opentext™

Case Study

IT Security Provider

IT firm uses ArcSight to dramatically improve cybersecurity visibility for telecommunications company.

Overview

As a provider of innovative cybersecurity solutions to customers around the world, this IT security provider, who prefers to remain anonymous, understands the challenges of securing large and complex IT environments.

The company has a customer portfolio that includes banks, manufacturers, and airlines. These clients utilize the solutions the IT security provider sells to collectively monitor thousands of devices, systems, and applications. Some have a significant workforce with minimal IT knowledge, which creates security risks and technological gaps.

Challenge

One such customer is a large telecommunications provider that contacted the IT security provider to help resolve a cybersecurity problem. The company's complex IT environment and multiple levels of bureaucracy were causing headaches for IT employees trying to monitor the company's environment for threats.

To detect security breaches or suspicious behavior, the telco needed to monitor data logs from thousands of devices and applications. This included applications created by the company's in-house developers, as well as many types of telecommunications equipment. "We're talking about a very large number of systems," says a manager at the IT security provider.

Interpreting the deluge of data logs generated by these devices and applications was difficult. The number of applications and devices was also rapidly increasing.

Collecting and ingesting the logs was timeconsuming. IT employees couldn't access the systems and logs belonging to some business units, but instead needed to ask for help from relevant managers. Someone also had to sign forms giving them permission to collect the data.

Even if employees did collect, ingest, and analyze the log data, they couldn't do it quickly enough to respond to breaches. "It was taking too much time. If there was an attack, it would

"This is for companies that don't just want a token SIEM. The system is very flexible. They can customize it and fine-tune it any way they want."

MANAGER
IT Security Provider

At a Glance

- **Industry**
  Software & Technology
- **Location**
  Undisclosed
- **Challenge**
  Help protect the operations and reputation of a large telecommunications company from cyber attack.
- **Products and Services**
  ArcSight
- **Success Highlights**
  + Enabled customer to monitor 2,000 systems
  + Simplified monitoring of applications created in-house
  + Customized alerts to increase accuracy of threat detection
  + Dramatically improved security visibility and significantly reduces time to detect threats

have been finished before they could act to prevent or stop it," says the manager. As a result, the company did not comprehensively monitor its systems for security threats.

There was also a risk that any of the company's many employees would inadvertently cause a security breach. They had minimal understanding of cybersecurity, and might be lured by attackers to click on links to malware or phishing schemes. Without a way to quickly monitor network activity, the company didn't know if users were adhering to security rules. "Their security department created security policies, but if users didn't abide by them there was no way to catch them," the manager says.

The telco was therefore highly vulnerable to data breaches. The company had also failed an audit, designed to check that systems followed the Payment Card Industry Data Security Standard (PCI DSS). If the company didn't resolve this problem, there would be potential financial sanctions.

Solution

To speed up the telco's ability to detect threats, employees needed a centralized mechanism to collect and ingest data logs from the entire business. They also needed a way to rapidly analyze the logs.

To achieve this, the company purchased a security information and event monitoring (SIEM) solution. This would automate the collection and analysis of log data, allowing IT employees to respond to threats much faster.

The company tested SIEM solutions from LogRhythm and OpenText™, and evaluated a solution from RSA. Like many of the IT security provider's customers, the telco scrutinized the products in detail, spending a year testing ArcSight Enterprise Security Manager (ESM) by OpenText™ proof of concept. "Our customers want to dig deep into the functionality," the manager says.

By late 2016, the company chose the OpenText™ solution, primarily because employees could integrate with various applications and devices, and because the system could be customized to detect threats more accurately and in real-time. "The Micro Focus (now part of OpenText™) product's flexibility was the deciding factor," says another manager at the IT security provider.

Results

Simplifies Security

The telco was in the final stages of integrating ArcSight ESM at the time of writing. The IT security provider expects the solution will provide significant benefits.

One will be simplifying the task of monitoring the complex IT environment. The telco has connected more than 2,000 systems to ArcSight ESM. "Even the employee attendance machine is connected to ArcSight," the manager says.

The OpenText solution also makes it easier to monitor applications that the telco has customized. To connect some SIEM tools to these applications, employees would usually need assistance from the software vendor that created the applications. But they found this wasn't necessary using ArcSight ESM.

Processing the log data was also much easier. Previously, even if IT staff members had access to log data, they weren't always able to understand it, the manager notes. "They would have to ask, 'What am I looking for? How can I detect if something is wrong?'" he says. By contrast, the OpenText solution performs the difficult and repetitive part of this process automatically. "ArcSight opens the logs, and reads and classifies them. It formats them in a way that administrators can understand," he says.

By collecting data from many systems, the ArcSight ESM gives the company a greater likelihood of detecting suspicious network activity. This allows staff members to respond to security events to determine the threat risk, reducing the risk of attacks interrupting operations or damaging the company's reputation. It will also save employees hours of work.

The company received encouraging evidence of this during the proof of concept test, when ArcSight ESM alerted employees to a vulnerability they had not previously seen. "It was something they could not detect before. That was a major convincing argument to purchase ArcSight," the manager says.

Provides Accurate Threat Detection

Another important benefit is that users can customize ArcSight ESM so that it provides more accurate alerts about potential breaches.

For example, organizations can create use case rules and content that directs the SIEM which specific system activity they are most concerned about. This is particularly helpful for banks, which can create rules to alert them to certain activity involving their databases.

"The system is very flexible. They can customize it and fine-tune it any way they want," says the manager. "This is for companies that don't just want a token SIEM."

These rules can be used to identify potential network activity as suspicious, even if it doesn't technically breach company policies. For example, during the ArcSight ESM proof of concept test, a use case rule alerted the telco to a user logging on to the organizations' systems at 3 a.m.

> "Whenever we have a large customer with a lot of customizable solutions, then we go with ArcSight."
>
> **MANAGER**
> IT Security Provider

Connect with Us
OpenText CEO Mark Barrenechea's blog

Addresses Compliance

An increasing number of the IT security provider's customers are requesting SIEM tools to address regulatory compliance, according to another manager. "We are seeing [governments] enforcing banks to go through a SIEM solution for PCI compliance. I'm seeing customers request that more and more," she adds. With the ArcSight ESM implementation nearly complete, the telco is already looking at other ways it can improve security. This could include purchasing Fortify, which tests software code for vulnerabilities.

Learn more at
www.microfocus.com/opentext

opentext™