ANOMALI®

ThreatStream®

Threat Intelligence Platform

Anomali Match™

Threat Detection Engine

Anomali Lens™

Instant Threat Intelligence Access

Anomali®

Anomali harnesses threat data, information, and intelligence to drive effective cyber security decisions. It is a platform that automates detection, prioritization, and analysis of the most serious threats to your organization. With machine learning, automation, and an expansive partner ecosystem, Anomali empowers your analysts to leverage threat intelligence for better insights and response to cyber attacks.

Platform Benefits:

- Identify targeted threats to your organization
- Automate detection and analysis of threats
- Improve response with insights into threat actors and behaviors
- Save time and resources by reducing impact of attacks
- Allow for collaboration between internal and external CTI groups

ThreatStream®

ThreatStream is the Threat Intelligence Platform built for analysts to create threat intelligence and investigate security incidents. Collect, contextualize, and risk rank complex, high-volume indicators with machine learning to prioritize alerts and guide security strategy.

- Map threat intelligence to threat models (Actor Profiles, Campaigns, and TTPs)
- Aggregate OSINT, 3rd party, Labs, and ISAC data
- Automate workflows for quicker analyst insights
- Securely share and collaborate threat intelligence with trusted partners
- Integrate with SIEM, FW, Endpoint, IDS, API and more

Anomali Match™

Anomali Match is a Threat Detection Engine purpose-built to automate and speed time to detection in your environment. Anomali Match correlates twelve months of metadata against active threat intelligence to expose previously unknown threats to your organization.

- Evaluate exposure to current and historical threats
- Automatically tie indicator matches to threat models (e.g. CVEs and MITRE ATT&CK)
- Review assets with known CVEs and associate to Anomali Match rules and alerts
- Prioritize analysts' work with high- fidelity alerts
- Review timeline of incidents and anatomy of attacks
- Detect and alert on traffic to DGA domains with 90%+ accuracy

Anomali Lens

Lens enables threat and security analysts to make faster and more accurate decisions. Lens provides instant access to strategic and tactical intelligence from any mobile or browser page. Analysts at all levels are empowered with real-time scores and context that accelerates decision making. Executives can easily access threat intel on their devices to stay informed about the latest threats to their business.

Threat Intelligence Sharing

Anomali provides a complete threat sharing platform for ISAC and ISAO partners to power secure sharing and collaboration. Partners leverage ThreatStream to offer their members a branded threat sharing portal with community training, education, and an Anomali Analyst license.

- Dedicated Trusted Circle in Anomali
- Admin access to vet and control membership
- STIX/TAXII server for programmatic access
- Industry-specific tactical and operational research from Anomali Threat Analysis Center

APP Store

The Anomali APP Store is a unique cyber security marketplace providing instant access to a growing catalog of threat intelligence providers,integration partners, and threat analysis tools.

SDKs

The Anomali SDK Suite is an open and integrated ecosystem that brings a new level of customization and capability to your security program.

Technology Partners

Leverage the Feeds, Enrichments, Integrations, and ULink to unite security solutions and increase collaboration.

- ***Feeds*** — Integrate proprietary threat intelligence feeds
- ***Enrichments*** — Develop custom data enrichments
- ***Integrator*** — Create downstream integrations with SIEM firewalls, endpoint systems and other security and IT solutions
- ***Universal Link*** — Create upstream links that ingest data from vulnerability scanners, big data, SIEM, and other security and IT solutions

Professional Services

Workflow Service

- Tailors tactical-level, operational, and strategic threat intelligence workflows to your organization
- Improves operational efficiency by aligning process and collaboration to platform functions
- Refines tasks, processes, and orchestration
- Provides KPIs to help determine proficiency and maturity of your CTI program

Intelligence Augmentation Service (IAS)

- Request custom research on specific threats in your environment
- Malware analysis and triage
- Context surrounding IOCs and intelligence analysis
- Actor, TTPs, signatures, etc.
- Executive summaries and regular reporting

Premium Domain Monitoring Service

- Track suspicious domain registrations
- Alerts for newly registered domains
- Receive Threat Bulletins with domain details
- Receive associated IOCs for further investigation

Custom Integrations, Feeds, and SDK Support

- Create custom integrations and feeds
- Receive support for SDK usage

Community

Weekly Threat Briefing

- Digest of key security threat news
- Recommendations for response
- Every security alert includes specific, associated IOCs
- Integrates with ThreatStream, Anomali Match, Splunk App

STAXX

- Subscribe to any STIX/TAXII feed
- Preconfigured with Limo, a curated list of intelligence feeds
- Investigation portal for advanced analysis
- Installs in minutes; simple configuration wizard

ANOMALI®

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