Trust Audit

Civitas Analytica — Engineered truth.

pack_sha256	`590b8bfd12038147354597b9d55da55a702401763b879f5c4918700244ea7abf`
pack_type	`trust_audit`
library	dfir
client	acme
engagement	eng42

Executive Summary

SEVERITY-WEIGHTED SCORE	0.0%
TOTAL CONTROLS	84
MET	0
PARTIAL	0
GAP	84

Key Gaps

- `DFIR-005` Preparation readiness control 05 - GAP - severity 5 - missing evidence 3
- `DFIR-010` Preparation readiness control 10 - GAP - severity 5 - missing evidence 3
- `DFIR-019` DetectionAnalysis readiness control 05 - GAP - severity 5 - missing evidence 3
- `DFIR-024` DetectionAnalysis readiness control 10 - GAP - severity 5 - missing evidence 3
- `DFIR-033` Containment readiness control 05 - GAP - severity 5 - missing evidence 3
- `DFIR-038` Containment readiness control 10 - GAP - severity 5 - missing evidence 3
- `DFIR-047` Eradication readiness control 05 - GAP - severity 5 - missing evidence 3
- `DFIR-052` Eradication readiness control 10 - GAP - severity 5 - missing evidence 3
- `DFIR-061` Recovery readiness control 05 - GAP - severity 5 - missing evidence 3
- `DFIR-066` Recovery readiness control 10 - GAP - severity 5 - missing evidence 3

- `DFIR-075` PostIncident readiness control 05 - GAP - severity 5 - missing evidence 3
- `DFIR-080` PostIncident readiness control 10 - GAP - severity 5 - missing evidence 3

