Redefining SecOps in the Era of AI

Making the Case for a Consolidated Platform Approach

Don't have a traditional security operations center yet still want similar outcomes? From continuous protection with uninterrupted monitoring to threat detection and prevention, having the ability to holistically organize and manage security operations is paramount for a healthy security posture.

In addition to increasing attack frequency and sophistication, attacks are becoming more costly, many driven by the surge in ransomware bolstered by rising cryptocurrency prices. Unfortunately, an attack can go undetected for a long time, leading to increased dwell times and further delaying investigation, mitigation, or remediation. While reasons for operational inefficiencies differ among organizations, many of them include:

- Limited visibility into their devices, applications, networks, and systems.
- Not knowing where all the exposed assets are and how to prioritize protecting them.
- Not understanding which tools to use and integrating them with the existing infrastructure.

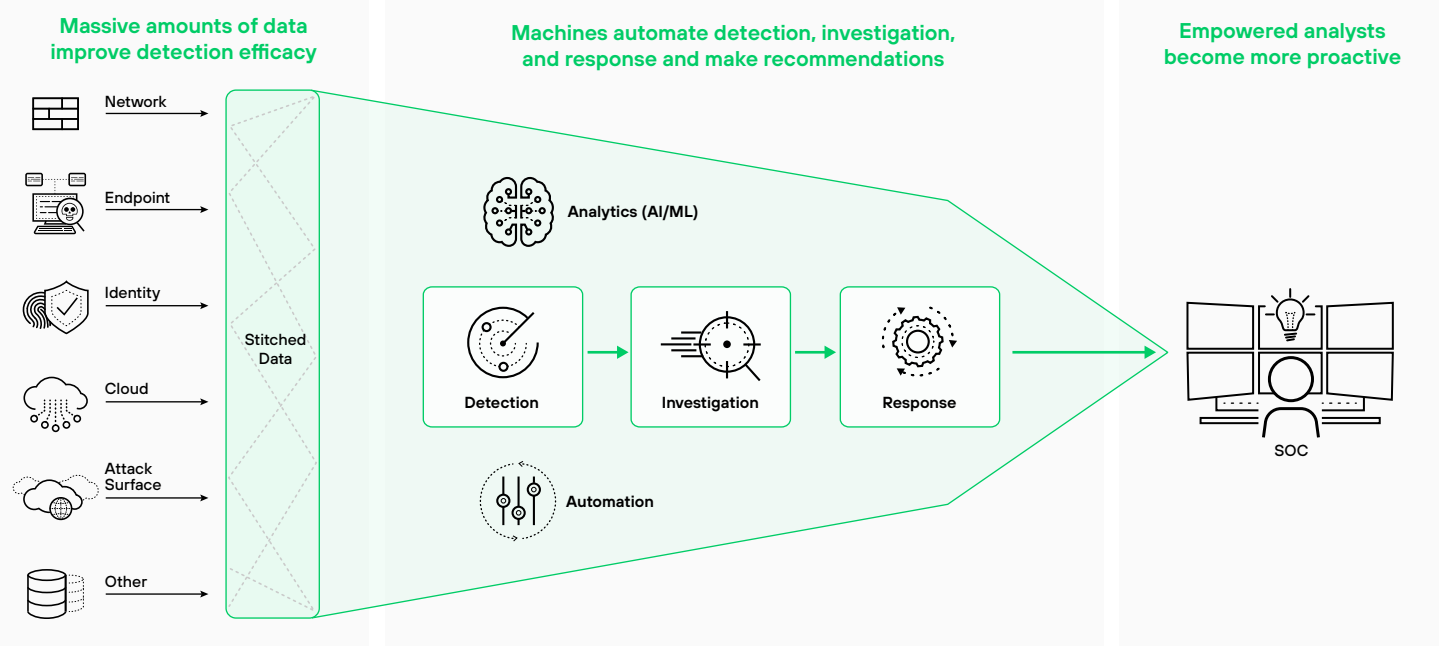

Figure 1: We must transform the SOC to be machine-led, human-empowered

The Cortex portfolio provides a unified solution, designed to empower security analysts to take control of their threat landscape. Backed by powerful machine learning (ML), data analytics, artificial intelligence (AI), and automation capabilities, Cortex provides SOC teams with the tools they need to protect their organizations.

