Microsoft Defender Live Response: Prevention & Response Proof

Security Engineer Project Report

Executive Summary

This project validates Microsoft Defender for Endpoint's ability to prevent malicious activity and enable rapid incident response. The test environment simulated common attack vectors including credential theft, ransomware, and execution of unauthorised binaries. Preventive controls automatically blocked attacks, while Live Response was used to contain and remediate in real time. All actions generated a verifiable audit trail, directly supporting ISO 27001 Annex A controls for malware protection, incident response, and logging.

Scope and Environment

- **Stack:** Microsoft Defender XDR, Defender for Endpoint (Live Response), Intune onboarded Windows 11 VM.
- **Objective:** Demonstrate endpoint protection and prove containment/remediation capability.
- **Controls Enforced:**
    1. ASR rule: Office spawning child process → blocked.
    2. ASR rule: LSASS credential theft → blocked.
    3. Unsigned executables → blocked.
    4. Ransomware behaviours → blocked.

ISO 27001 Annex A Mapping

- **A.8.8 – Malware Protection**: Attack Surface Reduction (ASR) policies prevented malware techniques.
- **A.12.4 – Logging and Monitoring**: Device Timeline and Action Center captured detections and response activity.
- **A.16.1 – Incident Management**: Live Response enabled investigation, containment, and remediation.
- **A.12.6 – Technical Vulnerability Management**: Blocking unsigned executables mitigated exploitation risk.
- **A.13.1 – Network Security**: Device isolation restricted lateral movement.

Prevention Evidence

- **Action:** Executed test scenarios simulating credential dumping, ransomware, and child-process spawning.
- **Result:** Defender blocked all attempts.
- **Proof:** Device Timeline showed AntivirusDetection events; ASR logs recorded blocked behaviours.

Response Evidence

- **Playbook Executed:**
    1. Connected to lab endpoint via Live Response.
    2. Retrieved file: `C:\Users\Public\demo-lr.txt`.
    3. Killed malicious process (PID 7780).
    4. Quarantined malicious file.
    5. Isolated device, then safely released.
- **Audit Trail:** Action Center logs displayed all commands with timestamps. Device Timeline confirmed remediation activity.

Results

- **Prevention:** Confirmed through automated ASR/AV detections.
- **Response:** Confirmed through file collection, process kill, remediation, and isolation.
- **Compliance Proof:** All actions generated timestamped evidence, supporting auditability and regulatory assurance.

Value for Security Engineer Role

- Proves ability to configure, test, and validate Microsoft Defender XDR capabilities.
- Demonstrates practical skills in incident detection, containment, and recovery.
- Provides compliance-ready evidence mapped directly to ISO 27001 Annex A controls.
- Shows readiness to operate in enterprise environments with strict governance requirements.