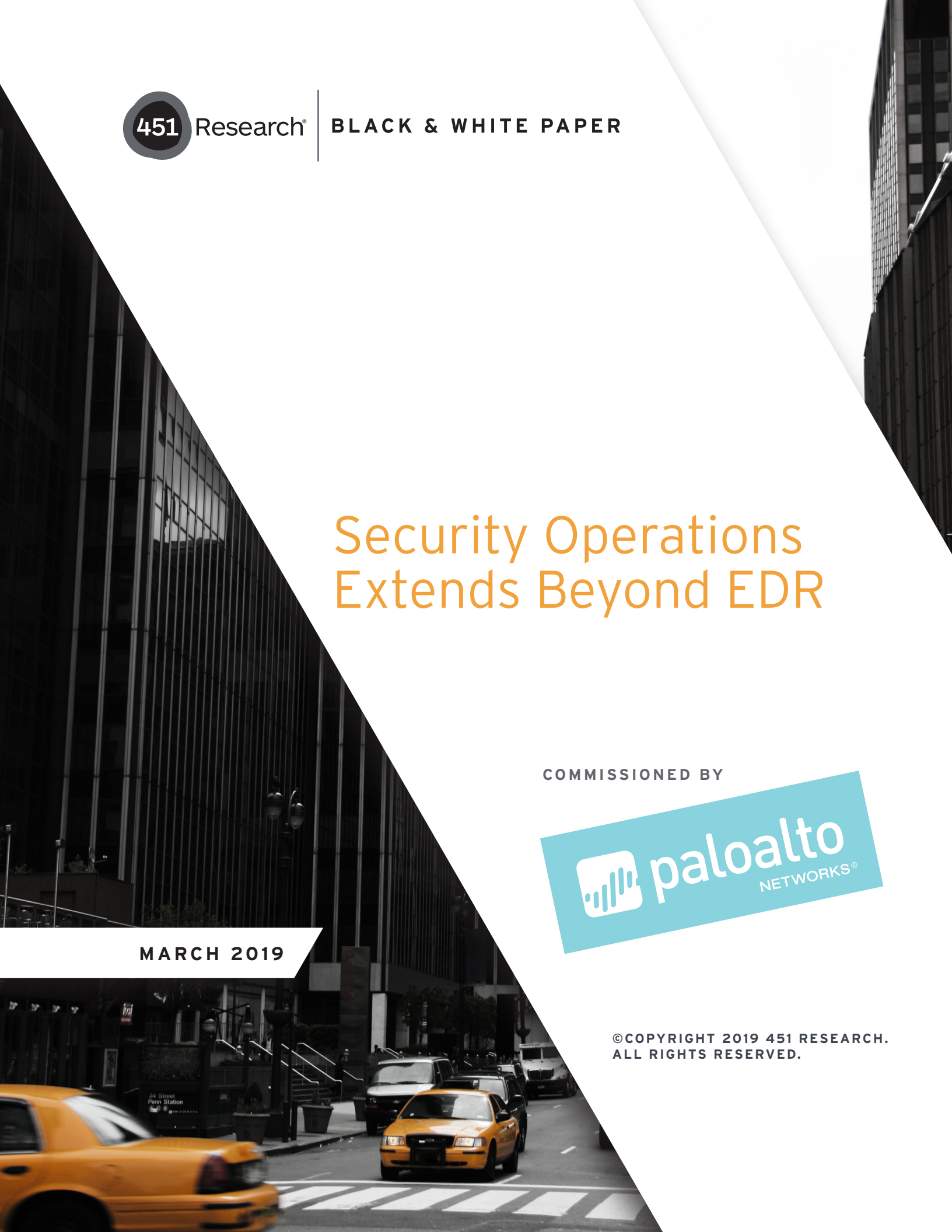
451 Research | BLACK & WHITE PAPER



Security Operations Extends Beyond EDR

COMMISSIONED BY

paloalto NETWORKS®

MARCH 2019

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners – what they are doing, and why they are doing it.

ABOUT THE AUTHOR

FERNANDO MONTENEGRO

SENIOR ANALYST, INFORMATION SECURITY

Fernando is a Senior Analyst on the Information Security team, based in Toronto. He has broad experience in security architecture, particularly network security for enterprise environments. He currently focuses on covering vendors and industry events in the endpoint security and cloud security spaces.

Executive Summary

Because security teams are being asked to do more with less as they face increasingly complex scenarios and tight timelines, many security leaders are evaluating their practices. As a result, many of them have adopted endpoint detection and response (EDR) tooling and process options to help them investigate and respond to incidents more effectively. While EDR does add valuable security capabilities, especially for organizations with no other in-depth form of visibility, there are broader questions: Are there other opportunities for improvement? What else is being used besides EDR? How do organizations plan their security operations for increased effectiveness?

As part of a custom research effort commissioned by Palo Alto Networks, we surveyed respondents with experience in deploying EDR from a variety of midsized and larger organizations in North America, Europe and Asia. Results indicate that most organizations have security operations centers (SOCs) or security teams, although only a portion of those SOCs have around-the-clock coverage. Most organizations practice tiered triage, where tier 1 analysts interpret alerts then pass them on to investigators at tier 2. Many organizations also employ, and derive value from, specialized threat-hunting (tier 3) teams. Both tier 2 and tier 3 teams use a variety of data sources when investigating incidents or hunting for undetected threats. These include endpoint data, network data, additional open source intelligence and cloud-based data, as well as collaborative efforts across industry and government.

The survey data indicates that there are many opportunities for improving security operations, both within each tier and across tiers. These opportunities include addressing the significant amount of manual work required in triage and the number of alerts that are escalated to tier 2 unnecessarily. Organizations looking to improve security operations and security readiness within modern environments should consider opportunities – in terms of both organization and technology – to extend detection and response practices by consolidating data sources and improving automation and communication.

Introduction

In practical terms, all security teams need to address adversaries with a wide range of capabilities and objectives despite the unforgiving reality of economics: there are not enough resources to do everything. There is tremendous pressure from the organization to respond faster to business needs while maintaining the appropriate security posture. The shifts in technology also affect this dynamic: existing mindsets about how security should be handled no longer necessarily apply, and processes should be reviewed.

The importance of proper endpoint security has increased in the modern environment. With mobile devices accessing a variety of cloud and on-premises resources, the endpoint has become a key asset for both defenders – in many cases, it is tightly tied to a specific user – and attackers – who can use the endpoint as a launch point for more sophisticated attacks.

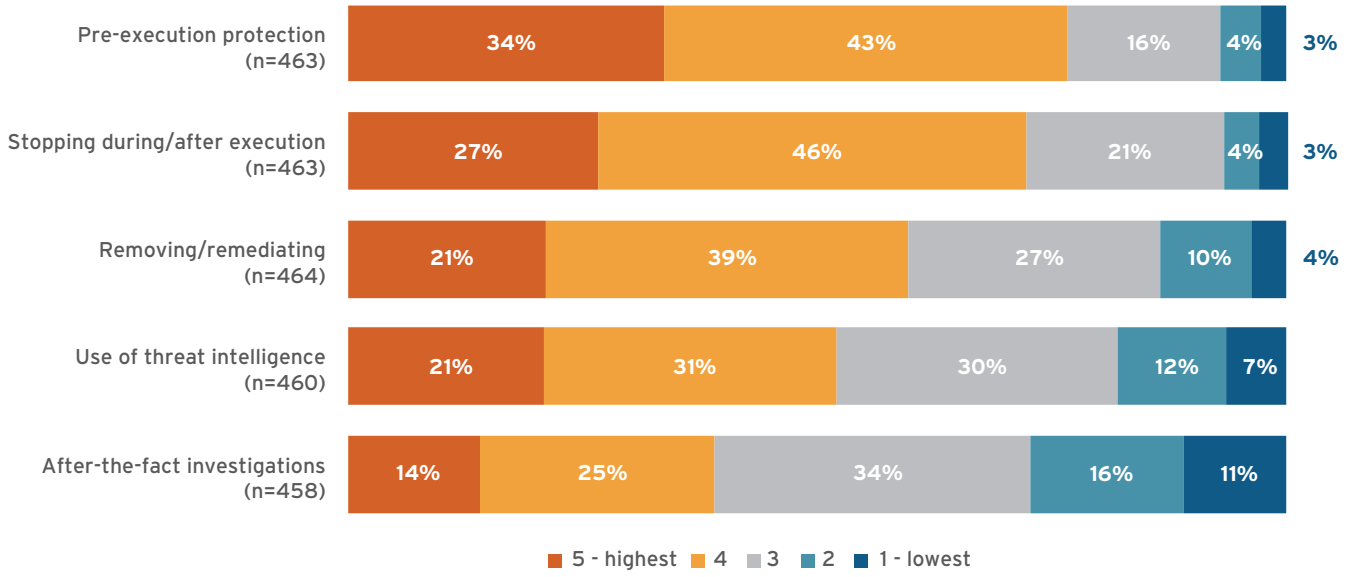
As the endpoint gains importance, and improved protection features help organizations fend off many attacks, attention turns to how to handle the remaining workload: the incidents that occur because of failed endpoint protection. The industry has broadly adopted the term 'endpoint detection and response,' referring to products that provide detection of malicious activity, investigative features, and response options against those threats. EDR was originally designed for larger organizations with the idea that they have the personnel and infrastructure in place to support its use.

Recently, 451 Research asked a broad set of security professionals across several industries about their perception of the value of endpoint security, including both protection and 'EDR' components (See Figure 1).

Figure 1: Satisfaction rating for endpoint solutions against use cases

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

Q: On a scale of 1 to 5, where 1 is 'very ineffective' and 5 is 'very effective', how would you rate your current endpoint security solution against the following use cases?



As the data shows, participants' satisfaction varies significantly by use case. The level of satisfaction with pre-execution protection is notably higher than for additional phases of the incident lifecycle. Notably, there is much more dissatisfaction with support for investigations. These responses point to an interesting relationship between use cases: unless protection capabilities deliver good results, the experience with EDR tools may be particularly stressful for teams as they handle a high number of alerts without a strong ability to investigate. Against this backdrop of how organizations feel about endpoint security, security leaders are asking themselves where else can improve their practices. Our research followed this general theme.