Full Controls Table

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
`DFIR-001`	Preparation readiness control 01	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	1	0
`DFIR-002`	Preparation readiness control 02	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	2	0
`DFIR-003`	Preparation readiness control 03	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with	GAP	3	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			remediation tracking for Preparation exceptions.			
DFIR-004	Preparation readiness control 04	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	4	0
DFIR-005	Preparation readiness control 05	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	5	0
DFIR-006	Preparation readiness control 06	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	1	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-007	Preparation readiness control 07	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	2	0
DFIR-008	Preparation readiness control 08	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	3	0
DFIR-009	Preparation readiness control 09	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	4	0
DFIR-010	Preparation readiness control 10	Ensure Preparation procedures are documented, exercised, and	Policy/procedure artifact showing ownership and cadence for Preparation.;	GAP	5	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		reproducible for incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.			
`DFIR-011`	Preparation readiness control 11	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	1	0
`DFIR-012`	Preparation readiness control 12	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	2	0
`DFIR-013`	Preparation readiness control 13	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation	GAP	3	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			execution.; Review evidence with remediation tracking for Preparation exceptions.			
DFIR-014	Preparation readiness control 14	Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.	GAP	4	0
DFIR-015	DetectionAnalysis readiness control 01	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	1	0
DFIR-016	DetectionAnalysis readiness control 02	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	2	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-017	DetectionAnalysis readiness control 03	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	3	0
DFIR-018	DetectionAnalysis readiness control 04	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	4	0
DFIR-019	DetectionAnalysis readiness control 05	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	5	0
DFIR-020	DetectionAnalysis readiness control 06	Ensure DetectionAnalysis procedures are documented, exercised, and	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.;	GAP	1	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		reproducible for incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.			
`DFIR-021`	DetectionAnalysis readiness control 07	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	2	0
`DFIR-022`	DetectionAnalysis readiness control 08	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	3	0
`DFIR-023`	DetectionAnalysis readiness control 09	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.			
DFIR-024	DetectionAnalysis readiness control 10	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	5	0
DFIR-025	DetectionAnalysis readiness control 11	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	1	0
DFIR-026	DetectionAnalysis readiness control 12	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	2	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-027	DetectionAnalysis readiness control 13	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	3	0
DFIR-028	DetectionAnalysis readiness control 14	Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.	GAP	4	0
DFIR-029	Containment readiness control 01	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	1	0
DFIR-030	Containment readiness control 02	Ensure Containment procedures are documented, exercised, and	Policy/procedure artifact showing ownership and cadence for Containment.;	GAP	2	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		reproducible for incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.			
`DFIR-031`	Containment readiness control 03	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	3	0
`DFIR-032`	Containment readiness control 04	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	4	0
`DFIR-033`	Containment readiness control 05	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment	GAP	5	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			execution.; Review evidence with remediation tracking for Containment exceptions.			
DFIR-034	Containment readiness control 06	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	1	0
DFIR-035	Containment readiness control 07	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	2	0
DFIR-036	Containment readiness control 08	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	3	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-037	Containment readiness control 09	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	4	0
DFIR-038	Containment readiness control 10	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	5	0
DFIR-039	Containment readiness control 11	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	1	0
DFIR-040	Containment readiness control 12	Ensure Containment procedures are documented, exercised, and	Policy/procedure artifact showing ownership and cadence for Containment.;	GAP	2	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		reproducible for incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.			
`DFIR-041`	Containment readiness control 13	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	3	0
`DFIR-042`	Containment readiness control 14	Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.	GAP	4	0
`DFIR-043`	Eradication readiness control 01	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication	GAP	1	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			execution.; Review evidence with remediation tracking for Eradication exceptions.			
DFIR-044	Eradication readiness control 02	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	2	0
DFIR-045	Eradication readiness control 03	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	3	0
DFIR-046	Eradication readiness control 04	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-047	Eradication readiness control 05	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	5	0
DFIR-048	Eradication readiness control 06	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	1	0
DFIR-049	Eradication readiness control 07	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	2	0
DFIR-050	Eradication readiness control 08	Ensure Eradication procedures are documented, exercised, and reproducible for	Policy/procedure artifact showing ownership and cadence for Eradication.;	GAP	3	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.			
DFIR-051	Eradication readiness control 09	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	4	0
DFIR-052	Eradication readiness control 10	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	5	0
DFIR-053	Eradication readiness control 11	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication	GAP	1	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			execution.; Review evidence with remediation tracking for Eradication exceptions.			
DFIR-054	Eradication readiness control 12	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	2	0
DFIR-055	Eradication readiness control 13	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	3	0
DFIR-056	Eradication readiness control 14	Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-057	Recovery readiness control 01	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	1	0
DFIR-058	Recovery readiness control 02	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	2	0
DFIR-059	Recovery readiness control 03	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	3	0
DFIR-060	Recovery readiness control 04	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks)	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.			
DFIR-061	Recovery readiness control 05	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	5	0
DFIR-062	Recovery readiness control 06	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	1	0
DFIR-063	Recovery readiness control 07	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	2	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-064	Recovery readiness control 08	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	3	0
DFIR-065	Recovery readiness control 09	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	4	0
DFIR-066	Recovery readiness control 10	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	5	0
DFIR-067	Recovery readiness control 11	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks)	GAP	1	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.			
`DFIR-068`	Recovery readiness control 12	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	2	0
`DFIR-069`	Recovery readiness control 13	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	3	0
`DFIR-070`	Recovery readiness control 14	Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-071	PostIncident readiness control 01	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	1	0
DFIR-072	PostIncident readiness control 02	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	2	0
DFIR-073	PostIncident readiness control 03	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	3	0
DFIR-074	PostIncident readiness control 04	Ensure PostIncident procedures are documented, exercised, and	Policy/procedure artifact showing ownership and cadence for PostIncident.;	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		reproducible for incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.			
`DFIR-075`	PostIncident readiness control 05	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	5	0
`DFIR-076`	PostIncident readiness control 06	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	1	0
`DFIR-077`	PostIncident readiness control 07	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident	GAP	2	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
			execution.; Review evidence with remediation tracking for PostIncident exceptions.			
DFIR-078	PostIncident readiness control 08	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	3	0
DFIR-079	PostIncident readiness control 09	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	4	0
DFIR-080	PostIncident readiness control 10	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	5	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
DFIR-081	PostIncident readiness control 11	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	1	0
DFIR-082	PostIncident readiness control 12	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	2	0
DFIR-083	PostIncident readiness control 13	Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.	GAP	3	0
DFIR-084	PostIncident readiness control 14	Ensure PostIncident procedures are documented, exercised, and	Policy/procedure artifact showing ownership and cadence for PostIncident.;	GAP	4	0

CONTROL_ID	TITLE	OBJECTIVE	EVIDENCE EXPECTATIONS	STATUS	SEVERITY	EVIDENCE_COUNT
		reproducible for incident response readiness.	Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.			

Gap Register

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
`DFIR-001`	Preparation readiness control 01	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
`DFIR-002`	Preparation readiness control 02	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
DFIR-003	Preparation readiness control 03	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-004	Preparation readiness control 04	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-005	Preparation readiness control 05	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-006	Preparation readiness control	GAP	1	0	3	Policy/procedure artifact showing

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
	06					ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-007	Preparation readiness control 07	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-008	Preparation readiness control 08	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-009	Preparation readiness control 09	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-010	Preparation readiness control 10	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-011	Preparation readiness control 11	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-012	Preparation readiness control 12	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						(logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-013	Preparation readiness control 13	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-014	Preparation readiness control 14	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.
DFIR-015	DetectionAnalysis readiness control 01	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-016	DetectionAnalysis readiness control 02	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-017	DetectionAnalysis readiness control 03	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-018	DetectionAnalysis readiness control 04	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets,

