How to Plan for Tomorrow's SOC, Today

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

Table of Contents

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 tools like machine learning (ML), automation, and artificial intelligence (AI). SOCs built around legacy security information and event management (SIEM) weren't necessarily designed for the purpose of accurate detection. As such, they aren't effective in leveraging ML for detection engineering that keeps pace with digital transformation, cloud initiatives, and advanced attack campaigns.

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
- Lack of interoperability of systems
- Lack of automation and orchestration
- Inability to collect, process, and contextualize threat intelligence data
- SOC is often disconnected from the cloud

5 Steps Toward Creating a Future-Forward SOC

Step 1: Transform the Manual SOC Model

The manual SOC model, whether delivered as on-premises software or to the cloud, was built around the human analyst. SOC analysts pored through hundreds of alerts per day, triaged manually by collecting contextual data, and spent the bulk of their time on false positives and manual effort. As alert volumes grew and data became harder to integrate from more systems, the human-led approach broke down. Instead, the modern way to scale an effective SOC is with automation as the foundation and with analysts working on a small set of high-risk incidents.

Just as flying a commercial airplane no longer requires constant, hands-on control by the pilot, an automation-led SOC handles the bulk of low-risk, repeated alerts, analysis tasks, and mitigations. This frees the analysts to work on urgent, high-impact incidents while the underlying platform autopilots the SOC to safe outcomes, learning from each activity and offering information and effective recommendations to the captain at the controls. This is our vision for the autonomous SOC.

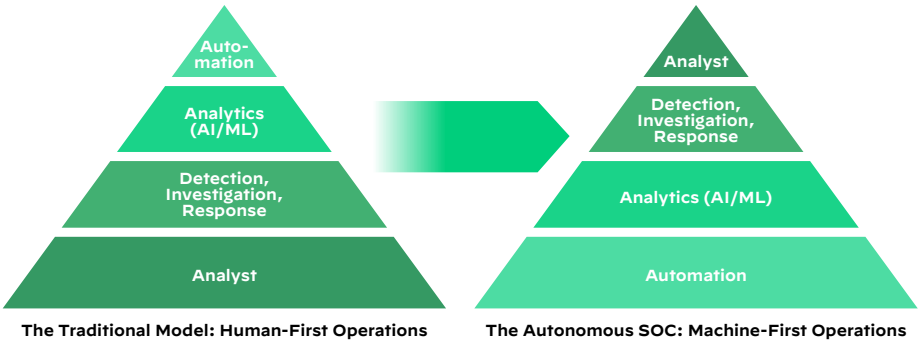

Figure 1: Human-first operations vs. machine-first operations

Ultimately, better data modeling and integration combined with automated analytics and detection ease the burden on security engineers who no longer need to build custom correlation rules to integrate data and detect threats. Unlike legacy security operations, the modern SOC leads with data science applied to massive data sets rather than only relying on human judgment and rules designed to catch yesterday's threats.

The modern SOC must be built with a different approach to solving modern threats by utilizing new architectures, data utilization, processes, and continuously updated knowledge of the threat landscape, such as:

- Broad and automated data integration, analysis, and triage
- Unified workflows that enable analysts to be productive
- Embedded intelligence and automated response that can block attacks with minimal analyst assistance

Step 2: 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-premises, security IT teams are challenged with complete visibility of their attack surface. How could you expect to know your attack surface if you do not have a clear picture of which cloud providers are connected, the services from those cloud service providers (CSPs) that are being utilized, and ultimately the assets that have access back to the on-premises environments?

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 take 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.

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 Enterprise Strategy Group (ESG) in a 2022 survey of 280 IT and cybersecurity professionals (from the US, Canada, Europe, Central/South America, Africa, Asia, and Australia), 22% report managing the complexity of too many disconnected point tools for cybersecurity a challenge, with 66% of respondents using 25 or fewer security products.[1] As things stand today, it is unnecessary to have sensors and enforcement happening across various tools, so organizations should consolidate where appropriate.

