SOP Vulnerability Scanner + MS Security

Purpose

The purpose of this SOP is to define the standardized procedures for conducting **vulnerability scanning** across all internal IT assets and integrating the results with **Microsoft Security tools** to enhance detection, prioritization, and remediation of security risks. This process aims to improve the organization's cybersecurity posture, prevent data breaches, and ensure compliance with financial and data protection regulations.

Scope

This SOP applies to all internal IT assets within the corporate infrastructure, including:

- Windows endpoints
- Financial systems and applications
- Network infrastructure devices
- Microsoft 365 cloud assets
- Azure workloads
- On-premises environments

Third-party devices and BYOD systems are excluded unless explicitly onboarded.

Definitions

- **MDVM**: Microsoft Defender Vulnerability Management
- **MDE**: Microsoft Defender for Endpoint
- **CVE**: Common Vulnerabilities and Exposures
- **CVSS**: Common Vulnerability Scoring System

Objectives

- Proactively identify and remediate vulnerabilities before they can be exploited
- Integrate vulnerability data into Microsoft security tools for enhanced visibility and automation
- Provide accurate reporting for compliance, risk management, and executive oversight
- Reduce time to detect (TTD) and time to respond (TTR) to vulnerabilities

Roles and Responsibilities

Role	Responsibility
Security Team	Configure and manage scanning tools, validate results, report findings
System/Asset Owners	Approve, schedule, and assist in applying remediation
IT Operations	Execute patching, configuration changes, and testing

Tools Utilized

Tool	Purpose
Microsoft Defender Vulnerability Management (MDVM)	Real-time endpoint vulnerability assessment
Microsoft Defender for Endpoint	Threat detection and posture analytics
Microsoft 365 Defender Portal (security.microsoft.com)	Central dashboard for endpoint vulnerabilities
Nessus	Agentless/internal scanning for operating systems, web servers, and applications
OpenVAS	Open-source vulnerability scanning across internal networks
Nmap	Port scanning and network service discovery

What is Vulnerability Scanning?

A proactive cybersecurity practice that uses automated tools to identify known security flaws (vulnerabilities), misconfigurations, and outdated software versions that could be exploited.

Why It's Important

- Protects against exploitation of known vulnerabilities
- Supports cybersecurity compliance (PCI DSS, ISO 27001, etc.)
- Enables visibility into organizational risk posture
- Helps prioritize and justify remediation actions

Vulnerability Management Lifecycle

A structured process followed to identify, assess, and remediate vulnerabilities effectively:

1. Asset Discovery & Grouping

- Identify all corporate IT assets (endpoints, cloud services, network devices).
- Group assets based on criticality, function, or department.
- Maintain an updated inventory using Monday.com

2. Scanning Configuration

- Define scan scopes, exclusions, scan types (credentialed/uncredentialed).
- Schedule scans based on risk level.
- Ensure authenticated scans for more accurate vulnerability detection.

3. Scanning Execution

- Initiate scans using MDVM, Nessus, OpenVAS, and Nmap.
- Use safe scan options to minimize operational disruption.
- Log scan activity and outcomes.

4. Vulnerability Aggregation and Correlation

- Collect scan results from all tools into centralized dashboards or reports.
- Correlate findings across tools for duplicate detection and false positive filtering.

5. Risk Scoring and Prioritization

- Leverage CVSS scores, exploitability, asset criticality, and Microsoft Secure Score.
- Prioritize vulnerabilities:
    - Critical (CVSS 9.0–10): Immediate action
    - High (7.0–8.9): Within 5 business days
    - Medium & Low: Based on business context

6. Remediation & Mitigation

- Patch software, reconfigure settings, disable unused services.
- Use automation via Microsoft Intune/NinjaOne where applicable.
- Document change requests if immediate patching is not feasible.

7. Validation and Re-Scan

- Conduct post-remediation scans to confirm successful mitigation.
- Mark false positives or deferred issues with justification.

8. Scan Frequency

Scan Type	Frequency
Internal Vulnerability Scan (Nessus/OpenVAS)	Monthly
Endpoint Scan via MDVM	Continuous

Network Discovery (Nmap)	Bi-weekly
Onboarding or Major Change Scan	Ad-hoc
Validation Scan	Post-remediation

9. Reporting & Documentation

- Monthly vulnerability report (executive summary + technical detail)
- Trend graphs, risk heatmaps, and top vulnerable assets
- Tracking for remediated vulnerabilities
- Archived reports stored for minimum 12 months.

Audit and Compliance

- Aligns with:
  - **ISO 27001 – A.12.6.1** (Technical Vulnerability Management)
  - **PCI DSS – Req. 6.1 and 11.2**
  - **NIST 800-53 – RA-5**
- Evidence:
  - Scan reports
  - Remediation logs
  - Exception register
  - Audit trails from Defender

Review and Maintenance

- This SOP must be reviewed annually or:
  - After a critical security incident
  - Upon introduction of new tools or regulatory requirements
  - Upon infrastructure changes

Date: 06/06/2025