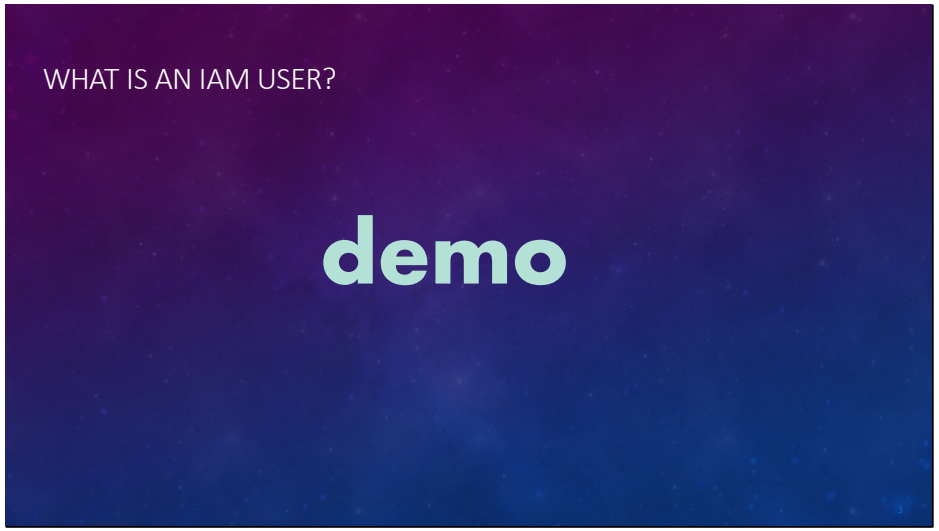

ROAD TO IAM ZERO
PAUL SCHWARZENBERGER
OCTOBER 2023


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

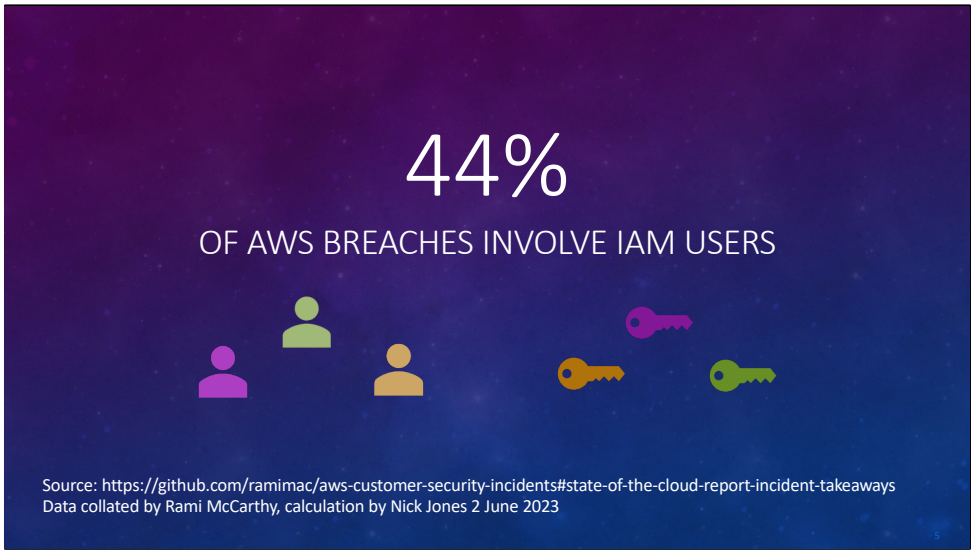
UBER – personal data
DXC – crypto mining £70,000 over a weekend due to AWS access key breach to GitHub
JUSPAY – Credit card payment company, 35 million people affected
RONIN – Crypto currency $600 million loss

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-

CONTINUED 4

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



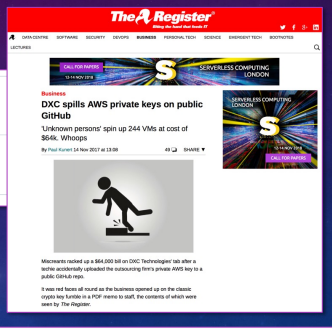
Source: https://github.com/ramimac/aws-customer-security-incidents#state-of-the-cloud-report-incident-takeaways

