ThreatConnect

Upgrading from an Open Source TI Database: A ThreatConnect Customer Success Story

CUSTOMER'S PROFILE:

CUSTOMER SINCE: 2018

DEPLOYMENT TYPE: On-Premises

INDUSTRY: IT/Tech

TI/SOC/IR TEAMS: 10-15 Threat Intel Analysts

Customer's Problem:

The customer needed a Threat Intelligence Platform to replace an open source database (CRITS) that had become overloaded and unusable. The replacement platform needed to make conducting analysis easy in order to identify and mitigate suspected threats in a highly-scripted and automated environment.

CUSTOMER'S THREE PRIMARY OBJECTIVES:

- Successfully transfer all existing data from the open source threat intel database to ThreatConnect.
- Maintain all original creation dates, as the customer relied upon the dates heavily for reporting, metrics, and memorialization.
- Because the customer had more than 3 million intelligence artifacts, the transition had to be fast and error free to ensure a seamless transition from a dev environment to production.

What Were They Doing Before ThreatConnect?

The customer was utilizing an open source solution to store data on indicators of compromise (IOCs) along with other data points.

Open Source Solution for Storing IOCs

Unstructured Data

Analysts struggle with adoption due to volume and aggregation

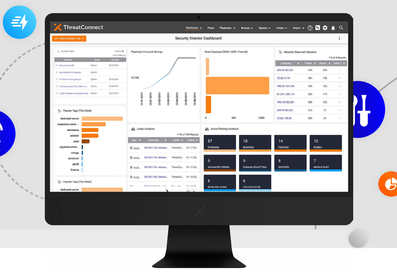
ThreatConnect's Solution

Implementing the ThreatConnect Platform was the solution. The robust and scalable API allowed the organization to find a solution that met their primary objectives:

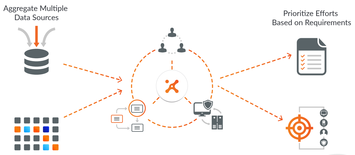
1. Utilizing ThreatConnect's API, the customer was able to script the transition process with the Python SDK. ThreatConnect's Customer Success team assisted by providing recommendations on best practices once the data resided within the ThreatConnect platform.
2. The customer leveraged ThreatConnect's robust documentation throughout the data migration process to ensure they had a thoroughly documented API and SDK, which were paramount to the success of this transition.
3. ThreatConnect's Engineering team worked with the customer to provide a tailored solution that modified ThreatConnect's system dates to match the customer's existing 'first seen' and 'modified date' fields in their current solution.
4. Custom indicators and attributes now give the customer greater flexibility in packaging their data within the Platform.

Results

In a matter of days, the customer completely transitioned from their old way of collecting and utilizing threat intelligence, and fully embraced the use of a customized and highly extensible security operations solution in order to meet their requirements. The customer is now able to provide a more efficient and robust capability to other parts of their organization that include the Incident Response team, the Security Operations Center, and the Network Operations Center.



What They Are Able To Do With ThreatConnect



BENEFITS:

- Data points (IOCs) automatically delivered to their SIEM, endpoint devices, vulnerability scanners, and other network devices through supported integrations.
- Provides context around related incidents and expedites the incident handling process by building associations with other data objects within the Platform.
- Ability to create custom dashboards and advanced queries that support daily operations, business requirements, and strategic objectives.
- Reduction in the number of resources and overhead costs required to support an open source solution in order to meet their operational requirements.

About ThreatConnect®

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit www.ThreatConnect.com.

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708

ThreatConnect.com