# G-Cloud 15
# Service Definition
# For
# Managed XDR Powered by Barracuda

Delivering IT for future-thinking organisations

enquiries@quadris.com | 0161 537 4980 |www.quadris.com

# 1 Service description

Managed XDR Powered by Barracuda provides end-to-end protection across the full cyber attack lifecycle, from initial access through to lateral movement, privilege escalation and data exfiltration.

Telemetry from integrated security controls is continuously collected, normalised and correlated using an open XDR architecture. Detection logic aligned to the MITRE ATT&CK framework identifies genuine threats with high confidence, while automated playbooks and SOC-led response actions are used to rapidly contain and remediate incidents.

The service reduces alert fatigue, removes the need for in-house 24/7 monitoring and improves operational efficiency by presenting all security activity through a single, unified management interface.

# 2 Who this service is for

This service is suitable for public sector organisations that:

- Require continuous, specialist-led threat monitoring and response
- Have limited internal security resources or coverage gaps
- Need improved visibility across multiple security domains
- Want to meet evolving regulatory and assurance requirements
- Prefer a managed service model over in-house SOC operations

# 3 Service features

- 24/7/365 SOC-led monitoring and response
- AI-driven threat detection and analytics
- Automated Threat Response (ATR) playbooks
- MITRE ATT&CK-aligned detection rules
- Open XDR integrations across existing tools
- Single-pane-of-glass security dashboard
- Enterprise-grade threat intelligence
- Highly scalable cloud architecture

## 4 Service Features

Barracuda Managed XDR can include the following monitored and managed capabilities, depending on buyer requirements:

- **XDR Endpoint Security** – Detection and response for Windows, macOS and Linux endpoints
- **XDR Email Security** – Monitoring and response for phishing, malware and business email compromise
- **XDR Cloud Security** – Detection of anomalous access, privilege misuse and cloud account compromise
- **XDR Network Security** – Identification of command-and-control traffic, data exfiltration and reconnaissance
- **XDR Server Security** – Advanced detection of server-side attacks such as privilege escalation and brute force
- **Managed Vulnerability Security** – Regular vulnerability scanning with contextual reporting and prioritisation

## 5 Service Benefits

- Reduced likelihood and impact of cyber security incidents
- Faster detection and response times
- Lower operational overhead and alert fatigue
- Access to specialist SOC expertise without additional staffing
- Improved cyber resilience and assurance
- Support for audit and compliance activities

## 6 Implementation and onboarding

Quadris supports onboarding through a structured, low-risk approach that includes:

- Service scoping and requirements confirmation
- Secure integration of supported data sources
- Configuration of detection rules and response playbooks
- Validation testing and service activation
- Knowledge transfer (where applicable)

## 7 Security and compliance

The service supports common public sector security and compliance requirements by providing:

- Continuous monitoring and centralised logging
- Incident investigation and reporting
- Audit-ready evidence and reporting outputs
- Support for environments requiring SIEM, SOAR and vulnerability management capabilities

# 8 Service constraints

- Functionality is dependent on supported integrations and data sources
- Internet connectivity is required
- Automated response actions operate within buyer-approved permissions and policies

# 9 Pricing

The service is priced on a subscription basis, dependent on:

- Number and type of protected assets
- Enabled service components
- Selected Quadris support model

Pricing details are published separately in the Digital Marketplace pricing document.

# 10 Quadris support model

Quadris provides two support options to align with buyer operational preferences.

## 10.1 Base Support Service – Assisted Self-Managed Operation

Quadris provides optional support services for Barracuda XDR to assist organisations in the effective operation, administration, and ongoing use of the service. These support services are designed to meet differing operational models within the public sector, from self-managed environments requiring limited assistance to fully managed services delivered on behalf of the buyer.

Quadris support services are offered in addition to the Barracuda XDR software subscription.

### 10.1.1 Service description

Under this model, the buyer retains responsibility for operating Barracuda XDR, with Quadris providing enablement, guidance, and escalation support. This option is suitable for organisations with in-house security or infrastructure teams who wish to respond and investigate their own alerts and investigations, while accessing specialist expertise when required.

### 10.1.2 Inclusions

- Initial configuration guidance
- Administrator training
- Named technical contact
- Advisory support for incident interpretation
- Escalation to Barracuda where required

### 10.1.3 Buyer responsibilities

- Day-to-day monitoring and response decisions
- Execution and approval of remediation actions
- Internal incident management and reporting
- Ongoing service administration

## 10.2 Managed Support Service – Quadris-Operated Service

### 10.2.1 Service description

Under this model, Quadris operates Barracuda Managed XDR and coordinating directly with Barracuda's SOC as a Service on behalf of the buyer. Quadris assumes responsibility for configuration, monitoring, management, and incident response activities, providing a managed security service aligned to public sector operational requirements. This option is suitable for organisations seeking to reduce operational overhead or lacking in-house SOC expertise.

### 10.2.2 Inclusions

- Continuous monitoring and incident handling
- Execution of agreed response playbooks
- Incident reporting and remediation coordination
- Service optimisation and review
- Vendor and SOC liaison

### 10.2.3 Buyer responsibilities

- Define escalation thresholds and risk appetite
- Approve high-impact remediation actions
- Maintain internal governance and compliance oversight

## 10.3 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying Barracuda XDR subscription.
- All services are delivered remotely unless otherwise agreed.

## 10.4 Support Service Responsibility Matrix (RACI)

| Activity | Base Support Service (Assisted Self-Managed) | Managed Support Service (Quadris-Operated) |
|---|---|---|
| Service onboarding | Quadris (R) / Buyer (A) | Quadris (R) |
| Platform configuration and tuning | Buyer (R) / Quadris (C) | Quadris (R) |
| 24/7 monitoring | Barracuda SOC (R) | Barracuda SOC (R) |
| Threat detection | Barracuda SOC (R) | Barracuda SOC (R) |
| Incident investigation | Buyer (R) | Quadris (R) / Buyer (I) |
| Automated response execution | Buyer (R) | Quadris (R) / Buyer (C) |
| Incident reporting | Buyer (R) | Quadris (R) |
| Service optimisation | Buyer (R) | Quadris (R) / Buyer (C) |
| Escalation management | Buyer (R) | Quadris (R) |

R = Responsible, A = Accountable, C = Consulted, I = Informed