Orange
Cyberdefense

Customer stories

Arriva Trains Wales is part of the Arriva Group. They wanted to protect its business systems and its financial and customer data from a potential breach.

Customer profile

Industry: Transport
Location: Europe

Solutions provided

- LightCyber - Magna
- Behavioral Attack Detection

Business results

- Visibility of network and end points in one integrated system
- Low number of daily alerts, with high accuracy
- Magna is working as a new audit tool for the network
- Ransomware alerts allowed Arriva to quickly quarantine an infected computer
- Easy set up with minimum configuration
- Unauthorized and risky employee activities uncovered

Background

Arriva Trains Wales is part of the Arriva Group, a part of Deutsche Bahn (DB), one of the largest providers of passenger transport in Europe, employing more than 55,000 people and delivering more than 2.2 billion passenger journeys across 14 European countries each year. The Arriva train network extends throughout Wales and the border counties of England, providing local and long distance services to destinations including major cities such as Cardiff, Birmingham and Manchester. It has over 2,200 employees, 247 stations and a fleet of 128 trains.

The challenge

Committed to the highest levels of quality and reliability for its customers, Arriva Trains Wales wanted to protect its business systems and its financial and customer data from a potential breach. Paul Stern, IT Network and Security Manager, understood that traditional security was no longer enough to detect a would-be attacker and that eventually one would gain access to the network. “If an attacker wants to get into a network, there are a million ways and eventually they will succeed,” said Paul. “It’s the new reality of security.” They also wanted to address a PCI DSS requirement to detect security events on their internal network.

The firm’s Qualified Security Assessor (QSA) for PCI compliance put the problem simply to Paul, “If you had an attacker on your network, how would you be able to detect it?” At the same time, the parent company was driving adherence to the PCI DSS (Payment Card Industry Data Security Standard). “We budgeted for PCI DSS and started looking for the best solution out there to give us visibility inside our network,” said Paul.

We picked Light-Cyber because it could clearly show us what was going on. Magna could tell us straightaway if something was wrong on our network.

Paul Stern, IT Network and Security Manager

The solution

"We looked at two behavioral analysis type solutions," said Paul. "We picked Light-Cyber because it could clearly show us what was going on." The other solution had a futuristic interface that was appealing but could not clearly show the real issues. In contrast, "Magna could tell us straightaway if something was wrong on our network," explained Paul. Another important consideration was having integrated visibility of both the network and the endpoints to provide a high level of accuracy and actionability. During the evaluation, Magna even found ransomware files on a host that had not yet fired and stopped the threat even before it started.

Arriva did an initial evaluation by deploying the LightCyber Magna solution in their network. During the evaluation, they became accustomed to looking at Magna every day to know the status of their network and see other discoveries it made, including finding operationalized malware that escaped perimeter security and was communicating with sites or other software. It also uncovered risky behavior that could compromise the network. Some of the findings included some unauthorized remote access tools and also IT applications that were out-of-date. "After the month evaluation, LightCyber took Magna out and we immediately missed it. It was easy to establish a business case for it, so we purchased the product."

Setting up the Magna appliance was astonishingly easy. "It worked almost right out of the box," said Paul. Magna immediately started learning the Arriva environment. "It really didn't have to be taught or configured," said Paul. "There's not enough of us to have to invest time to try to make something work. There can't be any of this messing around."

The outcome

"Magna is kind of an audit tool for our network," said Paul. "We deployed a tool from one of our partners, and Magna showed that it was port scanning the network and pinging various internal IP addresses. We never would have known this without Magna. It gives me confidence when I see how it finds various activities on the network. I know Magna will find any active attacks if and when they occur."

Magna found other irregularities. At one point it highlighted unusually high traffic utilization from some devices. It turned out that an employee was uploading video from company CCTV camera to his Facebook account. While this was not a strict security issue, it was in violation of company policies, and the incident was curtailed.

Business benefits

Generally, Magna produces 4-5 alerts per day for Paul's team. The number is easily manageable, and Arriva Trains can review all them and prioritize their response. No staff time is involved with trying to sort through a voluminous number of alerts that are mainly comprised of false positives. Having a new approach to security based on behavioral profiling has been critical to fulfilling PCI responsibilities and protecting the integrity of the company. "Our executives watched as the CEO of TalkTalk went on national television and had to explain about their recent data breach," said Paul. "Right then we decided that we never wanted to be in that position. That's why we have LightCyber.

About Orange Cyberdefense

In 2019 SecureData UK & SecureLink UK were acquired by Orange Group to be part of Orange Cyberdefense, the Group's expert cybersecurity business unit. Today Orange Cyberdefense is Europe's leading managed security, threat detection and threat intelligence services provider. We help customers anticipate threats, identify risks, protect their IT assets, detect breaches and respond to security incidents. With a 25+ years track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world, we can offer a global protection with local expertise.