

#### ThreatConnect Customer Success Story







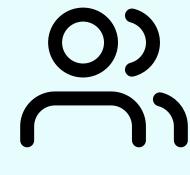
# **Creating an Efficient Reporting Workflow To and From the Security Operations Center**

A ThreatConnect Customer Success Story

**CUSTOMER'S PROFILE:** 

**CUSTOMER SINCE:** 2018

**DEPLOYMENT TYPE: Dedicated** Cloud



Government

**INDUSTRY:** 

20 Person **SOC Team** 

TEAM:

### Needed an easy and effective workflow for different parts of the

**Customer's Problem:** 

organization to report incidents and events to the Security Operations Center.

**DOING BEFORE** THREATCONNECT?

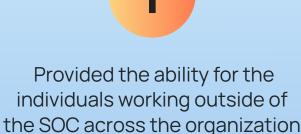
WHAT WERE THEY

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

Primarily using email for all reporting and

### Solution and Results: Here's what we implemented and here's what happened:

ThreatConnect's



to access their own section of ThreatConnect so they can put in intelligence and enrich data before informing the SOC

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

**GROUP 2** 

Set up a ThreatConnect Community open to all respective groups using the Platform so

the SOC can provide sanitized reports back to them



**GROUP 1** 



**GROUP 3** 

## Sanitized report is created for distribution

**Security Operations Center** 

Identifying information is scrubbed

Further analysis is completed

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 enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and Al-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights, and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their organizations' most critical assets. Learn more at www.threatconnect.com.

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



Thank you for downloading this ThreatConnect eBook! Carahsoft is the trusted partner for ThreatConnect Cybersecurity solutions available via GSA 2GIT, CMAS, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring ThreatConnect's solutions, please check out the following resources and information:

For additional information: carah.io/threatconnect

To purchase, check out the contract vehicles available for procurement: carah.io/threatconnect-contracts

For additional resources:
Carah.io/threatconnect-resources

To set up a meeting: threatconnect@carahsoft.com 703-230-7472

