THREATCONNECT®

CASE STUDY

Fortune 500 Organization Automated Data Aggregation, Threat Prioritization, and Community Collaboration and Turned One Threat Analyst into the Equivalent of Three.

SUMMARY:

One of the top three worldwide providers of equipment to the Oil & Gas industry deployed ThreatConnect® and was able to greatly improve their threat intelligence program. This was achieved through enhanced workflow capabilities including threat data aggregation, threat prioritization, and community collaboration. This case study showcases how the ThreatConnect platform:

- Allows threat intelligence teams to take advantage of scaled and repeated processes across any number of industries facing persistent cyber threats
- Eliminates the need for manual processes
- Automates aggregation of threat data across multiple sources, allowing the organization's employees to focus on the threats with the most potential to do damage
- Helps protect its internal IT network and system, and also contributes to the combat of cyber threats throughout their entire community

CHALLENGE

The organization's cyber threat intelligence team previously consisted of one employee with an enormous workload. Each day, he had to manually review over 100 phishing emails and one terabyte of security-related data (the informational equivalent of 2,000 hours of music CDs). Then, this staffer needed to manually send queries about potentially troublesome incidents to the incident response team, which covered more than 1,200 locations on six continents. He was tracking his adversaries in spreadsheets, which made the information hard to find and to track. The employee was also acting alone, as he had no way of communicating with peers in the industry about potential threats or solution development.

BACKGROUND

The organization's leadership realized that their proprietary information and sensitive data would be an appealing target to threat actors. Protecting the organization's IT network and systems was not only critical for internal operations and business strategies, but also critical for the security of the entire Oil & Gas industry. However, when the organization reached out to vendors for a new system, they found that plenty of companies claimed to offer "threat intelligence platforms" when they really didn't. Leadership was not simply looking for a threat feed or a feed aggregator, but a true TIP with analysis and workflow capabilities. The organization implemented ThreatConnect, which allowed the cyber threat intelligence team to be more efficient in their daily duties while protecting their internal IT network and systems.

ORGANIZATION

Confidential

INDUSTRY

Oil & Gas

CHALLENGE

The threat intelligence team could not sustain the enormous workload and manual workflow. They had no way of collaborating with industry peers on threats or solution development.

SOLUTION

ThreatConnect provided a Threat Intelligence Platform (TIP) that eliminated manual processes and allowed collaboration with industry peers by providing access to industry and technology communities.

RESULTS

- Eliminated manual analysis of 1 terabyte of data per day
- Automatic analysis of over 100 phishing emails per day
- Connected organization to peers in 70 countries

CASE STUDY

Fortune 500 Organization Automated Data Aggregation, Threat Prioritization, and Community Collaboration and Turned One Threat Analyst into the Equivalent of Three.

SOLUTION

By implementing the ThreatConnect platform, the organization eliminated their manual processes by automating aggregation of threat data from multiple sources. Threats are now prioritized in terms of their damage potential. This way, the organization's cyber threat team can easily assess whether the situation presents a risk to one of their lines of business and launch remediation efforts if needed. Utilizing the ThreatConnect TIP, the organization is able to automatically connect to peers in 70 countries.

The organization also had some specific needs that had to be addressed. ThreatConnect's powerful API allowed them to build out and implement the platform so that it exactly matches an organization's requirements. The company also had a lot of help from ThreatConnect's customer success team. For example, ThreatConnect's engineers wrote an organization-specific script that automatically scraped emails for indicators and victims once per day. The script extends to the organization's active directory, which allows the analyst to see the data's context and trends.

ThreatConnect also gave the organization access to the ThreatConnect TC Exchange. Industry and technology communities freely share threat trends and responses, while collaborating upon code, application modifications, and solution development. One of the organization's users stated, "*I can reach out to literally hundreds of informed people now. Before ThreatConnect, I could get together with maybe one or two [peers within the industry].*"

WHAT IS THREATCONNECT?

ThreatConnect is the first and only Threat Intelligence Platform built to bridge incident response, defense, and threat analysis. Government agencies and Fortune 500 organizations worldwide leverage the power of ThreatConnect every day to aggregate, analyze, and act on their threat intelligence data. Available as both on-premises and in the cloud, ThreatConnect increases productivity and delivers dynamic knowledge management, high context indicators, and automated responses to counter sophisticated cyber attacks.

3865 WILSON BLVD., SUITE 550, ARLINGTON, VA 22203
P 1.800.965.2708 F +1.703.229.4489

RESULTS

Preventative Defense

The organization's cyber threat intelligence program is also augmenting the security of its internal network and the vast numbers of analysts collaborating within ThreatConnect. They created an extensive adversary "rating" report, in which suspected attackers are ranked according to their potential impact, the sophistication of their tools, and other criteria.

Internal Collaboration

The organization has introduced new industrial control systems security measures based upon intelligence aggregated and analyzed within ThreatConnect. For the first time, the company is able to hold regular meetings with engineers, developers, and sales staff worldwide to raise their awareness of cyber threats and then develop an action plan. The organization has seen such success with ThreatConnect that they have recommended the platform to their peers, increasing industry collaboration.

Increased Efficiency

By automating the analysis of security data, ThreatConnect saved the organization a large amount of time and streamlined their workflow. Analysts no longer need to manually look through enormous amounts of security data or phishing emails, which frees them up to analyze threats.

www.ThreatConnect.com