paloalto NETWORKS

CORTEX™
BY PALO ALTO NETWORKS

The State of SOAR Report, 2019

The Third Annual State of Incident Response Report

TABLE OF CONTENTS

Executive Summary

Note: Following Demisto's acquisition by Palo Alto Networks in 2019, the Demisto product was renamed Cortex™ XSOAR. As this 2019 report was initially published prior to the acquisition, references to Demisto, the company, have been left as is throughout the report to maintain the accuracy and integrity of the original report.

The challenges facing security teams are, perhaps unfortunately, common knowledge by now. A constant rise in alert volume, a stark security skills gap, piecemeal processes, and siloed tools have made security operations a tough place to be. In 2018, Demisto commissioned a large study to delve deeper into these issues, their manifestations, and possible solutions.

The 2019 report broadens the perspective from security orchestration, automation, and response (SOAR) to the security incident response lifecycle. Demisto commissioned a study with 552 respondents to find out specific challenges at each stage of the incident response lifecycle, how current product capabilities help overcome these challenges, and what capabilities are missing within security products today.

Shift to Security Incident Response Lifecycle

For this third annual report, we decided to broaden our focus from SOAR to the security incident response lifecycle. This lifecycle is a continuous and cyclical process of alert ingestion, enrichment, management, investigation, response, and measurement. The lifecycle is meant to act as a vendor-neutral outlook at how security teams handle incidents today. This report will provide an overview of the security incident response lifecycle and our findings from each stage of the lifecycle.

Playbooks on the Rise

As more organizations leverage SOAR for incident response, we've found their willingness to use automatable playbooks increase as well. This year, around 52% of respondents cited using either automated playbooks or a combination of automated and manual playbooks for implementing incident response processes. This is a stark departure from Demisto's 2018 State of SOAR report where over 50% of respondents stated that they either did not have set processes in place or that the processes were rarely updated after initial implementation.

The SIEM Catch-22

Organizations continue to rely heavily on Security Information and Event Management (SIEM) tools for multiple stages of the incident lifecycle. Around 75% of respondents stated using SIEMs for incident ingestion and enrichment, 66% leveraged SIEMs for investigation, and 66% preferred SIEMs for tracking metrics and performance. However, this SIEM prominence was partly undercut by respondents citing a "feature wish list" for each lifecycle stage—features that respondents felt the current SIEM tools lack.

It Takes a (Security Product) Village

While security products continue building up diverse feature-sets with the aim of becoming a "one stop shop", organizations still prefer to rely on a suite of security products with niche strengths.

Around 48% of respondents cited using six or more security tools for incident response. More than 68% of respondents preferred using "best of breed" products across vendors rather than purchasing multiple solutions from the same vendor. With these points in mind, product interconnectivity across vendors is crucial for good user experience.

Ingestion and Enrichment: Need for Automation and Correlation

Within incident ingestion and enrichment, 56% of respondents included automated data enrichment as part of their feature wish list. This was closely followed by automated prioritization of alerts (47.8%) and correlation of alerts/indicators across products (47.5%) respectively. Security teams clearly desire more high-fidelity data at their fingertips so that they have more time and information for decision-making.

Incident Management: Auto-Documentation and Mobile Support in Demand

Within the "manage" phase of the incident lifecycle, more than 60% of respondents wished for tools that automatically captured information for post-incident review. A mobile application for incident management was also desirable, with 47% of respondents including it in their wish list and only 25% of respondents claiming to have mobile support from their current products. Other capabilities in demand included the ability to add notes and tags to individual artifacts (51.27%) and the ability to reconstruct incident timelines (51.27%).

Incident Investigation: Where's the Evidence?

For incident investigation, around 60% of respondents cited an "evidence board" and "attack reconstruction" as abilities they needed but currently lacked. Since investigation is usually a time-consuming and tool-spanning process, respondents also desired a common platform for cross-team investigation (53.54%) and automated remote execution of actions across security tools (52.36%).

Response: SOAR Moves the Needle

60.5% of respondents confessed to manually updating point product policies, highlighting a time sink that security products have still not successfully plugged. However, among respondents that used SOAR, 60.5% of them stated that they DID NOT need to manually update point product policies.

Looking at wish lists, almost 54% of respondents cited the need for industry-specific response templates. Roughly 52% of respondents also wished for live runs of playbooks for each incident, providing food for thought as SOAR vendors chart out their product roadmaps.

Performance Measurement: Machines Are Learning

Respondents desired "measurement multipliers": features that could continue to improve their efficiencies with time. Roughly 61% of respondents wished for "machine learning recommendations" for improving security operations (with only 30% of respondents claiming that this feature was already present in their security products). Around 49% of respondents also included "customizable dashboards for each user" in their wish lists, underlining the need to provide security teams with the flexibility to slice and dice their own data.

SOAR's Place in the Puzzle

SOAR products have now grown to an extent where they are a critical part of the SOC puzzle. Around 33% of respondents used SOAR for incident ingestion and enrichment, roughly 28% used SOAR for case management and incident investigation respectively, and close to 33% used SOAR for response and performance measurement respectively. With SOAR products championing so many features that respondents included in their "wish lists", the data suggests that SOAR solutions will continue to ensconce themselves in a security team's life.

1. Understanding SOAR

The term "SOAR" was coined by Gartner in late 2017 to refer to security technologies that helped SOC teams standardize, manage, and automate processes across products. The primary use cases for SOAR tools are in security operations and incident response. The general-purpose nature of these tools, however, has led to emerging use cases in cloud security orchestration, vulnerability management, threat hunting, and more.

Here are the building blocks that make up SOAR:

- **Orchestration** refers to the act of integrating disparate technologies, usually through workflows, so that they can function together. This means using security-specific and non-security-specific technologies simultaneously in a way that eases coordination.
- **Automation** refers to the process of machines executing tasks hitherto performed by humans. In the context of SOAR, automation is ideally seen as human enhancement and not human replacement. Automation of repeatable, low-level tasks acts in concert with human decision-making for overall acceleration of incident investigations.
- **Incident management and response** is a crucial element of SOAR. Fundamentally, SOAR seeks to foster a comprehensive, end-to-end understanding of incidents by security teams, resulting in better and more informed response.
- **Dashboards and reports** form a critical part of SOAR. One of the ways to achieve unified response is by providing data visualizations where incidents can be easily seen, correlated, triaged, documented, and measured.

