

**Proposed Features, Prioritization, and Success Metrics (Alert Triage Workflow)**

**Proposed Features:**

1. **Alerts Overview Section:** Provides a visual breakdown of alerts by severity, helping engineers immediately identify critical items needing attention.
2. **Alert List Panel:** Displays a quick-scan list of alerts including severity, service, resource, and timestamp. Designed for fast browsing and prioritization.
3. **Alert Detail Panel:** Shows essential context when an alert is selected: cause, affected resource, severity, timestamp, and quick actions such as Acknowledge, Assign, and Resolve.
4. **Investigation Tabs:** Consolidates all investigation tools into a single panel with three tabs:
  - **Details:** Clear explanation and context of the alert.
  - **Logs:** Direct access to logs/events for validation.
  - **Recommendations:** Guided next steps for remediation.
5. **Simple Resolution Workflow:** A lightweight checklist to verify findings and ensure proper closure of alerts.

**Feature Prioritization:**

- **Fast Understanding:** Split-pane layout allows browsing alerts while reviewing details.
- **Minimize Tool Switching:** All investigation data is unified in one screen.
- **Clear Navigation:** Tabs and action buttons are placed logically for efficiency.
- **High-Severity Focus:** Prioritized visual cues guide the engineer toward urgent alerts first.

**Success Metrics:**

- Reduction in average triage time per alert.
- Decrease in false positives due to improved context visibility.
- Faster response to high-severity alerts.
- Increased number of alerts resolved without leaving the dashboard.
- Improved satisfaction among security engineers using the workflow.

This workflow design focuses on creating a practical, minimal, and efficient experience that enables engineers to triage alerts with clarity and speed.