ThreatConnect

Automating the Process of Blocking Malicious Indicators with Playbooks: A ThreatConnect Customer Success Story

CUSTOMER'S PROFILE:

CUSTOMER SINCE: **2016**

DEPLOYMENT TYPE: **Dedicated Cloud**

INDUSTRY: **Professional Services**

TEAM: **Network Engineers & TI Analysts**

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 analysts.

What Were They Doing Before ThreatConnect?

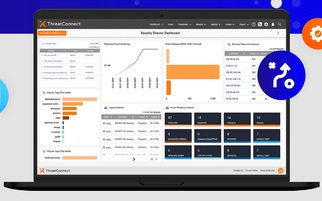
Threat Intel analysts were identifying indicators in ThreatConnect and submitting tickets or sending emails to the Networking team for them to manually put the blocks in place.

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.

ThreatConnect's Solution and Results:

Here's what we implemented and here's what happened

- 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 Analysts the ability to directly push IOC's 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 total amount of malicious indicators that have been blocked which can be used for tracking and reporting metrics.



What They Are Able To Do With ThreatConnect

OUTCOME

The analysts were able to speed up the process from identifying malicious indicators and getting block controls put in place for them. This has drastically reduced the workload of the Threat Intel team since they don't have to leave the ThreatConnect Platform to submit tickets or send emails. This has also reduced the workload for the Network Engineers since they don't have to field requests from the Threat Intel team anymore. All in all, the customer is now more secure due to a much more efficient malicious indicator blocking process.

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