Collaboration

A ThreatConnect Customer Success Story

Analytical Processes:

Engaging actively in the public ThreatConnect Customer Slack channel
Creating and providing Playbook apps to the Github Repo for other customers
Building custom apps for their environment in collaboration with the ThreatConnect dev team

When an incident was marked as closed and processed.
The Customer provided a start date
Differentiate between the time an incident was created and
The ability to create custom attributes that were tailored to
ThreatConnect was able to provide the customer with the
Ingest the ISAC indicators in an automated fashion into their SIEM,
The customer was able to leverage ThreatConnect's TAXII feed
Capability in order to ingest data from their specific industry

Attacks and past incidents
Correlating
Visibility in SIEM
And
Automation
Make Threat Intelligence
Make Analysis from malware
Use metrics on team efficiency
Focus on relevant intelligence

Correlating past incidents and correlate the data received with their ThreatConnect instance.
The customer needed a way for their Intelligence and Incident Response (IR) analysts to
Submit potentially malicious files to their FireEye AX appliance with the ability to store
The customer was able to leverage ThreatConnect's TAXII feed
Capability in order to ingest data from their specific industry

What They Are Able To Do With ThreatConnect

Before ThreatConnect?

Manually import relevant data

After ThreatConnect?

Ingest ISAC data and deploy it to their
SIEM and identify suspicious incidents.

Benefits

Focus on relevant intelligence
Manual import of data

Results

ThreatConnect's solution

Make analysis from malware
Use metrics on team efficiency
Focus on relevant intelligence

Copyright © 2019 ThreatConnect, Inc.