Calculation by Nick Jones

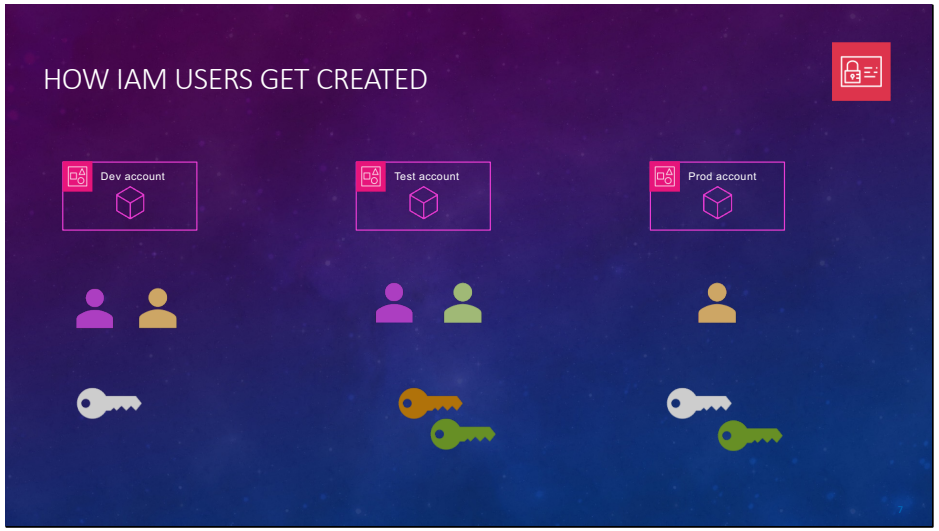
CONTINUED 5

WHY AWS IAM USERS ARE BAD

AWS_ACCESS_KEY_ID	Updated 1 minute ago
AWS_SECRET_ACCESS_KEY	Updated 1 minute ago

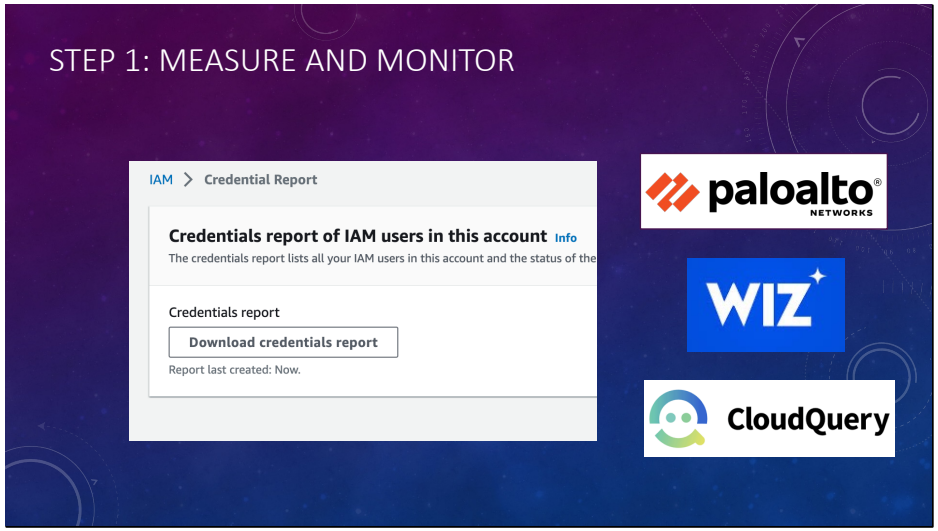


Failed	Medium	CIS.1.4	Ensure access keys are rotated every 90 days or less	4 of 4