2. A Comparison with 2018

While the 2019 State of SOAR report takes a broader, lifecycle-focused approach than the 2018 report, there are a few year-by-year comparisons that jumped out and merit discussion.

Playbooks on the Rise

We asked respondents how they implemented and enforced incident response processes. The responses were quite encouraging and painted a more optimistic picture of SOCs than the 2018 report.

Roughly 52% of respondents cited using either automated playbooks or a mixture of automated and manual playbooks to implement incident response processes (figure 1). While this was not a SOAR-specific question—the playbooks could have been implemented using any security tool with the requisite capabilities—it was heartening to see a clear shift towards standardizing, enforcing, and automating repeatable incident response processes.

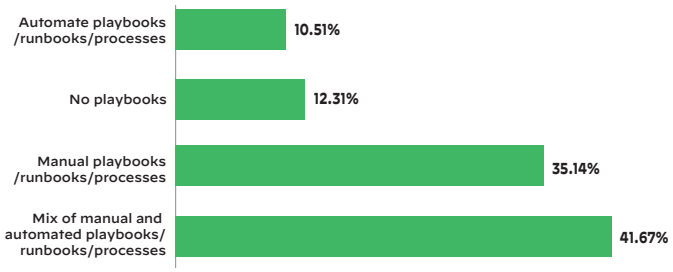

Figure 1: Incident response process implementation

In the 2018 report, we had asked respondents about both the presence of IR processes and the frequency with which they were updated. Over 50% of respondents stated that they either did not have set processes in place or that the processes were rarely updated after initial implementation (figure 2).

Two points must be noted here:

- We did not survey the same respondents for the 2018 and 2019 reports. While we tried to capture responses from the same representative pool of security practitioners, the individual responses come from different sets of individuals.
- The question asked for the 2019 report was about IR process implementation, while the question asked for the 2018 report was about IR process implementation and update frequency.

Taking these caveats into consideration, we offer up this comparison as more of a qualitative insight than an exercise in scientific rigor.

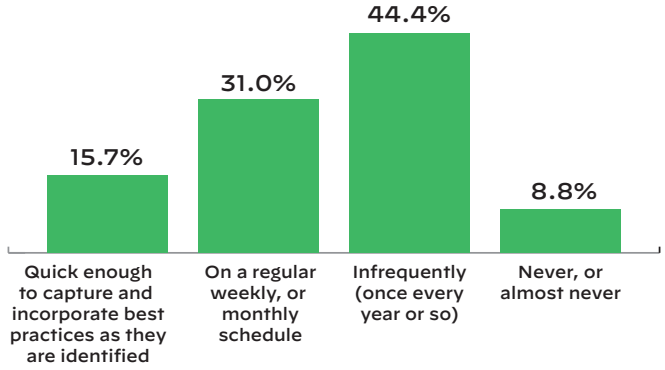

Figure 2: Incident response playbooks/runbooks/processes update frequency

Security Tools, Security Tools Everywhere

It's a well-accepted if regrettable truth that no one security product can solve all SOC problems. Security teams end up using a suite of products that span across vendors, functions, and data standards. While each product brings unique value to the table, security teams struggle to switch context, centralize data, and coordinate actions across different tabs and consoles.

These pain points were borne out in both the 2018 and 2019 reports. For both reports, we asked respondents to estimate the number of distinct security products they needed to manage for incident response.

Even though the respondents were different for each survey, we observed a similar split in responses across both years. Close to 50% of respondents claimed using six or more distinct security products for incident response in both 2018 and 2019 (figures 3 and 4).

These results can help us infer that **product proliferation is not going away any time soon**. Security vendors should aim to improve user experience in the face of multiple tools by encouraging product inter-connectivity, data standardization and transfer, and remote execution of actions across products.

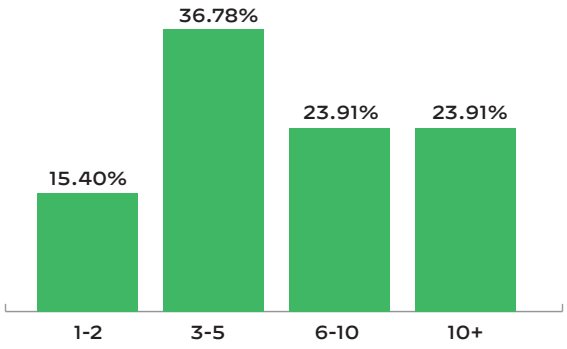

Figure 3: Number of security products managed

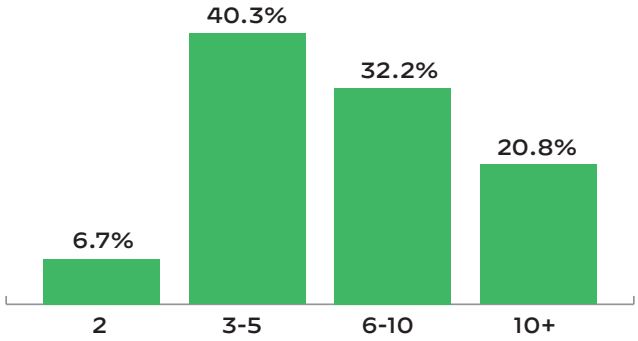

Figure 4: Information security tools in use in organization (management)

3. Defining the Security Incident Response Lifecycle

Every security team has its own set of security tools, competencies, common use cases, and compliance requirements. One of the few common threads that weaves across all these elements is the **steps followed while responding to a security incident**.

With this in mind, we defined a security incident response lifecycle and asked respondents to:

- Outline pain points during each lifecycle step
- List common security tools used for each step
- Rank capabilities that they felt were both missing and needed

We defined the security incident response lifecycle as a continuous and cyclical process of incident ingestion and enrichment, incident management, deeper investigation, enforcement of response actions, performance measurement, and the adoption of lessons learned to improve operational efficiency going forward.

Below, we will use phishing response as an example to outline each step in the lifecycle. This is merely illustrative; each lifecycle step can have more actions than the ones listed below.

Incident Ingestion and Enrichment

The email gets forwarded by a concerned employee to the organization's quarantine mailbox. The security team studies the email and checks the reputation of indicators attached to the email (sender name and address, IP, domain, etc.).

