How to Plan for Tomorrow's SOC, Today

4 Steps + 3 Keys to Transform Security Operations to Combat Advanced Attacks and Improve SOC Efficiencies

Table of Contents

Introduction: Global Disruptions Take Center Stage 3

SOCs Are Challenged Like Never Before 3

What Is Needed? A Sea Change 4

4 Steps Toward Creating a Future-Forward SOC 4

Step 1: Auditing Your Environment Can Help Reduce the Security Risk of Tool Sprawl. 4

Step 2: Automate Workflows 6

Step 3: Augment People with ML-Driven Intelligence 6

Step 4: Optimize Security Teams 7

ASM, SOAR, and XDR: The Bedrocks for SOC Transformation 8

Key 1: ASM—Power Up Your Risk Management Function by Understanding Your Attack Surface. . . .8

Key 2: SOAR—Orchestrating Across Your Product Stack for Efficient Incident Response 9

Key 3: XDR—The Next Logical Evolution of EDR 11

XDR Fills the Detection and Response Void 11

Cortex XDR, Cortex XSOAR, and Cortex Xpanse: Better Together, End to End 12

Begin Your SOC Transformation Today 13

Introduction: Global Disruptions Take Center Stage

Organizations are in the proverbial crosshairs for everything from errant insider threats to well-funded nation-states poised for cyberwarfare, with no signs of threats diminishing in quantity or severity.

With cryptocurrencies at record prices, ransomware attacks continue to plague organizations of all sizes. Nation-state attacks have reportedly risen 100% between 2017 and 2020,[1] targeting enterprise, media and communications, critical infrastructure, and the public sector.

Supply chain attacks such as those on SolarWinds can infect whole ecosystems through a single third-party vendor. And the recent four zero-day vulnerabilities in Microsoft Exchange Server traced back to the state-sponsored APT group Hafnium all further underscore the need for SOC and security teams to rethink their strategies moving forward, including having real-world incident response plans and current risk assessments in place.

And in a year like no other, companies and organizations across the globe were tasked with undertaking a phenomenal exercise because of the COVID-19 pandemic: bring workers online, remotely, quickly, and securely.

Sometime around mid-March 2020, a strange and unprecedented event occurred: a sudden mass exodus of millions of employees (worldwide) away from the relative safety net of conducting business in a controlled and secure environment. Seemingly overnight, operations were migrated—some of them business-critical—to home networks on multiple devices with little to no planning for this widespread event, executed in a short timeframe.

Not only did this place a huge reliance on corporate cybersecurity teams, protocols, and systems, it exposed technology gaps between corporate locations and remote home offices. The necessity to support a fully remote user workforce and ecosystem, including updating incident response plans, became job number one for countless IT and security teams.

The resulting security challenges for businesses and their supply chains have certainly been impacted by the abrupt shift in operations, but it's also exposed a host of other issues that are a direct result of a collective response to the global pandemic. Furthermore, as workers pivot between home and corporate networks, this hyper-distributed workforce will continue to be vulnerable, with threat actors continuing to take advantage of the situation, potentially for years.

In this paper, we will review some best practices and technologies to support SOC transformations that align with industry methodologies, including those from NIST and SANS, as well as insights and predictions from analyst firms such as Gartner, Forrester, and Enterprise Strategy Group (ESG).

> "COVID-19 refocused security teams on the value of cloud-delivered security and operational tools that don't require a LAN connection to function, reviewing remote access policies and tools, migration to cloud data centers and SaaS applications, and securing new digitization efforts to minimize person-to-person interactions."
>
> **–Christy Pettey, Gartner**

Palo Alto Networks Security Operations Center Mission Statement: Defend our information and technology resources, intellectual property, and ability to operate by disrupting our adversary's ability to conduct their operations and achieve their desired outcomes.

SOCs Are Challenged Like Never Before

Modern security threats are evolving at a faster pace than security technologies. While well-funded threat actors are investing in new tools like machine learning, automation, and artificial intelligence, SOCs built around legacy security information and event management (SIEM) fail to provide a flexible and scalable solution that keeps pace with digital transformation, cloud initiatives, and advanced attack campaigns.

Challenges such as noisy false positives, event storage (volume and cost), poor investigation workflows combined with the adoption of hybrid and multicloud architectures and the proliferation of devices and endpoints can overwhelm security analysts struggling to identify, manage, and remediate critical threats.

