AT&T Alien Labs™ threat intelligence

Powering timely, resilient threat detection and response

AT&T Alien Labs™ is the threat intelligence unit of AT&T Cybersecurity. Our research team delivers tactical threat intelligence that powers resilient threat detection and response — even as your IT systems evolve and adversaries change their tactics, techniques, and procedures (TTPs).

Alien Labs includes a global team of threat researchers and data scientists who, combined with proprietary technology in analytics and machine learning (ML), analyze one of the largest and most diverse collections of threat data in the world.

Collecting diverse threat data

Proprietary threat data from AT&T includes visibility into the AT&T IP network, our Unifed Security Management® (USM™) global sensor network, and the Open Threat Exchange® (OTX™) — a collaborative threat-sharing community of more than 100,000 IT and security professionals in 140 countries.

Figure 1: Alien Labs collects data from diverse, global sources and has visibility into and insights from the AT&T IP network.

With an unrivaled vantage point of the threat landscape, Alien Labs threat intelligence makes it easier for our customers to quickly identify, assess, and respond to threats.

- Large collection of threat data from diverse sources
- 100,000 contributors to the Open Threat Exchange
- In-depth threat analysis using analytics, machine learning, and a global research team
- Continuous feedback and refinement of threat models
- Direct integration with the USM platform
- Correlation rules mapped to Cyber Kill Chain® and MITRE ATT&CK™
- OTX integration with third-party security tools
- Support for managed threat detection and response

The volume of threat data Alien Labs collects across mutliple, global sources gives our Labs team unique visibility of the global threat landscape. This includes:

- Visibility into 220+ petabytes of traffic and 100 billion probes for vulnerabilities on the AT&T IP network
- Insight from analysts at 8 global SOC locations
- Observations of more than 20 million threats from our USM global sensor network
- Analysis of more than 250,000 suspicious files and 400,000 suspicious URLs

Powering resilient threat detection

Alien Labs goes beyond simply delivering threat indicators. We enrich our threat intelligence with qualitative research that provides insight into adversary TTPs. By identifying and understanding the behaviors of adversaries (and not just their tools) and supporting threat detection at multiple stages of an attack, we help power resilient threat detection even as attackers change their approaches or as an organization's IT systems evolve.

Alien Labs uses proprietary analytics, machine learning (ML), and a global team of threat researchers to validate, analyze, and interpret the large volume of threat data we collect. Our malware analysis technology includes, for example, use of sandboxing for dynamic analysis, agents for static analysis, and supervised machine learning (see figure 2).

Alien Labs curated threat intelligence is directly integrated with the USM platform for threat detection and response. For example, the Labs research team continuously updates intrusion detection system (IDS) signatures, Yara rules, and more than 850 correlation rules in USM on a daily basis. This helps decrease the time from public disclosure of a threat to customers being able to detect, investigate, and respond. Alien Labs also provides intelligence to help support the investigation of and response to threats.

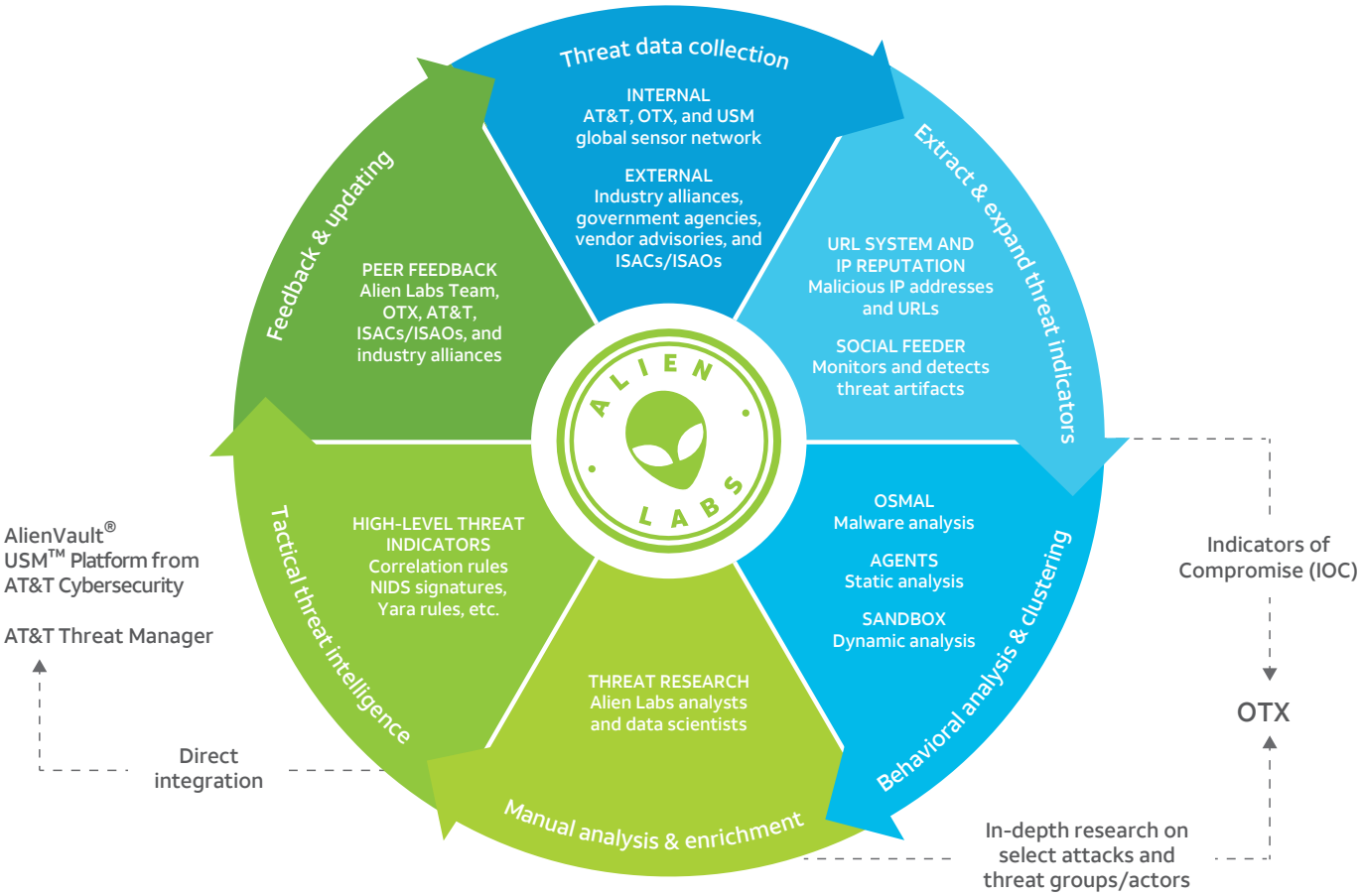

Figure 2: Alien Labs threat analysis and continuous feedback loop includes daily processing of more than 250,000 suspicious files and 400,000 suspicious URLs.

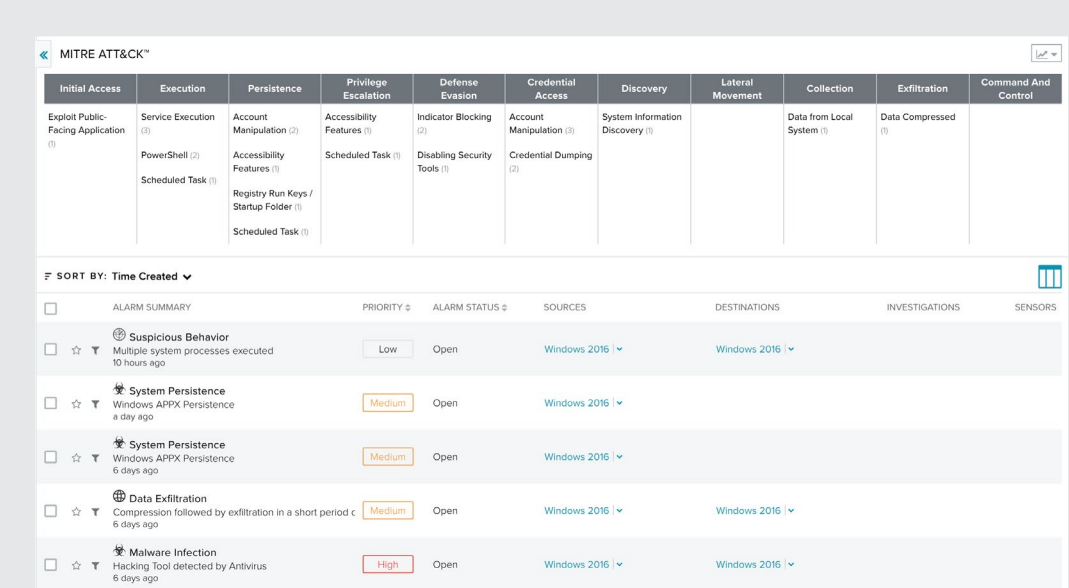

Figure 3: USM Anywhere threat detection and response dashboard. Alien Labs maps its correlation rules to the Cyber Kill Chain and the MITRE ATT&CK matrix.

To provide for vigilant coverage of adversary TTPs, Alien Labs maps its correlation rules to industry best-practice frameworks, including the Cyber Kill Chain® and the MITRE ATT&CK™. (See Figure 3).

Alien Labs also maximizes the expertise of our AT&T peer-group and threat-sharing community by continuously feeding knowledge back into our threat analysis systems, further refining our threat models, filling knowledge gaps, and quickly identifying emerging threats.

