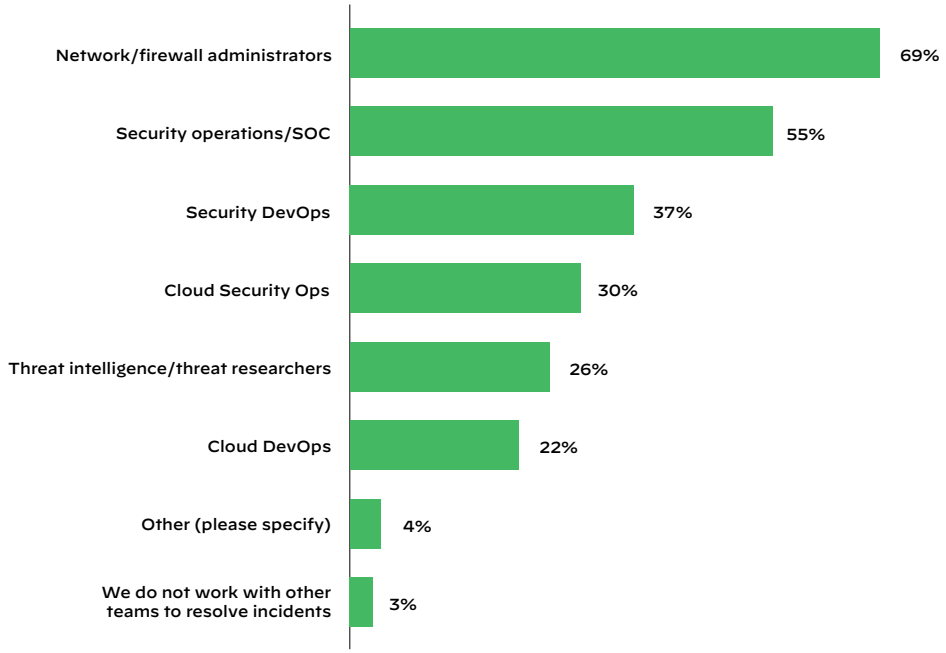

Figure 5: Responses to question "Do you work with other teams to resolve incidents? If so, which teams?" (Multiple answers allowed)

response, but 71% collaborate with network/firewall administrators. Figure 5 shows the results for all respondents. Other groups that get involved in dealing with incidents include cloud security ops, threat intel, cloud DevOps and more.

The need to be in touch with so many other groups, and coordinate activities with them, is further suggestive of a high stress level for the small incident response teams. For example, it is already challenging to investigate a threat and determine the best approach to its remediation. But, if a security analyst must also write emails updating other teams and orchestrate response steps with external people, that adds time and pressure to the whole situation. Automation can ease this burden.

Threat Management Is 50% Manual

Half of respondents manage threat feeds manually. The other half uses an assortment of threat feed management tools, as shown in Figure 6. Fifty percent is a high number for such a critical workflow, especially given how serious some of today's threats can be. With small teams, there is a risk of security staff overload due to threat management. In parallel, companies are exposed to the risk of mishandling security alerts. False positives waste time and resources. False negatives, wherein a real threat is marked as benign, can lead to security breaches.

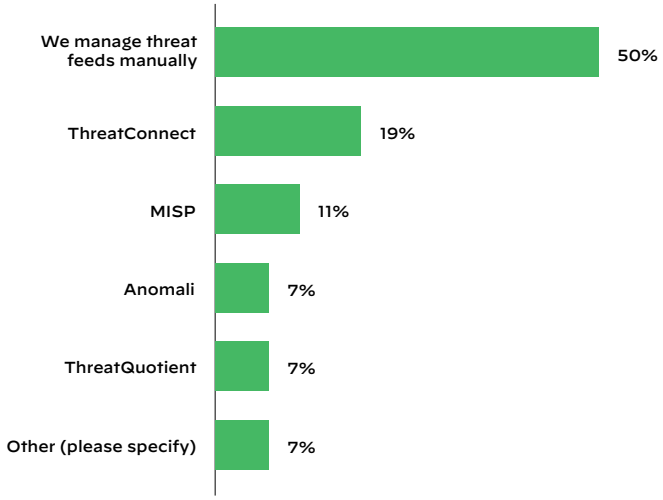

Figure 6: Responses to question "How do you manage threat feeds now?"