[1] *Nation States, Cyberconflict and the Web of Profit*, HP Wolf Security, April 8, 2021, https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/.

Furthermore, the cost to maintain SIEMs extends beyond the initial investment, including infrastructure and personnel who have to continually tune and optimize SIEM functionality.

Challenges from legacy SOC environments can include:

- Lack of visibility and context
- Increased complexity of investigations
- Alert fatigue and "noise" from a high volume of low-fidelity alerts generated by security controls
- Lack of interoperability of systems
- Lack of automation and orchestration
- Inability to collect, process, and contextualize threat intelligence data

By 2024,

80%

of all modern SOCs will leverage tools using machine learning, up from less than 10% today, but it won't significantly reduce industry-wide average attacker dwell time. –Gartner

What Is Needed? A Sea Change

The impacts from extensive breaches and work-from-home implementations have accelerated the need for newer, more nimble approaches to SOC operations and subsequent management. Combined with cloud and digital transformation initiatives and an expanded attack surface, organizations are ripe for SOC transformation.

One key reason is that perimeter-centric strategies for network security don't work anymore. Location of security infrastructure and systems extend beyond the traditional internet perimeter to the cloud and every connected device or endpoint—each requiring some level of visibility and control of respective activity and behavior to prevent compromise.

And as companies migrate more and more data resources and applications to the cloud, security issues such as lack of visibility, inability to maintain regulatory compliance, cloud app data theft, and inability to monitor data to and from cloud apps expose potential gaps in the cloud ecosystem.

4 Steps Toward Creating a Future-Forward SOC

Step 1: Auditing Your Environment Can Help Reduce the Security Risks Associated with Tool Sprawl

Leonardo da Vinci once said, "Simplicity is the ultimate sophistication." Due to acquisitions, mergers, and a lack of standardization for similar security products, many organizations are burdened with a disparate swath of tools across their security stack. To put it simply, having too many tools results in too many issues. And with resources both in cloud environments and on-prem, security IT teams are challenged with complete visibility of their attack surface.

For some teams, tool sprawl can begin by deploying a point solution to fix a specific issue. Unfortunately, this piecemeal approach, combined with managing numerous agents, can (ironically) leave networks even more vulnerable, exposing gaps due to issues from a lack of interoperability and improper configurations across the various solutions.

One of the first steps an organization can do to reduce the security impact of tool sprawl is to audit protected systems and entities. Identify precisely what is being protected and what is being prevented from happening. Is it intellectual property? Customers' personal information? By identifying as much as possible, whether software or physical assets, an organization can better prioritize protecting high-value and high-risk data.

As per NIST, "The Identify Function assists in developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs."[2]

