SLASHNEXT

Phishing URL Analysis and Enrichment

High-precision real-time threat intelligence for powerful phishing IR and threat hunting.

SlashNext URL Analysis and Enrichment delivers highly accurate, definitive verdicts on suspicious URLs, even for previously unknown zero-hour threats and those employing multiple evasion TTPs. Compared to lighter-weight URL lookups and domain reputation-based systems, SlashNext's patented technology delivers highly precise detection, analysis, and enrichment for more actionable intelligence for IT security teams, security vendors, and MSSPs.

Dramatically reduce the effort involved in responding to suspicious URLs in emails, or other indicators of compromise, with automated and accurate analysis on-demand and at scale. SlashNext enables organizations to save dozens—if not hundreds of hours—per week by automating IR playbooks such as those for abuse inbox management and threat hunting. Security vendors and MSSPs can also dramatically improve the blocking efficacy of their offerings.

Abuse Inbox Management and Phishing IR

Increased cyber awareness training and single-click reporting of suspicious emails 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.

SlashNext URL Analysis and Enrichment works with leading SOAR and SIEM platforms to provide greater accuracy and threat coverage with automated phishing URL analysis. SlashNext patented technology dynamically inspects page contents to identify phishing threats while simultaneously retrieving detailed forensic evidence, including screenshots, HTML, and rendered text. With the pre-built integration app, SOC and IR teams can quickly operationalize SlashNext for definitive phishing verdicts (malicious or benign) on suspicious URLs.

Phishing and C2 Threat Hunting

Phishing attacks have surpassed malware infections in recent years. Targeted attacks that use to be carried out by APT malware and RAT toolkits are getting replaced by more evasive phishing campaigns with malicious aims beyond credential stealing. 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.

SlashNext URL Analysis and Enrichment effectively identifies and remediates phishing threats on compromised machines faster with real-time threat intelligence. Expedite phishing URL and C2s hunting with pre-built playbooks in your SOAR and SIEM platforms.

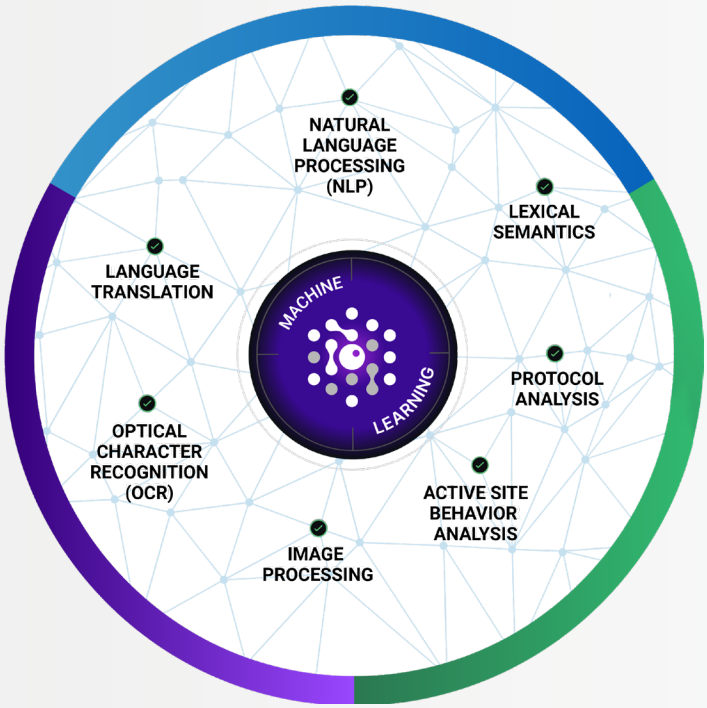
KEY BENEFITS

- **Automate Phishing IR –** Increase performance of phishing IR and threat hunting playbooks.
- **Accurate, Definitive Verdicts –** High-precision binary verdicts on suspicious phishing URLs for rapid detection of genuine threats for all major types of social engineering threats
- **Zero-Hour Threat Detection** — Dynamic, run-time URL analysis uncovers live, unknown threats missed by URL inspection and domain reputation analysis methods.
- **Overcome Evasion Tactics** — Run-time analysis, including those hosted on compromised websites and legitimate hosting infrastructure
- **Extreme Accuracy** – Patented SEER threat detection technology delivers binary verdicts with >99.95% accuracy.
- **Detailed Reporting** – URL enrichment and forensics data includes IOCs, screenshots, HTML, and rendered text.
- **Resource Savings –** Reduce costs and investments associated with researching suspicious URLs.
- **Pre-Built Integrations** – Expedite phishing IR and threat hunting with leading SOAR and SIEM platform integrations.

Blocking Mode Stops Fast-Moving Phishing Threats

Cybercriminals move fast. They can set up and take down a phishing attack after successfully completing their scam within minutes. This makes it very hard for current defenses to identify and block access to a phishing site before users click through it. Defending against these speedy attacks requires timely, accurate, automated threat detection to drive an effective blocking response. SlashNext preemptively sources data and has a continuously updated list of definitive zero-hour phishing threats that can be used for automated, real-time blocking. And if a host look-up or quick inline response is needed, organizations can perform a URL reputation scan and get an instant response that also can be used for blocking.