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-019	DetectionAnalysis readiness control 05	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-020	DetectionAnalysis readiness control 06	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-021	DetectionAnalysis readiness control 07	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						(logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
`DFIR-022`	DetectionAnalysis readiness control 08	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
`DFIR-023`	DetectionAnalysis readiness control 09	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
`DFIR-024`	DetectionAnalysis readiness control 10	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.;

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-025	DetectionAnalysis readiness control 11	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-026	DetectionAnalysis readiness control 12	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
DFIR-027	DetectionAnalysis readiness control 13	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
`DFIR-028`	DetectionAnalysis readiness control 14	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.
`DFIR-029`	Containment readiness control 01	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
`DFIR-030`	Containment readiness control 02	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
`DFIR-031`	Containment readiness control 03	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
`DFIR-032`	Containment readiness control 04	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
`DFIR-033`	Containment readiness control 05	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						(logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-034	Containment readiness control 06	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-035	Containment readiness control 07	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-036	Containment readiness control 08	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-037	Containment readiness control 09	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-038	Containment readiness control 10	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-039	Containment readiness control 11	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-040	Containment readiness control 12	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-041	Containment readiness control 13	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.
DFIR-042	Containment readiness control 14	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						evidence with remediation tracking for Containment exceptions.
DFIR-043	Eradication readiness control 01	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-044	Eradication readiness control 02	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-045	Eradication readiness control 03	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						for Eradication exceptions.
DFIR-046	Eradication readiness control 04	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-047	Eradication readiness control 05	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-048	Eradication readiness control 06	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
DFIR-049	Eradication readiness control 07	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-050	Eradication readiness control 08	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-051	Eradication readiness control 09	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-052	Eradication readiness control	GAP	5	0	3	Policy/procedure artifact showing

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
	10					ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-053	Eradication readiness control 11	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-054	Eradication readiness control 12	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-055	Eradication readiness control 13	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-056	Eradication readiness control 14	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.
DFIR-057	Recovery readiness control 01	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-058	Recovery readiness control 02	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						(logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-059	Recovery readiness control 03	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-060	Recovery readiness control 04	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-061	Recovery readiness control 05	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-062	Recovery readiness control 06	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-063	Recovery readiness control 07	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-064	Recovery readiness control 08	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-065	Recovery readiness control 09	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-066	Recovery readiness control 10	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-067	Recovery readiness control 11	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						with remediation tracking for Recovery exceptions.
DFIR-068	Recovery readiness control 12	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-069	Recovery readiness control 13	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.
DFIR-070	Recovery readiness control 14	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						Recovery exceptions.
DFIR-071	PostIncident readiness control 01	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-072	PostIncident readiness control 02	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-073	PostIncident readiness control 03	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
DFIR-074	PostIncident readiness control 04	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-075	PostIncident readiness control 05	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-076	PostIncident readiness control 06	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-077	PostIncident readiness control	GAP	2	0	3	Policy/procedure artifact showing

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
	07					ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-078	PostIncident readiness control 08	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-079	PostIncident readiness control 09	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
DFIR-080	PostIncident readiness control 10	GAP	5	0	3	Policy/procedure artifact showing ownership and cadence for

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
`DFIR-081`	PostIncident readiness control 11	GAP	1	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
`DFIR-082`	PostIncident readiness control 12	GAP	2	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
`DFIR-083`	PostIncident readiness control 13	GAP	3	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records

CONTROL_ID	TITLE	STATUS	SEVERITY	EVIDENCE_COUNT	MISSING_EVIDENCE	EVIDENCE EXPECTATIONS
						(logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.
`DFIR-084`	PostIncident readiness control 14	GAP	4	0	3	Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

Evidence Appendix

`DFIR-001` - Preparation readiness control 01

GAP | severity 1 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` - incident response plan evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` **- chain-of-custody template evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` **- escalation matrix evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` **- training exercise records evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` **- tabletop outcomes evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` **- post-incident review minutes evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-002` - Preparation readiness control 02

GAP | severity 2 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` **- incident response plan evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` **- escalation matrix evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` **- training exercise records evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` **- tabletop outcomes evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` **- post-incident review minutes evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` **- lessons learned register evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-003` - Preparation readiness control 03

GAP | severity 3 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating

Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` - incident response plan evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-002` - communications playbook evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` - escalation matrix evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` - training exercise records evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` - tabletop outcomes evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-004` - Preparation readiness control 04

GAP | severity 4 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` - incident response plan evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-002` - communications playbook evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` - training exercise records evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` - tabletop outcomes evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-005` - Preparation readiness control 05