HOW IAM USERS GET CREATED
Dev account
Test account
Prod account

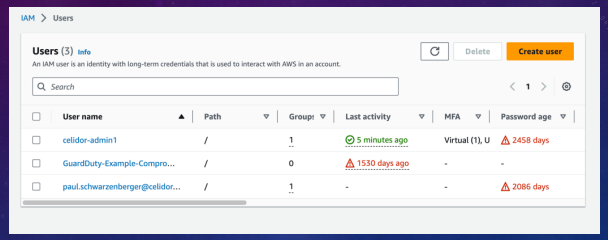
5 STEPS TO IAM ZERO

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

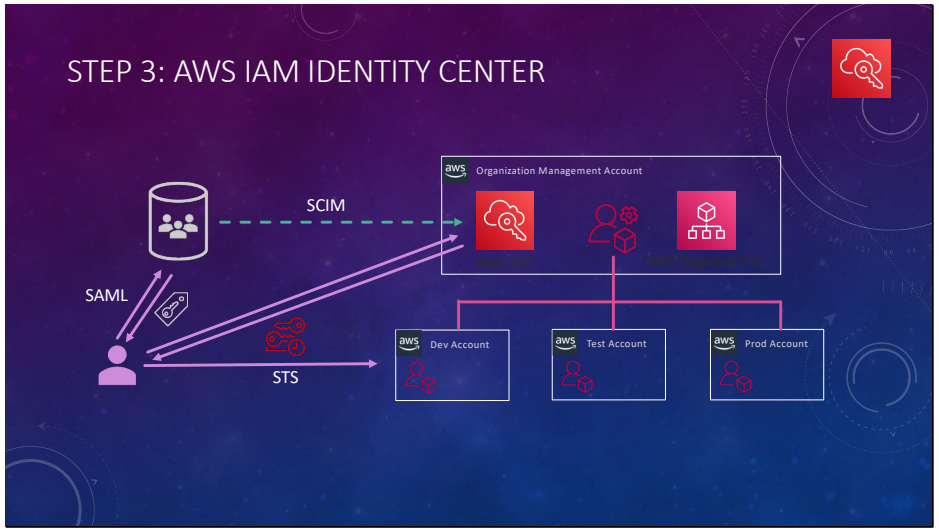


https://www.paloaltonetworks.com
https://www.wiz.io
https://www.cloudquery.io

STEP 2: REMOVE INACTIVE USERS



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



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

STEP 4: ALTERNATIVE MACHINE ACCESS

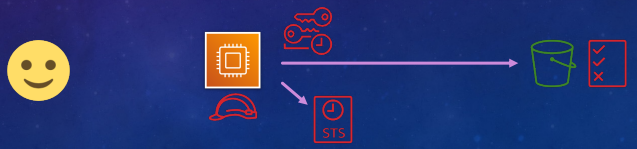
- Assume IAM role from AWS principal
- Resource based policies
- OpenID Connect
- IAM Roles Anywhere

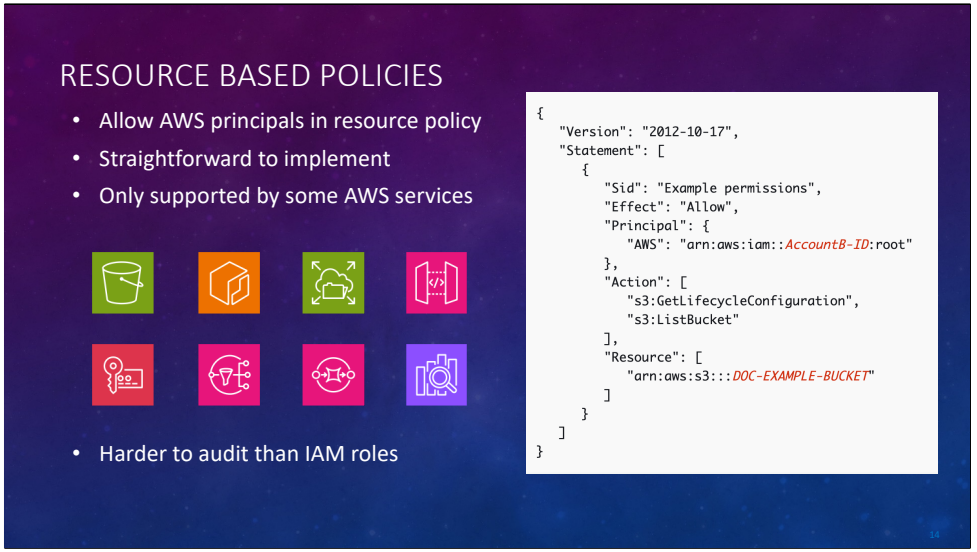
ASSUME IAM ROLE FROM ANY AWS PRINCIPAL

How should you connect your new supplier?

- Option 1 – IAM user access key

- Option 2 – IAM role





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 silde☹2nd row): KMS, SNS, SQS , OpenSearch

