Incident & Evidence Note – HC-IR-1066

Timestamp & Context

- 2025-09-11T13:45:00Z – Incident Manager John Smith created ticket HC-IR-1066 after automated alert flagged unauthenticated email sent to student Sam Rivera.
- Scope: Inspect IdP logs ±15 minutes from email delivery and capture suspicious email metadata.

Authorization

- John Smith (Incident Manager) approved collection of:
  - IdP sign-in records for Sam Rivera, 2025-09-11T13:30-14:00Z.
  - Suspicious email header (.eml, metadata only).
- No additional assets or bulk mailbox content authorized.

Actions Taken

- 13:47Z – Queried IdP logs for Sam Rivera in approved window.
- 13:50Z – Exported suspicious email header (.eml format).
- 13:52Z – Generated SHA-256 hashes for both artifacts.
- 13:55Z – Uploaded artifacts to secure evidence repository; logged chain-of-custody.

Evidence Captured

- EV-001 – `HC-IR-1066-email-header.eml` - SHA-256: `b2e70976a832a7a5c1ef979042a3cdac4cbea710dbcd0e69eb405f2d258c2346`
  - Why: Minimum necessary metadata to confirm authentication alignment (SPF/DKIM/DMARC) and detect spoofing.
- EV-002 – `HC-IR-1066-idp-logs-1330-1400.csv` - SHA-256: `c52df5aa4ff5507ecf844a98edd42309d4266f41747bd09264b79f6047320769`
  - Why: Limited log segment showing login activity near phishing email; filtered to Sam Rivera only to protect unrelated users.

Chain of Custody

Time (UTC	ItemID	From	To	Location	Action	Sign/ID
13:52Z	EV-001	Collector	Evidence Repo	`/evidence/HC-IR-1066/EV-001`	Intake + hash	JD

13:52Z	EV-002	Collector	Evidence Repo	`/evidence/HC-IR-1066/EV-002`	Intake + hash	JD
13:55Z	EV-001/002	Evidence Repo	IR Manager Review	Same	Accessed for decision	JS

Redaction

- Masked Sam Rivera's email -> `studentID@redacted.edu`
- Filtered IdP log (.csv) to Sam Rivera's records only; removed all other user entries.
- Removed non-target IP addresses from log output.
- Documented edits ("PII redacted") in evidence manifest.

Next Step Recommendation

- Recommend soft containment (per NIST/CSF "Respond" phase and SWGDE proportionality guidance):
  - Quarantine suspicious email.
  - Reset Sam Rivera's password; revoke active sessions/tokens.
  - Block look-alike domain `blackb0ard-mail.support` at mail gateway.
- Handoff: containment/recovery actions to IdP Manager and Mail Security Team.