Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - Windows Log Correlation and Analysis in Splunk



Analyze recovered Windows event logs in Splunk to reconstruct a cyberattack timeline. You'll correlate logon events, process executions, and service installations, then verify your conclusions on a compromised Windows machine.