Managed Detection and Response Service (MDR)

Security Operations Centre (SOC) Services

The Managed Detection and Response (MDR) service is a security monitoring service that monitors log feeds from across an agency's network and generates alerts for any potential incident on a near-real time basis.

MDR is delivered through a Brisbane based Security Operations Centre (SOC). The primary function of the SOC is to detect and respond to all types of cyber-attacks from zero-day exploits through to privilege escalation, crypto-mining and more.

Benefits

- Managed within Queensland Government facilities
- Increased visibility for agencies to better manage security risks
- Whole-of-government situational awareness
- Forward defense capability
- Intergrated with other government-wide services (e.g. QGCSOC)
- Managed by security specialists with extensive experience
- Locally driven threat intelligence complementaed by external feeds
- Strong third-party relationships

Prerequisites

Use of whole-of-government Internet gateway service, QGISP.

Features

Monitoring and detection of agreed monitored behaviour policies.

- 24 x 7 service
- 24 x 7 event/incident monitoring
- 24 x 7 human-in-the-loop security alerting function, manned during business hours

Variants

- Customised onboarding process
- Customised MDR service
- Customised security monitoring use case development and tuning
- Customised dashboards

Metrics

Availability: 24 x 7 - 99.99%

Alert notification: 90% within 30mins by email

Monthly service report: 90% within agreed week of the month

Average time to introduce new detection measure for major global security threats: 90% <=72 hours

Reporting

Reporting is provided as a dashboard for users to view information.

Additional and related services

- QG Internet Service Provider (QGISP)
- QG ISP Security Services
- Managed QG services (e.g. QCloud)

Options

- Brand impersonation monitoring and protection
- Remote incident response
- Brand impersonation intelligence
- Threat hunting professional services
- Customised security monitoring use case development and tuning
- Customised dashboards

Ordering

Please contact your CITEC representative

07 3222 2555 service@citec.com.au