ANOMALI
THREATSTREAM

GET RELEVANT, ACTIONABLE INTELLIGENCE TO MAKE INFORMED DECISIONS

A WORLD OF THREAT INTELLIGENCE—MADE USEFUL

To fully protect your organization, you need to see and understand every threat, identify which ones are a priority, and connect that information to your workflows for a fast, effective response. At most organizations, the problem isn't a shortage of threat data—it's information overload. To make this information truly useful, you need to quickly understand what's relevant to your environment, evaluate it in context, then put it to work. The Anomali ThreatStream Threat Intelligence Platform aggregates data from multiple sources to deliver operationalized threat intelligence that helps you understand your risk, make informed and proportionate decisions, and improve your security posture.

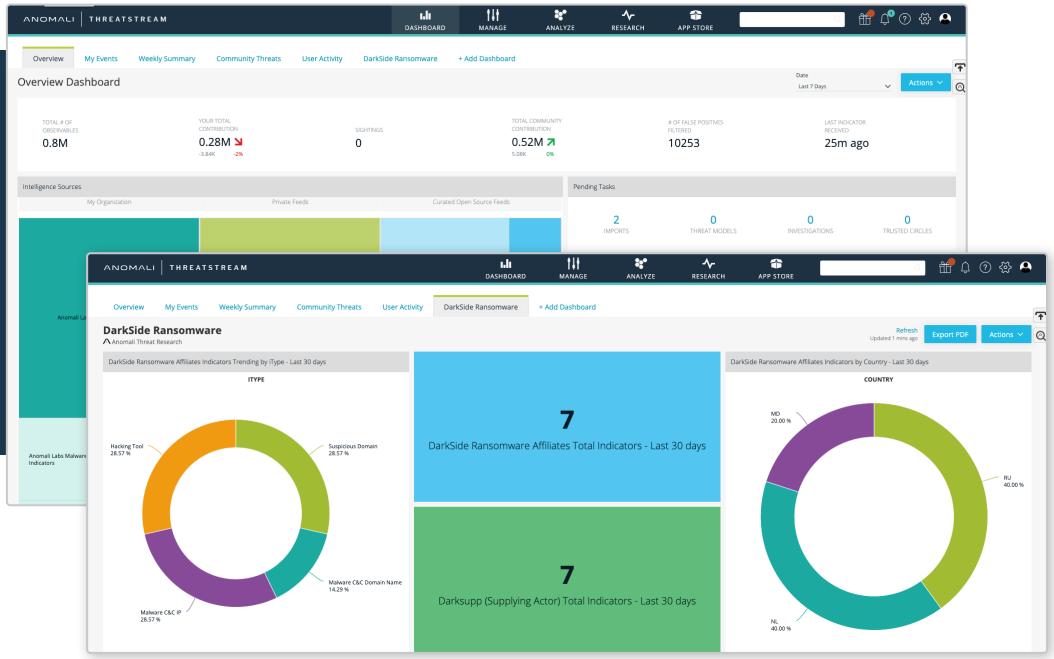
ThreatStream makes intelligence actionable by:

- Reducing noise by removing duplicate, out-of-date, and inaccurate information
- Delivering a prioritized list of the information that's relevant to you
- Enriching information for full context and significance
- Connecting threat data to threat models and workflows
- Distributing machine-readable threat intelligence across your security stack
- Supporting collaboration and information sharing across the security community

BENEFITS

- Stay ahead of relevant emerging threats to cut through the noise and focus on what matters to you
- Reduce the risk of security breaches with automated distribution of intel to your security controls
- Improve operational efficiencies with Automated intel collection, curation, and enrichment
- Research, pivot on, and investigate threats, TTPs, and actors
- Improve security team productivity to reduce risks and potential impact of security breaches
- Secure threat sharing across trusted communities to power secure collaboration
- Find and evaluate third-party threat feeds, intel, and tools quickly in an integrated threat intelligence marketplace to

Automate and accelerate the process of collecting all relevant global threat data, giving you the enhanced visibility that comes with diversified, specialized intelligence sources, without increasing administrative load.



KEY FEATURES

COLLECT

Capture all relevant global threat data automatically for enhanced visibility without increasing administrative overhead.

- **Automated threat data collection** from hundreds of diverse sources of threat intelligence and machine-readable IOCs, including Anomali Labs curated feeds, open-source OSINT feeds, specialized premium feeds, and information sharing and analysis centers (ISACs)
- **Contextualized information** enriched with relevant actors, campaigns, and tactics, techniques, and procedures (TTPs)
- **Commercial threat feeds** that can be easily trialed and licensed via the integrated Anomali APP Store marketplace

MANAGE

Curate diverse threat intelligence into a single set of normalized, actionable data.

- **Data deduplication and false positive removal** at scale to deliver high-fidelity threat intelligence
- **Threat intelligence scoring** for confidence and severity with a powerful machine learning algorithm
- **Global Intelligence feed ROI optimizer** to assess sources based on score, quality, and organizational relevance

INTEGRATE

Deliver operational threat intelligence to your security controls for real-time blocking and monitoring.

- **Turnkey integrations** with leading enterprise SIEMs, firewalls, EDRs, and SOARs
- **Extensible platform** with restful API and SDKs for feeds, enrichments, and security system integrations
- **Security tool integration** for inbound data ingestion and outbound response orchestration via API/appliance

INVESTIGATE

Accelerate insights with an integrated platform and investigations workbench for analyst research, analysis, and finished intelligence publication.

- **MITRE ATT&CK mapping** with an immediate view of global threats impacting your organization's security posture
- **Visual link analysis investigation** to expand from indicator to associated higher-level threat models
- **Integrated sandbox detonation** of suspicious files for investigation and MRTI for dissemination

COLLABORATE

Distribute and collaborate on threat intelligence with your peers and partners

- **Collaborative threat visibility and identification** in ThreatStream Trusted Circles (used by over 2,000 organizations) for secure rapid response and ongoing intelligence collaboration with industry peers
- **STIX/TAXII compliant** for bi-directional intelligence exchange between TAXII servers and clients
- **High-quality publishing** to distribute threat bulletins and other finished intelligence products to stakeholders at your desired level of detail

KEY USE CASES

AUTOMATE YOUR INTELLIGENCE-GATHERING
Centralize the collection, curation management, normalization, and integration of threat intelligence from all sources into your operational environment.

GET THE THREAT INTELLIGENCE YOU NEED
Find, evaluate, and integrate the right premium threat intelligence feeds and indicator enrichments for your organization.

IMPROVE THE EFFECTIVENESS OF YOUR SECURITY CONTROLS
Enable real-time blocking and monitoring while reducing false positives.

PROFILE YOUR ADVERSARIES
Quickly understand the context of SIEM and SOAR alerts with analysis across actors, campaigns, incidents, malware, signatures, TTPs, and vulnerabilities.

SHARE THREATS ACROSS TRUSTED COMMUNITIES
Securely collaborate with internal colleagues and peers at similar organizations to speed threat identification and get advice to help manage threats.

ABOUT ANOMALI

Anomali provides threat detection and response solutions that enable cyber resilience and elevate a cyber-fused response using integrated threat intelligence. Anomali extends and amplifies threat visibility by curating structured and unstructured global intelligence and security incident data to inform decisive response.

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

ANOMALI™