Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - Elastic ML Advanced Investigation



Hunt for signs of SQL injection, command injection, and cross-site scripting in HTTP logs. Use Elastic ML and ES|QL to investigate anomalies and create a detection rule for a known pattern.