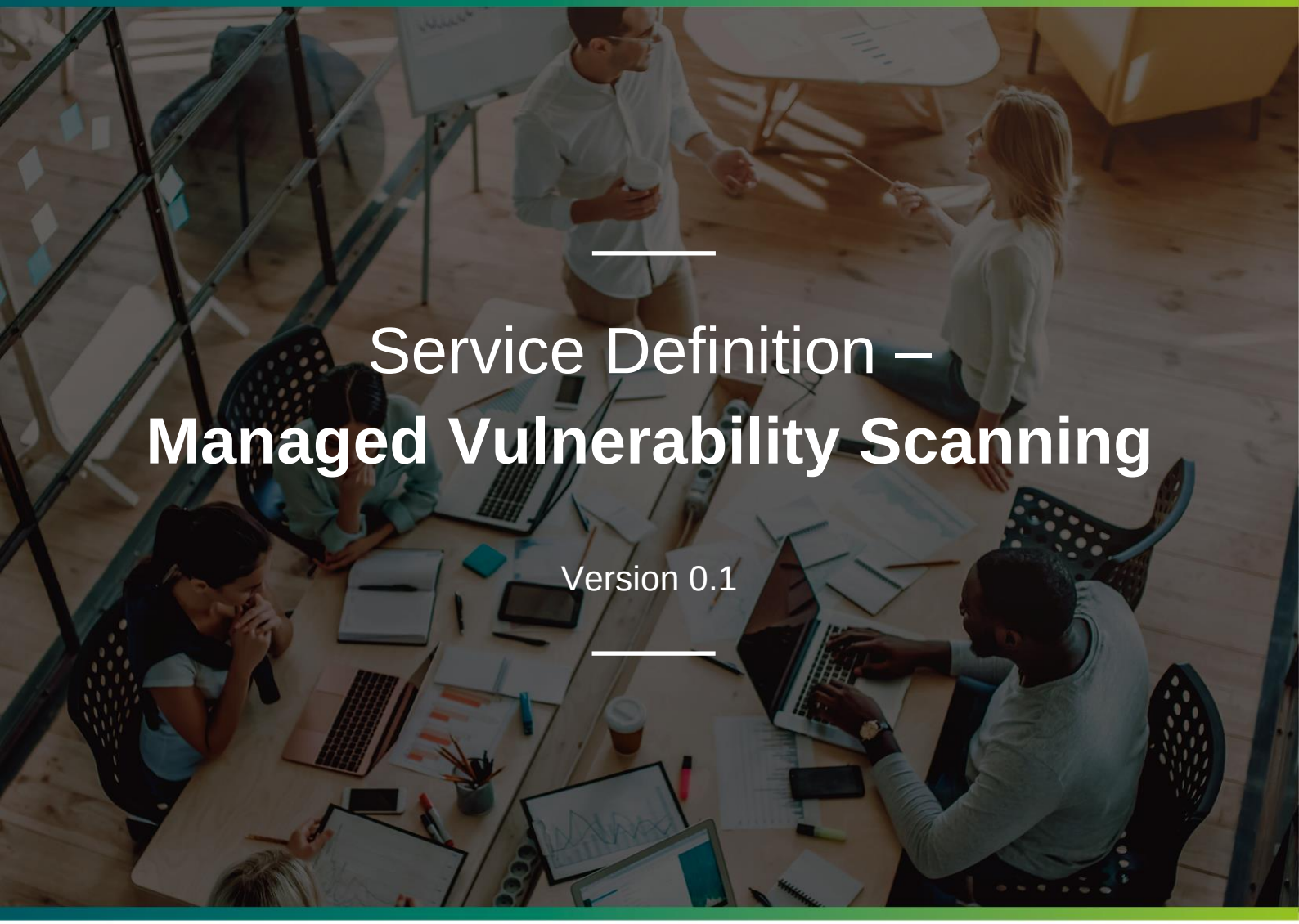

Service Definition –
Managed Vulnerability Scanning

Version 0.1

CREST

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service description

Redcentric Managed Vulnerability Scanning enables organisations to identify, prioritise, and remediate software vulnerabilities affecting their digital infrastructure, applications, and services that can be exploited by a cyber attacker to cause harm to their business.

