INPHYSEC
a Fujitsu company

Securing public confidence in Health data

Security Information & Event Management (SIEM) and Security Operations Centre (SOC).

INPHYSEC, a Fujitsu company, was awarded the SIEM service to detect malicious activity in a public facing, high threat, cyber environment following an open tender. Subsequently a SOC was created to provide end to end security managed services protecting 5,000 end points. The SIEM and SOC services have been delivered successfully for over 2 years.

Around the world, public health systems are increasingly a target for malicious actors and frequently become casualties of both malware and ransomware attacks. A large government agency recognised these risks and went to market for a SOC and SIEM service. The brief was for services that would supplement the in-house security team and would provide detection and alerting for security events.

The requirements were to provide security monitoring of legacy systems, server and desktop systems, networking infrastructure, and multicloud services including AWS and Azure environments.

Challenges

The technical environment of Health, Aged Care and Social Care systems was extraordinarily complex, compounded by the continual introduction of new critical systems in various stages of development or deployment. This meant the work effort could not be sized or estimated in any rapid fashion, so timelines and resourcing remained uncertain. This meant that delivering to a previously drafted business case and budget became challenging.

These operational issues were underpinned by a significant threat because all health and human services and the systems they operate are in a sector that is frequently targeted by malicious attackers. Orchestrated attacks from nation states and organised crime are now business as usual. INPHYSEC was able to meet the detection and alerting requirements while also gently challenging priorities and proposing additional requirements to improve prevention and response capabilities.

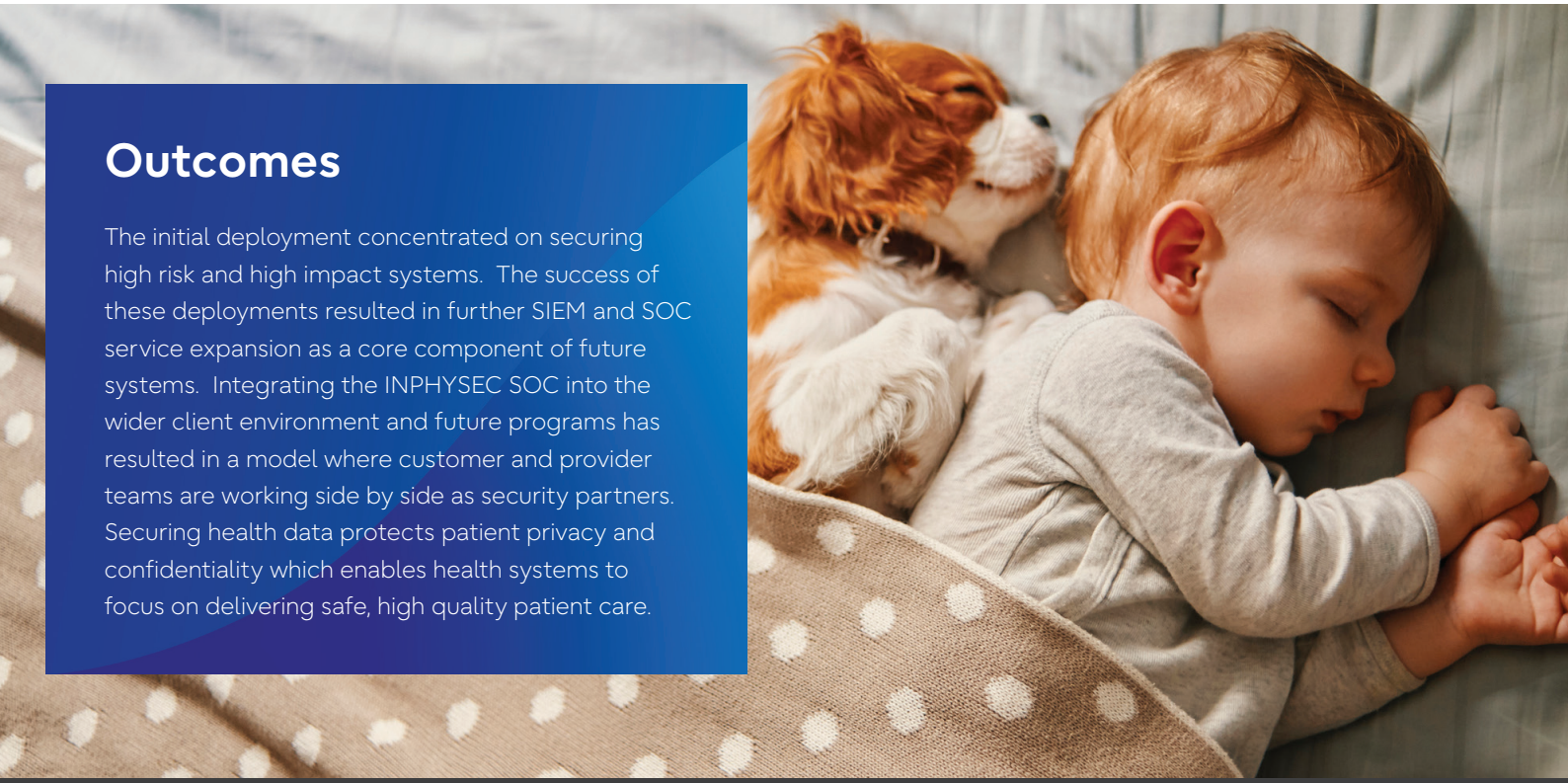
A stand-alone SIEM provides visibility, but it does not provide a mechanism for prevention or response. Once a problem is identified, the system needs to rapidly trigger the right response, this required additional capacity over the initial specification. While the government agency valued this, it presented a challenge to provide these additional capabilities within budget and within the tight timeframe.

Solution

The INPHYSEC solution was a combination of two systems. The tendered SIEM service, which provides visibility across a very wide set of data sources enabling detection and alerting for these sources and a Protect SOC system built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks including malware. The combined solution provided both visibility and crucially the ability to prevent and respond to security issues.

The government agency environment was complex – to give context, INPHYSEC processes 500,000 events in a 3-hour window or over 65 million events over a week. The team applied data science techniques to this data to identify anomalies. Through this analysis they highlighted priority issues to the government agency, including early identification of simple misconfigurations that could have led to security events.

Solution deployment was segmented into stages. Each stage was project managed with clear, agreed deliverables planned to meet the client's prioritised requirements and risk profile. The initial deployment was against a tight timeframe because the existing SOC contract was coming to an end and the customer was intending to replace its incumbent service provider.



Outcomes

The initial deployment concentrated on securing high risk and high impact systems. The success of these deployments resulted in further SIEM and SOC service expansion as a core component of future systems. Integrating the INPHYSEC SOC into the wider client environment and future programs has resulted in a model where customer and provider teams are working side by side as security partners. Securing health data protects patient privacy and confidentiality which enables health systems to focus on delivering safe, high quality patient care.

INPHYSEC
a Fujitsu company

Contact us today

security@inphysec.co.nz 0800 463 673 (NZ) / +64 27 554 9243 www.inphysecsecurity.com