Cortex XSOAR and Xpanse

Streamline Attack Surface Remediation Workflows and Maximize Efficiency Using the Cortex XSOAR and Cortex Xpanse Integration

Automated Attack Surface Remediation Increases SOC Productivity

Organizations have no way to fully map their external attack surfaces—yet this is exactly where attackers often start cyberattack campaigns. Many organizations keep track of known assets using spreadsheets and emails, which are manual and error-prone methods. Cloud migration and digital transformation have exponentially exacerbated the problem.

Organizations typically rely on vulnerability scanners to identify their unique attack surface. This approach falls short, however, because it requires an asset list to perform scans, which misses the unknown assets attackers use to gain access and exploit an organization.

To close this critical gap, your organization needs an automated attack surface management (ASM) solution that provides a complete and accurate inventory of your global internet-facing assets and misconfigurations to continuously discover, evaluate, and mitigate your external attack surface. Cortex® Xpanse™ is fully integrated with Cortex XSOAR.

Cortex XSOAR with the Xpanse Content Pack

Cortex® XSOAR unifies case management, automation, real-time collaboration, and threat intelligence management to transform every stage of the incident lifecycle, resulting in significantly faster responses that require less manual review.

The Xpanse content pack for Cortex XSOAR provides full coverage of the Expander product capabilities from Xpanse to enable your security operations center (SOC) to automate remediation of your company's attack surface. The integrations included in the pack enable fetching and mirroring of Xpanse issues into Cortex XSOAR incidents as well as ingestion of indicators (IPs, domains, and certificates) referring to the corporate network perimeter as discovered by Xpanse.

Leveraging both technologies, your security team will be able to respond to asset vulnerabilities and incidents with automated orchestration playbooks. You can trigger scans to enrich incidents and automatically generate tickets for on-premises and cloud assets. Your team can use this powerful integration to:

- Assign incident severity
- Automate vulnerability management
- Orchestrate certificate management
- Diagnose endpoints
- Threat hunt for compromised assets

Cortex XSOAR and Xpanse help you:

- **Discover assets:** Scan the internet and accurately attribute unknown assets using multiple sources to reduce false positives and map your full attack surface.
- **Enrich incidents:** Use automated playbooks to enrich incidents using Xpanse asset information and threat intelligence indicators, helping you reduce mean time to detect and respond (MTTD and MTTR) across your cloud native, hybrid, and on-premises environments.
- **Automate remediation:** Improve your team's efficiency with a host of integrations and prebuilt scripts to automate attack surface management.

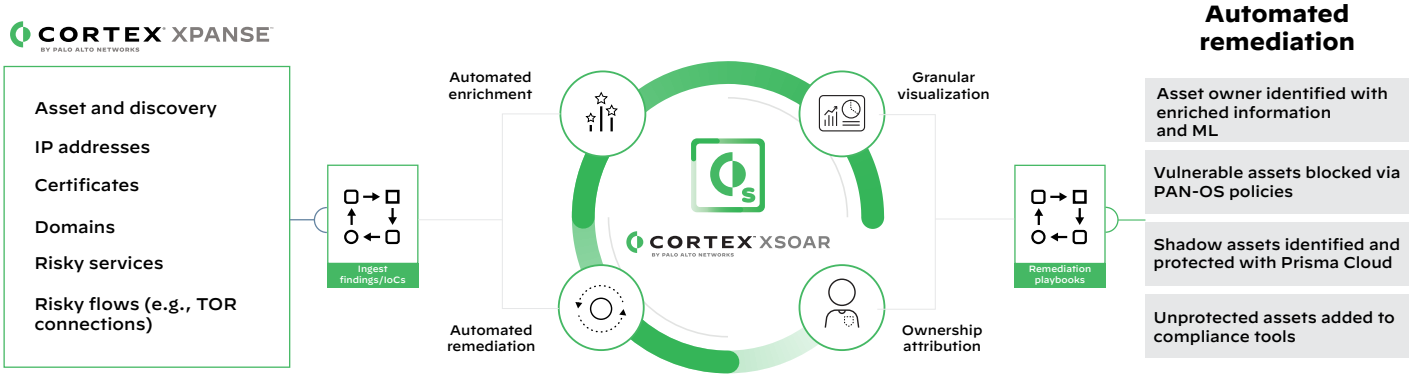

Figure 1: Cortex XSOAR and Xpanse integration

Through a powerful set of playbooks, analysts can correlate the discovered information with data provided from internal security systems (e.g., Cortex® Data Lake, Cortex® XDR™, Prisma® Cloud, Panorama™ network security management, Active Directory®, SIEM) to help pinpoint the right owners of assets and automate remediation.

Bridge gaps and advance the maturity of your security program by tapping into the fastest growing community of security experts. Visit paloaltonetworks.com/cortex/xsoar-ecosystem for a list of available integrations and featured content packs.

Cortex XSOAR Marketplace Content Pack Overview

The Cortex XSOAR Marketplace is a digital storefront for discovering turnkey security orchestration content packs centrally within Cortex XSOAR.

