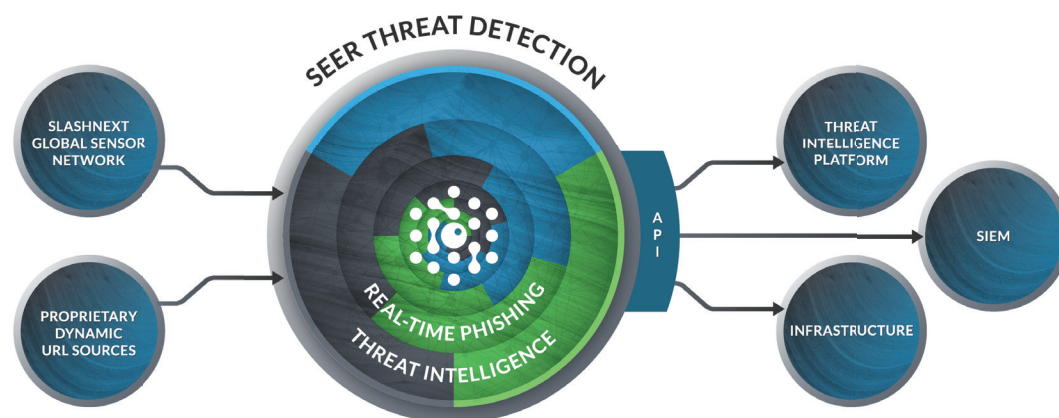# SLASHNEXT

Phishing IR

Expedite Phishing IR with Accurate, On-Demand Phishing URL Analysis

SlashNext Phishing URL Analysis enables security and IR teams to dramatically reduce the time and effort involved in researching suspicious URLs. Whether in phishing emails, network logs, or other digitial sources, security teams can now get accurate, definitive, fully automated analysis of suspicious URLs on demand. Together with automation tools such as Security Orchestration, Automation and Response (SOAR) platforms, SlashNext can save dozens—if not hundreds—of hours per week by expediting phishing IR applications such as abuse inbox management.

ACCURATE URL ANALYSIS, ON-DEMAND

SlashNext Phishing URL Analysis is based on patent-pending, real-time SEER™ threat detection technology. SEER uses browsers in a purpose-built cloud to dynamically inspect page contents and server behavior using advanced computer vision, OCR, and natural language processing. SEER generates far more clues than other analysis methods. Together with mature machine learning algorithms, delivering highly accurate, binary verdicts (not risk scores) with near-zero false positives.

SlashNext detects phishing sites that evade URL inspection and domain reputation analysis methods. With more powerful real-time analysis, SlashNext detects previous unknown phishing URLs that may never be detected by other systems or found in any commercial or free phishing URL databases. And with browser-based analysis, SEER detection technology is able see through the growing variety of URL obfuscation techniques and evasion tactics, including:

- Shortened links
- Multiple URL re-directs / forwarding
- Multi-stage attacks
- Phishing pages hosted on compromised websites
- Phishing pages hosted on legitimate cloud infrastructure

THE SLASHNEXT ADVANTAGE

- **Fast, Accurate Verdicts**
  Accurate, binary verdicts (not risk scores) with near-zero false positives.

- **Forensics Data**
  Get more than verdicts. Access IOCs, screen shots, HTML, and more.

- **Automate Phishing IR**
  Save hundreds of hours by fully automating URL analysis as part of phising IR playbooks.

- **Real-Time**
  Live URL analysis rather than simple check against known threat database.

- **Broader Detection**
  Detects all six major categories of phishing, not just credential stealing and malware sites.

- **More Powerful Analysis**
  Detects threats missed by URL inspection and domain reputation analysis methods.

- **Overcomes Evasion Tactics**
  Detects phishing pages hidden behind URL obfuscation techniques and redirects as well as phishing pages hosted on compromised websites or legitimate hosting infrastructure.

- **Simple API Access**
  Access the industry's best phishing URL analysis on demand, even with custom systems.

