MYTHAL EVIDENCE PACKAGE

NIST SP 800-82r3 (ICS Security)

Framework code: NIST_800_82

Tenant	Meridian Continental Railway (MCR) — SIMULATED demo tenant
Reporting period	From inception through June 24, 2026 at 11:24 UTC
Generated by	Mythal Compliance Reporter agent · v1.0
Report ID	MYTHAL-EV-NIST_800_82-20260624-112433
Signed	hmac:3d90f8818c815de6b1228ad2
Watermark	SIMULATED — demo content, not for regulatory submission

Purpose of this report

This evidence package documents Mythal's compliance posture against **NIST SP 800-82r3 (ICS Security)**. 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	**0**
Distinct controls covered	**0**
Closed remediation plans referenced	**0**
Total plans in lifecycle (any status)	**1785**
Posture status	**NO EVIDENCE YET**

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
3.2	0	ICS Security Program — vulnerability management
5.3	0	Identification and Authentication policy
6.2.2	0	Patch management for ICS environments
6.4	0	Network segmentation between business and control systems

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.

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

Finding #1 · CVE-2024-20353 — Status: CLOSED

Title	Apply Cisco see vendor advisory to mcr-net-adaptive-0004.meridian.rail (CVE-2024-20353)
CVE	CVE-2024-20353 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-net-adaptive-0004.meridian.rail · Cisco Adaptive Security Appliance · IT / VPN-Concentrator · criticality: Critical
Approvals required	security
Plan trace ID	01KT0FBSRV96KXWJGJQ56VPED3

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-06-11 18:26	hmac:PBNHME

Execution steps

Step	Tool	Status	Started	Completed
1	panorama	success	18:26:20	18:26:22
2	panorama	success	18:26:22	18:26:23
3	panorama	success	18:26:23	18:26:25
4	qualys	success	18:26:25	18:26:27

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-2024-20353 on 01KSBCWFF7H9QV255PHPHWF79R from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2024-20353 on mcr-net-adaptive-0004.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2024-20353: KEV=False, EPSS=0.905, exploit-in-wild=True, ransomware-associated=False.

Finding #2 · CVE-2024-20359 — Status: CLOSED

Title	Apply Cisco see vendor advisory to mcr-net-adaptive-0004.meridian.rail (CVE-2024-20359)
CVE	CVE-2024-20359 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-net-adaptive-0004.meridian.rail · Cisco Adaptive Security Appliance · IT / VPN-Concentrator · criticality: Critical
Approvals required	security
Plan trace ID	01KT0FBRE01JWCF11TXH0QJWYE

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-06-07 01:06	hmac:KFSES4

Execution steps

Step	Tool	Status	Started	Completed
1	panorama	success	01:06:51	01:06:52
2	panorama	success	01:06:52	01:06:54
3	panorama	success	01:06:54	01:06:55
4	qualys	success	01:06:55	01:06:58

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-2024-20359 on 01KSBCWFF7H9QV255PHPHWF79R from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2024-20359 on mcr-net-adaptive-0004.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2024-20359: KEV=False, EPSS=0.725, exploit-in-wild=True, ransomware-associated=False.

Finding #3 · CVE-2024-20353 — Status: CLOSED

Title	Apply Cisco see vendor advisory to mcr-net-firepower-0001.meridian.rail (CVE-2024-20353)
CVE	CVE-2024-20353 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-net-firepower-0001.meridian.rail · Cisco Firepower Threat Defense · DMZ / Industrial-DMZ · criticality: Critical
Approvals required	security
Plan trace ID	01KT0FBS56A2AJJFGEP2XKKZ9E

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-06-06 02:31	hmac:RDW0WF

Execution steps

Step	Tool	Status	Started	Completed
1	ansible	success	02:31:38	02:31:40
2	ansible	success	02:31:40	02:31:42
3	ansible	success	02:31:42	02:31:45
4	qualys	success	02:31:45	02:31:47

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-2024-20353 on 01KSBCWFF7H9QV255PHPHWF79N from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2024-20353 on mcr-net-firepower-0001.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2024-20353: KEV=False, EPSS=0.905, exploit-in-wild=True, ransomware-associated=False.