Methodology and Demographics

The data for the remainder of this report comes from a survey commissioned by Palo Alto Networks that was fielded in Q4 2018. The data consists of 250 completed responses from individuals that self-reported to have met the following qualification criteria:

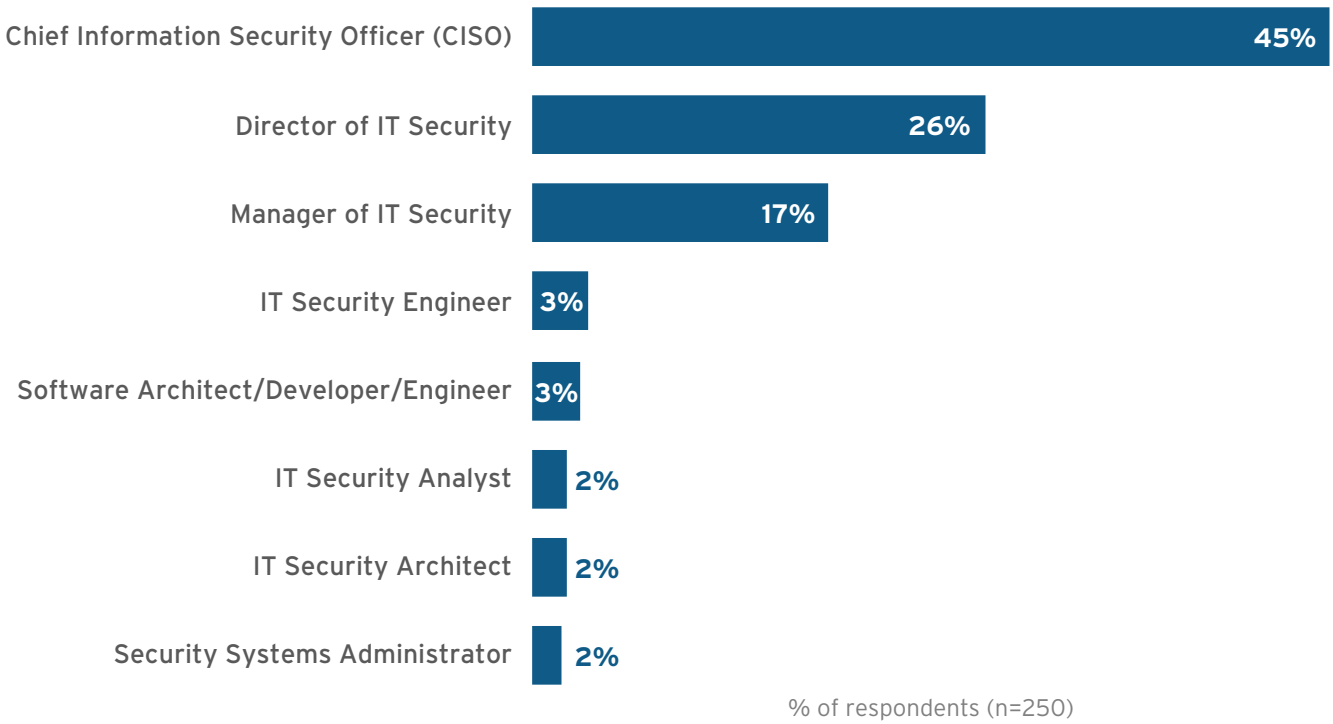
- Organization is located in the US, UK, Germany or Japan (with predefined maximum counts for each country).
- Organization is in one of several sectors: manufacturing, technology services, retail, financial services transportation, healthcare, utilities, telecommunications, entertainment/media and hospitality.
- Organization has at least 250 employees.
- Respondent is familiar with EDR practices and requirements.
- Organization is planning to deploy or is already using EDR technology or similar tooling.

Based on the criteria above, the sample of respondents breaks down as follows:

The self-reported title breakdown skews toward security management respondents.

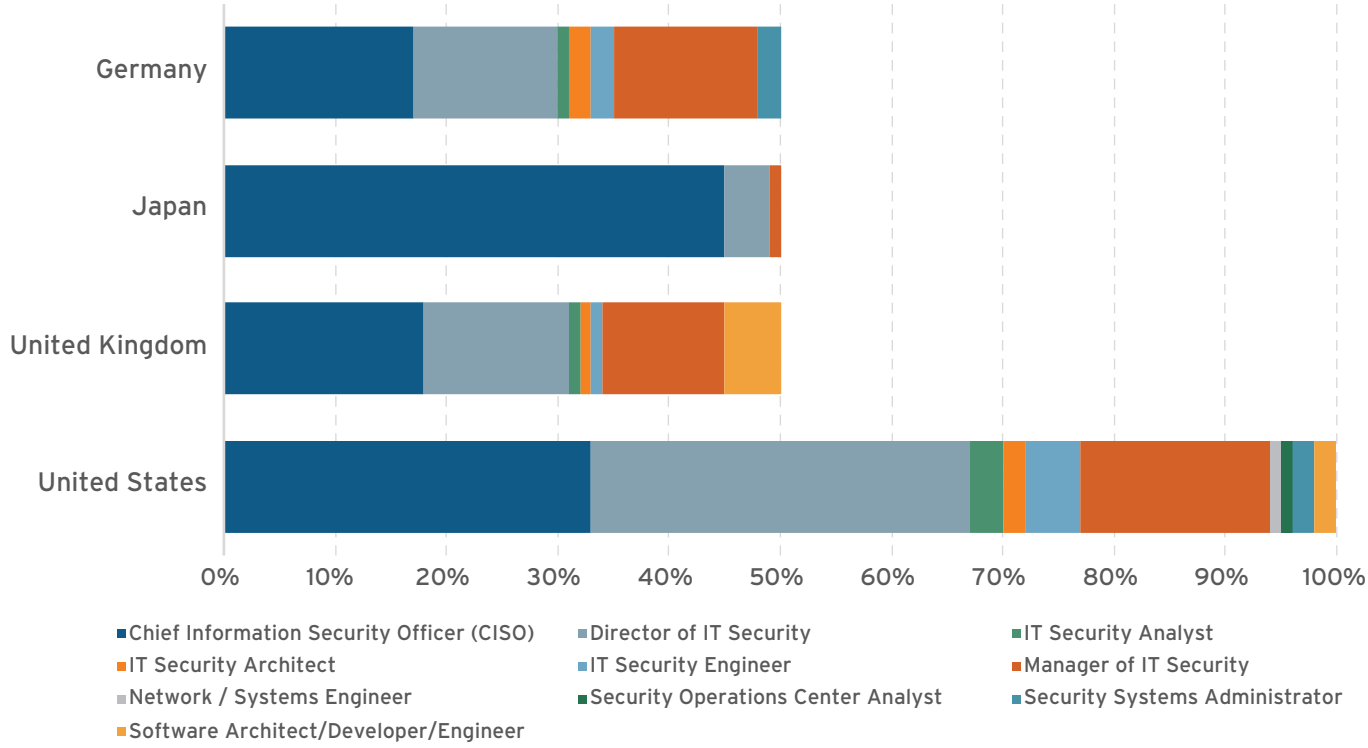
Figure 2: Respondent titles

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: Which of the following best describes your title?



Breaking this down by country of origin, there was a notable variance between respondent titles in Japan compared to the rest of the world.

Figure 3: Respondent titles by country

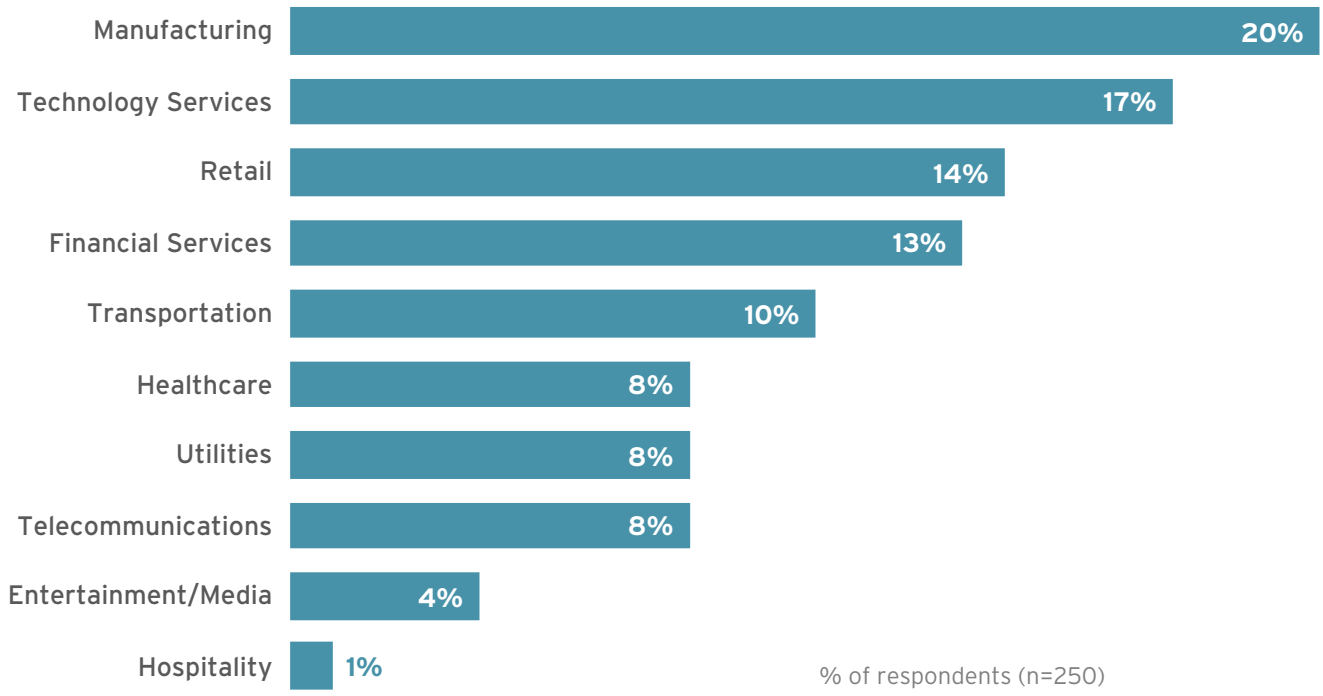


Still, regardless of country, many respondents indicated they have managerial roles with likely oversight over security operations. This indicates that the topic is of interest to security leadership teams, and they can contribute with insights that include tactical and strategic considerations for evolution.

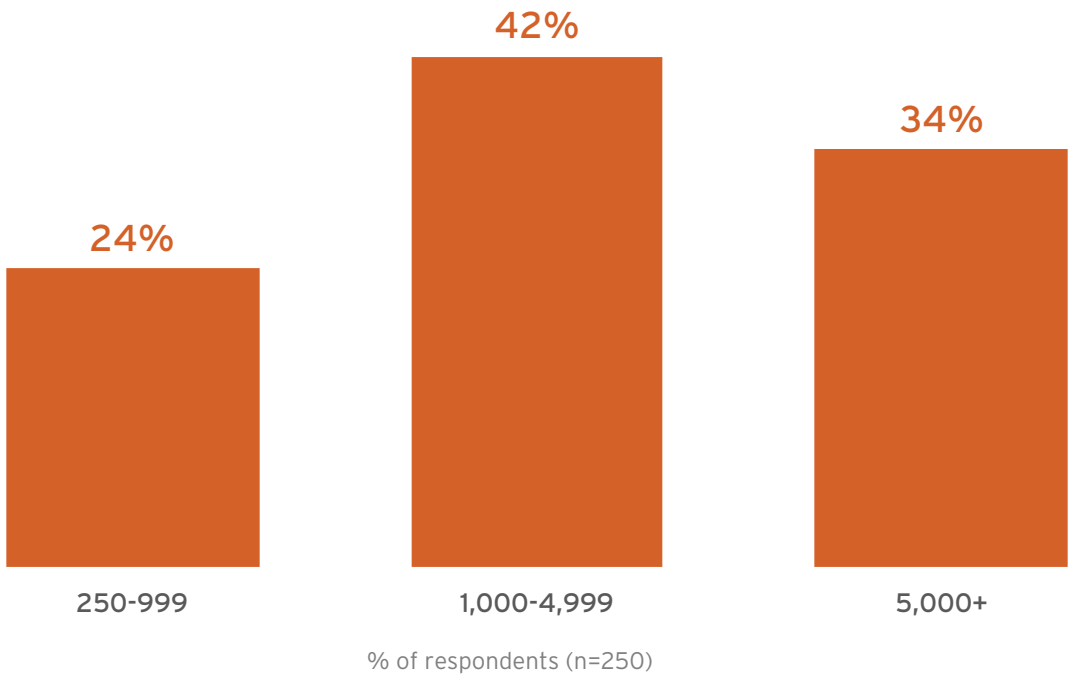
From an industry perspective and organization size, the reported breakdown of responses is shown below. The mixture of responses from different sectors is helpful to obtain a global view of practices, and the organizational size also captures a wide range of organizations.