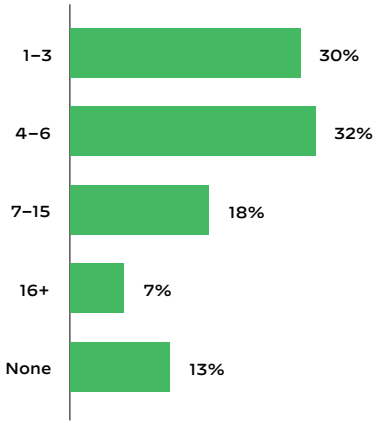

Figure 7: Responses to question "How many threat feeds do you currently subscribe to?"

Phishing, Malware and Endpoints Are Highest Volume Incidents

Asked what are the three highest volume incident types their teams have to deal with, 74% said phishing alerts. Fifty-six percent chose malware alerts, and 53% said endpoint security alerts. Network security weighed in at 40%. The remainder, include anomalous user logins, remote access/VPN, SIEM alerts and cloud service provider alerts, garnered between 15% and 17%. These findings make sense, given the prevalence of phishing as a vector for ransomware and a wide range of attacks. Malware, too, seems proportional to the volume of malware attacks occurring today.

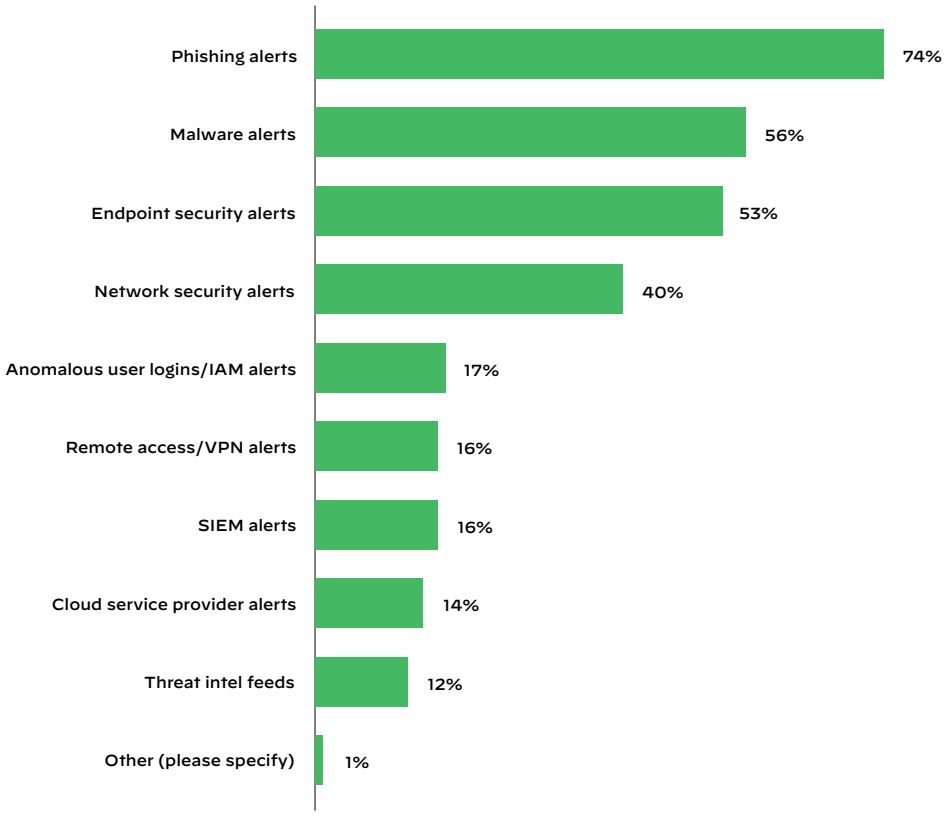

Figure 8: Responses to question "What are the 3 highest volume incident types your team has to deal with? " (Select 3)

Prevalence of Incidents vs. Response Times

The prevalence of an incident type does not necessarily translate into an undue burden on the incident response team. With phishing alerts, for example, while 74% of respondents place it in their top three highest volume incidents, 40% of these alerts can be resolved in 30-60 minutes. Another 29% of phishing alerts can be resolved within one-to-four hours. Only 5% of phishing alerts take one-to-two days to resolve, and just 2% take over two days. Figures 9 and 10 show details on how long each type of incident takes to resolve.

Several incident types that fewer respondents placed in their top three highest volume incidents appear to take quite a lot longer to resolve than the more prevalent ones. For example, with vulnerability findings, while over 50% said incidents were handled in fewer than eight hours, 16% said it took one-to-two days to resolve, and 18% said it took over two days.

