ATLAS Intelligence Feed (AIF) – The High-Octane Fuel of NETSCOUT Arbor Edge Defense

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). This paper will provide details behind the unique fusion of People, Collection and Process, which make up the AIF and allow NETSCOUT AED to be an effective network perimeter enforcement point.

This paper describes the process resulting in the delivery of Indicators of Compromise (IoCs) for threat detection in AED. The AIF subscription includes other relevant services. For the full list of services, consult the AIF for AED datasheet.

The People – ATLAS Security and Engineering Research Team (ASERT)

Super Remediators

As part of a group of experts known as super remediators, the ATLAS Security Engineering & Response Team (ASERT) delivers world-class security research and analysis

Behind NETSCOUT's AIF is the ATLAS Security and Engineering Research Team (ASERT). ASERT is a world-class security research and analysis team that is comprised of experts from diverse backgrounds including military intelligence, law enforcement, software engineering, cyber threat intelligence, malware reverse engineering, and data science. ASERT tracks more than 170 threat actor sets across 60 nations and monitors real-time communications from more than 60 botnets. ASERT routinely collaborates with many of the world's computer emergency response teams (CERTs) and governments. The team also participates in numerous trusted sharing groups and is an active part of a large cybersecurity community that is working behind the scenes to defend the world's digital infrastructure. For more than a decade, ASERT's world-class security researchers and analysts have been building the tools and front-line databases to analyze attacks and malware at internet scale.

Tangible examples of ASERT analysis manifest themselves in many places such as:

- The AIF, which continuously arms the NETSCOUT AED product with highly curated, actionable threat intelligence.
- The NETSCOUT Threat Intelligence Report https://www.netscout.com/threatreport, which highlights key trends and provides analysis of events we've seen across the threat landscape, including in DDoS, Crimeware, and APT.
- The ASERT Blog – http://www.netscout.com/asert, which discusses and provides deep analysis into the threat landscape, late-breaking events, and best practices in defense.

The Collections - Active Threat Level Analysis System (ATLAS)

11 Years

NETSCOUT Arbor has actively monitored this space since 2007, when the company launched its Active Threat Level Analysis System (ATLAS).

One-third of internet traffic statistics are shared by organizations (Including 90% of tier 1 service providers)
Through telemetry on a massive scale, ATLAS delivers unparalleled visibility into the backbone networks at the core of the internet.

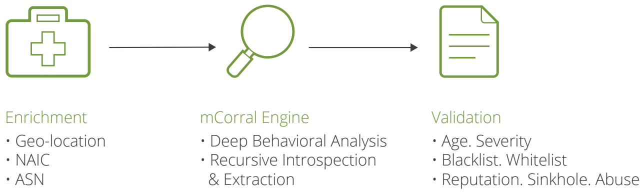
The system used to gather events and is the basis for analysis and conversion into global threat intelligence for NETSCOUT is called the Active Threat Level Analysis System (ATLAS). ATLAS provides ASERT unparalleled visibility at a global scale collecting, analyzing, prioritizing, and disseminating data on emerging threats across the internet, giving security teams relevant, actionable threat intelligence that can be used to defend against cyber threats in today's interconnected world.

Over 11 years in the making, ATLAS' internet-scale visibility into approximately 1/3 of the world's internet traffic provides ASERT a unique view into the threat landscape as demonstrated by a steady stream of discoveries and continuous protection for our customers.

A closer look at ATLAS, reveals multiple collections including:

