Automating Analytical Processes:

A ThreatConnect Customer Success Story

CUSTOMER'S PROFILE:

CUSTOMER SINCE: **2016**	DEPLOYMENT TYPE: **On-Premises**
INDUSTRY: **Industrial**	TEAM: **Less than 5 TI analysts in the SOC**

Customer's Problem:

1 INGESTING ISAC DATA AND MAINTAINING VISIBILITY IN SIEM

The Customer needed an automated process to ingest indicators from ISAC communities and then to provide the data to their SIEM integration, QRadar. Automated ingestion would provide the customer's Incident Response (IR) team the ability to monitor for relevant and actionable intelligence within their network.

2 MAKE THREAT INTELLIGENCE ACTIONABLE AND TIMELY

The customer needed a tracking process for how long it was taking for intelligence to be processed once it was provided to the organization. Identifying how long the organization was susceptible to an attack based off of intelligence that they received would provide a true measure of their processes and their effectiveness.

3 AUTOMATION OF ANALYTICAL PROCESSES

The customer needed a way for their Intelligence and Incident Response (IR) analysts to submit potentially malicious files to their FireEye AX appliance with the ability to store and correlate the data received with their ThreatConnect instance.

4 CORRELATING CURRENT ATTACKS AND PAST INCIDENTS

The Customer wanted to be aware when new intelligence came into ThreatConnect that had IOC's matching prior internal incidents.

What Were They Doing Before ThreatConnect?

IOCs from AMA reports required **ad-hoc manual import** into security controls

Analysts checking TI vendor reports for relevant data **MANUALLY**

ThreatConnect's Solution

INGESTING ISAC DATA AND MAINTAINING VISIBILITY IN SIEM

The customer was able to leverage ThreatConnect's TAXII feed capability in order to ingest data from their specific industry ISAC communities into the ThreatConnect platform. Utilizing the ThreatConnect QRadar custom app, the customer was able to ingest the ISAC indicators in an automated fashion into their SIEM, and determine whether industry provided data was useful and accurate within their own organization.

Results

The Customer was able to retrieve the ISAC data and deploy it to their SIEM and identify suspicious incidents. This automated process allowed the organization's analyst to focus on incidents occurring in near real-time as opposed to spending time moving data manually from one source to another. This also provided an effective way to measure value on the data the customer was receiving from all its various sources/partners.

MAKE THREAT INTELLIGENCE ACTIONABLE AND TIMELY

ThreatConnect was able to provide the customer with the ability to create custom attributes that were tailored to differentiate between the time an incident was created and when an analyst actually reviewed the data. Utilizing the Playbooks capability, the Customer provided a start date attribute with each incident created/opened and then again when an incident was marked as closed and processed.

Results

The ability to identify how long intelligence data was known by the organization and how long it takes to deploy to appropriate applications and systems provides an organization a key performance metric on how susceptible their organization was to a given threat over a specified period of time. Minimizing an adversary's attack surface limits not only the damage they can inflict but also allows an organization to have a greater knowledge and timeline of events.

AUTOMATION OF ANALYTICAL PROCESSES

The solution was a joint effort with the Customer and ThreatConnect. Utilizing Playbooks, the customer recognized the ability of the Platform to allow them to create a custom Playbook application that provided the required automation. The customer developed a Playbook application that took submitted malware samples from the ThreatConnect malware vault and sent them to FireEye AX for processing. The Playbook application then retrieved the results and added indicators found in the FireEye AX report to ThreatConnect so further associations could be made.