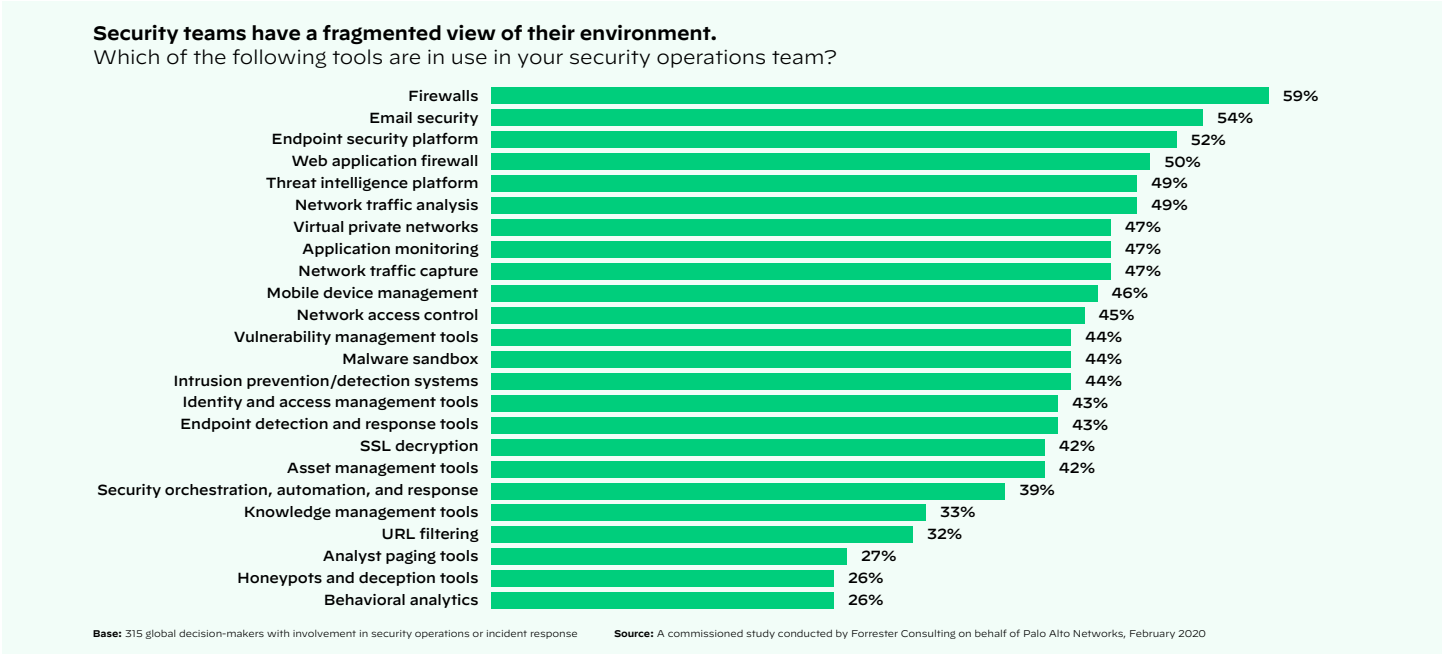

Figure 2: Tools security operations pros use, self-reported to ESG

1. "Cybersecurity Process and Technology Survey," ESG, June 2022, https://research.esg-global.com/reportaction/ESG-ISSACybersecurityProcessAndTechnologySurveyCSR/Toc.

Step 3: Automate Workflows

Security leaders must consider whether a tool requires a human to configure or run it. 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 crucial to achieving 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 security orchestration, automation, and response (SOAR) solution can help orchestrate actions across the product stack for faster and more-scalable IR.

