FUJITSU

CyberDefence solution secures Health Services

Government health agencies are responsible for the digital transformation of their health services. As hospitals replace legacy, paper-based systems with modern, digitally integrated systems, they increasingly become targets for malicious actors to hack their systems and steal personal or health information then use ransomware or destructive viruses to create havoc.

The Pandemic has motivated threat actors to accelerate their cyber-attacks on Health organisations around the world, disrupting and compromising health services at a critical time for communities and governments. The potential cyber breaches could threaten the continued operations of the health services that depend on mission critical applications to admit, diagnose, treat and discharge large patient volumes every day of the year.

Sophisticated cybersecurity technology can reduce the vulnerability to cyberattacks without interfering with the user experience. These high-end technologies can protect critical systems and sensitive information with improved threat detection capabilities and by augmenting the ability to react to cyberattacks.

"Fujitsu established a CyberDefence Service capability for real-time analysis of security alerts generated by endpoints and networks. The CyberDefence Service was designed to detect and alert High Priority Incidents and trigger Major Incident Management Teams. It included advanced attack and readiness operations for example ransomware or intrusion led incident capture for analysis, containment and eradication."

Fujitsu Team Lead

Challenge & Solution

Challenge

This large Australian government agency is responsible for providing technology to hundreds of community and acute hospital health service providers. When another government agency had a cyber breach, the decision was made to invest and improve cybersecurity.

As part of the application landscape, the agency identified the need to upgrade their cybersecurity threat intelligence and response capability to anticipate and respond to an increasingly aggressive threat landscape.

The greatest concern for the Fujitsu team was the implementation. The team would need to overcome the challenges presented by a complex environment of modern and legacy technology.

Solution

Fujitsu planned the Design, Build and Run of the web filtering and network intrusion applications to defend against malicious cyberattacks.

The Fujitsu Cyber team worked closely with the customer to understand the business priorities and how to architect a technical solution to protect the application stack across the software development lifecycle and de-risk the end users. The Australian Cyber Security Centre (ACSC) Essential 8 was the core framework that informed design.

Fujitsu planned the Design, Build and Run of the web filtering and **network intrusion applications**

The **Fujitsu Cyber team** worked closely with the customer to understand the business priorities

The **Australian Cyber Security Centre (ACSC) Essential 8** was the core framework that informed design.

Outcomes

The outcome is a more security conscious enterprise that is cognizant of social engineering, phishing and other intrusion techniques designed to hack the security. The Fujitsu team continues to work side by side with the customer's security experts to proactively assess systems for vulnerabilities, accelerate remediation and continuously monitor the environment for all potential threats. The dashboards indicate zero breaches, but the vigilance continues unabated.

The CyberDefence Service has enabled the organisation to be prepared to respond to a potential breach with a Cybersecurity Incident Response Plan (IRP) designed to prepare for, detect, respond to and recover from network security incidents. Future threat responses include a virtual run of IRP as a desk top exercise which will enable Fujitsu to more effectively support the customer to recognise, mitigate and eliminate or repel attacks.

Finally, the legacy Cybersecurity platform - which was considered to have a zero-day vulnerability with no known patch - was dismantled and decommissioned.

> "Fujitsu delivered a Cybersecurity implementation to upgrade infrastructure, application and data security for a large, complex health system. The program included a suite of cyber applications including new, proactive web filtering to block malicious sites, infrastructure end point protection and network intrusion prevention."
>
> Fujitsu Team Lead