SLASHNEXT

Highest Accuracy and Fastest Response Required to Manage Abuse Inbox with Limited Resources

The Company

Nvidia Corporation is an American multinational technology company based in Santa Clara, California. It designs graphics processing units for the gaming and professional markets, as well as system on chip units for the mobile computing and automotive market..

The Challenge

NVIDIA challenge was to find a solution to effectively manage a growing abuse inbox with limited resources has become an increasing problem for SOC and IT teams. Automating URL analysis with SOAR playbooks has helped, but the efficacy of the automation is only as good as the threat intelligence and URL analysis. The incumbent solution:

- Missed critical threats and returned false negatives on previously unknown threats
- Failed to identify URL obfuscation techniques, re-directs, and multi-stage attacks
- Returned inconclusive threat risk scores rather than accurate, definitive results

The Solution

SlashNext Real-Time Phishing Forensics and SlashNext Incident Response for with automation and playbooks for Cortex XSOAR. SlashNext cloud-based analysis engine is purpose-built to analyze URLs, domains, and IPs using virtual browsers and patented AI threat detection technology, offering the industry's largest threat database. SlashNext's pinpoint 99.9% accuracy and 48-hour time to detection advantage enable SlashNext to protects organizations from threats launched from legitimate, trusted sites that easily evade current security tools. SlashNext returns a binary verdict (malicious or benign) and forensic information, including a screenshot of the attack page, threat name and type, threat status, and first/last seen date.

The Challenge

- Missed critical threats and returned false negatives on previously unknown threats
- Failed to identify URL obfuscation techniques, re-directs, and multi-stage attacks
- Returned inconclusive threat risk scores rather than accurate, definitive results

The Solution

- SlashNext Incident Response, Abuse Inbox Management playbook and Cortex XSOAR

The Results

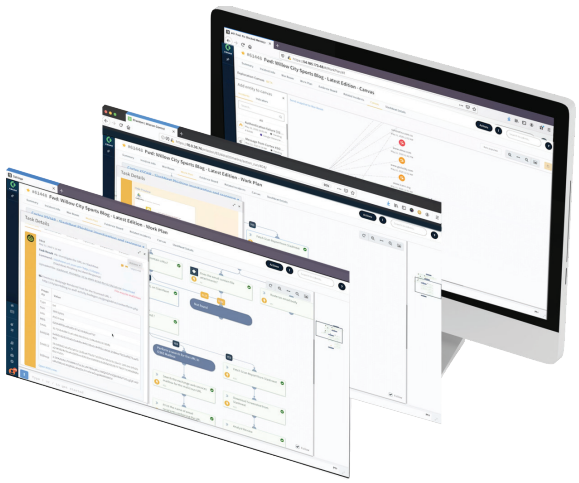
- Coverage for a broad phishing attack surface
- Largest threat database with 99.07% efficacy
- Highly effective with signifcant savings of time and cost

The Results

SlashNext Real-Time Phishing Forensics and SlashNext Incident Response for Cortex XSOAR provides a live threat intelligence API for real-time data on novel phishing attacks for rapid incident response —12-month subscription term. NVIDIA leveraged SlashNext abuse inbox management playbook and Palo Alto Network's Cortex XSOAR to simplify and expedite abuse inbox management and phishing incident response.

"From our internal testing of phishing URLs against their SlashNext's Incident Response API they had the highest accuracy, quality, and time to detection, with the correct phishing classifications," said Travis Carroll, NVIDIA Monitoring & Incident Response Manager. "Along with their Palo Alto Networks Cortex XSOAR integration and playbooks it makes automating abuse inbox remediation and brand protection highly effective, saving us significant time and cost."

With a 99.07% detection rate, broad coverage, and 1 in 1M false positives there has been a significant savings of time and resourse. SlashNext Incident Response reduces IR response times with prebuilt playbooks for Abuse Inbox Management and Online Brand Protection. Mitigate the risk of compromise with run-time analysis using virtual browsers to detect zero-hour phishing threats hours before other vendors.



SlashNext Incident Response Abuse Inbox Management with Cortex XSOAR

Additional Resources

Abuse Inbox Management Protection
https://www.slashnext.com/abuse-inbox-management/

Automate Online Brand
https://www.slashnext.com/solution-automate-online-brand-protection/

SlashNext Product Demo: https://www.slashnext.com/resource/slashnext-360-defense-as-a-service/

Read the Blog: SlashNext Reinvents Incident Response with Cortex XSOAR

About SlashNext

SlashNext is the authority on multi-channel phishing and human hacking, leading the fight together with its partners to protect the world's internet users from targeted phishing anywhere. SlashNext 360° Defense Service utilizes our patented AI SEERTM technology to detect zero-hour phishing threats by performing dynamic run-time analysis on billions of URLs a day through virtual browsers and machine learning. Take advantage of SlashNext's phishing defense services using mobile apps, browser extensions, and APIs that integrate with leading mobile endpoint management and IR services.

For more information, visit www.slashnext.com

6701 Koll Center Parkway, Suite 250, Pleasanton CA 94566 | slashnext.com | info@slashnext.com | 800.930.8643