How Automation Makes Life Easier in the SOC (and NOC)

- **Accelerate incident response**: By replacing low-level manual tasks with corresponding automations, security automation can shave off large chunks from incident response times while also improving accuracy and analyst satisfaction.
- **Standardize and scale processes**: Through stepwise, replicable workflows, security automation can help standardize incident enrichment and response processes that increase the baseline quality of response and is primed for scale.
- **Unify security infrastructures**: A SOAR platform like Cortex XSOAR can act as a connective fabric that runs through previously disparate security products, providing analysts with a central console from which to action incident response.
- **Increase analyst productivity**: Since low-level tasks are automated and processes are standardized, analysts can spend their time making more important decisions and charting future security improvements rather than getting mired in grunt work.
- **Leverage existing investments**: By automating repeatable actions and minimizing console switching, security orchestration enables teams to coordinate among multiple products easily and extract more value from existing security investments.
- **Streamline incident handling**: By applying automation to incident ticket management via integrations with key ITSM vendors like ServiceNow, Jira, and Remedy, as well as communication tools such as Slack, security teams can speed incident handling and closure. Incidents can also be distributed automatically to the respective stakeholders based on predefined incident types.
- **Improve overall security posture**: The sum of all aforementioned benefits is an overall improvement of the organization's security posture and a corresponding reduction in security and business risk.

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.

Step 4: 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 time 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 ML 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 ML techniques can be used to read the digital markers from 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.

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 and automate system-level action, workflows, and decision-making.

Step 5: 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, must be baked into any cohesive SOC transformation strategy. By leveraging automation technologies, organizations can be more efficient at protecting the business.

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.[2] 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.[3]

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 says, "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 Palo Alto Networks SOC team follows this general philosophy:

- 80% of the SOC staff has 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.

2. "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.
3. "CISO Benchmark Study," Cisco, March 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

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

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

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

One foundational component of a SOC transformation is a strong risk management function. Identifying what you are trying to protect and prevent from being attacked is a logical first step in a risk management process that establishes the context for a risk management plan or strategy, whether basic or more robust. By starting with identification, you can prioritize what's at risk and analyze what it would take to 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.