To understand the ramifications of this range of response times, consider how distracting it would be to handle a high volume of 30-to-60-minute phishing incidents while staying on top of a smaller number of VPN alerts or vulnerability findings that take days to sort out. It would be a process of constant toggling between incident response workflows—not at all ideal for the small incident response teams featured in this study. And, while 30–60 minutes may seem like a quick time to resolution, if a team is handling a large number of such incidents, it could be overwhelming.

Table 1: Percent of Respondents Reporting an Incident Type as the Top Three Highest Volume vs. Length of Time It Takes to Resolve the Incident Type						
	% of respondents saying this is one of top 3 highest volume incidents	Resolved in 30–60 minutes	Resolved in 1–4 hours	Resolved in 5–8 hours	Resolved in 1–2 days	Resolved in 2+ days
Phishing	74%	40%	29%	15%	5%	2%
Malware or endpoint	56%/53%	21%	42%	15%	8%	2%
Cloud service provider	14%	16%	35%	21%	7%	2%
Remote access/VPN	16%	25%	31%	17%	12%	1%
Vulnerability findings	Not measured	10%	20%	23%	16%	18%

Note: Yellow shading highlights a particularly high proportion of long incident response times.

It is possible to imagine that a team could easily get completely overrun with incident responses, given the report timeframes here. A five-person team, for example, could easily get swamped if they get 50 malware or endpoint alerts per day. Table 2 shows a simple time estimate for resolving these incidents based on the survey findings. With 21 of these incidents (42%) taking between one-to-four hours to resolve, the team will have to work for between 21 and 84 hours—but they only have 40 hours of collective person-hours per day. When the other incidents are factored in, the team needs to find between 63 and 154 hours for these incidents in a 40-person-hour day.

Of course, the incident response times reported in the study don't always represent a 100% full-time focus on an incident. However, even allowing for toggling in and out of a single incident response as a team manages multiple incidents, the overstretching of team time resources still looms as an operational challenge.

Table 2: Estimated Time to Resolve Malware or Endpoint Alerts for a Five-Person Team						
Team size	**Team hours/day**	**Total number of alerts**	**Handled in 30–60 minutes**	**Handled in 1–4 hours**	**Handled in 5–8 hours**	**Total hours**
			21%	42%	15%	
Five	40	50	10.5	21	7.5	
Low time estimate (hours)			5.25	21	37.5	63.75
High time estimate (hours)			10.5	84	60	154.5

Incident Response Automation Is Happening

Survey respondents are automating incident response, as shown in Figure 11. For at least one respondent, automation has paid off. He said, "Security automation allows you to drastically reduce your incident response and dwell times and stay ahead of threats. Incident response that could take hours or even days can be reduced to mere seconds."

The rate of automation appears to lag behind incident load. For example, 28% of respondents have automated network security operations, but 40% put it in the top 3 highest volume incident types. Seventy -four percent of respondents ranked phishing alerts as a top-3 for volume, but just 37% have automated the phishing incident response process.

One respondent put the issue in perspective, noting, "We need automation for our common tasks, not once-per-year occurrences. Vendors often seem to be selling automation for those rare events, but overlooking the fact that we spend most of our time on phishing."

There are a number of reasons for this divergence between acknowledging a challenge and implementing automation to solve it. Automation projects take time and resources, so they tend to get executed when possible, not when needed. It's also likely that a high volume incident like phishing may not get

