Identifying Additional Insights on Cyber Adversaries: A ThreatConnect Customer Success Story

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.

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

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.

Customer's Two Primary Objectives:
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.

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.

What They Are Able To Do With ThreatConnect
- Gathered info and analysis in ThreatConnect
- Collaborated in platform with ThreatConnect Research Team
- Shared with Customer
- Created a private community for enhanced collaboration regarding their adversaries.