Results

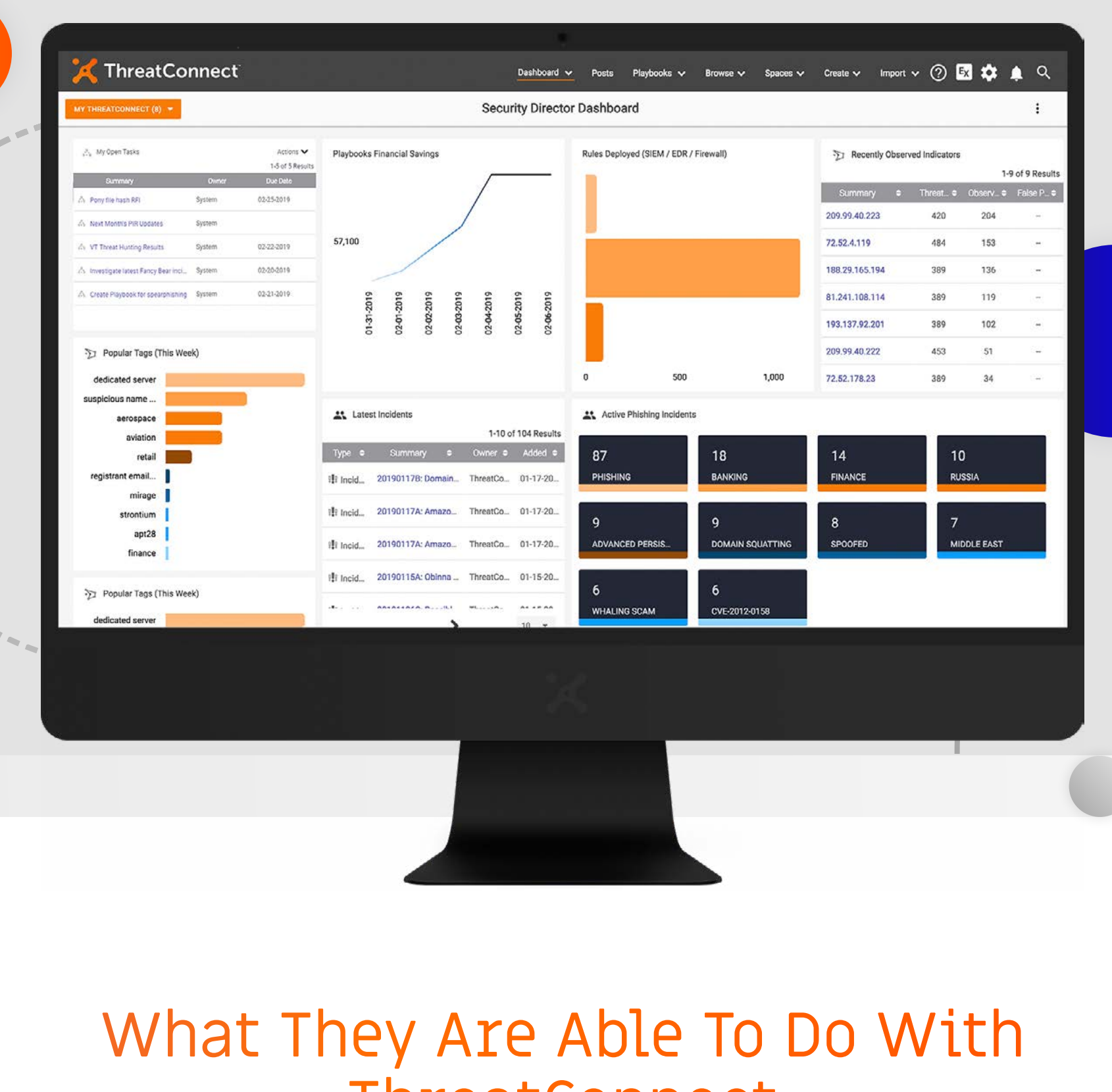
The automation of analytic processes using Playbooks provides an analyst more time to do analysis and dive further into the associations of a threat. No longer is an analyst manually having to process a malware sample and take the indicators to ThreatConnect and look for the associations.

