ATLAS Intelligence Feed

For Arbor Availability Protection System and NETSCOUT AED (Arbor Edge Defense)

HIGHLIGHTS

- **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** – Provides valuable context to each attack, enabling a faster, more informed response.
- **Threat Validity & Prioritization –** Goes beyond collecting and analyzing threat data to validate that threats are real and current.

Given the influx of threats coming at your business from every possible angle, entry-point and vector, what do you need to stay ahead? Context can help you gauge risk, prioritize your security operations team's time, and move on to the next threat at hand. The right security intelligence fuels the creation of mechanisms to recognize and block network-based attacks. Security intelligence identifies attacks, but understands and catalogs the attack infrastructure, methods and other indicators so that broader measures can be taken with confidence.

Dynamics of an Effective Threat Intelligence Feed

Effective threat intelligence requires three things:

1. A continuous source of real world network traffic and data;
2. A robust infrastructure for gathering and analyzing network traffic and threat data; and
3. A 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 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 from NETSCOUT®, in conjunction with your Arbor Availability Protection System (APS) or NETSCOUT AED, enables you to quickly address advanced attacks, whether they be DDoS-related, or part of a larger advanced threat.

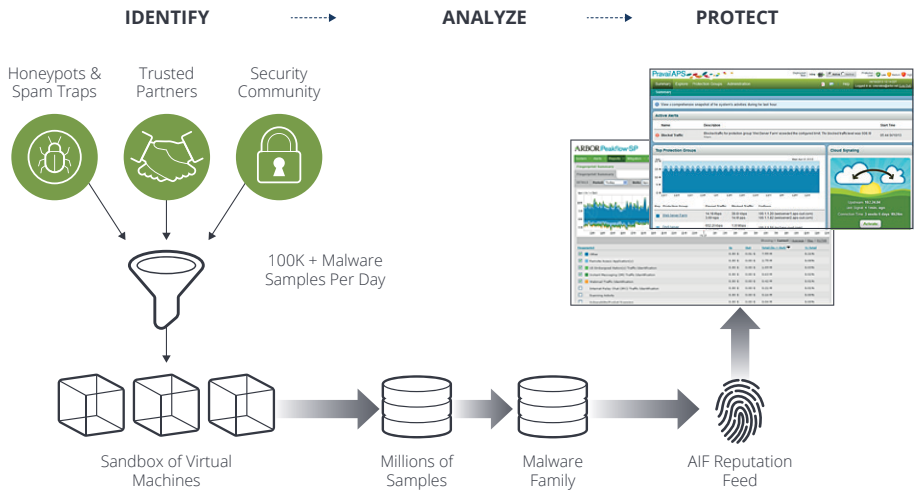

Figure 1: Workflow for threat intelligence feed analysis and development.

Applying Standard ATLAS Intelligence Feed

Standard ATLAS Intelligence Feed for Arbor APS or NETSCOUT AED offers you additional abilities to address some of the most prevalent attacks targeting organizations like you, including malware, botnets and DDoS attacks. The policies and countermeasures are updated with new attack information to provider broad, accurate detection. Beyond blocking threats based on bandwidth thresholds, the Arbor APS or NETSCOUT AED uses the threat feed policies to identify multiple types of attacks including 'low and slow' attacks aimed at the application layer. This feed helps detect and stop certain categories of botnets from compromising your network, enabling your security devices to do the jobs they were intended to do. Examples of the policies and countermeasures in the Standard ATLAS Intelligence Feed are found in Figure 2.

	Threat Policy Types		APS	AED
Command & Control	• Peer to Peer • HTTP • IRC		✓	✓
DDoS Reputation Threats	• Attacker • Target		✓	✓
Malware	• Webshell • Ransomware • RAT • Fake Anti Virus • Banking • Virtual Currency • Spyware • Drive By • Social Network	• DDoS Bot • Dropper • Ad Fraud • Worm • Credential Theft • Backdoor • Exploit Kit • Point of Sale • Other	✓	✓
IP Geo Location	• Identification by country for sources of inbound traffic • Identification by country for destinations of outbound traffic		✓	✓
DDoS RegEx	• Identifies DDoS attackers based upon IP address indicators from ATLAS • Identifies DDoS targets based on indicators from ATLAS HTTP Flooder		✓	✓
Web Crawler Identification	Identifiy inbound connections to web services from known search engines		✓	✓

Figure 2: Example threats identified using the AIF Standard feed. All countermeasures and policies are continuously updated, so above list may change at any time.

Applying Advanced ATLAS Intelligence Feed

The Advanced ATLAS Intelligence Feed is designed for organizations that are concerned with stealthy, more subtle attacks. With these advanced features you get all of capabilities included in the Standard feed, along with additional policies for uncovering attack behaviors indicative of ongoing, campaign-style attacks–those that are highly customized to a specific businesses and difficult to detect as they may appear legitimate. Examples of such policies included in the Advanced feed are listed in Figure 3.

	Threat Policy Types	APS	AED
Location-Based Threats	• Traffic Anonymization Services • TOR • Proxies • Sinkholes • Scanners • Other	✓	✓
Email Threats	• Spam • Phishing	✓	✓
Targeted Attacks	• APT • Hactivism • RAT • Watering Hole • Rootkits	✓	✓
Mobile	• Mobile C&C • Spyware • Malicious Apps	✓	✓

Figure 3: Example threats identified using the AIF feed. Countermeasures and policies are continuously updated, so the above list may change at any given time. Policies in the Advanced subscription are currently not available to SP, TMS or Cisco ASR 9000 DDoS Protection customers.

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 Advanced ATLAS Intelligence Feed, you also have access to an early warning service which provides targeted early warnings about potential DDoS attacks as identified from NETSCOUT's ATLAS infrastructure which has visibility into one-third of the global internet traffic, and monitors 30+ active botnet systems.

As new attack information is discovered, the ATLAS Intelligence Feed is updated, and changes are delivered automatically to your Arbor APS or NETSCOUT AED via a subscription service over a secured SSL connection arming them with the latest threat intelligence. The best way to protect you is to have the most up-to-date intelligence from the broadest view, enriched by seasoned experts.

This world-class team of security researchers are dedicated to discovering and analyzing emerging internet threats and developing targeted defenses. Arbor employs a sophisticated combination of attack data collection, partner information and analysis tools to create policies that detect threats while providing context so that you can make informed protection and mitigation decisions. This is the ATLAS Intelligence Feed.

HOW DOES THIS FEED DETECT THREATS TO MY NETWORK?

- Identifies threats regardless of attack volume; no waiting for an attack to reach a volume threshold before defending.
- Uses multiple levels of protection aligning with confidence levels.
- Applies attack intelligence contributed from advanced controlled detonation of millions of malware samples.
- Includes reverse engineering of specific malware, and all malware related to a botnet.
- Actively monitoring Internet threats around the clock utilizing NETSCOUT's global Sensors network.
- Historical tracking of botnets, their location and attack methods over time.

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_012_EN-1805 10/2018