GAP | severity 5 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` - incident response plan evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-002` - communications playbook evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-003` - stakeholder contact list evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` - training exercise records evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` - tabletop outcomes evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` **- policy update changelog evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` **- control improvement backlog evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-006` - Preparation readiness control 06

GAP | severity 1 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` **- incident response plan evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-002` **- communications playbook evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-003` **- stakeholder contact list evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` **- tabletop outcomes evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` **- control improvement backlog evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` **- executive briefing records evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-007` - Preparation readiness control 07

GAP | severity 2 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-001` **- incident response plan evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-002` **- communications playbook evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-003` **- stakeholder contact list evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-004` **- evidence handling standards evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-008` **- tabletop outcomes evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` **- executive briefing records evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` **- regulator/customer comms log evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-008` - Preparation readiness control 08

GAP | severity 3 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating

Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-002` - communications playbook evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-003` - stakeholder contact list evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-004` - evidence handling standards evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-009` - Preparation readiness control 09

GAP | severity 4 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-002` **- communications playbook evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-003` **- stakeholder contact list evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-004` **- evidence handling standards evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` **- chain-of-custody template evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` **- evidence retention decisions evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-010` - Preparation readiness control 10

GAP | severity 5 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-003` **- stakeholder contact list evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-004` **- evidence handling standards evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` **- chain-of-custody template evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-011` - Preparation readiness control 11

GAP | severity 1 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-003` **- stakeholder contact list evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-004` **- evidence handling standards evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` **- chain-of-custody template evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` **- escalation matrix evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-012` - Preparation readiness control 12

GAP | severity 2 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-004` **- evidence handling standards evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` **- chain-of-custody template evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` **- escalation matrix evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-013` - Preparation readiness control 13

GAP | severity 3 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-004` **- evidence handling standards evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` **- chain-of-custody template evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` **- escalation matrix evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` **- training exercise records evidence owner review log ticket runbook timeline**

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-014` - Preparation readiness control 14

GAP | severity 4 | evidence_count 0

Ensure Preparation procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Preparation.; Operational records (logs, tickets, reports, or runbooks) demonstrating Preparation execution.; Review evidence with remediation tracking for Preparation exceptions.

`DFIR-Q-005` - chain-of-custody template evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` - escalation matrix evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` - training exercise records evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-015` - DetectionAnalysis readiness control 01

GAP | severity 1 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-001` - incident response plan evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-009` **- edr telemetry evidence evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-013` **- ioc tracking artifacts evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` **- time sync ntp evidence evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` **- logging retention policy evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` **- admin account monitoring records evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-016` - DetectionAnalysis readiness control 02

GAP | severity 2 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-001` - incident response plan evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-002` - communications playbook evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-009` - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` - time sync ntp evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-017` - DetectionAnalysis readiness control 03

GAP | severity 3 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-002` - communications playbook evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-003` - stakeholder contact list evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-009` - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-010` - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` - time sync ntp evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

DFIR-Q-016 - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

DFIR-018 - DetectionAnalysis readiness control 04

GAP | severity 4 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

DFIR-Q-003 - stakeholder contact list evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

DFIR-Q-004 - evidence handling standards evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

DFIR-Q-009 - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

DFIR-Q-010 - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-019` - DetectionAnalysis readiness control 05

GAP | severity 5 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-004` - evidence handling standards evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-005` - chain-of-custody template evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-009` - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-010` - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-020` - DetectionAnalysis readiness control 06

GAP | severity 1 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-005` - chain-of-custody template evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-006` - escalation matrix evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-009` - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-010` - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-021` - DetectionAnalysis readiness control 07

GAP | severity 2 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-006` - escalation matrix evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-007` - training exercise records evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

`DFIR-Q-009` - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-010` - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-012` - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

DFIR-022 - DetectionAnalysis readiness control 08

GAP | severity 3 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

DFIR-Q-007 - training exercise records evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

DFIR-Q-008 - tabletop outcomes evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

DFIR-Q-010 - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

DFIR-Q-011 - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-012 - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-023 - DetectionAnalysis readiness control 09

GAP | severity 4 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

DFIR-Q-008 - tabletop outcomes evidence owner review log ticket runbook timeline

tags: preparation, planning, governance, readiness, incident_response, dfir | hits: 0

No direct evidence hits for this query.

