ThreatConnect

Identifying Additional Insights on Cyber Adversaries:

A ThreatConnect Customer Success Story

CUSTOMER'S PROFILE:

CUSTOMER SINCE: **2016**	DEPLOYMENT TYPE: **Cloud**
INDUSTRY: **MANUFACTURING**	TI/SOC/IR TEAMS: **Less than 25 people**

Customer's Problem:

A small threat intelligence team needed additional insights on several cyber adversaries that posed a risk to their organization. The customer reached out to the ThreatConnect's Customer Success and Research teams seeking additional information.

CUSTOMER'S TWO PRIMARY OBJECTIVES:

- Validate their own findings regarding the adversaries they were tracking.
- Identify any known intelligence and operations gaps in analysis that pose a risk to themselves and their environment.

ThreatConnect's Solution

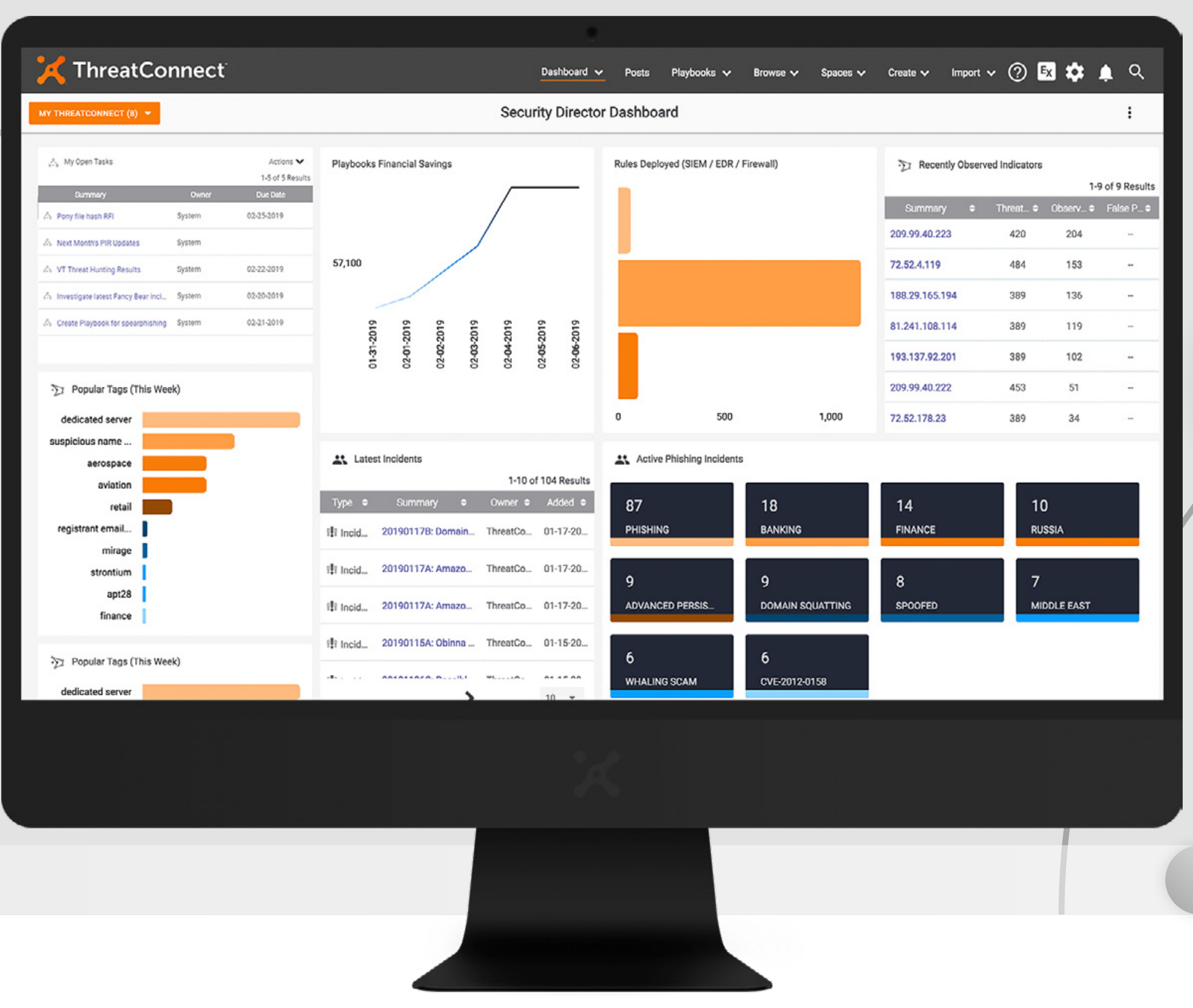
The ThreatConnect Research Team created a private community for the customer to enhance collaboration regarding their adversaries. The customer shared the information about the adversary that they were tracking with the Research team to do their own validation.

