COCC White Paper

Security Operations

The Value Behind a Defensible and Monitored Network

For all financial institutions today, security has become a major component of a strong business strategy. Banks and credit unions simply cannot survive without addressing defense, detection, and risk management against the vast array of cyber threats that exist today. Security monitoring is a key component of this. "Prevention is ideal," writes Dr. Eric Cole, SANS Institute fellow and instructor, "but detection is a must." Detection is just one essential piece of the puzzle for every financial institution that hopes to thrive in a world where cyber attackers are ever-present and smarter than ever.

Aside from the simple fact that hackers, fraudsters, and other adversaries are becoming more creative and driven, the financial industry faces a number of other challenges as well. Regulatory compliance, legal risks, and cost effectiveness all come into play when an organization devises their security strategy. The burden then lies with these financial institutions to monitor the activity that occurs, review changes, and look for events that are unusual, suspicious, or malicious. And when an incident does occur, the institution needs to be prepared to respond effectively.

What Are the Options for Financial Institutions?

Common options for organizations looking to gain centralized security visibility include:

Log Collection and Reporting

Simply stated, this option collects logs and offers reporting and alerting features. While these tools can be inexpensive and offer some quick visibility, they are often utilized for very specific use-cases that may not take a holistic approach to collecting, normalizing, and correlating events from a wide variety of device types. Additionally, these types of tools are not generally best-suited for investigations.

SIEM Tool

Security information and event management, or SIEM, is a tool that is internally managed and monitored by the financial institution. This tool aggregates data about the network and computing environments into a centralized interface and often includes correlation capabilities. An SIEM is also more purpose-built for investigations beyond reporting and alerting. However, the costs to own and operate an SIEM are higher and take time to integrate with your organization's security practices and IT technologies. It also requires staffing security professionals to maintain the platform and monitor effectively.

Outsourced SOC

By outsourcing security monitoring to a security operations center, or SOC, the financial institution shares their log data with a managed security provider (MSP), which then provides security analysis. The MSP can generally offer advanced technology and scalability, the expertise of security analysts on staff, and greater visibility and threat intelligence. On the other hand, if the MSP is limited in terms of its knowledge of the business or environment, and if the relationship and scope are limited as well, then this option could mean greater complexity for the financial institution.

COCC's Approach: Continuous Security Monitoring via SOC

Deep Visibility

Day to day, the SOC is responsible for collecting log events from the financial institution's network devices, as well as collecting log events from the existing MSP environment. The SOC will collect packet data and inventory assets, their purposes, and their importance to your financial institution.

Data Enrichment

The SOC uses threat intelligence data from third parties and internally generated resources to enrich the existing data, allowing the utility to correlate potential threats across multiple financial institutions and across different platforms. Custom detection and correlation rules identify behaviors of anomalous or security-oriented nature.

Security Monitoring

Skilled and certified security analysts are on-staff to support ongoing monitoring, responding to alerts, and analyzing "events of interest" (EOI). Analysts follow defined escalation and notification procedures for incidents. 24x7x365 monitoring is a valuable capability in a detection service. Security metrics, notifications of emerging industry threats, and routine security reports are provided.

Regulatory Compliance

The Continuous Security Monitoring service helps clients to meet the needs for regulatory compliance. This includes standardized compliance reporting for log review and enhancements to an institution's maturity level in regards to detection capabilities.

Reduced/Avoided Overhead

With the COCC Hosted SOC, the SIEM technology is managed and maintained in our data center – allowing our technical teams to manage the hardware provisioning, updates, upgrades, performance tuning, feeds, and other day-to-day logistics. Trained and certified security professionals help the financial institution gain visibility and access to incident handling guidance, augmenting the need for additional, specialized staff. A streamlined implementation process and focus on the financial industry enable cost-saving and time-saving benefits, and a faster ROI.

COCC's Solution

COCC's Hosted SOC solution is available to its client financial institutions. This robust solution offers the best of SIEM and an outsourced SOC, including skilled and certified security professionals on staff, enterprise monitoring tools, and extensive knowledge of cybersecurity and detection. These security services are coupled with COCC's renowned customer service and support. To learn more, contact StrategicProducts@cocc.com.