DFIR Triage Playbook

1. Validate alert.

2. Identify affected assets.

3. Assign severity.

4. Contain if necessary.

5. Document actions.

6. Escalate per policy.