Automated Penetration Testing and Response

PENTERA | CORTEX XSOAR BY PALO ALTO NETWORKS

Overview

Continuous security validation covers all computing assets and is critical for security operations. Security teams need to stay above the CVSS "noise" and focus remediation efforts solely on the breachable vulnerabilities with direct business impact to their network.

This integration combines Pentera's threat facing remediation prioritization capabilities with Cortex XSOAR's security orchestration and automation to help security teams standardize their response processes, execute remediation tasks at scale, and accelerate time to detect and remediate vulnerabilities.

Integration Features

- Ingest Pentera alerts within Cortex XSOAR for playbook-driven enrichment and response.
- Automatically trigger prioritized task-based playbooks to remediate pentesting findings.
- Instantly notify managers of breachable controls and re-run Pentera to validate the effectiveness of remediation once done.

Use Case #1 Automate Dynamic Vulnerability Alert Ingestion and Response - Password Policy

Challenge: Password policies are a continuous undertaking that organizations need to review regularly. The lack of an automated solution that checks the cyber security posture on-demand, leaves security teams in catch-up mode, unable to ensure their password policy is properly kept across the entire organization.

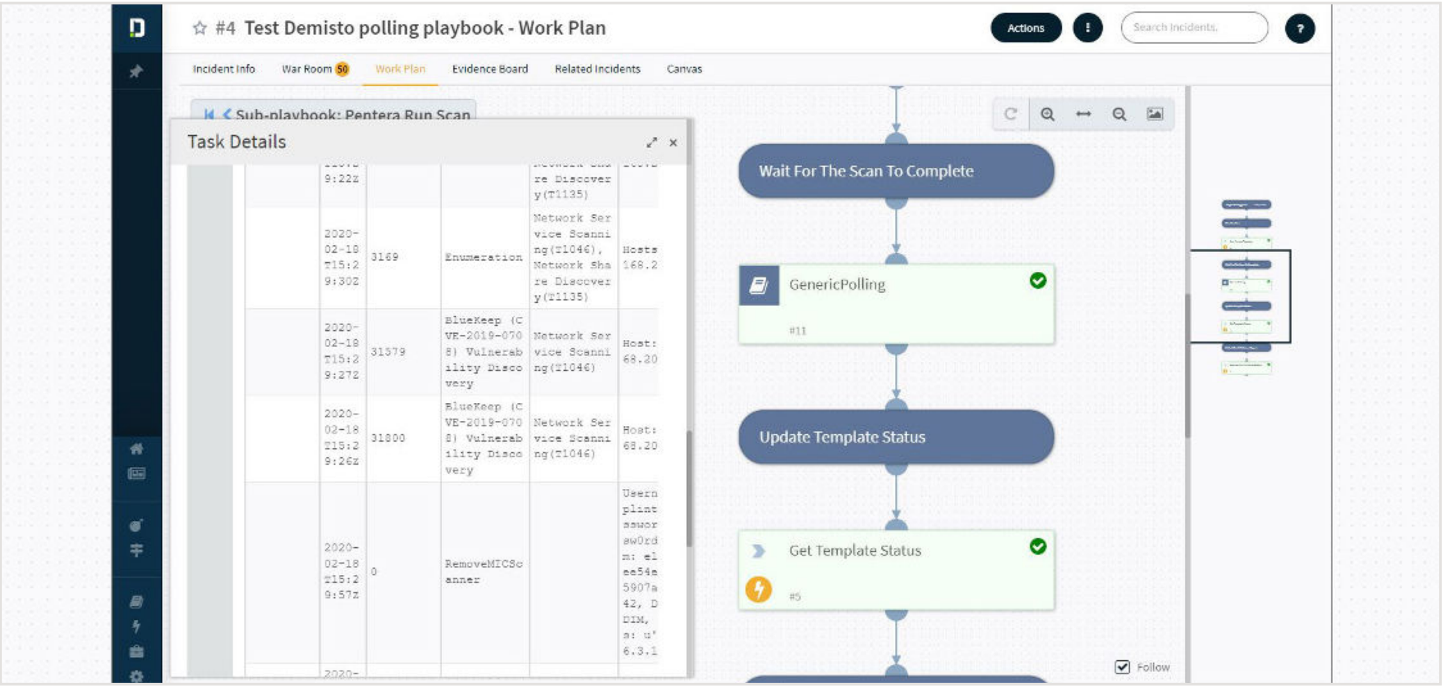
Solution: Continuously validate the effectiveness of enterprise passwords and take action on easily crackable passwords with focus on high privileged accounts. Once Pentera flags a password that doesn't meet the standard, automated playbooks through Cortex XSOAR take action and remediate the vulnerability based on corporate policy.

Benefit: The solution will rid security teams of the repetitive work of continuously challenging the organization's password policy. A more standardized process implemented via automated playbooks can pave the way to a more cost-effective process.

Use Case #2 Automated Real-Time Validation for Critical Vulnerabilities

Challenge: Continuous security validation is critical for the ongoing cyber hygiene of an organization's network. However, critical vulnerabilities require on-demand testing as they influence many components of the network. Security teams struggle with prioritizing remediation and understanding the true impact of vulnerabilities have on their specific network.

Solution: After running automated tests for critical vulnerabilities, the integration allows security teams to automate the response process based on the findings. For example, Pentera discovers the vulnerability of different components of the network, e.g a server or an endpoint. Endpoint vulnerabilities are a simpler fix that can be auto-remediated in a single workflow. Server vulnerabilities might trigger a more complex workflow or playbook, with high-risk tasks automatically prioritized based on business impact severity.



☆ #4 Test Demisto polling playbook - Work Plan

Task Details

9:22Z			re Discovery(T1135)	
2020-02-18T15:29:30Z	3169	Enumeration	Network Service Scanning(T1046), Network Share Discovery(T1135)	Hosts 168.2
2020-02-18T15:29:27Z	31579	BlueKeep (CVE-2019-0708) Vulnerability Discovery	Network Service Scanning(T1046)	Host: 68.20
2020-02-18T15:29:26Z	31800	BlueKeep (CVE-2019-0708) Vulnerability Discovery	Network Service Scanning(T1046)	Host: 68.20
2020-02-18T15:29:57Z	0	RemoveMICScanner		Usernplintsswor ew0rdm: elee54e5907a42, DDIM, s: u'6.3.1
2020-				

Benefit: The solution allows security teams to automate and optimize the response process based on business impact. The tasks are automatically sent to the relevant remediation teams and tagged with the severity level.

About Pentera

Established in 2015 with offices in Israel, Boston, London and Zurich, Pentera, the first automated network penetration testing platform that assesses and helps reduce corporate cybersecurity risks. Hundreds of security professionals and service providers around the world use Pentera to perform continuous, machine-based penetration tests that improve their immunity against cyber-attacks across their organizational networks. Learn more at www.pentera.io.

About Cortex™ XSOAR

Palo Alto Networks Cortex XSOAR is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, case management and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity.

paloalto® NETWORKS