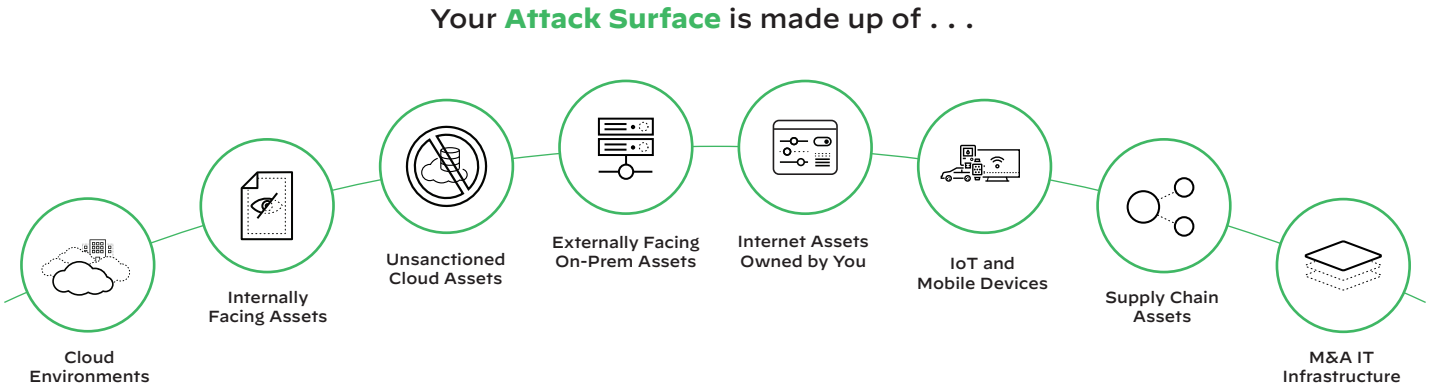

Figure 3: Components of the attack surface

Yet, whether one chooses to deploy attack surface management (ASM) solutions or perform proactive assessments like penetration testing or vulnerability scanning, there is clearly a 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 the *2021 Cortex Xpanse Attack Surface Threat Report*, we outlined some key findings from our research of the public-facing internet attack surfaces of some of the world's largest businesses. From January to March, the Cortex Xpanse research 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),[4] which has surged in use since early 2020 as enterprises expedited moves to the cloud to support remote workers affected by new work-from-home 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.[5]
- **Adversaries jump on new vulnerabilities**. Attackers began scanning within 15 minutes following announcements of new Common Vulnerabilities and Exposures (CVEs) released between January and March and launched scans within five minutes of the Microsoft Exchange Server zero-day security update.[6]

4. *2021 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, May 2021, https://www.paloaltonetworks.com/engage/cortex-xpanse-general/xpanse-attack-surface-threat-report-2021.
5. Ibid.
6. Ibid.

- **Vulnerable systems abound**. 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.[7]
- **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.[8]

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

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. 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

A comprehensive SOAR solution 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.

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 solutions continue to build toward becoming the control plane for the modern SOC environment, potentially 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 into their products, which are preprogrammed and optimized for the specific technology.

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, orchestrating across the entire product stack of a SOC.

7. *Cortex Xpanse Attack Surface Threat Report, 2021.*
8. Ibid.

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	Count	Analyst Hours Saved
Artifact Enrichment	2.498	1,457
Dedupe	10,063	821
Email User	464	193
Re-image Machine	8	4
Password Reset	8	4
100% End-to-End Automated Workflows	57	29
Other Jobs*	*	133

Repetitive, tedious SOC work that nobody wants to do

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

XSOAR automates the workload of 16.5 FTEs

Figure 4: Top automation time savers

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."

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 due to 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.[9]

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

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.

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 verifying 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.

Takeaway: Cortex XDR can be utilized in multiple permutations of SecOps architecture, providing enterprise threat detection and response with prevention capabilities that include EDR/EPP, particularly for organizations that do not require the full feature set of a SIEM. Cortex XDR can also be deployed with a SIEM to deliver EDR/EPP functionality, focused threat detection, response, and prevention.

9. *2020 Cyber Resilient Organization Report*, IBM Security, June 2020, https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.

Key 4: XSIAM—the AI-Driven SOC Platform to Accelerate Response and Outpace Threats

Security information and event management (SIEM) solutions were built to facilitate alert and log management but have relied heavily on human-driven detection and remediation with bolt-on analytics and automation only here and there. The SIEM category has served security operations for years with significant manual overhead and slow incremental improvement in security outcomes. Combating today's threats requires us to radically reimagine how we run cybersecurity in our organizations using AI.

With Cortex XSIAM, security professionals manage intelligence and automation while letting the intelligence and automation manage information and events. Imagine a world where security alerts from your infrastructure were organized and addressed automatically.

XSIAM is designed to be the center of SOC activity, augmenting SIEM and specialty products by unifying broad functionality into a holistic solution. XSIAM capabilities include data centralization, intelligent stitching, analytics-based detection, incident management, threat intelligence, automation, attack surface management, and more—all delivered within an intuitive, automation-first user experience.

Takeaway: Cortex XSIAM is the automation-first platform for the modern SOC, harnessing the power of machine intelligence to radically improve security outcomes and transform security operations. XSIAM customers can consolidate multiple products into a single coherent platform, cutting costs and improving analyst experience and productivity.

Cortex XSIAM, Cortex XDR, Cortex XSOAR, and Cortex Xpanse

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 be 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 security analysts 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 XSIAM, Cortex XDR, Cortex XSOAR, and Cortex Xpanse, which seamlessly work together as a force multiplier across your security operations. Immediate high-level advantages follow.

