ATLAS Intelligence Feed Service

for NETSCOUT Threat Mitigation System

HIGHLIGHTS

Threat Intelligence Designed for the Network Perimeter

ATLAS® Intelligence Feed (AIF) for NETSCOUT® Threat Mitigation System (TMS) is a subscription-based service designed to optimize the TMS defenses to protect the network environments where deployed.

Key Benefits

Dynamic Updates for Accurate Protection – Updates with the latest threat information to maintain the most accurate detection policies.

Campaign-Based Attack Identification – Identifies singular points of compromise and related attacks that are part of an orchestrated campaign.

Fast Attack Response – Through the the use of a Mitigation Template, enables a faster, more informed response to DDoS protection.

Threat intelligence must be a part of your protection strategy. If you combine the sheer amount of Internet traffic your organization consumes with the number of security threats possible, you begin to see the risks your company faces. Having actionable intelligence could mean the difference between protected, versus unguarded. A strong security posture requires a combination of known effective defenses and fast analysis of data from the wild. This combination of intelligence can offer proactive measures that increase protection confidence.

The ATLAS Intelligence Feed service (AIF) provides you with tailored information about DDoS attacks relevant to your NETSCOUT Threat Mitigation System infrastructure (TMS). In this case AIF enables your TMS to perform its best for detecting and mitigating all forms of DDoS attacks via a unique and powerful fusion of:

- **People –** NETSCOUT's ATLAS Security and Engineering Research Team (ASERT) is an industry renowned elite group of security researchers and Super Remediators that routinely collaborates with government CERTS and is an active part of a large cybersecurity community.
- **Collections –** Cohesively known as ATLAS, years of unparalleled global collection consisting of anonymized data sent from over 350 Arbor product deployments, private and public threat intelligence sources, sinkholes, botnet monitoring, darknet forum monitoring, honeypots, and sinkholes.
- **Process –** Enrichment, Deep Behavioral Analysis, Recursive Introspection & Extraction, and Validation.

ATLAS Intelligence Feed in NETSCOUT TMS

Truly great threat intelligence goes beyond collecting and analyzing attack data. It should make a marked improvement over existing staff and processes. This information must be actionable through seamless integration into your security posture. The risk from each threat should be clear, and the actions to be taken should be evident. AIF, in conjunction with TMS, enables you to quickly address advanced attacks, whether they be DDoS-related or part of a larger advanced threat campaign against your organization. It consists of:

Early Warning System®	The difference between being ready for an attack versus reacting to an attack that is already in progress can represent long-term outage, and revenue loss. With the ATLAS Intelligence Feed, you also have access to an early warning service which provides targeted early warnings derived from NETSCOUT's botnet monitoring system and honeypot infrastructure, to ensure the maximum protection against DDoS attacks.
Application-Layer Signatures	More and more DDoS attacks are going after the application layer which are often more challenging for organizations to protect. With AIF for NETSCOUT Threat Mitigation System you are provided up-to-date signatures of botnet traffic for the most effective DDoS mitigation capabilities at the application layer.

DDoS Mitigation Template	It is sometimes difficult to know where to begin when trying to protect against all the known attacks, let alone the new attack types entering the network landscape. A DDoS mitigation template, refreshed monthly, helps protect you against late-breaking DDoS attacks by providing effective mitigation recommendations and best practices to ensure your unique environment is protected.
DDoS RegEx	There are common patterns across different DDoS attack types. DDoS RegEx identifies DDoS attackers based upon IP address indicators and also identifies DDoS targets based on indicators analyzed by NETSCOUT security researchers to quickly protect against multi-vector attacks. With the AIF service for your NETSCOUT Threat Mitigation System, regular expression analysis identifies attackers as well as the DDoS targets.

As new attack information is discovered, the ATLAS Intelligence Feed is updated, and changes are delivered automatically to your NETSCOUT Networks Threat Mitigation System via a subscription service over a secured SSL connection.

Effective threat intelligence requires three things:

1. Continuous source of real-world network traffic and data;
2. Robust infrastructure for gathering and analyzing network traffic and threat data; and
3. Dedicated team to manage data and add the "human intelligence" to the analysis.

Truly great threat intelligence goes beyond collecting and analyzing attack data. It should make a marked improvement over existing staff and processes. This information must be actionable and seamlessly integrated into your security posture. The risk from each threat should be clear, and the actions taken should be evident. The best way to be protected, is to have the most up-to-date intelligence from the broadest view, enriched by seasoned experts, and AIF for TMS enables you to quickly address multi-vector DDoS attacks.

LEARN MORE

For more information about ATLAS Intelligence Feed Service visit:

https://www.netscout.com/global-threat-intelligence

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECPDS_019_EN-1902 03/2019