G-Cloud 15 Lot3 Service Definition for Vulnerability Scanning Managed Service

Delivering IT for future-thinking organisations

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

1 Introduction

Vulnerability Scanning as a Service (VSaaS) is a cloud-supported security service designed to help organisations identify, assess, and manage security vulnerabilities across their IT environments. The service provides continuous, automated vulnerability scanning and reporting using the Qualys cloud-based vulnerability management platform.

The service is delivered as a fully managed or assisted service and is suitable for UK public sector organisations requiring regular vulnerability visibility, prioritised remediation guidance, and support for security assurance and compliance activities. Scanning is non-intrusive and designed to operate without disruption to business operations.

2 Service Scope

The service provides ongoing vulnerability scanning, analysis, reporting, and remediation guidance for supported assets. Vulnerability identification is performed independently of native platform tools, ensuring consistent visibility across on-premises, cloud, and hybrid environments.

3 Supported Environments

- On-premises infrastructure
- Public and private cloud environments
- Hybrid environments
- Network devices, servers, and endpoints
- Internet-facing and cloud-hosted websites
- Microsoft 365 tenants

4 Functional Capabilities

4.1 Vulnerability Scanning

- Daily automated vulnerability scanning of all network-connected assets
- Non-intrusive scanning designed to avoid service disruption
- Detection of:
- Missing security patches
- Misconfigurations
- Default or weak credentials
- Exposed services and ports
- Validation of findings against the Qualys continuously updated vulnerability database

4.2 Vulnerability Intelligence

- Use of over 157,000 Qualys detection plugins
- Automatic near real-time updates to vulnerability signatures
- Severity-based categorisation to support risk prioritisation

5 Reporting and Visibility

- Self-service, interactive dashboards providing near real-time vulnerability status
- Access to historical scan results and trend analysis
- Centralised “single pane of glass” interface via the Quadris EyeQ platform
- Export of vulnerability and asset data in CSV format
- Clear, actionable remediation guidance aligned to each identified vulnerability

6 Service Benefits

- Regular automated scanning supports continuous improvement of security posture
- Non-disruptive scanning ensures no impact to end users or service availability
- Near real-time reporting suitable for regulated and high-compliance environments
- Supports Cyber Essentials Plus and other security audit and assurance activities
- Weekly remediation guidance supports timely resolution of vulnerabilities
- Severity-based prioritisation helps focus effort on the highest risks
- Access to experienced security engineers for remediation guidance
- Increased assurance for operational and executive stakeholders

7 Service Management

7.1 Management Interface

- Secure, web-based dashboards accessed via the Quadris EyeQ platform
- Dynamically updating views of vulnerability status
- Role-based access to dashboards and reports

7.2 Monitoring and Oversight

- Continuous monitoring of scan execution and results
- Identification of scan failures or anomalies
- Ongoing review of vulnerability trends and risk exposure

8 Security

8.1 Data Security

- Vulnerability data handled in accordance with Qualys platform security controls
- Secure transmission of scan data using encrypted communications
- Logical separation of customer data within the platform

8.2 Platform Assurance

- Service delivered using the Qualys cloud-based vulnerability management platform
- Vulnerability intelligence updated continuously to address emerging threats

9 Onboarding and Implementation

9.1 Onboarding

- Initial assessment of customer environment
- Identification and validation of assets to be scanned
- Configuration of scanning scope and schedules
- Dashboard setup and access provisioning

9.2 Configuration

- Selection of assets, IP addresses, domains, and cloud services
- Scheduling of daily automated scans
- Configuration of reporting and access controls
- Deployment is designed to be rapid and minimally disruptive.

10 Quadris Support Services

Quadris provides optional support services for Vulnerability Scanning as a Service (Qualys) to assist organisations in the effective operation, interpretation, and ongoing use of the service. These support services are designed to align with differing operational models within the public sector, ranging from assisted self-managed use to a fully managed service operated by Quadris.

Quadris support services are offered in addition to the Vulnerability Scanning as a Service subscription.

10.1 Base Support Service – Assisted Self-Managed Operation

The Base Support Service is intended for organisations that wish to retain operational responsibility for vulnerability scanning activities while receiving structured onboarding, guidance, and access to experienced Quadris security engineers.

Under this model, the buyer performs day-to-day vulnerability management activities, with Quadris providing advisory support, best-practice guidance, and escalation assistance where required.