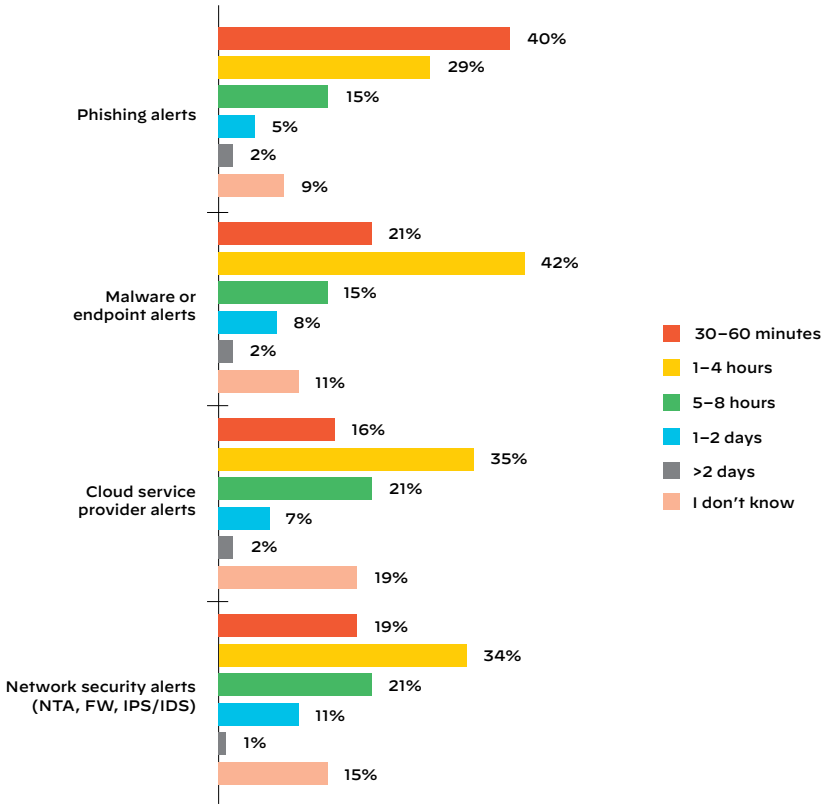

Figure 9: Responses to question "How long does it take to resolve each of these?" (Chart 1 of 2)

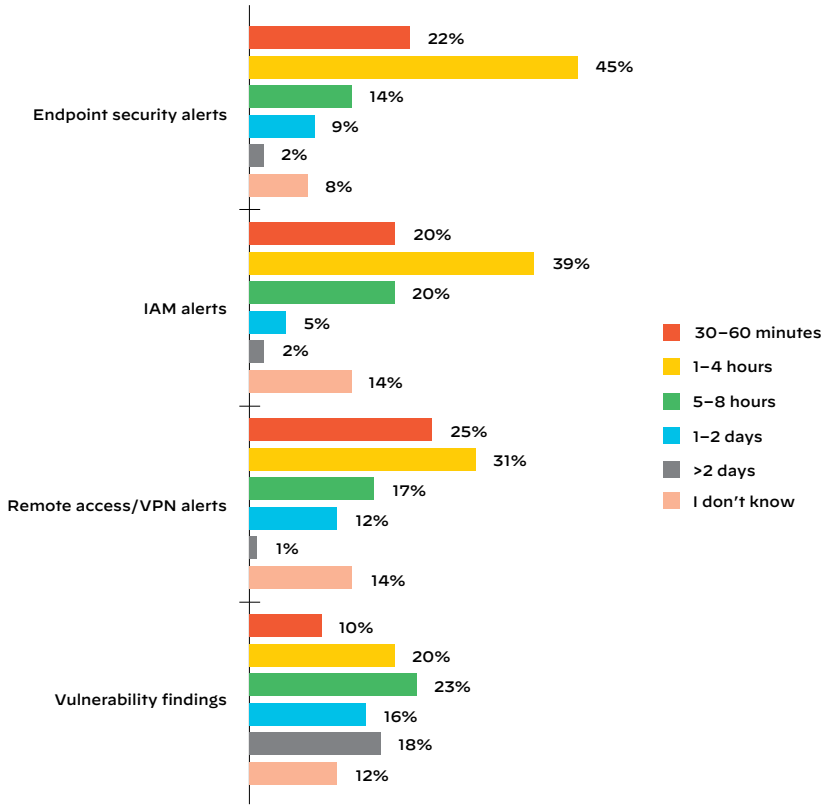

Figure 10: Responses to question "How long does it take to resolve each of these?" (Chart 2 of 2)

the highest priority for automation because it takes relatively less time to resolve each incident, as the data in Figure 9 suggests. A deluge of incidents could still create a substantial time burden, of course. A respondent offered some nuance on this issue, though, noting, "Phishing still needs a personal investigation for multilayered links. Automation has sped up response more than 10x."

People surveyed in this study have many plans for security automation in the near future. Asked which security operations they plan to automate in the next 18 months, 22% said "breach response, such as ransomware," 19% said "cloud security and configuration" and 18% said "network policy management. Sixteen percent of respondents said they will automate network security operations, access investigation, phishing response and threat intelligence within 18 months.

