1. Investigation Steps

Investigation steps are based on the incident response lifecycle which is focused on defending and recovering from attacks. The process includes preparing for potential incidents, detecting, and analyzing threats to recover the affected systems.

Log actions for a mock incident:

Time Stamp	Action
2025-10-10 13:27:00	Isolated affected user's device from the network.
2025-10-10 13:44:15	Suspicious login session terminated on the mail server.
2025-10-10 14:03:04	Collected memory dump from the isolated device for forensic analysis using velociraptor.
2025-10-10 14:30:25	No mail forwarding rules were created on the compromised user account.

2. Phishing Checklist

Phishing checklist created in google docs. This checklist helps to reduce human errors and provide clear, repeatable process for complex and higher security operations.

Initial Assessment

[ ] Confirm email headers.
[ ] Check link reputation via VirusTotal/URLScan.
[ ] Check file hash via VirusTotal.
[ ] Identify affected users.

Containment & Eradication

[ ] Force password reset for compromised users.
[ ] Block malicious IP at firewall.
[ ] Delete malicious emails from inboxes.

Post-Incident

[ ] Notify affected users and security awareness.
[ ] Incident Response Report.

3. Post-Mortem

Post-Mortem is an analysis of security incident or simulated attack to identify the root cause, evaluate the response. Summary of lessons learned from a simulated breach.

Simulated Scenario: The phishing incident had a minor data leak because the initial network isolation failed.

Lesson Learned: The failure to immediately isolate the endpoint allowed minor data access. I learned that network segmentation controls must be validated. The primary process improvement is the integration of an automated isolation step using a SOAR playbook.