6_Security_Operations_Workflow

What to Learn

A SOC follows structured workflows to ensure consistent and efficient response to alerts. Workflows define how alerts are triaged, escalated, and resolved.

Workflows often include alert intake, validation, classification, escalation, and closure.

Clear workflows reduce confusion and improve response times.

How to Learn

Study SOC workflow diagrams and standard operating procedures (SOPs).

Simulate mock incidents to see how workflows dictate analyst actions.

Compare workflows across organizations to understand variations in maturity.

Example / Use-Case

An alert on unusual outbound traffic is triaged by Tier 1, escalated to Tier 2 for investigation, and resolved by Tier 3 with a firewall block. The workflow ensures no stage is skipped.