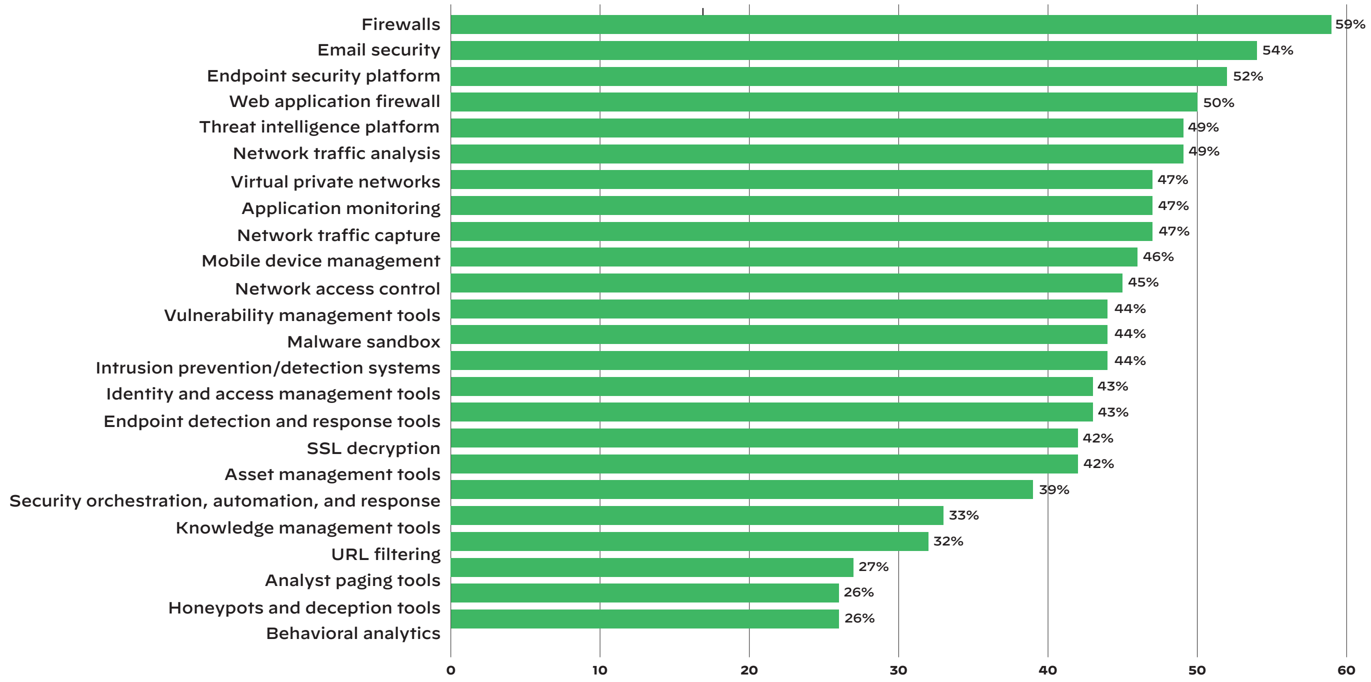
[2] "The Five Functions," NIST, May 12, 2021, https://www.nist.gov/cyberframework/online-learning/five-functions.

Examples of outcome categories within this function include:

- Identifying physical and software assets within the organization to establish the basis of an asset management program
- Identifying the business environment the organization supports, including the organization's role in the supply chain, and the organization's place in the critical infrastructure sector
- Identifying cybersecurity policies established within the organization to define the governance program as well as identifying legal and regulatory requirements regarding the cybersecurity capabilities of the organization
- Identifying asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basis for the organization's risk assessment
- Identifying a risk management strategy for the organization, including establishing risk tolerances
- Identifying a supply chain risk management strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks

Once an organization has a clear understanding of what is being protected, a logical next step is to identify solutions that can solve multiple needs if possible. As reported by ESG, in a 2019 survey of 406 IT and cybersecurity professionals (U.S. and Canada), 42% of respondents used between 10 and 25 security tools, with another 26% using between 26 and 50 security tools.[3] As things stand today, it is unnecessary to have sensors and enforcement happening across various tools, so organizations should consolidate where appropriate.

Which of the following tools are in use in your security operations team?



Base: 315 global decision-makers with involvement in security operations or incident response

Figure 1: Tools security operations pros use. A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

[3] *ESG Research Report: The rise of cloud-based security analytics and operations technologies*, Enterprise Strategy Group, December 23, 2019, https://research.esg-global.com/reportaction/Cloud-BasedSecurityAnalytics2019/Marketing.

Step 2: Automate Workflows

Security leaders must consider whether a tool requires a human to configure or run. Must an expert interpret or triage the result? Are people needed to test things? Security leaders can identify repeatable, low-level tasks that can work with human decision making to help accelerate incident investigations. While advancements in machine learning and artificial intelligence hold great promise, retaining the human element for knowledge transfer in either direction is imperative to achieve optimal outcomes for a smooth SOC transformation.

With too many manual processes involved in security operations and incident response (IR), including numerous threat feeds to monitor, investing in automation capabilities such as those in a SOAR solution can help orchestrate actions across the product stack for faster and more scalable IR.

Manual Alert Investigations Plague Teams

One area that is a continued sticking point for SOC teams is managing the number of alerts. Deploying solutions that can automate a range of tasks, decisions, and workflow associated with alert triage (alert prioritization/ranking, causal event correlation, and enrichment) can help streamline investigations.

1 – 5 Year Prediction on Automation Takeaways

New SOC operations can start using automation from day one, while more established organizations will have to re-tool and figure out where the move to automation can begin. This is a good three-year goal for an established organization: to move 50% of SOC work into the hands of automation. By year five, most SOC teams can be closer to 75% of activities automated yet continue to rely on human engineers for other activities like threat hunting.

