excite CYBER

LOG SOURCES

- Applications
- Network Security
- Cloud Security
- Data Security
- Identity & Access Management (IAM)
- Zero Trust
- Endpoint

DATA INGESTION & OPTIMISATION

Data ETL
Extraction & transformation of data.

LOG & ALERT AGGREGATION & CORRELATION

Alert Enrichment
Integrations with common third-party data sources.

SOAR
Central aggregation of alerts for effective triage. Automated response actions.

Cloud-Native SIEM
Data aggregation, correlation, and storage.

Detection Rules
Alerting mechanisms continuously developed.

Threat Intelligence
Continuous threat intelligence feeds.

SECURITY OPERATIONS

Security Operations Centre
Australian SOC in Sydney & Hobart.

Triage & Analysis
Analysing alerts and log data from multiple feeds to ascertain if an alert is a True or False Positive.

Threat Hunting
Conducting proactive scans of the environment to identify IOCs.

Remediation
Deliver containment actions or provide guidance on remediation steps to remove threats.

SERVICE DELIVERY

Real-Time Reporting
Centralised view of security operations.

ITSM
Tracking of notable alerts and ongoing initiatives.

Service Management
Customer success & advisory.