- **Integrations**
  Packaged integrations with leading SOAR and SIEM solutions.

BROADER PHISHING THREAT DETECTION

SlashNext Phishing URL Analysis is able to detect the broadest variety of phishing threats. While most anti-phishing technologies are designed only to spot fake login pages for major brands, SlashNext detects all six major categories of phishing and social engineering threats.

CREDENTIAL STEALING
Fake login pages, etc.

SCAREWARE
Tech support scams, fake virus alerts, etc.

ROGUE SOFTWARE
Rogue apps, browser extensions, fake AVs, etc.

PHISHING EXPLOITS
Weaponized documents, etc.

SOCIAL ENGINEERING SCAMS
Credit card and Bitcoin fraud, money transfer scams, fake deals, prizes, etc.

PHISHING CALLBACKS (C2s)
Data exfiltration, C2 callbacks, etc.

GET MORE THAN A VERDICT

SlashNext Phishing URL Analysis provides more than accurate, binary verdicts on suspicious URLs. It also provides extensive forensics data, including IOCs, screen shots, HTML, and other artifacts. This additional information simplifies and informs phishing IR reporting, on-going vulnerability management, and can even aid in on-going phishing awareness training and testing with employees.

AUTOMATED PHISHING IR

As an API-based service, SlashNext Phishing URL Analysis is easily integrated with popular SIEMs and Security Orchestration, Automation and Response (SOAR) platforms. Pre-packaged integrations with leading solutions from Splunk and Demisto provide quick operationalization for a variety of phishing IR playbooks. SlashNext even provides sample playbooks to simplify implementation for different phishing IR use cases.

QUICK ACCESS TO FORENSICS DATA LIKE WEBPAGE SCREENSHOTS, HTML AND TEXT
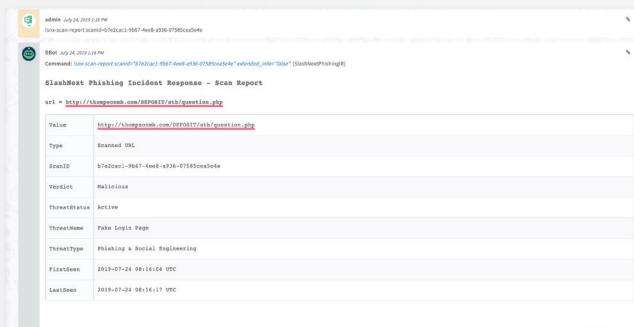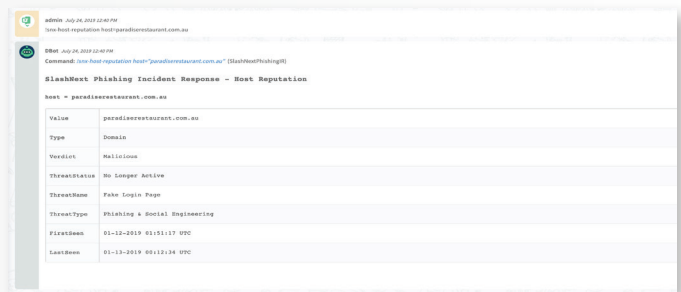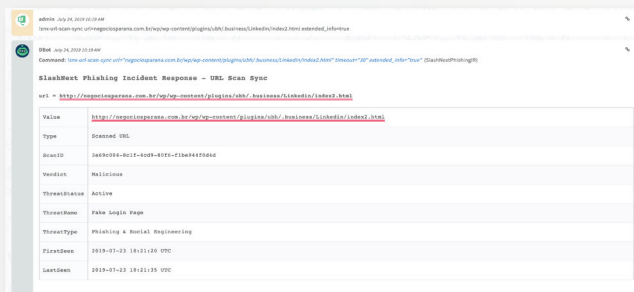
REQUEST A DEMO TODAY AT WWW.SLASHNEXT.COM/DEMO