CASE STUDY Unified security operations | MICROSOFT SENTINEL | ENERGY

Sentinel SIEM for an energy provider with 60% fewer false positives.

A large Australian energy provider had security logs spread across on-premises servers and Azure in several locations. We brought them into **one Microsoft Sentinel view** and **automated threat detection and response**.

CLIENT: ONE OF AUSTRALIA'S TOP ENERGY SUPPLIERS

ALERT NOISE
60%
Fewer false positives after rule tuning

DETECTION
256
Custom and built-in analytics rules in Sentinel

DEVICES
40+
Ubiquiti network devices connected to Sentinel

DELIVERY
4
Phases, from log ingestion to dashboards and governance

CLIENT BACKGROUND

The client is **one of Australia's top energy suppliers**, serving commercial, industrial and residential customers with a nationwide operations footprint.

Its IT ran across on-premises systems and Microsoft Azure environments at several sites. Security visibility was limited, which made threats hard to spot in time and slowed incident response.

BEFORE
Scattered security logs
On-premises devices and cloud, no SIEM or SOAR

→

AFTER
One Microsoft Sentinel view
Central detection, automated response, dashboards

THE CHALLENGE

Lack of security visibility
Logs spread across on-premises devices and cloud platforms slowed detection.

Manual alert triage
Teams investigated alerts by hand, which raised response times.

Microsoft tools not integrated
Native Microsoft security data sources were not feeding coordinated monitoring.

No central SIEM and SOAR
Log correlation and automated response were limited without a SIEM with SOAR.

Too many false positives
Analysts were overwhelmed by noisy alerts that hid real threats.

Heavy compliance reporting
Australian energy sector security mandates needed extensive manual reporting.

WHAT WE DELIVERED

01 **Unified log ingestion** — LOG ANALYTICS
40+ Ubiquiti devices, servers, virtualization and Microsoft cloud logs in one workspace.

02 **Analytics rules and detection engineering** — 256 RULES
256 rules detect identity abuse, network and endpoint threats, and data theft.

03 **Noise reduction and precision tuning** — KQL
KQL tuning of detection thresholds cut false positives and sharpened alerts.

04 **Automated response with SOAR** — PLAYBOOKS
Playbooks enrich alerts, notify teams, open ServiceNow tickets and isolate risky devices.

05 **Governance and behaviour analytics** — RBAC · UEBA
RBAC, retention, long-term archiving and UEBA to support compliance and catch insider risk.

06 **Dashboards for security and leadership** — WORKBOOKS
Sentinel Workbooks show threat trends, device behaviour and risk by site and business unit.

RESULTS

60%
Fewer false positives
Optimized analytics rules lowered false positives by 60%.

Faster incident response
Automation reduced manual triage and cut response and resolution times.

256
Analytics rules live
Custom and built-in rules cover identity, network, endpoint and data theft.

Unified security visibility
Central SIEM dashboards give real-time threat visibility across environments.

Audit ready. Logging and retention policies support continuous compliance with Australian energy regulations.

TECHNOLOGIES USED

Microsoft Sentinel · Log Analytics · KQL · Microsoft 365 Defender · ServiceNow

FINAL PERSPECTIVE

Microsoft Sentinel brought the client's **security operations into one automated model**: faster threat response, fewer false alarms and simpler compliance reporting.

Considering Microsoft Sentinel?

Talk to a Krish security engineer.

krishservicesgroup.com/contact-us
+1 (813) 494-4015

Read this case study online: krishservicesgroup.com/case-study/microsoft-sentinel-for-an-australian-energy-provider/