Case Management

The security team opens a ticket to capture the status for the phishing email. They mail the end user, confirming receipt of the forwarded phishing email. They add notes and comments to record their findings from the incident, measure SLAs for each step of investigation and response, and generate reports once the incident is resolved.

Incident Investigation

The suspected phishing email has a PDF attachment. The security team detonates this file using a malware analysis tool and captures the results. They also check whether other end users were affected by the same phishing email, or emails that look like they're part of the same phishing campaign.

Response and Enforcement

Based on the data gathered during enrichment and investigation, the security team decides that the email is a verified phishing attempt. They send an email to the end user with this update, delete the email from all inboxes they can find, add indicators of compromise (IOCs) to dynamic block lists, and update the ticket assigned to the phishing email.

Performance Measurement

The security team measures the mean time to respond (MTTR) to the phishing incident and checks whether this time is within organizational SLA requirements. They also hold a debrief to discuss lessons learned from this incident: which actions were useful, which actions took the most time, and how they can better respond to similar incidents in the future.

The following sections will go through each stage of the security incident response lifecycle in greater detail.

4. Incident Ingestion and Enrichment

Organizations today have employees, computing resources, and customers spread across the world, resulting in a corresponding increase in the threat surface they must contend with. In order to respond to incidents, security teams need to discover that there's an incident in the first place. This is no mean task.

Common Tools Used

We asked respondents what tools they commonly used for incident ingestion and enrichment, allowing for multiple options due to the disparate nature of incident detection in today's security landscape.

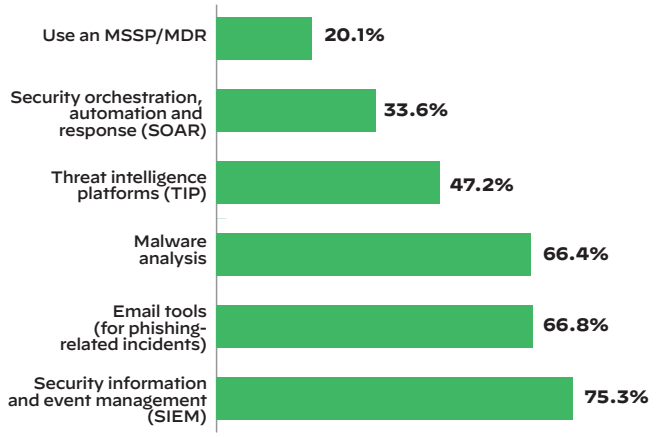

Figure 5: Incident ingestion and enrichment tools

The most striking data point from the responses (figure 5) was the prominence of security information and event management (SIEM) tools, with around 75% of respondents citing these tools as important sources for incident ingestion and enrichment. SIEMs have a range of capabilities—monitoring machine data across sources, prioritization and aggregation, and rules for adapting detection with time—that are critical for incident ingestion and enrichment, so we believe SIEMs' importance to be well-merited here.

However, around 67% of respondents stated that they used email tools to ingest phishing incidents and roughly 66% of respondents highlighted malware analysis tools as important ingestion and enrichment sources. These results imply some limitations that SIEM tools have, namely that **SIEMs are not used as a sole detection source for all incidents** and that they lack the niche capabilities that other tools (like malware analysis) possess.

Wish List of Capabilities

For incident ingestion and enrichment, we asked respondents to highlight product capabilities their tools possessed and create wish lists of capabilities their tools lacked.

The results (figure 6) underline the need for automation and correlation while ingesting and enriching incidents. Only 34% of respondents claimed to have "automated data enrichment" capabilities in their current products, and 56% of respondents made it a part of their wish list. Around 48% of respondents wished for "automated prioritization of alerts", and 47.5% of respondents cited the need for "correlation of alerts and indicators across products".

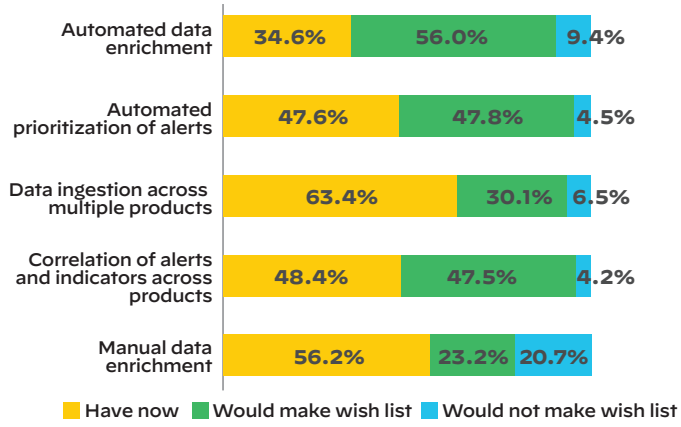

Figure 6: Incident ingestion and enrichment wish list

These figures throw into sharp relief the sheer amount of manual work security teams need to do while conducting incident triage. While we acknowledge all the heavy lifting that SIEMs do here, there are still two challenges to contend with:

- **Too many false positives:** It's always safer to set the sensitivity levels of SIEMs higher than necessary, lest any serious incident slip through the cracks. The downside of this caution is a ballooning number of false positives that analysts must manually study and cast away.
- **Multiple detection sources:** The threat surface is simply too large and varied for SIEMs to be the only tool for incident ingestion. The problem with multiple tools for incident ingestion (email inboxes, malware analysis, cloud security, etc.) is the manual post-incident correlation that security teams must perform to uncover larger attack campaigns.

5. Case Management

During incident response, security teams have scores of balls up in the air. As they quickly transition across consoles to gather additional context and contain the incident, it's critical for them to have central case management capabilities and avoid fragmented documentation.

Common Tools Used

We asked respondents what tools they commonly used for case management.

Results (figure 7) show almost 70% of respondents entrusting their case management to ticketing solutions. Since ticketing systems often span across teams (IT, security, support, and so on), it makes sense for central management to occur on these tools. The caveat here is that ticketing systems sometimes lack in depth what they possess in breadth. Security-focused case management tools can make up the difference. These tools ranked second in the results, proving the tool of choice for around 36% of respondents.