Cortex Is a Holistic Ecosystem for Proactive Security Operations

A solution to address the above challenges is a suite of products that enables tighter control of security operations; a holistic ecosystem with a view of the security posture for targeted threat detection, behavioral monitoring, intelligence, response, asset discovery, and risk assessment—a virtual SOC that can be managed without dependencies on a physical location or assets.

You can now achieve this reality—*SOC virtualization*—with the Cortex® suite of products: Cortex XSIAM, Cortex XDR, Cortex Xpanse, and Cortex XSOAR, which seamlessly work together as a force multiplier across your security operations regardless of team size or scope.

Our Approach

While each product brings unique features and benefits, the positive results exponentially increase when combined. These four products help lower the risk and impact from breaches with a comprehensive product suite for **teams of any size**, with best-in-class detection, investigation, automation, and response capabilities, bar none.

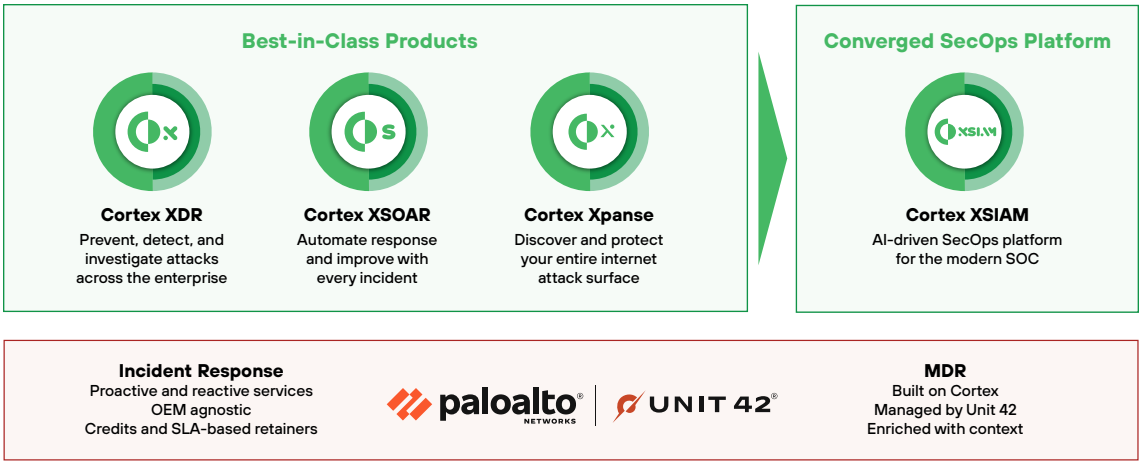

Figure 2: Unified architecture enriched with Unit 42 Threat Intelligence

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

- Cortex XSIAM is the AI-driven platform that transforms the SOC, harnessing the power of AI and automation to simplify operations, stop threats at scale, and accelerate incident remediation.
- Cortex XDR provides endpoint security and EDR to block sophisticated attacks using AI-driven analysis and a range of protection modules.
- 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.

Cortex XSIAM for an AI-Driven SecOps Platform

Cortex XSIAM® is the AI-driven platform that transforms the SOC, harnessing the power of AI and automation to simplify operations, stop threats at scale, and accelerate incident remediation. With XSIAM you can:

- Reduce risk and operational complexity by centralizing multiple products into a single, coherent platform purpose-built for security operations.
- Unify best-in-class security operations functions, including SIEM, EDR, XDR, SOAR, CDR, ASM, UEBA, and TIP.
- Centralize all of your security data and use AI models designed specifically for security.

- Automate data integration, analysis, and response actions, enabling analysts to focus on the incidents that matter.
- Easily add new data sources while an extended data model normalizes and correlates data for schema on-read data access via a streamlined data onboarding process.
- Automatically stitch together endpoint, network, cloud, identity, and other data so it can detect advanced threats with precision and simplify investigations with cross-data insights.
- Swiftly investigate incidents by providing a complete picture of every attack with intelligent alert grouping and root cause analysis. Embedded automation enriches alerts, responds to malicious activity, and closes low-risk alerts before they reach the queue—enabling analysts to focus on the few threats that require human intervention.