Redcentric will perform regular vulnerability scanning of the customer's internal and external (internet-facing) assets including but not limited to end user devices, servers, and network devices.

The service is designed to provide organisations with greater insight and actionable information than a typical vulnerability scanning solution by enriching the data indicate which vulnerabilities pose the greatest risk in the context of their exploitability and presenting the information in an easy-to-use dashboard interface based on Jira.

The service benefits from human oversight to complement industry-leading tooling, ensuring findings can be tailored and presented in accordance with business context, and that the customer is able to interact with human operators to query and interpret findings, and determine the best possible course of response and remediation.

1.1. Key features, benefits and outcomes

- ✓ Identify, track, and remediate vulnerabilities as they emerge to reduce susceptibility to exploit-based attacks.
- ✓ Prioritise patching and mitigation efforts to manage the risk of vulnerability exploitation.
- ✓ Assess vulnerabilities with contextual knowledge and remediate based on true risk scores.
- ✓ Reduce vulnerability noise due to false positives and low-impact issues to streamline remediation efforts.
- ✓ Eliminate complexity by centralising vulnerability management across your organisation with a single provider.
- ✓ Remove the time-burden from valuable employees who can be focused on value-adding activities.
- ✓ Limit patching disruption to avoid downtime whilst ensuring impactful issues are quickly addressed.
- ✓ Improve visibility and track remediations throughout the patching lifecycle.

1.2. Service scope

The service scope can fall into one of two possible categories:

- **External assets only** – only including assets that can be reached over-the-internet without internal network access provisioning.
- **Internal and external assets** – including both internet accessible assets and assets requiring an internal network connection.

1.2.1. Quantity of hosts

The standard service price includes up to 750 hosts in the scope. Additional hosts will incur further charges. These are specified in the Proposal document.

Assets that are deployed using a standard device build can be de-duplicated to control the number of hosts being scanned, decrease scanning and processing time, and avoid incurring additional costs. For example, a sample of end-user devices can be scanned as opposed to the full user estate.

1.2.2. Quantity of scans

The service includes 12x scans per year (typically 1x per month). Additional full scans in excess of the 12x annual scans can be performed but will incur a charge. 1 extra full scan can performed without incurring an additional charge. Any further scans will be charged as per the Proposal document.

Ad-hoc scans may be performed where there is a requirement to assess smaller subset of assets for vulnerabilities. This should comprise <10% of the total hosts covered by the service.

- The customer shall endeavour to provide reasonable notice of a request to scan of at least five working days.
- If more than 3 ad-hoc scans are required over a rolling 3-month period, then any additional scans may be chargeable.

1.2.3. Scanning environments without external network connectivity

If scanning of environments that do not have internet access is in scope, additional effort will be required to manually update and prepare the scanning agent running on the dedicated server. These charges will be scaled directly to the additional manual effort required and will be provided on a case-by-case basis.

1.2.4. Scanning multiple environments requiring additional scanner hosts

Charges may apply where additional scans are required if not all ranges are reachable from a single host, depending upon the number of additional hosts required.

1.3. Deployment and on-boarding

The customer will provide Redcentric with an asset list encompassing domain and host addresses.

If Internal assets are in-scope that are not reachable over the internet, internal servers should be assigned to Redcentric for the deployment of the scanning service. Redcentric uses a network-based (as opposed to agent-based) solution that scans all hosts that are reachable from the allocated server(s) with the scanning software deployed. The server must be a Windows or Linux host that meets the minimum specifications. Redcentric must also be assigned remote access (e.g. via Customer Name's VPN) and be assigned admin rights to the server.

1.3.1. Server requirements for internal scanning

The minimum requirements for any internal scanner hosts can be found here: https://docs.tenable.com/general-requirements/Content/NessusScannerHardwareRequirements.htm

1.4. Regular scanning

Vulnerability scanning of all assets within scope will be scheduled via the vulnerability scanning platform, in-line with the agreed scanning periodicity. Our cloud-based scanning platform will be utilised to scan externally facing assets.