CORRELATING CURRENT ATTACKS AND PAST INCIDENTS

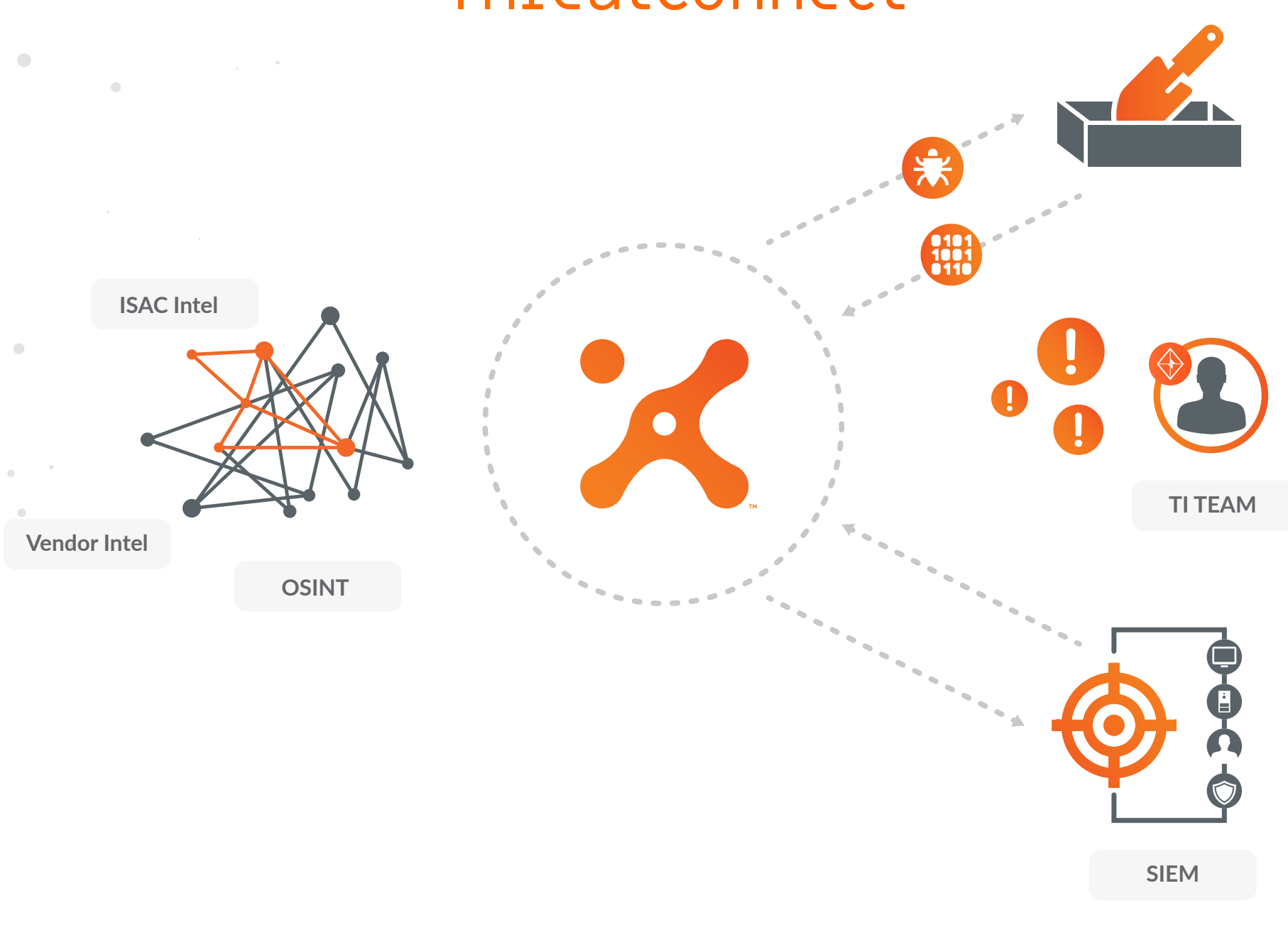
The solution consisted of building a custom Playbook app that enabled the customer to easily correlate between previous incidents and new data coming in to the ThreatConnect platform. This allowed the organization to have an indication of a previous known threat and whether that threat was active.

Results

The ability to automatically correlate IOCs to a known threat group or a previous incident provides an organization with Indications and Warning (I&W) that the adversary is active. This allows the organization to quickly attribute past attacks and add further prevention and detection capabilities relevant to the threat from the new intelligence available.



What They Are Able To Do With ThreatConnect



Benefits

- Focus on relevant intelligence instead of sifting out noise
- Use metrics on team efficiency
- Make analysis from malware samples immediately actionable

Collaboration

Thanks to ThreatConnect's proactive customer support and active user community, the customer is getting even better continued results through the following:

- Building custom apps for their environment in collaboration with the ThreatConnect dev team
- Creating and providing Playbook apps to the Github Repo for other customers
- Engaging actively in the public ThreatConnect Customer Slack channel

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 ThreatConnect.com**.

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

ThreatConnect.com