PERCH

CASE STUDY

5 Hurdles to Threat Intelligence: How one Regional Bank Cleared Them All

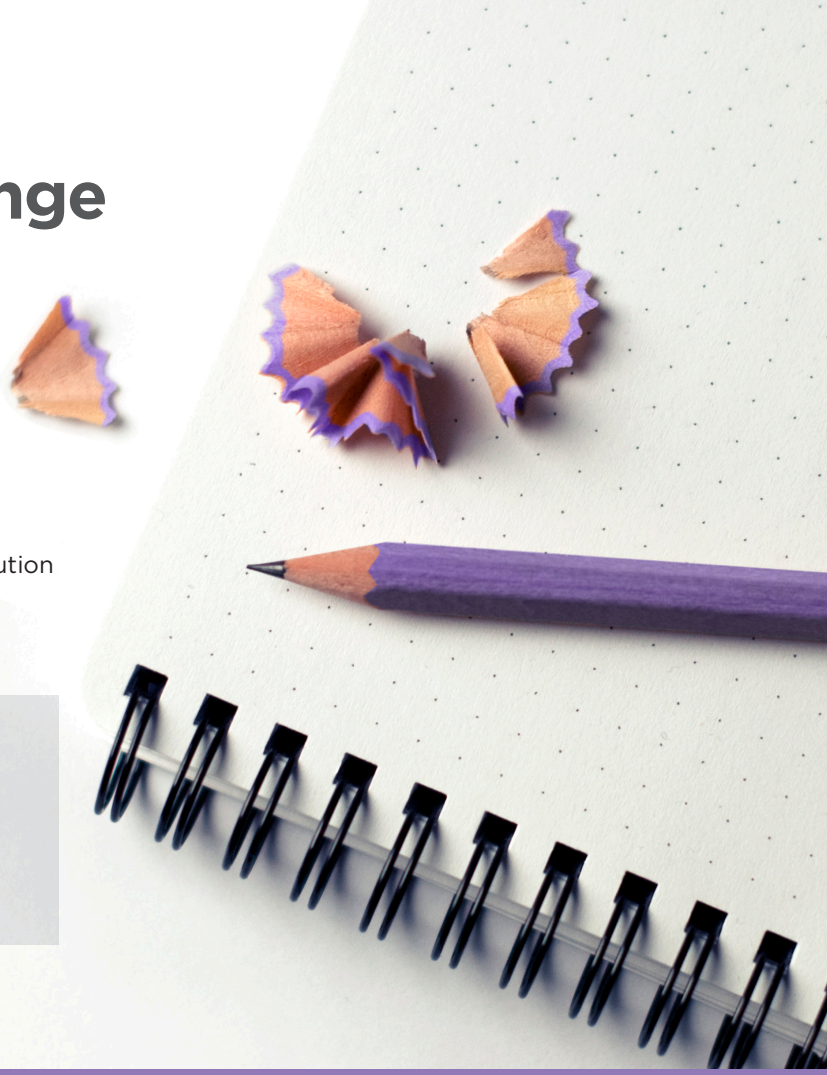
A Blueprint for Small and Mid-Sized Banks

The Threat Intelligence Challenge

Implement and maintain a true threat intelligence program: for years, it was only something that the largest of banks could do. Development costs, complexity and staffing requirements were only a few of the problems organizations face when traveling the road of building a threat intelligence program for their financial institution.

This case study outlines those hurdles and their solution as experienced by Michael Cole, Chief Information Security Officer at First Financial Bank.

1. Complexity
2. Development Costs
3. Intelligence Data Source
4. Cybersecurity Assessment Requirements
5. Staffing



5 Hurdles

1. Complexity

"Implementing an effective threat intelligence program for a community bank is nearly impossible, and there isn't a road map or blueprint on how to do so," Cole recalled. Although First Financial Bank has always had a strong and mature cybersecurity program, he knew more was possible.

2. Development Costs

Cole had seen several Threat Intelligence Platforms (TIPs) on the market, but none appeared attractive. They either came at costs well above the budget of a community bank's information security budget or required significant time and personnel commitments that were not feasible.

3. Intelligence Data Source

In addition, Michael wanted the ability to use the threat intelligence data produced by FS-ISAC (Financial Services Information Sharing and Analysis Center) as a means to detect the threats in his network that other banks and credit unions warn him about. "To be honest," Michael said, "we never really thought it was possible to have an effective TIP, let alone one that would let us pull in the valuable threat data FS-ISAC provides its members."

IMPLEMENTING AN EFFECTIVE THREAT INTELLIGENCE PROGRAM FOR A COMMUNITY BANK IS NEARLY IMPOSSIBLE, AND THERE ISN'T A ROAD MAP OR BLUEPRINT ON HOW TO DO SO

Michael Cole
Chief Information Security Officer
First Financial Bank

4. Cyber Requirement

Other intelligence sources can be useful supplements, but **using curated intelligence from your industry's sharing community (ISAC or ISAO) is acknowledged by information security professionals as the most valuable**; but require significant investment to use efficiently.

Adding to Cole's challenges, state and federal examiners now expect community banks and credit unions to participate and share their threat data with other peers in FS-ISAC.

"The new Cybersecurity Assessment Tool (CAT) expects banks to implement a threat intelligence program and to share their threat data to reach the evolving level," stated Cole. "That's far easier said than done for most of us."

5. Staffing

Cole's key deliverables were: a platform with an affordable cost of entry that also alerts him when his bank has a match for a particular threat that another financial institution warned him about.

But he also wanted a platform that could: help him by reviewing the alerts and threats for him, and only get him involved when it was absolutely necessary.

"One of the biggest wins we get from Perch is not only the ability to detect those threats, but also having help from Perch's security analysts to tell us what threats are real and which ones are false positives," Cole said.

ONE OF THE BIGGEST WINS WE GET FROM PERCH IS NOT ONLY THE ABILITY TO DETECT THOSE THREATS, BUT ALSO HAVING HELP FROM PERCH'S SECURITY ANALYSTS TO TELL US WHAT THREATS ARE REAL AND WHICH ONES ARE FALSE POSITIVES

Michael Cole
Chief Information Security Officer
First Financial Bank

Outcome

First Financial Bank was able to implement an effective threat intelligence program that detects and responds to threats that other financial institutions warned about, provides managed security services to reduce TCO, and satisfies regulatory expectations for cybersecurity maturity.

Perch's Community Defense Platform for threat intelligence, including managed services for alert response, proved the perfect combination of innovative technology and customer service to meet all five of these hurdles.

"Perch has been one of the best value platforms we have implemented within our environment, in terms of ROI and enabling us to respond to threats that matter," reflected Cole. "Being able to protect ourselves from the threats that others in our community warned us about is what true threat intelligence is all about."

Email FSISAC@PerchSecurity.com,
or create an account online at PerchSecurity.com.

Founded in 2016 in Tampa, FL, Perch Security was created to meet cybersecurity needs by enabling institutions of any size to detect the threats their sharing community warns them about — without costly equipment or analyst hours. Perch's goals are to help our customers detect 100% of the threats shared with them, connect them with their best sources of intelligence, and to strengthen sharing communities through increased participation.

PerchSecurity.com