Cortex XSIAM is powering Palo Alto Networks own SOC and turning over a trillion events per month into a handful of analyst incidents per day. Unlike legacy SOC solutions, where operationalizing and optimizing the product is an exercise left to the customer, Cortex XSIAM benefits from continuous updates from the Palo Alto Networks Unit 42® research team.

Palo Alto Networks experts collect threat intel from more than 90,000 customers, update machine learning (ML) detection models, and automatically distribute the latest protections to Cortex XSIAM deployments. Insights from across the threat landscape help safeguard customers from the latest advanced and fast-moving threats. By fusing leading technology with shared intelligence and research, Palo Alto Networks shares the responsibility of protecting our customers' ongoing operations.

The AI-Driven Security Operations Platform

Cortex XSIAM puts the SOC in full control of enterprise security—from endpoint to cloud—by centralizing, stitching, and optimizing data, specifically for detecting and preventing security incidents. Cortex XSIAM uses artificial intelligence, which leverages thousands of mature ML data models designed to quickly and accurately identify malicious security events.

These models are built based on learned behavior from tens of thousands of environments, which help to differentiate between anomalous vs. malicious activities. This significantly reduces false positives and improves detection and prevention capabilities, stopping attacks before they become security incidents. Cortex XSIAM analytics provide technique-based intelligence, allowing multiple alerts to be stitched and grouped into a smaller number of incidents. These incidents are fully enriched with relevant context and are either resolved with automation or presented to an analyst with an appropriate severity classification (critical, high, low, etc.) that is defined leveraging an AI SmartScoring system.

CORTEX XSIAM®
BY PALO ALTO NETWORKS

A new design for security operations that:

- Redefines SOC architecture into an automation-first approach
- Unifies best-in-class SOC functions to improve analyst experience
- Consolidates multiple products into a single platform
- Extends the SOC to the cloud for complete visibility
- Increases analyst productivity by focusing on the incidents that matter

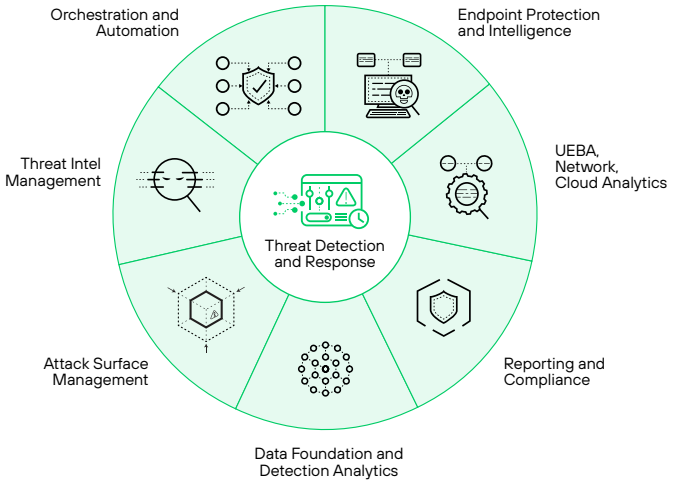

Figure 3: Cortex XSIAM

Key Benefits of Cortex XSIAM

Simplify Security Operations with a Converged Platform

The convergence of SOC capabilities, such as XDR, CDR, SOAR, ASM, and SIEM, into a single platform—with a single frontend and backend—is a game-changer for security operations. It eliminates the hassle of console switching, providing a streamlined experience. The platform offers broad integration support, making it easier to onboard various data sources without the need for extensive engineering and infrastructure work. This enables SOCs to seamlessly incorporate additional security-related data, enhancing their ability to analyze and detect security threats with greater precision. This empowers SOC teams with superior and simplified investigation, enabling them to identify and remediate threats faster and more effectively.

