THREATQUOTIENT™ SLASHNEXT

THREATQ™ AND SLASHNEXT®

SlashNext Protects Organizations from Zero-Hour Phishing Threats with the Industry's Broadest, Most Up-to-the-Minute, Blocking-Ready Phishing Threat Intelligence

With the combination of SlashNext and the ThreatQ™ threat intelligence platform, IT security teams can better understand and automate protection from zero-hour phishing and social engineering threats on the Web—regardless of phishing attack vector.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

SLASHNEXT REAL-TIME PHISHING INTELLIGENCE

SlashNext Real-Time Phishing Threat Intelligence is the industry's broadest, most up-to-minute intelligence on zero-hour phishing and social engineering threats on the Web. It's a continuously updated, dynamically-sized threat feed covering all six major categories of phishing. SlashNext uses multiple sources to do proactive threat hunting, and inspects hundreds of millions of suspicious URLs daily. This results in tens of thousands of new phishing site detections per day. Together with automated URL re-checking and retirement, it results in a dynamic, real-time feed of live threats. Threat detection is powered by SlashNext patent-pending SEER™ (Session Emulation and Environment Reconnaissance) technology. SEER uses virtual browsers in a purpose-built cloud to follow URL redirects and dynamically inspect page contents and server behavior. More thorough page and site analysis, together with machine learning, deliver higher-fidelity, binary verdicts rather than threat risk scores.

INTEGRATION HIGHLIGHTS

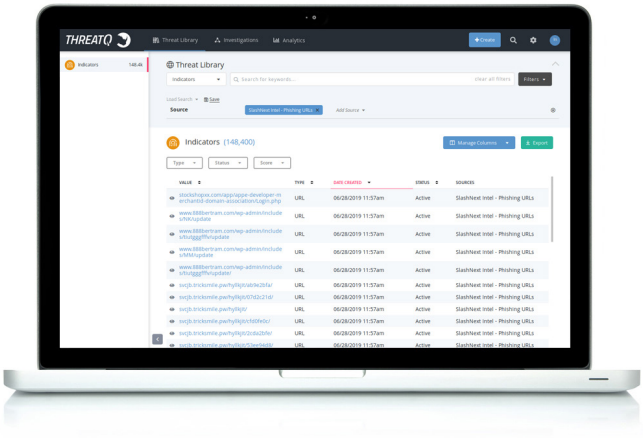
Access a continuously updated, dynamic list of active zero-hour phishing URLs, domains and IPs with IOC metadata right in the ThreatQ platform

Covers all six major categories of phishing threats (not just credential stealing)

Reduce costly, time-intensive research on suspicious URLs by checking against definitive real-time phishing threat intelligence, not inconclusive threat risk scores

Access proactive global threat hunting for advance visibility of phishing threats

"Blocking-Ready" threat intelligence can be forwarded to infrastructure, such as firewalls, to protect employees from live threats



ADVANTAGES

- **Comprehensive:** Covers six phishing threat categories (credential stealing, scareware, rogue software, phishing exploits, social engineering scams and phishing callback C2s)
- **Real-Time:** Continuously updated list of zero-hour phishing URLs, domains and IPs with IOCs
- **Blocking-Ready:** Confirmed malicious sites rather than risk scores. Automated URL re-checking and retirement delivers dynamic list of active phishing threats with near-zero false positives
- **SEER Technology:** Detects phishing sites that evade outdated URL inspection and domain reputation analysis methods
- **Preemptive:** Global, proactive threat hunting provides advance visibility of threats
- **Easily Accessible:** Web API access to threat data in multiple machine-readable formats
- **SlashNext Expertise:** Proprietary detection technology and quarterly threat intelligence reports

INTEGRATION USE CASES

The integration supports a variety of use cases such as:

Empower threat research teams to better understand and protect employees from zero-hour phishing and social engineering threats

Strengthen existing anti-phishing security infrastructure (firewalls, DNS) through automated comparison and ingestion of live threat feed data

Protect employees by blocking access to live malicious phishing sites

Test for gaps in current multi-layer security infrastructure to assess phishing risk exposure

ABOUT THREATQUOTIENT™

ThreatQuotient 's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For additional information, please visit threatquotient.com.

ABOUT SLASHNEXT

SlashNext helps organizations close the gaps in their defenses against today's—and tomorrow's—phishing and social engineering threats. SlashNext provides IT security teams with Real-Time Phishing Threat Intelligence as well as Targeted Phishing Defense solutions to protect users on enterprise networks. SlashNext real-time anti-phishing solutions are powered by SlashNext award-winning SEER™ threat detection engine, a more effective, cloud-powered approach to real-time phishing site detection. SlashNext is headquartered in Silicon Valley and is backed by top-tier venture capital firms.

For more information visit: www.SlashNext.com.

TQ_ThreatQ-Digital-SlashNext-Solution-Overview_Rev1