Defender TVM Remediation Plan

Role: Security Operations (SOC) Analyst – Lab Project

Tools: Microsoft Defender for Endpoint (TVM), Microsoft Endpoint Manager (Intune), Microsoft 365 Security & Compliance Center, Windows 10/11

Frameworks: ISO/IEC 27001:2022, Microsoft Threat & Vulnerability Management (TVM)

Project Summary

Built and tested a remediation plan using Microsoft Defender for Endpoint's Threat & Vulnerability Management (TVM) to identify security misconfigurations and unpatched software, then deploy targeted fixes using Intune remediation scripts. The plan prioritised vulnerabilities based on threat exposure score and business impact, mapped to ISO/IEC 27001:2022 controls.

Objectives

• Identify vulnerabilities in Windows 10/11 endpoints using Defender TVM.

• Prioritise remediation actions based on risk score and MITRE ATT&CK mapping.

• Deploy Intune remediation scripts to affected devices.

• Verify fixes and update compliance reports.

Scope

• Uses Defender for Endpoint TVM to scan all onboarded Windows devices for misconfigurations and unpatched applications.

• Maps findings to CVEs and MITRE ATT&CK techniques.

• Pushes remediation scripts via Intune for high-priority issues.

• Confirms resolution and recalculates exposure score.

Implementation Steps

1. Onboarded Windows 10/11 endpoints into Defender for Endpoint.

2. Enabled TVM in Microsoft 365 Security portal to continuously scan for vulnerabilities.

3. Reviewed Security Recommendations and assigned remediation actions.

4. Created Intune remediation scripts targeting vulnerable endpoints.

5. Deployed scripts and monitored execution status in Intune.

6. Verified remediation success in TVM dashboard and reduced exposure score.

ISO/IEC 27001:2022 Control Mapping

Control	Goal	Coverage
A.8.8 – Management of Technical Vulnerabilities	Ensure vulnerabilities are identified, assessed, and remediated in a timely manner.	TVM scans for vulnerabilities, assigns priority, and verifies remediation via Intune.
A.8.15 – Logging	Ensure security-relevant events are recorded.	TVM generates logs for all vulnerability detections and remediation actions.
A.8.16 – Monitoring Activities	Continuously monitor for security weaknesses.	TVM dashboard updates in near real-time; Intune provides deployment reports.

Results & Impact

- Reduced exposure score by up to 40% in lab tests after remediation.
- Fully automated vulnerability detection and remediation pipeline.
- Improved endpoint compliance posture aligned with ISO/IEC 27001:2022.

Key Skills Demonstrated

- Vulnerability management and risk prioritisation.
- Intune device management and automation scripting.
- Compliance mapping to ISO/IEC 27001:2022.
- Microsoft Defender for Endpoint TVM configuration.