AI-Powered Defense to Stop Threats

Out-of-the-box AI models go beyond traditional methods, connecting events across various data sources and offering a comprehensive overview of incidents and risks in a single location. This empowers organizations to enhance their detection, analysis, and response capabilities. XSIAM identifies threats and anomalous activity across data sources, alerting analysts to potential threats for investigation and remediation. XSIAM seamlessly connects low-confidence events, transforming them into high-confidence incidents, enabling security teams to prevent, detect, and respond more efficiently.

Automated Operations to Accelerate SOC Outcomes

XSIAM uses native automation and built-in integrations for seamless orchestration and execution of tasks such as incident enrichment, threat analysis, and response actions. With hundreds of tried and tested content packs in the Cortex Marketplace, SOCs can optimize processes and interactions across their entire security program. By automating previously manual tasks, embedded automation saves time and effort in responding to incidents or managing risks such as attack surface exposures.

Moreover, users have the flexibility to add, customize, or modify automations according to their specific needs. The platform also features alert-specific playbooks that trigger automatically, ensuring security tasks are executed promptly, and risks are addressed, even before an analyst gets involved. Additionally, XSIAM learns from manual analyst actions and provides recommendations for future automation. This continuous learning process enhances the platform's ability to automatically resolve incidents, improving efficiency and accuracy over time.

Takeaway: Cortex XSIAM redefines security operations by centralizing and optimizing data across platforms—from cloud to endpoint—powered by AI and Palo Alto Networks vast threat intelligence. This convergence of technology not only streamlines SOC processes but significantly enhances threat detection and response capabilities, ensuring that organizations stay ahead of sophisticated cyberthreats.

Cortex XDR for Endpoint Protection and Extended Detection and Response

Cortex XDR® can stop attacks at the endpoint with a single agent that features:

- AI-driven local analysis and behavioral analysis continuously updated to defend against the latest attack techniques.
- A range of protection modules to protect against pre-execution and postexecution exploits.
- A suite of endpoint protection features such as Device Control, host firewall, and disk encryption.

Once you prevent everything you can at the endpoint, Cortex provides rapid detection and response that automates evidence gathering, groups alerts into incidents, and reveals the root cause to speed triage and investigations for analysts of all skill levels.

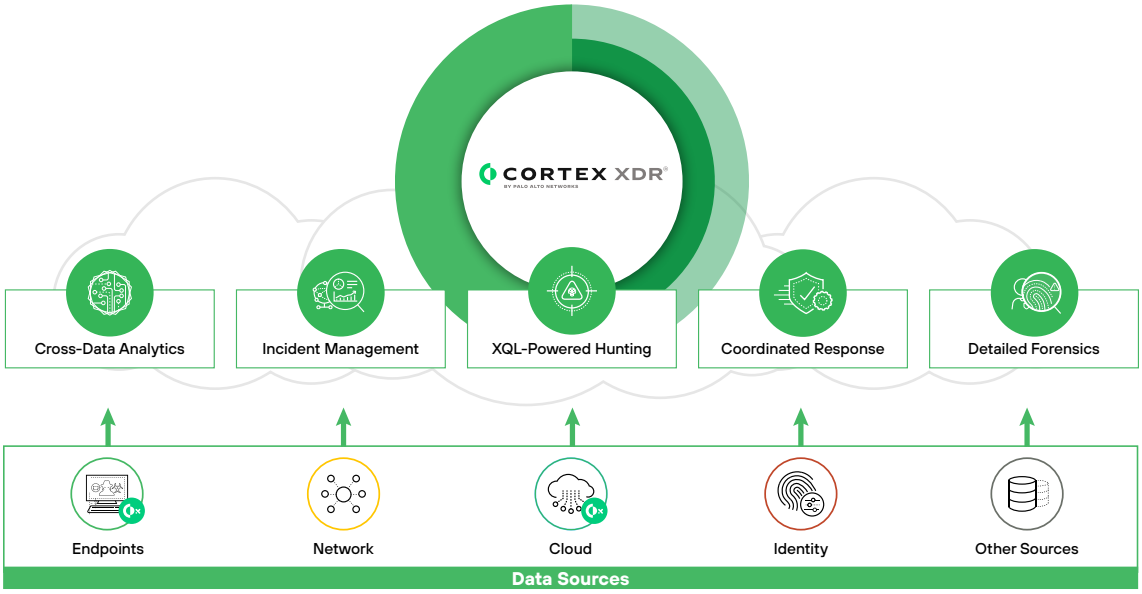

Figure 4: Faster detection and response with AI/ML analytics with Cortex XDR

XDR Fills the Detection and Response Void

Before 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 taking advantage of all the efficiencies gained from an XDR approach to security architecture.

