Alert Triage Workflow: Cloud Security Dashboard

1. Problem Statement & User Persona

Problem Statement

Security Operations (SecOps) teams face a "context gap." They receive thousands of alerts (e.g., "GuardDuty finding"), but determining *actual* risk requires manually piecing together data from disparate logs, IAM policies, and resource configurations. This manual correlation slows down Mean Time To Respond (MTTR) and increases burnout due to false positives.

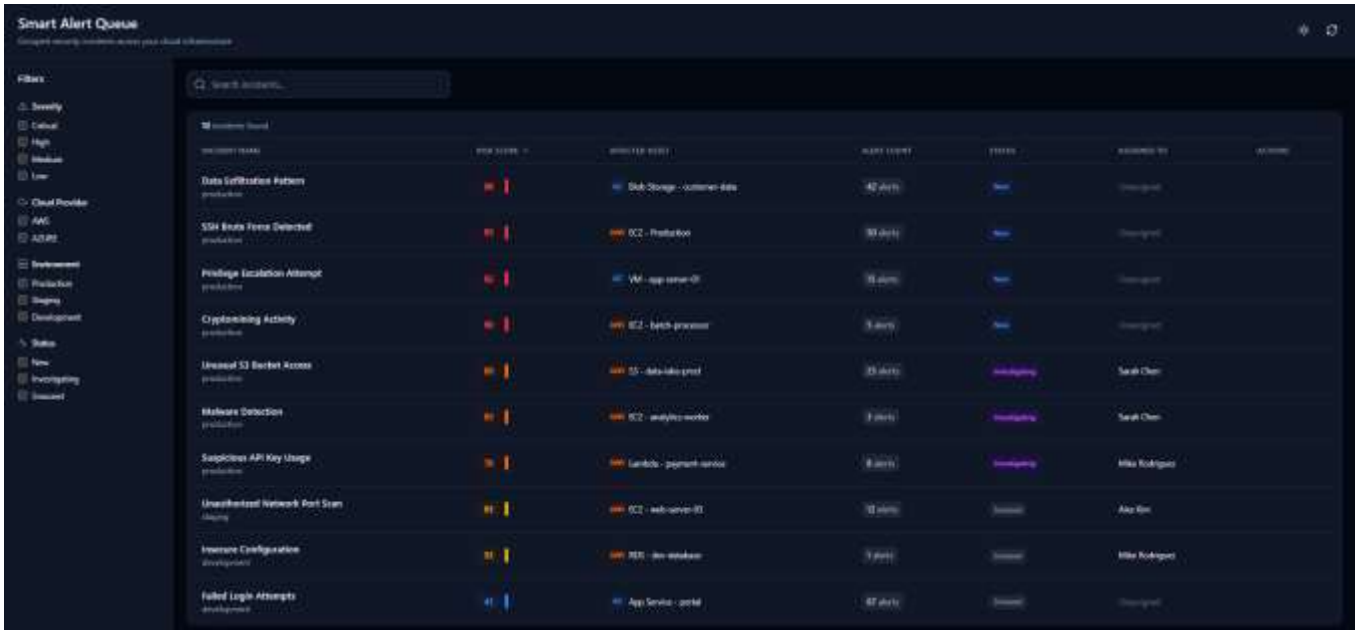
User Persona: "Amit" – Senior Cloud Security Engineer

- **Role**: Responsible for the security posture of a multi-cloud environment.
- **Goal**: Identify true threats within minutes and remediate them without breaking production apps.
- **Frustrations**:
    - "I get pinged for an 'open port' at 3 AM, only to find out it's a test instance with no data."
    - "I have to open 5 different tabs (AWS Console, Splunk, Jira, etc.) just to understand one alert."

---

2. Visual Designs & Wireframes

Screen 1: The "Smart Queue"



Screen 1 - smart queue

➢ Link : https://good-match-23539538.figma.site/

- **Goal**: De-clutter the noise.
- **Key Features**:
    - **Auto-Grouping**: Similar alerts (e.g., 50 "SSH Brute Force" attempts on one host) are grouped into a single "Incident".
    - **Risk Score**: A dynamic score (0-100) based on asset value (e.g., Prod Database vs. Dev Sandbox).
    - **Quick Actions**: Hover actions to "Snooze" or "Assign".

Screen 2: The Investigation Context (Graph View)

