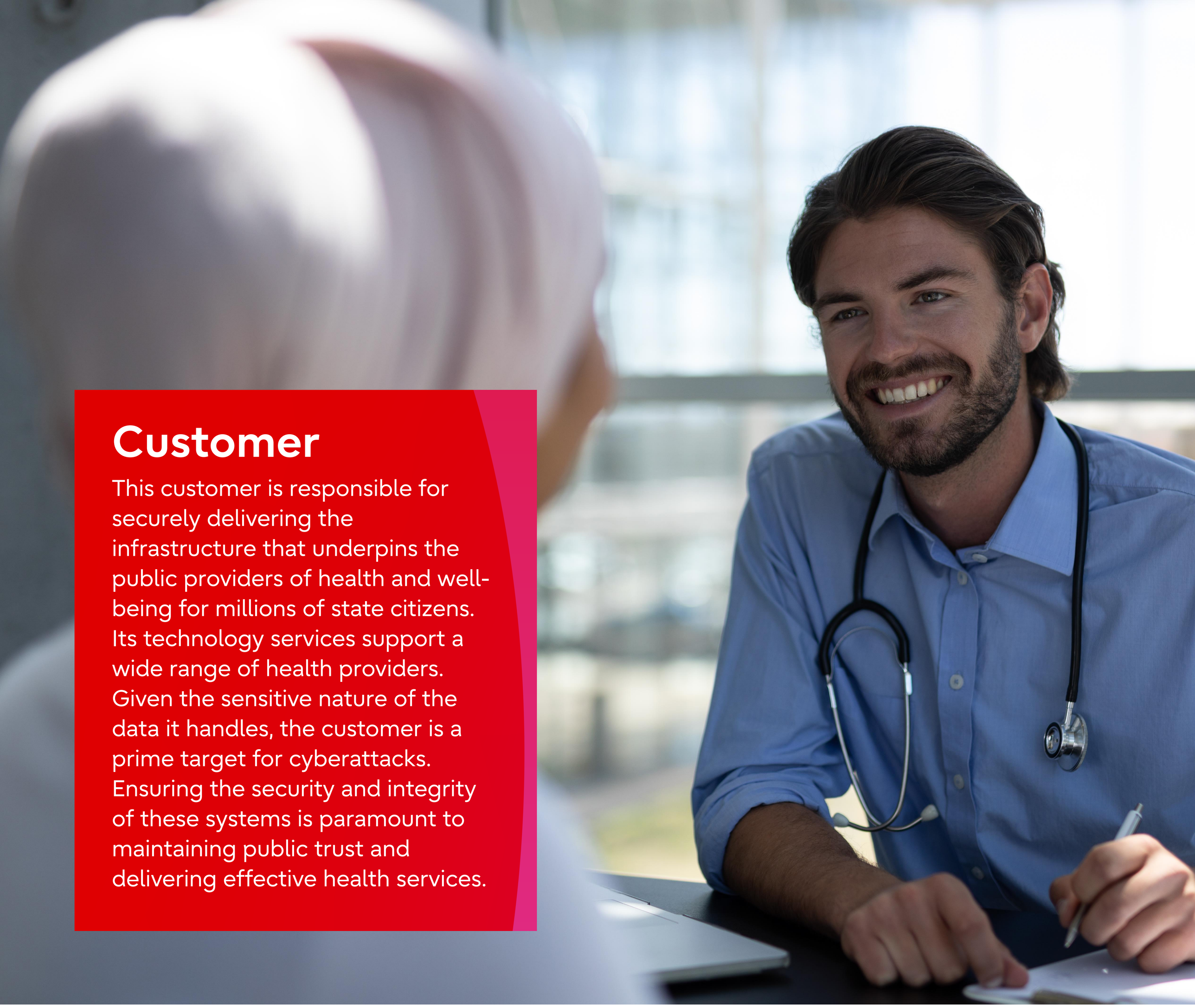
FUJITSU

Australian Government Health Agency

Cybersecurity SIEM

In an era where cyber threats are becoming increasingly sophisticated, this Public Health customer recognised the need to enhance its cybersecurity infrastructure. The customer's existing Security Information and Event Management (SIEM) system was lacking in functionality and no longer capable of effectively managing the growing volume and complexity of cyber threats. The customer successfully replaced its outdated SIEM system with a cutting-edge solution that leverages artificial intelligence and has the capacity to integrate feeds from the Australian Signals Directorate (ASD) Australian Cyber Security Centre to better secure Australian health services.



Customer

This customer is responsible for securely delivering the infrastructure that underpins the public providers of health and well-being for millions of state citizens. Its technology services support a wide range of health providers. Given the sensitive nature of the data it handles, the customer is a prime target for cyberattacks. Ensuring the security and integrity of these systems is paramount to maintaining public trust and delivering effective health services.

