DATA SHEET

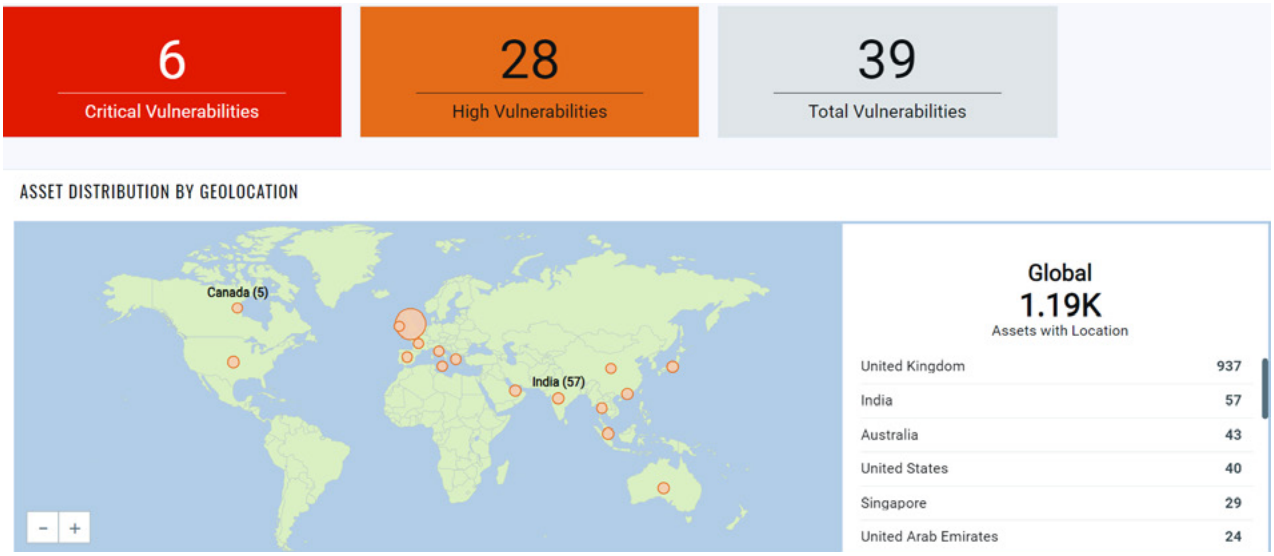
VULNERABILITY ASSESSMENTS

OVERVIEW

Redpalm's Vulnerability Assessment as a Service (VAaaS) leverages Vulnerability Management technology for comprehensive scan audits across internal and external network devices, servers, databases, endpoints, and cloud environments. As a managed service, it eliminates the need for hardware, software, and maintenance, providing detailed reports and actionable remediation advice from our cybersecurity specialists.

The vulnerability scanning tool we use is an approved tool by the National Cyber Security Centre (NCSC) for Cyber Essentials Plus, ensuring it meets high standards of security and reliability.

EXAMPLE DASHBOARD



SCOPE

Our service targets any internal or external system with a reachable IP address or supported OS for the Cloud Agent, providing continuous monitoring. Standard reports focus on vulnerabilities scoring 7.0 or higher on the CVSS v3.1 scale with anything above 7.0 needing to be remediated within 14 days of a patch being released to meet the Cyber Essentials criteria, and includes:

Executive Summary: High-level summary with trends over time.

Detailed Vulnerability Report: Used for understanding vulnerabilities and remediation.

Missing Patches Report: Lists missing patches and their details.

Vulnerabilities Overview Report: High-level overview of detected vulnerabilities.

Top 10 Most Prevalent Vulnerabilities Report: Common vulnerabilities detected.

Top 10 Most Vulnerable Hosts Report: Most vulnerable hosts across the IT estate.

Year-Round Protection While some organisations perform penetration tests once or twice a year, continuous protection is essential to guard against new vulnerabilities that a pen test might not cover. Our VAaaS provides all-year-round monitoring and protection, ensuring your systems are secure at all times.

SEVERITY LEVELS AND ACTIONS

Severity	CVSS v3.1 Score Range	Definition
Critical	9.0 – 10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0 - 8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0 - 6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1 - 3.9	Vulnerabilities are non-exploitable but would reduce an organisation's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

REVIEW MEETINGS

Regular meetings are held to discuss reports and insights, offering an opportunity for consultation with Redpalm experts.

WHY CHOOSE REDPALM

Redpalm offers an ITIL-aligned service desk with decades of IT support experience, certified engineers, adherence to cybersecurity best practices, bespoke support contracts, and a proven track record of excellent IT support and infrastructure projects.

ACCREDITATIONS

ISO 9001, ISO 27001
IASME Cyber Assurance Level 2
ICO Registered
Cyber Essentials PLUS
Cyber Essentials Trusted Partner

CHALLENGES ADDRESSED

Resource Constraints: Managing in-house resources for training, reporting, and data interpretation.
Skill Gaps: Understanding and prioritising vulnerabilities.
Cost Constraints: Budget limitations for tools and expertise.
Prioritisation Issues: Inefficient resource use due to difficulty in risk-based prioritisation.
Patch Management: Keeping systems updated with the latest patches.
Tool Misconfiguration: Ensuring accurate setup and configuration of assessment tools.

BENEFITS OF USING REDPALM

Expertise: Access to highly skilled cybersecurity professionals.
Cost-Effective: Affordable alternative to in-house teams and tools.
Timely & Actionable Reports: Clear reports with actionable recommendations.
Ongoing Support: Continuous monitoring and support for emerging vulnerabilities.
Continuous Improvement: Regular updates to adapt to evolving threats and improve security posture.