According to Forrester analyst Allie Mellen, who covers SecOps, "XDR and SIEM are not converging but colliding."[1] In her 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."*[2]

1. Allie Mellen, "XDR Defined: Giving Meaning To Extended Detection And Response," Forrester, April 28, 2021.
2. Ibid.

Takeaway: XDR can outperform SIEM in threat detection, investigation, response, and hunting with an approach rooted in endpoint threat detection and response.

Cortex Xpanse for Complete, Accurate, and Continuously Updated Inventory of All Global Internet-Facing Assets

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 and evaluate supplier risk or assess the security of M&A targets.

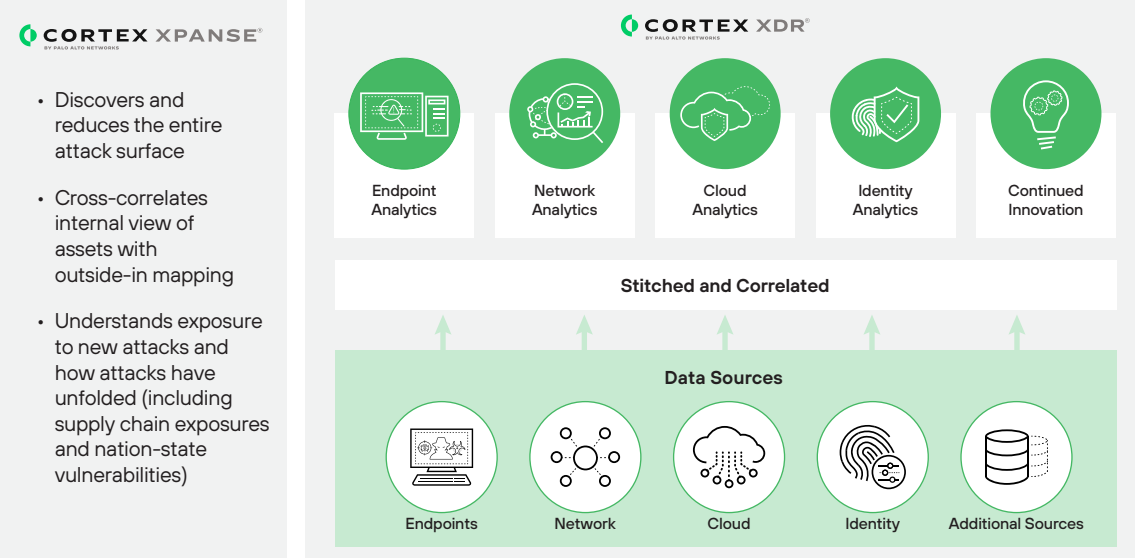

Figure 5: Ultimate visibility and detection across the internet attack surface, endpoints, cloud, and network

In our recent report, *Unit 42 Attack Surface Threat Report: Lessons in Attack Surface Risk*, we outlined some key findings from their research of the public-facing internet attack surfaces of some of the world's largest businesses. Unit 42 conducted a comprehensive analysis of public internet data, leveraging Palo Alto Networks Cortex Xpanse. Their report distills insights from several petabytes of data collected in 2023 to provide security leaders with a clear picture of the evolving global attack surface and what risks to look for in their environment.

Some findings in the report include:

- **Attack surface change inevitably leads to exposures.**
  Across industries, attack surfaces are always in a state of flux. The research indicates that, on average, an organization's attack surface has over 300 new services every month. These additions account for nearly 32% of new high or critical cloud exposures for organizations.[3]
- **Opportunities for lateral movement and data exfiltration are abundant.**
  Just three categories of exposures—IT and Networking Infrastructure, Business Operations Applications, and Remote Access Services—account for 73% of high-risk exposures across the organizations we studied and can be exploited for lateral movement and data exfiltration.[4]

3. *Unit 42 Attack Surface Threat Report: Lessons in Attack Surface Risk*, Palo Alto Networks, September 2024.
4. Ibid.

