4_Security_Tools_Overview

What to Learn

Security tools empower SOC analysts to detect, prevent, and respond to threats effectively. These include SIEM systems, intrusion detection systems, endpoint detection tools, and vulnerability scanners.

Each tool has its purpose, and together they create a layered defense strategy.

Knowing tool categories helps analysts understand when and why each is deployed.

How to Learn

Study the core functionality of tools such as Splunk (SIEM), Suricata (IDS), Wazuh (EDR), and Nessus (vulnerability scanning).

Reading documentation and following tutorials strengthens practical familiarity.

Simulated environments allow analysts to see how tools detect suspicious behavior in controlled scenarios.

Example / Use-Case

A SIEM correlates login attempts with IDS alerts to reveal a brute-force attack in progress. Without tool integration, the attack might have gone undetected.