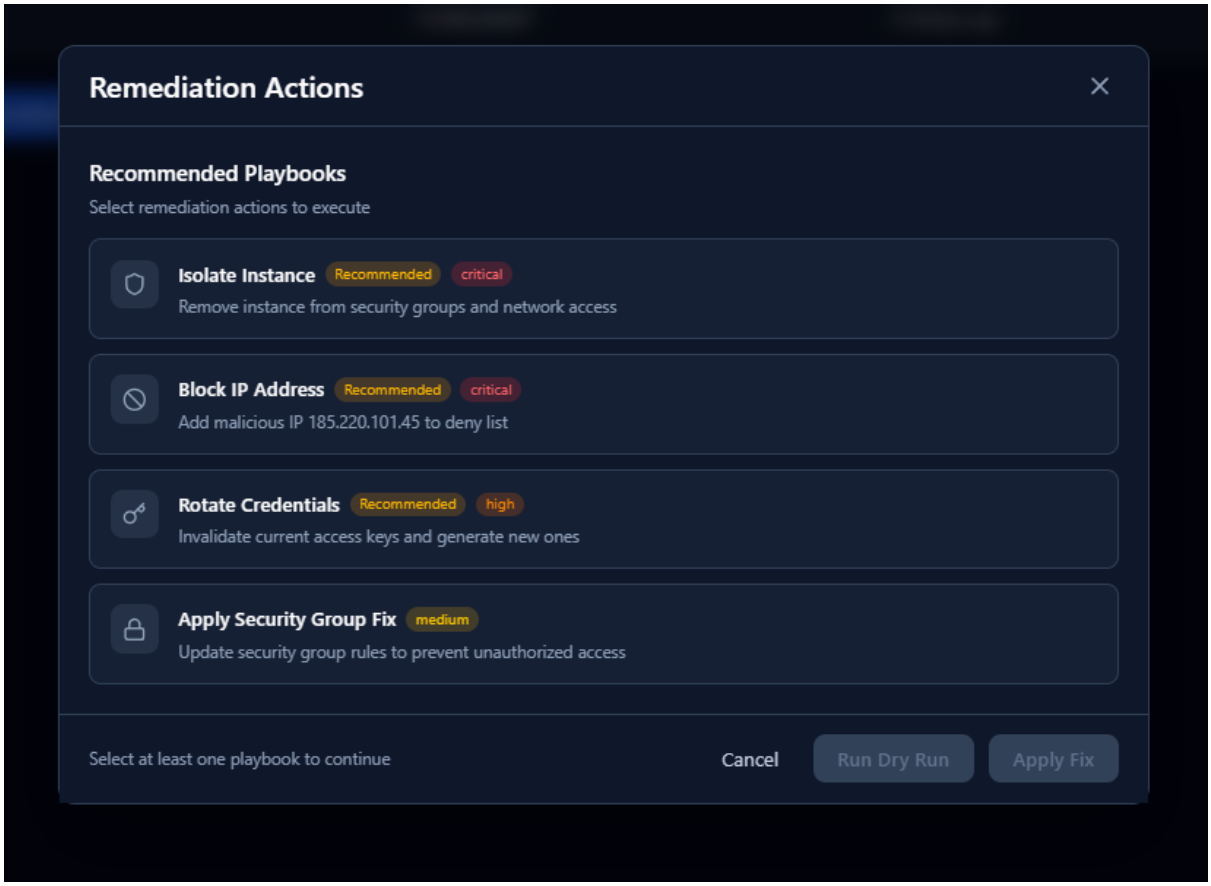
Screen 2 - Investigation Graph

Goal: Instant situational awareness.

- **Key Features**:
    - **Attack Path Graph**: Visualizes *how* the attacker got in. Internet -> Load Balancer -> Vulnerable Pod -> S3 Bucket.
    - **Timeline**: Correlates the alert with recent deployments or config changes (answering "Did we just deploy this bug?").
    - **Enriched Signals**: Shows IP reputation and user behavior anomalies side-by-side.

➢ Link : https://revel-sled-88186127.figma.site/

Screen 3: Guided Remediation



Screen 3 - Remediation Modal

- **Goal**: Safe, decisive action.
- **Key Features**:
    - **Playbook Suggestions**: Recommend specific actions based on the alert type (e.g., "Isolate Instance").
    - **Impact Analysis**: Pre-calcualted warning: "Stopping this instance will disconnect 3 active services."
    - **One-Click Execution**: Integrated with infrastructure-as-code or cloud APIs to apply the fix immediately.

➢ Link: https://gong-dude-95471966.figma.site/

---

3. Proposal Write-up

Prioritization & Philosophy

We prioritize **"Context over Volume"**. Instead of showing a list of 10,000 logs, we synthesize them into ~50 actionable "Incidents." The design prioritizes the **Investigation View** (Screen 2) as the primary workspace, as this is where analysts spend 80% of their time attempting to understand the "Blast Radius."

Key Features

1. **Visual Blast Radius**: Using a graph database to map relationships between assets.
2. **Temporal Correlation**: Overlaying CloudTrail events (who changed what) with GuardDuty findings (what went wrong).
3. **Safe-Action Framework**: Remediation actions run a "Dry Run" first to predict downtime, addressing the engineer's fear of breaking production.

Success Metrics

- **Reduction in MTTR (Mean Time To Respond)**: Target < 15 minutes for Critical alerts.
- **Triage Efficiency**: Average alert handling time reduced from 45 mins to 10 mins.
- **False Positive Rate**: Percentage of alerts marked as "Ignore" decreases by 30% (due to better auto-suppression).

---

4. Development Action Items (Bonus)

- **Backend**:
    - Build an aggregation service to consume findings from AWS Security Hub and Azure Sentinel.
    - Implement a graph service (e.g., Neo4j or AWS Neptune) to ingest and map asset relationships.
- **Frontend**:
    - Select a visualization library (e.g., React Flow or D3.js) for the interactive node graph.
    - Develop the "Dry Run" API to simulate remediation impacts (e.g., checking dependencies before stopping an instance).
- **Integration**:
    - Set up bi-directional sync with Jira/ServiceNow for ticket tracking.