THREATCONNECT™

CASE STUDY

COMMUNITY COLLABORATION ENABLES THREAT DETECTION

SUMMARY:

This case study illustrates how industry partners benefited using a ThreatConnect® private community to collaborate on intelligence, quickly leading to the detection of a specific threat.

BACKGROUND:

The private community in this Case Study was created by an organization (Organization #1) with a threat intelligence analysis team acting as the chief moderator. The moderator invited five participating organizations within its industry to join after careful vetting. The participating organizations' threat intelligence programs and staff have varying levels of maturity; some do not have a security staff member dedicated to threat intelligence analysis.

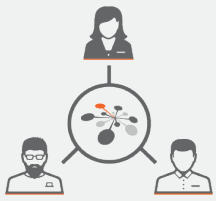
Several of the partner organizations had not worked together before the establishment of the ThreatConnect Community. The moderator does not allow for anonymous profiles in the community, which increased trust and transparency amongst the participating members. Organization #1 chose to moderate the community themselves rather than engage with the ThreatConnect Intelligence Research Team (TCIRT). All sharing and collaboration happened within the ThreatConnect Private Cloud platform.

The moderator established rules and guidelines for participation, including but not limited to:

- Intended goals of the community
- Acceptable use of community data for defensive actions,
- Restrictions on use of community data related to internal reporting, public exposure, and malicious intent, timeliness and sanitization of contributed intelligence, and
- Social spirit (citizenship) of community members related to collaborative working, growth and trust.

Initially, due to its mature threat intelligence program, the moderator initialized most of the threat intelligence sharing within the community. However, soon after the sharing of relevant intelligence on a threat that had targeted several of the group members, the community came together with several members providing unique insight into the threat. The sharing proved valuable not only in directly increasing defenses across the community through the shared data, but also through the collaboration that occurred during the process of sharing. Many of the less mature participants were able to gain insights on analytic tradecraft and make better connections to recognize various incidents as originating from a single threat group.

Before community collaboration began within ThreatConnect, the partner organizations did not know that they shared this common threat.



Sharing communities exist today, but are largely maintained through email and word of mouth. The ThreatConnect platform was designed to enable community collaboration with structured data in a controlled manner. Today's ThreatConnect communities support industry, geographic, and threat-themed sharing partners.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com
P 1.800.965.2708 F +1.703.229.4489

COMMUNITY COLLABORATION ENABLES THREAT DETECTION

DETAILS:

The following steps provide a high level overview of how the community's five participating organizations worked together to uncover additional details about a specific threat:

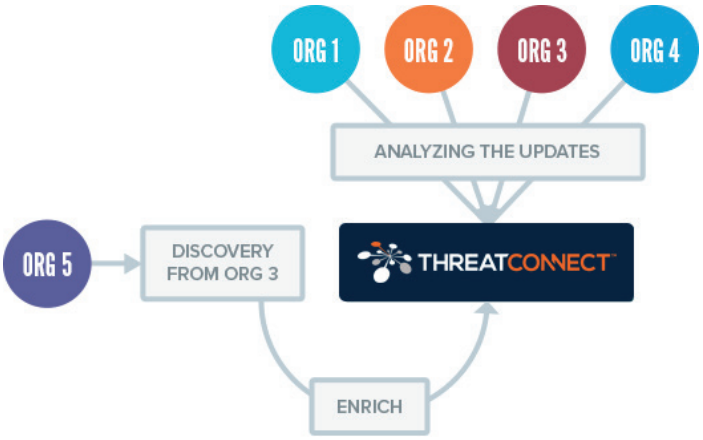
Time = 0:

The community moderator (Organization #1) imports a mature threat (50+ indicators) into ThreatConnect, and contributes it to the community. Using ThreatConnect's community comment feed, the community moderator notifies the community partners (five organization members) of the threat and requests feedback.

Time = 1:

Organizations #2, 4, and 5 provide feedback (via the ThreatConnect community comment feed) that they had not seen this threat on their network. Since it is new to them, Organization #2 creates network signatures for detection. Organization #3 provides an additional spear-phish email from a sender not seen before, but using the same command and control (C2 node). The threat is enriched within ThreatConnect.

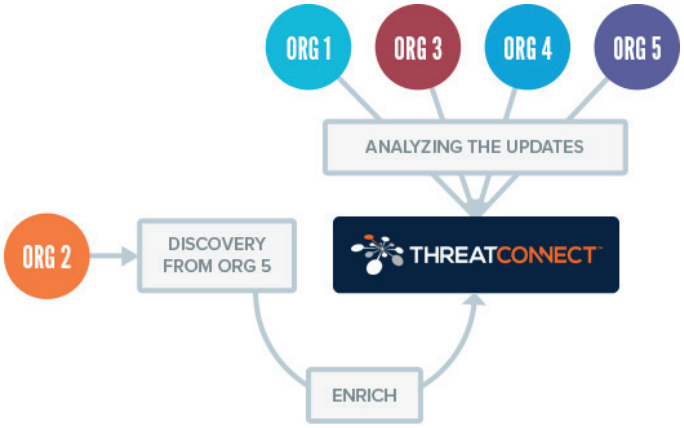
COMMUNITY COLLABORATION ENABLES THREAT DETECTION



Time = 2:

Organization #5 takes the information provided from Organization #3, finds the same spear-phish email and detects an infection not seen before.

Organization #5 shares incident details (omitting the sensitive details of the infected host, but providing all relevant threat indicators including MD5 hash values of the malware).



Time = 3:

Organization #2, who did not see the threat on their network in Time = 1, finds the malware from Organization #5 (Time = 2) in their malware repository from previous incidents. Organization #2 contributes incident details from their original case which includes callback domain names. They realize their previous incident is related to the more current threat information being shared and since they were previously targeted by this threat, they could be targeted again.

COMMUNITY COLLABORATION ENABLES THREAT DETECTION

KEY TAKEAWAYS:

Community enrichment:

- Enrichment from one member leads to further enrichment from the other participants and the entire private community benefits from greater threat awareness. As each organization contributes what they know, the knowledge of the threat's capabilities and infrastructure are more complete to all of the community participants. By sharing data with the community, the moderator has effectively increased the number of analysts looking at this threat.

Analyst learning:

- Analysts communicated across ThreatConnect's community comment feed, and shared techniques on how to conduct analysis and find this adversary operating on their respective networks. Analysts grew their skills through community participation and secure collaboration for, all to see, with structured data that was both searchable and pivotable via an email.

Faster threat awareness:

- A more comprehensive picture of an evolving threat by community members led to data being shared faster and more often.

Predictive defense:

- The threat continues to change and morph. By having analysts from multiple organizations using and sharing data on ThreatConnect, the ability to track infrastructure movements and share what they know creates defensive actions that are dynamic, and in some cases, predictive.

Secure sharing and notification:

- ThreatConnect enabled five organizations to have a common picture of the threat intelligence in a secure manner through a private community group. When something new was added, organizations "following" the threat received a notification via email, and were able to react and update accordingly.

CONCLUSION:

This private community was able to pro-actively share information within a trusted and secure environment in ThreatConnect that led to in-depth analysis and the ability to add a predictive defense across multiple organizations. New threat activity was shared and risk mitigated by sharing relevant threats and information passed through different organizations' environments. Simply by sharing structured data within a private community, these five organizations were able to raise awareness of threats and proactively stop them.

CONNECT WITH US

Interested in learning more about how ThreatConnect can help unite your security team and protect your enterprise?

www.ThreatConnect.com

TOLL FREE: 1.800.965.2708
LOCAL: +1.703.229.4240
FAX: +1.703.229.4489