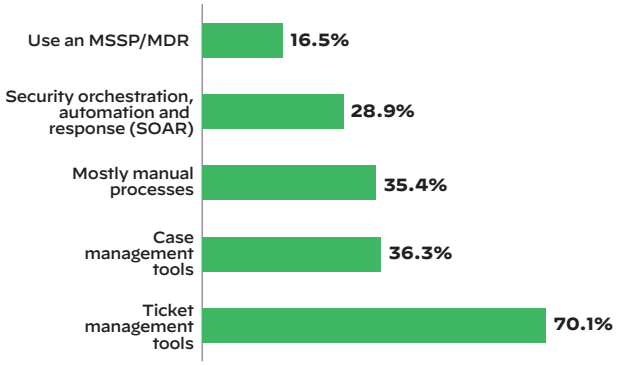

Figure 7: Case management tools

Wish List of Capabilities

For case management, we asked respondents to highlight product capabilities their tools possessed and create wish lists of capabilities their tools lacked.

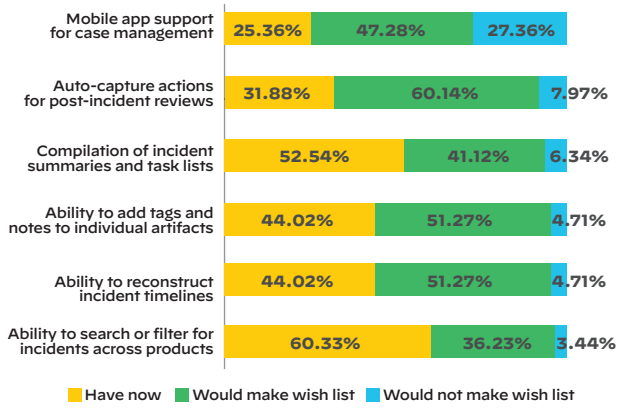

Figure 8: Case management wish list

More than 60% of respondents wished for tools that automatically captured information for post-incident review (figure 8). A mobile application for incident management was also desirable, with 47% of respondents including it in their wish list and only 25% of respondents claiming to have mobile support from their current products. Other capabilities in demand included the ability to add notes and tags to individual artifacts (51.27%) and the ability to reconstruct incident timelines (51.27%).

We can surmise from the results that data collection and summarization during incident response is still too manual and fragmented, preventing security teams from performing at maximal efficiency. Many of the "wished for" capabilities (reconstructing incident timelines, adding tags and notes to artifacts) seem like they would be better fulfilled by a more security-focused tool than general-purpose ticketing systems.

6. Incident Investigation

Once incident triage has been completed, an attack investigation usually requires additional tasks, such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, poring over logs, and finalizing resolution.

Common Tools Used

We asked respondents what tools they commonly used for incident investigation.

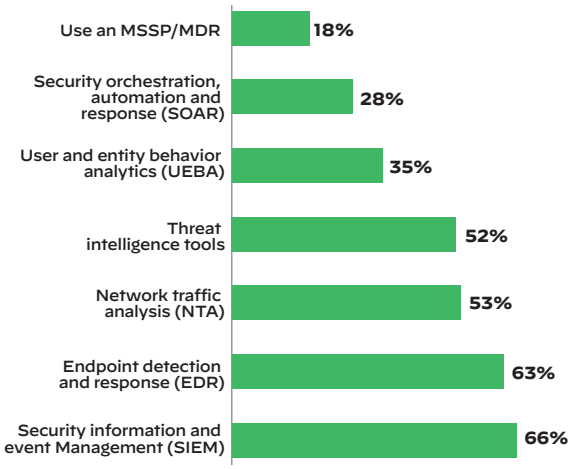

Figure 9: Incident investigation tools

SIEM tools occupied pole position in the results (figure 9), with 66% of respondents citing them as critical consoles for investigation. Endpoint detection and response (EDR) tools and network traffic analysis (NTA) tools also ranked well, selected by 63% and 53% of respondents respectively. We can infer from these results that attackers leave breadcrumbs across sources.

SIEMs, EDR tools, and NTA tools all ranked well for investigation, implying that attacks usually have unique signatures at different levels of security (the network level, the endpoint level, and so on). Unfortunately, it's left to security teams to manually piece together data across these sources and create an overall picture of the attack.

Wish List of Capabilities

For incident investigation, we asked respondents to highlight product capabilities their tools possessed and create wish lists of capabilities their tools lacked.

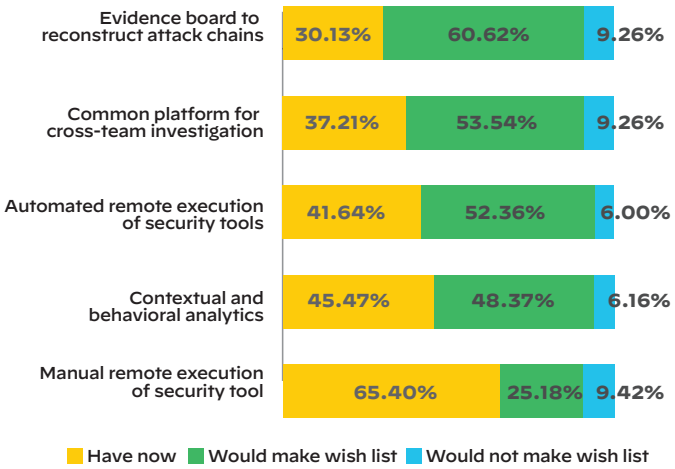

Figure 10: Incident investigation tools wish list

Around 60% of respondents cited an "evidence board" and "attack reconstruction" as abilities they needed but currently lacked (figure 10). Since investigation is usually a time-consuming and tool-spanning process, respondents also desired a common platform for cross-team investigation (53.54%) and automated remote execution of actions across security tools (52.36%).

The common thread running across all these wished-for capabilities is the presence of **disparate security tools that lack interconnectivity.** Security tools often provide unique value, but if these individual tool utilities don't coalesce into a unified whole, security teams are left needing to cross-reference data across tools and lend structure to their chaotic investigations.

7. Response and Enforcement

Response and enforcement are probably the most important and least discussed step in the security incident response lifecycle. After security teams are presented with rich, high-fidelity data by a host of security tools, there's often a "so what?" question that escapes their lips. If alerts are not met with action, the rows and columns of nuanced data count for nothing.

Common Tools Used

We asked respondents what tools they commonly used for response and enforcement.