- **Anonymized Feedback Data** – For almost 20 years, NETSCOUT Arbor Visibility and DDoS defense products have been deployed in a majority of the world's internet service provider and large enterprise networks. These products continuously send anonymized data back to ATLAS, providing information about observed DDoS attacks and other forms of cyber threats. This feedback also provides valuable victimology data, highlights trends into various attack groups, gives insights into specific malware families, peer, vertical and/or regional diversity. Today there are over 350 ISPs and numerous large enterprises sending data about DDoS and other attack activity to ATLAS. In this form, NETSCOUT operates one of the largest commercially run collection platforms in the world.
- **Public Data Sources** – Agreements with third parties and other holdings on the internet.
- **Private Intel Partners** – Relationships with worldwide cybersecurity researchers, 20+ malware sharing partners. This results in a continuous flow of indicators and malware samples, which are then analyzed and yield coverage across command-and-control infrastructure used by the adversary.
- **Darknet Forum Monitoring** – Conducting self-driven research or partnering with well-known intelligence providers in this space, ASERT monitors underground markets, darknet forums, ads for booters and stressers or bad actors advertising a new botnet. These forums host a plethora of DDoS for hire services, crimeware, banking malware, ransomware, key loggers, RATs. etc.
- **Honeypots** – ASERT has operated a growing number of honeypots for years to infiltrate and gain access to how botnets are being used. Most recently ASERT deployed a network of honeypots, which look like a collection of IoT devices deployed around the world, mimicking common protocols used by various IoT devices. The honeypot infrastructure provides visibility into the attack landscape as well as provides early access to malware that is dropped on such systems.
- **Botnet Monitoring in BladeRunner** – This system is designed to monitor botnet command-and-control communication, providing visibility into activity such as DDoS targeting as well as the introduction of new configurations such as web injects in malware families. ASERT also monitors a variety of downloader malware families to collect secondary payloads that are then pushed into their automated analysis pipeline.
- **Sinkholes** – ATLAS analyzes 60+ malware families around the world via sinkholes. These provide telemetry into communication where ASERT can look at check-ins and determine regionality, specific industry attack verticals etc.

The Malware Analysis Process – Rigorous & Highly Curated



Enrichment
- Geo-location
- NAIC
- ASN

mCorral Engine
- Deep Behavioral Analysis
- Recursive Introspection & Extraction

Validation
- Age. Severity
- Blacklist. Whitelist
- Reputation. Sinkhole. Abuse

Upon collection of hundreds of thousands of malware samples a day, a rigorous, but highly automated multi-phased process occurs. A brief description of each phase follows:

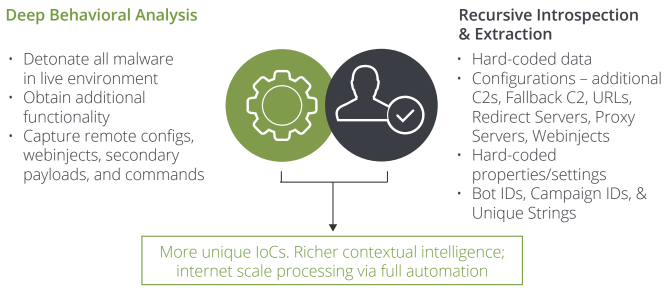
Enrichment

Regardless of the source of the data (see collections above), ASERT enriches data automatically using a variety of tools including cross-referencing to Geo-location, North American Industry Classification System (NAIC) codes, or Autonomous System Numbers (ASN). The objective is to add more context to the data and enable researchers and analysts to gain valuable insight into the threats they are facing. In addition to automated enrichment, ASERT also participates with numerous trusted research organizations and groups to collaborate with research and analysis. It enables ASERT to make better-informed decisions about the threats we are researching and provide value back to the community to better protect all organizations.

Where possible, ASERT pairs automated research and analysis process with intelligence gleaned from underground forums and market places. ASERT uses access to underground data for adversary tracking; keeping apprised of new threats in DDoS, IoT, and Crimeware; and bolstering research efforts as they pertain to client investigations, blogs, and customer alerting.

In addition to enriching data using external sources, ASERT also enriches data using a robust in-house dictionary comprised of overviews for malware families observed across a network. An indicator present in the AIF will have a direct correlation to a policy and name. Each of these policies will have a description of the malware threat and its general capabilities.

mCorral Engine – The Differentiator



Deep Behavioral Analysis

- Detonate all malware in live environment
- Obtain additional functionality
- Capture remote configs, webinjects, secondary payloads, and commands

Recursive Introspection & Extraction

- Hard-coded data
- Configurations – additional C2s, Fallback C2, URLs, Redirect Servers, Proxy Servers, Webinjects
- Hard-coded properties/settings
- Bot IDs, Campaign IDs, & Unique Strings

More unique IoCs. Richer contextual intelligence; internet scale processing via full automation

ASERT's homegrown mCorral engine is 10+ years in the making. It's what truly differentiates NETSCOUT's AIF from other threat intel sources. mCorral consists of dozens of sandbox machines, instrumented for IoC extraction. These sandbox machines execute in Linux, Mobile, and Windows environments and have the ability to process large-scale malware as well as phishing emails, malicious documents, and malicious URLs.

