

Automating Security for Australia's Energy Sector

The Energy Behind the Firewall

An Australian Energy Provider partnered with Krish to deploy Microsoft Sentinel. This implementation consolidated security monitoring across on-premises and Azure cloud environments, enabling centralized visibility, threat detection, and automated incident response compliant with local energy sector mandates.

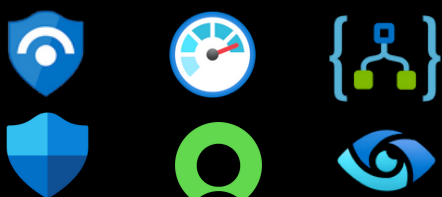
CLIENT BACKGROUND

The client is a leading Energy Provider based in Australia, delivering power and energy services across industrial, commercial, and residential sectors. They operate a distributed IT infrastructure spanning on-premises and Azure cloud environments.

BUSINESS VALUE

- **Unlocked Unified Visibility:** Gained complete, real-time visibility across the entire hybrid environment from a single console.
- **Cut Response Times:** Slashed incident triage and resolution times through intelligent SOAR automation.
- **Eliminated 45% of False Alerts:** Fine-tuned analytics significantly reduced alert noise, letting the SOC focus on genuine threats.
- **Ensured Regulatory Adherence:** Streamlined compliance with stringent Australian energy sector mandates through comprehensive logging and reporting.
- **Boosted SOC Productivity:** Empowered the security team with enriched alerts, automated workflows, and centralized dashboards.

TECHNOLOGIES



CONCLUSION

With Microsoft Sentinel, the provider gained centralized visibility, faster threat detection, and automated response, easing compliance challenges while strengthening overall security operations.

PROBLEMS

- **Fragmented Security Environment:** Critical security data was isolated across numerous disparate on-prem and cloud tools.
- **Lack of Integrated SIEM/SOAR:** Missing a unified platform for effective security information correlation and automated response orchestration.
- **Crippling Manual Workflows:** Security teams were bogged down by time-intensive manual processes for investigation and remediation.
- **Complex Compliance Hurdles:** Demonstrating adherence to specific energy sector regulations was inefficient and resource-intensive.

SOLUTIONS

- **Centralized Security Ecosystem:** Critical security data was isolated across numerous disparate on-prem and cloud tools.
- **Lack of Integrated SIEM/SOAR:** Missing a unified platform for effective security information correlation and automated response orchestration.
- **Crippling Manual Workflows:** Security teams were bogged down by time-intensive manual processes for investigation and remediation.
- **Complex Compliance Hurdles:** Demonstrating adherence to specific energy sector regulations was inefficient and resource-intensive.