NeoPay Incident Response (IR) Simulation

WE Innovate X Zero$ploit

Supervised by : Muhammed Badawy

Incident Response Team:

Omar Hassan – Ali Abdelrahman – Ahmed Thabet – Noha ElSayed

Version: *1.0*
Owner: *SOC Lead, NeoPay Global*
Planned Duration: *4–6 hours (tabletop first, optional live-fire lab)*
Timezone: *Africa/Cairo (UTC+3)*

---

1) Purpose and Outcomes

Purpose
Run a realistic, fintech-focused incident simulation to train SOC analysts, IR team, and stakeholders to detect, contain, and recover from a multi-vector intrusion.

Learning Outcomes

- Practice rapid triage with incomplete data.
- Coordinate across SOC, Incident Command, Forensics, IT Ops, Legal, and Comms.
- Exercise containment decisions under business pressure.
- Produce regulator-ready documentation and after-action improvements.

---

2) Scenario Background

Organization: NeoPay Global, a Cairo-based fintech handling digital payments, mobile wallets, and Open Banking APIs.

Threat Actor: Glass Jackal, a financially motivated group targeting payment platforms.
Primary Objectives: Exfiltrate wallet tokens, pivot to cloud payment keys, and attempt fraudulent test transactions.
Initial Foothold: Spearphish a helpdesk user with a ticket-reply lure that harvests credentials and MFA via reverse-proxy phishing kit.
Complications: A developer's GitHub PAT leaked in an old CI job artifact, enabling read access to a private repo with a misconfigured test Stripe key.

High-level Kill Chain

1. Recon on employee LinkedIn and public job boards.
2. Phishing page proxied to Okta sign-in.
3. Conditional access bypass using attacker-owned residential IP pool.
4. Device registration of a rogue compliant device.
5. Cloud pivot to storage and CI secrets.
6. Test-mode fraud on payment gateway; attempt to swap to live secrets.

7. Exfiltration of select wallet refresh tokens and limited PII.

---

3) Exercise Objectives

- Detect phishing-driven cloud account compromise quickly.
- Identify and sever access paths: rogue device, sessions, tokens, and PATs.
- Contain fraud attempts on payment rails while keeping merchant uptime.
- Preserve evidence and maintain a defensible timeline.
- Communicate accurately to executives, partners, and regulators.

---

4) Scope and Rules of Engagement

- **In-scope systems:** Okta, Azure AD, Email, EDR on Windows endpoints, GitHub Enterprise, CI/CD, Payment Gateway keys, ELK/SIEM.
- **Out-of-scope:** Production transaction data modification, irreversible destructive actions.
- **Allowed controls during exercise:** Suspend user, revoke tokens, disable devices, rotate keys, network blocks, scripted queries in SIEM.
- **Evidence handling:** Chain of custody form for any disk or memory images.
- **Safety:** Do not run real malware. Use test indicators and synthetic payloads.

---

5) Roles and Responsibilities

- **Incident Commander (IC):** Owns decisions, timeline, priorities, approvals.
- **SOC L1:** Monitor alerts, perform initial triage and ticketing.
- **SOC L2/IR Analyst:** Lead investigation, correlation, and scoping.
- **Forensics:** Imaging, volatile data capture, log preservation.
- **Threat Intel:** Enrichment, ATT&CK mapping, IOCs.
- **IT Ops / Cloud:** Account controls, token revocation, key rotation.
- **Payments SME:** Stripe keys, transaction monitoring, merchant comms.
- **Legal & Compliance:** Regulator liaison, breach assessment.
- **Comms/PR:** Internal and external messaging.
- **Exercise Controller (White Team):** Delivers injects and evaluates.

---

6) Timeline and Injects (Tabletop)

Duration target: 4 hours. White Team releases injects by time.

Time (hh:mm)	Inject	Content	Expected Actions
00:00	Kickoff	Short briefing, rules, objectives	Confirm roles, start logging timeline
00:15	Phish Alert	Helpdesk user reports odd Okta prompt loop	SIEM search for Okta sign-in anomalies; check recent MFA push spam
00:30	Alert Burst	Okta sign-in from new device, Cairo IP, then residential IP outside Egypt	Validate impossible travel, device registration event, conditional access check, suspend user
00:45	EDR Hit	Sysmon ID 3 outbound to phishing infra, Chrome extension installed recently	Isolate endpoint, preserve volatile data, capture browser artifacts
01:10	Cloud Signal	Azure audit shows new device compliant via Intune spoof	Revoke device token, block, force reauth, review Intune compliance policies
01:30	Secret Exposure	GitHub audit log: PAT used from unusual ASN to pull private repo	Revoke PAT, rotate repo deploy keys, check CI secrets history
02:00	Payment Noise	Stripe test-mode fraud spikes on “micro-refund” pattern	Rate-limit test keys, rotate keys, engage Payments SME, monitor live-mode
02:30	Data Risk	Small set of wallet refresh tokens accessed in storage logs	Invalidate tokens, force app re-login, notify product and support
03:00	Exec Ping	CEO requests business impact summary and ETA	Issue exec brief, outline containment and residual risk
03:30	Regulator Query	Compliance asks for 24-hour notification draft	Prepare draft notice, data classification, preliminary IOCs
04:00	Wrap	Stabilization and recovery checkpoints	Commit action items, schedule hot-wash

Optional Live-fire Lab: Replace alerts with lab SIEM queries and synthetic logs.

