**IAM Permissions Explorer: Product Strategy & Roadmap**

**1. Proposed Features**

To solve the "Production Paradox" (the fear of breaking things while securing them), I propose three core features:

- **Impact Simulator (The "Dry Run"):** Before revoking a permission, the system enters a "Shadow Mode" for 48-72 hours. It monitors real-time traffic to see if any service attempts to use the targeted permission. If a call is detected, the simulation fails, preventing a production outage[2].
- **Auto-Right Size Engine:** Using ML to analyse the last 90 days of logs, the system generates a "Least Privilege" policy side-by-side with the current bloated one. It highlights exactly which lines of JSON code can be safely removed[3].
- **One-Click "Request Justification":** Instead of manual Slack messages, Kunal can trigger an automated workflow. The resource owner receives a notification to justify the permission. If they don't respond within a set period, the permission is auto-flagged for the next "Simulated Revocation" cycle.

---

**2. Prioritization (RICE Framework)**

I have prioritized these features using the RICE score to maximize security impact with minimal engineering risk.

| Feature | Reach | Impact | Confidence | Effort | RICE Score |
|---|---|---|---|---|---|
| **Impact Simulator** | 10/10 | High (3) | 90% | High (4) | **6.75** |
| **Auto-Right Size Engine** | 10/10 | Med (2) | 80% | Med (3) | **5.33** |
| **Justification Workflow** | 5/10 | Low (1) | 90% | Low (1) | **4.5** |

**Rationale:** The **Impact Simulator** is the P0 (highest priority) because it directly solves the "Fear of Breaking" pain point, which is the biggest barrier to adopting IAM security tools[5].

---

**3. Success Metrics (KPIs)**

To measure the effectiveness of the IAM Explorer, we will track:

- **Permission Reduction Rate:** % decrease in "Admin" and "Write" permissions across the cloud estate over 3 months.
- **False Positive Rate (Simulation):** % of simulated revocations that correctly identified a "rare but critical" permission before it was deleted.
- **Mean Time to Remediate (MTTR):** The average time it takes from identifying a "Ghost Identity" to successfully revoking its access.

- **Zero-Outage Compliance:** A binary metric ensuring that 100% of permission removals performed through the "Impact Simulator" resulted in zero production downtime.