Figure 4: Industry and organization size of respondents

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: Which of the following best describes your organization's industry?



Q: How many employees does your organization employ globally?

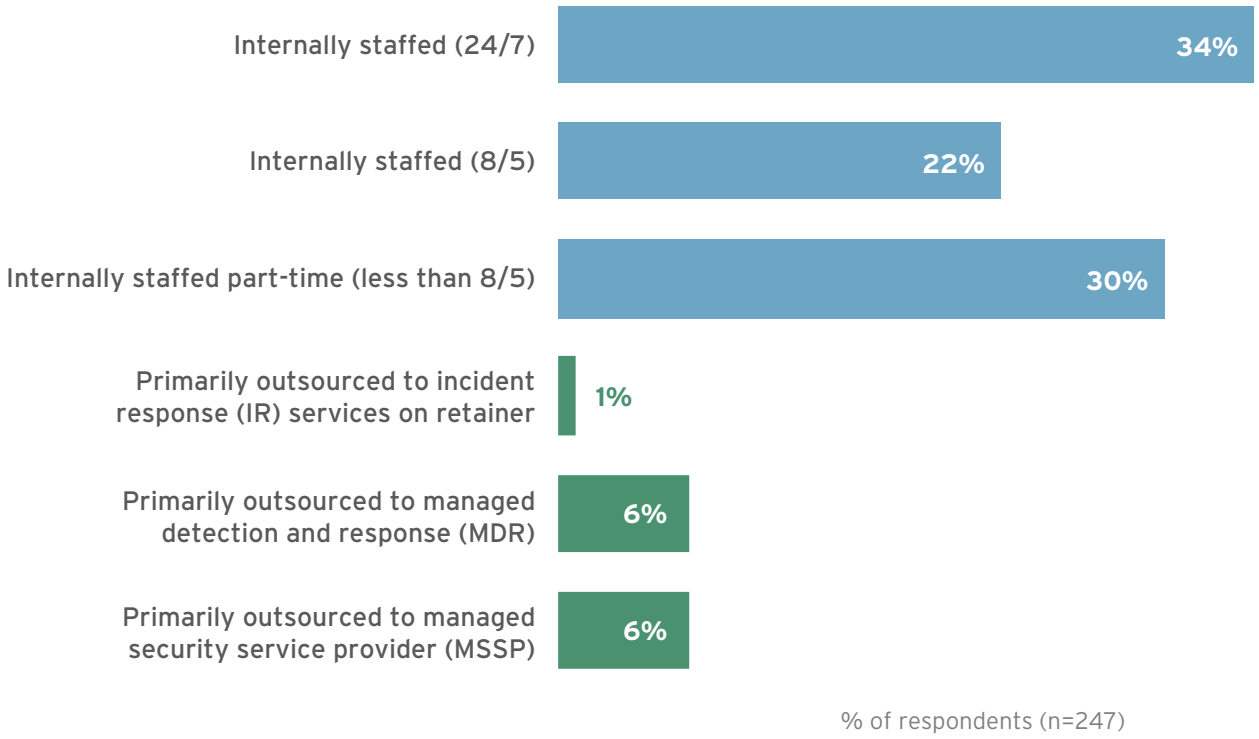


Enterprise SOC Coverage and Organization

Almost all of the respondents (99%) indicated that their organization has a security operations center, but drilling down further revealed that there are significant differences in how the SOCs operate. As the figure below shows, internally staffed SOCs represent 86% of the total, but only 34% of those SOCs are staffed on a 24/7 basis. Even if those SOCs outsourced to managed detection and response providers or MSSPs offer 24/7 coverage, more than half of organizations still likely do not have the capacity to provide human oversight when responding to fast-moving security events.

Figure 5: Security operations center staffing

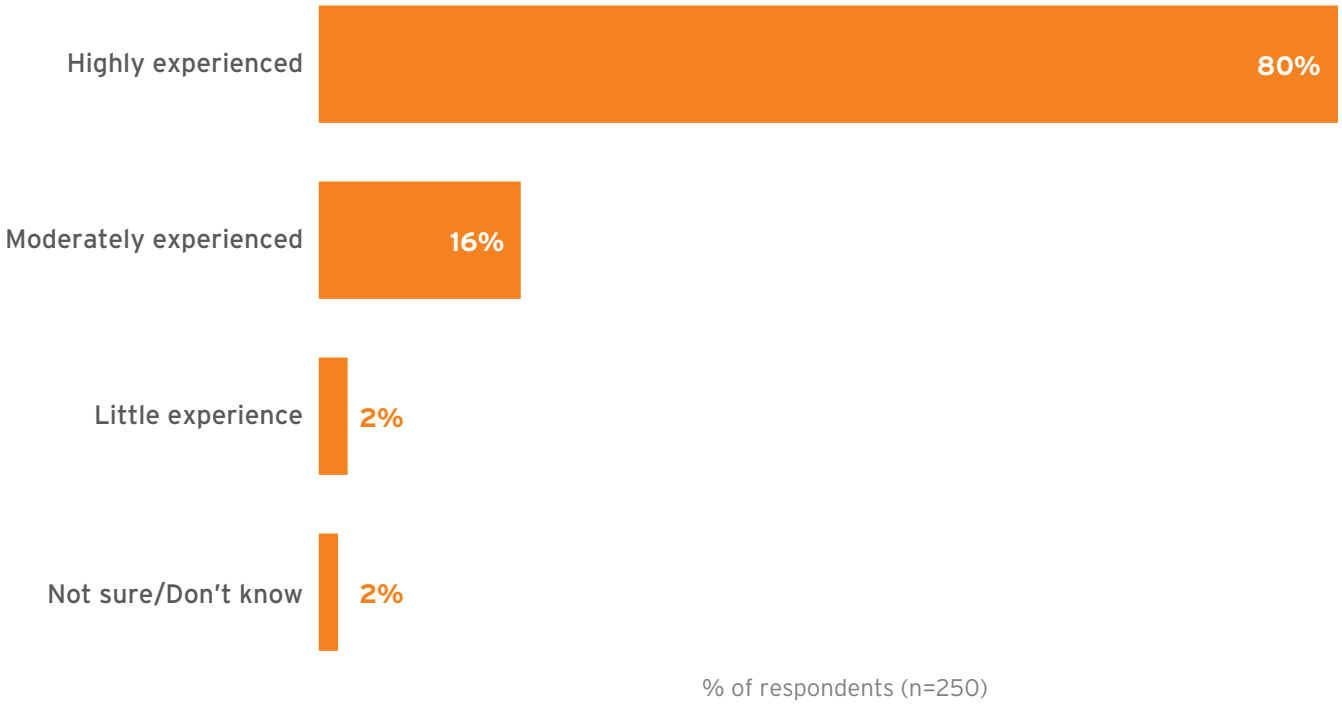
Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: Which best describes your security operations center (SOC) capabilities?



Most respondents indicated a high level of familiarity with EDR within their organizations. Even if accounting for human bias in responding positively about one's own organization, the data below seems to indicate that organizations should be able to, at least from their perspective, use EDR tools effectively. This leads to the question: Is that the case? Are security teams responding efficiently to incidents? This was a key point for this study.

Figure 6: Analyst EDR experience

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: How would you characterize the experience level of most analysts using endpoint detection and response tools in your organization?



The research considered a security operations model whereby various security activities fall under different teams or different analysts within smaller teams in a tiered fashion:

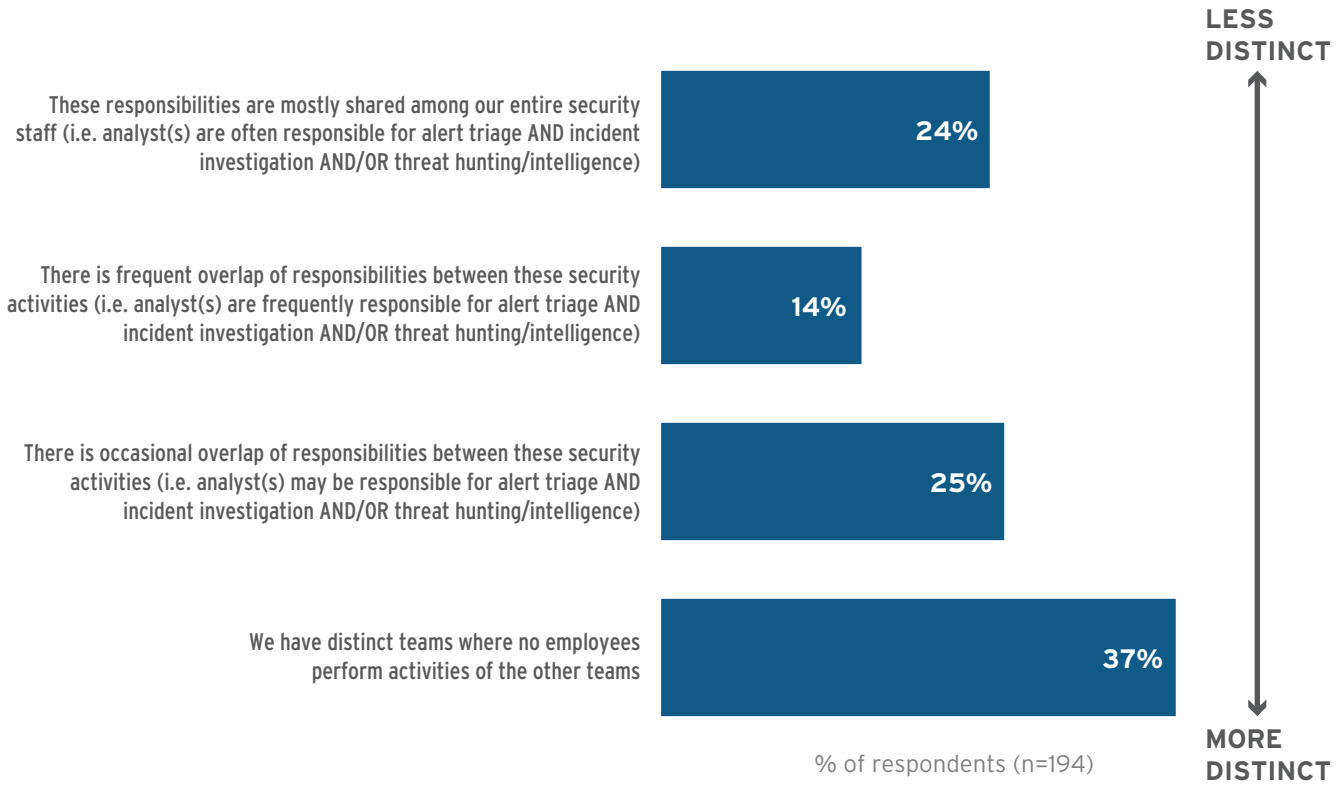
- Tier 1 activities typically consist of triaging incoming alerts and processing incidents that don't need to be escalated to tier 2 for further investigation.
- Tier 2 activities loosely relate to security investigations – as opposed to alert triage – often including more specialized tools and resources.
- Tier 3 activities consist of independent 'threat hunting' in one's own environment, and more specialized responses to security incidents.

