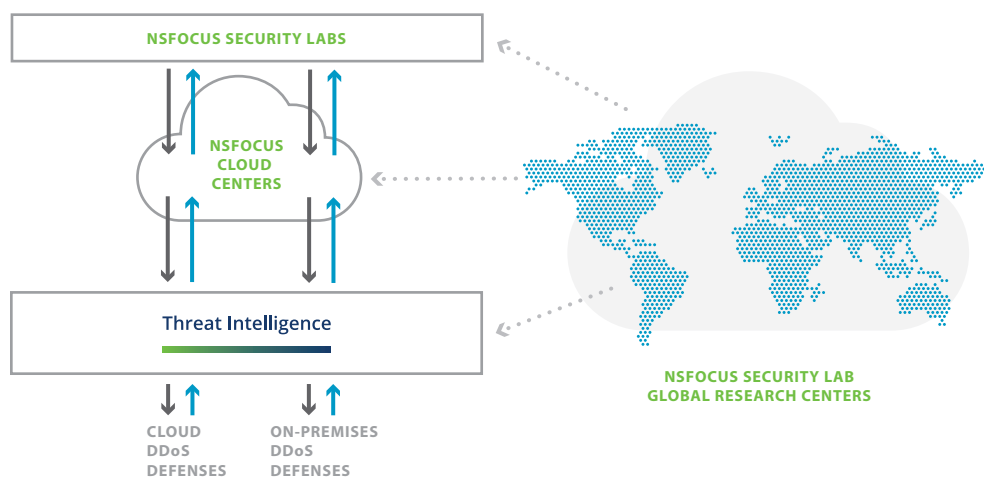# TI

Threat Intelligence

Modern day 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, rival companies. Even unwitting employees, customers, partners and private citizens' 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 (TI) Subscription Service provides you with actionable intelligence that minimizes your risk and improves your overall security posture.

GLOBAL THREAT INTELLIGENCE – INCLUDING CHINA

The NSFOCUS TI Subscription Service provides complete visibility into the global threat landscape. Because as much as 40% of the world's hacking activity originates from China, 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 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 of the evolving threat landscape possible. Having access to this unique intelligence enables our customers to implement countermeasures quickly to protect their critical assets.

ACTIONABLE THREAT INTELLIGENCE

Simply researching, understanding, analyzing, and reporting on new threat actors, vectors, and motivations is not sufficient to provide comprehensive security. In order to provide value, the intelligence must be actionable and incorporated directly into security policies to actively block intrusions. The NSFOCUS TI Subscription Service provides access to IP reputation, malicious Web/URL, command and control, and malware data feeds. These feeds have been integrated into NSFOCUS On-Premises and Cloud DDoS Defenses.

BENEFITS

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

Reduce operating costs through dynamic, automatic updates to security policies

Simplify threat hunting initiatives by identifying new and emerging threats

KEY FEATURES

Global threat intelligence
– including China

Actionable threat intelligence

Integration with NSFOCUS network and application security products

Extensive sensor and honeypot network

Regular and user configurable data feed update intervals

Standards-based API for 3rd party integration

THREAT INTELLIGENCE DATA FEEDS

The NSFOCUS data feeds themselves provide information in four crucial areas, and are delivered worldwide by strategically located NSFOCUS Cloud Centers:

IP Reputation Data Feed
This is a 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
This is a domain reputation list that includes malicious websites that are the source of malware or phishing attacks.

Command & Control Data Feed
This is a set of IP addresses 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
This is a 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 updated regularly 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 3rd 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 On-Premises DDoS Defenses to actively block all traffic originating from malicious sources. This information can also be applied to supporting 3rd party security products. These feeds enable you to implement a proactive, dynamic, and adaptive security model that 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.

Data Feed	SKUs	Capacity
IP Reputation	TI-IP-10	10
	TI-IP-50	50
	TI-IP-100	100
	TI-IP-250	250
	TI-IP-UL	Unlimited
Malicious Web/URL	TI-URL-10	10
	TI-URL-50	50
	TI-URL-100	100
	TI-URL-250	250
	TI-URL-UL	Unlimited
Command & Control	TI-CC-10	10
	TI-CC-50	50
	TI-CC-100	100
	TI-CC-250	250
	TI-CC-UL	Unlimited
Malware (Hash signatures)	TI-MW-10	10
	TI-MW-50	50
	TI-MW-100	100
	TI-MW-250	250
	TI-MW-UL	Unlimited