

ROAD TO IAM ZERO - AGENDA

- What is an IAM user?
- Why IAM users are bad
- 5 steps to eliminate IAM users

WHAT IS AN IAM USER?

demo

EXAMPLE BREACHES



UBER – personal data

DXC – crypto mining £70,000 over a weekend due to AWS access key breach to GitHub

JUSPAY – Credit card payment company, 35 million people affected

RONIN – Crypto currency \$600 million loss

REFERENCES:

UBER: <https://www.bbc.co.uk/news/technology-42075306>

DXC:

https://www.theregister.com/2017/11/14/dxc_github_aws_keys_leaked/?utm_campaign=Security%2BNewsletter&utm_medium=email&utm_source=Security_Newsletter_co_52

LOGICGATE: <https://techcrunch.com/2021/04/13/logicgate-risk-cloud-data-breach/>

CODECOV: <https://blog.christophetd.fr/cloud-security-breaches-and-vulnerabilities-2021-in-review/>

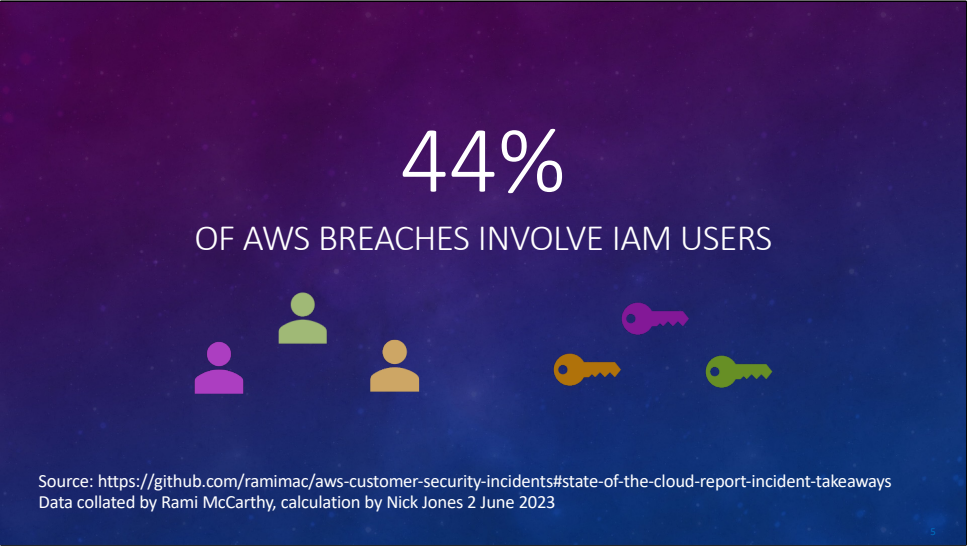
KASPERSKY: <https://blog.christophetd.fr/cloud-security-breaches-and-vulnerabilities-2021-in-review/>

ASTRAZENECA: <https://securitylabs.datadoghq.com/articles/public-cloud-breaches->

2022-mccarthy-hopkins/

JUSPAY: <https://www.csoonline.com/article/3603473/juspay-data-breach-could-have-far-reaching-consequences.html>

RONIN: <https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain/?sh=7da45ce42686>

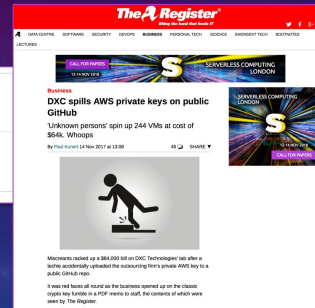


Source: <https://github.com/ramimac/aws-customer-security-incidents#state-of-the-cloud-report-incident-takeaways>

Calculation by Nick Jones

WHY AWS IAM USERS ARE BAD

🔑 AWS_ACCESS_KEY_ID	Updated 1 minute ago
🔑 AWS_SECRET_ACCESS_KEY	Updated 1 minute ago



