MYTHAL EVIDENCE PACKAGE

NIST Cybersecurity Framework 2.0

Framework code: NIST_CSF_2

Tenant	Meridian Continental Railway (MCR) — SIMULATED demo tenant
Reporting period	From inception through June 17, 2026 at 14:37 UTC
Generated by	Mythal Compliance Reporter agent · v1.0
Report ID	MYTHAL-EV-NIST_CSF_2-20260617-143756
Signed	hmac:01da1b8a27d4d7f5323770c2
Watermark	SIMULATED — demo content, not for regulatory submission

Purpose of this report

This evidence package documents Mythal's compliance posture against **NIST Cybersecurity Framework 2.0**. It captures every closed remediation plan during the reporting period along with the agent reasoning trace, signed approvals, execution records, and verification outcomes. Each entry maps to one or more controls in the framework. Auditors should treat the reasoning trace excerpts as the primary audit log — they are recorded as actions occur, not reconstructed.

Executive summary

Evidence units captured	**4**
Distinct controls covered	**2**
Closed remediation plans referenced	**2**
Total plans in lifecycle (any status)	**11**
Posture status	**READY**

Reading guide

Section 1 lists each framework control and the count of evidence records mapped to it. Section 2 walks through each closed plan in detail — what was found, who approved it, which patch tool applied the fix, the verification result, and the agent reasoning trace excerpt. Section 3 documents the methodology and the signed integrity check.

Section 1 · Control mapping

Each control in the framework along with the count of evidence records and a brief description.

Control	Evidence count	Description
DE.CM	0	Detect · Continuous Monitoring
ID.RA	0	Identify · Risk Assessment
ID.RA-01	0	Vulnerabilities to organizational assets identified and documented
PR.IP	0	Protect · Information Protection Processes
PR.IP-12	0	Vulnerability management plan developed and implemented
RC.IM	0	Recover · Improvements
RC.RP-01	2	—
RS.MI	0	Respond · Mitigation
RS.MI-01	2	—
RS.MI-03	0	Newly identified vulnerabilities are mitigated or documented as accepted risks

Section 2 · Closed plan detail

Each closed remediation plan associated with this framework. For each plan we record the CVE, the affected asset, who approved the action, what was applied, the verification outcome, and an excerpt from the agent reasoning trace.

2 closed plan(s) detailed below. Reading top-to-bottom yields the chronological narrative of cyber actions for the period.

Finding #1 · CVE-2023-38737

Status: CLOSED

Title	Apply IBM 24.0.0.3 to target-liberty (CVE-2023-38737)
CVE	CVE-2023-38737 · CVSSv3 7.5 · KEV-listed: no
Asset	target-liberty · IBM Open Liberty · IT / POC-Lab · criticality: High
Approvals required	security
Plan trace ID	01KV6AF1ABW2WRM4E5NQ8WVMWR

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KV6A2MY0CZSYF4YJ17CXTQ2	2026-06-15 20:54	hmac:BHD965

Execution steps

Step	Tool	Status	Started	Completed
1	ansible	success	20:54:55	20:55:08

Verification outcome

Re-scan clean: **YES** · Health check pass: **YES** · Exploit re-test blocked: **YES**

Reasoning trace excerpt (first 3 decisions)

[scanner_liaison/INGEST] Normalized CVE-2023-38737 on poc-target-liberty from Qualys VMDR (POC). CVSSv3=7.5.

[threat_intel/ENRICH] Enriched CVE-2023-38737: KEV=False, EPSS=0.588, exploit-in-wild=True, ransomware-associated=False.

[threat_intel/RECONCILE] Reconciled CVE-2023-38737 against live CISA KEV + EPSS feeds: KEV=False, EPSS=0.42, exploit-in-wild=False.

Finding #2 · CVE-2020-1938

Status: CLOSED

Title	Apply Apache 9.0.89 to target-tomcat (CVE-2020-1938)
CVE	CVE-2020-1938 · CVSSv3 9.8 · KEV-listed: yes
Asset	target-tomcat · Apache Apache Tomcat · IT / POC-Lab · criticality: High
Approvals required	security
Plan trace ID	01KV6AF0G2AMA8EA35P0SDS1BQ

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KV6A2MY0CZSYF4YJ17CXTQ2	2026-06-15 19:04	hmac:4C3AKK

Execution steps

Step	Tool	Status	Started	Completed
1	ansible	success	19:04:50	19:05:30

Verification outcome

Re-scan clean: **YES** · Health check pass: **YES** · Exploit re-test blocked: **YES**

Reasoning trace excerpt (first 3 decisions)

[scanner_liaison/INGEST] Normalized CVE-2020-1938 on poc-target-tomcat from Qualys VMDR (POC). CVSSv3=9.8.

[threat_intel/ENRICH] Enriched CVE-2020-1938: KEV=True, EPSS=0.953, exploit-in-wild=True, ransomware-associated=False.

[threat_intel/RECONCILE] Reconciled CVE-2020-1938 against live CISA KEV + EPSS feeds: KEV=True, EPSS=0.94, exploit-in-wild=True.

Section 3 · Methodology

All evidence in this report is captured by the Mythal Compliance Reporter agent at the moment each remediation plan closes. The reasoning trace is appended-only and signed at the message level. Approvals carry HMAC signatures bound to the approver identity, the plan ID, and the decision timestamp. Execution records carry the tool ID, the action ID returned by the patch tool, and the structured result payload.

Integrity check

This report was generated at **2026-06-17T14:37:56+00:00** and signed with the integrity hash **`hmac:01da1b8a27d4d7f5323770c2`**. Any modification to the source records would invalidate this signature.

Limitations

This is a SIMULATED report from a demo tenant. Actions described against assets are produced by the Mythal simulator and are not real changes to a production environment. For a production deployment, every action described above corresponds to a real signed operation on a customer-owned asset and is suitable for regulatory submission.

End of report · MYTHAL-EV-NIST_CSF_2-20260617-143756 · Page count determined by content · Generated by Mythal Compliance Reporter v1.0