DATASHEET

NSFOCUS

NTI

NSFOCUS THREAT INTELLIGENCE

Modern cyber criminals are more sophisticated, organized, skilled and persistent than ever. The threat actor landscape has evolved from single individuals with a hobby and an agenda, to include cyber-terrorists, cyber-criminals, professional hackers, hostile nation states, and rival companies. Even unwitting employees, customers, partners and individuals' Internet-connected devices have become compromised.

At the same time, new vulnerabilities are discovered daily in protocols, operating systems, networking devices, and applications. Keeping pace with threat actors and new threat vectors created to exploit these vulnerabilities, is a daunting task. As a result, despite significant investments in network and application security, organizations continue to experience disruption of online systems and costly data breaches.

NSFOCUS Threat Intelligence (NTI) Subscription Service provides you with actionable intelligence that minimizes your risk and improves your overall security posture.

KEY BENEFITS

Minimize risk, improve security, and protect valued assets with actionable threat intelligence

Improved visibility into North Asia threat landscape including countries like Vietnam, China, and Korea.

Simplify and accelerate identification of new and emerging threats

KEY FEATURES

Cloud-based Forensics Portal for in-depth threat analysis

Ability to upload suspicious files for automated malware analysis

Extensive sensor and honeypot network

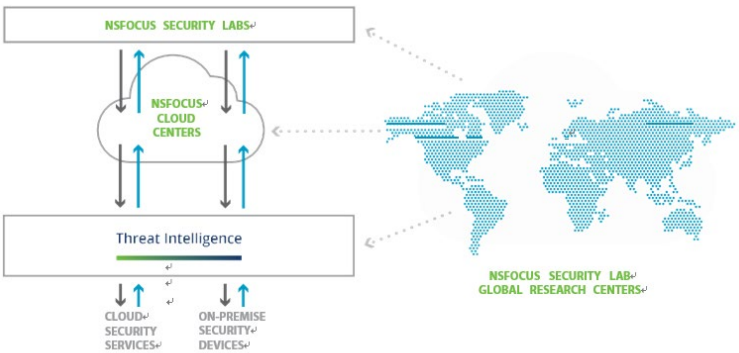
Access to strategic reports on campaigns, threat actors, and threats related to your industry

Standards-based API for third-party integration

GLOBAL THREAT INTELLIGENCE – INCLUDING NORTH ASIA

The cloud-based NTI Subscription Service provides complete visibility into the global threat landscape. Because as much as 40% of the world's hacking activity originates from countries like Vietnam, China, and Korea, without having local sensors, honeypots and real- time access by threat researchers, you do not have a complete picture. This increases your vulnerability to new threats originating from this part of the world. The NSFOCUS Security Lab is an internationally-recognized cyber security research and threat response center at the forefront of vulnerability assessment, threat detection, and mitigation research.

A worldwide team of researchers and engineers creates the threat intelligence at the core of the subscription using data collected from around the world, including NSFOCUS monitored sensors, honeypots, and managed networks in China. This team has access to information not readily available in other subscription offerings and allows us to provide our customers with the most complete view possible of the evolving threat landscape. Access to this unique intelligence enables our customers to quickly implement countermeasures to protect their critical assets.



THREAT INTELLIGENCE DATA FEEDS

NSFOCUS Threat Intelligence data feeds provide information in four critical areas, and are delivered worldwide from strategically located NSFOCUS Cloud Centers:

IP Reputation Data Feed

» list of IP addresses that have earned a negative reputation through involvement in suspicious activity, including phishing attacks, spam, botnets, DDoS attacks, APT attacks, and more.

Malicious Web/URL Data Feed

» domain reputation list that includes malicious websites that are the source of malware or phishing attacks.

Command & Control Data Feed

» set of IP addresses and domains that are known to control botnet armies used to take services offline. This feed is used to prevent your own resources from participating in a cyber-attack, as well as conserving your compute and network resources.

Malware Data Feed

» set of MD5 file hashes that can be used to identify malware in email or file transfers, as well as stored data.

All feeds are regularly updated with the latest threat intelligence information and the update interval is user configurable. They are also available in JSON and XML formats, in addition to STIX and TAXII for integration with third-party security products.

Integrating these real-time threat intelligence feeds directly into your security infrastructure enables you to update your security policies automatically and dynamically to minimize your window of exposure and reduce your overall risk. Once a threat is discovered, you can apply this information into your NSFOCUS or third-party security devices to actively block all traffic originating from malicious sources. The data in the feed updates automatically throughout the day, enabling you to implement a proactive, dynamic, and adaptive security model that significantly improves upon the static, preventive models of the past.

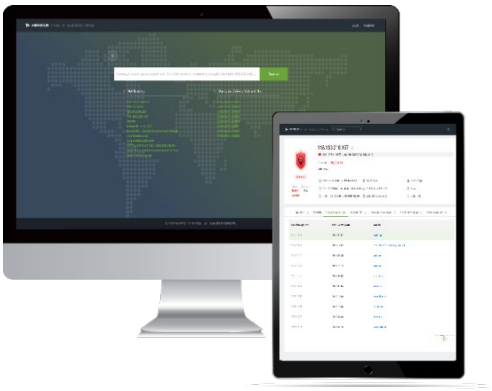
ORDERING INFORMATION

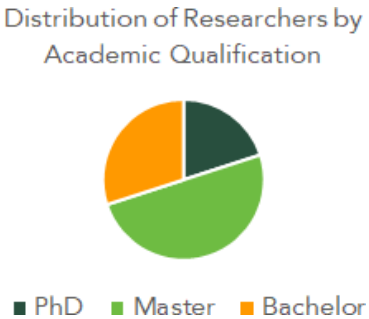
Subscriptions for NSFOCUS Data Feeds can be purchased individually or as a bundle. Enterprise capacity licensing is available and additional discounts are provided for subscription customers who opt-in to provide anonymous data back to NSFOCUS Security Lab researchers.

NSFOCUS THREAT INTELLIGENCE (NTI) PORTAL

In addition to Threat Intelligence Data Feeds, customers also have access to the NTI Portal as part of the offering. With the NTI Portal, users can:

» Gain additional insight into various threats/threat actors
» Research IP, domain, vulnerability, and/or malware Hash
» Gain hot intelligence and latest original vulnerabilities by quick query
» Create customizable views, searches, and results
» Upload logs for automated threat hunting
» Upload malware for automated analysis
» Monitor/track IP addresses with automatic notification





NSFOCUS RESEARCH TEAM

NSFOCUS Security Labs is composed of eight laboratories, with more than 200 full-time security researchers specializing in vulnerability discovery, attack and exploitation study, security threat monitoring, AI-based intelligence defense, big data, and cloud security. All data are fed into the NTI - NSFOCUS's intelligence brain, and translated into actionable insights.