

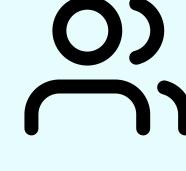
Automating the Process of Blocking Malicious Indicators with Playbooks:

A ThreatConnect Customer Success Story

CUSTOMER'S PROFILE:

CUSTOMER SINCE: 2016

DEPLOYMENT TYPE: Dedicated Cloud



Professional Services

INDUSTRY:

TEAM: Network **Engineers &** TI Analysts

Needed to decrease the time between the Threat Intel

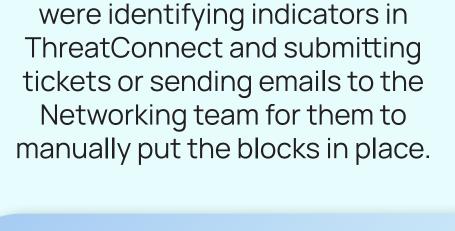
Customer's Problem:

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.

THREATCONNECT?

WHAT WERE THEY DOING BEFORE





ThreatConnect



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.

Solution and Results: Here's what we implemented and here's what happened

ThreatConnect's

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.

Security Director Dashboard

Rules Deployed (SIEM / EDR / Firewall)



ThreatConnect ThreatConnect Playbooks Customer's Threat Intel pushes IOCs to team identifies IOCs



SOFTWARE TECHNOLOGIES LTD.

Check Point Firewall

OUTCOME

in ThreatConnect

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.

The analysts were able to speed up the process from identifying malicious



Learn more at www.threatconnect.com.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and Al-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights, and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

ThreatConnect.com 3865 Wilson Blvd., Suite 550 Arlington, VA 22203 sales@threatconnect.com +1 (800) 965.2708