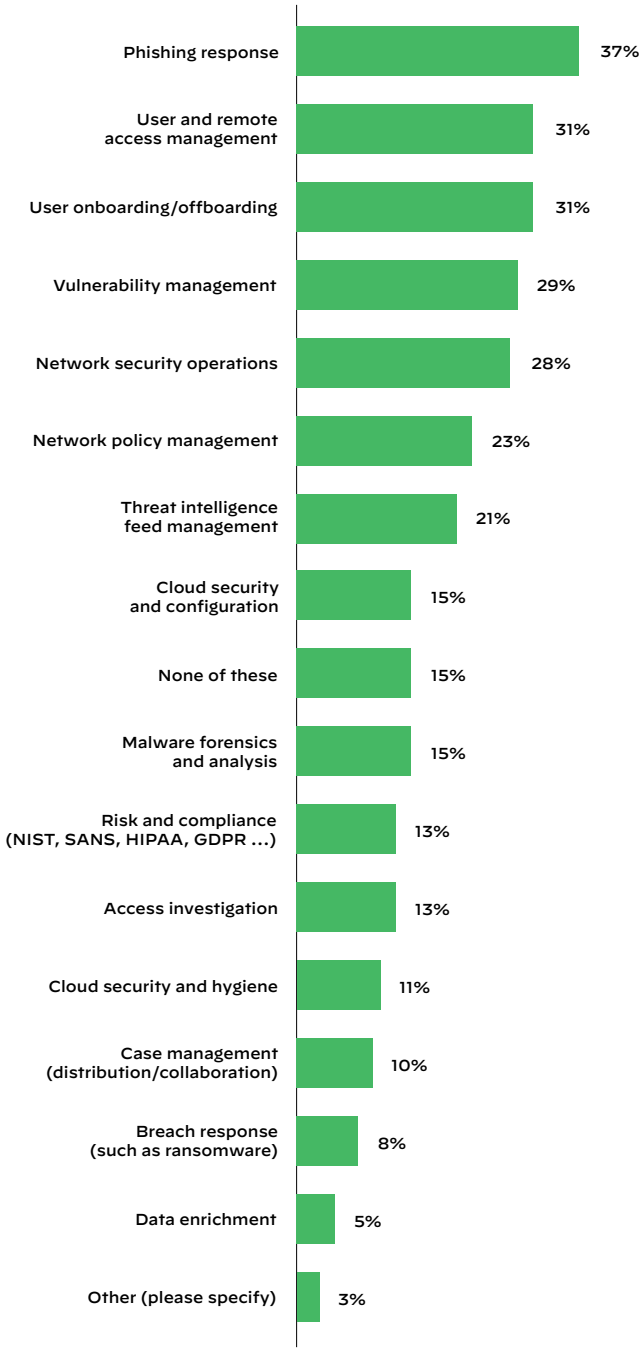

Figure 11: Responses to question "Which of these incident response processes, if any, have you automated?" (Multiple answers allowed)

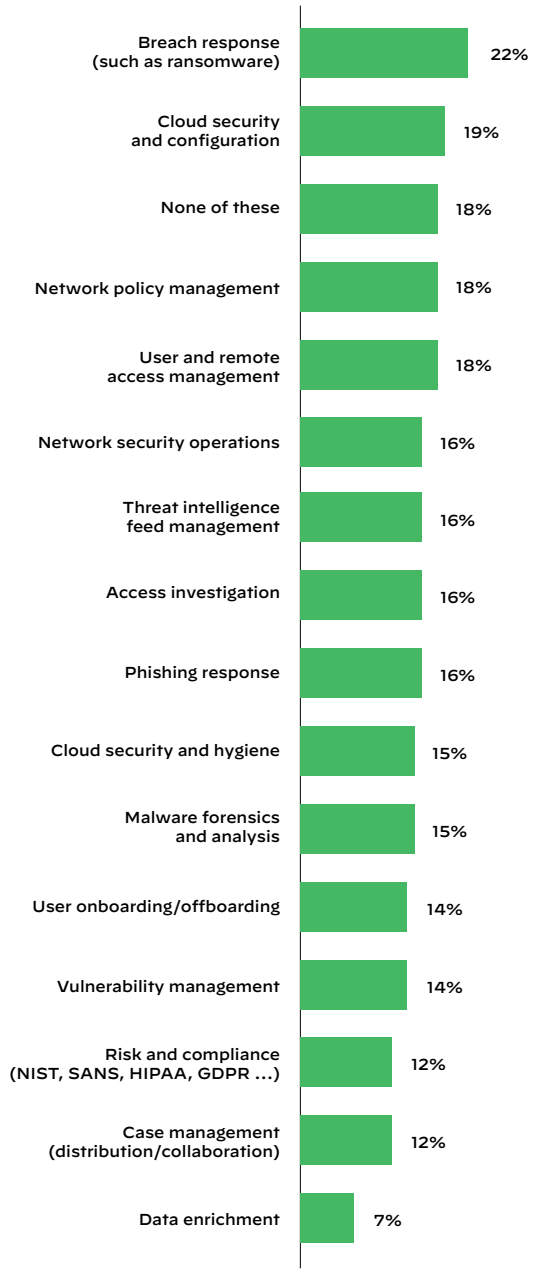

Figure 12: Responses to question "Which of these, if any, do you plan on automating in the next 18 months?" (Multiple answers allowed)

When asked "If resources were not a problem, what would be the one thing/area you would automate in your operations. One respondent said "account security." Another said "threat analysis," while other responses included "ticketing," "malware incident response" and "help desk incident response."