There are two main components to the mCorral engine:

1. **Deep Behavioral Analysis**

   On a daily basis, ATLAS harvests hundreds of thousands of malware samples. These samples are run through the mCorral engine where each sample is detonated in a live network environment. This live environment is important because a lot of malware will only reveal additional commands or downloads when they can reach out to C2 servers to gain additional instructions, configuration files, secondary payloads, etc. Unlike NETSCOUT, some feed vendors only analyze the binary in a non-live, static environment where they look at what they can see on the surface such as clear-text functions, strings, and PE header information – and then call it quits. Deep Behavioral Analysis in a live environment is important for ASERT to get the additional functionality, capabilities, remote configs, web injects, secondary payloads and commands associated with IoCs.

   For example:

   Dridex is a well-known banking trojan. By default, when you open up a Dridex infection it may only have a couple of surface level IoCs like a C2 IP address and a URL to a fake banking website where it will attempt to steal your banking credentials. If the detonation is done in a closed environment (i.e. no live access to the internet) additional information doesn't get exposed. When Dridex is executed in ASERT's mCorral's live environment, upon contact with a C2 more context is added to the IoC such as updated additional C2 servers, config files, additionally targeted institutions etc. This information gets resubmitted back into the engine to increase the number of IoCs into the AIF – which ultimately arms the NETSCOUT AED device.

2. **Recursive Introspection & Extraction**

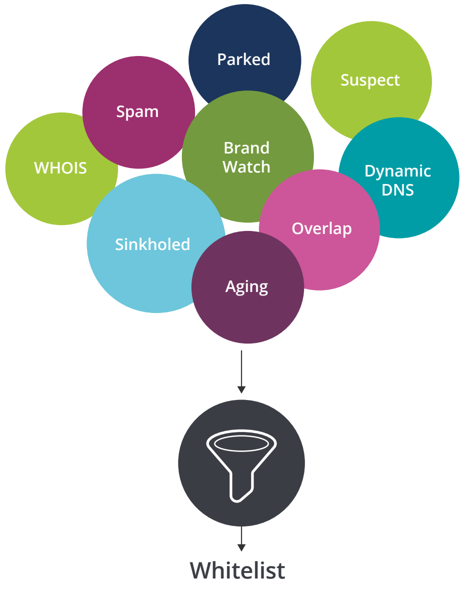
   After the live Deep Behavioral Analysis, mCorral engine looks for key characteristics matched to analyst-defined parameters and pushes matches through the Recursive Introspection and Extraction engine. This process consists of hundreds of custom analyzer modules that use memory dumps and PCAPs of network traffic to carve out additional IoCs. This introspection allows ASERT to carve out indicators that may be encrypted, or stored in such a way that any normal sandbox run, live or otherwise, would never extract the details. Not only does this produce more indicators pushed into AIF, those indicators are of much higher quality than those scraped from the surface of a particular malware sample. The high quality nature of these IoCs provide value to cybersecurity teams and threat analysts by fully extracting every possible indicator from a given malware sample and more holistically protecting their environments.

   Here's an example:

   Not all traffic or binaries are in clear text. In a static environment looking for surface level IoCs, these binaries would be ignored. To extract IoCs, these binaries require custom analyzers for decryption or decompression. Using their custom analyzers, ASERT can decrypt, decompress and/or reverse engineer the code to look at memory dumps or PCAPs enabling them to extract more data. ASERT's highly curated analysis strips out more unique IoCs, enriching context, and adds more value to the AIF arming the NETSCOUT AED product.

