CUSTOMER SINCE: 2016
DEPLOYMENT TYPE: Dedicated Cloud
INDUSTRY: Professional Services
TEAM: Network Engineers & TI Analysts

CUSTOMER’S PROFILE:

Customer’s Problem:
Needed to decrease the time between the Threat Intel team identifying indicators affecting their industry, and the Networking team implementing the appropriate block controls. Additionally, they wanted to make the process of requesting the block easier on the Threat Intel team.

What Were They Doing Before ThreatConnect?

Threat Intel analysts were identifying indicators in ThreatConnect and submitting tickets or sending emails to the Networking team for them to manually put the blocks in place.

The Threat Intel team didn’t know if the indicator was getting blocked when they put in the tickets due to a lack of any sort of feedback loop between them and the Networking 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.

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

What They Are Able To Do With ThreatConnect

Customer’s Threat Intelligence Team
ThreatConnect Playbooks push IOCs to Check Point Firewall

Malicious indicators are added to Check Point Block Lists

OUTCOME

The analysts were able to speed up the process from identifying malicious indicators and getting block controls put in place to only a few hours. This has drastically reduced the workload of the Threat Intel team since they don’t have to constantly check the ThreatConnect Playbooks to submit tickets or send emails.

The Playbooks allow the Threat Intel team to directly push IOCs into their Check Point Firewall.

When the Playbook gets triggered, the indicator gets pushed to the Check Point block list. Now, when malicious indicators are identified, the block is happening instantaneously.

They now have a Dashboard within ThreatConnect that shows the amount of malicious indicators that have been blocked which can be used for tracking and reporting metrics.

In conjunction with ThreatConnect’s Customer Success team, the customer was able to quickly learn how to build Playbooks and create the proper workflow.

A Playbook was written to give the Threat Intel team the ability to identify and block malicious indicators in real time.

What We Implemented:

- Automation of the process of blocking malicious indicators
- ThreatConnect Playbooks
- Integration with Check Point

What Happened:

- Increased efficiency in the process of blocking malicious indicators
- Reduced workload for the Threat Intel and Networking teams
- Enhanced visibility through Dashboard reporting

This has made the customer more secure due to a much more efficient malicious indicator blocking process.

Copyright © 2019 ThreatConnect, Inc.