Most respondents indicated that they perform all three types; 90% of organizations said they perform tier 1 and tier 2 activities, and 71% said they perform threat hunting. A significant number of respondents (52%) indicated that team activity is segregated, and there is limited or no contact between these teams.

Figure 7: IT security staff organization

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018

Q: How are these security activities distributed among your organization's security staff (Security Alert Triage, Incident Investigation, and Threat Hunting/Intelligence)?

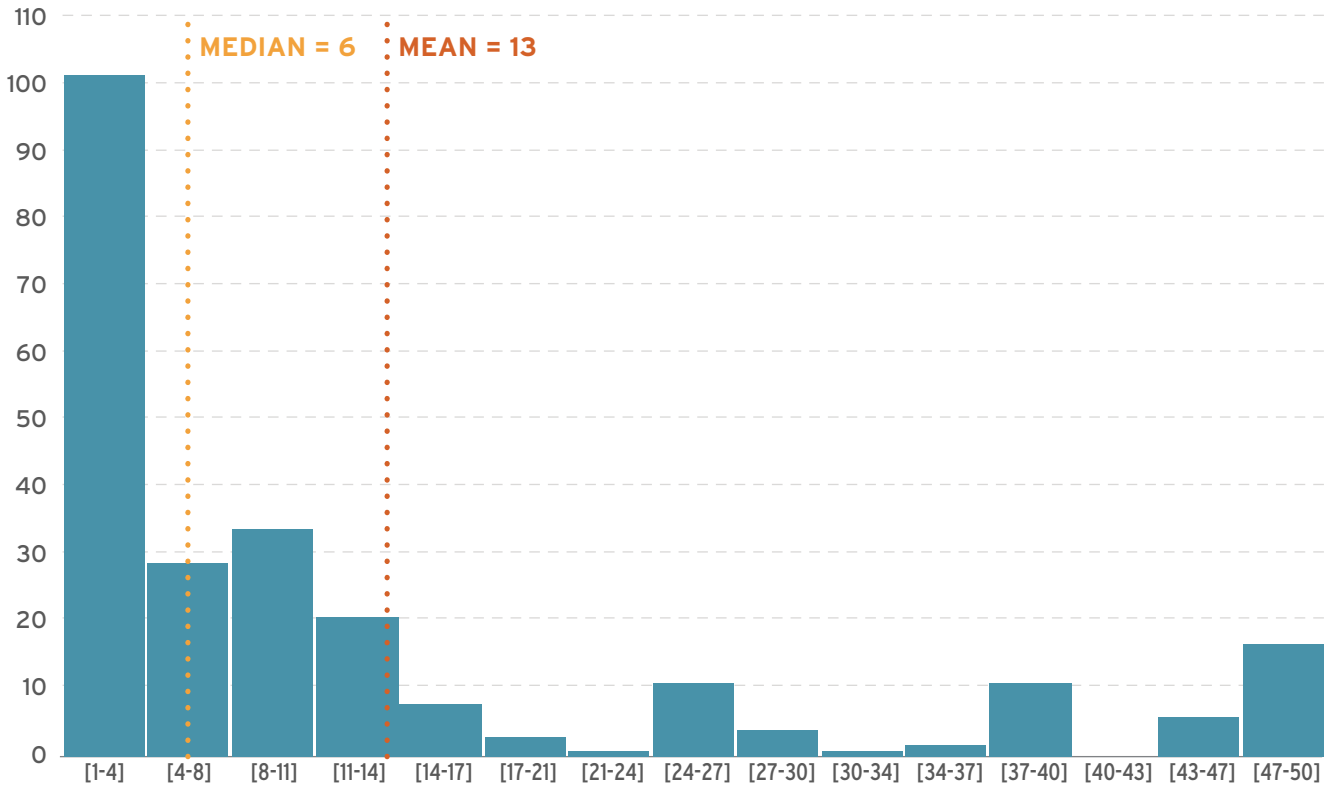


This insight is relevant because it possibly exposes the prevalence of more defined, formal hand-off processes between teams. This type of more explicit separation can aid in managing teams separately, but it may not be as efficient for sharing both tactical information about incidents, as well as collective organizational knowledge.

The complexity of security operations is also often cited as a key concern. According to Figure 8 below, the mean number of tools reportedly being used in SOCs is 13. Unless organizations ensure that their technology choices can integrate effectively and efficiently across operations, they risk creating significant friction and overwork for their teams.

Figure 8: Number of tools used in SOC

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: How many vendors do you use in your security technology stack?



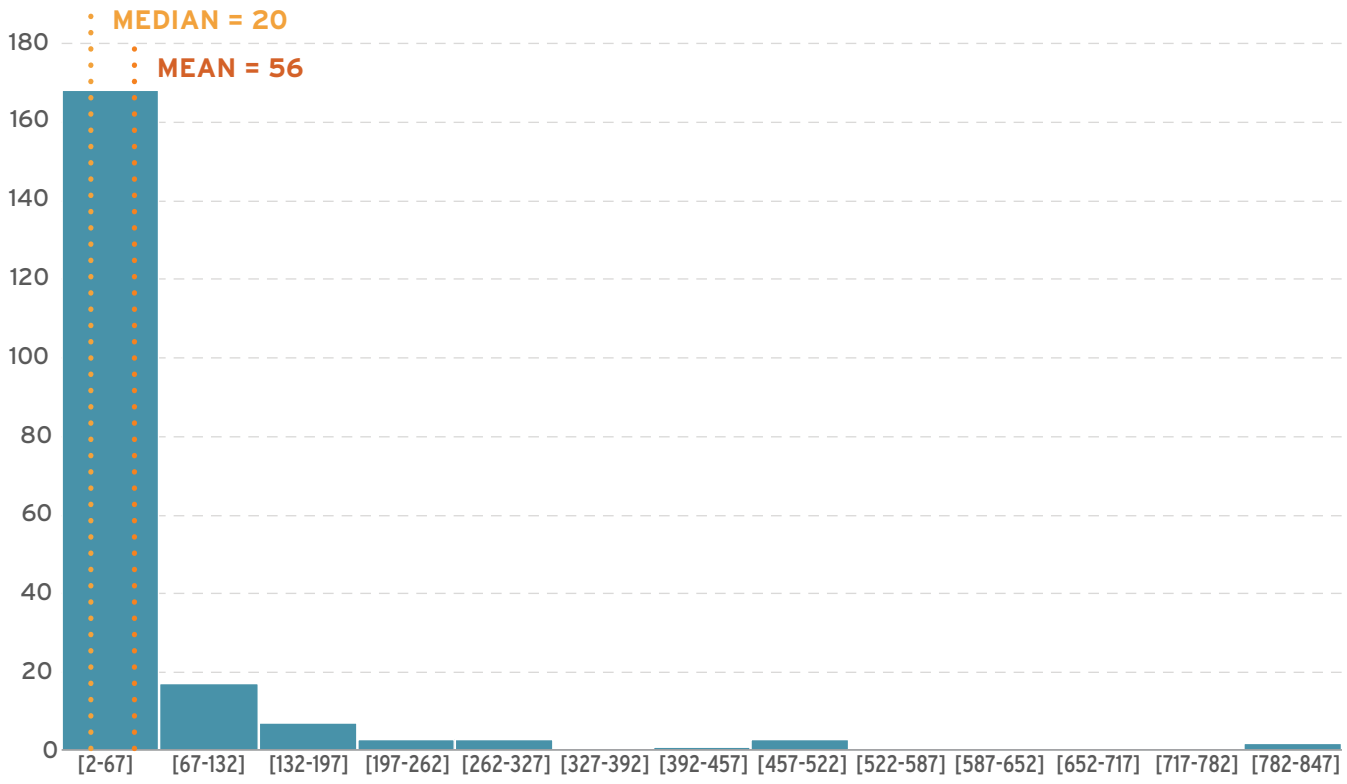
Tier 1 Security Practices

One of the main objectives for tier 1 teams is to process incoming alerts as efficiently as possible. Efficiency gains in addressing alerts at this level – without further escalation – mean that more specialized resources at tiers 2 and 3 can be better utilized.

The makeup of a 'triage team' within organizations varies significantly. Figure 9 below – which was already filtered for statistical outliers in the response (those with a 'z score' of 2 or higher) – indicates that there is some variance in how team sizes are reported. Still, mean and median numbers indicate that many organizations dedicate significant resources to manning their triage teams. The number of alerts being handled by those triage teams appeared to vary along a similar distribution.

Figure 9: Team size for tier 1 activities

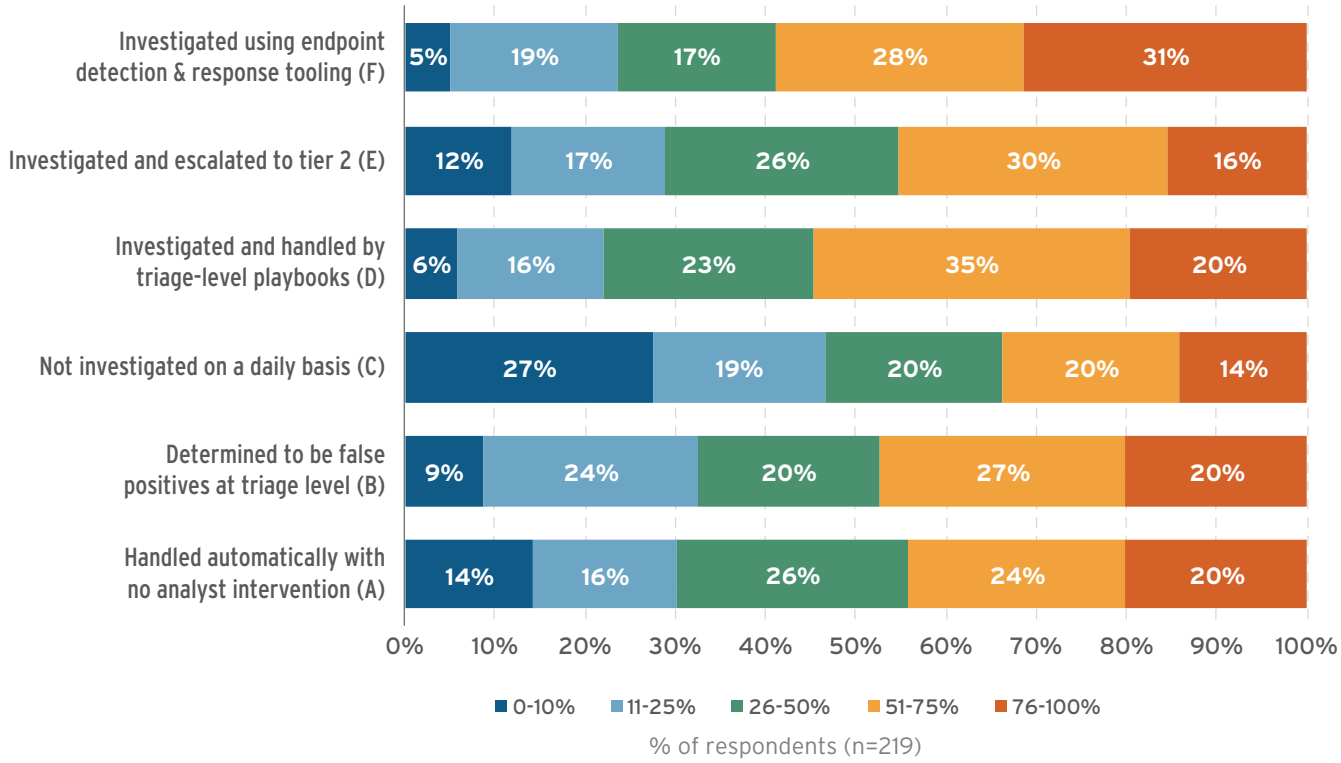
Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: How many full-time resources (employees) are in your Alert Triage Team?