- **Critical IT and security services are dangerously exposed to the internet.** Over 23% of exposures involve critical IT and security infrastructure, opening doors to opportunistic attacks. These include vulnerabilities in application-layer protocols like SNMP, NetBIOS, PPTP, and internet-accessible administrative login pages of routers, firewalls, VPNs, and other core networking and security appliances.[5]

Understanding the Attack Surface

One foundational component of a SOC transformation is to have a strong continuous risk management function. Identifying the "things" you are trying to protect and identifying what is exposed that allows it to be 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.

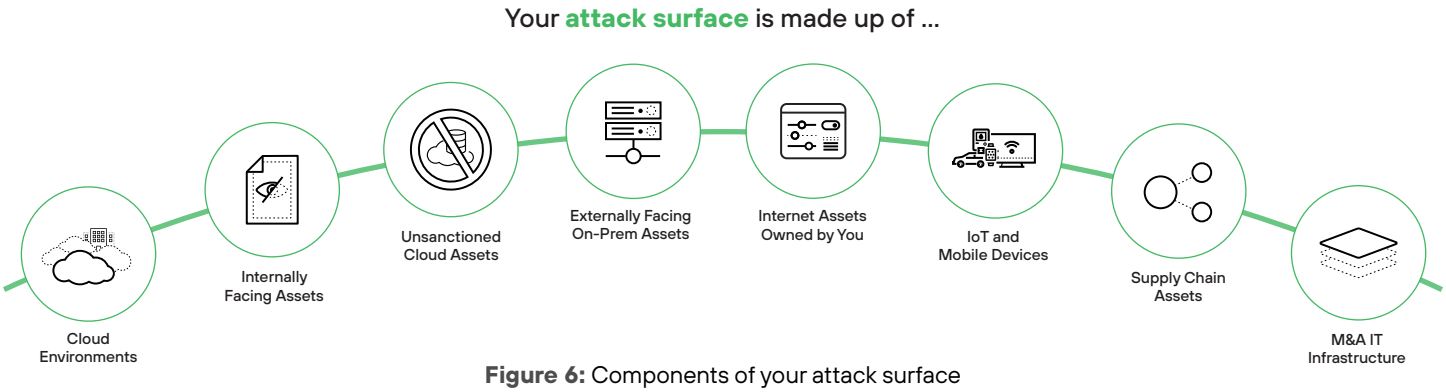

Figure 6: Components of your attack surface

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. 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.

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 is the best way to continuously assess an organization's external attack surface in a cost-effective, repeatable, and scalable manner.

Cortex XSOAR for an Enterprise-Ready SOAR Solution

Cortex XSOAR® delivers enterprise-ready workflow automation, case management, and integrated threat intelligence to turbocharge security operations. XSOAR orchestrates workflows across your security operations, enabling your team to standardize response, accelerate triaging, and automate repetitive tasks for any security use case. XSOAR users can access the industry's most mature and comprehensive integration marketplace to easily automate any security use case. And XSOAR's unique War Room gives analysts all the incident context (threat intel, users, assets, related activity) needed for quick, decisive action.

5. *Unit 42 Attack Surface Threat Report: Lessons in Attack Surface Risk*, Palo Alto Networks, September 2024.

With thousands of customer deployments of all sizes worldwide, XSOAR has a proven track record supporting SecOps teams that range from several people to global service providers serving hundreds of clients. Our ease of deployment and robust scalability are unmatched in the industry. Whether you're a three- to five-person team or a large MSSP with dozens of analysts, XSOAR is built to allow for easy deployment (SaaS, on-premises, or multitenant) but also has the flexibility to scale with your operations.

