IAM Permissions Explorer (Option 3):

Made By: Gaurav Sidharth Bharane
Linkedin: linkedin.com/in/gaurav-bharane

---

1. Problem Statement & User Persona

Problem Statement

In cloud environments, IAM permissions tend to grow over time due to changing responsibilities, temporary access, and legacy policies. As a result, users and roles often end up with **more permissions than necessary**, increasing the security risk and making audits difficult.

Cloud security engineers need a simple and reliable way to understand **which permissions are actually being used**, identify excessive access, and reduce it safely—without disrupting running systems.

The objective of the IAM Permissions Explorer is to provide **clear visibility into permission usage** and support confident, informed access cleanup.

User Persona: Cloud Security Engineer

Role

- Oversees IAM users, roles, and permissions across cloud accounts
- Performs access reviews and investigates permission risks

Challenges

- Limited visibility into excessive and unused permissions
- Risk of service impact when reducing access

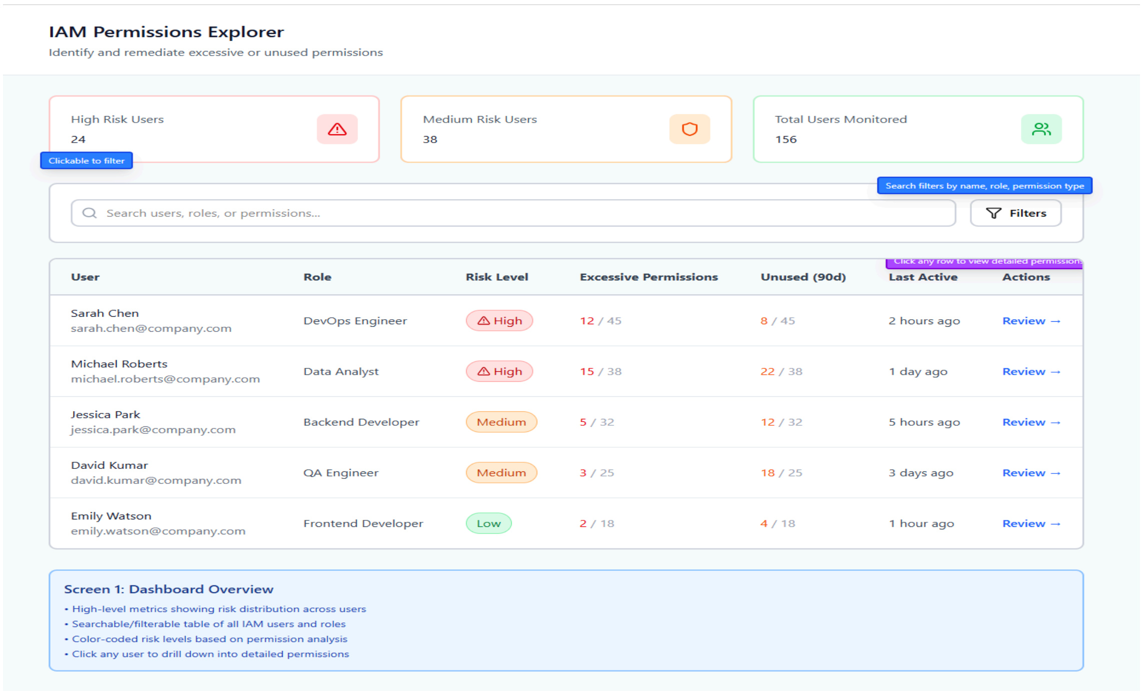
Goals

- Quickly identify high-risk identities from a central dashboard
- Review permission usage with confidence
- Safely reduce access while minimizing operational risk

2. Wireframes (Figma – 3 Screens)

Link: https://pack-bold-02064716.figma.site/

Screen 1: IAM Permissions Overview



IAM Permissions Explorer

Identify and remediate excessive or unused permissions

High Risk Users ⚠
24

Clickable to filter

Medium Risk Users
38

Total Users Monitored
156

Search filters by name, role, permission type

Search users, roles, or permissions...

