

DETAILED FINDINGS

Every exposure, with evidence and remediation.

The full finding queue behind the executive summary — attributable and actionable.

Prepared for

Northwind Trading Co.

REPORTING PERIOD Q3 2026 · as of 12 Aug 2026	SCOPE 320 endpoints · fleet-wide	CLASSIFICATION Sample
REPORT ID SAD-FIND-2026-0142	PREPARED BY Sargha · Araghatta LLC	AUDIENCE Security & platform teams

Findings queue — Northwind Trading Co.

Every open finding with the evidence Sargha collected and the recommended remediation. Findings are ordered by severity and blast radius. This sample shows the top of the queue.

API keys in shell profiles and .env files

CRIT

Provider API keys are stored in plain text in shell profiles and .env files.

FINDING ID	SAD-2026-0007
AFFECTED	14 endpoints
EVIDENCE	Masked fingerprints of 3 distinct keys on 14 endpoints; 1 key still valid at time of report.
REMEDIATION	Rotate exposed keys immediately; move them to a secret manager; brief affected users.

Unregistered MCP server on vulnerable version

CRIT

An MCP tool-server (server-filesystem) is running on a version with a known path-traversal issue and is not in the approved registry.

FINDING ID	SAD-2026-0011
AFFECTED	3 endpoints
EVIDENCE	Process tree shows server-filesystem@1.1.0 bound to an agent with filesystem scope on 3 hosts.
REMEDIATION	Upgrade to a patched build or remove; register approved MCP servers; restrict agent filesystem scope.

Unapproved coding agents with credential access

HIGH

Autonomous coding agents run unattended with access to source and stored credentials.

FINDING ID	SAD-2026-0019
AFFECTED	31 endpoints
EVIDENCE	31 endpoints run coding agents outside the approved allow-list; 6 hold long-lived tokens.
REMEDIATION	Bring agents under policy; scope tokens; require human-in-the-loop for credentialed actions.