Clarus utilises the Nessus vulnerability scanning engine. Nessus is an industry leading solution that maintains more than 78,000+ vulnerability identification signatures, covering both local and remote security flaws. Nessus can be configured to deliver credentialed and uncredentialed checks against multiple technology platforms.

1.5. Data Enrichment

The data set is exported from Nessus and cross-referenced with Redcentric's vulnerability scoring database and relevant external sources such as the Known Exploited Vulnerabilities (KEV) database and the Exploit Prediction Scoring System (EPSS). This provides additional metrics that can be used to calculate the risk score of the issue and guide remediation priority and urgency.

To enhance our risk assessment, we consider, for example:

- Whether exploit code exists on the public internet.
- Whether exploit code is likely to become publicly available in the future.
- The extent to which the vulnerability has been exploited previously.
- How we have classified the issue previously as part of penetration testing and incident response.
- How the customer has internally risk assessed the type of vulnerability previously.

1.6. Assessment

We will utilise a differential approach to the output, looking to identify changes from the initial benchmark. These will be classified as follows:

- New vulnerability introduced to the environment - Where a new vulnerability is identified, we will review the technical output to confirm the validity of the issue (removing common false-positives) and pass to the triage and escalation stage.
- Removal of vulnerability from the environment - Where a previously identified vulnerability has been remediated and confirmed through ongoing vulnerability scanning, the remediation tracker will be updated to reflect the change in status of the issue.
- Change in severity - Changes within the threat landscape can have an impact on the relative severity rating of known vulnerabilities. Where this occurs, we will review all severity ratings associated with that change and apply new severity ratings as required.

1.7. Triage and Escalation

Where a new vulnerability is identified, we will review the technical output and assign a priority level and update the remediation tracker. Where a vulnerability is categorised as critical, we will report as agreed within the escalation plan. Otherwise, new vulnerabilities will be managed as part of the ongoing remediation tracking workflow.

1.8. Remediation Tracking

After the triage and escalation phase, all technical details relating to individual vulnerabilities will be uploaded to the Clarus portal for access by the customer. The remediation tracker utilises a ticketing-based system to track individual vulnerable hosts along with the overarching vulnerability exposure. The tracker focuses on four swim lanes, ‘Backlog’ - contains details of new vulnerabilities found, ‘In Progress’ - captures tickets that have been allocated for remediation activity, ‘Risk Accepted’ - captures any vulnerability where the customer has chosen to accept the risk and finally, ‘Remediated’, for issues where the customer has completed remediation activity to close the item.

1.9. Remediation Validation

During each subsequent vulnerability scan hosts will be checked against existing vulnerabilities, if all hosts within a defined vulnerability category are identified as no longer being vulnerable, the ticket is automatically moved to the ‘Remediated’ column.

1.10. Reporting

Ongoing scanning will be delivered monthly for both internal and external network assets. The output will be triaged and processed by the Redcentric team and then uploaded to the Clarus portal, where the findings will be presented to the customer team for remediation.

After the completion of each monthly scan a reporting email will be generated providing a summary of the findings and any key changes from the previous scan.

Redcentric will make its consultants available for a debrief session each month that can be used as an opportunity for the customer to ask questions about the findings and establish a remediation plan under the guidance of Redcentric consultants.

The customer will be provisioned with a maximum of six accounts within the Clarus portal. Each account is to be assigned to a named individual within the customer's organisation. Additional reporting capability exists within the platform for wider distribution of relevant information to individual support teams for the purposes of remediation.

2. Assumptions, Dependencies and Requirements

2.1. Customer Obligations

- The customer will be responsible for updating the details of network ranges if there are any changes to the scope during the period of the contract.
- The customer will be responsible for the setup and maintenance of the internal server used to deliver the scanning platform.
- The customer will be responsible for the creation of service accounts as required.
- The customer will be responsible for network configuration allowing remote access from the Redcentric remote locations to the vulnerability scanning devices.
- The customer will be responsible for network configuration allowing access from the vulnerability scanning devices to all in scope systems.
- The customer will gain the appropriate approval from any third-party hosting / support services as required.
- The customer will be provisioned with a maximum of six accounts within the Clarus portal. Each account to be assigned to a named individual within the customer's organisation.