Even after deploying a SIEM, or other solutions for better security insights and visibility, SOC teams are often flooded with low-fidelity alerts generated by their security controls. A 2019 survey of CISOs reported that "over 41% see more than 10,000 and that some claim to see more than 500,000 alerts daily." The same report noted that respondents revealed only 24% of investigated alerts were considered legitimate, down from 34% in 2018. The report also observed a substantial drop in the number of legitimate alerts that were in fact remediated—from 51% in 2018 to 43% in 2019.[4]

As one would expect, these types of numbers are not sustainable. The overwhelming number of false positives creating "noise" is often a result of a combination of poorly tuned algorithms, legacy detection tools, and/or configuration errors. These issues, combined with a lack of correlation from disparate tools and operations often done in silos, don't always enable consolidation of event data. Even the use of SIEM or log management tools requires tuning or customization to accurately correlate alerts. What further muddies the waters is that even though tools may trigger alerts, they are not necessarily malicious. As such, many low-fidelity alerts go ignored.

Step 3: Augment People with ML-Driven Intelligence

A key component in a modern SOC transformation is to ensure that security teams are leveraging machine learning to its full potential to augment and complement humans in security. Advanced analytics and AI can significantly reduce the amount of time that teams spend processing massive amounts of data in the enterprise to come up with critical security insights. By automatically detecting anomalous patterns across multiple data sources and automatically providing alerts with context, machine learning today can deliver on its promise of speeding investigations and removing blind spots in the enterprise.

This works by training machine-learning models, using them to detect patterns among and across the data, and then testing and refining the processes. ML techniques can gather, integrate, and analyze data and interrogate the data to reduce the amount of time and knowledge needed for a human to perform these tasks. This also minimizes the challenge for a SOC team trying to find threat context and evidence across multiple layers of security that are embedded in data.

Supervised machine-learning techniques can be used to fingerprint devices, such as desktop computers, mail servers, or file servers, and then learn the behavior of different types of devices and detect anomalous behavior. The promise of machine learning is having the ability to determine causal inferences around what is happening in an environment and letting the software direct next steps instead of relying on human interaction. For instance, flagging "bad" actions based purely on behavior and interactions within the joined datasets, so it can then propagate a decision to the rest of the network with explicit instructions such as instructing an agent to contain it or a firewall not to communicate with it.

[4] *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*, Cisco, March 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

At a high level, machine-learning techniques can:

- **Integrate**–Enable the data to tell a story about what is happening
- **Analyze**–Extract insights about the problem space and make predictions
- **Automate**–Accelerate human decision making, automate system-level action, workflows, and decision making

Step 4: Optimize Security Teams

Beyond investing in security solutions and tools, the most important factor in any successful SOC will remain the human element. While machine learning and automation will undoubtedly improve outcomes like response times, accuracy, and remediation overall—especially for low-level, repetitive tasks—attracting, training, and retaining security personnel, including engineers, analysts, and architects, needs to be baked into any cohesive SOC transformation strategy. By leveraging automation technologies, organizations can be more efficient at protecting the business at hand.

According to the Bureau of Labor Statistics, the number of individuals employed within the cybersecurity sector is slated to grow by 31% between 2019 and 2029.[5] Additionally, the National Center for Education Statistics (NCES) shows the number of new cybersecurity programs has increased by 33% while cybersecurity job postings have grown by 94% in the past six years.[6]

In concert with filling critical roles is adopting cybersecurity awareness training to ensure employees, contractors, and in some cases, partners, are well-versed in helping to prevent breaches. Stolen credentials, phishing attacks, and social engineering require people to execute campaigns, so building a cyber-savvy team holds long-term value. As the noted cryptographer and computer security professional Bruce Schneier said, "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

SOCs Can Come in Many Flavors

At Palo Alto Networks, our SOC story is highly optimized in that we actively chose to break away from the traditional four-tier SOC approach, ranging from Tier 1 analysts who monitor, prioritize, and investigate SIEM alerts to Tier 4 SOC managers responsible for recruitment, security strategy, and reporting to management. Taking more of a hybrid approach, the PANW SOC team follows this general philosophy:

- Staff the SOC with 80% of people who have previous SOC experience
- Cross-train the SOC team in all domains, including alert triage, incident response, threat hunting, and others
- Provide a well-funded annual training budget for all analysts

