Case Study

BINARY DEFENSE

Binary Defense Helps Financial Institution Tune Current SIEM

Business

One of the largest banks in the US, with 24-hour ATM and mobile banking options for customers

Challenge

Needed improved SIEM threat detection and monitoring capabilities

Results

Binary Defense tuned the existing SIEM to monitor for threats 24/7

Client team received education and strategy for avoiding cyberattacks

Combined protection from Binary Defense and client team made them more poised to keep their data secure

[1] https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#9bb985b6e906

Financial industry a frequent target for hackers

It's said that there are two types of financial services firms: those that have faced a cyberattack, and those that will. Considering the type of information banks store in their servers - including bank accounts, social security numbers, etc. - it's no wonder hackers are clamoring to get their hands on that info. And they try at an alarming rate - as much as 30 times per second, per institution, on average!

With limited internal resources and budget constraints, financial institutions often look to third party cybersecurity providers to implement solutions to help protect their data. It's often close to impossible for a financial institution to create and sustain their own 24/7 Security Operations Center (SOC).

The largest banks in the US turn to Binary Defense

One of the largest banks in the United States, which offers a wide range of financial products and services for both individuals and businesses, had implemented a Security Information & Event Management (SIEM), but found that it was unable to provide around-the-clock monitoring. In addition, the bank found that its cybersecurity team needed advanced training in the latest threats facing their industry.

The answer? The cybersecurity experts at Binary Defense.

Working as an extension of their team

Binary Defense acts as an extension of their clients' teams, learning as much as possible about each client's unique challenges. From the information gathered, Binary Defense tuned the existing SIEM and began monitoring for abnormal activity. In addition, they trained the internal team at the financial institution on how to respond to alerts passed along to them from Binary Defense. During implementation, Binary Defense also worked with staff at the institution to develop plans to help remediate an attack, should one occur. By developing those use cases, the client is much better prepared and educated to detect and protect against malicious attacks.

Binary Defense also alerted the client security team to multiple attack types that were never previously reported, helping the client avoid the risk of potentially millions of dollars of damage. Additionally, the Binary Defense team detected penetration tests and actual malicious threats through the 24/7 monitoring.

With the strength of the Binary Defense SOC monitoring their institution's SIEM 24/7, and the knowledge of the client team on how to respond to attacks, the financial institution is now much more poised to thwart an attempt by hackers to steal their valuable information.

600 Alpha Parkway, Stow OH 44224
+1 800-246-2792
info@BinaryDefense.com

BINARY DEFENSE™

Learn More about us
www.BinaryDefense.com