ANOMALI

ISAC

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 and Analysis Sharing Organization to include any "sector, subsector, region or any other affinity".

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'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)

ISAC’s are just one use-case for Community Edition.

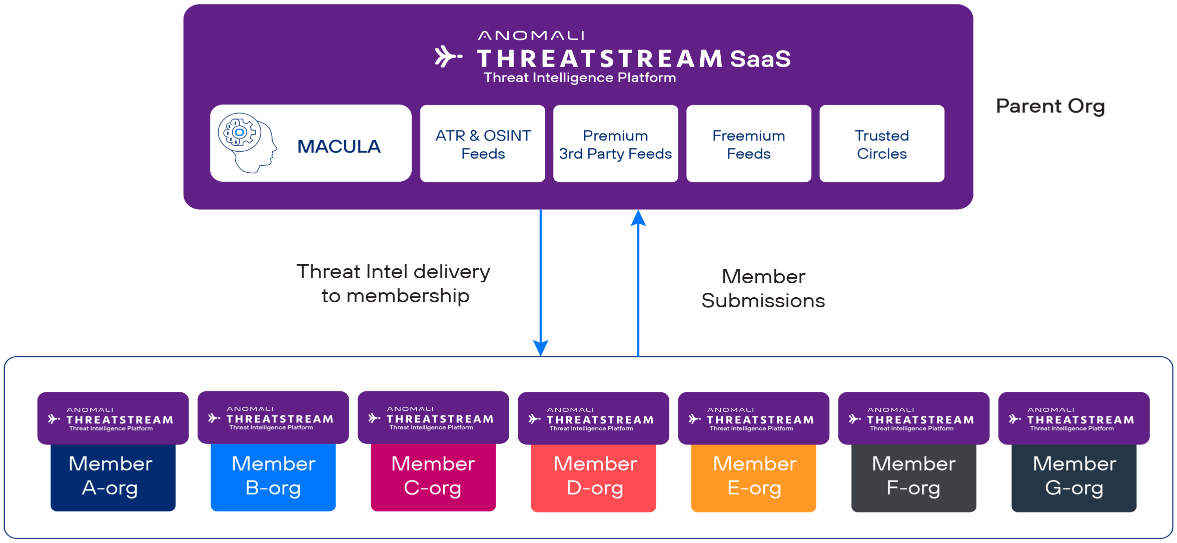


Fig 1. Community Edition Architecture

Comunity Edition Features	Community Edition (Member)	ThreatStream Enterprise (Parent)
Threat Intelligence Collection		
Multiple ISAC Sources	●	●
Simple Intel Submission Workflow	●	●
Manual Export — Observables in STIX, Threat Models in PDF	●	●
TAXII Server/Client*	●	●
Anomali Open Source Feeds		●
Anomali Premium Feeds		●
Marketplace — Anomali APP Store		●
Freemium feeds from Anomali APP Store		●
Feeds SDK		●
Enrichments SDK		●

Comunity Edition Features	Community Edition (Member)	ThreatStream Enterprise (Parent)
Threat Intel Management		
User Accounts — Unlimited	●	●
Dashboard for searching, viewing, alerting	●	●
Feeds normalization, de-deduplication, 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 Lens Freemium		●
Threat Intel Integration		
Integrations Tier0 (API)		●
Integrations Tier1 (SIEM)		●
Integrations Tier2 (EndPoint, Firewall, SOAR, etc.)		●
Integrations SDK		●
Platform and Support		
Technical Support — Standard 24x5 Support	●	●
Dedicated Customer Success Manager		●
Anomali University	●	●
Deployment Platform — Saas	●	●

Licensing details

- The primary ISAC organization purchases ThreatStream Enterprise, (including Match and Copilot) with pricing based on the size of the parent organization.
- Primary can add CE bundles in 20 member increments, plus additional member licenses as needed, sold in one increment

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 to defend against cybersecurity threats.

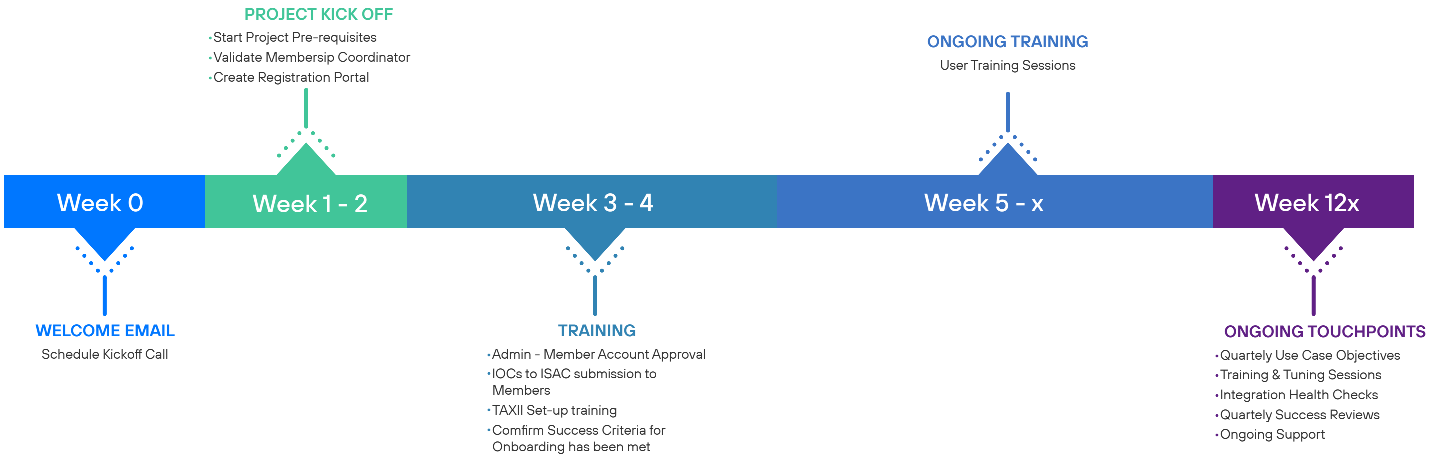
Powered by Anomali, the platform will enable users to centralize a range of data and intelligence and other relevant authorities. The intention is for ongoing cyber hazards, and risk to be tailored specifically for Local, Tribal, and Territorial governments.

The Anomali ThreatStream Community powering the State of Maryland ISAC is purpose-built to facilitate the collection and management of threat intelligence., from multiple sources and at scale, enabling these processes to be automated, thus mitigating time-intensive manual tasks.

The Anomali ThreatStream Community 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.

SAMPLE DEPLOYMENT TIMELINE



Week 0

WELCOME EMAIL

Schedule Kickoff Call

Week 1 - 2

PROJECT KICK OFF

- Start Project Pre-requisites
- Validate Membersip Coordinator
- Create Registration Portal

Week 3 - 4

TRAINING

- Admin - Member Account Approval
- IOCs to ISAC submission to Members
- TAXII Set-up training
- Comfirm Success Criteria for Onboarding has been met

Week 5 - x

ONGOING TRAINING

User Training Sessions

Week 12x

ONGOING TOUCHPOINTS

- Quartely Use Case Objectives
- Training & Tuning Sessions
- Integration Health Checks
- Quartely Success Reviews
- Ongoing Support

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 (ThreatStream). For further information, please visit www.anomali.com

Security Operations Done Differently.

Anomali is the leading AI-Powered Security Operations Platform that delivers mind-blowing speed, scale and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, XDR, SOAR, and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about AI-Powered Security Operations Platform.

ANOMALI