🛠️ RUNBOOK 01 — Investigating Failed Logins

Step-by-Step

1. Run detection query
2. Adjust time range to last 15–60 minutes
3. Identify source IP
4. Count failures per user
5. Check for successful login after failures
6. Determine if brute force pattern exists
7. Document findings
8. Escalate if threshold exceeded

🛠️ RUNBOOK 02 — Privilege Escalation Investigation

1. Identify elevated event
2. Confirm user role
3. Review previous activity
4. Validate business justification
5. Escalate if unauthorized

🛠️ RUNBOOK 03 — New Service Investigation

1. Identify service creation event

2. Check service binary path
3. Verify digital signature
4. Search for similar events
5. Disable service if malicious
6. Escalate