❌ Failed

■ Medium

CIS.1.4

Ensure access keys are rotated every 90 days or less

4 of 4

HOW IAM USERS GET CREATED



Dev account



Test account



Prod account

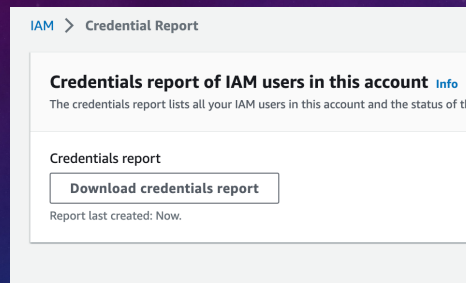


5 STEPS TO IAM ZERO

1. Measure and monitor
2. Remove inactive users
3. AWS IAM Identity Center
4. Alternative machine access
5. Prevent using SCPs



STEP 1: MEASURE AND MONITOR

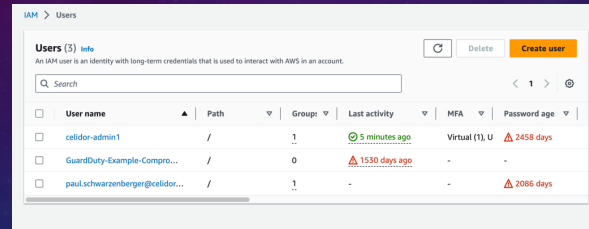


<https://www.paloaltonetworks.com>

<https://www.wiz.io>

<https://www.cloudquery.io>

STEP 2: REMOVE INACTIVE USERS



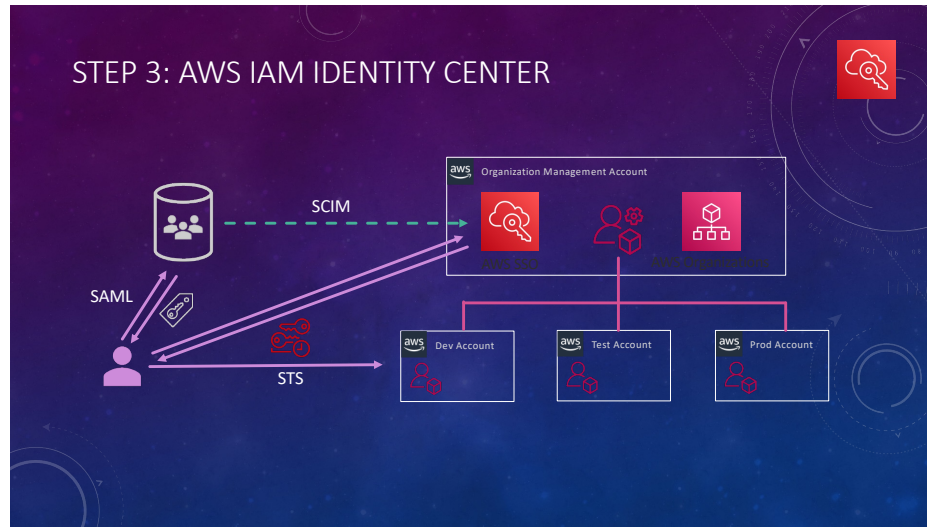
The screenshot shows the AWS IAM console 'Users' page. It features a search bar, a 'Delete' button, and a 'Create user' button. Below is a table with columns for User name, Path, Groups, Last activity, MFA, and Password age.

User name	Path	Groups	Last activity	MFA	Password age
cellidor-admin1	/	1	5 minutes ago	Virtual (1), U	2458 days
GuardDuty-Example-Compro...	/	0	1530 days ago	-	-
paul.schwarzenberger@cellidor...	/	1	-	-	2086 days

<https://www.wiz.io/blog/how-to-get-rid-of-aws-access-keys-part-1-the-easy-wins> –
Scott Piper

<https://www.wiz.io/blog/how-to-get-rid-of-aws-access-keys-part-3>

STEP 3: AWS IAM IDENTITY CENTER



<https://aws.amazon.com/iam/identity-center/>

STEP 4: ALTERNATIVE MACHINE ACCESS













- Assume IAM role from AWS principal
- Resource based policies
- OpenID Connect
- IAM Roles Anywhere



ASSUME IAM ROLE FROM ANY AWS PRINCIPAL



How should you connect your new supplier?

