UoS/DH/25/26/QTR1/Vulnerability Scanning Tool (September 2025)

University of Salford – Vulnerability Scanning Tool (September 2025)

The University of Salford Digital IT team is seeking to procure a vulnerability scanning solution to operate over the next three years.

Mandatory Requirements

The proposed system **must**:

- Perform internet-based vulnerability scans of our perimeter and internet-facing systems.
- Support regular scans of our PCI DSS environment and provide quarterly ASV certificates to meet PCI DSS compliance requirements.
- Conduct web application scanning of internet-facing web services.
- Identify vulnerabilities across common infrastructure components, including:
    - Virtual servers
    - Firewalls
    - Storage appliances
    - Network switches
- Perform agentless scans of a limited number of internal systems to:
    - Validate findings from existing tools
    - Provide additional assurance where required
- Support both scheduled and on-demand scan execution.
- Automatically email scan results to relevant resolver teams for remediation.
- Allow license recycling for decommissioned or out-of-scope devices, with a cooling-off period of up to 90 days.

Preferred Features

The system **should**:

- Integrate with Microsoft Entra for account and identity management.
- Provide reporting capabilities to track and measure the effectiveness of vulnerability remediation efforts.

- Allow flexible license allocation between systems and web applications.

Optional Features

The system **could**:

- Integrate with ServiceNow to enable automated ticket creation for resolver teams.

Scope and Context

- Internal agent-based scanning is already in place and **out of scope**, except for ad-hoc validation scans as described above.
- Estimated scanning requirements:
  - ~300 systems (perimeter and internal)
  - ~10 systems within the PCI DSS zone
  - ~100 web applications

Submission Details

Please send quotations and correspondence to:

Adam Clayton
Head of Information Security
r.a.clayton@salford.ac.uk