OTX: Supporting collaborative defense

The Open Threat Exchange (OTX) provides users the abiity to collaborate, research, and receive alerts on emerging and evolving threats with open integration to any security product.

Alien Labs collects threat indicators from the OTX community (including malicious IP addresses and URLs, domain names, malware samples, and suspicious files), runs the data through our analysis engine, and further researches high-priority threats. For example, the Labs team will reverse-engineer malware samples, do a "deep dive" into specific threat groups and their infrastructure, or analyze emerging variations of common cyberattacks, such as phishing, distributed-denial-of-service (DDoS), man-in-the-middle, (MitM), password attacks, and more.

OTX is free to join. Threat data on the platform is organized into "pulses" that provide context about threats as well as the TTPs adversaries use to orchestrate attacks, including the industries they are targeting.

OTX users can publish their own pulses and subscribe to the pulse feeds of others. Users can also create public and private groups to share threat data with peers, similar to what ISACs/ISAOs do today.

"Connecting the dots between seemingly different data points allows a defender to recognize relationships among incidents and identify common characteristics. This allows the analyst to understand the tactics, techniques, and procedures (TTPs) of their adversary."[1] – Forrester Research

1) Zelonis, J. (2017). Achieve Early Success in Threat Intelligence With the Right Collection Strategy. Retrieved from Forrester Research, Inc.

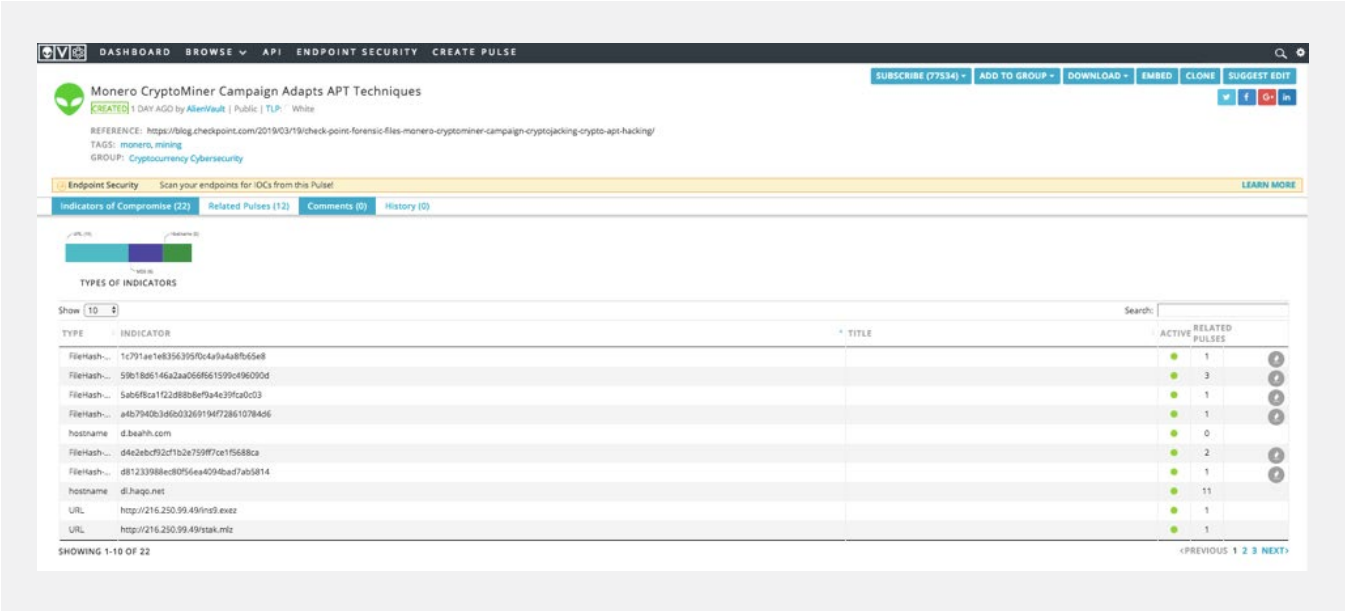

Figure 4: A pulse provides more context on a given threat.

Alien Labs regularly publishes IOCs and select threat research on threat actors and attacks to OTX. Users can subscribe to this feed to receive automatic alerts.

Users can also utilize OTX threat intelligence within their organization's security monitoring and management tools by taking advantage of our OTX DirectConnect API and DirectConnect SDK (software development kit). Learn more.

- Connect to the OTX API using DirectConnect Agents, which are available for several specific products and third-party tools.
- Connect through a USM Appliance and AlienVault OSSIM installation by simply entering an OTX API key from the USM Appliance OTX Configuration web page.

Additional resources

Alien Labs Open Threat Exchange Data Sheet

AlienVault USM Anywhere Data Sheet

AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide collaborative defense, security without the seams, and solutions that fit your business. Our unique approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning — helping enable our customers around the globe to anticipate and act on threats to protect their business.