Palo Alto Networks and Horizon3

Automating Remediation for Exploitable Assets

Key Benefits

- **Identifies exploitable weaknesses and attack paths** by running autonomous penetration tests across your environment.
- **Provides detailed evidence, impact, and remediation** guidance for each weakness.
- **Automatically ingests exploitable assets** as incidents, and runs playbooks to assign, track, and close them.
- **Prioritizes exploitable attack paths** instead of generic Common Vulnerabilities and Exposures (CVE) lists.
- **Shrinks mean time to remediate** (MTTR) by automating responses for the weaknesses that matter most.
- **Proves to leadership, auditors, and regulators** that critical exposures are fixed and independently verified.

The Challenge

Traditional scanners and alerts tell you what's potentially wrong. Even with solutions that can orchestrate incident response and vulnerability workflows at scale, organizations still struggle with a critical question: Which weaknesses in our environment are exploitable right now—and can we prove that our fixes worked?

The Solution

Organizations need a solution that combines autonomous penetration testing with orchestration and automation. An automated testing engine safely discovers and exploits real attack paths across the environment to identify which assets are both exploitable and vulnerable.

An orchestration platform ingests those findings and then automates the remediation cycle within the existing incident response and remediation workflows. Instead of triaging massive vulnerability lists, teams get proof-based, automated vulnerability management. This solution focuses on critical attack paths with proven impacts, orchestrates fixes through automated playbooks, and runs automated verification to produce evidence that those paths are no longer exploitable.

Horizon3 NodeZero®

The Horizon3.ai NodeZero® offensive security platform reduces risk by validating what attackers can exploit. It identifies weaknesses, prioritizes what's most important, provides clear remediation guidance, and verifies that fixes work—continuously fortifying your defenses over time.

You can uncover blind spots that go beyond known CVEs, including compromised credentials, exposed data, misconfigurations, weak controls, and risky policies. NodeZero moves through your network as an attacker might—safely chaining weaknesses into real attack paths. Continuous, autonomous penetration testing validates security posture, prioritizes weaknesses, and gives teams clear proof of the potential business impact.

Palo Alto Networks Cortex XSOAR

Palo Alto Networks Cortex XSOAR® is the industry's most comprehensive SOAR platform that unifies workflow automation, case management, and Threat Intel Management on a single platform. With Cortex XSOAR, security teams take action on threat intelligence, standardize processes, and automate repeatable tasks to efficiently manage incidents across their product stack and reduce response times.

Palo Alto Networks and Horizon3 - Automating Remediation for Exploitable Assets_PAN.indd 1 10/14/26 2:28 PM

Palo Alto Networks and Horizon3 NodeZero

Most Palo Alto Networks customers already have strong controls and automation but still operate in a world of probabilities. Scanners say something *might* be exploitable. Simulations say a control *should* detect or block.

This integrated solution moves you from probability to proof:

- **Proof of exploitability:** NodeZero shows which weaknesses and assets attackers can use to compromise your environment.
- **Proof of remediation:** Cortex XSOAR orchestrates the fix, and NodeZero's 1-click verify demonstrates that the same paths now fail.
- **Proof of continuous improvement:** Scheduled playbooks and status synchronization keep your SecOps fabric aligned to the real attack surface over time.

For existing Palo Alto Networks customers, the integration doesn't replace your scanners or processes. It amplifies the value of Cortex XSOAR by ensuring your automation always points to the smallest set of weaknesses that create the biggest risk and by giving you the evidence to prove that risk is shrinking.

Use Case 1: Prioritize What's Exploitable

Challenge

Scanner-driven CVE lists and generic high or critical alerts tend to overwhelm SOC and vulnerability teams. They know everything is "critical" but not what is exploitable or a real risk.

Solution

With the Cortex XSOAR and NodeZero solution:

- NodeZero highlights both weaknesses tied to real attack paths and high Common Vulnerability Scoring System (CVSS) scores.
- Cortex XSOAR playbooks prioritize and route those specific weaknesses to the appropriate teams.

This integrated solution enables teams to fix the comparatively small number of weaknesses that attackers can exploit instead of paging through endless CVE dashboards.

Use Case 2: Reduce MTTR with Proof-Based Automation

Challenge

Even when organizations know what to fix, MTTR drags due to manual triage, coordination, and limited capacity to confirm whether fixes worked.

Solution

With the Cortex XSOAR and NodeZero integration:

- NodeZero feeds data into Cortex XSOAR, which:
  - › Autocreates incidents for new high or critical exploitable weaknesses.
  - › Runs scheduled and event-driven playbooks to keep exposure visible and manageable.
- After remediation, 1-click verify retests the critical paths in minutes to confirm closure, and Cortex XSOAR can autoclose incidents with proof.

With the integrated solution, organizations shorten remediation from multiweek cycles to just hours or days—from exploit discovery to verified remediation—with MTTR targets that align to automated workflows instead of manual effort.