Filters

Click any row to view detailed permission

User	Role	Risk Level	Excessive Permissions	Unused (90d)	Last Active	Actions
Sarah Chen sarah.chen@company.com	DevOps Engineer	⚠ High	12 / 45	8 / 45	2 hours ago	Review →
Michael Roberts michael.roberts@company.com	Data Analyst	⚠ High	15 / 38	22 / 38	1 day ago	Review →
Jessica Park jessica.park@company.com	Backend Developer	Medium	5 / 32	12 / 32	5 hours ago	Review →
David Kumar david.kumar@company.com	QA Engineer	Medium	3 / 25	18 / 25	3 days ago	Review →
Emily Watson emily.watson@company.com	Frontend Developer	Low	2 / 18	4 / 18	1 hour ago	Review →

Screen 1: Dashboard Overview

- High-level metrics showing risk distribution across users
- Searchable/filterable table of all IAM users and roles
- Color-coded risk levels based on permission analysis
- Click any user to drill down into detailed permissions

Purpose

Provide a centralized dashboard that enables security engineers to **quickly assess IAM risk across users and roles** and prioritize reviews based on permission exposure.

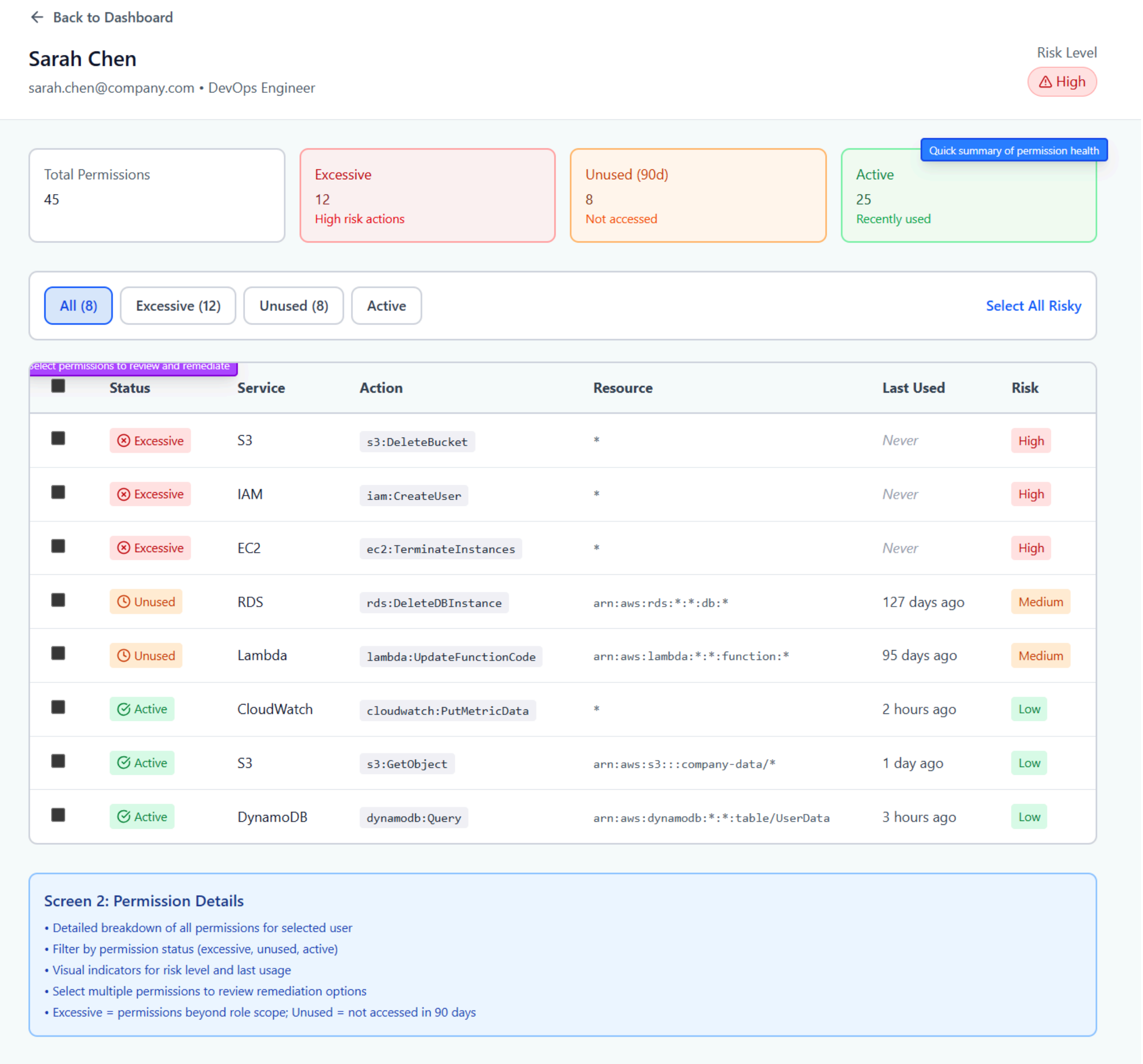
Key Elements

- **Risk Summary Cards**
  Show High Risk, Medium Risk, and Total Users, with quick filters on selection.
- **Search Bar**
  Enables fast lookup of users, roles, or permissions by name.
- **Filters**
  Filter identities by type (User/Role), risk level, and unused permissions (30/ 60/ 90 days).
- **IAM Identities Table**
  Lists users and roles with identity name, role or job function, risk level, counts of excessive and unused permissions (90 days), last active date, and an action to review details.