Finding #4 · CVE-2024-3400 — Status: CLOSED

Title	Apply Palo Alto Networks PAN-OS 11.1.2-h3 (and other branches) to mcr-net-palo-0001.meridi
CVE	CVE-2024-3400 · CVSSv3 9.5 · KEV-listed: no
Asset	mcr-net-palo-0001.meridian.rail · Palo Alto Networks PAN-OS · DMZ / Industrial-DMZ · criticality: Critical
Approvals required	security
Plan trace ID	01KT0FBWH0N4S70H6A7R01E8WR

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-06-05 02:48	hmac:A31T3K

Execution steps

Step	Tool	Status	Started	Completed

1	ansible	**success**	02:48:35	02:48:37
2	ansible	**success**	02:48:37	02:48:39
3	ansible	**success**	02:48:39	02:48:41
4	qualys	**success**	02:48:42	02:48:44

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-2024-3400 on 01KSBCWFFC2P58R6EYB3TNH84Z from cisa_kev. CVSSv3=9.5.

[supervisor/ORCHESTRATE] Driving CVE-2024-3400 on mcr-net-palo-0001.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2024-3400: KEV=False, EPSS=0.711, exploit-in-wild=True, ransomware-associated=False.

Finding #5 · CVE-2024-38063 — Status: CLOSED

Title	Apply Microsoft 23H2-build-22631.3296 to mcr-ws-hr-0007.meridian.rail (CVE-2024-38063)
CVE	CVE-2024-38063 · CVSSv3 7.7 · KEV-listed: no
Asset	mcr-ws-hr-0007.meridian.rail · Microsoft Windows 11 · IT / Workstations-HR · criticality: Low
Approvals required	security
Plan trace ID	01KSH8MTDQ6ZNTRMWHXBGTMDCT

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-05-27 14:30	hmac:XX6D6P

Execution steps

Step	Tool	Status	Started	Completed
1	sccm	success	14:30:30	14:30:32
2	sccm	success	14:30:33	14:30:35
3	sccm	success	14:30:35	14:30:38
4	qualys	success	14:30:38	14:30:40

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-2024-38063 on 01KSBCWFC2WWWE3FQGS2YHVBCZ from qualys. CVSSv3=7.7.

[supervisor/ORCHESTRATE] Driving CVE-2024-38063 on mcr-ws-hr-0007.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2024-38063: KEV=False, EPSS=0.74, exploit-in-wild=True, ransomware-associated=True.

Finding #6 · CVE-2023-20198 — Status: CLOSED

Title	Apply Cisco 17.9.4a to mcr-net-ios-xe-0002.meridian.rail (CVE-2023-20198)
CVE	CVE-2023-20198 · CVSSv3 9.8 · KEV-listed: no
Asset	mcr-net-ios-xe-0002.meridian.rail · Cisco IOS-XE · IT / Core-Switch · criticality: Critical
Approvals required	security
Plan trace ID	01KSH8NGNM0R7DS3S5A6VBZ4V1

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-05-27 04:43	hmac:GTA1BR

Execution steps

Step	Tool	Status	Started	Completed
1	panorama	success	04:43:33	04:43:35

2	panorama	**success**	04:43:35	04:43:36
3	panorama	**success**	04:43:37	04:43:38
4	qualys	**success**	04:43:38	04:43:40

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-2023-20198 on 01KSBCWFF7H9QV255PHPHWF79P from defender. CVSSv3=9.8.

[supervisor/ORCHESTRATE] Driving CVE-2023-20198 on mcr-net-ios-xe-0002.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2023-20198: KEV=False, EPSS=0.98, exploit-in-wild=True, ransomware-associated=False.

Finding #7 · CVE-2025-21418 — Status: CLOSED

Title	Apply Microsoft 2025 cumulative update to mcr-ws-fin-0002.meridian.rail (CVE-2025-21418)
CVE	CVE-2025-21418 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-ws-fin-0002.meridian.rail · Microsoft Windows 10 · IT / Workstations-FIN · criticality: Low
Approvals required	security
Plan trace ID	01KSGWX6AAHPWXJTTBFTMFW27Z

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-05-26 02:58	hmac:C10J3D

Execution steps

Step	Tool	Status	Started	Completed
1	sccm	success	02:58:37	02:58:40
2	sccm	success	02:58:40	02:58:42
3	sccm	success	02:58:42	02:58:45
4	qualys	success	02:58:45	02:58:47

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-2025-21418 on 01KSBCWFC2WWWE3FQGS2YHVBCT from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2025-21418 on mcr-ws-fin-0002.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2025-21418: KEV=False, EPSS=0.729, exploit-in-wild=True, ransomware-associated=False.