SEER THREAT DETECTION TECHNOLOGY



Threat Detection That Overcomes Evasion Tactics

SlashNext uses its own proprietary, scalable, cloud-based analysis engine that was purpose-built for analyzing phishing sites. Our patented SEER™ (Session Emulation and Environment Reconnaissance) threat detection technology uses virtual browsers to dynamically inspect page contents and server behavior using a combination of computer vision, NLP, and OCR. This deeper analysis, together with mature machine learning algorithms and virtual browsers, enables SlashNext to accurately detect zero-hour phishing pages and extract numerous enrichment artifacts for further analysis and reporting.

This unique combination of techniques sees through evasion tactics and accurately detects phishing pages, even those hidden behind CAPTCHAs and hosted on legitimate infrastructure. It also follows through on all URL re-directs and performs runtime analysis on the final page of multi-stage threats.

Detects All Major Phishing Payloads

Unlike other phishing URL analysis technologies which largely focus on identifying fake log-in pages for major brands, SlashNext detects all major phishing payload threats.

Credential Stealing
Fake login pages, etc.

Tech Support Scams
Fake virus alerts, pop-ups, on-line support scams

Rogue Software
Rogue browser extensions, fake AVs, etc.

Document Theft
Document, IP, and media theft

Money Transfer Scams
Wire transfers, Bitcoin, gift card, fake deals, etc.

Extreme Accuracy with >99.95% Precision

Perform runtime behavioral analysis on suspicious URLs/webpages using patented, cloud-powered SEER threat detection technology. SEER uses virtual browsers to dynamically analyze page contents (images, text etc.) and server behavior. Mature machine learning algorithms enable definitive, binary verdicts (not threat scores) with >99.95% precision.

Full Automation with URL Enrichment

URL Analysis & Enrichment is fully automated and needs no manual intervention. Just submit URLs to SlashNext cloud via automated playbook commands and get accurate, binary verdicts. Eliminate countless hours of analysis and further research on inconclusive results.

SlashNext enriches URLs with a definitive verdict plus forensics data, including screenshots, HTML, and rendered text combined with reporting artifacts. This simplifies phishing IR processes and reporting. IoCs such as screenshots can even aid in employee phishing training and testing programs.

Zero-Hour Detection at Cloud Scale

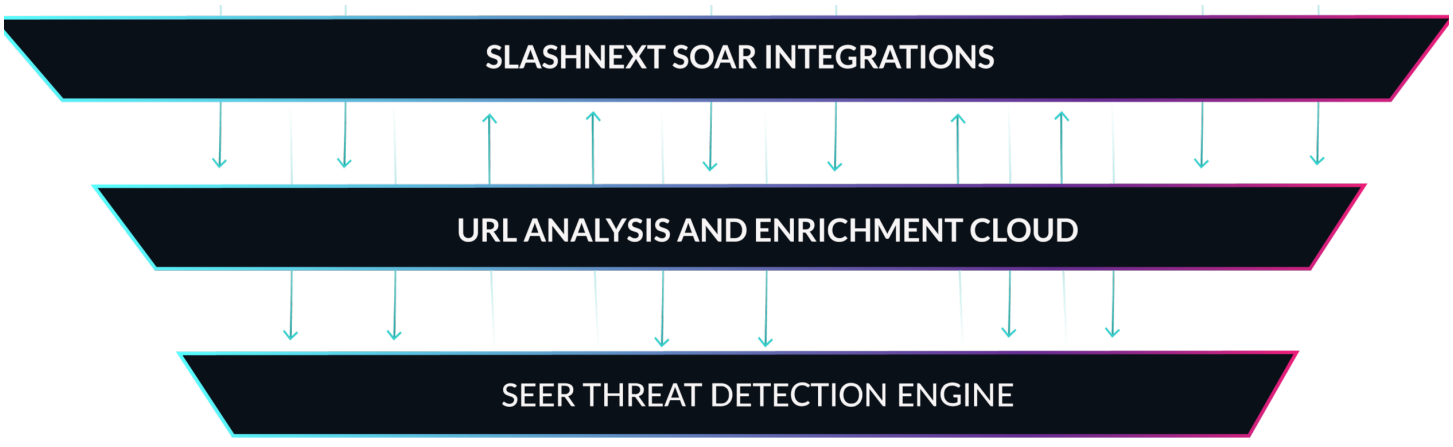
SlashNext URL analysis operates at cloud scale, using millions of virtual browsers to analyze many millions of suspicious webpages daily. Analyze thousands, or even millions, of suspicious URLs on demand.

SEER threat detection technology catches phishing threats missed by URL inspection and domain reputation technologies. With its patented approach, SEER follows all URL re-directs and multi-stage attacks to analyze final destination pages. This enables detection of phishing URLs/webpages hosted on compromised websites and legitimate hosting infrastructure.

Deployment Flexibility with Pre-Build Integrations

URL Analysis & Enrichment is easily accessed via pre-built integration apps with leading SOAR, SIEM, and TIP solutions for phishing IR, threat research, and more.

As a cloud-powered, API-based service, security teams can leverage our Linux utilities and SDK to build custom apps and automation workflows.



Learn More about SlashNext Anti-Phishing and IR Solutions.

Request a demo today at www.slashnext.com/request-a-demo

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

REV 041720