Some of the more interesting data comes from asking organizations how tier 1 teams process incoming alerts. Respondents were asked about their estimates – in percentage terms – for how the alerts were handled at the tier. Figure 10 highlights both positive and negative aspects of tier 1 processes. On the positive side, it seems to agree with data about EDR experience since EDR is used in a non-trivial number of cases by many respondents (top row, labeled 'F'), but the satisfaction of the information for triage is still a concern (Figure 1).

Figure 10: Dissecting alerts

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: Thinking of all incoming alerts – what percentage are:



The figure also shows, however, several areas for potential improvement at tier 1:

- While over half of respondents said they use tier 1 triage playbooks to handle more than 50% of alerts (row D), a significant number do not, which means there is likely a significant amount of manual work within tier 1.
- Nearly half of respondents said that over 50% of alerts are determined to be false positives (row B). This creates significant work for the team and suggests the potential for improving alerting mechanisms and communication among tiers.
- Respondents indicated that automation only plays a part in triage (row A). This opens the discussion about whether limitations with current tools or practices can be overcome with newer approaches to automation.
- In addition to the manual work, the chart also shows that many alerts end up being escalated to tier 2 (row E). In a more optimized SOC, this should not be a frequent occurrence.

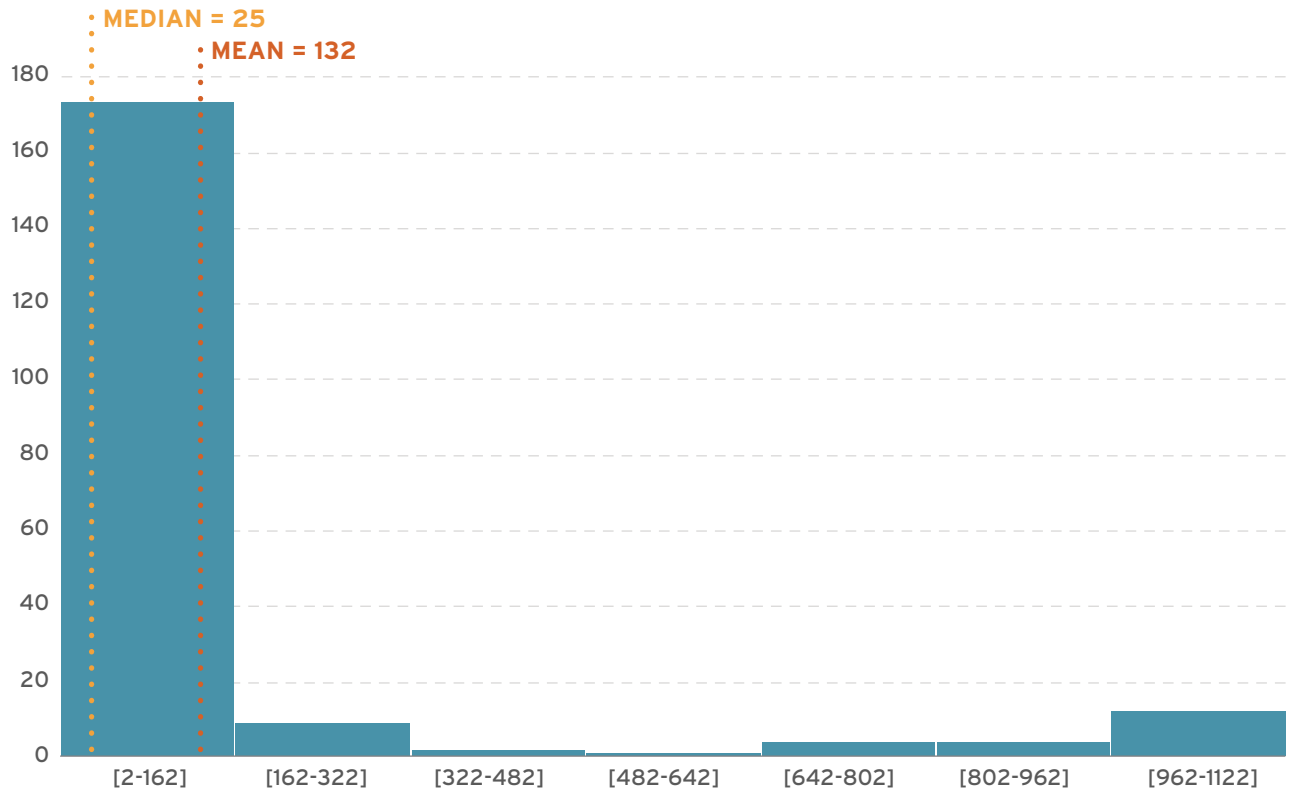
Tier 2 Security Practices

The main objective of tier 2 teams is to resolve the overall incident, either by further investigating and closing the incident or engaging in a broader incident response or crisis response process. To accomplish this, tier 2 resources are usually more specialized, and tier 2 teams may require additional time to handle each incoming request.

When looking at tier 2, we found a similar variance in team size and number of incoming alerts as tier 1. Outliers were filtered to simplify visualizations.

Figure 11: Team size for tier 2 activities

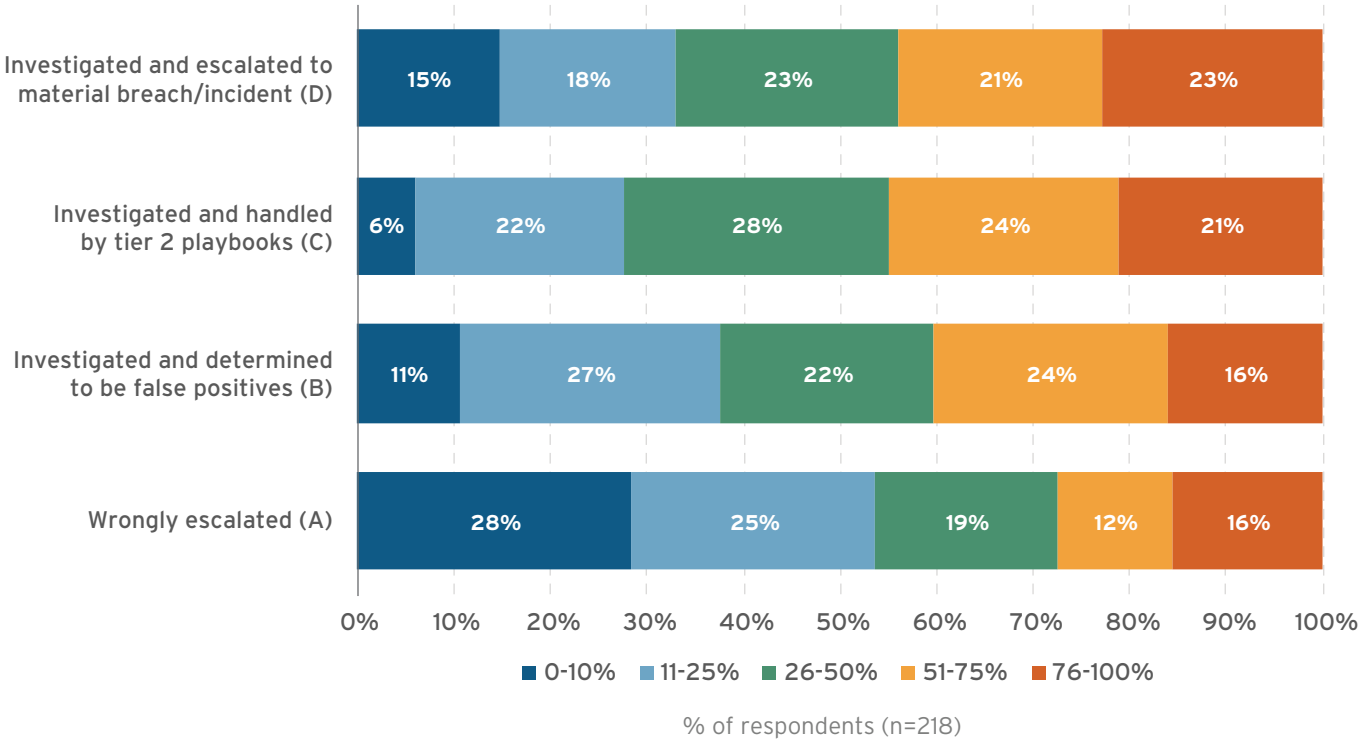
Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: How many full-time resources (employees) are in your Incident Investigation Team?



The data on how tier 2 teams handle the incoming workload is important because inefficiencies in this phase can result in a waste of expensive resources.