Finding #8 · CVE-2025-22226 — Status: CLOSED

Title	Apply VMware vendor advisory (see references) to mcr-vmw-esxi-0029.meridian.rail (CVE-2025
CVE	CVE-2025-22226 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-vmw-esxi-0029.meridian.rail · VMware ESXi · IT / Virtualization · criticality: Critical
Approvals required	security
Plan trace ID	01KSGSMXYTYDV4VMEETZ11XCEV

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-05-26 02:46	hmac:1ZY3XV

Execution steps

Step	Tool	Status	Started	Completed

1	ansible	**success**	02:46:46	02:46:48
2	ansible	**success**	02:46:48	02:46:50
3	ansible	**success**	02:46:50	02:46:52
4	qualys	**success**	02:46:52	02:46:54

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-2025-22226 on 01KSBCWFFFMKEJYD81WN5R3PK3 from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2025-22226 on mcr-vmw-esxi-0029.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2025-22226: KEV=False, EPSS=0.866, exploit-in-wild=True, ransomware-associated=False.

Finding #9 · CVE-2025-20362 — Status: CLOSED

Title	Apply Cisco next IOS-XE maintenance train to mcr-net-firepower-0001.meridian.rail (CVE-202
CVE	CVE-2025-20362 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-net-firepower-0001.meridian.rail · Cisco Firepower Threat Defense · DMZ / Industrial-DMZ · criticality: Critical
Approvals required	security
Plan trace ID	01KSG3M4JNVNA158BDSJ540KWD

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-05-25 18:54	hmac:N0YCRW

Execution steps

Step	Tool	Status	Started	Completed
1	ansible	success	18:54:06	18:54:08
2	ansible	success	18:54:08	18:54:10
3	ansible	success	18:54:10	18:54:12
4	qualys	success	18:54:13	18:54:15

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-2025-20362 on 01KSBCWFF7H9QV255PHPHWF79N from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2025-20362 on mcr-net-firepower-0001.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2025-20362: KEV=False, EPSS=0.741, exploit-in-wild=True, ransomware-associated=False.

Finding #10 · CVE-2011-3402 — Status: CLOSED

Title	Apply Microsoft 2011 cumulative update to mcr-ws-fin-0002.meridian.rail (CVE-2011-3402)
CVE	CVE-2011-3402 · CVSSv3 9.0 · KEV-listed: no
Asset	mcr-ws-fin-0002.meridian.rail · Microsoft Windows 10 · IT / Workstations-FIN · criticality: Low
Approvals required	security
Plan trace ID	01KSG3M1MN90E8ZG1YQFRJ5GFH

Approvals

Scope	Decision	Approver	Decided at	Signature
security	APPROVED	01KSBCWF9TEAWS8BQTJS1920	2026-05-25 17:41	hmac:H4DCYS

Execution steps

Step	Tool	Status	Started	Completed

1	sccm	**success**	17:41:50	17:41:53
2	sccm	**success**	17:41:53	17:41:56
3	sccm	**success**	17:41:56	17:41:58
4	qualys	**success**	17:41:58	17:42:00

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-2011-3402 on 01KSBCWFC2WWWE3FQGS2YHVBCT from cisa_kev. CVSSv3=9.0.

[supervisor/ORCHESTRATE] Driving CVE-2011-3402 on mcr-ws-fin-0002.meridian.rail.

[threat_intel/ENRICH] Enriched CVE-2011-3402: KEV=False, EPSS=0.803, exploit-in-wild=True, ransomware-associated=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 **2026-06-24T11:24:33+00:00** and signed with the integrity hash **`hmac:3d90f8818c815de6b1228ad2`**. 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_800_82-20260624-112433 · Page count determined by content · Generated by Mythal Compliance Reporter v1.0