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

Customer's Problem:

The customer, a large organization, was facing challenges in managing and responding to cyber threats. Specifically, they were looking to improve their ability to work with partners to share threat intelligence and respond to incidents in a more efficient manner.

Customer's Team:

The customer's security operations, or SOC, team consisted of around 25 people dedicated to managing and responding to cybersecurity incidents. The team faced challenges in managing the workload and coordinating with partner organizations.

What Were They Doing Before ThreatConnect?

Before using ThreatConnect, the customer was collaborating with partners primarily through email, which was a manual and delayed process. They were looking to improve their ability to share threat intelligence and respond to incidents in a more efficient manner.

ThreatConnect's Solution:

ThreatConnect's intelligence-driven security operations platform provided the customer with the tools needed to improve their incident detection and response capabilities. The platform allowed the customer to:

1. Use Playbooks to automate the initial SIEM alert triage, consolidating alert information, and identifying the victim member organization, revealing existing threat intelligence.
2. Enrich indicators and triaged SIEM alerts via third-party databases, including those from ThreatConnect's Threat Intel and Geo Location communities.
3. Coordinate with threat intelligence vendors to remove any customer-owned IP addresses from blacklists.

What Are They Able To Do With ThreatConnect:

ThreatConnect allowed the customer to:

- Coordinate with partners to share and consolidate alerts with victims, internally and externally.
- Utilize Playbooks to automate the initial SIEM alert triage, identifying a specific network infrastructure vendor and its associated back into ThreatConnect for further triage and enrichment.
- Additional IOCs could then be ingested and associated with indicators of compromise.
- Improved focus on alerts within partner organizations within the partner members whose networks were compromised.
- Adversaries were monitored by leveraging ThreatConnect's threat intelligence.
- Increased focus on alerts within partner organizations improved as a result of shared threat intelligence.
- Victim incident response processes unveiled after remediation of a compromised network.

Victims within the partner organizations were notified by the community feature within ThreatConnect which allowed them view other organization's info to be shared to partners within their networks.

Benefits:

- Automation and orchestration reduced the response efforts.
- Significant workload reduction through Playbooks automation.
- Improved focus on alerts within partner organizations.

The customer's team, consisting of around 25 people, improved as a result of their collaboration with ThreatConnect.

Results:

- Utilizing Playbooks, the customer was able to streamline indicator enrichment by leveraging ThreatConnect's Threat Intel and Geo Location communities.
- Additional IOCs were ingested and associated with indicators of compromise.
- Improved collaboration with partners through the community feature within ThreatConnect.
- Increased focus on alerts within partner organizations.
- Improved sharing of threat intelligence and incident information internally and externally.
- Efficient coordination with threat intelligence vendors to remove any customer-owned IP addresses from blacklists.
- Increased focus on alerts within partner organizations.
- Adversary capabilities were identified and mitigated by incident responders.

---

ThreatConnect® 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 efficiency. Visit www.ThreatConnect.com to learn more about ThreatConnect.