1. IAM Policies for User Roles within the SOC

IAM (Identity and Access Management) policies are a critical component of ensuring secure access to resources within the SOC (Security Operations Center) environment. By defining access controls, adhering to the principle of least privilege, ensuring compliance, managing risk, enabling incident response, supporting scalability, promoting auditing and accountability, and facilitating continuous improvement, IAM policies play a central role in protecting sensitive data and systems from unauthorized access and security breaches.
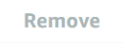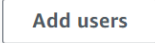
2. Role-Based Access Control (RBAC)- Tech Admin

Implement RBAC to assign permissions based on job responsibilities, minimizing the risk of unauthorized access.

| | | | | |
|---|---|---|---|---|
| ☐ | SOC | ⚠ 0 | ⊘ Defined | 11 days ago |
| ☐ | TechAdmin | 2 | ⊘ Defined | 6 days ago |

3. User Roles and Permissions

The Tech Admin group has been granted full administrative access, providing users with comprehensive control over the system. Giovanni and Matthew serve as the technical leads within this group, overseeing its operations.

**Users in this group (2)**          🔄  Remove  Add users

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

🔍 Search                                          ⟨ 1 ⟩  ⚙

| ☐ | User name ↗ | ▲ | Groups | Last activity ▽ | Creation time ▽ |
|---|---|---|---|---|---|
| ☐ | Giovanni | | 1 | Yesterday | 6 days ago |
| ☐ | Matthew | | 1 | 11 hours ago | 6 days ago |

## Permissions policies (1)  Info

You can attach up to 10 managed policies.

[Simulate ⤢]  [Remove]  [Add permissions ▼]

Filter by Type

[🔍 Search]    [All types ▼]              ‹ **1** ›  ⚙

| | Policy name ⤢ ▲ | Type ▽ | Attached entities ▽ |
|---|---|---|---|
| ☐  ⊞  📦 AdministratorAccess | | AWS managed - job function | 3 |

## Allowed services (393)

IAM reports activity for services and management actions. Learn more about action last accessed information. To see actions, choose the appropriate service name from the list.

Filter by services access history

[🔍 Search]    [No Filter ▼]

‹ **1** 2 3 4 5 6 7 … 40 ›  ⚙

| Service ▽ | Policies granting permis… | Last accessed ▽ | Access by members |
|---|---|---|---|
| Amazon EC2 | AdministratorAccess | Today | Matthew and 1 more |
| AWS Health APIs and Not… | AdministratorAccess | Today | Matthew and 1 more |
| AWS User Notifications | AdministratorAccess | Today | Matthew and 1 more |
| AWS Signin | AdministratorAccess | Today | Matthew and 1 more |
| AWS Service Catalog | AdministratorAccess | Today | Matthew and 1 more |
| Amazon CloudWatch Logs | AdministratorAccess | Yesterday | Matthew and 1 more |