Creating a private community allowed the customer to interact with the ThreatConnect Research team and provide comments and analytical notes on the threats, adversaries, and infrastructure involved - all while working within the ThreatConnect Platform. Working within the private community allows only invited users to participate in the effort.

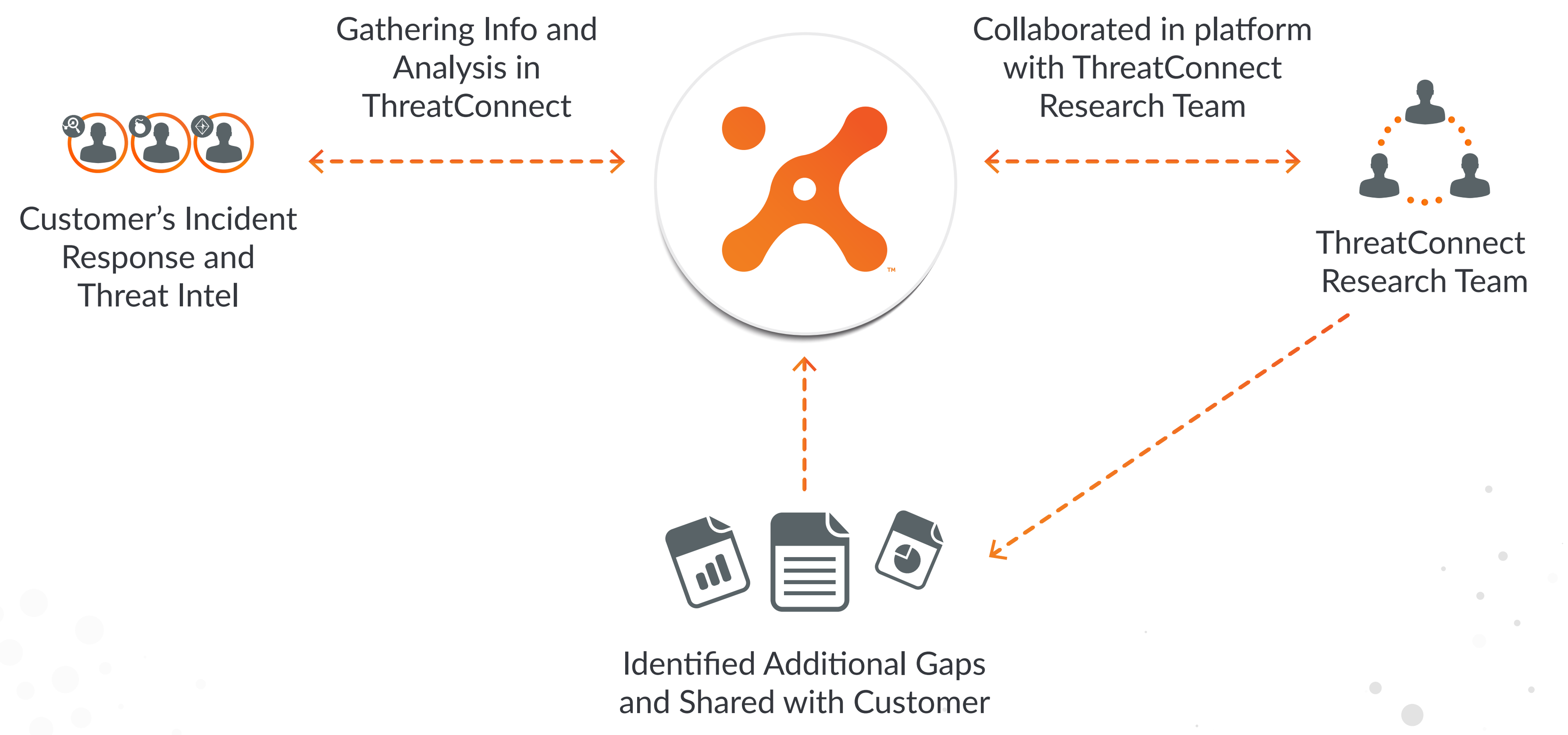
Results

The ThreatConnect Research Team was able to identify additional adversarial assets including social media accounts and forum handles that were previously unknown to the customer's team.

- After a thorough analytical review of the customer's indicators, the ThreatConnect Research team identified a subset of threat activity previously identified within six ThreatConnect Communities and eight ThreatConnect Sources, including the ThreatConnect Intelligence feed and Technical Blogs and Reports source.
- The ThreatConnect Research team provided their finished analysis to the customer and provided best analytical practices on how to correlate and pivot for specific threats across the different sources within ThreatConnect.
- The additional findings from the Research team provided the customer with additional rules and signatures for network detection while simultaneously enhancing their knowledge of specific threats and adversaries.



What They Are Able To Do With ThreatConnect



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.

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

ThreatConnect.com