

Security Incident Playbook

Triage Rules

- HIGH risk: failed login burst + new country OR night access + device mismatch OR failed login burst + device mismatch.
- MED risk: either failed login burst (below escalation threshold) OR night access alone OR new country alone OR new device alone.

Operator Actions

Failed Login Burst

- Confirm source IP reputation and ASN.
- If failures exceed threshold, enforce rate limiting and consider temporary lock.

New Country Access

- Trigger step-up authentication.
- Validate with user via out-of-band channel if available.

Evidence Requirements

- Decisions must cite policy/playbook sections used.
- If no evidence is found, do not escalate solely based on speculation.