THREATCONNECT™

CASE STUDY

THIS IS HOW WE DO IT:

A FINANCIAL GIANT'S THREAT INTEL SUCCESS STORY

See how a Fortune 100 financal services organization integrated security infrastructure, increased efficiency, and identified attacks before they occurred.

SUMMARY:

This is the story of how a Fortune 100 financial services organization integrated its security infrastructure, increased the efficiency of its cybersecurity team, and thereby identified attacks before they occurred. For obvious reasons, we can't disclose their name, so for the sake of readability and anonymity, we will identify them in this story as FSV1.

By deploying ThreatConnect, FSV1 restructured, streamlined, and improved their threat intelligence program. ThreatConnect provided increased efficiency, integration with the organization's existing tools and systems, and automated data aggregation. This case study showcases how FSV1 used ThreatConnect to:

- Centralize data from disparate sources to more quickly identify and mitigate threats
- Save the organization an enormous amount of time by streamlining their workflow
- Enable the organization to find threats before they do any damage

Challenge

FSV1 had a threat response team with many security tools and applications in place. The tools were not integrated and their process was not scalable. The bottom line is that FSV1's team did not have a central place to keep track of their tasks and data. As a result, each team member had multiple windows open and multiple places that he or she stored their data. At best, the team had a master spreadsheet that served as a list of all of the threats they had observed. But, FSV1 received up to 250,000 potential threats every day. Thus, the spreadsheet became enormous and disorganized. When a team member wanted information on a past threat, they had to send a query into the master spreadsheet, and the results could take hours due to the massive volumes of data.

In addition, FSV1 couldn't properly analyze malware that was attempting to attack their network. Their filters and firewalls were so stringent, everything was being blocked. As a result, the organization's threat response team was not able to capture or analyze the malware. Also, FSV1 wasn't able to to study potential attacks on their network, learn from them for future reference, and build a knowledge base. This prevented the company from building out a proper defense strategy.

Organization

Confidential

Industry

Financial Services

Challenge

FSV1's threat intelligence program had neither a central place for their data, nor a central tool to manage their entire security infrastructure. There was no way for FSV1 to enable cross-team workflows and tasks, nor have the procedures in place to ensure efficiency.

Solution

ThreatConnect provided a Threat Intelligence Platform (TIP) to serve as the center of FSV1's threat intelligence program. By using a TIP, all of the company's tools and systems, data, and tasks are now hosted in one central place.

Results

- Eliminated the slow process of manually querying 250,000 potential incidents per day
- Automated reporting of data that previously took hours to compile
- Identified potential phishing attacks within a few hours of their inception

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203

P 1.800.965.2708 F 1.703.229.4489

www.ThreatConnect.com

THREATCONNECT™

CASE STUDY

Background

At the end of 2014, FSV1 was attacked by a foreign advanced persistent threat (APT) group in the midst of other high-profile and highly publicized briefs. At the time, FSV1 didn't have a threat intelligence team in place and couldn't properly address threats. They did have a small threat response team, but the employees were improperly trained on the tools and procedures. A targeted spear-phishing campaign fell through the cracks. Fortunately, the phishing campaign didn't affect FSV1's network, but it was the impetus for them to start building out a threat intelligence program. Leadership started to shape the program with various threat intelligence tools, and the company as a whole began implementing the various systems and tools as well. But, FSV1 still didn't have a process in place on how to use the tools, resulting in many of the tools going unused.

Solution

The happy ending: FSV1 deployed ThreatConnect to be the brain of their threat intelligence program. Using ThreatConnect, they built out a uniform procedure so employees could use the company's existing tools and systems to mitigate potential threats. ThreatConnect became a living database that allowed the integration of tools FSV1 already had.

FSV1 started by integrating ThreatConnect into their security information and event management (SIEM) to aggregate their data and then create rules in their SIEM, making the data more powerful. FSV1 also began integrating ThreatConnect with all of their current tools and systems, making each component even stronger and smarter than before, strengthening the company's entire security infrastructure.

Where previously, FSV1 had to input data manually, ThreatConnect automated the company's data ingest. The team can store incidents in one central, and easily-referenced place and pull in data from many new - and different - sources to thoroughly scan for threats. The FSV1 team can now customize each incident using a number of different attributes, making them more easily identifiable.

ThreatConnect helped unite FSV1's entire team: Powerful API allows engineers to write an organization-specific script so management can receive a report at the push of a button; the security director or CISO can now go into ThreatConnect and at a glance see the team's volume of activity, how long each task took to complete, or how long it took them to analyze an incident. Leadership is now able to make informed decisions and adjust organizational workflow to be more efficient.

Results

INCREASED EFFICIENCY

ThreatConnect saved FSV1 an enormous amount of time by streamlining their workflow and cut down on the time spent on each task. For example, an IP query used to take 20-30 minutes in the logger. Using ThreatConnect, the team can find an IP instantaneously.

AUTOMATION AND INTEGRATION

ThreatConnect eliminated the need for a master spreadsheet and served as a central knowledge base for all of FSV1's data, processes, tools, and systems. Because everything was synced, the company can easily determine what needs to be done immediately.

ATTACKS IDENTIFIED BEFORE THEY OCCURRED

ThreatConnect enables FSV1 to find threats before they do any damage. With ThreatConnect's track feature, the organization can enable WhoIs and DNS look-ups on potential threats. This information has led to catching potential phishing attacks within hours of their creation. FSV1 can now disable phishing sites and take them down within hours.

What is ThreatConnect®?

ThreatConnect is the first and only Threat Intelligence Platform (TIP) 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
www.ThreatConnect.com