ThreatConnect

ThreatConnect and SlashNext Phishing Incident Response Playbook

SLASHNEXT

Overview

SlashNext Phishing URL Analysis and Enrichment enables SOC and IR teams to dramatically reduce the time and effort involved in researching and reporting on suspicious URLs. Whether in emails, network logs, or other digital sources, teams can now get accurate, definitive, automated analysis of suspicious URLs on demand and at scale.

With SlashNext, ThreatConnect® Platform users can save dozens—if not hundreds—of hours per week by getting accurate, definitive verdicts and enrichment of suspicious URLs as part phishing IR and threat hunting playbooks. Users can also automate phishing site blocking for protection via ThreatConnect platform integrations with existing infrastructure.

The Challenges

Teams Are Overwhelmed By The Volume Of Potentially Malicious Phishing Urls

Increasing cyber education has helped improve employee awareness and recognition of the rising number of phishing threats. It has also increased the volume of potential phishing incidents reported by users which can quickly inundate an abuse in-box and IR team.

Researching Threats Takes Time And The Results Are Not Always Conclusive

Researching suspicious phishing URLs can take 5 to 10 minutes (or more) per incident. Available URL scanners and phishing threat databases typically return inconclusive results, have high rates of false positives, and often don't cover newer and previously unknown threats.

The Solution

Automated, Accurate Phishing URL Analysis

SlashNext Phishing URL Analysis and Enrichment provides analysis of suspicious URLs on demand as part of phishing IR and threat hunting playbooks. Unlike other URL scanners and phishing threat databases, SlashNext does dynamic, runtime analysis of page contents and server behavior and uses mature deep learning algorithms to deliver accurate, binary verdicts on suspcious URLs at scale.

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Key Features

Phishing-Focused URL Analysis:
cloud-based, scalable, purpose-built phishing URL analysis engine that uses patented SEER™ threat detection technology.

Deep, Accurate Analysis:
dynamic, runtime analysis using virtual browsers to analyze page contents (images, text etc.) and server behavior. Deep learning algorithms provide definitive, binary verdicts (not threat scores) with >99.95% precision.

Multi-Payload Detection:
SlashNext detects all major types of payload threats, not just fake log-in pages for major brands.

Fully Automated:
Submit URLs to SlashNext cloud APIs through automated playbooks, eliminating countless hours of analysis and further research on inconclusive results.

Simplifies IR Analysis and Reporting:
with definitive verdicts, forensics data–including IoCs, screen shots, HTML, text and image files–plus reporting artifacts.

Zero-Hour Detection:
SlashNext detects phishing threats missed by URL inspection and domain reputation technologies by following URL re-directs and multi-stage attacks to detect phishing URLs hosted on compromised websites and legitimate hosting infrastructure.

How to Get Started

For more information about this app, please contact your ThreatConnect Customer Success representative or email **sales@threatconnect.com.**

The SlashNext & ThreatConnect Advantage

Unlike other security vendors, SlashNext is entirely focused on phishing threats involving URLs, regardless of phishing attack vector. Its global, multi-vector URL sourcing network combined with its patented and highly accurate, real-time phishing site detection capabilities provides ThreatConnect Platform users with the industry's most accurate URL analysis capabilities to expedite phishing IR and threat hunting.

SLASHNEXT

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 anti-phishing and phishing incident response solutions to protect users, both inside and outside network perimeter protections.

To learn more about SlashNext real-time anti-phishing solutions, visit www.SlashNext.com

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708