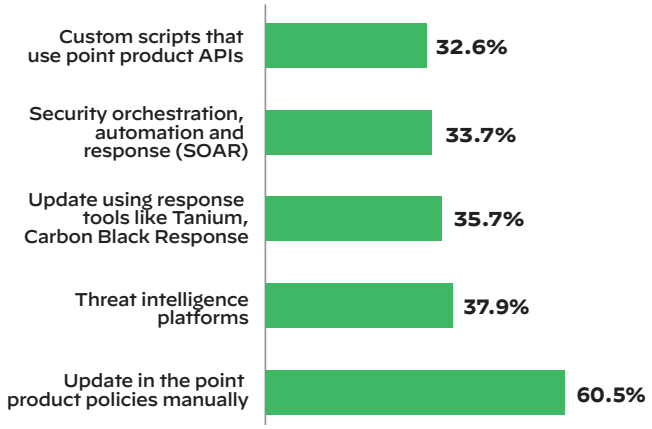

Figure 11: Response and enforcement actions in point tools—mechanisms used

The results make for somber reading and underscore the challenges that security teams face today (figure 11). 60.5% of respondents confessed to manually performing updates and blocks on point products. While 38% of respondents cited threat intelligence platforms as mechanisms for response, the scope of these tools is relatively narrow and can't cover the entire spectrum of necessary response and enforcement actions.

Fortunately, we found that SOAR tools have already begun to move the needle toward coordinated and automated response. Upon filtering only for respondents that used SOAR, we found that **60.5% DID NOT need to manually perform response actions on point products** (figure 12). This is an appreciable

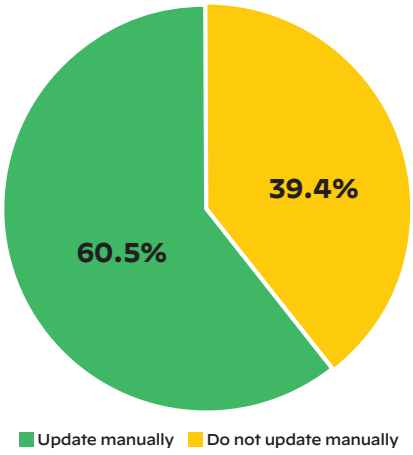

Figure 12: Need for manual response actions on point products

shift; moreover, the 40% can partially be accounted for by limited API functionalities of third-party products that don't allow for every response action to be remotely executed from within SOAR products.

Wish List of Capabilities

For response and enforcement, we asked respondents to create wish lists of capabilities their current tools lacked.

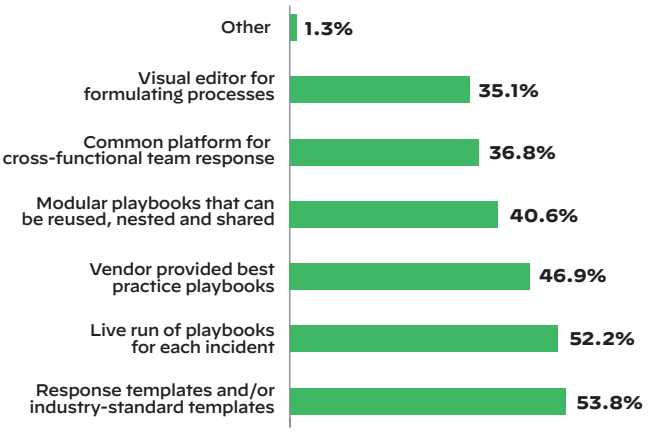

Figure 13: IR and analyst performance tracking capabilities wish list

Almost 54% of respondents cited the need for industry-specific response templates (figure 13). Roughly 52% wished for live runs of playbooks for each incident and 47% asked for vendors to provide best-practice playbooks. These results highlight clear areas of improvement for SOAR tools, namely the **need for standardization and user guidance.** SOAR tools should strive for a balance between robust out-of-the-box content and the flexibility for users to easily create their own content.

8. Performance Measurement

Once incidents have been driven to resolution, it's vital that security teams measure their performance to ensure they can repeat what worked and avoid what didn't work or took too much time. This measurement ideally spans across use cases (what's our average response time for phishing incidents?), personnel (what's Bob's average response time for phishing incidents?), incident phase (which step of phishing investigation is taking the most time?), and more.

Common Tools Used

We asked respondents what tools they commonly used for performance measurement.

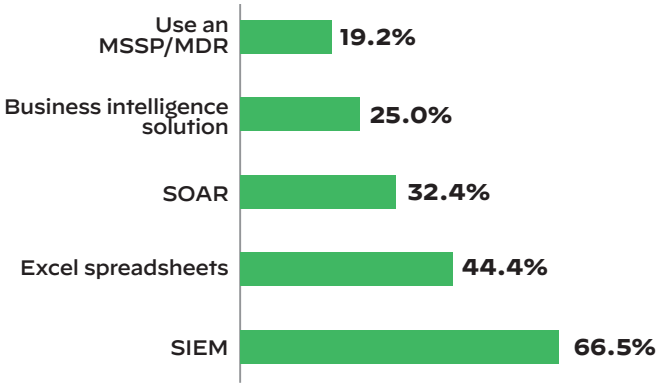

Figure 14: Tools for incident response and analyst performance metrics

SIEMs ruled the roost again, with 66% of respondents privileging them for performance measurement (figure 14). Interestingly, **Excel spreadsheets ranked second with 44% of responses**.

This should be an eye-opener for security vendors and hammer home two things:

- SIEMs can't take care of all performance measurement needs, either through limited scope of security data or product capabilities that are lacking.
- Security teams don't just use security tools; they use whatever tools solve their problems.

Wish List of Capabilities

For performance measurement, we asked respondents to highlight product capabilities their tools possessed and create wish lists of capabilities their tools lacked.

Results showed that respondents desired **"measurement multipliers"**: features that could continue to improve their efficiencies with time (figure 15). Roughly 61% of respondents wished for "machine learning recommendations" for improving security operations (with only 30% of respondents claiming that this feature was already present in their security products). Around 49% of respondents also included "customizable dashboards for each user" in their wish lists, underlining the need to provide security teams with the flexibility to personalize the data at their disposal.