Our rationale is that we can:

- Maintain a nimble team, able to pivot between responsibilities (and tiers)
- Support business continuity
- Provide a more engaging atmosphere and reduce staff burnout
- Promote an environment of continuous learning
- Provide greater coverage with less staff by relying on the right technology to get the job done

[5] "Occupational Outlook Handbook, Information Security Analysts," U.S. Bureau of Labor Statistics, April 9, 2021, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[6] "CISO Benchmark Study, Cisco, March 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

ASM, SOAR, and XDR: The Bedrocks for SOC Transformation

Laying a foundation to build a resilient and effective SOC starts with taking the above four steps and considering the following three technology "keys" to help inform your security operations strategy.

Key 1: ASM—Power Up Your Risk Management Function by Understanding Your Attack Surface

One foundational component of a SOC transformation is to have a strong risk management function. Identifying the "things" you are trying to protect and prevent from being attacked is a logical segue into a risk management process that establishes the context for a risk management plan or strategy, whether basic or more robust. By starting with *identification*, the ability to prioritize what's at risk makes it easier to analyze what it would take to actually mitigate each risk.

A critical step to informing any risk management function is to have a clear understanding of one's attack surface—you can't protect what you can't see.

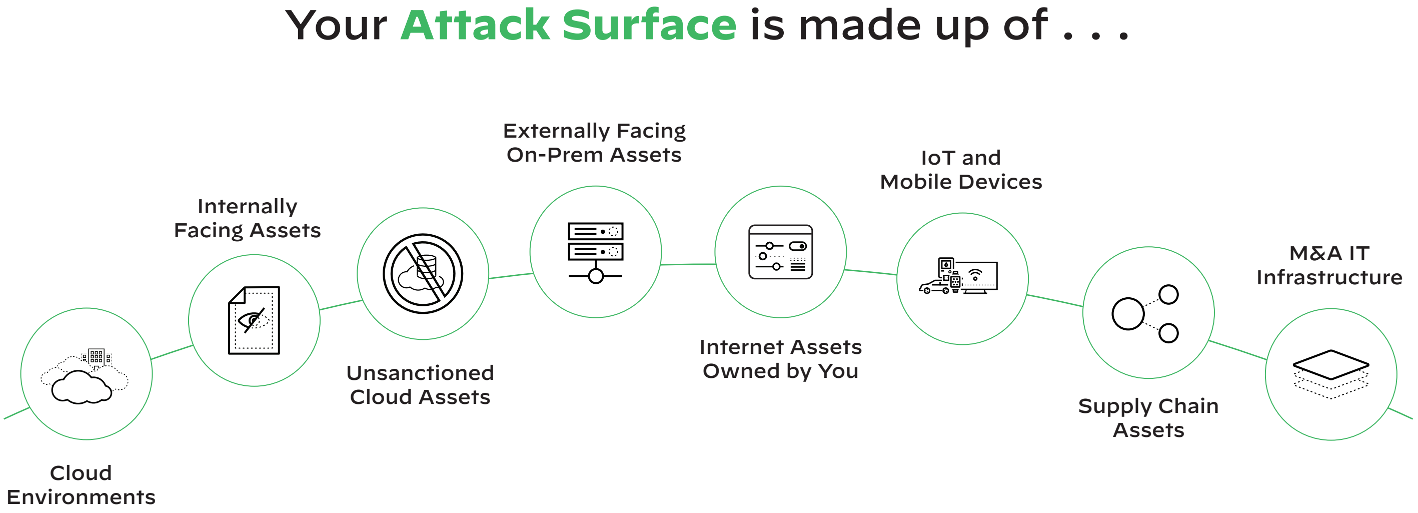

Your Attack Surface is made up of . . .
Cloud Environments
Internally Facing Assets
Unsanctioned Cloud Assets
Externally Facing On-Prem Assets
Internet Assets Owned by You
IoT and Mobile Devices
Supply Chain Assets
M&A IT Infrastructure

Figure 2: Components of the attack surface

Defined by SANS Institute:

> Attack surface management (ASM) "is an emerging category of solutions that aims to help organizations address this challenge by providing an external perspective of an organization's attack surface. An organization's attack surface is made up of all internet-accessible hardware, software, SaaS and cloud assets that are discoverable by an attacker. In short, your attack surface is any external asset that an adversary could discover, attack, and use to gain a foothold into your environment."[7]

SANS lists some common use cases for adoption of an ASM solution, including:

- Identification of external gaps in visibility
- Discovery of unknown assets and shadow IT
- Attack surface risk management
- Risk-based vulnerability prioritization
- Assessment of M&A and subsidiary risk

[7] Pierre Lidome, "The SANS Guide to Evaluating Attack Surface Management," SANS Institute, October 26, 2020, https://www.sans.org/reading-room/whitepapers/analyst/guide-evaluating-attack-surface-management-39905.

