Creating an Efficient Reporting Workflow To and From the Security Operations Center
A ThreatConnect Customer Success Story

**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.

**ThreatConnect’s Solution and Results:**
Here’s what we implemented and here’s what happened:

**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.

---

**Group 1**
- Set up Communities within ThreatConnect to 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 so the SOC can provide sanitized reports back to them.

**ThreatConnect’s Customer Success Story**

**Custom since:** 2018

**Team:** 20 Person SOC Team

**Profile:**
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.

**Configuration:**

- **Group 1:** Set up Communities within ThreatConnect to 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 so the SOC can provide sanitized reports back to them.

**Industry:** Government

---

**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.

---

**Group 1**
- Identified potential indicators
- Further analysis is completed
- Sanitized report is created for distribution

**Group 2**
- Provides the ability for the individuals working outside of the SOC to access the organization’s threat intel and help to triage events as part of a security operations center.

---

**Contact:**
3865 Wilson Blvd | Suite 550 | Arlington, VA 22203
sales@threatconnect.com | P: 1.800.965.2708

---

**Security Operations Center**

- Security Operations Center
- Identifying indicators:
- Further analysis is completed
- Sanitized report is created for distribution