ANOMALI

Solutions Brief

ANOMALI FOR ISACS

Solutions Overview

OVERVIEW

ISACs (Information Sharing and Analysis Centers) are sector-specific organizations (created by Presidential Directive 63 in 1998) as a mechanism to share information about IOCs with the broader community at risk. This was subsequently expanded in 2015 to an ISAO (Information Sharing and Analysis Organization) to include any "sector, subsector, region or any other affinity".

COMMUNITY-SHARING MODELS

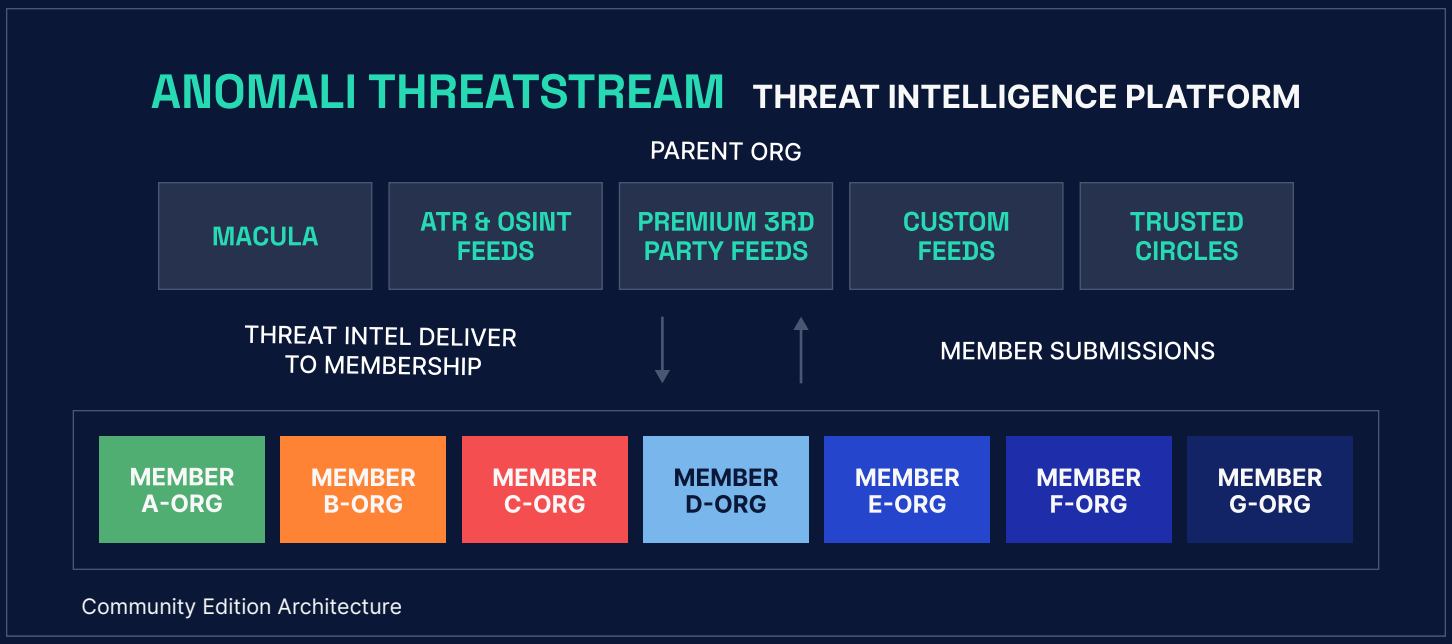
There are multiple community-sharing models, including:

- Dedicated ISACs/ISAOs – dedicated analysis centers with security intel capability that are sector-focused (Healthcare, Financial Services, Energy, Multi-state, Elections Infrastructure, etc.).
- Managed Security Services and Resellers – for example, Verizon VTIPS.
- Holding Companies – where enterprise customers share intel with downstream entities.
- Special Events – where security sharing around high profile events (Super Bowl, Elections, etc.) are implemented.

ANOMALI COMMUNITY EDITION (CE)

Anomali's Community Edition (CE) is an offering that provides a (parent) company the rights and means to share intelligence with other organizations (members), with the following variables:

- CE customers might charge for their services.
- Recipients of intel do not have to be a ThreatStream customer.
- The parent collects and curates intelligence through ThreatStream and then shares the finished intelligence downstream with members.
- CE is built on ThreatStream Trusted Circles.
- Parent has full ThreatStream capabilities.
- Members have access to a limited ThreatStream portal (some have access to STIX TAXII feed).



