Anomali ThreatStream

Get actioned visibility into your adversaries

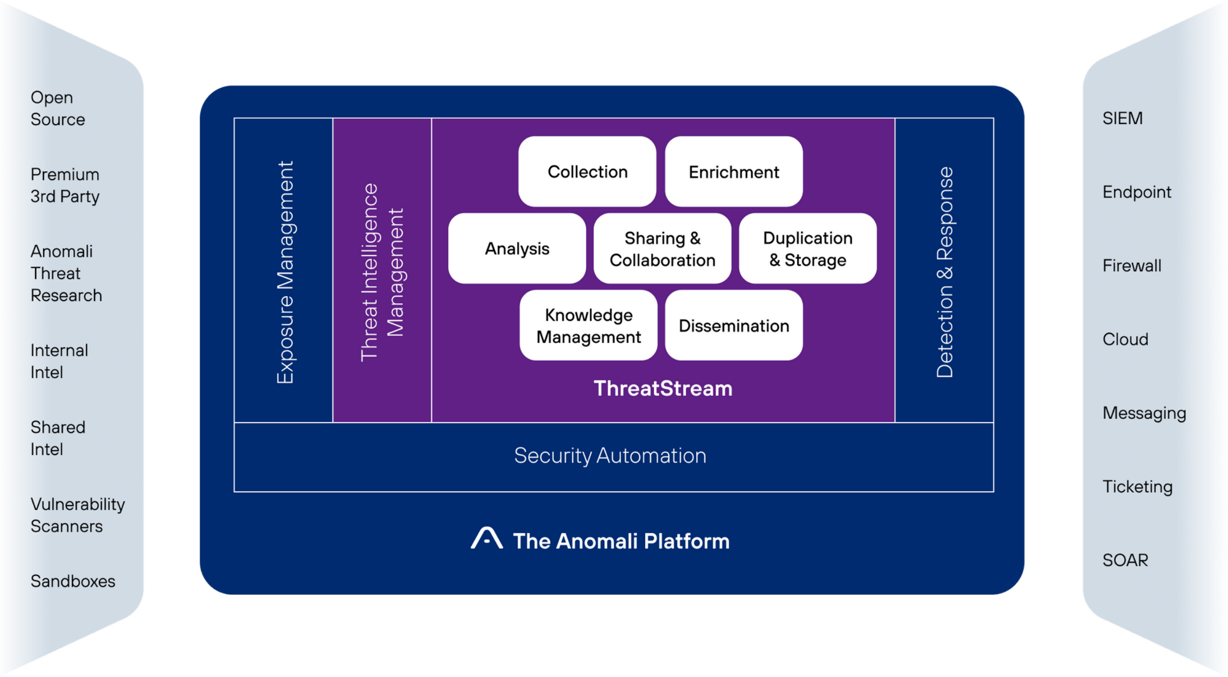
As cybercrime intensifies, security teams face the challenge of managing vast amounts of threat data, identifying and prioritizing the most relevant threats, and feeding that information into security controls and workflows—and do it fast, before attackers have a chance to strike.

Anomali ThreatStream transforms raw data into actionable threat intelligence and insights so you can make informed decisions, respond quickly, and block threats in real time.

Threat intelligence from hundreds of diverse sources is curated, centralized, and enriched to provide context for SOC alerts and investigations. Relevant intelligence is distributed automatically across your existing security controls to stop breaches and strengthen your attack surface. An integrated investigations workbench deepens insight and accelerates threat research.

BENEFITS

- Cut through the noise to focus on relevant emerging threats
- Reduce risk with automated distribution of intel to your security controls
- Improve security team productivity and operational efficiency
- Research, pivot on, and investigate threats, TTPs, and actors
- Distribute machine-readable threat intelligence across your security stack
- Find and evaluate third-party threat feeds, intel, and tools quickly
- Collaborate and share threats securely across trusted communities



Connecting the Anomali Security Operations Platform to the global community of cybersecurity researchers, ThreatStream puts the world's largest repository of actioned intelligence at your fingertips. High-quality data helps teams investigate security events and assess threats in real time. Filtered for relevance and pushed into Anomali Match, ThreatStream intelligence can be correlated automatically with vulnerabilities in your own environment to enable analytics-powered security operations.

Transform raw threat data into visibility and insight

As a high-performance threat intelligence management platform, ThreatStream curates and enriches raw data from hundreds of diverse sources of threat intelligence, including Anomali Labs curated feeds, open-source OSINT feeds, specialized premium feeds, and information sharing and analysis centers (ISACs). Real-time dashboards and machine-readable threat intelligence help security teams work quickly and effectively to assess, prioritize, and proactively stop threats.

Capture all relevant global threat data

Automated intelligence collection, curation, and enrichment helps security teams quickly understand the context of SIEM and SOAR alerts with analysis across actors, campaigns, incidents, malware, signatures, vulnerabilities, indicators of compromise (IOCs), indicators of attack (IOAs), and attacker tactics, techniques, and procedures (TTPs).

To ensure relevance and quality while reducing noise, threat intelligence is correlated to your industry, sector, technology, and geography with duplicate, out-of-date, and inaccurate information removed. Third-party threat feeds, enrichments, and tools can be easily trialed and licensed in an integrated threat intelligence marketplace to enhance and customize your threat intelligence resources.

Gain visibility and insight into relevant threats

Threat intelligence sources are assessed and optimized based on quality and relevance to your organization, and individual threats are scored for confidence and severity using a powerful ML algorithm. Dashboards provide instant visibility into key metrics on all your threat data, and powerful reporting tools help you share intelligence with the right level of detail for diverse stakeholder personas.

Deliver operational threat intelligence across your security controls

Built on an extensible platform with a restful API and SDKs, ThreatStream allows turnkey integration with leading enterprise security controls including SIEMs, firewalls, EDRs, and SOARs for both inbound data ingestion and outbound response orchestration. Real-time, automated blocking and monitoring enable a rapid response to potential attacks.

Accelerate research and investigations

An integrated platform and investigations workbench for analyst research, analysis, and finished intelligence publication accelerates insights. MITRE ATT&CK mapping provides an immediate view of global threats impacting your organization's security posture, with visual link analysis investigation to expand from indicator to associated higher-level threat models. An integrated sandbox allows detonation of suspicious files for investigation.

Distribute and collaborate on high-quality intelligence

Used by over 2,000 organizations, ThreatStream Trusted Circles enable threat visibility and identification, secure rapid response, and ongoing intelligence collaboration with industry peers. Within your organization, reporting and publishing tools make it simple to distribute threat bulletins and other finished intelligence products to stakeholders at your desired level of detail.

Key Use Cases

Monitor the threat landscape

Know your adversaries with visibility and analysis across relevant actors, campaigns, incidents, malware, signatures, TTPs, and vulnerabilities

Automate and manage the intelligence lifecycle

Enable fast, efficient threat intelligence collection, curation, integration, analysis, and publication

Enhance security control efficacy

Automate real-time intelligence distribution for proactive blocking and monitoring

Enrich SecOps workflows

Accelerate triage and incident response with attacker insights, TTPs, attack flows, and related observables

Enable collaboration

Securely collaborate with internal colleagues and peers at similar organizations to speed threat identification and get advice to help manage threats

ANOMALI