ThreatConnect.

Creating an Efficient Reporting Workflow To and From the Security Operations Center

A ThreatConnect Customer Success Story

CUSTOMER'S **PROFILE:**

CUSTOMER SINCE: **2018**

DEPLOYMENT TYPE: **Dedicated Cloud**

INDUSTRY: **Government**

TEAM: **20 Person SOC Team**

Customer's Problem:

Needed an easy and effective workflow for different parts of the organization to report incidents and events to the Security Operations Center.

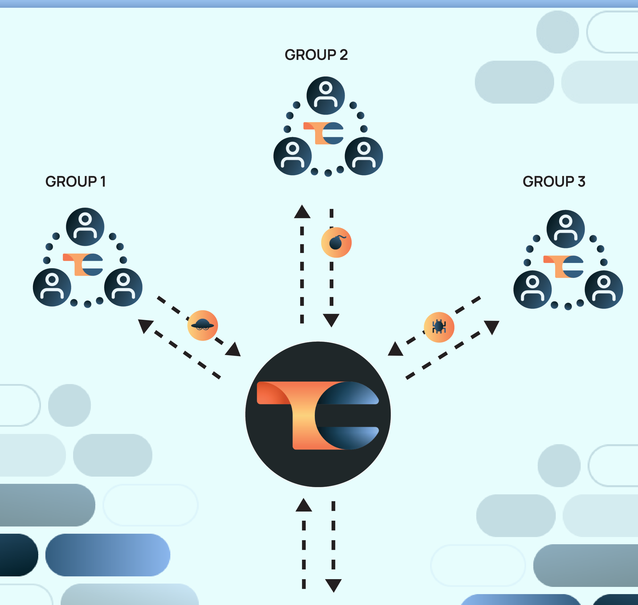
WHAT WERE THEY DOING BEFORE THREATCONNECT?

Primarily using email for all reporting and aggregation. There was no known method of housing this data for historical records so that it could be leveraged in any future analysis.

ThreatConnect's Solution and Results:

Here's what we implemented and here's what happened:

1. Provided the ability for the individuals working outside of the SOC across the organization to access their own section of ThreatConnect so they can put in intelligence and enrich data before informing the SOC
2. Set up individual Communities within ThreatConnect in which only the individual groups and the SOC have viewing rights to allow the respective group to report incidents and events to the SOC
3. Set up a ThreatConnect Community open to all respective groups using the Platform so the SOC can provide sanitized reports back to them



Security Operations Center

- Identifying information is scrubbed
- Further analysis is completed
- Sanitized report is created for distribution

Outcome: 3 months after we launched, the customer was able to establish a streamlined communication process between the SOC and individual groups throughout the organization. This led to a decrease in the time it takes to notify the SOC of a potential incident or indicator of compromise, as well as an improvement in the quality and amount of historical data being housed for future queries.

ThreatConnect.com
3865 Wilson Blvd.,
Suite 550 Arlington, VA 22203
sales@threatconnect.com
+1 (800) 965.2708