Yet, whether one chooses to deploy ASM solutions or perform proactive assessments like penetration testing or vulnerability scanning, what is clear is the need to identify both product and operational requirements to determine the best fit. Both product and operational requirements can include functionality, feature/s, capability, and evaluation criteria to help summarize the features and capabilities you might expect in an ASM solution or tool.

In their recent report, "2021 Cortex Xpanse Attack Surface Threat Report: Lessons in Attack Surface Management from Leading Global Enterprises," Palo Alto Networks outlined some key findings from their research of the public-facing internet attack surfaces of some of the world's largest businesses. From January to March, their team monitored scans of 50 million IP addresses associated with 50 global enterprises to understand how quickly adversaries can identify vulnerable systems for fast exploitation.

One interesting discovery was that nearly one in three vulnerabilities they uncovered were due to issues with the Remote Desktop Protocol (RDP), which has surged in use since early 2020 as enterprises expedited moves to the cloud to support remote workers affected by new WFH protocols due to the COVID-19 pandemic. Other findings include:

- **Adversaries work nonstop**. In a game of never-ending "cat and mouse," threat actors were found to conduct a new scan once every hour, whereas global enterprises can take weeks.
- **Adversaries jump on new vulnerabilities**. Attackers began scanning within 15 minutes following announcements of new Common Vulnerabilities and Exposures (CVE) released between January and March and launched scans within five minutes of the Microsoft Exchange Server zero-day security update.
- **Vulnerable systems abound**. Cortex® Xpanse™ discovered that, on average, global enterprises present a new serious exposure every 12 hours, or twice daily. Issues included insecure remote access (RDP, Telnet, SNMP, VNC, etc.), database servers, and exposures to zero-day vulnerabilities in products such as Microsoft Exchange Server and F5 load balancers.
- **Cloud comprised the most critical security concerns**. Cloud footprints were responsible for 79% of the most critical security issues found in global enterprises, reiterating the inherent risk of cloud-hosted/based services, compared to 21% for on-premises.

Takeaway: *Advancements in scanning technologies allow attackers to locate attack vectors quickly and easily, revealing abandoned, rogue, or misconfigured assets that can become backdoors for compromise. Deploying an attack surface management solution can provide a continuous assessment of an organization's external attack surface.*

Key 2: SOAR—Orchestrating Across Your Product Stack for Efficient Incident Response

Gartner defines security orchestration, automation, and response (SOAR) as "solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format."[8] Workflows can be orchestrated via integrations with other technologies and automated to achieve desired outcomes, such as:

- Incident alert triage
- Threat qualification
- Incident response
- Threat intel curation and management
- Compliance monitoring and management

When it comes to SOAR, solutions running a playbook outlining automated response workflows may come to mind, yet an effective SOAR strategy goes beyond just leveraging automation to streamline and eliminate manual tasks. A comprehensive SOAR platform that addresses all aspects of incident management needs to provide comprehensive out-of-the-box integrations of commonly used tools in the SOC, best practice playbooks to aid in automating workflows, as well as integrated case management and real-time collaboration to enable cross-team incident investigation.

[8] Toby Bussa et al., *Market Guide for Security Orchestration, Automation and Response Solutions*, Gartner, 21 September 2020, https://www.gartner.com/en/documents/3990720-market-guide-for-security-orchestration-automation-and-r.

Last but not least, the ability to serve as a central repository for threat intelligence (both internal and external) enables automated correlation between indicators, incidents, and intel, so security analysts and incident responders get enriched strategic intelligence for added insight into threat actors and attack techniques.

