

THREAT SENTRY
SECURITY

VULNERABILITY ASSESSMENT REPORT

THREAT SENTRY SECURITY

Vulnerability Assessment Report

Internal and External Infrastructure

Item	Detail
Client	Meridian Health Partners (fictional)
Engagement	Vulnerability assessment
Scan dates	10-12 April 2025
Report date	18 April 2025
Version	1.0 (Sample)
Prepared by	Threat Sentry Security

SAMPLE DOCUMENT. Meridian Health Partners is a fictional organization. All hosts, IP addresses, people, findings and scores are invented for demonstration and do not describe any real engagement, system or company.

CONFIDENTIAL - Client use only (sample)

1. Executive Summary

TSS conducted an authenticated vulnerability assessment of Meridian Health Partners' internal and external infrastructure on 10-12 April 2025. A total of 142 assets were scanned, and 187 unique vulnerabilities were identified. Findings are ranked by CVSS score, exploit availability and the business criticality of the affected asset.

Severity	Count	% of total	SLA to fix
Critical	6	3%	7 days
High	29	16%	30 days
Medium	74	40%	60 days
Low	58	31%	90 days
Info	20	10%	Best effort

Overall posture: MODERATE. Most exposure comes from missing operating system patches on Windows servers and end-of-life software. Six critical issues should be resolved within a week.

2. Scope and Methodology

Item	Detail
Assets	142 hosts: 38 servers, 87 workstations, 11 network devices, 6 external-facing services
Ranges	10.20.0.0/22 (internal), 203.0.113.0/28 (external)
Scan type	Credentialed internal scan plus unauthenticated external scan
Tools	Industry-standard commercial and open-source scanners, followed by manual validation

Item	Detail
Exclusions	Medical devices on VLAN 90 (excluded at client request)

Findings were validated manually to remove false positives. Risk scoring combines CVSS v3.1 with exploit maturity and asset criticality.

3. Top Vulnerabilities

ID	Vulnerability	Severity	CVSS	Hosts	Fix
V-01	Unsupported Windows Server 2012 R2	Critical	10.0	4	Upgrade or isolate
V-02	Missing critical OS patch enabling remote code execution (SMB)	Critical	9.8	7	Apply vendor patch
V-03	Apache Log4j outdated library in billing app	Critical	9.8	1	Upgrade library
V-04	Default credentials on network printer web UI	Critical	9.1	3	Change credentials
V-05	Outdated OpenSSH (multiple CVEs)	High	8.1	9	Update package
V-06	SMB signing not required	High	7.4	31	Enforce signing
V-07	Unquoted service path privilege escalation	High	7.8	12	Quote paths
V-08	Expired / self-signed TLS certificates	Medium	5.9	14	Reissue from CA
V-09	SNMP community string 'public'	Medium	5.3	8	Use SNMPv3
V-10	Directory listing enabled on intranet	Low	3.7	2	Disable

4. Remediation Guidance

V-01 Unsupported Windows Server 2012 R2 (Critical)

Four servers run an operating system that no longer receives security updates. **Impact:** Any new vulnerability stays permanently exploitable. **Fix:** Migrate workloads to a supported OS; until then, segment these hosts, restrict inbound access and enable enhanced monitoring.

V-02 SMB Remote Code Execution (Critical)

Seven servers lack a patch for a wormable SMB flaw. **Impact:** Unauthenticated remote code execution and rapid ransomware spread. **Fix:** Install the vendor patch, block SMB at the perimeter, and confirm patch compliance with a rescan.

V-03 and V-04 (Critical)

• **V-03:** Upgrade the vulnerable logging library in the billing application and redeploy.

• **V-04:** Change default credentials on three printers and place them on a management VLAN.

5. Asset Risk Overview

Asset group	Hosts	Critical	High	Risk
Windows servers	38	5	14	High
Workstations	87	0	8	Moderate
Network devices	11	1	4	Moderate
External services	6	0	3	Moderate

6. 30 / 60 / 90 Day Action Plan

Window	Actions	Expected outcome
0-30 days	Resolve all Critical (V-01 to V-04); patch SMB; change default credentials; begin High items	Critical count reduced to 0
31-60 days	Complete High items; enforce SMB signing; reissue certificates; implement monthly patch cycle	High count reduced by 80%
61-90 days	Address Medium/Low findings; migrate unsupported systems; schedule rescan	Overall risk lowered to Low

7. Next Steps

TSS recommends a validation rescan at 30 days and a quarterly scanning cadence. Findings that cannot be remediated should be documented as accepted risk with an owner and review date.