

1 0 0
0 1 1
0 0 1
1 0 0
0 1 0
1 0 0
0 1 1
1 1 0
0 0 1
1 0 0
1 0 1
0 0 0
0 1 1
0 0 1
0 1 0
1 0 0
0 1 0
1 1 0
0 1 1
1 0 0
1 1 1
1 0 0
0 1 1
1 0 1
0 1 1
1 1 0
0 1 1
1 1 0
1 1 1
1 0 0

ANOMALI[®]

THREAT PLATFORM FOR BUSINESS RISK

ThreatStream[®]

The most widely adopted
Threat Intelligence
Platform

Anomali Enterprise[®]

Uncover existing threats in
your data

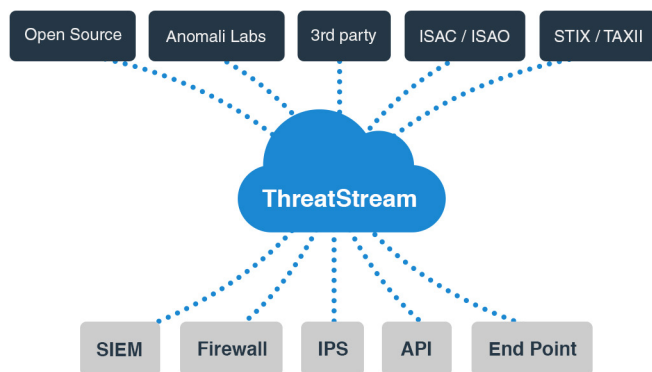
STAXX[™]

Free, easy way to
subscribe to any STIX/
TAXII feed

ThreatStream®

Threat Intelligence Platform

ThreatStream enables enterprises to create their most strategic and streamlined defense. Complex, high volume threat data is automatically aggregated, enriched, and integrated into existing solutions, freeing analysts to generate threat intelligence to inform security decisions.



- Aggregate threat data from any intelligence source
- Normalize, de-duplicate, and enrich threat intelligence data
- Integrate IOCs into SIEMs, firewalls, endpoints, or via API
- Identify threats based upon risk with Anomali Enterprise

STAXX™ *Free STIX/TAXII Solution*

STAXX gives you a free, easy way to subscribe to any STIX/TAXII feed. Simply download the STAXX client, configure your data sources, and STAXX handles the rest.

- Installs in minutes; simple configuration wizard
- Powerful search and dashboarding features
- Export IOCs for internal integration
- Investigate IOCs with free STAXX online portal



0 0 0
1 1 0
0 1 1
0 1 0
1 0 0
0 0 1
1 1 0
1 0 1
0 1 1
0 0 0
0 1 0
0 0 0
1 1 0
0 1 1
1 0 0
0 0 1
1 0 0
1 0 1
1 1 1
0 0 1
1 1 0
0 1 1
1 1 0
1 0 1
1 1 1
1 0 1
1 1 1
0 0 1
0 1 0

1 0 0
0 1 1
0 0 1
1 0 1
0 1 0
1 0 0
0 1 1
1 1 0
0 0 1
1 0 0
1 0 1
0 0 0
0 1 1
0 0 1
0 1 0
1 0 0
0 1 0
1 1 0
0 1 1
1 0 0
1 1 1
1 0 0
0 1 1
1 0 1
0 1 1
1 1 0
0 1 1
1 1 0
1 1 1
1 0 0
1 0 1

Anomali Enterprise™

Uncover Existing Threats

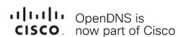
Anomali Enterprise exposes previously unknown threats in your enterprise by correlating internal events with threat intelligence. This enables rapid detection and response and reduces the potential impact of incidents and breaches.

- Identify past and current incidents
- Search retrospectively across 365+ days of data
- Generate internal threat intelligence
- Share and collaborate through ThreatStream

Anomali Integrations

Rapidly Operationalize Threat Intelligence

Anomali offers pre-built, fully supported integrations with SIEMs, firewalls, endpoint systems and other security and IT solutions. Restful APIs also allow for custom integrations.



Apps and Add-ons

Limo

Limo is an out-of-the-box TAXII service for users who want to get started with threat intelligence and stay up to date on the latest threats.

- Fully STIX 2.0/TAXII compliant
- Pre-configured in Anomali STAXX
- Intelligence from open source, Anomali Labs, and MHN feeds

APP Store

Anomali offers a threat intelligence directory where organizations can access premium feeds from partners.

- Trial and evaluate different feeds
- Purchase feeds directly within the Anomali platform
- Integrate feeds with internal systems via ThreatStream

Weekly Threat Briefing

Anomali Labs issues a Weekly Threat Briefing containing a digest of key security threat news and recommendations for response.

- Every security alert includes specific, associated IOCs
- Health Check feature lets you evaluate your exposure
- Integrates with ThreatStream, Anomali Enterprise, Splunk App

Professional Services

Augment your Threat Intelligence Program

Workflow Service

- Creates tactical-level threat intelligence workflows
- Improves operations
- Refines tasks, processes, and orchestration
- Customized to your use cases and environment

RFI Service

- Request personalized, custom research on specific threats in your environments
- Malware analysis and triage
- Context surrounding IOCs
- Intelligence analysis
- Actor, TTP, signatures, etc.

Domain Monitoring Service

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