DFIR-Q-010 - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

DFIR-Q-011 - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-012 - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-013 - ioc tracking artifacts evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-024 - DetectionAnalysis readiness control 10

GAP | severity 5 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-012` - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-013` - ioc tracking artifacts evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-025` - DetectionAnalysis readiness control 11

GAP | severity 1 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-012` - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-013` - ioc tracking artifacts evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` - time sync ntp evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-026` - DetectionAnalysis readiness control 12

GAP | severity 2 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-012` - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-013` - ioc tracking artifacts evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` - time sync ntp evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-027` - DetectionAnalysis readiness control 13

GAP | severity 3 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-012` **- forensic timeline notes evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-013` **- ioc tracking artifacts evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` **- time sync ntp evidence evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` **- logging retention policy evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-028` - DetectionAnalysis readiness control 14

GAP | severity 4 | evidence_count 0

Ensure DetectionAnalysis procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for DetectionAnalysis.; Operational records (logs, tickets, reports, or runbooks) demonstrating DetectionAnalysis execution.; Review evidence with remediation tracking for DetectionAnalysis exceptions.

`DFIR-Q-013` **- ioc tracking artifacts evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` - time sync ntp evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-029` - Containment readiness control 01

GAP | severity 1 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-009` - edr telemetry evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` **- endpoint quarantine actions evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` **- containment approval trail evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` **- containment verification checks evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-030` - Containment readiness control 02

GAP | severity 2 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-009` **- edr telemetry evidence evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-010` - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` - containment verification checks evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-031` - Containment readiness control 03

GAP | severity 3 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating

Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-010` - siem alert triage logs evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` - containment verification checks evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-032` - Containment readiness control 04

GAP | severity 4 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-011` - incident classification records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-012` - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` - containment verification checks evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-033` - Containment readiness control 05

GAP | severity 5 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-012` - forensic timeline notes evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-013` - ioc tracking artifacts evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` - containment verification checks evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-034` - Containment readiness control 06

GAP | severity 1 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-013` - ioc tracking artifacts evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-014` - time sync ntp evidence evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` **- host isolation records evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` **- network segmentation indicators evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-019` **- access revocation logs evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` **- containment verification checks evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-035` - Containment readiness control 07

GAP | severity 2 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-014` **- time sync ntp evidence evidence owner review log ticket runbook timeline**

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync | hits: 0

No direct evidence hits for this query.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-017` - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` - containment verification checks evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-036` - Containment readiness control 08

GAP | severity 3 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-015` - logging retention policy evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring | hits: 0

No direct evidence hits for this query.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-037` - Containment readiness control 09

GAP | severity 4 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-016` - admin account monitoring records evidence owner review log ticket runbook timeline

tags: detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-038` - Containment readiness control 10

GAP | severity 5 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-039` - Containment readiness control 11

GAP | severity 1 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-040` - Containment readiness control 12

GAP | severity 2 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating

Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-041` - Containment readiness control 13

GAP | severity 3 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-042` - Containment readiness control 14

GAP | severity 4 | evidence_count 0

Ensure Containment procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Containment.; Operational records (logs, tickets, reports, or runbooks) demonstrating Containment execution.; Review evidence with remediation tracking for Containment exceptions.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-023 - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-043 - Eradication readiness control 01

GAP | severity 1 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

DFIR-Q-017 - host isolation records evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-025 - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

DFIR-Q-029 - vulnerability closure notes evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` **- persistence hunting artifacts evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-031` **- root cause remediation tickets evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-032` **- change management records evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-044` - Eradication readiness control 02

GAP | severity 2 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-017` **- host isolation records evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-018` **- network segmentation indicators evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-025 - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

DFIR-Q-030 - persistence hunting artifacts evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-031 - root cause remediation tickets evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-032 - change management records evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

DFIR-045 - Eradication readiness control 03

GAP | severity 3 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

DFIR-Q-018 - network segmentation indicators evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` - credential reset evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` - persistence hunting artifacts evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-031` - root cause remediation tickets evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-032` - change management records evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-046` - Eradication readiness control 04

GAP | severity 4 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-019` - access revocation logs evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` - credential reset evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-031` - root cause remediation tickets evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-032` - change management records evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-047` - Eradication readiness control 05

GAP | severity 5 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-020` - temporary firewall changes evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-021` - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

DFIR-Q-026 - credential reset evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

DFIR-Q-027 - patch deployment logs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-031 - root cause remediation tickets evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-032 - change management records evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

DFIR-048 - Eradication readiness control 06

GAP | severity 1 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

DFIR-Q-021 - privileged account disablement evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access | hits: 0

No direct evidence hits for this query.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` - credential reset evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-027` - patch deployment logs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-032` - change management records evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-049` - Eradication readiness control 07

GAP | severity 2 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-022` - endpoint quarantine actions evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-023` - containment approval trail evidence owner review log ticket runbook timeline

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` - credential reset evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-027` - patch deployment logs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-028` - hardening checklist outputs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-032` **- change management records evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-050` - Eradication readiness control 08