Use Case 3: Demonstrate Resilience to Executives and Regulators

Challenge

Boards, auditors, and regulators increasingly expect evidence that critical vulnerabilities are identified as well as tested and fixed—especially under the NIS2 Directive, the Digital Operational Resilience Act (DORA), and similar regulatory frameworks.

Solution

With the Cortex XSOAR and NodeZero integration, security leaders can provide:

- The number of proven attack paths discovered during the last week.
- The number of paths remediated and verified as blocked by NodeZero.
- The trend of open, exploitable paths decreasing over time.

Your CISOs are able to show evidence and confidently say that you're now both patching and continuously testing your environment by using attacker-style techniques. You're also orchestrating remediation with automated workflows and verifying that critical paths are closed.

Palo Alto Networks and Horizon3 - Automating Remediation for Exploitable Assets_PAN.indd 2 10/14/26 2:28 PM

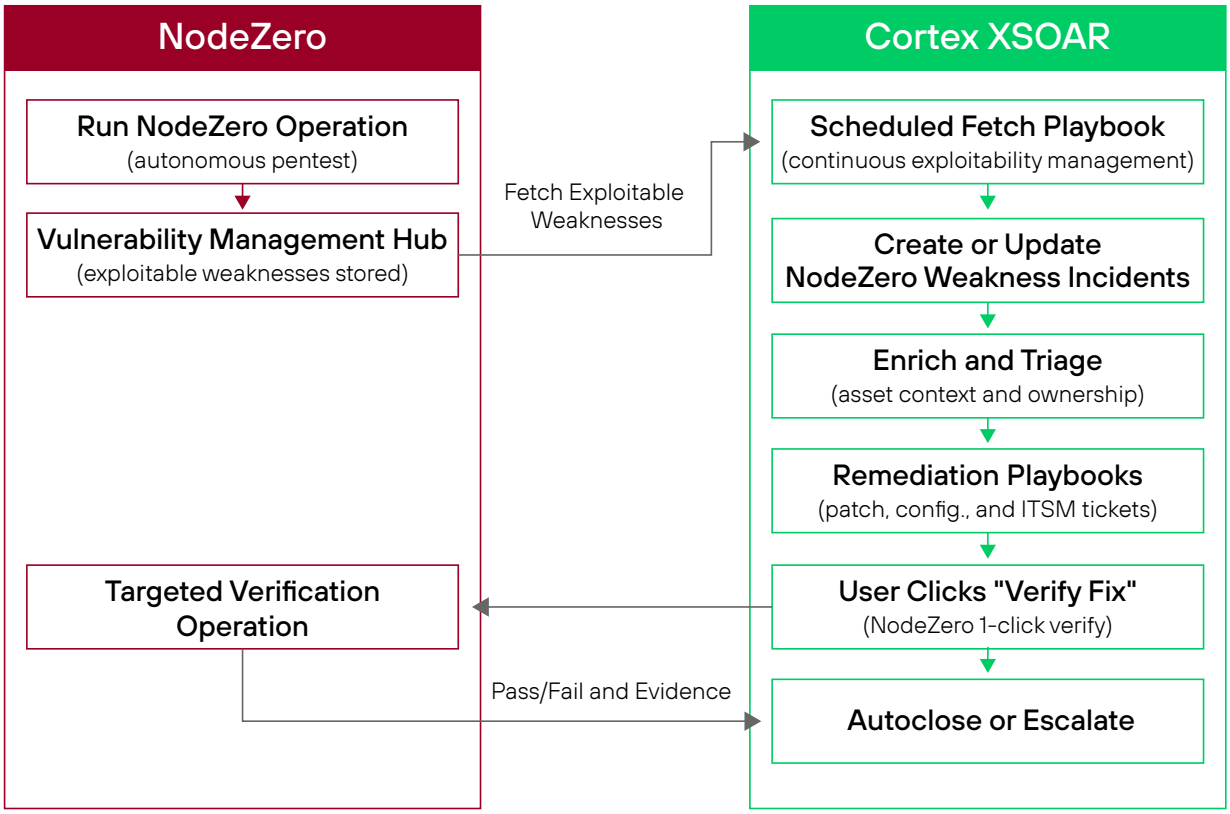


Figure 1. The Cortex XSOAR and NodeZero integration workflow

About Horizon3

Horizon3, the AI-Native Proactive Security Company behind NodeZero®, shifts the advantage from attackers to defenders by giving organizations the power to fight AI with AI. NodeZero, the World's Best AI Hacker™, autonomously tests your defenses at machine speed, safely finds and prioritizes exploitable attack paths, instantly verifies fixes, and drives a continuous hack, fix, verify loop. More than 7,000 organizations including the NSA, CISA, Fortune 100 enterprises, and major healthcare providers trust Horizon3 to prioritize what matters and for security you can prove. For more information, visit www.horizon3.ai.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

paloalto NETWORKS | HORIZON3

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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

parent_pb_horizon3.ai_040726