Figure 12: Tier 2 alerts

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: Thinking of all potential incidents (may contain multiple alerts) that are elevated to tier-2 – what percentage are:



When parsing out how tier 2 teams respond to inbound incidents, several trends emerge:

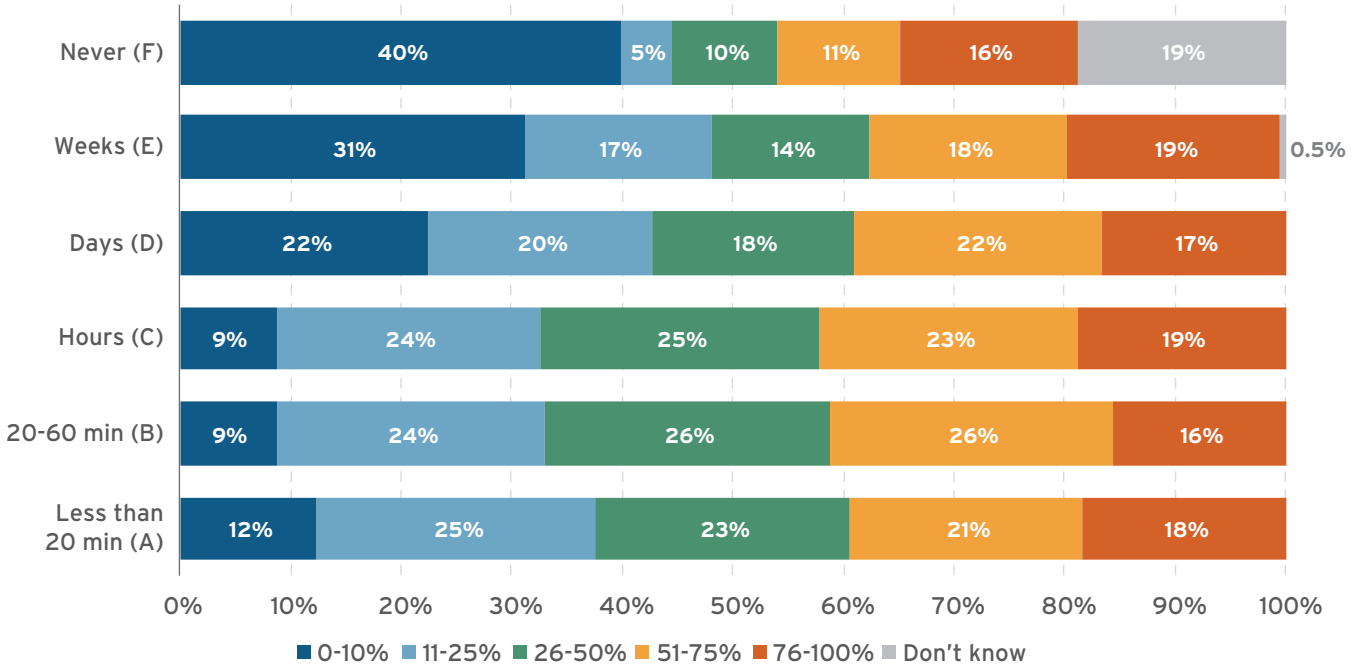
- A slight majority of respondents indicated that tier 2 playbooks capture half or less of all incidents escalated to tier 2 (row C).
- Nearly 40% of respondents indicated that half or more of all inbound requests were investigated and determined to be false positives (row B).
- Nearly half of respondents claimed that incidents that were wrongly escalated (and should likely have been dealt with at tier 1) represent 26% or more of all incoming incidents (row A). This is another indication of a breakdown in communication among tiers, leaving organizations with an additional area to consider improvements.

Taken together, these trends point to several opportunities for organizations to improve tier 2 workflows. These include better coverage for scenarios in playbooks, but more important, a ruthless review of how incidents are escalated. Here, there are various avenues for improvement, including better tuning of security-detection resources to reduce the number of alerts, and better enabling tier 1 resources to perform triage.

The impact of this inefficiency can be long-lasting. Unlike with tier 1, where time to respond to alerts is usually measured in minutes and hours, tier 2 investigations can span days, weeks or longer.

Figure 13: Time to complete security investigations

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: What percentage of investigations were completed within the following time periods:

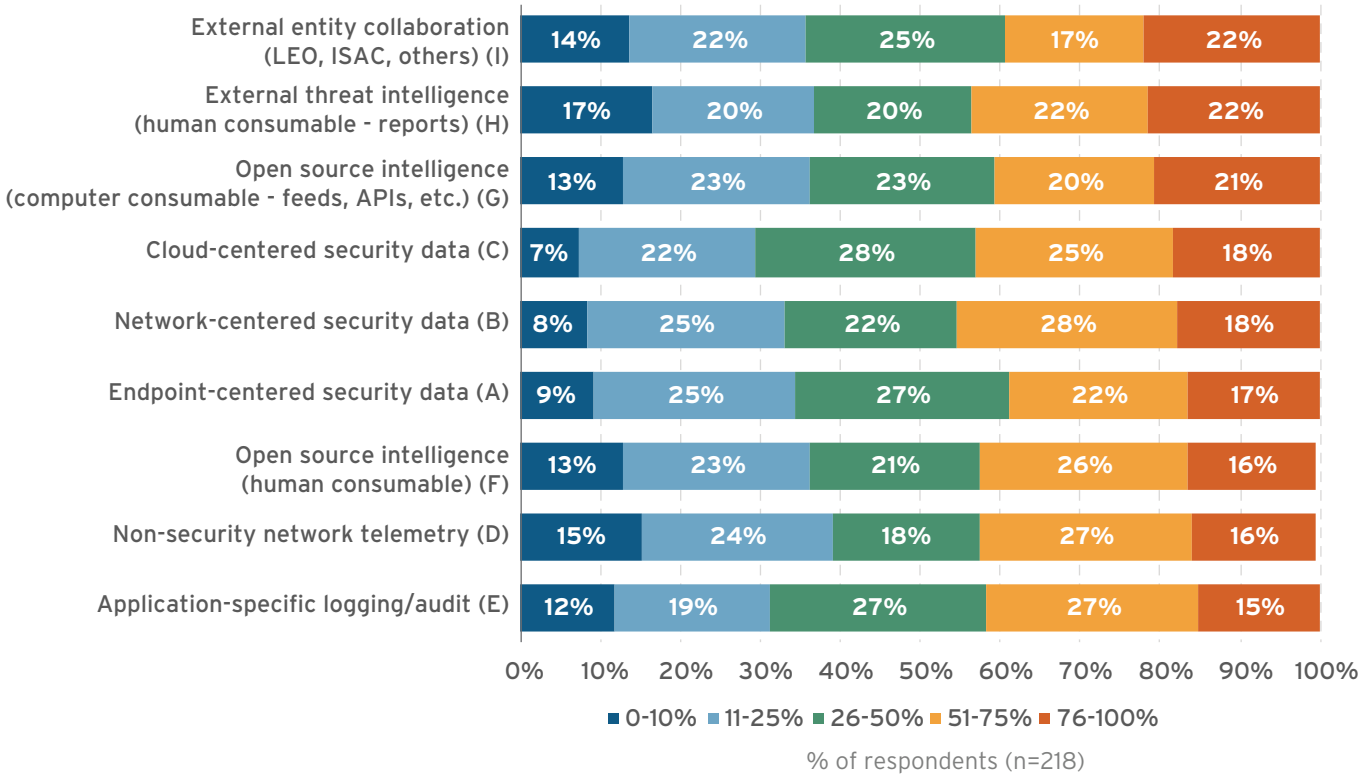


% of respondents (n=218)

In the model used in this study, one of the key differences between tier 1 and tier 2 workflows use a variety of data sources to conduct investigations. These sources include endpoint, network, cloud and application data from within the organization, as well as external sources, either collected manually or automatically.

Figure 14: Supplemental data for investigations

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: What percentage of investigations required the following types of supplemental data:



The responses did not vary significantly across different types of data. Approximately 40% of respondents reported the use of multiple data sources in half or more of the investigations conducted by their organizations. The broad adoption of multiple data sources highlights the need for efficient integration of multiple data sources into the investigation and response process.

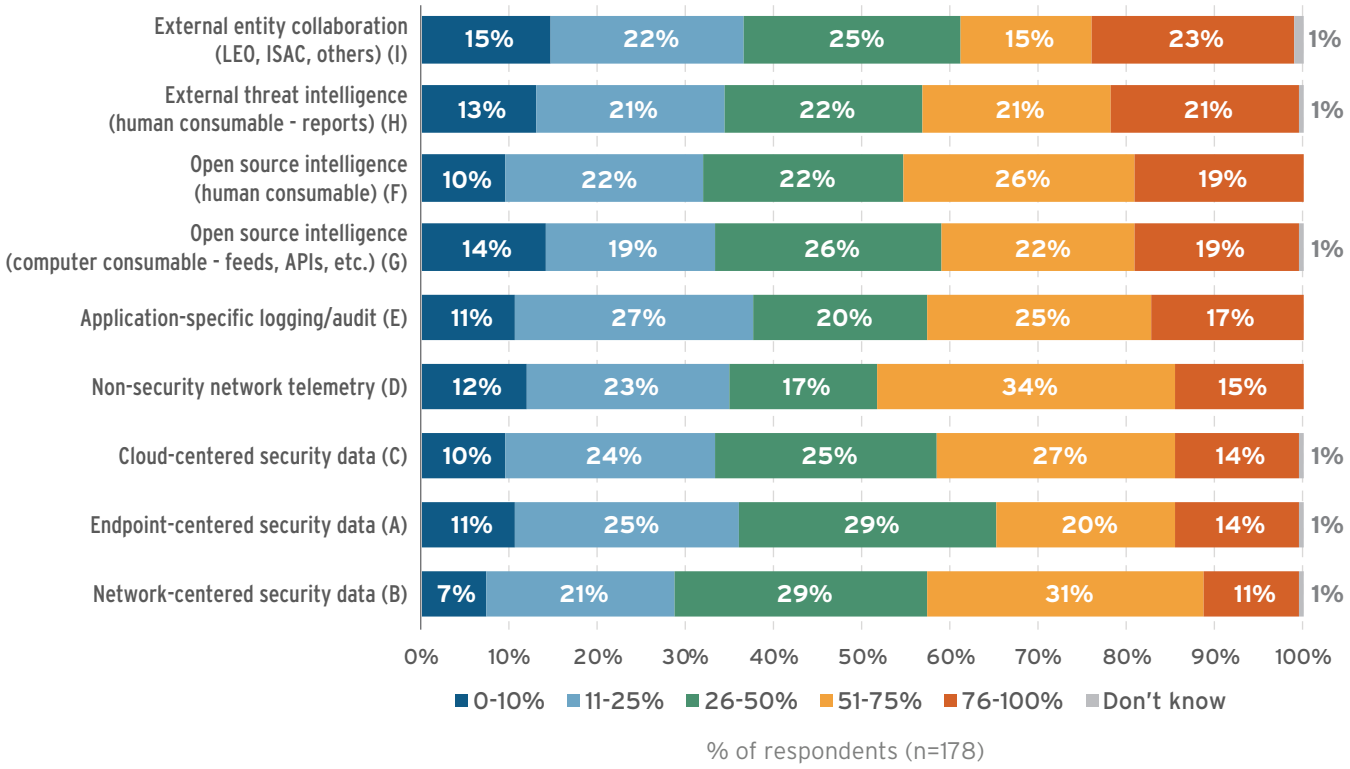
Tier 3 Security Practices

Under the model used in this research, Tier 3 teams perform independent threat hunting. This type of activity is independent of an existing incident and consists of searching for evidence of any yet-to-be-detected compromise of the organization's environment. Threat-hunting teams typically have deep expertise in security practices and modern attack techniques, as well as an understanding of the organization's environment.

Tier 3 teams also use various data sources as they perform their duties. There is broad usage of endpoint, network, application and cloud data, and interactions with different external entities, from threat intelligence providers to law enforcement agencies.

