G-Cloud 15 Service Description

Endpoint Security Operations (formerly Vulnerability Management Services - VMaaS)

Cloud21

A Tegria Company

Table of Contents

1. Proposed Services

Our Endpoint Security Operations service is designed around the complex requirements of the NHS and Education. Delivered by our qualified technical and security engineers, the service comes with a reporting snapshot providing full visibility into vulnerabilities across an IT estate and support for NHS security policies like NHS Cyber Alerts (formerly CareCERTs) and Data Security and Protection Toolkit ("DSPT").

Cloud21 can support organisations in the following activities:

- Endpoint Protection management (e.g. on/off-boarding devices, common policy configuration and changes)
- Endpoint health and compliance monitoring and resolution (e.g. agent status, Operating System build versions, Endpoint Protection definitions)
- Application hardening where possible (limited to a pre-defined list of 5 1st and 3rd party applications)
- NHS Cyber Alerts (CareCERT) investigation and recommendation/resolution (limited to High and Medium alerts; resolution limited to Hypervisor Host, Microsoft OS, and a pre-defined list of 1st and 3rd party applications)
- Annual table-top incident scenario testing
- Engaging and logging incidents with 3rd parties where direct resolution is not readily available (e.g. hardware component failures)
- Performing daily checks using existing toolsets (e.g. Sophos Central, Microsoft Defender for Endpoint) to identify existing and emerging threats and issues
- Operational escalations when internal teams cannot solve a problem
- Attend internal IT meetings (including Teams) to determine actions and provide updates

The Service covers Monday to Friday 8am-5pm excluding bank holidays (please ask for pricing for additional cover).

2. Monthly Reporting

Cloud21 provide reports and have virtual meetings monthly, with the relevant stakeholders. This will include metrics from various client solutions but show Endpoint Security compliance figures appropriate to monitoring the posture and exposure of the organisation.

3. Tools

We utilise existing tools in use with the buyer and are able to provide and work with a number of other vendor tools:

4. NHS Cyber Alerts Dashboard (optional)

This service depends on the client having Qualys VMDR as a prerequisite.
MSP version available on request (at cost), but MSP version outputs are via PDF/Email instead of Web portal access.

Cloud21 develop and maintain a Qualys dashboard to aid NHS organisations/providers in understanding compliance with CyberAlerts and supports evidence for DSPT submission.