

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

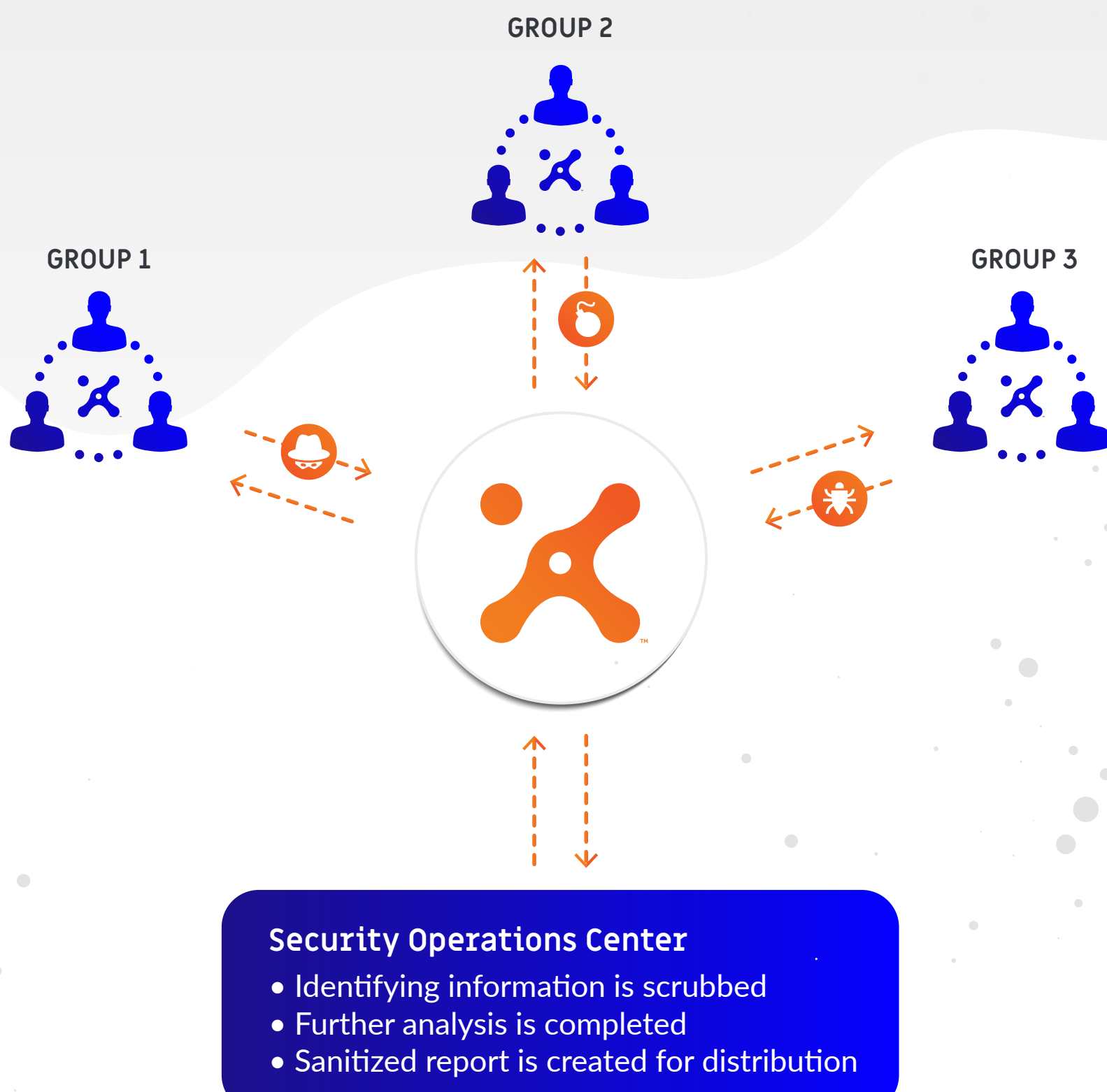
Provided the ability for the individuals working outside of the SOC across the organization to access their own section of ThreatConnect so they can put in intelligence and enrich data before informing the SOC

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



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.

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.