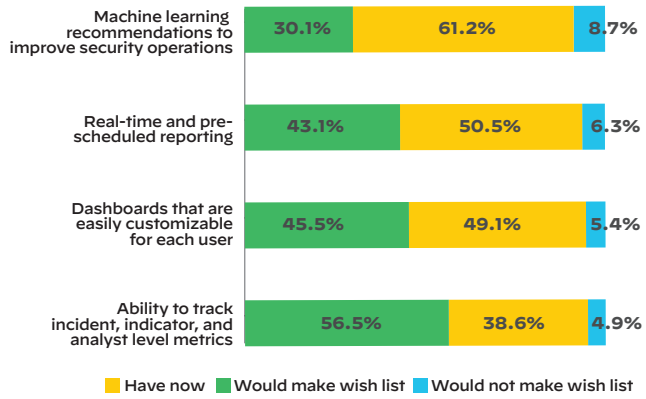

Figure 15: IR and analyst performance tracking capabilities wish list

9. A SOAR-Focused Debrief

In this section, we will view the survey responses through a SOAR-focused lens, presenting analysis on both SOAR strengths and areas of improvement.

- **Ever-present and growing across the lifecycle:** SOAR tools comprised a healthy and growing percentage of common tools used for **every lifecycle stage** (ranging from 28% to roughly 34%). This suggests that users have found proof of value from SOAR tools for all aspects of incident response and management; the relatively modest percentage figures should grow with increased tool adoption and maturing product capabilities.
- **Moving the response needle:** SOAR tools have already begun to make a quantifiable difference and move organizations towards coordinated and automated response. While around 60% of respondents confessed to manually performing updates and blocks on point products, when the respondents were filtered for only those that owned SOAR products, we found that roughly 60% of them DID NOT have to manually respond on point products anymore.

SOAR integration ecosystems are critical: While security vendors expand capabilities with the aim of being a "one stop shop", end users are more agnostic while viewing enterprise security. When asked how they evaluated vendors for IR activities, over 68% stated that they purchased best-of-breed

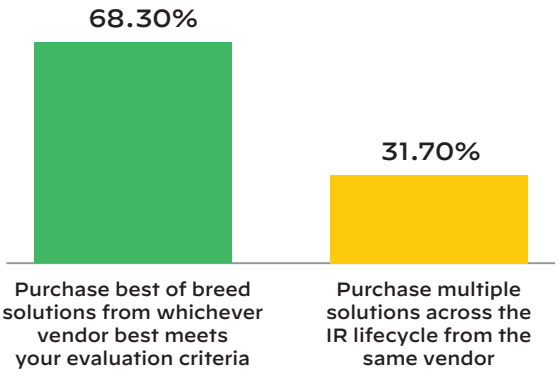

Figure 16: Evaluating solution for IR activities/processes

solutions, even if the solutions were offered by different vendors. Taking this end user sentiment into account, SOAR products will be a critical part of the security product stack of the future. Even looking beyond SOAR, security tools that implement open integration ecosystems and facilitate inter-product connectivity will be best suited for improving SOC efficiencies.

How Cortex XSOAR Helps

In table 1, we have listed the wish lists of product capabilities that respondents cited in the survey and aligned them with capabilities that Cortex™ XSOAR possesses. For a vendor-neutral look at SOAR's future, you can continue to the next section.

Table 1: How Cortex XSOAR Helps

Section of Security Incident Response Lifecycle	Wish List of Capabilities	How Cortex XSOAR Helps
Ingestion and Enrichment	Automated data enrichment	• Cortex XSOAR playbooks can automate data enrichment through product integrations with threat feeds, malware analysis, SIEMs, UEBA, and so on.
	Automated prioritization of alerts	• Pre-process rules can be assigned to alerts to parse and filter according to user-defined criteria. • Severity can automatically be assigned to alerts based on playbook criteria.
	Correlation of alerts and indicators across products	• Correlation of indicators across incidents. • Indicator reputation from multiple threat feeds (that end users possess) visible in one location. • Related Incidents screen shows customizable, temporal map of similar incidents based on extensive criteria.
Case Management	Auto-capture actions for post-incident review	• Cortex XSOAR War Room automatically documents all tasks, comments, and actions. • Evidence board can automatically populate key pieces of information (based on playbook triggers).
	Mobile app support	• Cortex XSOAR mobile application enables at-a-glance incident oversight. • Users can view standard/custom dashboards, incident queues, and task lists. • Execute incident actions (assign to analyst, set severity, close incident) on the go.
	Adding tags and notes to individual artifacts	• Users can add custom comments to playbook tasks. • Any entry in the War Room can be marked as notes; these notes show up on the incident summary page. • Any incident/indicator can have fields to enter custom comments.
Incident Investigation	Evidence board	• Cortex XSOAR evidence board enables collection of key information that led to incident resolution.
	Common platform for cross-team investigation	• Cortex XSOAR War Room lets users collaborate on joint investigations.
	Remote execution of actions across security tools	• Cortex XSOAR users can execute actions across all integrated products from the War Room in real time.
Response and Enforcement	Response templates or industry-standard templates	• Cortex XSOAR has out-of-the-box (OOTB) content for incident types, incident summaries, and playbooks. • OOTB content gets updated twice every month for all Cortex XSOAR deployments.
	Live run of playbooks for each incident	• Cortex XSOAR Work Plan screen shows live run of playbook for each incident. Easy for visibility and task-specific troubleshooting.
	Vendor provided best-practice playbooks	• Cortex XSOAR has hundreds of OOTB playbooks available in the product and on GitHub. • New playbooks are added twice a month as part of content updates.

Table 1: How Cortex XSOAR Helps (continued)		
Section of Security Incident Response Lifecycle	**Wish List of Capabilities**	**How Cortex XSOAR Helps**
Performance Measurement	Machine learning recommendations	• Cortex XSOAR uses machine learning to suggest ideal analyst owners, playbook arguments, commonly used security commands, and other aspects to improve security operations.
	Real-time and pre-scheduled reporting	• Cortex XSOAR contains an OOTB collection of reports that can be scheduled or executed in real time. • Reports can be fully customized based on OOTB and user-created widgets.
	Customizable dashboards for each user	• Cortex XSOAR contains standard dashboards that provide visibility into incident, indicator, analyst, and system data. • Dashboards can be fully customized based on OOTB and user-created widgets.

