

Workflow Automation – Splunk Phantom Playbook

1. Objective

Reduce response time by automatically escalating High-severity alerts to SOC L2.

2. Playbook Logic

- **Trigger:** New alert ingestion
- **Condition:** Alert severity equals *High*
- **Automated Actions:**
 - Assign incident owner to SOC L2
 - Set priority to High
 - Add escalation note to the case
 - Notify L2 analysts

3. Test Result

A mock High-priority alert was processed successfully and automatically assigned to SOC L2, validating correct automation behavior.