CUSTOMER CASE STUDY:

Bank of hope

ANOMALI®

Bank of Hope
Bankers. Experts. Neighbors.

CHALLENGE

Bank of Hope needed a way to easily investigate potentially risky IPs without having to log in to multiple security product dashboards. The bank depends on its security information and event management (SIEM) tool as the heart of its incident response program, but when the SIEM flagged a potential problem IP address the analysts needed to spend up to a half hour confirming its reputation.

SOLUTION

ThreatStream offered Bank of Hope a way to sync its actionable intelligence with the organization's SIEM tool and provide analysis with minimal effort.

RESULTS

- Reduced Mean-Time-To-Know
- SIEM Integration
- Headcount Savings

> *"Doing the research was a strenuous process, we had to go to multiple resources to understand the indication of relevance of that IP address to our environment.*
>
> *– Arindam Bose, Senior Vice President & Security Officer for Bank of Hope*

BANK OF HOPE CHALLENGE

When the SIEM pointed to a threat indication, IT security analysts spent an inordinate amount of time looking up potential malicious IPs to confirm their current reputation. Bank of Hope had several systems in its IT environment that provided outside threat intelligence related to malicious IPs, but each of these had its own portal and its own dashboards. Each system provided threat intelligence, but none were intuitively embedded with the SIEM.

So analysts were left with a manual process that required them to look up information within each IT tool that had its own built-in threat information. With a lean staff, the bank could ill afford the kind of resource drain that looking up suspicious IPs was putting on its security operations. Staffers could take up to a half hour simply to determine whether the IP address had a known bad reputation, let alone to start acting on a potential incident once bad news was confirmed.

"Doing the research was a strenuous process," said Arindam Bose, senior vice president and security officer for Bank of Hope. "We had to go to multiple resources to understand the indication of relevance of that IP address to our environment."

Bank of Hope needed a way to simplify the process so it could make better use of its analysts' bandwidth to work deeper into the forensics and incident response process.

OVERVIEW

Operating with $7.3 billion in assets Bank of Hope is the largest KoreanAmerican bank in the nation. As a major community financial institution with 50 branches across the U.S., Bank of Hope understandably must protect itself from a range of attacks against its IT systems. To keep tabs on the numerous security controls and monitoring systems it has in place, the bank depends on its security information and event management (SIEM) system to correlate events and help its analysts stay on top of trends. Unfortunately, until recently the bank's IT security analysts were taxed by the amount of work needed to analyze and verify indicators of compromise (IOCs) related to outside IP addresses that surfaced from its SIEM correlation engine.

THE THREATSTREAM SOLUTION

The bank turned to the power of ThreatStream to do exactly that. According to Bose, Bank of Hope chose ThreatStream for several reasons.

First and foremost, the ThreatStream Threat Intelligence Platform is able to tell analysts with just a few clicks what an IP address' threat score is, along with the confidence level based on reputation ranking. Not only is it able to utilize threat feeds already available to Bank of Hope, but it also provides other feeds that add value to Bank of Hope's analyses. In addition to IP reputation analysis, the tool can also replay executables in its sandbox environment to give Bank of Hope analysts a leg up on early analysis of potential IOCs and threat indicators.

But most importantly, ThreatStream integrates into Bank of Hope's SIEM, so staffers do not need to reroute their analysis process and can do early investigation from a single centralized platform.

"The SIEM is a critical component of our environment and the heart of our program. It pulls in logs from a variety of different systems and correlates those indications to determine whether an activity is malicious or not," Bose says. "Integrating ThreatStream in our SIEM portal means we don't have to go into five different systems, but can look at the validity of an IP or executable from a single place. The solution has minimized much of the team's overhead."

In addition, the bank needed a tool that could work with the FS-ISAC threat intelligence feed for information specific to the financial industry. ThreatStream worked with the bank to develop that capability natively. It was this last point that truly tipped the scale in favor of ThreatStream for Bank of Hope.

Deployment was relatively painless for Bank of Hope, only requiring about an hour a week for the first month. The institution credits ThreatStream's team with offering lots of guidance to get off the ground running.

THE THREATSTREAM IMPACT

Now that the tool is in place, Bose reports the value of ThreatStream to Bank of Hope is in the time it saves analysts and the opportunity they have to address more threats than they once could.

The time it takes to analyze a threat has gone down from 30 minutes to just a few minutes, time that adds up over the course of investigating many malicious IPs every week. "There has been a substantial decrease in terms of meantime-to-know," Bose says.

These efficiencies have enabled Bank of Hope to save on headcount. Because the tool automatically handles a large analytical workload, Bank of Hope was able to increase capacity without having to hire one or two additional analysts. What's more, the false positive rates have been very low, meaning analysts spend very little time chasing non-existent problems.

Overall, the ThreatStream implementation has been a huge success for the Bank of Hope team, so much so that it is now looking at integrating the tool into its IDS/IPS, giving it the potential to automatically block threats with very high malicious confidence ratings.