What would make security teams more likely to automate security? Figure 13 shows a strong preference for playbooks, with 43% of respondents saying hands-on training on building automation playbooks would make their organization more inclined to deploy security automation. Another 39% said that prebuilt automation scripts or playbooks for common use cases would help. As a respondent put it, "While SOAR platforms offer high integration, I need to see better out-of-the-box playbook capabilities and hybrid cloud interoperability."

Thirty-eight percent said they would want prebuilt integrations of tools to use in incident response. Further to this point, a respondent remarked, "It is currently difficult to integrate to a lot of tools in the security space. We currently own a lot of Cisco security tools, with the desire that Cisco create the integrations and tie the tools together. Of course, this would mean that they would need to create an integrated threat management dashboard to surface up intelligence across all of their products. This will take a lot of time so we are currently looking for an MSP that will provide us help hands to accomplish our goals."

Another respondent bolstered this point of view, saying, "There are too many tools/solutions that are needed to provide full defense-in-depth coverage in an IT security pattern today. Ingesting and normalizing the logs/alerts/events from all platforms is very difficult to get them aligned and useful to analysis. Solution providers who can provide a common format and clear integration will be critical to success. Once all logs are in one place, then the automation discussion can begin. Where newer technology is appealing is in providing assistance to flag specific events/alerts automatically, saving time for the analyst team to investigate only the highest likelihood for incidents."

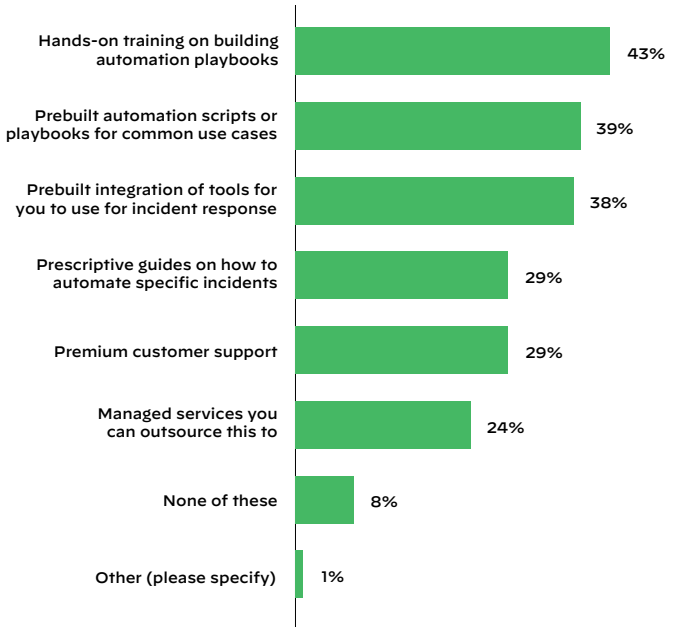

Figure 13: Responses to question "Which of these capabilities would make your organization more inclined to deploy automation?" (Multiple answers allowed)

A Variety of Factors Hold Back Security Automation

"Not sure where to start" is the number one reason for not deploying security automation, with 50% of respondents saying this was their most significant obstacle. Lack of budget and requisite skills were each named as barriers to automation by 21% of respondents. So, four out of five respondents are apparently not missing the money or trained people they need to automate. Fourteen percent said management does not understand the need. Twenty-nine percent say they are "managing fine with current processes."

A deficit in skills can hold things back. A respondent shared, "I think the challenges to automation are a) knowing what to automate and b) having the skill to do it. We have neither. Most organizations, based on my conversations, have the same struggle. The value of automation is clear, but putting it to practice is easier said than done."

Time is a factor for at least one respondent, who said, "The largest frustration is the time to implement with testing and each automation begets requests for more, so the implementation initiatives seem to take an inordinate amount of time."