---

7) Evidence and Artifacts Pack (Synthetic)

Provide these to participants as downloadable or copy-paste snippets during the exercise.

Email Header Sample

- From: it-support@neopay-support[.]com
- Reply-To: noreply@neopay-support[.]com
- SPF: softfail
- URL: https://signin-neopay-okta[.]com/session

Suspicious Domains and IPs

- signin-neopay-okta[.]com
- assets-okta-sso[.]net
- 185.203.112[.]77

Okta Log Snippets

- eventType: user.authentication.sso
- client.device: Windows, new
- outcome.result: SUCCESS
- geo.city: Cairo, then Amman within 8 minutes

Sysmon Highlights

- Event ID 3: Network connection to 185.203.112[.]77:443 by chrome.exe
- Event ID 11: FileCreate for %LocalAppData%\Chrome\Extensions\…
- Event ID 1: powershell.exe with encoded command touching registry Run key

GitHub Enterprise Audit

- action: oauth_authorization.create
- user: svc-ci-runner
- token_scope: repo, read:packages
- actor_ip: 91.214.46[.]19

Payment Gateway Logs

- surge of refunds in test mode from 3 merchant test accounts
- attempts to access live secret via CI variable list

---

8) IR Plan and Playbooks

8.1 Preparation

- Validate on-call roster and contact tree.
- Ensure SIEM dashboards for Okta, Azure AD, EDR, GitHub, Gateway are ready.

- Pre-stage token revocation scripts and key rotation runbooks.
- Enable mailbox auditing and safe links.
- Label data assets by sensitivity with retention settings.

8.2 Identification

Triage Checklist

- Correlate Okta anomalies with endpoint and network telemetry.
- Confirm user action with helpdesk and phone verification.
- Determine scope: users, devices, repos, keys, tokens.
- Start incident timeline and Slack bridge channel.

Queries

- ELK: search signin anomalies by deviceId, geo, ASN.
- Okta: list active sessions for suspect user and device enrollment events.
- EDR: recent chrome extension installs and PowerShell suspicious CLI.
- GitHub: PAT creations and token use from new IPs.

8.3 Containment

- Disable affected accounts, revoke sessions, wipe or quarantine devices.
- Revoke PATs, rotate secrets in CI/CD and payment gateway.
- Add network blocks for indicators at proxy and firewall.
- Temporarily enforce step-up MFA and device posture checks org-wide.
- Enable rate limits and velocity rules on refunds.

8.4 Eradication

- Remove persistence: startup entries, scheduled tasks, OAuth consents.
- Validate device compliance, reimage if integrity is doubtful.
- Hunt for lateral movement in cloud audit and IAM role usage.
- Review repo history for additional secrets exposure.

8.5 Recovery

- Gradually restore normal access controls.
- Monitor for reauth attempts from indicators.
- Validate payment flows in both test and live modes.
- Communicate recovery status to merchants and partners.

8.6 Lessons Learned

- 48-hour hot-wash with timeline, what worked, what did not, and top fixes.
- Update phishing training and device compliance policies.
- Adopt short-lived tokens and secret scanning in CI.
- Add real-time anomaly detection for refund patterns.

---

9) Communications Plan

Channels: Slack incident-bridge, Email, Conference line.
Cadence: Hourly internal updates, executive brief at key milestones.
Decision Log: Time-stamped in the ticket system.

Templates

- **Internal Alert:**
  - Subject: Security Incident Bridge Activated
  - Body: We are investigating suspicious Okta activity affecting limited users. Join bridge: … Actions so far: … Next updates at HH:MM.
- **Executive Brief (1 page):**
  - What happened, scope, customer impact, controls applied, next steps, ETA.
- **Regulatory Draft:**
  - Incident summary, data categories involved, detection time, containment steps, contact for follow-up.
- **Merchant Notice (if needed):**
  - No live transaction impact detected. We rotated keys and invalidated tokens. Monitoring continues. Support contacts included.

---

10) Decision Trees

Okta Compromise Tree

- If new device + geo anomaly → revoke device + force reauth.
- If OAuth consent present → remove grant and audit usage.
- If helpdesk user targeted → review privileged workflows.

Secrets Exposure Tree

- Identify blast radius → rotate secrets → invalidate tokens → scan repos → enable secret scanning gates in CI → notify developers.

Payment Abuse Tree

- Flag pattern → throttle test mode → verify live mode isolation → monitor anomalies → engage risk engine.

---

11) Metrics and Scoring

- **MTTD:** minutes from first alert to confirmed incident.
- **MTTR-Contain:** minutes from confirmation to full containment.
- **Scope Accuracy:** percent of affected accounts correctly identified.
- **Evidence Quality:** chain of custody completeness.
- **Comms Effectiveness:** timeliness and clarity scores from execs.
- **Regulatory Readiness:** draft completed within 6 hours.

Rubric (out of 100)

- Detection 20
- Investigation 25
- Containment 25
- Communications 15
- Documentation 15

---

12) MITRE ATT&CK Mapping

- Initial Access: Phishing (T1566), Valid Accounts (T1078)
- Execution: Command and Scripting Interpr