SOAR platforms continue to build toward becoming the control plane for the modern SOC environment, with the potential of becoming the control plane for various security operations functions. To achieve this end, SOAR platforms are starting to integrate threat intelligence, vulnerability management, etc., directly into the platform and expanding automation to use cases beyond the SOC. Leading security vendors are also embedding SOAR and incident management capabilities in their products, which are preprogrammed and optimized for the specific technology.[9]

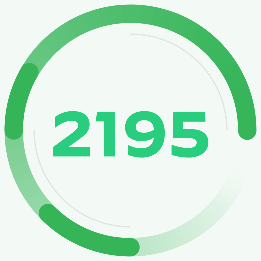
How a Security Company Automates Security

Cortex® XSOAR is leveraged within the Palo Alto Network SOC to minimize the repetitive and time-consuming tasks discussed in the above sections. Below is a snapshot of top automation "time savers'' for the month of February 2021.

Automation Type	Times Ran	Hours Saved
Artifact Enrichment	1195	697.08
De-Dupe	12744	1062
Email User	822	342.5
Password Reset	4	1.67
GCP Remediation	34	17
Other Jobs*	*	74.73

Repetitive, tedious SOC work that nobody wants to do

Total hours saved in February 2021



XSOAR automates the workload of 13.72 FTEs

*PhishMe metrics, RSS feed job, content update job, hunting assignments and metrics, daily monitoring ticket creation, and JIRA ticket pull

Figure 3: Top automation time savers

***Takeaway:** At the heart of any SOAR solution is the ability to set priorities and build streamlined workflows for security events that require minimal human involvement. Improved efficiencies are the result of a SOAR platform that can automate processes, as well as provide a single platform for minimizing complex incident investigations.*

[9] Bussa et al., Market Guide for SOAR, Gartner.

Key 3: XDR—the Next Logical Evolution of EDR

The term "XDR," short for "extended detection and response," was coined by Nir Zuk, CTO and co-founder of Palo Alto Networks in 2018. The basic reason for creating XDR was to stop attacks more efficiently, detect attacker techniques and tactics that cannot be prevented, and help SOC teams better respond to threats that require investigation. The vision is to provide a seamless approach to pulling disparate telemetry together from multiple (and in some cases, complementary) sources, including EDR, network traffic analysis (NTA), user and entity behavior analytics (UEBA), and Indicators of Compromise (IoCs).

XDR lets security teams stop attacks more efficiently and effectively by consolidating siloed tools, streamlining processes, and providing greater visibility for threat detection and investigations. Teams can eliminate blind spots, reduce investigation times, and ultimately improve security outcomes using XDR. And with XDR's ability to stop attack sequences at critical stages such as execution—before persistence techniques result in broader lateral damage—security teams finally have a solution to "head attacks off at the pass."

Forrester defines XDR as:

> The evolution of endpoint detection and response (EDR), which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management (IAM), cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.[10]

As an evolution of existing threat detection and response solutions, XDR includes features such as:

- Integrated threat intelligence
- Network analysis
- Machine learning-based detection
- Investigation response orchestration
- Dynamic deployment
- Integrated sandbox (WildFire®) capabilities

Factors driving the adoption of XDR include simplified visualization of complex attacks across the kill chain, more robust automation, advanced analytics, and machine learning. XDR's value is gaining momentum by the need in the market for tighter third-party integrations, better analytics, and faster response capabilities—especially when one considers that organizations may use up to 45 security tools on average while responding to an incident requires coordination across approximately 19 tools.[11]

XDR combines SIEM-like features of alert integration, normalization, and correlation with SOAR-like automated investigation and remediation.

XDR Fills the Detection and Response Void

Up until XDR, correlating telemetry from endpoints with other event data was an exercise in sifting through large volumes of data and false positives cluttering analysts' dashboards. Stitching disparate events together is resource-intensive and dependent on seasoned analysts to determine if alert escalations are warranted. As a result, SOC teams could find themselves wasting time to verify the accuracy of low-fidelity alerts while compromising the time needed to investigate legitimate alerts.

Impeded by this nonstop version of security "whack-a-mole" and an increase in attack sophistication and frequency, forward-thinking security organizations are beginning to position themselves to take advantage of all the efficiencies gained from an XDR approach to security architecture.

[10] Allie Mellen, "XDR Defined: Giving Meaning to Extended Detection and Response," Forrester, April 2021, https://go.forrester.com/blogs/xdr-defined-giving-meaning-to-extended-detection-and-response/.