10. Looking into SOAR's Crystal Ball

SOAR has come a long way these past few years, some of its elements almost unrecognizable from when pioneers in the space launched the first versions of their products. Acknowledging the rapid rate at which security products morph to meet user needs, this section of the report will project some future SOAR trends that will help sustain this industry's forward momentum.

Moving Beyond the SOC

Although the crux of this survey was to capture pain points and wish lists across the security incident response lifecycle, we also wanted to see what respondents felt about some potential future applications of SOAR. Chief among these applications is SOAR tools' capacity for use cases outside the SOC.

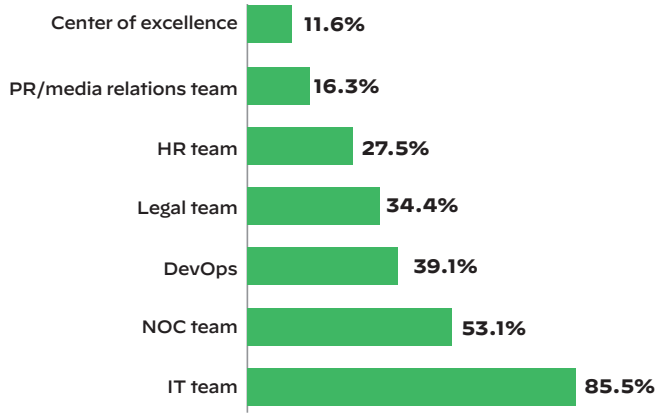

Figure 17: Which teams do you have to deal with on a daily basis (for IR) outside of the SOC?

We asked respondents which non-security teams they had to regularly work with for their day-to-day operations. A whopping 85.5% of them cited the IT team as their constant companions during incident response. Roughly 53% stated the same of the network operations center (NOC) team, with the DevOps team (39.1%) coming in at third.

SOAR products have the potential to be the connective fabric across security and non-security teams whenever multi-stakeholder collaboration is required during incident response. Playbooks can coordinate actions across products that are used by multiple teams (such as firewalls and ticketing systems) to ensure that cross-team communication keeps flowing and repetitive tasks are automated whenever possible.

We studied this general-purpose nature of SOAR through another lens as well: use cases. We asked respondents which non-IR use cases they had to manage on a day-to-day basis. Common use cases that resonated were vulnerability management (71.6%), security audits (67.8%), compliance checks (61.1%), and cloud security (41.1%).

The common theme among most of these use cases is that they are **operational (proactive) rather than response (reactive).** SOAR playbooks are multi-functional enough to cover both scenarios. While playbooks can be triggered upon incident ingestion, some vendors' playbooks can also be scheduled to run at predetermined intervals or triggered in real time. These playbooks can cover use cases such as security audits and compliance checks.

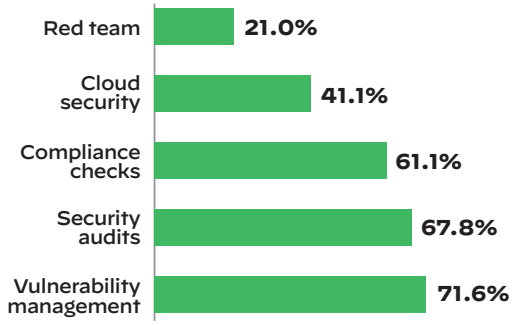

Figure 18: Non-IR processes to manage

As for cloud security alerts, SOAR tools can play the critical role of **coordinating response procedures across cloud and on-premises infrastructures.** Most organizations have one metaphorical foot in the cloud and the other on-premise, with products across the divide rarely "speaking' with each other. SOAR tools can connect these tool sets and impart agility—something that's sorely needed in cloud security—by automating actions such as provisioning/deprovisioning cloud instances, blocking indicators, changing security groups, and so on.

Regulation and Compliance

While responding to breaches on a security front can involve isolated teams, broader response usually requires coordinated participation from PR and media teams, legal departments, and IT teams to implement correctly. With the enforcement of GDPR and US state breach notification laws, the organizational consequences of handling a data breach in a sub-optimal manner are dire.

We asked respondents which regulations impacted their SOC policies and procedures. A considerable 61.5% highlighted local security breach notification laws as regulations that necessitated changes in their SOC. Roughly 48% cited GDPR as well which, while encapsulating certain breach notification laws as well, covers a wider range of guidelines overall. This was followed by industry-specific regulations such as PCI DSS (44.3%), HIPAA (43%), and GLBA (13.4%).

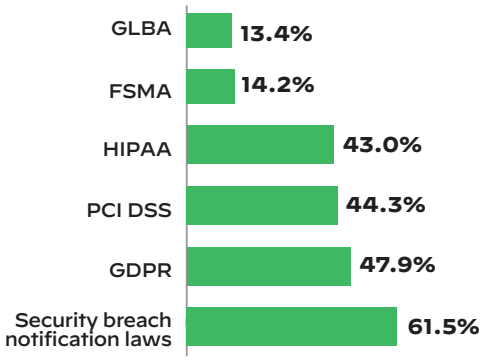

Figure 19: Regulations impacting SOC policies and procedures

Security orchestration tools, when combined with process knowledge within the organization, can be used to execute **compliance and breach notification playbooks** that will run in parallel to standard incident response playbooks. These playbooks can be populated with notification templates, contact details of law enforcement officials, and best practices to follow in the event of a breach.

Just like with incident response, these compliance playbooks will ensure that organizations follow the same process every time and eliminate any variance in response quality.

11. Survey Demographics

To highlight the depth and breadth of our study, we wanted to document the broad demographics of our respondents. These details include company size, company location, job roles, and the nature of the organizations' incident response function.

This vendor neutral research was independently conducted by Virtual Intelligence Briefing (ViB). ViB is an interactive online community focused on emerging through rapid growth stage technologies. ViB's community comprises more than 1.2 million IT practitioners and decision-makers who share their opinions by engaging in sophisticated surveys across IT domains, including Information Security.

The survey methodology incorporated extensive quality control mechanisms at 3 levels: Targeting, in-survey behavior, and post-survey analysis. The calculated margin of error is +/-3.4%. The effective margin of error as a result of extensive quality controls to assure high data quality is estimated to be +/1 2.7%. Learn more about ViB's research capabilities at https://vibriefing.news/research-services/.