Annotation

Risk levels are calculated using permission sensitivity and historical usage to prioritize access reviews.

Screen 2: Permission Details View



← Back to Dashboard

Sarah Chen

sarah.chen@company.com • DevOps Engineer

Risk Level

⚠ High

Quick summary of permission health

Total Permissions	Excessive	Unused (90d)	Active
45	12 High risk actions	8 Not accessed	25 Recently used

All (8) | Excessive (12) | Unused (8) | Active | Select All Risky

elect permissions to review and remediate

■	Status	Service	Action	Resource	Last Used	Risk
■	⊗ Excessive	S3	`s3:DeleteBucket`	*	*Never*	High
■	⊗ Excessive	IAM	`iam:CreateUser`	*	*Never*	High
■	⊗ Excessive	EC2	`ec2:TerminateInstances`	*	*Never*	High
■	◷ Unused	RDS	`rds:DeleteDBInstance`	`arn:aws:rds:*:*:db:*`	127 days ago	Medium
■	◷ Unused	Lambda	`lambda:UpdateFunctionCode`	`arn:aws:lambda:*:*:function:*`	95 days ago	Medium
■	✓ Active	CloudWatch	`cloudwatch:PutMetricData`	*	2 hours ago	Low
■	✓ Active	S3	`s3:GetObject`	`arn:aws:s3:::company-data/*`	1 day ago	Low
■	✓ Active	DynamoDB	`dynamodb:Query`	`arn:aws:dynamodb:*:*:table/UserData`	3 hours ago	Low

Screen 2: Permission Details

- Detailed breakdown of all permissions for selected user
- Filter by permission status (excessive, unused, active)
- Visual indicators for risk level and last usage
- Select multiple permissions to review remediation options
- Excessive = permissions beyond role scope; Unused = not accessed in 90 days

Purpose

Enable detailed analysis of a selected user or role to identify risky and unused permissions.

