GLOBAL INSURANCE GIANT TACKLES SECURITY WOES

The Business Challenge

As an insurance company, operating across three continents, the customer was having regular security incidents involving the compromise of user desktop and laptop devices. These were being caused by a combination of user behaviour and challenges in IT management.

Although the customer engaged with Daisy* security consultants to understand the root-causes of these incidents and to improve internal processes, they also wanted to improve the speed of response to incidents.

The customer had already purchased a vendor log collection and alerting system. However, this was being managed by a single person, so response to alerts was dependent upon that single person's working hours - not satisfactory when cyber security breaches can lead to loss of personal data. Reasonable progress had been made on the logging system configuration, although too many alerts were being generated for the customer to be able to correctly identify the most important events.

In addition, where an internal security issue was uncovered, the response required (usually to isolate the device from the network) was again dependent upon IT teams that didn't cover 24/7/365.

The Solution

The customer's existing system was provided by a vendor on our Select Vendor List. This meant that we have extensive experience in its configuration and were able to continue to support it from the Daisy Security Operations Centre (SOC) in the UK.

We helped to improve the configuration of the vendor logging solution, and integrated it into the Daisy SOC 24/7/365 monitoring, alert and response systems. This meant that the customer received significantly fewer alerts, as Daisy engineers screened for only significant events that needed investigation.

Where we deliver a 24/7/365 monitoring and alerting solution, escalation to the our incident response team normally only happens infrequently, in response to serious issues that cannot be managed by the customer's own IT (or security) function. However, for this customer, with regular user device compromises, a pre-agreed incident response to access the network and isolate compromised devices was put in place.

This meant that rapid response to incidents could be carried out 24/7/365 by our SOC Engineers without having to wake an on-call engineer within the customer's organisation. If this happened during the night or weekend, devices were then secured, with communication to the relevant IT support desk for the start of their next working day.

In addition to alerting, reporting, and incident response to support the customer technical teams, we also delivered regular senior management briefings to help the leadership team understand the current security issues, and root-causes. This was an important communication to gain management support for ongoing cyber security improvements.

Benefits

- 24/7/365 SOC monitoring and incident response
- Existing system upgraded with Daisy cyber security technologies
- Custom incident response to isolate compromised internal devices
- Consultancy support to identify root-causes and reduce repeat incidents
- Management briefings to help the leadership team understand security issues and improvements

AT A GLANCE

Industry sector: Insurance

Solutions/services taken:

- Incident Response
- 24/7/365 SOC monitoring

Length of relationship: 8 years

*The initial engagement was with ECSC, acquired by Daisy in 2023