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

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.

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. 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.

What They Are Able To Do With ThreatConnect

What They Are Able To Do With ThreatConnect

Aggregate Multiple Data Sources
Structured Data
Integrate into Customer Processes, Teams and Tools
Prioritize Efforts Based on Requirements
SIEM Alerts
Consolidation

Benefits:

- Provides access to all data types enabling analysts and decision makers to focus on the most important data.
- Provides an in-depth understanding of an organization’s current threat landscape.
- Provides a central point for intelligence sharing.
- Provides a single interface for reporting and communicating threat intelligence.
- Provides a comprehensive view of all threat intelligence.

What They Are Able To Do With ThreatConnect

Aggregate Multiple Data Sources
Structured Data
Integrate into Customer Processes, Teams and Tools
Prioritize Efforts Based on Requirements
SIEM Alerts
Consolidation

Benefits:

- Provides access to all data types enabling analysts and decision makers to focus on the most important data.
- Provides an in-depth understanding of an organization’s current threat landscape.
- Provides a central point for intelligence sharing.
- Provides a single interface for reporting and communicating threat intelligence.
- Provides a comprehensive view of all threat intelligence.