ThreatConnect

Using Automation to Collaborate with Partners:

A ThreatConnect Customer Success Story

CUSTOMER'S **PROFILE:**

CUSTOMER SINCE: **2017**

DEPLOYMENT TYPE: **Dedicated Cloud**

INDUSTRY: **Government**

TEAM: **Approx. 25 people**

Customer's Problem:

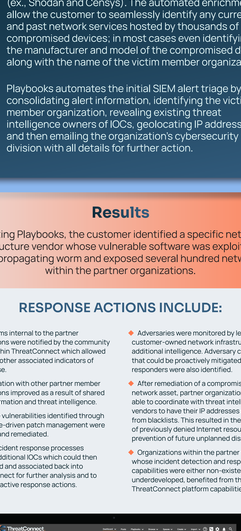
Needed a way to collaborate with partners to be able to streamline indicator enrichment and incident response to better identify and mitigate suspected threats in a timely, efficient manner.

CUSTOMER'S **THREE** PRIMARY OBJECTIVES:

- Identify mistakenly blacklisted IP addresses associated with partner organizations which disrupt legitimate, businesses-related operations.
- Automatically alert partner member organizations of suspected nation-state cyber espionage activities against them.
- Provide a list of Adversaries or "Hacktivists" with the infrastructure they are leveraging for Distributed Denial of Services (DDoS) attacks so the partner member can conduct timely investigations.

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 threat intelligence that could potentially impact or disrupt critical operations.



ThreatConnect's Solution

1. Playbooks capabilities provide customer and member organizations with enriched indicators and triaged SIEM alerts.
2. Playbooks provides the customer with automated Indicator enrichments via third-party databases (ex., Shodan and Censys). The automated enrichments allow the customer to seamlessly identify any current and past network services hosted by thousands of compromised devices; in most cases even identifying the manufacturer and model of the compromised device, along with the name of the victim member organization.
3. Playbooks automates the initial SIEM alert triage by consolidating alert information, identifying the victim member organization, revealing existing threat intelligence owners of IOCs, geolocating IP addresses, and then emailing the organization's cybersecurity division with all details for further action.

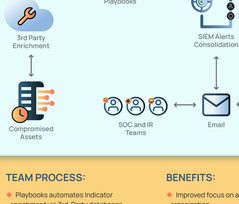
Results

Utilizing Playbooks, the customer identified a specific network infrastructure vendor whose vulnerable software was exploited by a self-propagating worm and exposed several hundred networks within the partner organizations.

RESPONSE ACTIONS INCLUDE:

- The victims internal to the partner organizations were notified by the community feature within ThreatConnect which allowed them view other associated indicators of compromise.
- Collaboration with other partner member organizations improved as a result of shared victim information and threat intelligence.
- Software vulnerabilities identified through intelligence-driven patch management were identified and remediated.
- Victim incident response processes unveiled additional IOCs which could then be ingested and associated back into ThreatConnect for further analysis and to initiate proactive response actions.
- Adversaries were monitored by leveraging customer-owned network infrastructure for additional intelligence. Adversary capabilities that could be proactively mitigated by incident responders were also identified.
- After remediation of a compromised network asset, partner organizations were able to coordinate with threat intelligence vendors to have their IP addresses removed from blacklists. This resulted in the restoration of previously denied Internet resources and prevention of future unplanned disruptions.
- Organizations within the partner members whose incident detection and response capabilities were either non-existent or underdeveloped, benefited from the ThreatConnect platform capabilities.

What They Are Able To Do With ThreatConnect



TEAM PROCESS:

- Playbooks automates Indicator enrichment via 3rd-Party databases
- Enrichments identify current and past internal/external victims
- Playbooks automates SIEM alert triaging and consolidates alerts with victims, Threat Intel, Geo Location, and then emails appropriate stakeholders
- Internal SOC/IR/TI teams allow info to be shared to partners within ThreatConnect community

BENEFITS:

- Improved focus on alerts within the organization
- Significant workload reduction through automated enrichment
- Consistent communication of threat and incident information internally and externally

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