Overall, though, the data for this question, coupled with the desire for playbooks shown in Figure 13, suggests that organizations want more ready-to-go solutions for security automation. With half of the respondents not knowing where to start, and 43% wanting training on building playbooks, it becomes apparent that security organizations need some prebuilt automations they can deploy with relative ease.

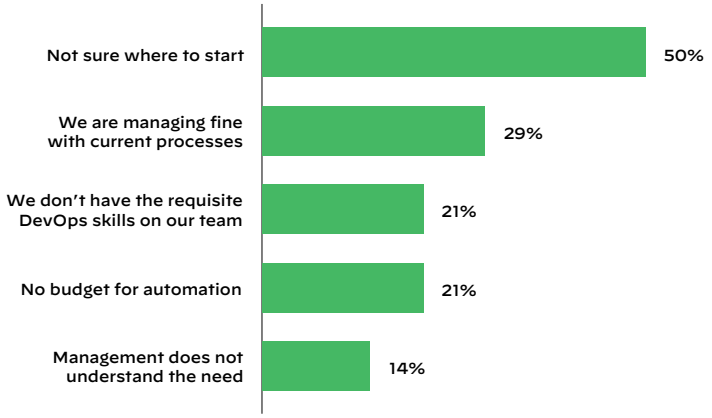

Figure 14: Responses to question "What are the reasons for not deploying automation in your security operations?" (Multiple answers allowed)

Further Insights

Respondents were asked to share any further comments they thought were relevant to the issue of security automation. One theme that emerged from their responses was the potential for artificial intelligence (AI) in making automation work better. For example, one respondent wanted "anything with a level of AI that can help me automate some of these processes." A second held that "Machine learning in the east to west traffic needs to be addressed by more vendors. I find this kind of information very valuable when diagnosing issues in our incidents. Just poring over firewall logs is not helpful. Our current solutions that leverage machine learning are some of the best solutions we have."

A third said, "We have been looking into utilizing AI for a lot of security functions that were once only performed by our CSOC." On a related front, a respondent expressed that every security automation product should include software that contains advanced analytics, such as machine learning and deep learning, with the goal of detecting anomalies.

Linking security automation with software development was another area of interest that came up in the free-form question. A respondent suggested integrating application vulnerability resolution into active development/deployment in the application security realm. To him, "Certain findings have to be resolved (remediation/mitigation) in order to proceed with actual deployment into a QA/Production environment." He felt it would be smart to make it a requirement in order to proceed further—to force developers to resolve existing flaws in a timely manner.

Change control was on the mind of another respondent, who felt that security automation often does not "play nicely" with change control in enterprise organizations. He recommended well-vetted playbooks tied to pre-approved changes as the answer. As he saw it, "Change processes are often slow, with weekly change cycles. Automation does not hold itself to such timelines. For the sake of tracking changes and troubleshooting if automated response goes awry, connecting to a ticketing system is a key integration for success and adoption."

Conclusion: Takeaways and Recommendations

This survey points to a transition unfolding in security organizations. Despite serious pressures, teams remain small, and processes are largely in-house and not fully automated. This is a precarious situation, one that will not likely be sustainable in the near future. Automation is essential if organizations want to keep up with threats, and especially if they want to continue to operate lean and in-house. However, despite a desire to automate, enough obstacles lay in the path that it's affecting progress toward the goal.

What should be done about this? It does not appear that money or executive buy-in are the most serious issues. A lack of skills is a factor for sure, so investing in recruiting and training would seem to be a wise move. Organizations may also want to look at opportunities to acquire solutions that reduce the complexity of automation, such as tools that offer prebuilt incident response playbooks. It is possible to achieve a higher level of automation, which will likely become a non-negotiable requirement to secure business operations. The challenge will be to embrace change and commit to making it happen.

Appendix: Survey Demographics

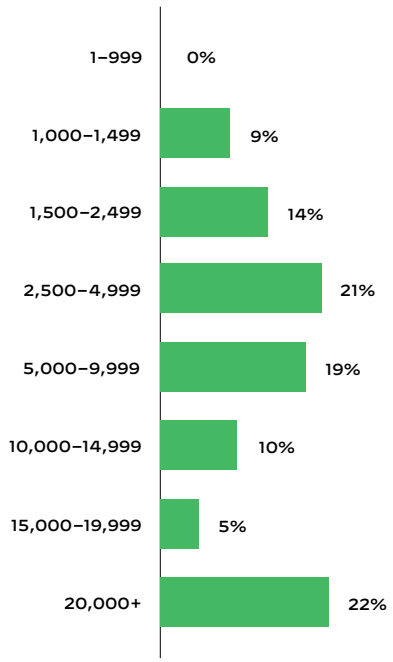

Figure 15: Responses to question "How many employees does your company have?"