Community Edition Architecture

COMMUNITY EDITION FEATURES

The table below outlines the features available to Community Edition (Member) users compared to Anomali ThreatStream Next-Gen Enterprise (Parent) users:

FEATURES	COMMUNITY EDITION (MEMBER)	THREATSTREAM NEXT-GEN ENTERPRISE (PARENT)
Threat Intelligence Collection		
Multiple ISAC Sources	✓	✓
Simple Intel Submission Workflow	✓	✓
Manual Export — Observables in STIX, Threat Models in PDF	✓	✓
TAXII Server*	✓	✓
Anomali Open Source Feeds		✓
Anomali Premium Feeds		✓
Marketplace — Anomali APP Store		✓
Freemium feeds from Anomali APP Store		✓

FEATURES	COMMUNITY EDITION (MEMBER)	THREATSTREAM NEXT-GEN ENTERPRISE (PARENT)
Feeds SDK		✓
Enrichments SDK		✓
Threat Intel Management		
User Accounts — Unlimited	✓	✓
Dashboard for searching, viewing, alerting	✓	✓
Feeds normalization, de-duplication, false-positive removal	✓	✓
Threat Models — MITRE ATT&CK, Diamond, Kill Chain	✓	✓
View full Threat Bulletins and Intelligence details pages	✓	✓
Investigations Workbench		✓
Anomali Enrichments — GeoIP/Open Ports/WHOIS History		✓
Anomali Agentic AI		✓
Threat Intel Integration		
Integrations Tier0 (API)		✓
Integrations Tier1 (SIEM)		✓
Integrations Tier2 (Endpoint, Firewall, SOAR, etc.)		✓
Integrations SDK		✓
Platform and Support		
Technical Support — Standard 24x7 Support	✓	✓
Dedicated Customer Success Manager		✓
Anomali University		✓

*TAXII Server access requires an additional purchase

LICENSING DETAILS

- The primary ISAC organization purchases ThreatStream Next-Gen Enterprise with pricing based on the size of the parent organization.
- The primary ISAC organization can add CE bundles in 20 member increments. Additional member licenses are sold individually as needed.

EXAMPLE USE CASE: STATE OF MARYLAND

The State of Maryland is seeing an exponential rise in cyber threats year over year. The latest signs are that the sector is under sustained and relentless attack from multiple adversaries, using an ever-increasing array of new techniques, tactics, and procedures (TTPs).

The financial and reputation repercussions of these attacks, and increased action by the regulatory bodies to hold companies to account with significant financial penalties, are putting pressure on the sector, forcing it to upskill and take a more proactive, intelligence-led stance on cybersecurity.

The State of Maryland is helping in the fight against cybercrime by enabling members to leverage a cyber threat intelligence platform to assist its members in defending against cybersecurity threats.

Powered by Anomali, the platform will enable users to centralize a range of data and intelligence for relevant authorities. The intention is for ongoing cyber hazards and risk to be tailored specifically for Local, Tribal, and Territorial governments.

The Anomali Community Edition is designed to enable the secure, meaningful, and automated sharing of relevant threat data (IOCs) via bi-directional TAXII capabilities. Strategic intelligence around threat actors, campaigns, TTPs, vulnerability, and other models can be distributed to all participants. This allows community members to take a proactive approach by gaining insight into their adversaries.

Participating members can gain additional benefits by upgrading to Anomali's enterprise-grade solutions to further operationalize the threat intelligence, through uniting all the tools in their security infrastructure, speeding the detection of threats, and enabling proactive defense measures.

CONCLUSION

Security threats are growing at an alarming rate, and are becoming far more subtle and sophisticated thanks to improvements in underlying technologies used by adversaries who are not hampered by rules of engagement. ISACs and ISAOs are particularly effective means of getting the word out quickly to relevant parties when a threat is detected. In the case of the state of Maryland, the ISAC was able to shut down threats to state agencies before the threat was able to take hold. This is a very effective and comprehensive solution to sectoral threats and is driven by the industry's largest threat intelligence repository.