10.2 Inclusions

- Initial service onboarding support, including:
    - Validation of scanning scope and asset eligibility
    - Review of scan configuration and scheduling
    - Verification of dashboard access and reporting visibility

- Administrator guidance covering:

    - Vulnerability scan interpretation
    - Severity categorisation and risk prioritisation
    - Use of dashboards and historical scan data
    - Exporting reports and evidence for audits

- Advisory support for:
    - Vulnerability remediation planning
    - Compliance and assurance activities (e.g. Cyber Essentials Plus)
    - Interpreting alerts, trends, and recurring vulnerabilities
- Liaison with Qualys technical support where required

10.3 Buyer Responsibilities

- Day-to-day operation of vulnerability scanning
- Review and interpretation of scan results
- Prioritisation and execution of remediation activities
- Maintenance of asset inventories and scan scope
- Ensuring authority to scan submitted IP addresses, domains, and assets
- Compliance with internal security, legal, and governance requirements

10.4 Intended Use

This service is suitable for organisations with internal IT or security capability that wish to retain control of vulnerability management while reducing risk through expert guidance and structured support.

10.5 Managed Support Service – Quadris-Operated Service

The Managed Support Service is intended for organisations that require Quadris to operate Vulnerability Scanning as a Service on their behalf. Quadris assumes responsibility for the configuration, execution, monitoring, and reporting of vulnerability scans in accordance with agreed policies and procedures.

The buyer retains overall accountability for risk ownership and remediation decisions but does not perform routine operational scanning tasks.

10.6 Inclusions

- Full service onboarding and configuration
- Ongoing management of vulnerability scanning, including:
    - Asset scope and scan schedule management
    - Validation of asset ownership and scan authority
    - Continuous monitoring of scan execution and results
    - Identification and escalation of critical vulnerabilities
- Proactive management of:
    - Scan failures or coverage gaps
    - Changes in asset exposure or risk profile
- Execution of
    - Regular vulnerability reporting
    - Remediation advisory reports and summaries
- Support for:
    - Audit preparation and compliance evidence
    - Security investigations and assurance activities
- Liaison with Qualys technical support for incident resolution

10.7 Buyer Responsibilities

- Defining vulnerability management policies and risk appetite
- Authorising remediation priorities and actions
- Implementing remediation activities within their environment
- Maintaining ownership of scanned assets
- Ensuring organisational compliance with data protection and legal obligations

10.8 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying Vulnerability Scanning as a Service subscription
- Quadris does not apply patches or configuration changes unless explicitly agreed

- Quadris does not provide general infrastructure or endpoint administration
- All services are delivered remotely unless otherwise agreed

10.9 Support Service Responsibility Matrix (RACI)

Key:
R – Responsible (performs the activity)
A – Accountable (owns the outcome / approval)
C – Consulted (provides guidance or input)
I – Informed (kept informed)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Service onboarding and initial configuration	R (Quadris) / A (Buyer)	R (Quadris) / A (Buyer)
Asset scope definition and validation	R (Buyer) / C (Quadris)	R (Quadris) / A (Buyer)
Scan schedule configuration	R (Buyer) / C (Quadris)	R (Quadris)
Ongoing scan execution	R (Buyer)	R (Quadris)
Scan monitoring and alert review	R (Buyer)	R (Quadris)
Scan failure investigation	R (Buyer) / C (Quadris)	R (Quadris)
Vulnerability analysis and prioritisation	R (Buyer) / C (Quadris)	R (Quadris) / A (Buyer)
Remediation execution	R (Buyer)	R (Buyer)
Remediation advisory guidance	C (Quadris)	R (Quadris)
Reporting and dashboard management	R (Buyer)	R (Quadris) / I (Buyer)
Audit and compliance support	C (Quadris)	R (Quadris) / A (Buyer)
Liaison with Qualys support	C (Quadris)	R (Quadris)
Legal authority to scan validation	A (Buyer)	A (Buyer)

11 Service Constraints and Dependencies

- The service identifies and reports vulnerabilities but does not automatically remediate them
- Remediation actions remain the responsibility of the buyer unless separately agreed

- The buyer must be able to demonstrate that any external IP addresses, domains, or websites submitted for scanning are owned by, or formally allocated to, their organisation
- The supplier reserves the right to refuse to scan assets where authority to scan cannot be satisfactorily evidenced
- Internet connectivity is required for scan management and reporting
- Service effectiveness is dependent on asset availability and network accessibility

12 Pricing and Licensing Model

Pricing is subscription-based and determined by the number and type of assets covered. The service provides predictable costs and represents a cost-effective alternative to manual vulnerability scanning.

13 Exit Management

- Vulnerability scanning activities cease on service termination
- Access to dashboards and reporting is withdrawn
- Final reports can be provided on request
- Support for planned service exit in line with G-Cloud requirements

14 Intended Users

- Central government departments
- Local authorities
- NHS and healthcare organisations
- Education and research institutions
- Other UK public sector bodies

15 Summary

Vulnerability Scanning as a Service (Qualys) provides a structured, repeatable approach to identifying and managing security vulnerabilities across complex IT environments. The service supports improved security posture, compliance readiness, and operational assurance, aligning with the expectations of a G-Cloud 15 Lot 3: Cloud Support service.