Challenge

Situation

The customer's existing SIEM system was struggling to keep up with the evolving cyber threat landscape. The system was outdated, lacked advanced threat detection capabilities and was unable to process the significant amounts of data generated by the customer's IT infrastructure. These factors increased the risk of vulnerability to cyberattacks, data breaches and other security incidents. The incumbent system could not take alert feeds from the Cyber Threat Intelligence Service (CTIS). Furthermore, monitoring all the alerts was manual and required a costly team of security specialists to constantly monitor detection.

Task

The primary task was to replace the aging SIEM system with a more advanced solution that could provide real-time threat detection, automated response capabilities and comprehensive security monitoring. The new system needed to be scalable, capable of handling large volumes of data and able to integrate with external threat intelligence sources, such as those provided by the ASD. The enhanced 24/7 detection capability would be closely interfaced with the cyber threat response capability from the Fujitsu Cyber Security Operations Centre (CSOC) so that detection and protection were designed to be seamless.

Solution

The customer embarked on a comprehensive project to replace its SIEM system.
The project involved several key steps:

1. **Assessment and Planning**
   Fujitsu conducted a thorough assessment of the existing SIEM system and identified the specific requirements for the new solution. This included the need for AI-driven threat detection, real-time monitoring and integration with ASD feeds.

2. **Vendor Selection**
   After evaluating several vendors, Fujitsu selected a leading cybersecurity provider known for its advanced AI capabilities and robust SIEM solutions. The chosen vendor's system was designed to leverage machine learning algorithms to detect and respond to threats in real-time. It made a good fit with the customer’s enterprise architecture.

3. **Implementation**
   The implementation phase involved deploying the new SIEM system across the customer's IT infrastructure. This included configuring the system to receive and process data from multiple sources, including web traffic, network devices, servers, storage and applications. The system was planned to integrate with ASD's threat intelligence feeds (on the roadmap for the next budget cycle) to enhance its ability to detect and respond to emerging threats.

   The Fujitsu and customer teams worked closely together to manage the Risks, Assumptions, Issues and Dependencies log and ensure there was a seamless transition from the old SIEM to the new SIEM. The continual focus on preventing risks to health providers from manifesting meant that the customer elected to slow down the project timeline. While this caused slight delay, it gave the teams more confidence to check in with each other and validate that the new system delivered the full scope and expected performance.

4. **Training and Support**
   To ensure the successful adoption of the new system, Fujitsu provided comprehensive training to the customer’s IT and security staff. This included hands-on training sessions, workshops and ongoing support from the vendor.

5. **Testing and Optimisation**
   Before fully transitioning to the new system, Fujitsu conducted rigorous testing to ensure its effectiveness. This involved simulating various cyberattack scenarios to evaluate the system's performance and making necessary adjustments to optimise its capabilities.

Outcome

Result

The replacement of the aging SIEM system with a new AI-driven solution has yielded significant benefits for the customer:

1. **Enhanced Threat Detection:** The new system's AI capabilities enabled it to detect and respond **Enhanced Threat Detection:** The new system's AI capabilities which are scheduled to be implemented will help optimise detection and response to threats in real-time, significantly reducing the risk of data breaches and other security incidents. While still in the planning phase at the time of writing, the possibility of integration with ASD's threat intelligence feeds would provide specific data on malicious actors attempting to infiltrate systems in real time, further enhancing effectiveness.
2. **Improved Efficiency:** The automation of routine security tasks, such as log analysis and incident response, have freed up the customer's IT and security staff to focus on more strategic activities. The result is improved overall efficiency and better allocation of scarce, specialised customer team members.
3. **Scalability:** The new SIEM system has been designed to scale with the customer's needs, ensuring it will handle the growing volume of data generated by hybrid and multi-cloud infrastructure. This scalability is crucial for maintaining effective security monitoring as the customer's operations expand in the future.
4. **Increased Resilience:** By incorporating advanced AI and planning to integrate with ASD's threat intelligence in the future, the customer significantly improved its cyber resilience. The new system provides robust defence against known and emerging threats, helping to safeguard sensitive commercial, technical, personal and health data while maintaining public trust.

The customer's successful replacement of its aging SIEM system with a modern, AI-driven solution demonstrates the importance of staying ahead of the evolving cyber threat landscape. By integrating advanced technologies and a roadmap for external threat intelligence, the customer has significantly enhanced its ability to protect the sensitive data it holds and ensure the security of its critical operations.

Contact

www.fujitsu.com/au
info@au.fujitsu.com
+61 2 9776 4555