ResolvX

Tabletop Exercise Report

Operation Locked Gate - Ransomware Scenario

IR-TTX-001 - v1.0 - 2026-02-14 - Internal - Restricted

Exercise Overview

Exercise Title	Operation Locked Gate
Exercise Type	Tabletop Discussion Exercise
Date Conducted	2026-02-14
Duration	3 hours (09:00 - 12:00)
Facilitator	GRC Lead - Derick G. Dmello
Observer	CISO
Scenario Summary	Ransomware infection from spear phishing; lateral movement to AWS EC2; data exfiltration before encryption; ransom demand received
IR Plan Version Tested	IR-PLAN-001 v1.0
Overall Rating	SATISFACTORY - Sound foundational capability; 3 medium findings; no critical gaps

Scenario: Operation Locked Gate

A threat actor sent a spear phishing email to ResolvX's Head of Finance, impersonating a client contact. The email contained a malicious attachment that, when opened, deployed a loader which established a beaconing connection to a command-and-control server. Over the following 48 hours the attacker moved laterally from the Finance endpoint into ResolvX's AWS environment via stored credentials found in a local browser cache. The attacker exfiltrated approximately 4.2 GB of data before deploying ransomware across 3 EC2 instances and the shared drive. A ransom note demanding payment in cryptocurrency was left on affected systems. AWS GuardDuty and Datadog both generated alerts which were unacknowledged for 2 hours before being discovered by the Head of Cloud Ops on a routine morning check.

The exercise tested the team's ability to execute IR-PLAN-001, the Ransomware Runbook (IR-RB-002), and the Data Breach Runbook (IR-RB-003) across all four NIST SP 800-61 phases - from detection through to recovery planning and regulatory notification decisions.

Participants

Role	Function in Exercise	Attended
GRC Lead	Incident Commander / Facilitator	Yes
CISO	Executive decision-maker / Observer	Yes
Head of Cloud Ops	Technical Lead - AWS isolation and recovery	Yes
IT Admin	Identity response; endpoint isolation via Jamf	Yes
DevSecOps Engineer	Malware analysis; secrets rotation	Yes
Legal Counsel (external)	GDPR notification decisions; law enforcement	Yes
VP Engineering	Recovery prioritisation; RTO planning	Yes
Head of HR	Personnel actions; awareness comms	Yes

Key Findings

ID	Finding	Severity	Detail	Resolution
F-001	**Terminate vs. Isolate Confusion**	Medium	Team initially proposed terminating compromised EC2 instances rather than isolating them. Termination destroys volatile memory, prevents EBS snapshot capture, and eliminates forensic evidence. The runbook IR-RB-002 has been updated to explicitly prohibit termination before isolation and snapshot.	IR-RB-002 updated; covered in next awareness briefing
F-002	**GDPR Notification Trigger Ambiguity**	Medium	Team was uncertain whether data exfiltration without confirmed access to specific records triggers GDPR Art. 33 notification. Clarified: exfiltration of personal data is a notifiable	IR-RB-003 updated; Legal to run GDPR

			breach regardless of whether encryption also occurred. IR-RB-003 and the Privacy Programme (POL-006) updated to include this clarification.	refresher by 2026-03-15
F-003	**Credential Rotation Scope Underestimated**	**Medium**	Team proposed rotating only credentials belonging to confirmed compromised accounts. Correct response for P1 ransomware is organisation-wide credential rotation - the assumption must be that all credentials stored anywhere on affected systems are compromised. IR-PLAN-001 Section 4.3.3 updated.	IR-PLAN-001 updated; added to security awareness content
F-004	**Out-of-Band Communications - Positive Finding**	**Positive**	The Signal IRT group was activated within 3 minutes of P1 declaration and used throughout the exercise. No sensitive incident details were shared on corporate Slack. This is a strong positive finding demonstrating effective preparation.	No action required
F-005	**Backup Readiness - Positive Finding**	**Positive**	Head of Cloud Ops confirmed AWS backup integrity and provided a credible RTO estimate within 45 minutes of the exercise start. The team made the correct decision to prioritise recovery over ransom payment, citing confirmed backup availability.	No action required
F-006	**Legal On-Call Response Time**	**Low**	External Legal counsel joined the exercise 12 minutes after being paged. For a real P1 incident this is acceptable, but a target of 5 minutes has been set. A standing on-call arrangement is being formalised in the retainer contract.	Legal on-call SLA to be formalised by 2026-03-31

Action Items

Action	Owner	Due	Status
Update IR-RB-002: prohibit terminating isolated instances before EBS snapshot	GRC Lead	2026-02-21	**Complete**
Update IR-RB-003: clarify exfiltration triggers GDPR notification regardless of encryption	GRC Lead	2026-02-21	**Complete**
Update IR-PLAN-001 Section 4.3.3: org-wide credential rotation for P1 ransomware	GRC Lead	2026-02-21	**Complete**
Formalise Legal on-call 5-minute SLA in retainer contract	Legal / GRC Lead	2026-03-31	**In Progress**
Run GDPR breach notification refresher for all IRT members	GRC Lead + Legal	2026-03-15	**Planned**
Include credential rotation scope in annual security awareness training	GRC Lead	2026-04-01	**Planned**
Schedule Tabletop Exercise 2 - Scenario: Vendor Data Breach	GRC Lead	2026-08-01	**Planned**

Conclusion

Overall Assessment: SATISFACTORY

The ResolvX IRT demonstrated sound foundational incident response capability during **Operation Locked Gate**. The team correctly applied the NIST SP 800-61 lifecycle, made appropriate containment decisions, and engaged Legal at the right stage for regulatory notification assessment.

Three medium findings were identified and all have been remediated through updates to IR-PLAN-001, IR-RB-002, and IR-RB-003. No critical gaps were found - the plan is fit for purpose with the documented updates applied. No major structural changes to the IR programme are required at this stage.

The next exercise (Tabletop 2, target August 2026) will test the data breach via vendor scenario, exercising IR-RB-003, POL-005 (Vendor Management), and POL-006 (Privacy Programme) together.

Document Control

Document ID	IR-TTX-001
Version	1.0
Exercise Date	2026-02-14
Report Author	GRC Lead - Derick G. Dmello
Reviewed By	CISO
Classification	Internal - Restricted
Retention	5 years
Framework References	NIST SP 800-61 Rev 2 s.3.4.1 - ISO/IEC 27001:2022 A5.27 - SOC 2 CC7.5