Content packs are prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services, and all the dependencies needed to support specific security orchestration use cases.

The Xpanse content pack automates attack surface management to identify unknown internet assets and quickly remediate misconfigurations with playbooks that hunt for internal activity related to detected services, provide incident enrichment from the internet and public cloud assets, and much more.

The pack includes:

- **9** automations
- **2** classifiers
- **2** dashboards
- **27** incident fields
- **1** incident type
- **15** indicator fields
- **2** integrations
- **2** layouts
- **7** playbooks
- **25** widgets

The pack is easily deployed with a single click from the in-product Cortex XSOAR Marketplace, giving you all the content needed to automate ASM with Cortex XSOAR.

To discover new SOAR content, visit paloaltonetworks.com/cortex/xsoar/marketplace.

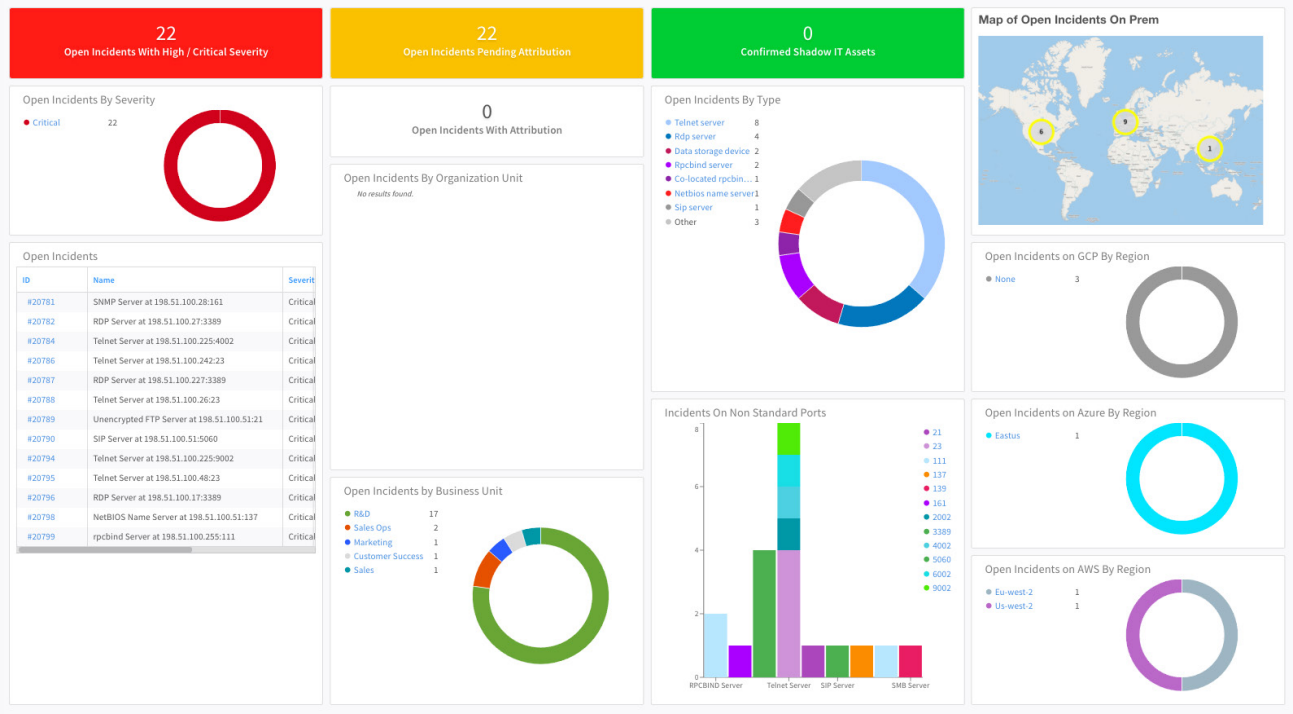

Figure 2: Xpanse incidents dashboard, the main dashboard for all Xpanse incidents

Incident Use Case

Challenge

Your attack surface is constantly shifting and expanding with the addition of new cloud instances, infrastructure, web gateways, contracted service providers, assets from mergers and acquisitions, and much more. You need a way to quickly inventory and discover exposures across this shifting landscape. You also need to remediate vulnerabilities from exposures in real time and prevent threats, including breaches and data loss.

Solution

Xpanse ASM provides an in-depth look at your constantly expanding attack surface and highlights all existing known and newly discovered vulnerabilities across your environment. Using the Xpanse content pack for Cortex XSOAR, your team is enabled to automate discovery, incident handling, and response for all the vulnerabilities discovered by Xpanse. The Xpanse integration provides additional context for any Cortex XSOAR incident.

Benefit

Automate the identification and remediation of web-facing exposures and vulnerabilities with Cortex XSOAR and Xpanse to scale your organization's security posture. Defend your attack surface without adding any new staff or expertise to your current SOC team.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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