ThreatConnect

CUSTOMER CASE STUDY - STATE GOV'T

State Government Intelligence Powered Operations

Background

In 2023, the State Government released a mandate to improve the threat intelligence community and collaboration statewide. The State had been leveraging an open-source threat intelligence platform (MISP) and struggled with state member adoption (cities, counties, emergency services, municipalities, public works, schools, etc.) facilitated by high volumes of uncontextualized threat data resulting in large amounts of false positives. The Cyber Threat Intelligence team in the State Cyber Command Center had expanded and needed a platform to help with automating and operationalizing their threat intelligence and related processes at scale - statewide. They needed a single place to aggregate and disseminate high-fidelity threat intelligence to their members. They also needed a tool that automates and integrates with their plethora of tools and security operations processes.

Challenges Faced

The State had been leveraging MISP and struggled with member adoption facilitated by high volumes of uncontextualized threat data resulting in large amounts of false positives. Navigating these challenges became even more complex due to the varying levels of cybersecurity maturity among the State's members. Many of them showed limited understanding of threat intelligence, and the majority lacked proficiency in effectively utilizing data within MISP. As a result, comprehending and leveraging the potential of MISP proved to be extremely difficult for its members.

The State had manual, ad-hoc, and fragmented processes for collecting, triaging, analyzing, investigating, and disseminating alerts, events, intelligence, and reports. They struggled with the time to detect and respond to the high alert, event, and incident volume. It took time to triage and investigate each alert because each one was uncontextualized. It was difficult to know which ones to prioritize because everything was labeled as critical.

Solution - ThreatConnect Intel Driven Operations Platform

Use Case 1 – Build a Unified Threat Library

The Challenge

The State received threat data in many formats and subscribed to multiple threat intelligence source feeds (CISA, CrowdStrike, MS-ISAC, and open source intelligence). They needed an environment to collect, normalize, associate, and enrich threat data to their existing collection before attempting to make sense of it. They also needed an easy way to judge the quality of the data before operationalizing it.

The Solution

The State used the ThreatConnect Platform to:

- Automatically normalize the collection of intelligence from CISA, CrowdStrike, MS-ISAC, and open source intelligence to better identify, detect, and respond to the specific types of threats that were targeting the State and its members.
- Automatically import structured and unstructured threat data from:
- Ad-hoc intelligence from different teams around the State.
- Ingestion of threat data via email and direct messaging.
- Analyze and enrich threat data to create high-fidelity and actionable threat intelligence.
- Leverage the Threat Graph in the ThreatConnect Platform to conduct investigations, searches, and visual associations between threat intelligence artifacts.
- Automatically create, export, and disseminate standalone intelligence reports to state members and leadership.
- Automatically create dashboards to visualize threat data ingested across the state, hits and incidents observed from members, and intelligence acted on and disseminated from the state.

The Outcome

What previously took the state days to do, they were able to do it in seconds using the ThreatConnect Platform.

Use Case 2 – Incident Investigation at Scale

The Challenge

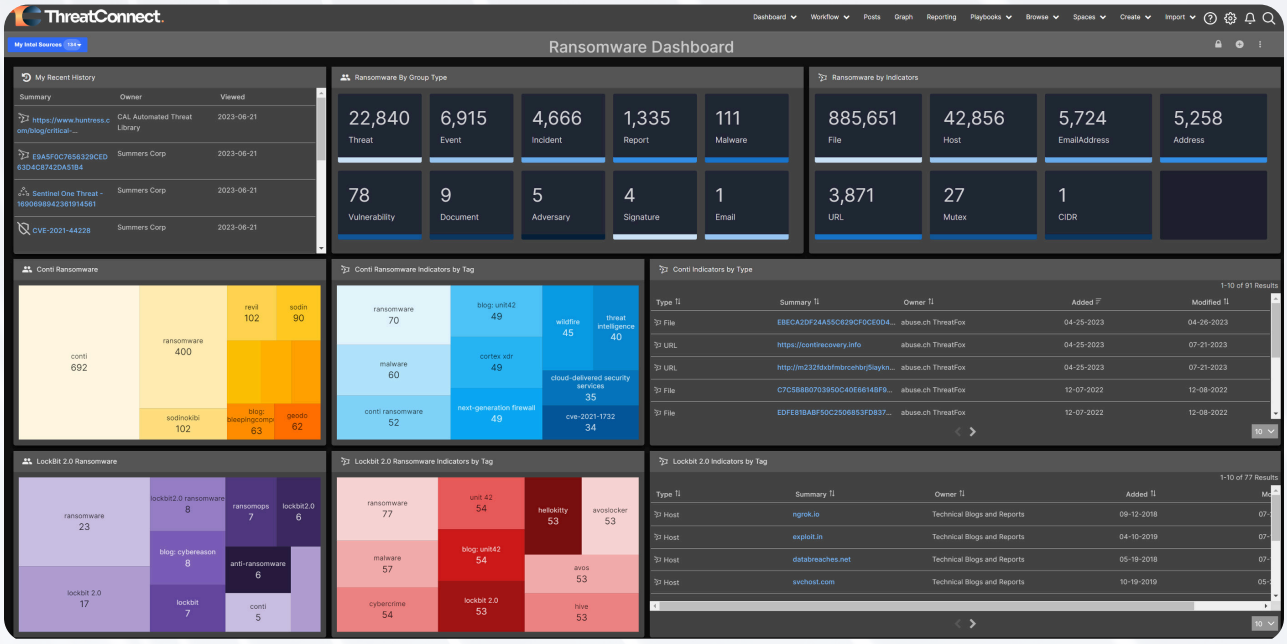
The State frequently receives incident information from its members retroactively, where they're asked to investigate, analyze, report on, and disseminate their findings quickly. This was difficult for them to do because they got little to no information or context around the requests, and they had manual and ad-hoc processes for conducting their investigations.