2.2. Redcentric Obligations

- Redcentric will be responsible for the configuration of the scanning platform to deliver the required ongoing vulnerability scanning service.
- Redcentric will respond to queries made via the Clarus platform within a maximum 7 days of a communication being logged (typical response times are within 48 hours).
- Redcentric will be responsible for analysing the output from the scanning platform.
- Redcentric will be responsible for the creation and maintenance of the Clarus Portal.
- Redcentric will not be responsible for the remediation of vulnerabilities.
- Core service delivery will be limited to twelve monthly scans per year (1x per month). This does not include the ad-hoc scans specified.

2.3. Change control

Change Control guidelines will apply from the point of service commencement and will be applicable until the service has been signed-off as completed by Redcentric and the customer. Any change required must be notified to the Redcentric Project Manager by the customer's delegate. A Change Control document will be agreed between the parties. All changes will be documented and managed, with a full list produced at closure. Where there is a commercial impact to the service, responsibility for authorising the additional costs must be approved by the appropriate parties and priced via the Redcentric Account Manager. Only when additional costs have been approved will work commence on the change required.

2.4. Limitations

The customer understands and accepts that the engagement will be limited to collection and triage of automated vulnerability scanning data of the systems in scope. Subsequent configuration changes could result in the introduction of new vulnerabilities or a weakened security posture. Ongoing scanning is representative of both the Redcentric security testing methodology and attack techniques known at the time of each scan.

As such, and due to limitations within the engagement scope, legal frameworks, the customer acknowledges that additional security weaknesses, which could not reasonably be identified during the engagement, may be present within the systems, and in no event will Redcentric, or its directors, agents, or employees, be liable for any decision made, or withheld, in reliance of the information contained within the formal output.

2.5. Data handling, storage and processing

Data is stored in Redcentric's modified Cloud-based Jira platform "Clarus". The data is stored in a dedicated customer Jira tenancy. The data is physically stored in the nearest location (in the case of the UK, Ireland) – https://www.atlassian.com/trust/reliability/infrastructure.

Vulnerability data is stored in the platform indefinitely to ensure that re-occurrence of issues can be identified.

In order to afford an appropriate level of data protection given the sensitivity of the information, the following operational processes will be applied:

- Only consultants with a direct delivery responsibility for the customer will be authorised to access the platform.
- Credentials for the platform are securely stored using Bitwarden. Only authorised consultants will have access to the Clarus platform.
- Consultants are not authorised to export data from the platform unless otherwise requested by an approved customer Clarus user.
- The assignment of new accesses for the customer and Redcentric must be approved by a nominated person.
- Redcentric systems and employees (i.e. non Cyber Security team employees) will not be authorised to access the customer Clarus instance or the data therein.
- Any email correspondence containing information from the Clarus platform, such as the regular update emails, will be protected using Twilio SendGrid here. It is configured to automatically attempt outbound TLS v1.1 or higher connections when sending emails. In practice, if the recipient's email server accepts incoming TLS v1.1 or higher connections, the email will be delivered via a secure TLS-encrypted connection.

2.6. Licensing of tools

No direct license procurement is required for the customer.

Document Control

Service Category	Cyber Security
Title	Managed Vulnerability Scanning Service Definition
Reviewer	Tom Holloway
Business Area	CSG
Review Cycle	Annual

Version and Change Control

Version	Date	Change
1.0	19/02/2024	Released

Ownership

Redcentric's Cyber Security Management Team is the collective owner of this document and responsible for ensuring that this definition is reviewed in line with the requirements of Redcentric's ISO 9001 Quality Management System.

Disclaimer

This information is subject to formal contract and is an indicative and unqualified invitation to treat not capable of acceptance. No contractual relationship shall exist until formal contract documentation has been negotiated and executed by both parties.

Redcentric does not warrant the completeness or accuracy of the information contained herein and shall not be responsible for technical or editorial errors or omissions. Other than as stated elsewhere in this document, Redcentric hereby excludes any express or implied warranties that may be contained in this document and further disclaims all liabilities which may arise due to, and/or as a consequence of, reliance on the information contained herein.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED