# Incident Response Playbooks (SOPs)

## 1. Phishing Email Playbook

Objective: Contain and remediate phishing attempts to prevent credential theft, malware infection, or data exfiltration.

Detection & Triage: Monitor SIEM alerts, identify IOCs (domains, links, attachments).

Containment: Isolate mailboxes, block malicious domains, disable compromised accounts.

Eradication: Remove malicious emails from inboxes, patch email filtering systems.

Recovery: Reset compromised passwords, re-enable accounts, notify employees.

Post-Incident: Document IOCs, update blocklists, conduct phishing awareness training.

## 2. Ransomware Playbook

Objective: Minimize downtime and data loss while containing and eradicating ransomware infections.

Detection & Triage: Monitor unusual file encryption, ransom notes, and EDR alerts.

Containment: Isolate infected systems, disconnect backups, disable shared drives.

Eradication: Wipe and rebuild compromised machines, remove persistence, patch vulnerabilities.

Recovery: Restore from clean backups, validate data integrity, reconnect systems gradually.

Post-Incident: Conduct RCA, update detection signatures, report to legal/compliance if necessary.

## 3. Insider Threat Playbook

Objective: Identify and mitigate malicious or accidental insider behavior before it escalates.

Detection & Triage: Monitor for unusual data access, privilege escalations, or abnormal activity.

Containment: Limit access rights, suspend suspicious accounts pending investigation.

Eradication: Remove unauthorized files, revoke access privileges, secure systems.

Recovery: Reinstate legitimate access only after remediation, monitor probation period.

Post-Incident: HR/legal review, strengthen access controls, expand insider threat training.