Case study

HORIZON POWER
energy for life

Critical information and infrastructure is protected with the implementation of a powerful Security Information and Event Management solution at Horizon Power.

THE CLIENT

Horizon Power is a State Government-owned, commercially-focused corporation that provides high quality, safe and reliable power to about 100,000 residents and 10,000 businesses, including major industry, across regional and remote Western Australia.

The organisation is responsible for generating, procuring, distributing and retailing electricity supplies. Its customers range from people living in remote, isolated communities with less than 100 people, to residents and small businesses in busy regional towns, to major mining companies in the resource-rich Pilbara region.

THE BUSINESS CHALLENGE

With the threat of security attacks happening in a matter of seconds, Horizon Power was keen to reduce the time taken to detect and respond to security incidents by implementing a Security Information and Event Management (SIEM) solution.

“Implementing the right SIEM solution would allow us to reduce the overall incident cost to our organisation,” said Jeff Campbell, IT Security Risk and Governance Specialist at Horizon Power. “It was important for us to review all SIEM solutions and select the most suitable option for our critical infrastructure environment.”

THE SOLUTION

Asterisk Information Security was selected to implement a SIEM solution and provide consulting services. Asterisk recommended the McAfee Security Information and Event Management (SIEM) solution, known as Enterprise Security Manager (ESM), as a best fit for Horizon Power’s operating environment.

ESM provides high-performance SIEM solutions that protect critical information and infrastructure. ESM reduces risk exposure and increases network and information availability by removing the scalability and performance limitations of security information management.

The ESM solution would correlate and remediate threats in minutes, instead of hours, which would allow Horizon Power to quickly mitigate risks to their information and infrastructure.

Asterisk applied the following methodology to implement the McAfee SIEM ESM solution:

1. Project kick off
2. Familiarisation
3. Planning and design
4. Undertake technical design
5. Document SIEM design and conduct a review with Horizon Power
6. Technical implementation
7. Configure and test
8. Final implementation
9. Post implementation
10. Ongoing Security Operations services

“Our experience has shown that it is important to consider people, process and technology aspects when undertaking a SIEM project,” said Steve Schupp, Principal Security Consultant at Asterisk. “Our approach ensures that customers can quickly obtain results from a SIEM deployment and build a process which embeds the technology into their security operations.”

THE BENEFITS

Asterisk successfully deployed the McAfee SIEM ESM solution and continues to provide Horizon Power with Security Analyst resources to manage and implement the organisation’s evolving requirements for security monitoring.

Horizon Power now has the ability to:

- Centralise security event logging from a variety of sources
- Identify incidents based on priority to allow a targeted response
- Generate reports for investigation, regulatory compliance and security management metrics
- Replay previously collected event data for post threat investigation

Immediate benefits have been realised through the detection and notification of unknown and malicious activities occurring in the operating environment, while at the same time, addressing audit and compliance requirements.