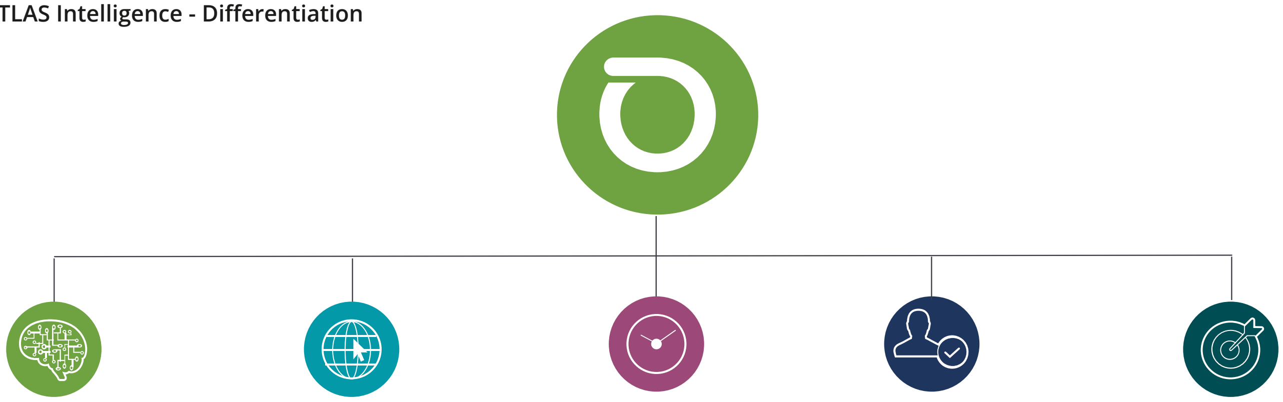
Validation, Whitelist and Confidence Score

The last step in the ASERT Threat Analysis process is Validation. The goal is to make sure only highly synthesized data is getting into the AIF to reduce false positives for NETSCOUT AED customers.



This Whitelist process includes monitoring for spam, parked domains, sinkholed domains, Who Is data, brand watch, etc. All of the indicators that make it into AIF pass through the Whitelist scoring pipeline and are weighted against dozens of criteria in an effort to eliminate false positives.

ATLAS Intelligence - Differentiation



Industry-renowned, elite security research group

Unparalleled data collections

Deep Behavioral Analysis

Recursive Introspection / Extraction

Accurate & effective scoring

People. Collection. Process

In addition, ASERT applies the notion of Confidence Scoring to each IoC. To determine a Confidence Score, ASERT's systems looks at a number of things including overlap with Spam list sources, contacts with sinkhole research servers, as well as lists of parked domains.

And lastly, ASERT then applies an Aging algorithm to add or remove IoCs. For example, a "High" confidence level is given when a threat is first directly observed. The added confidence level is given when a threat is observed again but decreased confidence level is added when the threat is not observed after a certain period of time. The goal is to provide quality vs. quantity of lower confidence IoCs in the NETSCOUT AED product.

The highly sophisticated process of Enrichment, Deep Behavioral Analysis, Recursive Introspection & Extraction, and Validation ensures that extraneous data is removed, leading to only pure synthesized, highly curated data being delivered through the AIF – ultimately to help customers block known bad traffic from entering or leaving their network.

One Final Validation Point:

Up to this point, this paper has described the unique, highly automated and curated process of NETSCOUT's AIF. But how do the results of this process compare to other threat intelligence feeds? In a comparison against 35+ open and commercial threat-intelligence sources, it was determined that 80% of IPs, 95% of domains, and 98% of URLs in NETSCOUT's AIF were unique.

Conclusion

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 that puts their organization in the news.

Fueled by the AIF consisting of:

- People – ASERT, industry renowned elite group of security researchers and Super Remediators.
- Collections – ATLAS, 11+ years of unparalleled global collection.
- Process – Enrichment, Deep Behavioral Analysis, Recursive Introspection & Extraction, and Validation.

NETSCOUT AED acts as the first and last line of smart, automated, perimeter defense for an organization.

LEARN MORE

For more information about NETSCOUT Threat Intelligence or NETSCOUT Arbor security products 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