- Option 1 – IAM user access key    →  
- Option 2 – IAM role     →  


RESOURCE BASED POLICIES

- Allow AWS principals in resource policy
- Straightforward to implement
- Only supported by some AWS services



- Harder to audit than IAM roles

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Example permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountB-ID:root"
      },
      "Action": [
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ]
    }
  ]
}
```

AWS resource-based vs identity-based policies:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_identity-vs-resource.html

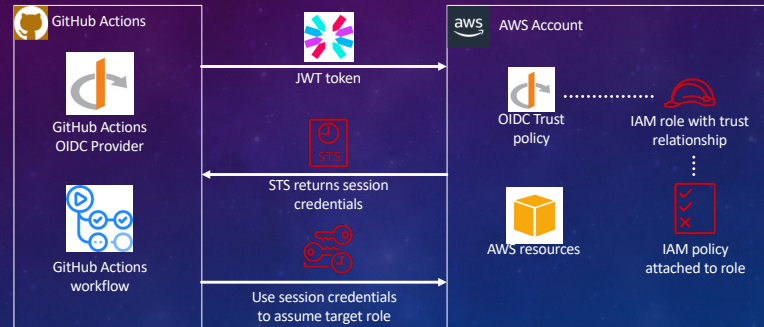
AWS services supporting resource-based policies:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

Examples shown on the slide (1st row): S3, ECR, EFS, API Gateway

Examples shown on slide (2nd row): KMS, SNS, SQS, OpenSearch

OPENID CONNECT



<https://github.com/domain-protect/domain-protect-deploy>

Diagram based on <https://www.npmjs.com/package/aws-cdk-github-oidc>

IAM ROLES ANYWHERE



July 2022: AWS IAM Roles Anywhere launched

July 2023: Support for OS key stores

September 2023: Support for PKCS11 smart cards and Yubikeys

<https://docs.aws.amazon.com/rolesanywhere/latest/userguide/introduction.html>

July 2022: <https://aws.amazon.com/about-aws/whats-new/2022/07/aws-identity-access-management-iam-roles-anywhere-workloads-outside-aws>

July 2023: <https://aws.amazon.com/about-aws/whats-new/2023/07/iam-roles-anywhere-credential-helper-os-certificate-stores>

September 2023: <https://aws.amazon.com/blogs/security/how-to-implement-cryptographic-modules-to-secure-private-keys-used-with-iam-roles-anywhere>

IAM ROLES ANYWHERE



Medium article: [AWS IAM Roles Anywhere with MacOS Keychain](https://medium.com/@paulschwarzenberger/aws-iam-roles-anywhere-with-macos-keychain-17764b5fb848)

GitHub repo: [celidor/aws-iam-roles-anywhere](https://github.com/Celidor/aws-iam-roles-anywhere)

<https://medium.com/@paulschwarzenberger/aws-iam-roles-anywhere-with-macos-keychain-17764b5fb848>

<https://github.com/Celidor/aws-iam-roles-anywhere>

STEP 5: PREVENT USING SCPS

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

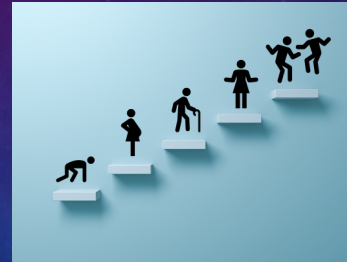
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PreventIamUserActions",
      "Effect": "Deny",
      "Action": [
        "iam:CreateLoginProfile"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

⊗ User was not created.
User: arn:aws:iam::915299531522:user/cpms-admin is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::915299531522:user/test-user with an explicit deny in a service control policy

<https://www.wiz.io/blog/how-to-get-rid-of-aws-access-keys-part-1-the-easy-wins> – Scott Piper

RECAP: 5 STEPS TO IAM ZERO

1. Measure and monitor
2. Remove inactive users
3. AWS IAM Identity Center
4. Alternative machine access
5. Prevent using SCPs



THANK YOU!

 Paul Schwarzenberger
CloudSecurityForum

 Paul Schwarzenberger

 @paulschwarzen

<https://www.linkedin.com/in/paulschwarzen>
<https://twitter.com/paulschwarzen>