GAP | severity 3 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-023` **- containment approval trail evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-024` **- containment verification checks evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` **- credential reset evidence evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-027` **- patch deployment logs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-028` **- hardening checklist outputs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-051` - Eradication readiness control 09

GAP | severity 4 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-024` **- containment verification checks evidence owner review log ticket runbook timeline**

tags: containment, isolation, segmentation, response, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` **- credential reset evidence evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-027` **- patch deployment logs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-028` **- hardening checklist outputs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-029` **- vulnerability closure notes evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-052` - Eradication readiness control 10

GAP | severity 5 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-027` **- patch deployment logs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-028` **- hardening checklist outputs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-029` **- vulnerability closure notes evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-053` - Eradication readiness control 11

GAP | severity 1 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-027` **- patch deployment logs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-028` **- hardening checklist outputs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-029` **- vulnerability closure notes evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` **- persistence hunting artifacts evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-054` - Eradication readiness control 12

GAP | severity 2 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-028` - hardening checklist outputs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-029` - vulnerability closure notes evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` - persistence hunting artifacts evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-055` - Eradication readiness control 13

GAP | severity 3 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-028` - hardening checklist outputs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-029` - vulnerability closure notes evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` **- persistence hunting artifacts evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-031` **- root cause remediation tickets evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-056` - Eradication readiness control 14

GAP | severity 4 | evidence_count 0

Ensure Eradication procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Eradication.; Operational records (logs, tickets, reports, or runbooks) demonstrating Eradication execution.; Review evidence with remediation tracking for Eradication exceptions.

`DFIR-Q-029` **- vulnerability closure notes evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` **- persistence hunting artifacts evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-031` **- root cause remediation tickets evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-057` - Recovery readiness control 01

GAP | severity 1 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-037` - recovery communications evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` - recovery validation metrics evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` - post-recovery monitoring evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` - customer impact closure notes evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-058` - Recovery readiness control 02

GAP | severity 2 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-025` - malware removal evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-026` - credential reset evidence evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` **- recovery validation metrics evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` **- post-recovery monitoring evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` **- customer impact closure notes evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-059` - Recovery readiness control 03

GAP | severity 3 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-026` **- credential reset evidence evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-027` **- patch deployment logs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` - restore test reports evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` - recovery validation metrics evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` - post-recovery monitoring evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` - customer impact closure notes evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-060` - Recovery readiness control 04

GAP | severity 4 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-027` - patch deployment logs evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-028` **- hardening checklist outputs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` **- backup status evidence evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` **- restore test reports evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` **- post-recovery monitoring evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` **- customer impact closure notes evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-061` - Recovery readiness control 05

GAP | severity 5 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-028` **- hardening checklist outputs evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-029` **- vulnerability closure notes evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` **- backup status evidence evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` **- restore test reports evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-035` **- service restoration runbooks evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` **- post-recovery monitoring evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` - customer impact closure notes evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-062` - Recovery readiness control 06

GAP | severity 1 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-029` - vulnerability closure notes evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-030` - persistence hunting artifacts evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` - restore test reports evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-035` - service restoration runbooks evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` - customer impact closure notes evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-063` - Recovery readiness control 07

GAP | severity 2 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-030` - persistence hunting artifacts evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-031` - root cause remediation tickets evidence owner review log ticket runbook timeline

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` **- restore test reports evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-035` **- service restoration runbooks evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-036` **- business continuity checkpoints evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` **- customer impact closure notes evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-064` - Recovery readiness control 08

GAP | severity 3 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-031` **- root cause remediation tickets evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-032` **- change management records evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` **- restore test reports evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-035` **- service restoration runbooks evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-036` **- business continuity checkpoints evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-065` - Recovery readiness control 09

GAP | severity 4 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-032` **- change management records evidence owner review log ticket runbook timeline**

tags: eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` **- restore test reports evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-035` **- service restoration runbooks evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-036` **- business continuity checkpoints evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-037` **- recovery communications evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-066` - Recovery readiness control 10

GAP | severity 5 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-035` **- service restoration runbooks evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-036` **- business continuity checkpoints evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-037` **- recovery communications evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-067` - Recovery readiness control 11

GAP | severity 1 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-035` **- service restoration runbooks evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-036` **- business continuity checkpoints evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-037` **- recovery communications evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` **- recovery validation metrics evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-068 - Recovery readiness control 12

GAP | severity 2 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

DFIR-Q-036 - business continuity checkpoints evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-Q-037 - recovery communications evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

DFIR-Q-038 - recovery validation metrics evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

DFIR-069 - Recovery readiness control 13

GAP | severity 3 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

DFIR-Q-036 - business continuity checkpoints evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-037` **- recovery communications evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` **- recovery validation metrics evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` **- post-recovery monitoring evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-070` - Recovery readiness control 14

GAP | severity 4 | evidence_count 0

Ensure Recovery procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for Recovery.; Operational records (logs, tickets, reports, or runbooks) demonstrating Recovery execution.; Review evidence with remediation tracking for Recovery exceptions.

