NullSight

SAMPLE EXPOSURE REPORT

Dark Web Exposure Report

A 30-day summary of credential, domain, and infrastructure exposures detected for the monitored organization.

Prepared for: Acme MSP, Inc.

Acme Healthcare	**Reporting period**	**Generated by**
Monitored organization	Apr 03 to May 03, 2025	NullSight v1.0

Executive Summary

During this 30-day reporting period, NullSight detected **14 new exposures** across the assets registered for Acme Healthcare. Three are classified as CRITICAL and require immediate remediation. The remaining items are documented for visibility and tracked through the standard PSA workflow in ConnectWise.

3 CRITICAL Active credential exposure with valid format	**7** HIGH Recent leak association or domain mention	**4** MEDIUM Historical or low-confidence findings

Key takeaways

- One executive personal email account was found in a recent stealer log. The associated session token has been invalidated by the MSP.
- Five distinct corporate addresses appeared across two unrelated breach databases. Password resets have been forced for all five.
- One IP range linked to client infrastructure was mentioned in a Russian-speaking criminal forum. Traffic to that range is being monitored at the firewall.
- No critical exposures remain unresolved at the time of reporting. Average time to ticket creation: 38 seconds.

Posture trend (last 90 days)

Overall exposure volume is down **22%** compared to the previous 30 days. Most of this decrease is attributed to a forced password rotation campaign initiated by the MSP after the March 2025 stealer log surge.

Note: This is a sample document. All organizations, addresses, ticket numbers, and findings shown are fictional. A real NullSight report uses live monitoring data from the assets you register through the MSP dashboard.

Detailed Findings

Top 5 findings of the reporting period, ordered by severity. Each detection generated an automated ticket in ConnectWise PSA at the time it was discovered. Full details for all 14 findings are appended in the JSON export delivered alongside this report.

SEVERITY	TYPE	ASSET	SOURCE	DETECTED	TICKET
CRIT	Credential exposure	admin@acme-health.com	Underground forum, stealer log	Apr 28, 14:02 UTC	CW-4821
CRIT	VIP email exposure	ceo.personal@gmail.com	Stealer log, infostealer family	Apr 22, 09:47 UTC	CW-4819
CRIT	Credential reuse	cfo@acme-health.com	Cross-source correlation	Apr 18, 22:13 UTC	CW-4814
HIGH	Domain mention	acme-health.com	Telegram channel, threat actor	Apr 26, 11:30 UTC	CW-4820
HIGH	IP infrastructure mention	203.0.113.42	Criminal forum thread	Apr 15, 06:11 UTC	CW-4817

Sources monitored this period

14,328 dark web sources were scanned. Coverage includes underground forums, criminal marketplaces, paste sites, leak databases, infostealer feeds, and Telegram threat-actor channels. Source diversity directly impacts detection completeness.

Recommended Remediation

Tier 2 customers receive active remediation guidance with each report. The actions below address the three Critical findings detected this period.

Force credential rotation for admin@acme-health.com
Reset the password and invalidate all active sessions. Verify MFA is enrolled. Review the last 30 days of activity for the affected account.

Personal email containment for the CEO
Coordinate with the executive to change the password on ceo.personal@gmail.com, enable hardware-key MFA, and review forwarding rules for unauthorized changes.

Cross-account audit triggered by CFO credential reuse
The same password hash appeared on two unrelated assets. Trigger a discovery scan across all CFO-linked accounts and rotate any matches.

Compliance notes

This report is delivered with a verifiable chain of custody and is suitable for inclusion in HIPAA, ISO 27001, and SOC 2 documentation packages. The signed PDF and accompanying JSON export are retained in the MSP's NullSight dashboard for 24 months.

Appendix

Report ID	NS-RPT-2025-04-A7F2
Sources scanned	14,328 (underground forums, leak databases, stealer feeds, Telegram channels, paste sites)
Detection latency	Median 38 seconds from source publication to PSA ticket creation
Assets monitored	1 corporate domain, 4 IP ranges, 47 user accounts, 3 executive personal emails
PSA integration	ConnectWise PSA (auto-ticket, client mapping, priority tagging)
Tier	Tier 2 Professional · Certified intelligence sources, audit-ready reports
Document SHA-256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855