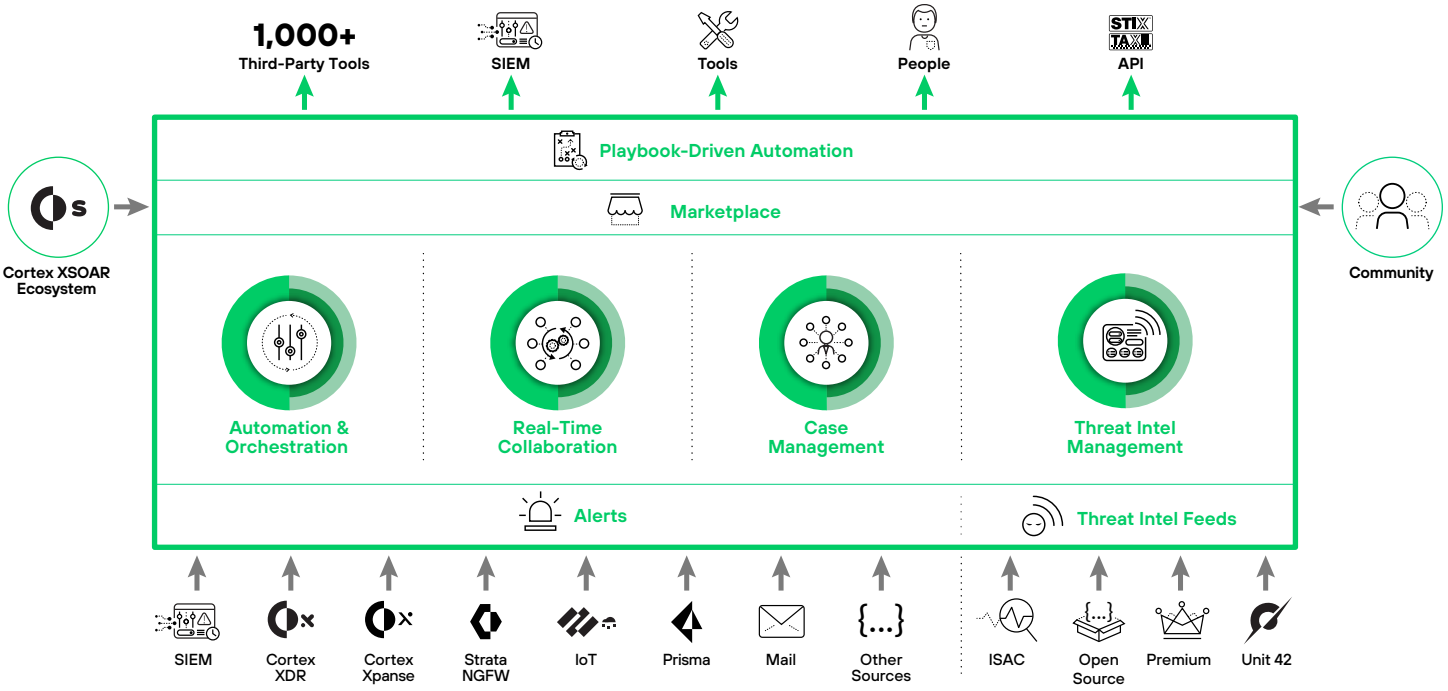

Figure 7: End-to-end workflow automation for security operations

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."[6] 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 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, integrated case management, and real-time collaboration to enable cross-team incident investigation.

6. Claudio Neiva et al., *Market Guide for Security Orchestration, Automation and Response Solutions*, Gartner, September 21, 2020.

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 solutions are integrating threat intelligence 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 and provide a single platform for minimizing complex incident investigations.