`DFIR-Q-037` **- recovery communications evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` **- recovery validation metrics evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` - post-recovery monitoring evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-071` - PostIncident readiness control 01

GAP | severity 1 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-072` - PostIncident readiness control 02

GAP | severity 2 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-033` - backup status evidence evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-Q-034` - restore test reports evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-073` - PostIncident readiness control 03

GAP | severity 3 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-034` - restore test reports evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-035` - service restoration runbooks evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-074` - PostIncident readiness control 04

GAP | severity 4 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-035` - service restoration runbooks evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-036` - business continuity checkpoints evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-075` - PostIncident readiness control 05

GAP | severity 5 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-036` - business continuity checkpoints evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-037` - recovery communications evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` **- regulator/customer comms log evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` **- evidence retention decisions evidence owner review log ticket runbook timeline**

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-076` - PostIncident readiness control 06

GAP | severity 1 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-037` **- recovery communications evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-038` **- recovery validation metrics evidence owner review log ticket runbook timeline**

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-077` - PostIncident readiness control 07

GAP | severity 2 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-038` - recovery validation metrics evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-039` - post-recovery monitoring evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-041` - post-incident review minutes evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-048` - evidence retention decisions evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics | hits: 0

No direct evidence hits for this query.

`DFIR-078` - PostIncident readiness control 08

GAP | severity 3 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-039` - post-recovery monitoring evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-040` - customer impact closure notes evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-079` - PostIncident readiness control 09

GAP | severity 4 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-040` - customer impact closure notes evidence owner review log ticket runbook timeline

tags: recovery, backup, restore, continuity, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-Q-042` - lessons learned register evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-080` - PostIncident readiness control 10

GAP | severity 5 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-081` - PostIncident readiness control 11

GAP | severity 1 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-043` - corrective action tracker evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-082` - PostIncident readiness control 12

GAP | severity 2 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating

PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-083` - PostIncident readiness control 13

GAP | severity 3 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-044` - policy update changelog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management | hits: 0

No direct evidence hits for this query.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

`DFIR-084` - PostIncident readiness control 14

GAP | severity 4 | evidence_count 0

Ensure PostIncident procedures are documented, exercised, and reproducible for incident response readiness.

Expected evidence: Policy/procedure artifact showing ownership and cadence for PostIncident.; Operational records (logs, tickets, reports, or runbooks) demonstrating PostIncident execution.; Review evidence with remediation tracking for PostIncident exceptions.

`DFIR-Q-045` - control improvement backlog evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-046` - executive briefing records evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness | hits: 0

No direct evidence hits for this query.

`DFIR-Q-047` - regulator/customer comms log evidence owner review log ticket runbook timeline

tags: postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications | hits: 0

No direct evidence hits for this query.

Query Log

QUERY_ID	QUERY_TEXT	TAGS	HITS
`DFIR-Q-001`	incident response plan evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
`DFIR-Q-002`	communications playbook evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir, communications	0
`DFIR-Q-003`	stakeholder contact list evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
`DFIR-Q-004`	evidence handling standards evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics	0
`DFIR-Q-005`	chain-of-custody template evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics	0
`DFIR-Q-006`	escalation matrix evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
`DFIR-Q-007`	training exercise records evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
`DFIR-Q-008`	tabletop outcomes evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
`DFIR-Q-009`	edr telemetry evidence evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics	0
`DFIR-Q-010`	siem alert triage logs evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring	0
`DFIR-Q-011`	incident classification records evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness	0
`DFIR-Q-012`	forensic timeline notes evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness	0

QUERY_ID	QUERY_TEXT	TAGS	HITS
DFIR-Q-013	ioc tracking artifacts evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness	0
DFIR-Q-014	time sync ntp evidence evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync	0
DFIR-Q-015	logging retention policy evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring	0
DFIR-Q-016	admin account monitoring records evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access	0
DFIR-Q-017	host isolation records evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-018	network segmentation indicators evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-019	access revocation logs evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-020	temporary firewall changes evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management	0
DFIR-Q-021	privileged account disablement evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access	0
DFIR-Q-022	endpoint quarantine actions evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-023	containment approval trail evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-024	containment verification checks evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-025	malware removal evidence evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics	0
DFIR-Q-026	credential reset evidence evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics	0
DFIR-Q-027	patch deployment logs evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-028	hardening checklist outputs evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-029	vulnerability closure notes evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-030	persistence hunting artifacts evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0