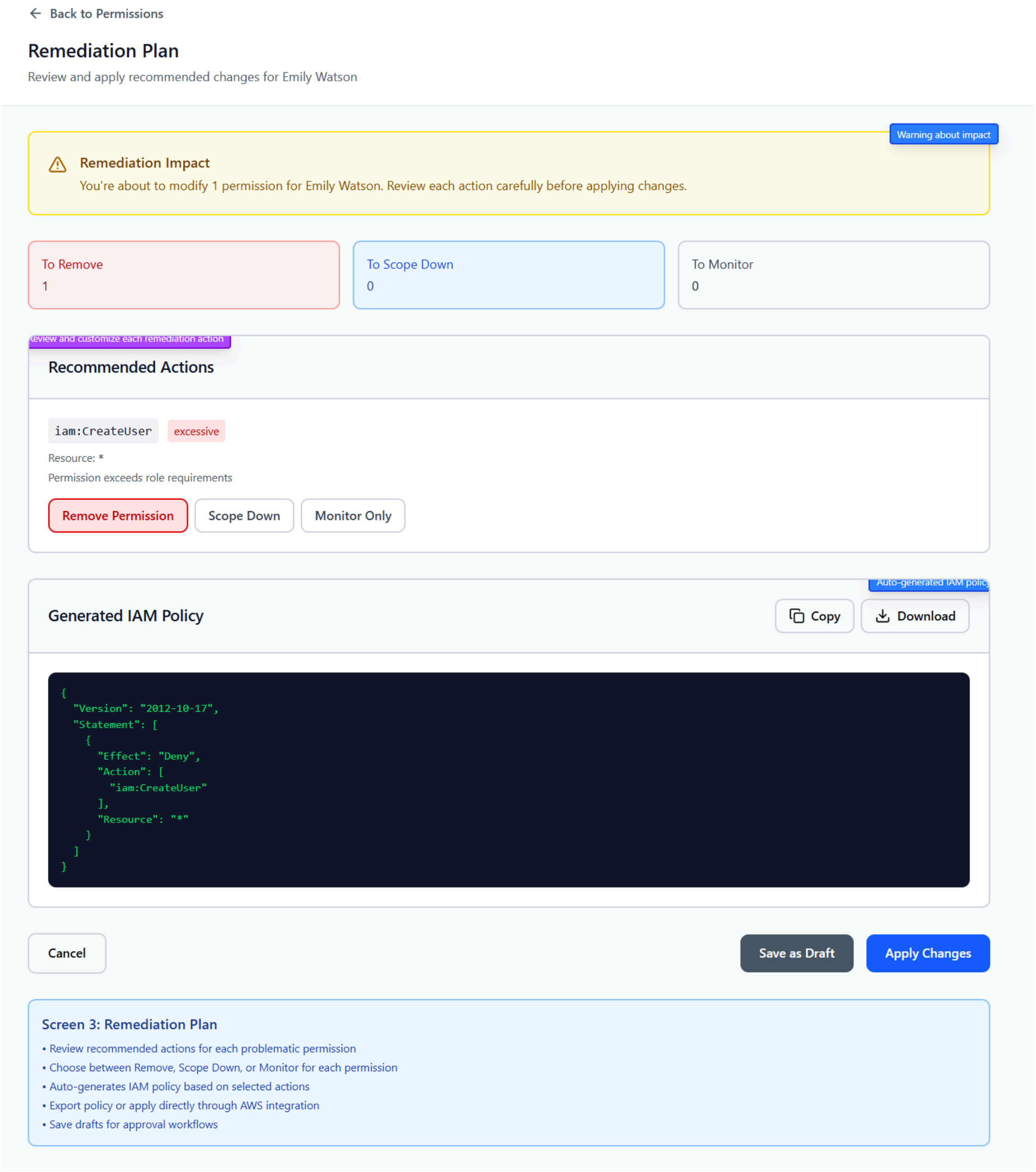
Key Elements

- Identity header with name, role, and overall risk level
- Summary cards showing total, excessive, unused (90 days), and active permissions
- Tabs to filter permissions by status (All, Excessive, Unused, Active)
- Permissions table displaying service, action, resource scope, last used date, usage status, and risk level
- Support for selecting permissions for review and remediation

Annotation

Excessive and unused permissions are highlighted to help users quickly prioritize cleanup.

Screen 3: Remediation Plan



Remediation Plan

Review and apply recommended changes for Emily Watson

Remediation Impact

You're about to modify 1 permission for Emily Watson. Review each action carefully before applying changes.

To Remove	To Scope Down	To Monitor
1	0	0

Recommended Actions

`iam:CreateUser` excessive

Resource: *

Permission exceeds role requirements

Generated IAM Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "iam:CreateUser"
      ],
      "Resource": "*"
    }
  ]
}
```

Screen 3: Remediation Plan

- Review recommended actions for each problematic permission
- Choose between Remove, Scope Down, or Monitor for each permission
- Auto-generates IAM policy based on selected actions
- Export policy or apply directly through AWS integration
- Save drafts for approval workflows

Purpose

Enable safe and controlled remediation of risky IAM permissions with clear visibility into impact.

Key Elements

- Remediation impact banner highlighting potential service impact
- Summary cards categorizing actions (Remove, Scope Down, Monitor)
- List of recommended actions for each risky permission
- Option to review, remove, scope down, or monitor permissions individually
- Controls to save changes as draft or apply after review

Annotation
Remediation actions require explicit user approval to prevent unintended service disruptions.

3. Features, Prioritization & Success Metrics

Key Features (MVP)

- **Risk-based IAM overview**
  A centralized dashboard that surfaces high-risk users and roles using risk indicators and unused permission counts (Screen 1).

- **Detailed permission analysis**
  Clear visibility into permission usage through summary cards, status-based filtering (Excessive, Unused, Active), and detailed permission metadata (Screen 2).

- **Guided remediation with safeguards**
  Actionable remediation recommendations, impact awareness, and approval-based execution to safely reduce access (Screen 3).

Prioritization Rationale

The MVP focuses on **visibility, prioritization, and safe decision-making**, which reflect how security engineers conduct access reviews in practice. Automated enforcement is intentionally excluded to ensure changes remain reviewable and do not introduce operational risk. Each feature directly supports a clear progression from risk discovery to controlled remediation.

Success Metrics

- Reduction in excessive and unused IAM permissions

- Time taken to identify and review high-risk identities

- Number of users or roles remediated per audit cycle

- Percentage of remediation recommendations reviewed or applied