7_Incident_Response_Basics

What to Learn

Incident response (IR) is the structured approach to managing and mitigating cyber incidents. It reduces damage and recovery costs.

IR phases include preparation, identification, containment, eradication, recovery, and lessons learned.

SOC analysts often serve as the frontline in incident detection and containment.

How to Learn

Study NIST and SANS incident response frameworks.

Review real-world IR case studies to understand how incidents unfold.

Practice tabletop exercises to build familiarity with IR processes.

Example / Use-Case

A ransomware attack is detected on an endpoint. The SOC isolates the machine (containment), wipes the malware (eradication), restores from backups (recovery), and later documents improvements to prevent future attacks (lessons learned).