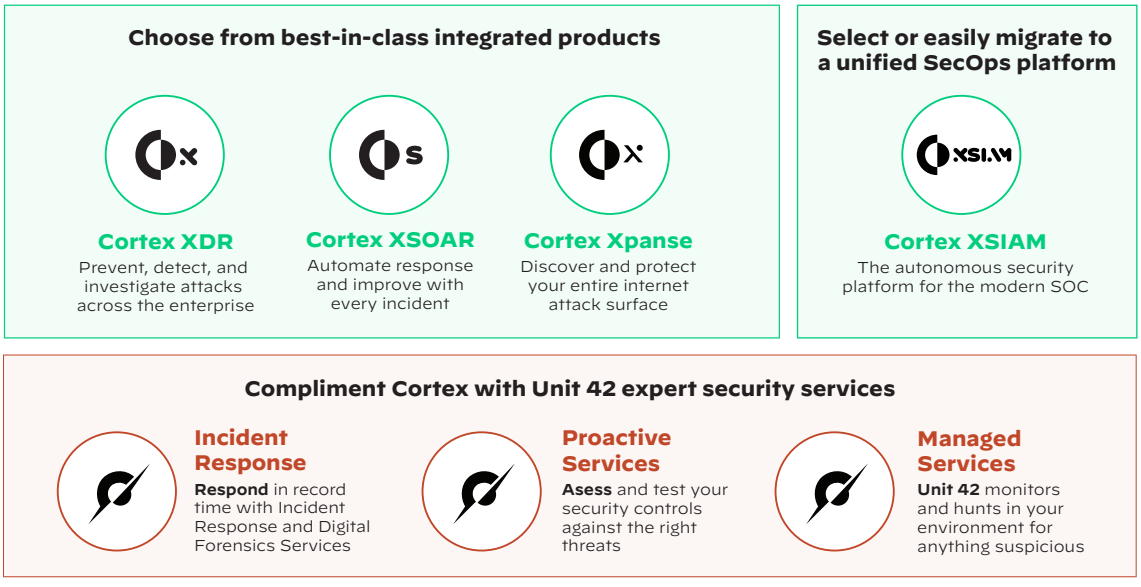

Figure 5: Palo Alto Networks solutions to help you create a future-forward SOC

Cortex XSIAM

Cortex® XSIAM™ natively integrates XDR, SOAR, threat intel, ASM, and SIEM capabilities to power the autonomous SOC. XSIAM (extended security intelligence and automation management) customers can consolidate multiple products into a single, coherent platform, cutting costs and improving analyst experience and productivity.

Cortex XDR

Cortex XDR® has the ability to stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts, providing detection and response that focus 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

Cortex® XSOAR™ is a single platform for end-to-end incident and security operational process lifecycle management. Security teams of all sizes can leverage the extensive 900+ prebuilt integration content packs and robust security-focused case management with real-time collaboration to orchestrate, automate, and 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 with the ability to automatically map threat information to incidents and operationalize threat intelligence with automation.

Cortex Xpanse

Cortex® Xpanse™ provides 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.

End to End Integration and Interoperability

SOC teams can close the loop on threats with continual synergies across the Cortex ecosystem:

- Cortex XSIAM unifies best-in-class functions, including EDR, XDR, SOAR, ASM, UEBA, TIP, ITDR, and SIEM. Using a security-specific data model and applying machine learning, XSIAM automates data integration, analysis, and triage to respond to most alerts, enabling analysts to focus on the incidents that require human intervention.
- Cortex XDR and Xpanse provide ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network.
- Cortex XDR and Xpanse leverage XSOAR for full orchestration, automation, and response capabilities.
- Cortex XSOAR leverages Cortex XDR and Xpanse to provide high-fidelity detections and alerts to drive orchestrated workflows.

Cortex: Reimagining SecOps to Stop Successful Attacks

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 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 pages for more information:

- Cortex Xpanse
- Cortex XSOAR
- Cortex XDR
- Cortex XSIAM
- Unit 42

Interested in scheduling a demo? Get started today.

Partner CTA

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