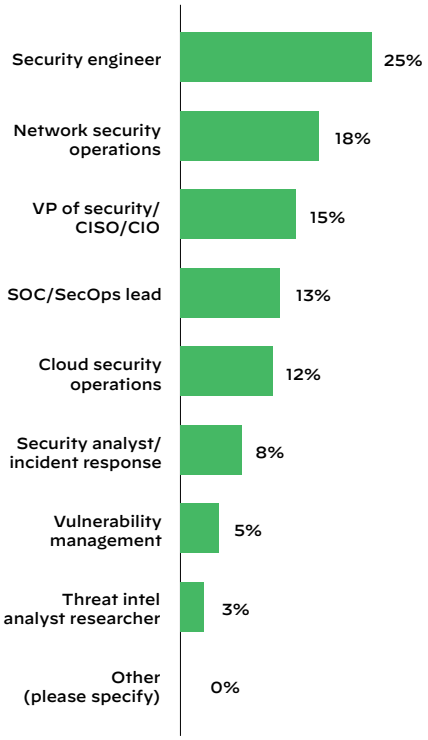

Figure 16: Responses to question "What is your primary role?"

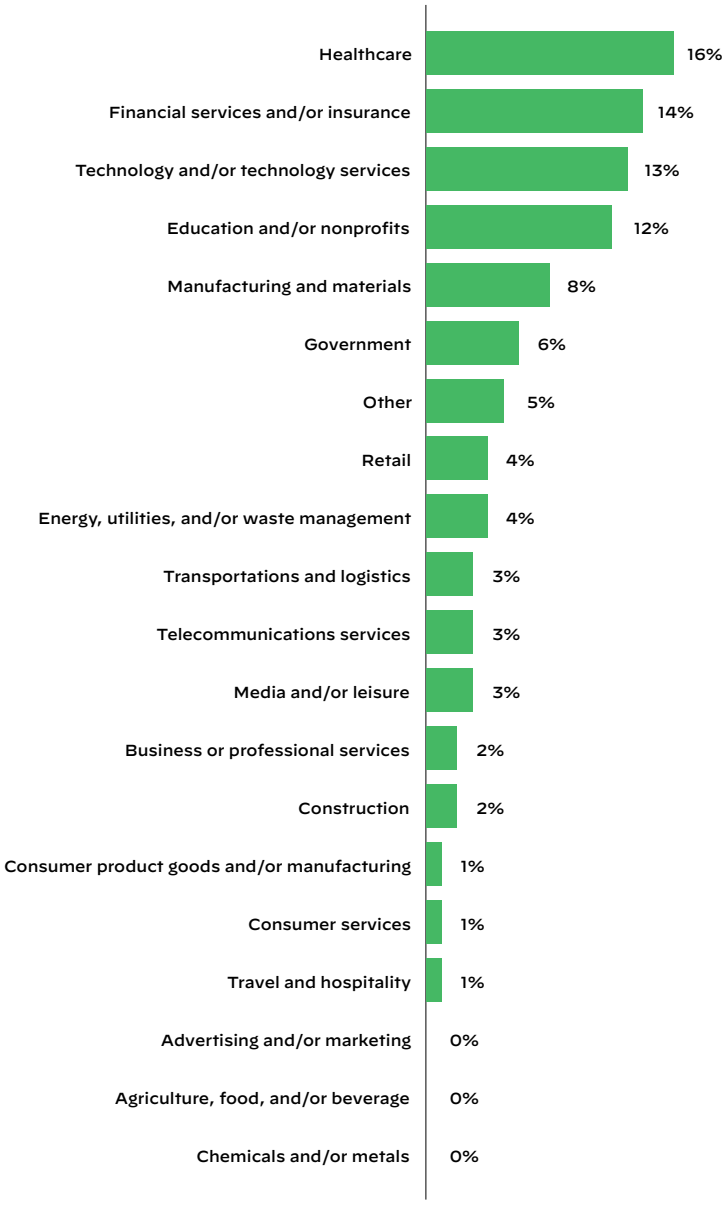

Figure 17: Responses to question "What is your organization's primary industry?"

This vendor-neutral research was independently conducted by Virtual Intelligence Briefing (ViB). ViB is an interactive online community comprised of over 2M IT practitioners and decision-makers who share their opinions by engaging in sophisticated surveys across IT domains, including Information Security.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com