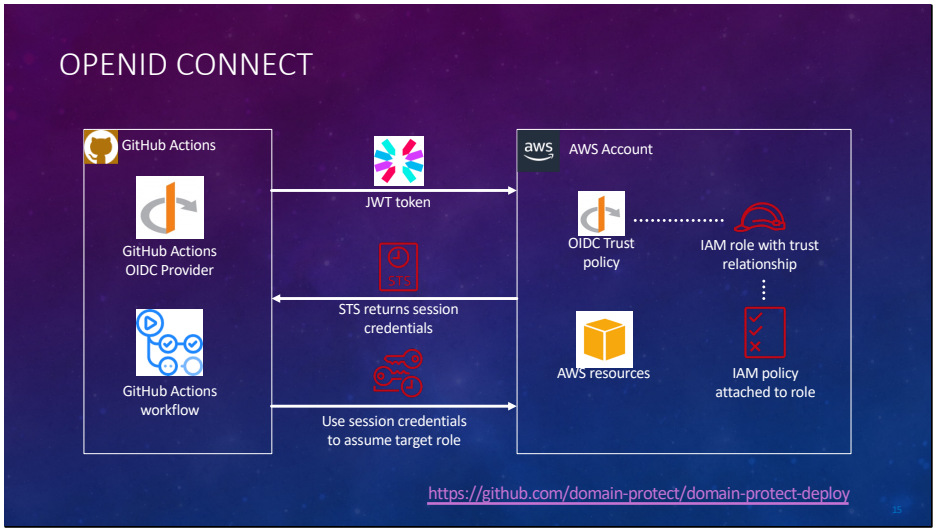
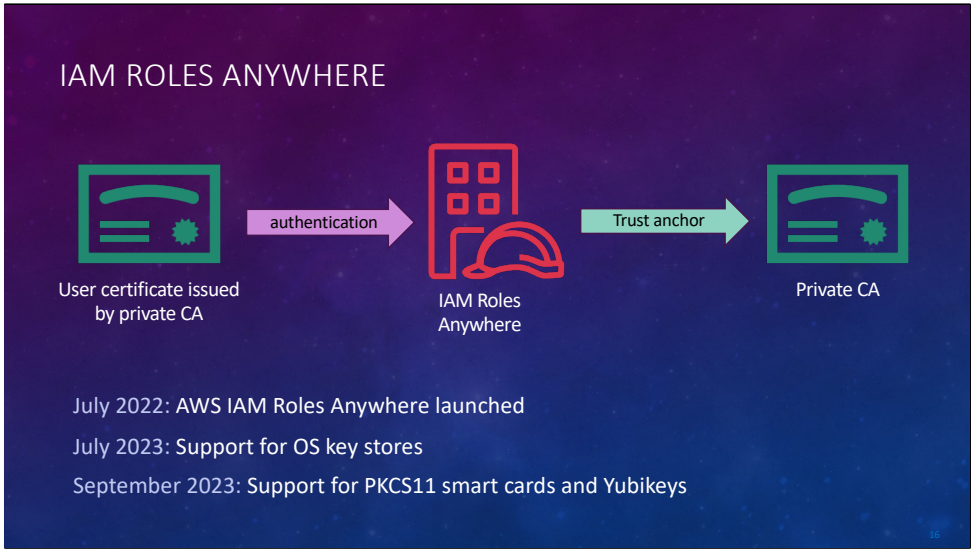


Diagram based on https://www.npmjs.com/package/aws-cdk-github-oidc



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

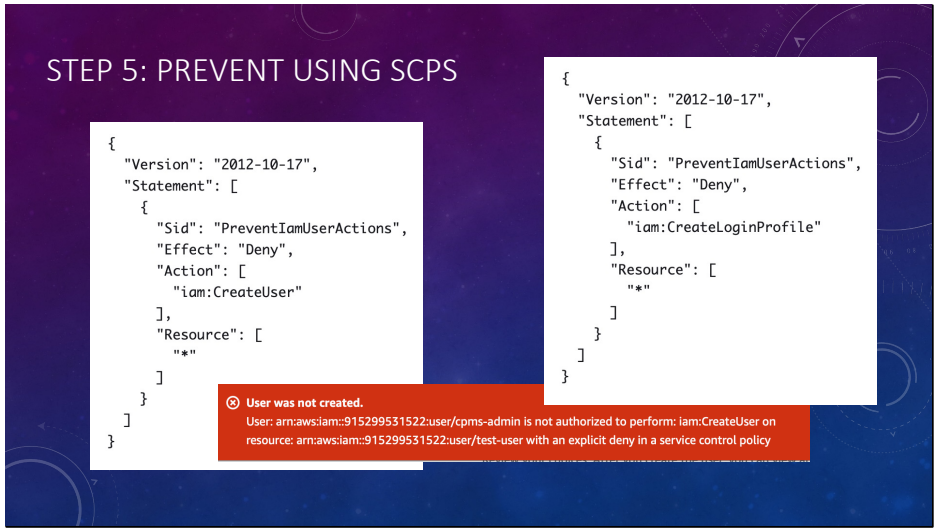
Medium article: AWS IAM Roles Anywhere with MacOS Keychain

GitHub repo: celidor/aws-iam-roles-anywhere

17

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

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



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

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

CONTINUED 20