Palo Alto Networks Cortex Xpanse and Synack

Integrate Attack Surface Management and Penetration Testing for Continuous Security Posture Improvement

Benefits of the Integration

- Integrates penetration and other security testing with your attack surface management workflows
- Makes sure your security testing stays current with newly discovered assets
- Automates security testing to help ensure exploitable vulnerabilities are identified and remediated before bad actors exploit them
- Leverages Cortex Xpanse tagging and filtering to prioritize testing of your most important assets
- Provides continuous alignment between security testing and evolving attack surfaces
- Delivers proactive vulnerability identification and remediation through automation
- Reduces risk and increases visibility across critical business assets

The Challenge

Traditional penetration testing and other security testing methods are unable to keep pace with the dynamic and evolving attack surface and threat landscape facing modern application deployments, resulting in the security posture degrading over time.

The Solution

Organizations need a solution that can automate the discovery of new and unmanaged assets to enable rapid and continuous penetration testing. This approach ensures that organizations are continuously testing the latest assets and addressing vulnerabilities in real time.

Synack Penetration Testing as a Service

Synack's Penetration Testing as a Service (PTaaS) platform manages security testing for critical vulnerabilities and gains visibility into the root causes of security risks. The platform harnesses a talented, vetted community of security researchers to deliver continuous penetration testing and vulnerability management, with actionable results.

Palo Alto Networks Cortex Xpanse

Cortex Xpanse® is an automated attack surface management (ASM) platform that provides a complete and accurate inventory of an organization's global internet-facing assets and misconfigurations to continuously discover, evaluate, and mitigate an external attack surface. It also flags risky communications and evaluates supplier risk or assesses the security of mergers and acquisitions (M&A) targets.

Palo Alto Networks Cortex Xpanse and Synack

The integration of Cortex Xpanse asset inventory with Synack PTaaS helps ensure that an organization's security testing stays up to date with its external attack surface and the evolving nature of threat landscapes. This helps to maintain and improve the security posture.

Use Case 1: Integrate Penetration Testing into Security Operations

Challenge

Penetration and other human-led security testing has traditionally been a siloed effort that has not been well

integrated into other security operations workflows, including ASM. Consequently, penetration testing has been relegated to static-type tasks, such as yearly compliance checks, rather than being used proactively to maintain strong security posture.

Solution

The integration of Cortex Xpanse ASM with Synack's PTaaS allows automatic or manual import of the Xpanse inventory into the Synack platform asset list. Once in the Synack asset list, assets are eligible for human-led testing by the Synack Red Team (SRT). Penetration and other security testing can then be conducted on demand or continuously to check for the latest exploitable vulnerabilities.

By integrating with Cortex Xpanse, security teams can automate asset discovery and testing, feeding critical vulnerability data directly into security operations workflows. This helps in closing security gaps quickly, with real-time visibility into risk and asset status.

Use Case 2: Ensure Security Testing Keeps up to Date with Attack Surface

Challenge

An organization's external attack surface is continuously evolving due to factors such as dynamic cloud deployment, intercompany supply chains, shadow IT, M&As, and more. Traditional penetration and other security testing have been unable to keep up with this pace of change.

Solution

The Synack PTaaS integration with Cortex Xpanse checks the Xpanse asset inventory daily, looking for newly discovered assets that could be vulnerable to exploitation. It then adds them to the Synack platform for testing by the Synack Red Team. Since attack surface inventory can become voluminous, the integration offers a variety of filters to help you to focus on the assets that matter most.

The ability to tag and filter assets in Cortex Xpanse helps ensure that the most business-critical assets are tested first, optimizing resource allocation and prioritizing high-risk areas.

By integrating Palo Alto Networks Cortex Xpanse and Synack PTaaS, organizations gain continuous and proactive security management for their dynamic attack surfaces. This integration helps teams stay ahead of potential risks, ensuring that vulnerabilities are identified and mitigated before they can be exploited, improving the overall security posture.

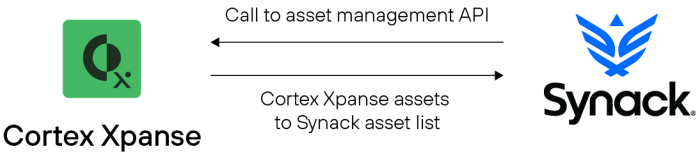

Figure 1: Integration communication flow

About Synack

Synack is committed to making the world more secure by harnessing a talented, vetted community of security researchers to deliver continuous penetration testing and vulnerability management, with actionable results. Synack's PTaaS platform has uncovered more than 71,000 exploitable vulnerabilities to date. For more information, visit www.synack.com.

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security, and security operations. For more information, visit www.paloaltonetworks.com.

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

parent_pb_synack_100324