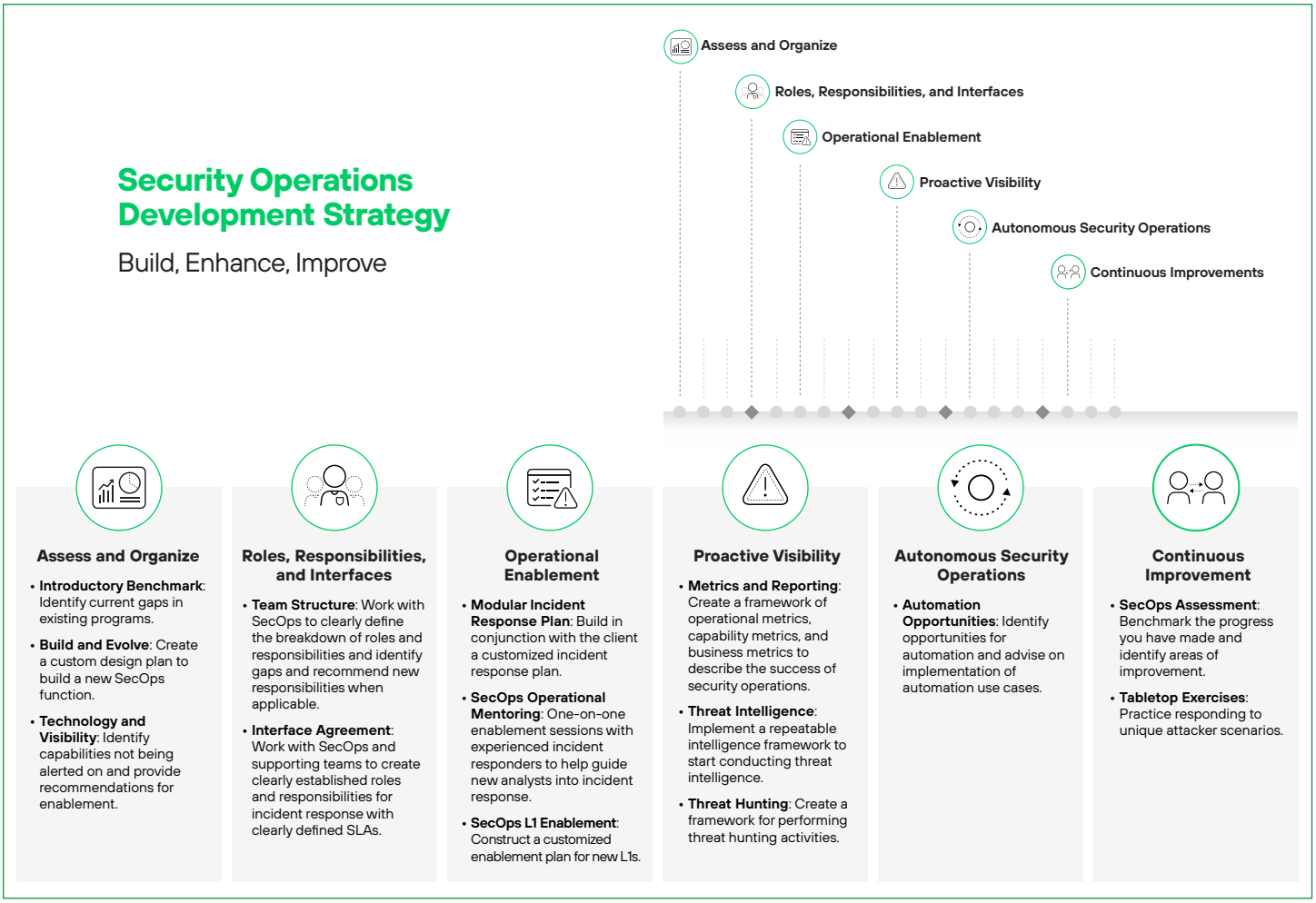

Figure 8: Build a virtual SOC team with Cortex Professional Services

Added Support with Our Extended Expertise Professional Services

Our Extended Expertise Program provides you with experts focused on your organization and uniquely qualified to advise you on getting the most out of your Palo Alto Networks deployment. In as little as 90 days, utilizing our Professional Services options such as the "Service for Cortex XDR" and/or "Service for Cortex XSOAR" can provide planning, remote configuration, scale, optimization, and project coordination to jump-start operations.

Launch a Virtual, AI-Driven SOC Today

Inspired 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 webpages for more information:

- Cortex XSIAM
- Cortex XDR
- Cortex Xpanse
- Cortex XSOAR
- Professional Services

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

cortex_wp_redefining-secops-in-the-era-of-ai_090724