Basic Incident Response Lifecycle

Section 1: The 6 Incident Response Phases

- Preparation – playbooks, rules, tools
- Identification – alert triage and confirmation
- Containment – isolate infected host
- Eradication – remove malware and close vulnerabilities
- Recovery – restore services and verify stability
- Lessons Learned – document and improve security

Section 2: Real-world example

1. Phishing email delivered malware to an employee device.
2. SOC identified malicious file hash using SIEM alerts.
3. The endpoint was isolated and malware was removed.
4. The system was restored from a clean backup.
5. A post-incident review recommended stronger email filtering.

Incident Response Documentation

1. Executive Summary

A phishing email containing a malicious attachment was detected on employee workstation WIN-USER-07. SOC responded by isolating the device, removing the malware, and restoring the system.

2. Timeline of Actions

Date & Time	Action
2025-08-18 10:35	Alert received from SIEM
2025-08-18 10:50	Workstation isolated
2025-08-18 11:10	Malware removed
2025-08-18 11:45	System restored from backup

3. Impact Analysis

Only one device was affected. No lateral movement or data exfiltration was detected.

4. Remediation Steps

- Isolated infected endpoint
- Removed malicious file
- Updated antivirus signatures
- Forced password reset for affected user
- Implemented email filtering rule to block similar threats

5. Lessons Learned

User awareness training should be improved, and suspicious email reporting should be encouraged.