The Solution

The State used the ThreatConnect Platform to automatically search for threat data related to the incident and find hits and matches. The state saw context and analysis around the threat data as well as second and third-level associations to get the full picture of the incident. The state then triggered a threat hunting workflow in ThreatConnect to get additional context around the incidentand generate a report of their findings to the state members, which automatically populated a dashboard that visualized the member declaring the incident, the time it took for the state to respond, and their productions.

The Outcome

What previously took the state 15 minutes to do per threat data point, they were able to do immediately using the ThreatConnect Platform.



Use Case 3 – Automated Phishing Analysis & Response at Scale

The Challenge

The State deals with many phishing emails via a process that's manual semi-automated, where they receive, triage, investigate, and track emails reported by members via their phishing provider and direct messaging. The State needed the ability to manage large volumes of phishing emails from its members across the state and dissect them individually using automation and a standardized methodology that supported rigor and audit requirements at scale.

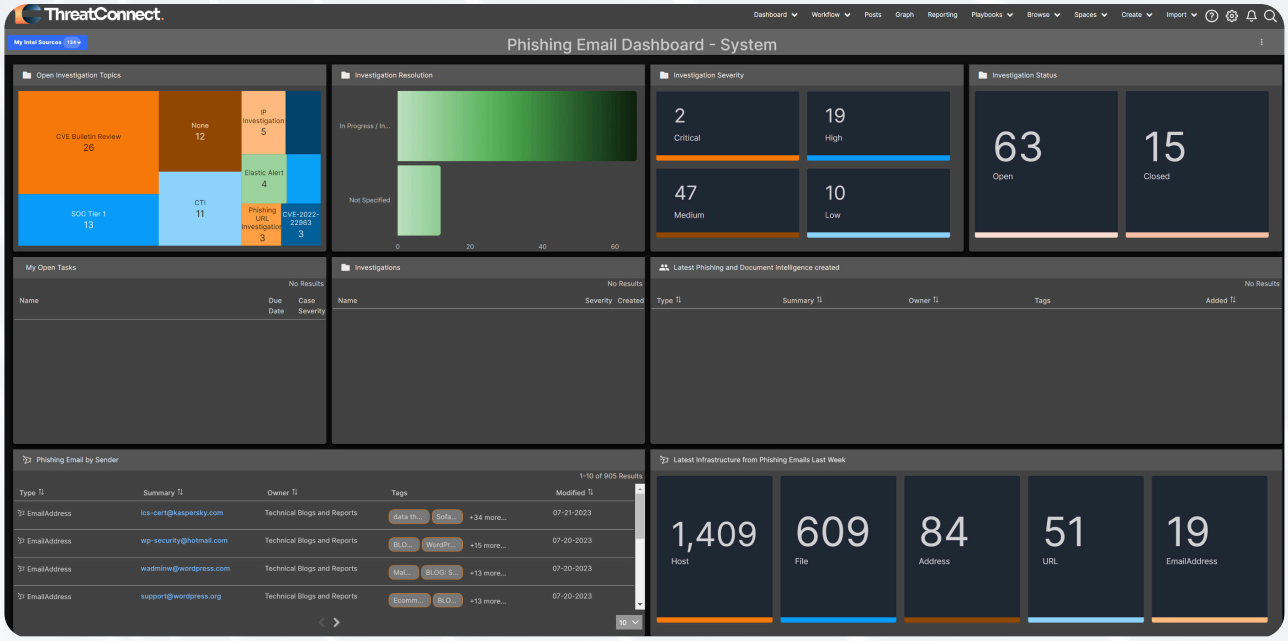
The Solution

The State used the ThreatConnect Platform to:

- Automate the ingestion and parsing of phishing emails that are submitted from state members via their phishing provider and direct messaging.
- Automatically correlate and enrich the threat intelligence artifacts within the phishing emails.
- Automatically detonate the file attachments in a sandbox environment and bring back relevant threat data and telemetry.
- Automatically send the details in a direct messaging channel to the Cyber Threat Intelligence team.
- Automatically populate, categorize, report on, and visualize the phishing volume via a Dashboard.