QUERY_ID	QUERY_TEXT	TAGS	HITS
DFIR-Q-031	root cause remediation tickets evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-032	change management records evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management	0
DFIR-Q-033	backup status evidence evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics	0
DFIR-Q-034	restore test reports evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-035	service restoration runbooks evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-036	business continuity checkpoints evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-037	recovery communications evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness, communications	0
DFIR-Q-038	recovery validation metrics evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-039	post-recovery monitoring evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-040	customer impact closure notes evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness, communications	0
DFIR-Q-041	post-incident review minutes evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-042	lessons learned register evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-043	corrective action tracker evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-044	policy update changelog evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management	0
DFIR-Q-045	control improvement backlog evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-046	executive briefing records evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-047	regulator/customer comms log evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications	0
DFIR-Q-048	evidence retention decisions evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics	0

Query Log

QUERY_ID	QUERY_TEXT	TAGS	HITS
DFIR-Q-001	incident response plan evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
DFIR-Q-002	communications playbook evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir, communications	0
DFIR-Q-003	stakeholder contact list evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
DFIR-Q-004	evidence handling standards evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics	0
DFIR-Q-005	chain-of-custody template evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir, evidence, forensics	0
DFIR-Q-006	escalation matrix evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
DFIR-Q-007	training exercise records evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
DFIR-Q-008	tabletop outcomes evidence owner review log ticket runbook timeline	preparation, planning, governance, readiness, incident_response, dfir	0
DFIR-Q-009	edr telemetry evidence evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring, evidence, forensics	0
DFIR-Q-010	siem alert triage logs evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring	0
DFIR-Q-011	incident classification records evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness	0
DFIR-Q-012	forensic timeline notes evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness	0
DFIR-Q-013	ioc tracking artifacts evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness	0
DFIR-Q-014	time sync ntp evidence evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, evidence, forensics, time_sync	0
DFIR-Q-015	logging retention policy evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, logging, monitoring	0
DFIR-Q-016	admin account monitoring records evidence owner review log ticket runbook timeline	detection, analysis, triage, telemetry, incident_response, dfir, readiness, privileged_access	0
DFIR-Q-017	host isolation records evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0

QUERY_ID	QUERY_TEXT	TAGS	HITS
DFIR-Q-018	network segmentation indicators evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-019	access revocation logs evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-020	temporary firewall changes evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness, change_management	0
DFIR-Q-021	privileged account disablement evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness, privileged_access	0
DFIR-Q-022	endpoint quarantine actions evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-023	containment approval trail evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-024	containment verification checks evidence owner review log ticket runbook timeline	containment, isolation, segmentation, response, incident_response, dfir, readiness	0
DFIR-Q-025	malware removal evidence evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics	0
DFIR-Q-026	credential reset evidence evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness, evidence, forensics	0
DFIR-Q-027	patch deployment logs evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-028	hardening checklist outputs evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-029	vulnerability closure notes evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-030	persistence hunting artifacts evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-031	root cause remediation tickets evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness	0
DFIR-Q-032	change management records evidence owner review log ticket runbook timeline	eradication, remediation, patching, hardening, incident_response, dfir, readiness, change_management	0
DFIR-Q-033	backup status evidence evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness, evidence, forensics	0
DFIR-Q-034	restore test reports evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-035	service restoration runbooks evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0

QUERY_ID	QUERY_TEXT	TAGS	HITS
DFIR-Q-036	business continuity checkpoints evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-037	recovery communications evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness, communications	0
DFIR-Q-038	recovery validation metrics evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-039	post-recovery monitoring evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness	0
DFIR-Q-040	customer impact closure notes evidence owner review log ticket runbook timeline	recovery, backup, restore, continuity, incident_response, dfir, readiness, communications	0
DFIR-Q-041	post-incident review minutes evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-042	lessons learned register evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-043	corrective action tracker evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-044	policy update changelog evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, change_management	0
DFIR-Q-045	control improvement backlog evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-046	executive briefing records evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness	0
DFIR-Q-047	regulator/customer comms log evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, communications	0
DFIR-Q-048	evidence retention decisions evidence owner review log ticket runbook timeline	postincident, lessons_learned, improvement, governance, incident_response, dfir, readiness, evidence, forensics	0