Protect your critical assets against cyber-threats

Highlights

Power of breach analytics and monitoring

Be prepared with an incident response plan

Use an expert like an MSSP

Challenge

The Financial Industry Regulatory Authority (FINRA) continues to recognize cybersecurity as one of most pressing issues threatening the financial services industry. Today, your financial firm faces distributed denial of service (DDoS), malware infections, insider threats, ransomware, cyber-enabled fraudulent wire transfers, nation state and terrorist attacks. Motivations range from opportunistic, to ideology, to financial gain.

At the same time the capabilities of malicious actors are increasing there is also a shortage of skilled cyber security personnel. According to the Center for Strategic and International Studies, in the U.S. alone 209,000 cyber security positions went unfilled. Together with the National Institute of Standards and Technologies, FINRA issued a series of recommendations for how businesses can fortify their cybersecurity defenses, including an analysis of existent practices and a checklist of recommendations for small financial firms. While these recommendations comprise a solid beginning to fortifying your firm against breaches, they are just that—a beginning.

Solution

To help financial services firms stay ahead of cyber-attacks in today's IT environment, Eastwind Networks works with Managed Security Service Providers (MSSPs) to provide affordable, best-of-breed breach detection solutions. The driving concept behind breach detection is to analyze the network and search for known bad, anomalous or suspicious activity, which may indicate an attempt or successful compromise of an organization. While the checklist and recommendations provided by FINRA constitute basic due diligence, the impact of a security breach should be enough to prompt financial firms to take extra steps in securing their business against internal and external threats. To remain a step ahead, these three security resources can take your business to the next level of security.

EASTWIND NETWORKS

SOLUTION BRIEF

Three resources for your cyber security checklist

1. Breach Analytics and Monitoring

The main function of breach analytics and monitoring is to identify attacks in near real time while also examining for breaches that may have occurred in the past. The average time to detect an attack is 200+ days. If your breach detection system didn't recognize it as it happened, it has no ability to go back in time and identify the threat when it occurred months ago.

Advances in intrusion detection have been substantial leading to next generation breach analytics and monitoring platforms. This is where the Eastwind Breach Analytics Cloud shines. This exceptional system serves as a time machine, ingesting new threat intelligence and searching past activity to identify attacks that occurred in the past. Eastwind's technology marries the numerous advances in capabilities such as heuristics, machine learning, statistical analysis and threat intelligence into a single product that continuously monitors potential problems from several vantage points using the right tool for the job to identify, prevent and triage breaches.

2. Incident Response Plan

An incident response plan (IRP) typically lays out all the steps needed to ensure detection, analysis, containment, eradication and recovery after a security breach has occurred. This process requires skills in short supply and is time critical to reduce risk and losses to the organization. A new cyber security market has developed for Security Incident Response Platforms (SIRP), also referred to as Security Automation and Orchestration.

These platforms allow organizations to define their incident response workflows to automate numerous steps increasing their efficiency and effectiveness while scaling more experienced staff. Automated incident response behaves like a dedicated CSIRT, but at machine speed, meaning it can quickly kill running processes, remove malicious files, halt data exfiltration and notify all appropriate parties, simultaneously. While larger firms may employ a dedicated 24x7 Computer Security Incident Response Team (CSIRT) to handle such response, smaller firms may outsource to third-party vendors.

3. Managed Security Service Provider

Partnering with a Managed Security Service Provider (MSSP) is an excellent way to ensure 24x7 coverage in addition to gaining access to highly skilled and experienced personnel. MSSP's can provide continuous monitoring for malicious activity, incident response capabilities and are able to cost effectively design, deploy and manage security solutions to provide complete visibility to threats, security gaps, network awareness and application usage. Many MSSPs also provide compliance offerings to meet industry specific standards and ensure clients meet a certain level of due diligence.

Extra Steps for Extra Precaution

By employing breach analytics and monitoring, a cohesive incident response plan bolstered by a SIRP, and partnering with an MSSP financial firms can enhance their compliance with FINRA's suggested cybersecurity and create a robust security toolkit to protect their bottom line and fortify against attack and intrusion. To help your business cost-effectively establish and maintain a multi-function security system with breach detection, Eastwind Networks works with Managed Security Service Providers to provide your business with the outsourced monitoring and detecting you need in today's challenging IT environment.

About Eastwind Networks

Eastwind Networks offers the only breach analytics cloud that provides complete visibility of your key cyber terrain. We collect and analyze telemetry from your corporate networks, virtual networks, cloud infrastructure providers, cloud application providers and your mobile workforce—quickly and easily. Always watching, our automated hunters enable organizations to identify malicious activity that has evaded other security solutions. Eastwind Networks as founded in 2014 and was named a Founders 50 member by Dell.