The Outcome

What previously took the state 15 minutes to do per threat data point, they were able to do it in minutes using the ThreatConnect Platform.



Use Case 4 – Event Prioritization & Alert Triage at Scale

The Challenge

The State is confronted with hundreds of alerts and events from their CrowdStrike endpoints statewide, where substantial amounts of time are wasted wading through false positives. When new schools are onboarded, the events balloon to tens of thousands. Without the insight of threat intelligence and orchestrated processes to help make sense of event data at scale, the State will continue to tread water while attacks linger.

The Solution

The State used the ThreatConnect Platform to:

- Automate the ingestion and parsing of alerts from CrowdStrike statewide.
- Automatically create each alert as an event, with associated context, threat data, and categorization of the event severity as either critical, high, medium, or low.
- For any critical and high events, automatically create a case with the event details and related threat intelligence artifacts.
- Automatically send highlights of the critical and high event cases to a direct messaging channel with a link back to the case.
- Automatically populate, categorize, report on, and visualize the alert, event, and case volume via CrowdStrike Alert Dashboards in ThreatConnect.

The Outcome

What previously took the state 20 minutes to do per alert (5 minutes to handle the alert and 15 minutes to investigate, enrich, and notify), they were able to do it in seconds using the ThreatConnect Platform.

Use Case 5 – Intel-Driven Vulnerability Prioritization & Response at Scale

The Challenge

The State was inundated with hefty volumes of uncontextualized critical vulnerabilities from many sources, tools, and members statewide, making it extremely difficult to know which ones to prioritize. They had difficulty correlating the vulnerabilities with threat intelligence, a hard time tracking which vulnerabilities were tied to specific state members, and a harder time reporting on it for their stakeholders.

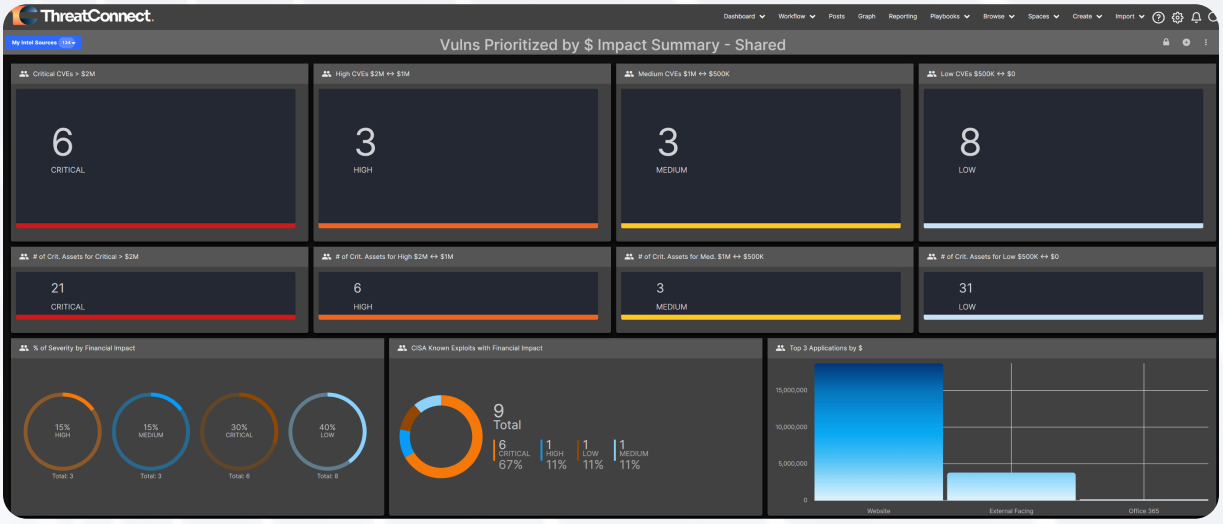
The Solution

The State used the ThreatConnect Platform to:

- Automatically ingest, parse, enrich, and contextualize vulnerabilities from the CISA Known Exploited Vulnerabilities Catalog, Google Project Zero, and National Vulnerability Database in ThreatConnect.
- Automatically ingest and correlate the contextualized vulnerabilities with vulnerabilities from their vulnerability scanner to associate state members and their related assets in ThreatConnect.
- Automatically correlate the contextualized vulnerabilities with threat intelligence.
- Automatically create a case for prioritized critical vulnerabilities to work through response and reporting via vulnerability bulletin reviews for pertinent stakeholders.
- Automatically populate, categorize, report on, and visualize the vulnerability volume across the state via a ThreatConnect Vulnerability Prioritization Dashboard.

