ATLAS Intelligence Feed (AIF)

for NETSCOUT AED (Arbor Edge Defense)

HIGHLIGHTS

Threat Intelligence Designed for the Network Perimeter

ATLAS Intelligence Feed (AIF) for NETSCOUT AED is a subscription-based service that is specifically designed to maximize the functionality of the NETSCOUT AED product and protect the customer environments that it's normally deployed in.

The AIF for AED Service Components

Dynamic IP Geo-location – Provides up-to-date IP Geo-location by correlating multiple sources to ensure the best accuracy and visibility.

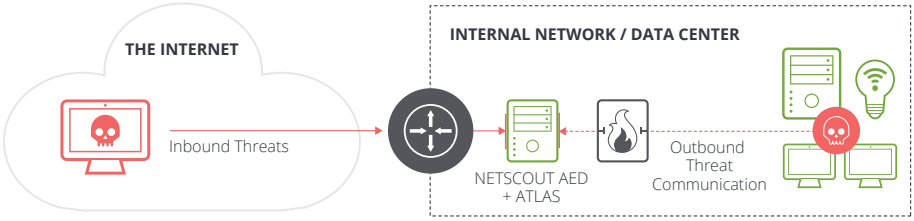
Crawlers – Provides up-to-date IP blocks from legitimate search engine bots to reduce false positives.

HTTP Regex & IOCs – Thousands of dynamically updated HTTP Regex & multiple types of Indicators of Compromise (IOCs) provide effective DDoS / APT detection & blocking.

Contextual Information - Context-rich intelligence to increase operational threat visibility and defenses.

DDoS Early Warning – With ASERT's presence in over 60 botnets, customers are provided an early warning and details of potential attacks targeting their organization.

As cyber threats continue to increase in frequency and sophistication, mature security teams will rely upon not only the latest cybersecurity technology, but also highly curated threat intelligence that arms these products enabling them to conduct more agile incident response and remediation- all to ultimately avoid the downtime or data breach which puts their organization in the news.



Deployed between the Internet router and firewall, NETSCOUT® Arbor Edge Defense (AED) acts as a first and last line of smart, automated, perimeter defense. Fueling NETSCOUT AED's high performing, stateless packet processing engine, is NETSCOUT's ATLAS Intelligence Feed (AIF) which is created 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, 11+ 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.

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.

The ATLAS® Intelligence Feed (AIF) from NETSCOUT, in conjunction with NETSCOUT AED, enables you to quickly address advanced attacks, whether they be DDoS-related or part of a larger advanced threat campaign against your organization.

ATLAS Intelligence Feed in NETSCOUT AED

One component of the ATLAS Intelligence Feed (AIF) subscription is a collection of HTTP Regex and Indicators of Compromise designed to maximize the effectiveness of the NETSCOUT AED. It consists of:

Reputation-Based Indicators of Compromise (IoCs) - Various types of threats that can be characterized by one or more communication endpoints including IP addresses, domains, and URLs. These types in this category include Adware, Backdoors, Banking, Credential Theft, Droppers, Exploit Kits, Fake AV, Point of Sale, Ransomware, Social, Spyware, Virtual Currencies, Webshells, worms, and others.
Campaigns and Targeted Attacks - This category includes various types of threats known to be associated with targeted attack activity. This category includes but not limited to elements such as Advanced Persistent Threats (e.g. APT DRPK, Operation Hangover, Fancy Bear), Hacktivism (e.g. Anonymous LOIC, JS-LOIC, SOIC tools), specific campaigns (e.g. Operation BlockBuster, Ghoul), RATs and Rootkits (e.g. Darkcomet, H-worm, njRAT, PLugX, Betabot, Blackenergy, Spyeye etc.)
Command & Control - Various types of cyber threats that generate outbound connectivity from internal compromised hosts to known Command and Control (C2) over HTTP (e.g. Emotet, LokiBot, Nymaim, TrickBot), IRC (e.g. DarkDOSer, pyLOIC), Peer-to-Peer (e.g. Hajime, Erzengel, Rex) and other protocols.
DDoS Attacks - Identify multiple types of DDoS attacks (i.e. Volumetric, TCP-state Exhaustion, Application-layer) that affect a variety of operating systems and infrastructure (e.g. Mirai, Emotet, Lizardstresser, XIR DOS, Armageddon, Athena, BroBot, DirtJumper, and many others)
Email and Mobile Malware - Various types of email threats (e.g. Phishing, SPAM) and mobile malware threats (e.g. malicious apps, spyware, CnC) that affect mobile devices such as Android and iPhone smartphones.

Early Warning System

The ATLAS Intelligence Feed (AIF) subscription provides more than just an intelligence threat feed. Another important component of AIF subscription is the Early Warning System. Behind NETSCOUT's ATLAS Intelligence Feed is the state-of-art Honeypot and Botnet monitoring system operated by ATLAS Security and Engineering Research Team (ASERT). When ASERT identifies or is alerted to a pending threat against one of a NETSCOUT Arbor customers, they will be notified and provided vital information (e.g. attack type, target IP address, domain, URL, ASN and CnC details) to prepare/mitigate the attack if it was to occur.

Additional Contextual Threat Intelligence

Another valuable component of the ATLAS Intelligence Feed subscription is the ability to provide additional contextual threat intelligence. When an IoC is detected and/or blocked with NETSCOUT AED, any additional information that exists in the vast NETSCOUT ATLAS Threat Intelligence database will automatically be provided. This additional contextual threat intelligence (e.g. malware samples, hashes, DNS resolutions and endpoint IOCs) enables cybersecurity teams to determine the risk to their organization; and/or using their arsenal of other security tools, proactively hunt for signs of compromise, eradicate and ultimately avoid the data breach.

LEARN MORE

For more information about NETSCOUT AED visit:

https://www.netscout.com/products/netscout-aed

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