2_Security_Monitoring_Basics

What to Learn

Security monitoring is the proactive observation of IT assets to detect anomalies, malicious activity, and performance issues. It forms the foundation of cyber defense.

Monitoring encompasses multiple layers: network monitoring, endpoint monitoring, application monitoring, and user activity tracking. Together, these layers provide visibility into the organization's threat landscape.

The goal is not only to identify threats but to reduce false positives and generate actionable alerts.

How to Learn

Students should begin by exploring system logs such as Windows Event Viewer and Linux syslog. Understanding the meaning of different event types provides context for monitoring alerts.

Hands-on practice with SIEM platforms (like Splunk or ELK) strengthens comprehension by showing how raw logs are transformed into dashboards and alerts.

Learning how to fine-tune detection rules helps analysts distinguish between benign anomalies and real threats.

Example / Use-Case

A sudden increase in outbound connections from a server is detected by monitoring tools. Analysts investigate and find a compromised account exfiltrating sensitive data.

This shows how monitoring helps detect and contain data breaches in real time.