Monthly Security Report

// FEBRUARY 2025 — REDACTED CLIENT, INC. — PUBLIC SAMPLE

This report summarizes security posture changes, vulnerability remediation progress, and key risk indicators for the reporting period. Prepared by RMA Security as part of the ongoing Security Partner engagement.

// 1.0 KEY METRICS

OPEN VULNERABILITIES	REMEDIATED THIS MONTH	MEAN TIME TO REMEDIATE	EXTERNAL EXPOSURE SCORE
12	8	14 days	B+

METRIC	JAN	FEB	TREND
Open Vulnerabilities (Critical/High)	18	12	▼ 33% improvement
External Attack Surface Changes	2 new	0 new	— Stable
Mean Time to Remediate (days)	21	14	▼ 33% improvement
Compliance Evidence Items Completed	12/40	22/40	▲ 25% progress
Patch Currency (% current within 30d)	74%	88%	▲ 14% improvement

// 2.0 VULNERABILITY STATUS

Open Vulnerabilities by Severity

SEVERITY	OPEN	REMEDIATED	ACCEPTED RISK	NOTES
CRITICAL	0	2	0	All critical findings remediated — SMB signing + NTLM relay chain closed
HIGH	3	4	0	Remaining: legacy auth still active on 3 service accounts
MEDIUM	6	2	1	Accepted: legacy print server (isolated VLAN, decommission Q2)
LOW	3	0	0	Informational items, no business impact

Key Remediations Completed This Month

✓ SMB signing enforced via GPO across all domain-joined systems (PT-001, PT-002 — closed)

✓ LLMNR/NBT-NS disabled via GPO + Intune remediation script (PT-003 — closed)

✓ Service account svc_backup rotated to gMSA; svc_sqlreport password rotated to 25+ chars (PT-004 — closed)

✓ Conditional Access policy deployed: block legacy authentication for all users

✓ DMARC policy moved from p=none to p=quarantine; SPF/DKIM validated

Pending Remediation (Owner: Client IT / MSP)

- 3 service accounts still using legacy authentication — target: disable by March 15
- Windows Server 2012 R2 decommission on 10.10.2.40, 10.10.2.41 — target: Q2 2025
- Intune compliance policy enforcement for personal devices — in testing, target: March 1

// 3.0 EXTERNAL ATTACK SURFACE

Weekly external scans identified no new exposed services or changes to the external attack surface this month. The following external-facing services remain monitored:

SERVICE	HOST	STATUS	LAST CHANGE
HTTPS (443)	app.redacted.com	Monitored — TLS 1.3, cert valid	No change
HTTPS (443)	portal.redacted.com	Monitored — TLS 1.2+, cert valid	No change
SMTP (25/587)	mail.redacted.com	DMARC p=quarantine deployed	Feb 12 — DMARC update
VPN (443)	vpn.redacted.com	MFA enforced, split tunnel disabled	No change

// 4.0 COMPLIANCE READINESS

Evidence collection for NIST CSF alignment is ongoing. Current progress against control families:

NIST CSF FUNCTION	CONTROLS MAPPED	EVIDENCE STATUS	NOTES
IDENTIFY	6/6	Complete	Asset inventory + risk assessment documented
PROTECT	8/12	In progress	Access control + awareness training gaps remaining
DETECT	4/6	In progress	Log aggregation deployment Q1; alerting rules pending
RESPOND	3/5	In progress	IR plan drafted; tabletop exercise scheduled Q2
RECOVER	1/3	Not started	Backup validation + recovery testing planned Q2

// 5.0 NEXT MONTH PRIORITIES

1. **Complete legacy auth migration** — disable on remaining 3 service accounts by March 15
2. **Deploy log aggregation** — centralize Windows event logs + firewall logs for detection capability
3. **Intune compliance enforcement** — move personal device policy from testing to enforcement
4. **Tabletop IR exercise** — schedule with leadership for Q2 (ransomware scenario)
5. **External pentest retest** — validate closure of initial assessment findings