3_Log_Management_Fundamentals

What to Learn

Log management is the systematic handling of log data generated by systems, applications, and security devices. It involves collecting, storing, normalizing, and analyzing logs.

Effective log management ensures that analysts can reconstruct incidents, understand attacker behavior, and fulfill compliance requirements.

Logs form the evidence backbone for security investigations.

How to Learn

Students should learn the types of logs: authentication logs, system logs, application logs, and firewall logs. Each log type provides a different perspective on security posture.

Exploring log retention strategies teaches how organizations balance cost with regulatory requirements.

Studying case studies on breaches shows how logs often serve as the first evidence of compromise.

Example / Use-Case

During an insider threat investigation, analysts review database logs and find unauthorized queries run after business hours. Log evidence reveals data theft, allowing response teams to take swift legal and technical actions.