THREATCONNECT™

CASE STUDY

THREATCONNECT® ISAC AND ISAO EDITION

A Cyber Threat Response Organization consisting of public and private sector members chose ThreatConnect's Information Sharing and Analysis Organization (ISAO) and Information Sharing and Analysis Center (ISAC) edition to facilitate the sharing of important cyber threat information amongst its membership.

About the Organization

The Organization was designed to bring together Chief Information Officers, Chief Information Security Officers and their threat analysis teams, from public sector and small to large private sector organizations located in the same U.S. state, to effectively analyze critical, real-time intelligence and respond to emerging cyber threats. The goal was to give cross-industry group members the opportunity to better protect their assets, state critical infrastructure, and key resources from across the state.

The Problem: No Way to Safely Collect and Share Cyber Threat Information

The Cyber Threat Response Organization set out to find a solution to share important threat data with its membership. Due to the complexity and confidential nature of cyber threats, the Organization established a list of requirements that needed to be met prior to service selection.

> "We needed a solution that would allow our vetted private and public sector members to share threat information so we could strengthen our ability to respond to respond to threats together."

Community Abilities

- Private member collaboration environment
- Anonymous member information sharing
- Document and threat indicator storage
- Membership growth scalability
- Support from a leading Threat Intelligence Research Team
- User-level access control

Member Requirements

- Advanced analytics
- Community notifications
- API access to community intelligence to develop
- Automated actions
- Access to other threat intelligence communities
- On-boarding support/training

Provider Technology Requirements

- Multi-source intelligence data aggregation
- Analytic features to produce actionable intelligence
- Workflow development support
- Critical analytic task prioritization
- Secure, easy to administer, and reliable

The Threat Response Organization chose the ThreatConnect ISAO edition on account of its ability to meet or exceed their criteria. The Organization assigned a staff member to develop, maintain, and lead recruiting for the ThreatConnect ISAC/ISAO group. Due to the confidential nature of some cyber threats, members are asked to accept a code of conduct, and be members of the FBI's InfraGard Program. By carefully vetting members and asking them to agree to minimum standards to participate, the Organization ensured the membership would only consist of high-quality participants with vested interest in the state's public and private sector business community.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
P 1.800.965.2708 F +1.703.229.4489
www.ThreatConnect.com

THREATCONNECT™

CASE STUDY

How ThreatConnect® Solved the Problem

ThreatConnect's ISAO/ISAC edition allowed the Cyber Threat Response Organization to provide a single Threat Intelligence Platform (TIP) for their membership to aggregate their threat data, analyze a complex set of indicators, and take corrective action against their adversaries. Members are able to maximize the value of their existing adversary knowledge. Using the various monitoring and alerting features for domain names, and Whois Registrations, members are able to automatically track and be alerted to new adversary actions, rather than having to manually search for them. Once alerted, the member has the ability to act on the community-based intelligence into their network defense products.

Main Benefits of ThreatConnect®

ThreatConnect allows the community members to pool their threat intelligence and their resources. Community members are seeing an improvement in the protection of their assets, key resources, and state critical infrastructure. ThreatConnect provided the ability to focus on bringing in intelligence that mattered to their state from multiple sources; automated tracking of adversary infrastructure, allowed contributions from their state community peers, and research contributed by ThreatConnect. This has allowed the membership to take a proactive stance against different adversaries; now having broad detection in place before they were targeted.

ThreatConnect® Enables the ISAO Community to be Proactive in their Network Defense

ThreatConnect helped the Cyber Threat Response Organizations members to aggregate their threat data.

The membership now has one platform to aggregate all of their intelligence sources, share what they know about threats they are seeing, collaborate with others for greater situational awareness about each adversary, and make it possible to track and follow only the most relevant and actionable data.

ThreatConnect eliminated working in a vacuum.

Members' existing knowledge of threat groups was limited to information they individually collected, and limited to taking action only after targeting occurred. They are now able to share information and effectively track and proactively protect their networks together.

ThreatConnect allows the membership to enrich and deeply analyze their shared threat intelligence.

Because of their participation in the community, they are able to get specific and relevant information on a threat group targeting entities in their state, and proactively establish workflows to preempt a threat infiltrating their network.

ThreatConnect® Makes the Community Membership Work More Intelligently

Learn more about how ThreatConnect can help your organization or community aggregate threat data, analyze and track specific threat information, and take action to defend your network. Sign up for a free account to get started at **www.threatconnect.com.**

ThreatConnect® ISAC/ISAO Community

Secure Platform

- Fine grained role-based access controls
- Security labels & robust sharing controls
- Anonymity options for sharing
- Secure login; 2 factor authentication

Collaboration

- Comment feed
- Automatic notifications

Data Ingest

- Document storage & elastic search
- API Integrations
- STIX/TAXII support
- Email ingest

Analytic Platform and Workflow

- Workflow support
- Diamond Model Methodology

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com
P 1.800.965.2708 F +1.703.229.4489