MICRO FOCUS

Case Study

Security

Paladion

A leading Managed Detection and Response (MDR) provider protects large organizations from cyberattacks and simplifies task of monitoring sprawling IT environments with Micro Focus ArcSight.

Overview

Eribus, et rehende ilit magnis venissinciam Established in 2000, Paladion has almost 1,000 employees and customers across the United States, India, Malaysia, and the Middle East. As a Managed Detection and Response service provider, Paladion's success depends on protecting diverse organizations from cybersecurity breaches. The company's clients include large banks, telecommunications providers, government entities, and retail organizations.

Challenge

The customers face sophisticated attacks and a dynamic threat landscape. To avoid being overwhelmed with security alerts, they need to identify the threats relevant to their vertical industry sector and configure their defenses accordingly.

"The outcome of a breach of credit card data isn't just a financial loss, it's damaging to a company's brand reputation."

DEEPAK JACOB

Projects Director for Europe, the Middle East and Africa
Paladion

They also need to monitor large IT environments. In many cases, they have thousands of devices generating vast amounts of data. They often find it insurmountable to check all data for signs of compromise.

For example, a large retail company (referenced throughout this study) contacted Paladion in 2014. The retailer operated many different businesses in several countries and had experienced several cybersecurity breaches, including one resulting in a financial loss.

Senior leaders were concerned by the widely reported security breach involving a large retail company from which customers' credit card details and other data were stolen. A similar incident would have been extremely damaging to Paladion's retail customers, says Deepak Jacob, Paladion's Projects Director for Europe, the Middle East and Africa. "The outcome of a breach of credit card data isn't just a financial loss, it's damaging to a company's brand reputation," he says.

Solution

Paladion doesn't just help customers detect cybersecurity attacks—the company also rapidly remediates threats.

PALADION
HIGH SPEED CYBER DEFENSE

At a Glance

- **Industry**
  Software & Technology
- **Location**
  United States, India, Malaysia, Middle East
- **Challenge**
  Protect banks, telecommunications providers, government entities, and retail organizations from cyberattacks.
- **Products and Services**
  ArcSight Enterprise Security Manager
  ArcSight Activate Marketplace
- **Success Highlights**
  + Monitored thousands of devices and data logs every second
  + Increased number of incidents detected from one to 40 per month
  + Decreased time to alert customers and remediate serious threats
  + Reduced risk of breaches and fraud; helps customers avoid financial loss and damage to operations

Paladion takes a multi-pronged approach to this challenge. To detect threats, the company automates the task of monitoring customers' systems. Paladion uses Micro Focus ArcSight Enterprise Security Manager (ESM) to rapidly collect log data from customers' devices and software, and analyzes it to detect threats. The software sends alerts about threats to a security operations center in Bangalore, India, which is staffed around the clock. This team is supported by other security centers in the United States, Canada, India, United Arab Emirates, and Malaysia.

Paladion also continually manages and customizes ArcSight ESM for each customer, which is vital to ensure threats are identified accurately and quickly. "A SIEM is not a setand-forget technology. It requires custom use cases for it to be effective," says Jacob.

The company's research team constantly examines new attack methods and learns how best to detect them. It then creates use case rules that tell ArcSight ESM what to do when it detects compromise or vulnerability. This speeds up the response to attacks, and ensures that security alerts point to actual threats, not innocuous activity. "If you don't monitor for the right things, your security won't be effective," says Jacob.

When Paladion develops a use case rule through ArcSight Activate for one customer, the rule also can be quickly deployed using ArcSight ESM to protect other customers. "One of the reasons we use ArcSight is because of this flexibility," says Jacob. He suggests this process would take much longer using other SIEM tools.

Paladion also goes a step further to detect threats. Log data collected by ArcSight ESM is fed into Paladion's proprietary analytics platform, which examines the data for suspicious activity. This considers user behavior and endpoint, application, and network activity.

The company doesn't stop at notifying customers about threats. When ArcSight ESM or Paladion's analytics platform detects a threat, Paladion can respond in two ways. First, Paladion's own security response orchestration platform uses supervised machine learning to automatically take action. It draws on years of data about how to remediate certain threats and can block access to a url or take myriad other steps. Second, Paladion's incident response team can work with clients to remediate more complicated threats.

In addition to providing rapid detection and response services, Paladion's security governance team helps customers improve their security policies and defenses. Paladion staff members also can work at a customer's site to test systems for vulnerabilities and train employees to follow security best practices. For example, Paladion trained employees for the retailer previously referenced.

Other Micro Focus security tools that Paladion uses to protect customers include Micro Focus Security Fortify to test software code for vulnerabilities, and Micro Focus ArcSight User Behavior Analytics (UBA) to check for anomalies in users' activities on company systems.

Results

Cypersecurity Visibility

Paladion has dramatically improved the cybersecurity visibility of more than 100 organizations. This is possible because ArcSight ESM can rapidly sort through thousands of data logs to find signs of attack. Paladion's analytics platform also improves the likelihood of detecting threats.

In the case of Paladion's retail customer, Micro Focus software collects data about 9,000 events per second. After filtering and correlating that data, the software issues approximately 40 alerts about potential security breaches each month. Because the retailer had no central monitoring in the past, it would have been unaware of these incidents.

The software alerts Paladion's customers to signs of security incidents involving their own employees. For example, the company's retail customer receives more than 100 alerts each month regarding potential violations of company cybersecurity policies, including alerts about unauthorized Internet and email use. The software also alerts the retailer to about 200 incidents of unauthorized system access each month. The retailer also used the software to trace the source of an internal security breach, which the retailer stopped.

The retailer's executives now have a much clearer understanding of their company's security posture, using reports generated by ArcSight ESM. The software also automatically checks compliance with the Payment Card Industry Data Security Standard and ISO standards.

Meanwhile, Paladion, as a managed security detection and response services provider, also monitors large numbers of devices for other customers—including 2,500 devices connected to ArcSight ESM for a telecommunications services provider, and 2,000 additional devices for a bank. As a result, these organizations have stopped or contained various breaches and minimized the risk of damage to their reputations and operations. For example, the bank avoided the loss of more than $200,000 by preventing fraud.

As a result, these organizations have stopped or contained various breaches and minimized the risk of damage to their reputations and operations. For example, the bank avoided the loss of more than $200,000 by preventing fraud.

> "One of the reasons we use ArcSight is because of its flexibility."
>
> **DEEPAK JACOB**
> Projects Director for Europe, the Middle East and Africa
> Paladion

Contact us at:
www.microfocus.com

Like what you read? Share it.

Rapid Threat Detection and Response

Paladion's research into attack methods and the company's creation of use case rules speed up the time to detect and contain breaches and fix security vulnerabilities.

This has helped customers respond quickly to rapidly spreading threats. Paladion defended the retailer mentioned in this study against the WannaCry ransomware, which spread in early 2017. Within four hours of the WannaCry outbreak, Paladion deployed a use case rule to protect the customer. As a result, only one of the retailer's many computers was compromised.

Paladion also has used ArcSight ESM to successfully defend customers against other wide-scale cybersecurity threats—including the Shamoon virus—and against attackers seeking to exploit the Heartbleed vulnerability.

Lower Security Costs

Jacob estimates that security costs of Paladion's customers are 70 percent lower than if they had established their own equivalent defenses. The biggest savings include not having to build a security operations center (SOC) and hire a security team.

He says some customers would require as many as eight security analysts, as well as an employee to respond to threats, supported by a data scientist, a threat researcher, an SIEM administrator, and an SOC manager. Combined with the cost of an SOC, these expenses could add up to more than $1 million.