Figure 15: Supplemental data used in threat hunting

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: What percentage of hunting activities required the following types of supplemental data:

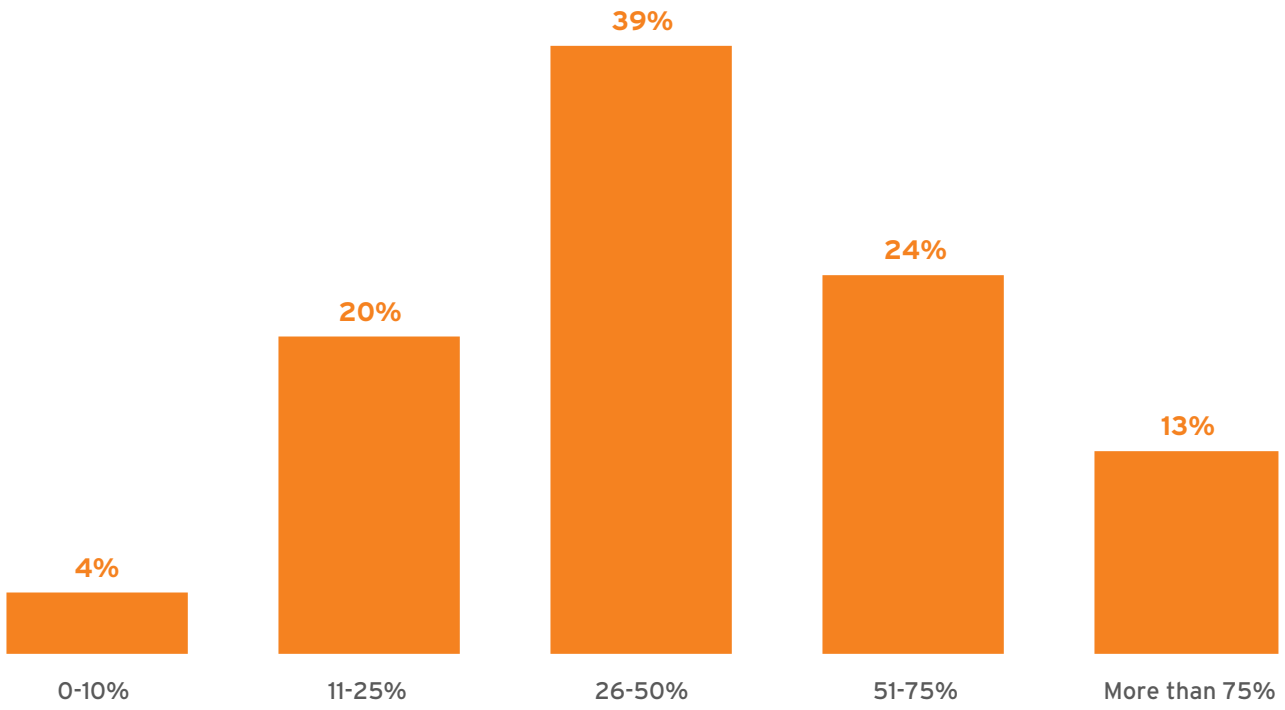


Threat hunting often involves processing information from a large number of hosts and can benefit greatly from automation. Indeed, according to survey results, use of automation is widespread. Most organizations (90%) indicated that they automate at least some aspects of threat hunting. With few exceptions – likely due to sample size – the proportion of respondents that indicated highly to mostly automated threat hunting appears consistent across industries, with a 50%/35% split between 'high' automation and 'mostly' automated.

In broad terms, threat hunting is supposed to be a complementary activity to existing security practices: the bulk of an organization's security operations should handle most incidents while threat hunting is aimed at rounding up the 'corner cases' in security incidents. But is that the case in practice? Figure 16 below illustrates that according to respondents, a surprisingly high number of investigations are opened not because of an incident, but because of a 'hunting' exercise.

Figure 16: Result of threat hunting

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: What percentage of investigations are initiated as a result of 'hunting'?



% of respondents (n=178)

The survey also found a similar distribution when considering threats found via existing processes or via hunting. This is potentially a damning indictment of existing processes and highlights the need for a broad rethinking of security operations. If tools and processes were working properly, we would expect the distribution to be much more positively skewed – that more respondents would indicate that threat hunting doesn't contribute as much to opening new investigations. Instead, many respondents indicated that half or more of their threat discovery is comes from hunting.

This finding also points back to the importance of deploying adequate endpoint protection in addition to any detection and response: if the detection and response tools aren't picking up on these incidents, organizations may be left exposed until the tier 3 team has time to find the issue.

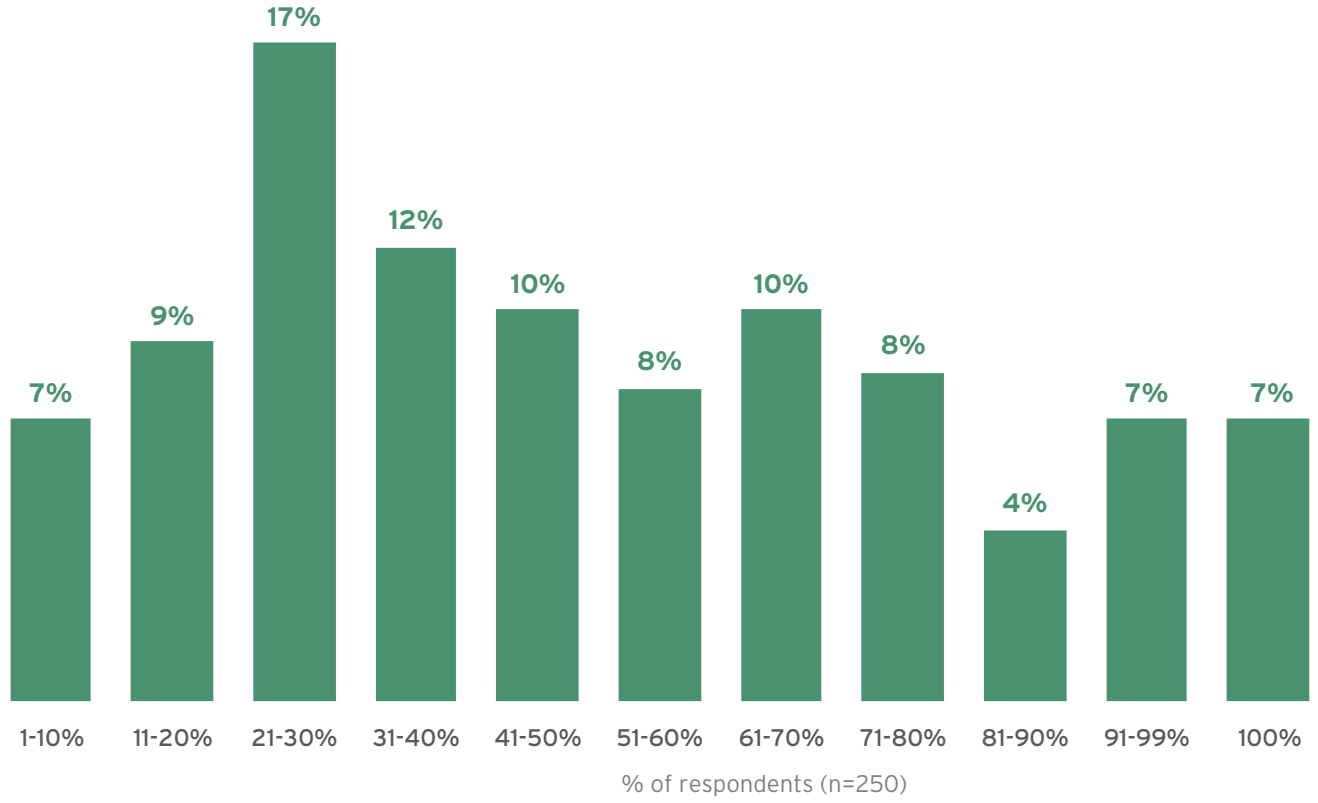
Measuring Outcomes

This study also examined how security management looks at the results from the teams' activity, both from tactical and strategic perspectives. The data shows that as security operations evolve, some challenges remain. References to 'security policies' within organizations can include both high-level directives and more tactical controls such as blocking specific elements. While high-level policies don't change often, more tactical elements do.

One of the topics that the study investigated is how often policies change in relation to alerts. This is interesting because the 'cost' of changing policies – even if there's no direct monetary cost – can potentially place a burden on already overworked teams. Roughly half of respondents indicated that 50% or more of alerts result in updated policies.

Figure 17: Alerts leading to updated policies

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: Please estimate the percentage of all alerts that have resulted in an updated policy, in an attempt to improve future triage practices?



This data is further evidence that organizations potentially spend significant resources updating security policies – more 'tactical' in nature. This is another area where the combination of better endpoint protection, more powerful alerts (through extension of data sources such as network and cloud data), and more seamless automation could help.

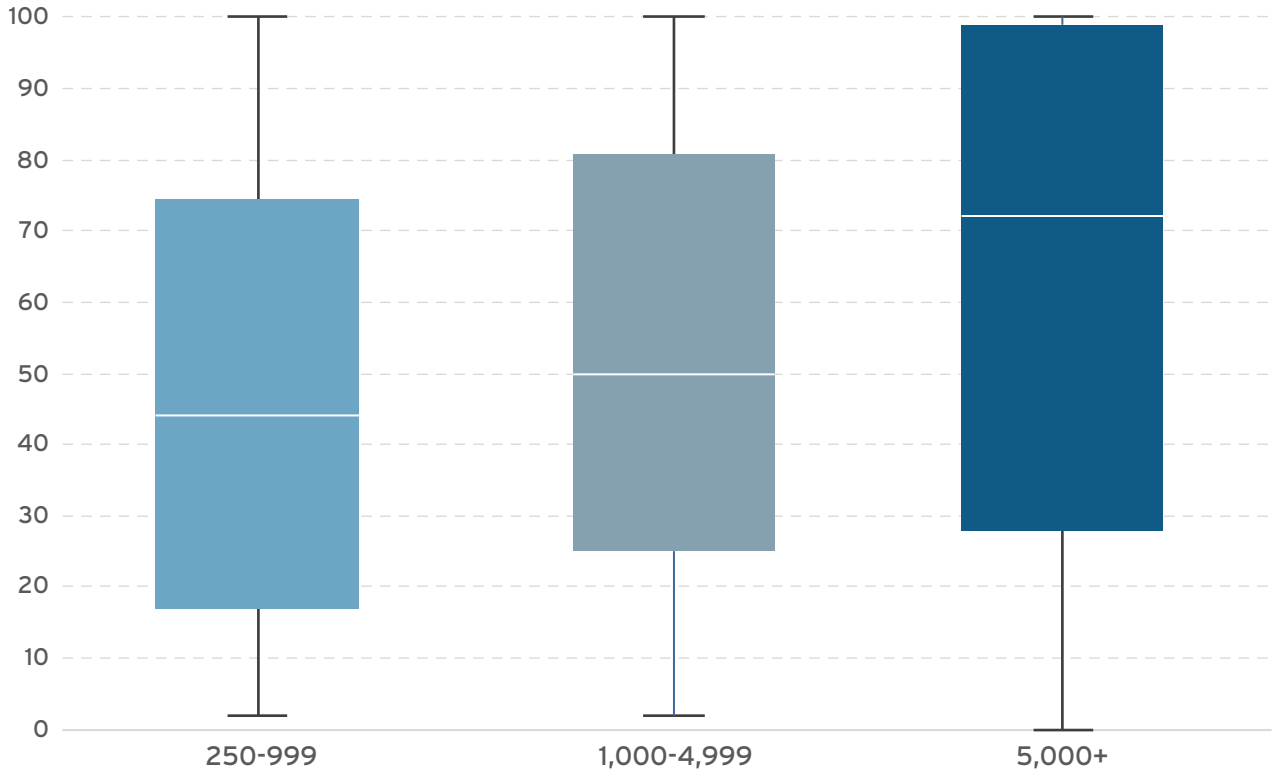
How Are Security Incidents Handled?