The Outcome

- What previously took the state 15 minutes to do per critical vulnerability, they were able to do in seconds using the ThreatConnect Platform.
- It previously took the state hours to produce critical vulnerability reports and bulletins, which took them minutes to do using the ThreatConnect Platform.



Use Case 6 – RFI Handling, Investigation & Response at Scale

The Challenge

The State receives many Requests for Intelligence (RFI) from its members via email and direct messaging. The State needed to investigate and respond to each member's RFI but struggled to handle, track, measure, and report on their ability to respond at scale.

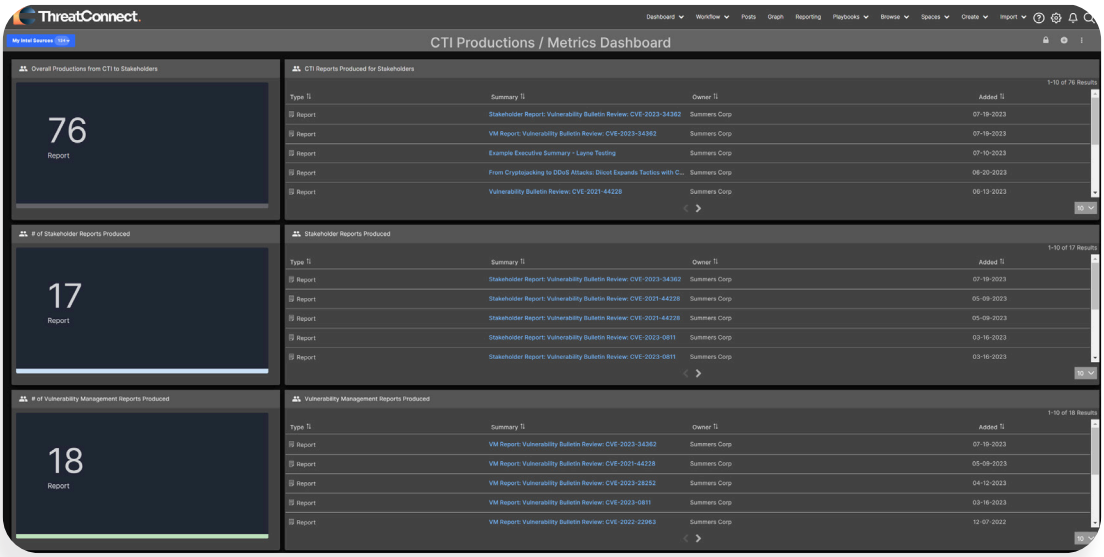
The Solution

The State used the ThreatConnect Platform to:

- Automatically ingest the RFI from direct messaging and record the submitting state member in ThreatConnect.
- Automatically correlate and enrich the RFI with related threat intelligence in ThreatConnect.
- Automatically generate a response to the direct messaging channel that the state member submitted the RFI, with the contextualized and enriched RFI with the contextualized and enriched RFI with related threat intelligence from ThreatConnect.
- Automatically populate, categorize, measure, report on, and visualize the RFIs and response time SLAs by State members via a ThreatConnect Dashboard.

The Outcome

What previously took the state 20 minutes to do per RFI (5 minutes to handle the request and 15 minutes to investigate, enrich, and respond), they were able to do in 5 minutes using the ThreatConnect Platform.



Implementation and Benefits

Listed above and broken down by use case.

Expanding Usage and Future Benefits

The State plans to widen the usage of ThreatConnect to additional members statewide and make access to and sharing of threat intelligence easier. They also plan to expand their alert response, escalation, and remediation workflows as they mature their operations. They want to integrate more downstream technology solutions to expand their data collection and enhance their enrichment and investigation processes through automation facilitated by ThreatConnect.

Advantages of (ThreatConnect Product)

Leveraging ThreatConnect, the State was able to effectuate intelligence-driven operations at speed and at scale, not only within the Command Center but statewide to critical infrastructure services. The State was able to leverage ThreatConnect as a force multiplier to not only level up the maturity of their analysts and related threat intelligence processes but provide a platform for its members to leverage structured best practices to do so as well. ThreatConnect helped accelerate state member onboarding and reduced the time and cost for the State to onboard its members. The State was also able to track, visualize, and report on the effectiveness of its operations and the incremental value it was delivering across the State to State Officials and Leadership.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708