SLASHNEXT CORTEX XSOAR BY PALO ALTO NETWORKS

Automate Phishing IR and Threat Hunting with On-Demand URL Analysis

OVERVIEW

SlashNext URL Analysis and Enrichment enables SOC and IR teams to dramatically reduce the time and effort involved in researching suspicious URLs. Whether in phishing emails, network or endpoint logs, or other digital sources, security teams can get accurate, definitive, fully automated analysis of suspicious URLs on demand. Together with Cortex XSOAR, SlashNext can save dozens—if not hundreds of hours—per week with automated IR playbooks such as those for abuse inbox management.

As an API-based service, SlashNext URL Analysis and Enrichment features a pre-built integration with the Cortex XSOAR platform. This provides quick operationalization for a variety of IR and threat hunting playbooks. SlashNext also provides sample playbooks to simplify implementation for different use cases.

INTEGRATION FEATURES

- Enables full automated analysis of suspected phishing URLs
- Extract and scan links or domains from suspicious emails or logs automatically
- Gain definitive verdicts and forensics evidence, including screenshots, text, HTML, and more to simplify reporting and analysis

COMPATIBILITY

Cortex XSOAR, SlashNext URL Analysis, and Enrichment

BENEFITS

- **Improve Productivity** – Accurate, definitive, binary verdicts on suspicious URLs to increase automation and performance of phishing IR and threat hunting playbooks.
- **Rapid Detection** — High-precision phishing URL analysis and enrichment enables rapid detection of genuine threats, and faster automated processing of false positives
- **Catch More Threats** — Detect all major types of social engineering threats with rich forensics data for additional analysis and reporting
- **Overcome Evasion Tactics** — SlashNext SEER™ technology does run-time analysis with browsers to overcome evasion techniques and accurately detect previously unknown threats, including those hosted on compromised websites and legitimate hosting infrastructure

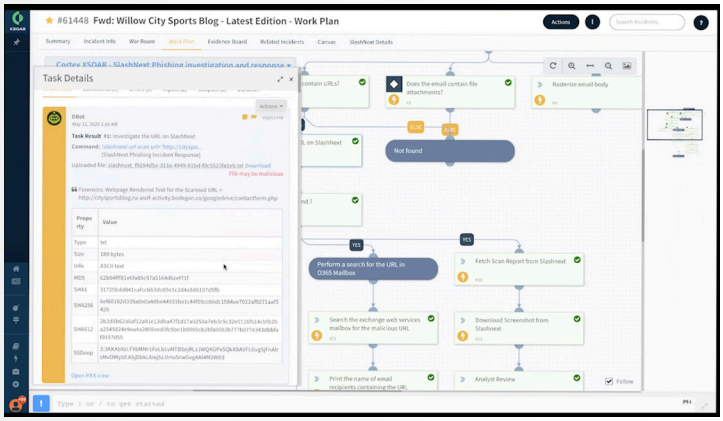
USE CASE #1: ABUSE INBOX MANAGEMENT AND PHISHING IR

Challenge: Increased cyber awareness training and single-click reporting of suspicious emails by users have created a new problem for SOC and IR teams: effectively managing a growing abuse inbox with limited resources. Even with automated playbooks, inaccurate or inconclusive phishing threat intelligence can cause teams to miss genuine threats, or waste time and effort manually researching false positives.

Solution: Accurate, automated phishing URL analysis with a pre-built integration app to allows users to quickly operationalize SlashNext for definitive phishing verdicts on suspicious URLs. The patented technology dynamically inspects page contents using computer vision, natural language processing, site behavior analysis, and machine learning to identify threats while simultaneously retrieving detailed forensic evidence, including screenshots, HTML, and rendered text.

Benefit: Greater accuracy and threat coverage enables better automation of playbook workflows, reducing the time and effort required to effectively manage suspected phishing incidents.

ABUSE INBOX MANAGEMENT PLAYBOOK



USE CASE #2: PHISHING AND C2 THREAT HUNTING

Challenge: Phishing attacks have surpassed malware infections in recent years. Targeted attacks that used to be carried out by APT malware and RAT toolkits are getting replaced by more evasive phishing and spear-phishing campaigns. A lack of accurate, phishing-focused threat detection and intelligence has made it difficult to identify phishing attempts in suspicious emails and C2 connections buried in network and endpoint logs.

Solution: Obtain real-time threat intelligence on phishing URLs and C2s with SlashNext Agentless Phishing intelligence and URL Analysis and Enrichment services using Cortex XSOAR threat hunting playbooks.

Benefit: Effectively identify and remediate phishing threats and compromised machines faster.

About SlashNext

SlashNext helps organizations close the gaps in their existing defenses against today's—and tomorrow's—more advanced phishing and social engineering threats. SlashNext provides IT security teams with a range of real-time phishing protection, phishing incident response, threat intelligence, and threat hunting solutions to protect users, both inside and outside network perimeter protections. SlashNext is headquartered in Silicon Valley and is backed by top-tier venture capital firms. For more information visit: www.SlashNext.com.

About Cortex XSOAR

Cortex XSOAR, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident 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. For more information, visit www.demisto.com.

4301 Hacienda Drive Suite 550, Pleasanton, CA 94588 | slashnext.com | info@slashnext.com | 800.930.8643