ANOMALI® INTEL471

KNOW YOUR ADVERSARIES

Detect and respond to cybercrime threats with Anomali® and Intel 471

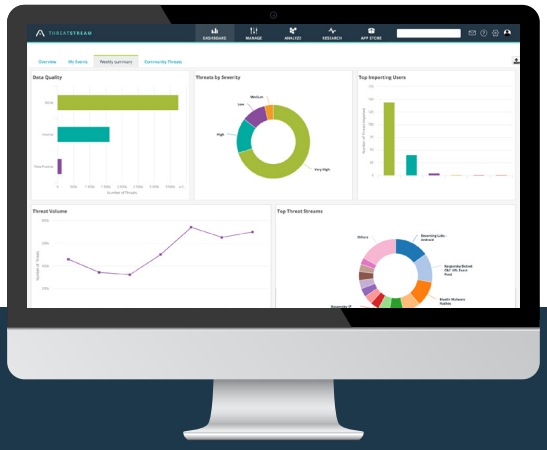
PREFERRED PARTNER

ANOMALI AND INTEL 471 JOINT SOLUTION FEATURES:

- The Anomali Threat Platform connects Intel 471's Cyber Underground Intelligence with your existing security stack to make it easier and faster to operationalize
- Prioritize threats that matter to you such as threat actors, exploits, malware, malicious infrastructure, and vulnerabilities to make informed security decisions
- Automate the ingestion of indicators and signatures into action–pivot on specific indicators, correlate observable types over a time range, and drill-down for highly contextual details
- Ingest technical data, finished intelligence, and human intelligence reporting from a globally dispersed capability fused with scalable collection capabilities

INGEST, ANALYZE, AND ACT:

- Ingest Intel 471's industry-leading Cyber Underground Intelligence alongside your other data and intelligence sources
- Analyze Intel 471's intelligence alongside other data sources
- Operationalize Intel 471's intelligence into your security stack



PROACTIVE CYBER UNDERGROUND INTELLIGENCE

The cyber underground threat landscape is continually expanding and as a result, organizations need credible intelligence and necessary context to visualize threats poised on the horizon. Security teams require solutions to help them respond faster, defend proactively, and protect efficiently—ultimately ensuring business continuity and resiliency. Intel 471 and Anomali equip businesses and their security teams with the right intelligence, enabling them with the best in class resources to reveal, prioritize, and prevent attacks before they occur.

TIMELY

Breaking insight and intelligence on the most sophisticated cybercriminals and damaging malware families.

RELEVANT

Intelligence directly related to your organization, your sector, your people and your supply chain.

ACTIONABLE

Intelligence that supports multiple use cases including executive support, security operations, vulnerability management, 3rd party risk, fraud, and more.

SECURITY OPERATIONS

CHALLENGE:

SOCs are overloaded with alerts and false positives, and it can be difficult to know what to investigate and when. Unless indicators are extremely timely and sourced with credibility and rich context, they won't successfully enable a prioritized response. SOCs have a high demand to detect cyber threats but need the right intelligence and capabilities to reveal and mitigate them.

SOLUTION:

Anomali's platform delivers Intel 471's Malware Intelligence, focused on the most impactful malware threats collected from monitoring malicious infrastructure. As soon as a cyber actor launches a new campaign, a SOC can ingest indicators rich with context such as expiry time, confidence level, MITRE ATT&CK tactics, TTPs, malware intelligence reporting, and more.

CUSTOMER BENEFIT:

Time is of the essence when faced with sophisticated cyber threats. SOCs are able to reduce false-positive alerts and prioritize resources against threats impacting what matters most: their people, assets, and business continuity. Having a source of technical indicators curated in near real-time from the underground enhances a SOC's ability to block and detect attacks before there are significant impacts on the organization.

3RD PARTY RISKS

CHALLENGE:

Today's organizations require a vast network of 3rd party suppliers and vendors to achieve their business objectives. The digital supply chain ecosystem has employees, customers, and other sensitive data spread across the globe, and there is a lucrative underground market where this information is highly sought after.

SOLUTION:

Intel 471 provides complete coverage of the underground, and delivers timely intelligence through Anomali to reveal threat actor communications aimed at buying and selling sensitive 3rd party data and access for suppliers, vendors, and employees. This includes the automated collection of intelligence elicited from actors in closed sources where automation is normally impossible.

CUSTOMER BENEFIT:

Anomali and Intel 471 clients can accurately apply intelligence against their internal 3rd party supplier databases to quickly and continuously assess potential exposure and risk. This joint solution enables organizations to proactively defend by getting close to the actors who pose the most impactful threats to their business.

APP STORE PREFERRED PARTNER COMPLIMENTARY OFFERING

Intel 471's Freemium Cybercrime Intelligence provides complimentary access to Intel 471's malware intelligence composed of three malware families (Emotet, Vidar and AZORult), and enables organizations to be proactive against cyber threats.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®