[11] Mellen, "XDR Defined," Forrester.

According to Forrester analyst Allie Mellen, who covers SecOps, "XDR and SIEM are not converging but colliding."[12] In a recent blog post, Mellen explains further:

> "XDR will compete head to head with security analytics platforms (and SIEMs) for threat detection, investigation, response, and hunting. Security analytics platforms have over a decade of experience in data aggregation; they apply to these challenges but have yet to provide incident response capabilities that are sufficient at enterprise scale, forcing enterprises to prioritize alternate solutions. XDR is rising to fill that void through a distinctly different approach anchored in endpoint and optimization."
>
> "The core difference between XDR and the SIEM is that XDR detections remain anchored in endpoint detections, as opposed to taking the nebulous approach of applying security analytics to a large set of data. As XDR evolves, expect the vendor definition of endpoint to evolve as well based on where the attacker target is, regardless of if it takes the form of a laptop, workstation, mobile device, or the cloud."[13]

Securing the endpoint is not enough. Organizations must unify it with cloud and network data through a single source of truth driven by comprehensive data and deep analytics.

***Takeaway:** XDR is a viable alternative approach to SIEM solutions by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments which is where enterprise data is moving.*

Cortex XDR, Cortex XSOAR, and Cortex Xpanse: Better Together, End to End

Let's face it. We understand most of our customers and potential customers don't want to be systems integrators. Nor do they want to "run ragged" performing manual, repetitive tasks. An array of siloed tools requires massive time and costs to maintain. Numerous and disparate solutions can limit security outcomes by introducing complexity and fractured visibility for the analytics required by modern SOCs.

And while we can't add hours to the day, we can help our customers optimize, reduce TCO, and integrate with more third-party tools than any other security provider for next-level operations. Beyond these results is the ability to equip the security analyst with the tools they need to keep their data safe so they can focus more on what matters and less on mundane tasks.

You can begin or accelerate your SOC journey by deploying the Cortex suite of products: Cortex XDR, Cortex XSOAR, and Cortex Xpanse, which seamlessly work together as a force multiplier across your security operations. Immediate high-level advantages include:

Cortex® XDR™: The ability to stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts, providing detection and response that focuses on incidents by automating evidence gathering, groups of alerts associated, putting those alerts into a timeline, and revealing the root cause to speed triage and investigations for analysts of all skill levels.

Cortex® XSOAR: A single platform for end-to-end incident and security operational process lifecycle management. Security teams of all sizes can leverage the extensive 725+ prebuilt integration content packs, robust security-focused case management with real-time collaboration to orchestrate, automate, speed incident response and any security workflow or security process across their environment. In addition, with integrated threat intel management, security teams get a central threat library, the ability to automatically map threat information to incidents, and operationalize threat intelligence with automation.

Cortex® Xpanse™: A complete and accurate inventory of an organization's global, internet-facing cloud assets and misconfigurations to continuously discover, evaluate, and mitigate an external attack surface, flag risky communications, evaluate supplier risk, or assess the security of M&A targets.

[12] Mellen, "XDR Defined," Forrester.

[13] Mellen, "XDR Defined," Forrester.

While each standalone product brings its own unique features and benefits, when combined, the positive results increase exponentially. These three products help lower the risk and impact from breaches with a comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities, bar none.

With end-to-end native integration and interoperability, SOC teams can close the loop on threats with continual synergies across the Cortex ecosystem. All three products work in concert to monitor the threat landscape and provide the most robust detection, response, and investigation capabilities:

- Cortex XDR and Cortex Xpanse provide the ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network.
- Cortex XDR and Cortex Xpanse leverage Cortex XSOAR for full orchestration, automation, and response capabilities.
- Cortex XSOAR leverages Cortex XDR and Cortex Xpanse to provide high-fidelity detections and alerts to drive orchestrated workflows.

Begin Your SOC Transformation Today

Driven by innovation to protect and defend our customers' most valuable resources, Palo Alto Networks is committed to bringing the newest and most advanced security solutions to market. We invite you to take a look at our solutions, reach out, and talk to us. We're here to help you learn more, do more, and secure more.

Visit our product pages for more information:

- Cortex Xpanse
- Cortex XSOAR
- Cortex XDR

Interested in scheduling a demo? Get started today.

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