The Problem Statement : Cloud security teams like Aman (oversight), Srishti (remediation), and Rohit (incident response) struggle with fragmented visibility across 50+ accounts. This dashboard gives Aman centralized prioritization, Srishti context-specific fixes, and Rohit forensic-grade investigation tools.

User Personas :

1) Primary Persona : Aman Yadav , Cloud Security Engineer

Role: Cloud Security Lead responsible for security posture and compliance.

- Demographics: 28-35 years old, 3-5 years cloud exp, works at mid-sized fintech (500 devs, 50+ AWS/Azure accounts).
- Goals: Proactive risk reduction, maintain >95% compliance, remediate critical misconfigs in <24hrs.
- Pain Points: Alert fatigue from thousands of findings, no single source of truth, manual ticket assignment.
- Behaviors: Monitors 100+ alerts/day, weekly team reviews, monthly compliance reporting, quarterly policy updates.
- Wants : "I need one dashboard showing all my accounts' risks , specially the critical ones .. not 10 tabs"
- Dashboard Priority: Top risks view + assignment workflow (prioritized list with "assign" buttons).

2) Secondary Persona : Srishti , Senior Platform Engineer

Role: Platform Engineer responsible for implementing security fixes.

- Demographics: 24-28 years old, 5+ years DevOps experience, individual contributor on infrastructure team.
- Goals: Fix security issues without breaking production, maintain deployment pace.
- Pain Points: Unclear remediation instructions, no context about business impact, separate security tool disrupting workflow.
- Behaviors: Fixes during maintenance windows, coordinates with security team, tracks own team's metrics.
- Quote: "Tell me exactly what to run and what it will break before I run it."
- Dashboard Priority: Team-specific view + remediation console (personalized fix list which filtered to my resources).

3) Edge Persona : Rohit , Incident response Lead

Role: Security Incident Responder during cloud breaches.

- Demographics: 35-45 years old, 10+ years security experience, part of 24/7 incident response team.
- Goals: Rapid control during incidents, forensic investigation, minimize blast radius.
- Pain Points: Cannot correlate misconfigs to active attacks, too many clicks to trace cross-account movement.
- Behaviors: Reacts to alerts, investigates under time pressure, creates post-mortem reports.
- Quote: "Show me every misconfiguration this attacker could have exploited in the last 48 hours."
- Dashboard Priority: Forensic investigation mode (time-based filtering + attack graph visualization).