

Module 4

Learn

- Playbook
- Six phases of incident response

Phase of incident response Playbook

Playbook: A manual that provides detail about any operational action

- Urgency • efficiency and accuracy
- Playbook clarify what tool should be to response to security incident

Incident Response: An organization's quick attempt to identify an attack, contain the damage, and correct the effect of a security breach

Phase:

- Preparation
- Detection and analysis
- Containment
- Eradication and recovery
- Post incident activity
- Coordination