Tracking specific responses to a security incident is difficult because they may depend on numerous factors that are specific to the company, the industry, the type of data, etc. They may also involve a series of steps, including containing the damage, performing root cause analysis, and updating security infrastructure and playbooks. In many cases, however, it seems the only security outcome is to reimage the affected device. This may be less than optimal because while it 'resolves' the original incident, it can leave the organization exposed to future incidents.

According to the data from the survey, about 50% of respondents indicated that reimaging is the only remediation step. However, there was a notable difference between smaller and larger organizations, which could be explained by a reliance on additional infrastructure services (reimage and restore from backup), but could also mean there is too much focus on simple remediation with no opportunity for deeper analysis.

Figure 18: Wiping as only response percentage

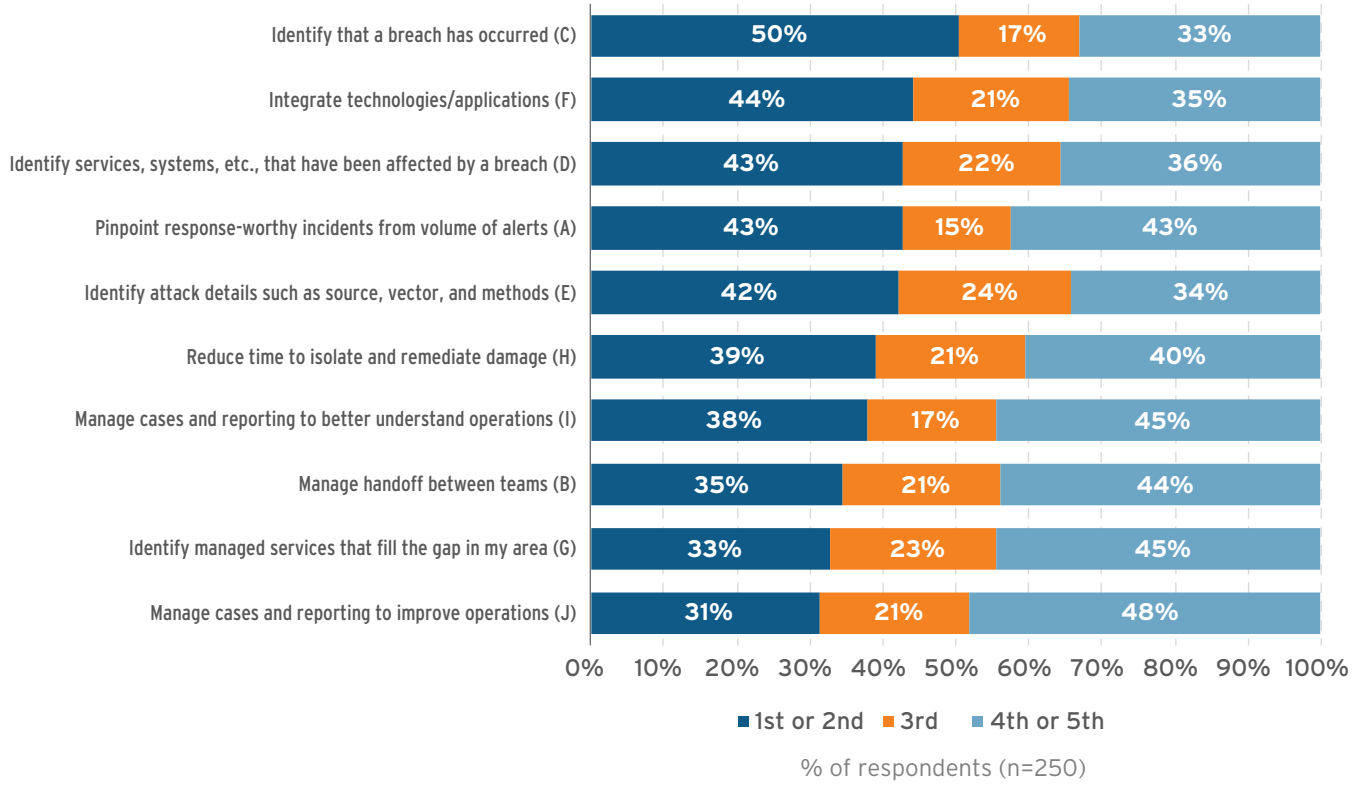
Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: How many employees does your organization employ globally?
Q: How often is wiping/reimaging the endpoint the only remediation step?



Finally, the collective responses regarding top improvements indicates a strong tendency toward getting a deeper level of understanding of environments and attacks, as well as the need for better integration of security tooling.

Figure 19: Eliminating bottlenecks

Source: 451 Research/Palo Alto Networks, Security Operations Study, 2018
Q: What are your top priorities for eliminating security operations bottlenecks?



These are areas that benefit operations across all tiers, from making tier 1 more efficient to giving threat hunters more time to delve deeper into more sophisticated attacks.

Extending Security Practices

The research shows that there are significant opportunities for improvement across security operations. The high number of 'false positive' alerts coming into tier 1 points to the need for improved alert tuning. This can be done with more customized configurations of other security controls. It can also be done by adding more high-quality signals from the rest of infrastructure – be they from network, endpoint protection, cloud or other sources – to generate better alerts. In a sense, this is equivalent to extending the detection and response and automating some of the higher-level tier 2 practices of using multiple sources of data, but in a way that fits with tier 1 workflows.

Tier 1 teams appear to lack the necessary resources – tooling, additional knowledge or organizational support – to update their own tooling to handle alerts in a more predictable fashion, whether automatically or, if necessary, via predefined playbooks. Higher levels of automation could codify some of the recommended practices. Improving the satisfaction in EDR tools by simplifying investigations for tier 1 triage can create efficiency in current resources and operational processes. Improvements along these areas should also help with the issue of hand-off between tier 1 and tier 2, leading to a reduction in number of cases escalated to tier 2, including those being escalated unnecessarily.

Reducing the number of cases escalated to tier 2 should allow teams to focus their resources on other practices. They may be able to leverage new tooling that allows for aggregation of multiple sources of data – endpoint, network, cloud, etc. – to reduce the time it takes to perform investigations. They may also improve overall team knowledge – both in terms of security techniques and organizational knowledge.

Better overall security health would also help threat-hunting teams. The high number of investigations and threats found by hunting indicates there are significant 'low-hanging fruit' issues. Reductions in those can free up threat-hunting resources to perform more sophisticated hunting. One avenue, for example, could be deeper investigations into early signals of attacks that might show up in prevention/protection layers such as endpoint protection or network firewalls. Another would be to mobilize threat intelligence, allowing automatic detection across data sources, moving the burden from manual handling in tier 3 to automated playbooks for tier 1.

Conclusions and Recommendations

In our opinion, organizations are rightfully looking carefully at how to improve security operations, particularly in response to incidents. This reflects the nature of modern response because security teams are asked to respond to several events in increasingly complex environments.

The data from this study indicates that even with reportedly high levels of experience with EDR tools, opportunities for improvement exist both within each tier and in the broader relationship between them. There are opportunities to address three key concerns: lack of people, increasingly complex investigations, and lack of integration and automation.

For those with EDR tooling (or planning to add it), there are still many opportunities to improve security operations. Specifically, organizations should address a few key areas:

- Continue to acquire other data sources for detection and response – internal and external to the organization – to extend, enrich and expedite alert triage, incident investigation, hunting and overall detection.
- Improve quality of incoming alerts by better tuning existing sensors and deploying new capabilities that ingest additional data such as network, endpoint and cloud, and help better interpret their environment.
- Pre-correlate data from multiple sources to improve playbook coverage and automation capabilities for tier 1 analysts.
- Improve tier 2 workflows by readily integrating multiple sources of information during investigations and updating playbooks to reduce uncertainty and manual efforts.
- Continue evolving automation of threat hunting, anticipating how teams operate in a manner that complements the analysts, not aiming to replace them.
- Identify opportunities for extracting better insights from existing incidents, particularly in terms of obtaining threat information that is more relevant to the organization itself.

Effectively addressing these issues should lead to improved operational metrics for security teams and improved skills development for analysts. Ultimately, it can lead to a more capable and responsive security practice, able to better support the agility that their business and the modern threat environment demand.

Evolving Detection and Response to Meet SOC Needs

For detection and response products to meet the challenges of the modern SOC, they must provide visibility into all data sources, not just endpoints, while easing operational burden across tier 1, tier 2 and tier 3 analysts. This means bringing together data from disparate sources, be it network traffic from local and remote enterprise locations, activity from endpoint and mobile devices, or across the hybrid cloud environment such as public cloud, software-as-a-service (SaaS) and private cloud. With data centralized, this information must then be correlated to accelerate triage and investigations while decreasing complexity in hunting and detection. A result that siloed tools, such as endpoint detection and response and network traffic analysis – EDR and NTA – cannot fulfill independently.

Security professionals need detection and response offerings that provide centralized, holistic visibility into all activity so they can easily gather intelligence and respond quickly to any form of threat. This new category of detection and response is XDR.

XDR: The Next Generation of Detection and Response

XDR represents the next stage in the evolution of detection and response, giving security teams complete visibility across network, endpoint and cloud data. With it, cybersecurity teams can usher in a new era of heuristics, analytics, machine learning, and modeling to strengthen your protection against successful cyberattacks. The result is simplified investigations across security operations, reducing the time it takes to discover, hunt, investigate and respond to any form of threat.

Introducing Palo Alto Networks Cortex XDR

Cortex XDR from Palo Alto Networks is the first-ever XDR offering, a cloud-delivered app that empowers security teams to not only detect and stop sophisticated attacks but adapt defenses to allow constant improvement and the prevention of future successful cyberattacks.

With Cortex XDR, data from network, endpoint and cloud assets are stitched together during ingestion, correlated and analyzed. Machine learning is applied to profile behavior and detect unseen attacks from managed and unmanaged devices, ensuring complete coverage. A powerful query engine provides the basis for threat hunting, and custom rules ensure in-house knowledge can be applied to detect threats unique to the enterprise.

Stitching together data from multiple sources allows Cortex XDR to speed alert triage and incident response by providing a complete picture of each threat and revealing the root cause automatically. Information from previous investigations is also applied as context to simplify the analysis of current threats, ensuring any security team member can make accurate decisions quickly and identify next steps.

Cortex XDR reduces the time and experience required at every stage of security operations, from triage to threat hunting. Tight integration with enforcement points lets you respond to threats quickly as well as apply the knowledge gained from investigations to detect similar attacks in the future.

Great security starts with ironclad prevention. Cortex XDR reuses existing prevention tooling such as the Palo Alto Networks Next-Generation Firewall, VM-Series, Traps™ endpoint protection and response, and others to not only protect your environments but act as sensors and enforcement points. To ensure at least one data source is available, Traps and WildFire® cloud-based threat analysis service is included with Cortex XDR.

Traps uses multiple methods of prevention to safeguard endpoints from malware, ransomware, and exploits. Together, Traps, Cortex XDR, and WidFire deliver consistent prevention, detection, and response across all your digital assets.

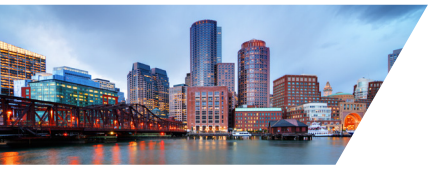
About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700



BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®