ThreatConnect

# Focusing on Relevant Intelligence
## A ThreatConnect Customer Success Story

CUSTOMER'S **PROFILE**:

CUSTOMER SINCE: **Dec. 2016**

DEPLOYMENT TYPE: **Cloud**

INDUSTRY: **Technology**

TEAM: **3-5 People**

## Customer's Problem:

**1** **FINDING** AND **USING** RELEVANT INTELLIGENCE.

The customer was struggling to create value out of their threat intelligence program. Their team needed a way to know what new threat activity may be relevant to their team and overall security posture.

**2** **RISK AWARENESS**

Another critical need for the customer was measuring risk based on current known vulnerabilities in their environment. They needed to match intelligence on exploits tied to malware with vulnerabilities found using their vulnerability management product (Qualys) to keep aware of what active threat groups or campaigns pose a risk to vulnerable assets in their environment.

**3** USING THREAT INTELLIGENCE FOR **DETECTION.**

The customer didn't just need to be aware of potential threats to their environment, they needed to detect any potential incidents or attempted breaches. They needed a capability that would match known indicators of compromise to network traffic in their environment in real-time.

## What Were They Doing Before ThreatConnect?

Manual entry of **IOCs of interest** into SIEM for detection


## ThreatConnect's **Solution**

**FINDING** AND **USING** RELEVANT INTELLIGENCE.

The customer is able to leverage ThreatConnect's robust tags along with its "Follow" feature to create notifications on threat intelligence of interest for their analysts to review and monitor. The Customer Success and Research teams assists the customer's team in identifying relevant "Follows" for notifications to their team.

**Results**

The customer is able to quickly identify and leverage IOCs associated with cyber actors targeting their industry, drastically reducing the time to detect malicious threat activity. They are able to save countless hours reading through weekly blogs to extract those IOCs and use for detection. The capability also increases the situational awareness of their analysts by bubbling up the most important and relevant content to the top of their reading list for the day.

**RISK AWARENESS.**

The customer uses ThreatConnect's integration with their vulnerability management solution, Qualys, to monitor currently unpatched vulnerabilities that known threats within ThreatConnect had exploited. This gives the customer's team the knowledge it needs to prioritize patching efforts within the environment.

**Results**

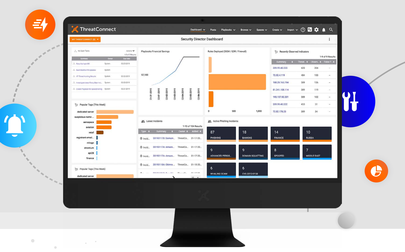
The customer is able to prioritize on the handful of threats being exploited by known threats from the hundreds on the usual patch list across the enterprise.

**USING THREAT INTELLIGENCE FOR DETECTION.**

The customer uses ThreatConnect's integration with Fidelis to enhance their detection of malicious traffic in their environment. ThreatConnect automatically vets and filters millions of IOCs for detection in Fidelis.

**Results**

Now focusing on already vetted IOCs, the customer has significantly reduced their mean time to detection (MTTD) as well as freeing their time to create their own intelligence for strategic reporting.



## What They Are Able To Do With ThreatConnect


### TEAM PROCESS:

- TI alerts regularly checked in SIEM
- TI team uses custom dashboards to view:
  - Latest intel from key sources
  - ROI from all sources

### BENEFITS:

- TI team no longer plugging in IOCs from reports – time saved
- Ability to brief the value of sources to leadership
- Spending more time creating their own Intelligence

### Collaboration

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

- Providing feedback to Customer Success team on objectives and success criteria
- Collaborating with ThreatConnect Research team on published threats
- 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