Using Automation to Collaborate with Partners: A ThreatConnect Customer Success Story

**Customer’s Problem:**

The customer’s internal SOC/IR/TI teams allowed them to collaborate primarily via email, which was a very manual and delayed process. They were looking to collaborate with key partner organizations to share intelligence-driven patch management, victim information, and threat intelligence.

**Customer’s ThreatConnect® Objectives:**

1. Utilizing Playbooks, the customer identified a specific network infrastructure vendor whose products were being compromised.
2. The customers’ partner member organizations were notified by the community feature within ThreatConnect, allowing them to view other organizations’ IOCs, geolocating IP addresses, and then emailing the organization’s threat intelligence owners of IOCs.
3. These customers’ third-party databases (e.g., Shodan and Censys) were being continually updated, allowing them to identify any current and past network services.

**What Were They Doing Before ThreatConnect®?**

Collaboration was being conducted primarily via email and was a very manual and delayed process. The customer was looking to collaborate with key partner organizations to share intelligence-driven patch management, victim information, and threat intelligence.

**ThreatConnect® Solution:**

ThreatConnect’s intelligence-driven security operations platform, ThreatConnect’s intelligence-driven security operations platform.

**What They Are Able To Do With ThreatConnect®**

Using Automation:

**Results**

- **Primary Actions:**
  - Utilization of Playbooks to identify specific network infrastructure vendors whose products were being compromised.
  - Cooperating with partner member organizations to notify them of suspected threat intelligence.
  - Identification of mistakenly blacklisted IP addresses associated with nation-state cyber espionage activities.
  - Coordination of victim incident response processes.
  - Utilization of ThreatConnect community info to be shared with partners within the government.

**Team Process:**

- **Primary Actions:**
  - Utilization of Playbooks to identify specific network infrastructure vendors whose products were being compromised.
  - Cooperation with partner member organizations to notify them of suspected threat intelligence.
  - Identification of mistakenly blacklisted IP addresses associated with nation-state cyber espionage activities.
  - Coordination of victim incident response processes.
  - Utilization of ThreatConnect community info to be shared with partners within the government.

**Benefits:**

- **Primary Actions:**
  - Coordination of victim incident response processes.
  - Identification of mistakenly blacklisted IP addresses associated with nation-state cyber espionage activities.
  - Coordination of victim incident response processes.
  - Utilization of ThreatConnect community info to be shared with partners within the government.

*Copyright © 2019 ThreatConnect, Inc.*