In total, the report surveyed 552 respondents across security job functions and industries—a set that is statistically representative of the security community at large.

Company Size and Industry

We tried to maintain an equitable distribution of business sizes and industries to cater results to the widest possible user base. The results (figures 20 and 21) confirm that we were able to represent a wide variety of businesses and avoid any biases resulting from niche, insulated samples.

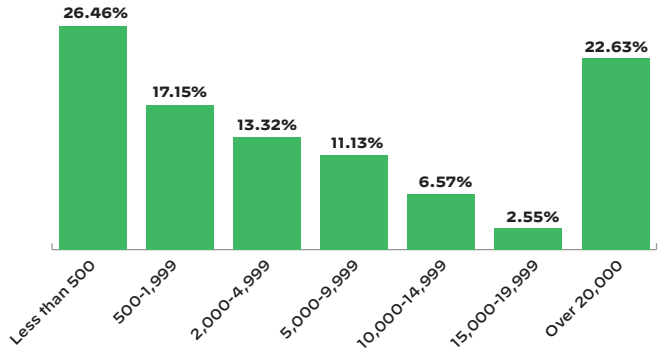

Figure 20: Number of employees

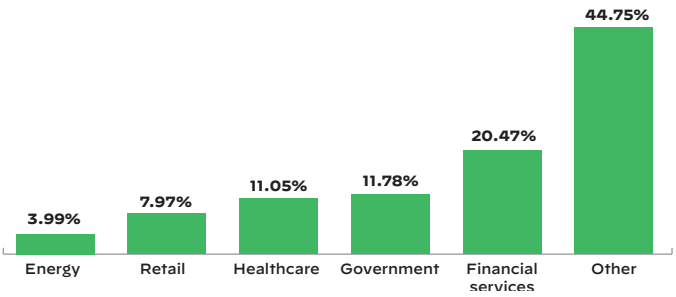

Figure 21: Primary industry

Job Role

We wanted to get the perspective of both employees and managers, and thus tried to represent the opinions of both sets in this research. Like any industry, cybersecurity is reliant on both the strategic vision of managers and the tactical execution of employees. The report managed to represent a healthy spread across this aisle (figures 22 and 23).

Company Location and Geographical Distribution

We wanted to have an international respondent spread in our research if possible and avoid any locational biases in responses. Our respondents ended up being mainly from North America

(figure 24). We concede that responses might be "localized' as a result. However, considering that North America is one of the forerunners in terms of information security, we hope the insights from this report provide value to readers across the globe.

In terms of geographical distribution of companies, the report was able to achieve a much more balanced sample (figure 25). The responses contained a good mix between companies that are centrally located, companies that are geographically dispersed in one country and across countries, and companies that observe a follow-the-sun model of operations.

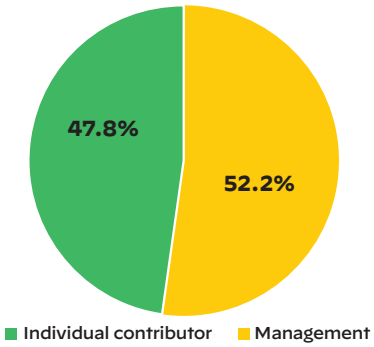

Figure 22: Job role level—individual contributor vs. management

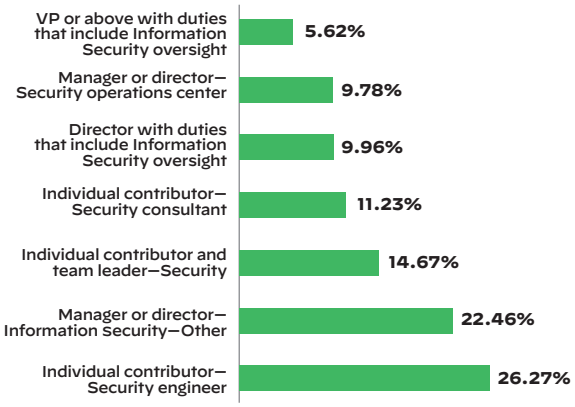

Figure 23: Job role sets

Incident Response Function

We wanted to focus the research on respondents whose security incident response functions were largely in-house. We believed these security practitioners would offer the most honest and relevant insights on challenges, tools used, and desired capabilities.

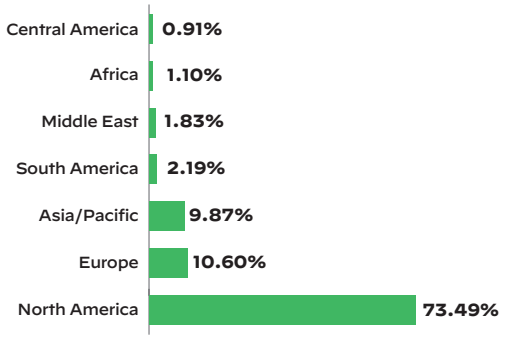

Figure 24: Company location

The survey demographics bear out our aim, with over 80% of respondents either performing incident response in-house or augmenting an in-house team with consultants on a per-need basis (figure 26).

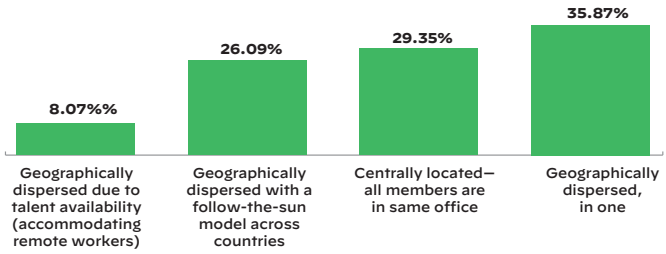

Figure 25: Geographic location

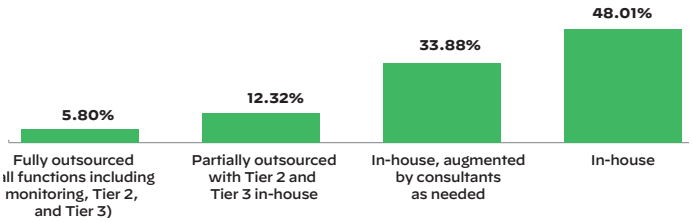

Figure 26: Security incident response function

Learn more about SOAR

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