PERCH

CASE STUDY

Threat Intelligence: Beyond the SIEM

Progress Bank shares why, how, and the results

Community banks and credit unions are discovering that their SIEM, while a valuable tool for log correlation and analysis, is an incomplete solution for building out a threat intelligence program. There are some missing pieces to complete that program: one of which is receiving threat intelligence from multiple sources and automating that intelligence to detect threats on the network.

Greg Jones, VP of IT for Progress Bank, a $1 Billion asset bank headquartered in Huntsville, AL experienced this firsthand. “When we went down the path of building out a threat intel program at Progress Bank, we quickly realized our SIEM wasn’t the right tool for the job. We love our SIEM; in fact, we couldn’t live without it. But it solves a different problem.”

Deeper Visibility: From System Logs to Network Packets

Progress Bank uses their SIEM to monitor for notable system events: account admin elevation, lockouts, bad logins and other account-or system-related events. Jones holds that the SIEM is an excellent tool for that log management and analysis.

“[But] our SIEM didn’t have any visibility into the network traffic of the bank,” said Jones. “When we thought about core requirements for a threat intelligence program, we needed visibility into the network packets themselves. For example, Windows doesn’t log anything if you access a malicious website.” **Jones needed a tool that could analyze network packets, including internal traffic, to detect lateral movement by a potential threat actor.**

A SIEM DOES THIS:

Log analysis looks at what the label says is in the packet
(dependent on what the application author chooses to log).

BUT NOT THIS:

Packet payload inspection reveals what’s actually inside.

Threat detection at the network layer provides visibility into data that cannot be seen in system logs. HTTP headers, user agents, file hashes, GET/POST requests and DNS requests can reveal substantial information about a threat. SIEMs do not inherently have the ability to capture these types of threat details.

Threat Intel Feeds are NOT Created Equal

Progress Bank also needed to consume and operationalize different threat feeds to detect network-based attacks. “Our SIEM vendor has its own proprietary threat intel feed. That’s useful, but we wanted to go beyond relying solely on the feed our vendor supports. We want to detect threats FS-ISAC or DHS warns us about as well. And if there are other useful feeds out there, we’d love to utilize those too.”

Greg Jones

Jones was decidedly searching for a new product to complete Progress’ threat intelligence program; and a key criterion for usability was the capability to consume threat feeds via the STIX protocol. Because STIX is an open standard, it can be used across any technology platform to send or receive cyber threats. “Unfortunately for us,” Jones said, “most SIEMs don’t accept the STIX protocol. And even if they did, we’d still be hamstrung in terms of extra licensing costs and configuration complexity.”

> **WE LOVE OUR SIEM; IN FACT, WE COULDN’T LIVE WITHOUT IT. BUT IT SOLVES A DIFFERENT PROBLEM.**

Greg Jones
VP Information Technology
Progress Bank

Perch: Complete the Threat Intel Picture

"We'll always love our SIEM – it is a critical cog in our security strategy," said Jones. "But in order for us to move beyond system logs to protect ourselves based upon the threats that others are warning us about, we need another complimentary solution."

Jones' search ended when he tested Perch Security. "Perch fits our needs. They can consume all of the intel channels we need, particularly from our ISAC. They can detect threats at the network layer and have visibility into things we just can't see on the SIEM. On top of all of those benefits, they perform all of the threat analysis for us and never bother us unless they need to escalate to us. It's a huge win for a small or midsize organization."

Perch Security has become a security control equally as critical for the bank as their SIEM. The complimentary nature of threat intelligence powered by Perch and the system log data of the SIEM work well hand-in-hand. "We're really happy with our decision to use Perch," Jones said. "They give me the comfort of knowing that the stuff running across my network is actually being looked at."

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

PERCH PROVIDES

1 **FS-ISAC threat intelligence consumption**

2 **Threat detection at network level**

3 **Perch threat analysis included in cost**

> “MOST SIEMS DON’T ACCEPT THE STIX PROTOCOL AND EVEN IF THEY DID, WE’D STILL BE HAMSTRUNG IN TERMS OF EXTRA LICENSING COSTS AND CONFIGURATION COMPLEXITY.”

Case Studies available online
PerchSecurity.com/Case-Studies

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