Maintaining Financial Service Security

With Observer® Platform Monitoring and Packet Analysis

Setting up alert triggers by both looking at suspicious traffic and analyzing packets is key. Engineers like me are beginning to see GigaStor™ as an active security tool in addition to its considerable value as an after-the-fact forensic device.

Senior Network Engineer

Headquartered in America's heartland, an S&P 400 financial services company has grown to include nearly 6,000 associates serving more than 11,000 customers. The organization provides electronic payment solutions, financial processing services, and business process automation to customers around the globe. With over 300 different products and services, the company relies heavily on complex network technologies to deliver its services and to protect client assets. In addition, the web-based financial applications must be available and secure 24 hours a day, 7 days a week, 365 days per year—without a hitch.

To support these critical applications and services and to maintain the highest security, the company's IT team depends on the Viavi Solutions™ Observer performance management platform.

A Team Effort

The company's network and security teams work together closely to keep their complex network secure and free of malicious activity. Their progressive security forensics strategy focuses on sharing information seamlessly despite the complexity of their network.

"We are a financial services company but we're not an individual bank," says a senior network engineer. "Every product has slightly different security requirements and different maintenance windows. While we keep everything logically separated, we combine everything at the service level. That gives the network security engineer and her team the ability to see everything, all at once, from one central location."

Part of the IT department's strategy is employing and sharing access to the same toolset for monitoring and troubleshooting. This focus helps to facilitate communication between the individual teams. "We are using some packet brokers with traffic being sent to GigaStor for long-term packet capture, along with various other forensic tools, and VPMs," according to the senior network engineer. "This way, the network security engineer has full visibility, from the front end to the back end, all the traffic and everything she needs to make sure that the bad guys don't get away with anything."

Hackers Unmasked

Recently, the team's intrusion detection system (IDS) alerted them to a potential breach. It took everything in their arsenal to get to the bottom of who was behind it. "We were under a DDoS attack. Our security group consists of three sections, one of which is the cyber intel group. They're actually tied into a global security community. They've got contacts at the FBI."

After reaching out to the FBI, the engineer began collecting packets from Observer GigaStor to see if the team could examine which protocols were involved in the attack. "It's hard for us to know what's going on from just an IDS alert. They give you just a smidgen of information and it's usually not enough to know what's really happening. So we need to review packet captures."

With the Observer platform, the security team captured and analyzed the traffic. By focusing on the payload of the TCP packets, they learned key details of the attack.

"It was a UDP reflection attack," said the security engineer. "We were seeing DNS, NTP, and SSTP. It was a typical attack pattern but we also noticed that, mixed in with all that UDP traffic, we were seeing some TCP traffic."

With the data contained in the packets, they were also able to positively identify the attackers. "We got a name to go with this hacker team," she says. "They were very vocal. Once we had this information, our cyber intel team started looking for Twitter feeds. We started building a whole profile about this group that was attacking our resources."

Tools Reveal Malicious Traffic

Because the team works so closely and uses the Observer Platform to set accurate baselines and analyze traffic patterns, they were recently able to thwart another serious attack when high levels of e-mail traffic on the network raised suspicion. "We saw what appeared to be a tremendous amount of e-mail activity," the network engineer noted, "but when we looked closer at the payload, it wasn't e-mail at all."

Using Observer Analyzer and the packet-capturing power of GigaStor, the team detected the actual source of the traffic and stopped the flow before it could impact their customers. "It was information that shouldn't have been going where it was. Setting up alert triggers by both looking at suspicious traffic and analyzing packets is key. Engineers like me are beginning to see GigaStor as an active security tool in addition to its considerable value as an after-the-fact forensic device."

Understanding normal traffic patterns on the network is the first step to combating malicious activity. By capturing packets, you can rewind time and see exactly how events unfold.

Easily Share Insight to Increase Awareness

Cyber attacks are becoming increasingly common, but most of the time the biggest problem that IT teams face is the ubiquitous "slow network" complaint. The IT department is the first line of defense for some of the world's largest financial institutions.

"The network stuff is usually the easiest to either confirm or rule out as a problem. In the process of doing that, we generally gather enough information to help other teams to get it fixed fast. We use the GigaStor for that a lot."

Once the information is collected, and the team has ruled out a network issue, they can pass along what they've learned with visual representations like those generated with the Observer Apex tool. Pre-built widgets enable sharing information with other groups, such as the security team, quickly and easily.

The Future of Performance Management

Since deploying Observer performance management products, the IT team has been able to more easily protect the sensitive information traversing their network. However, the security engineer is not ready to stop there.

"There are capabilities with GigaStor that we haven't even used yet," she says. "The security office is looking at creating a hunt team. Using certain indicators, we will start to proactively go out and find traffic that looks unusual and follow it out to see if we have a problem. This would be a step further than just signature alerts. These could be issues to which we may never have been alerted and GigaStor would be a big part of finding them."

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.

financialservice-cs-ec-ae
30179518 900 0815