REVERSEC

Sensible Security for AWS Workloads

Nick Jones – Oslo AWS User Group, May 2025

About Me

Nick Jones

- Global Head of Research @ Reversec
- Ex-Cloudsec Consulting Lead

Active in the community

- fwd:cloudsec EU Content Lead
- fwd:cloudsec NA Reviewer
- AWS Community Builder

Been in the game for a while

- 10+ years in cybersecurity
- ~7 in cloud security

At Present...

Freedom!

- Reversec is going independent
- Needed to migrate ~30/35 workloads out of the parent

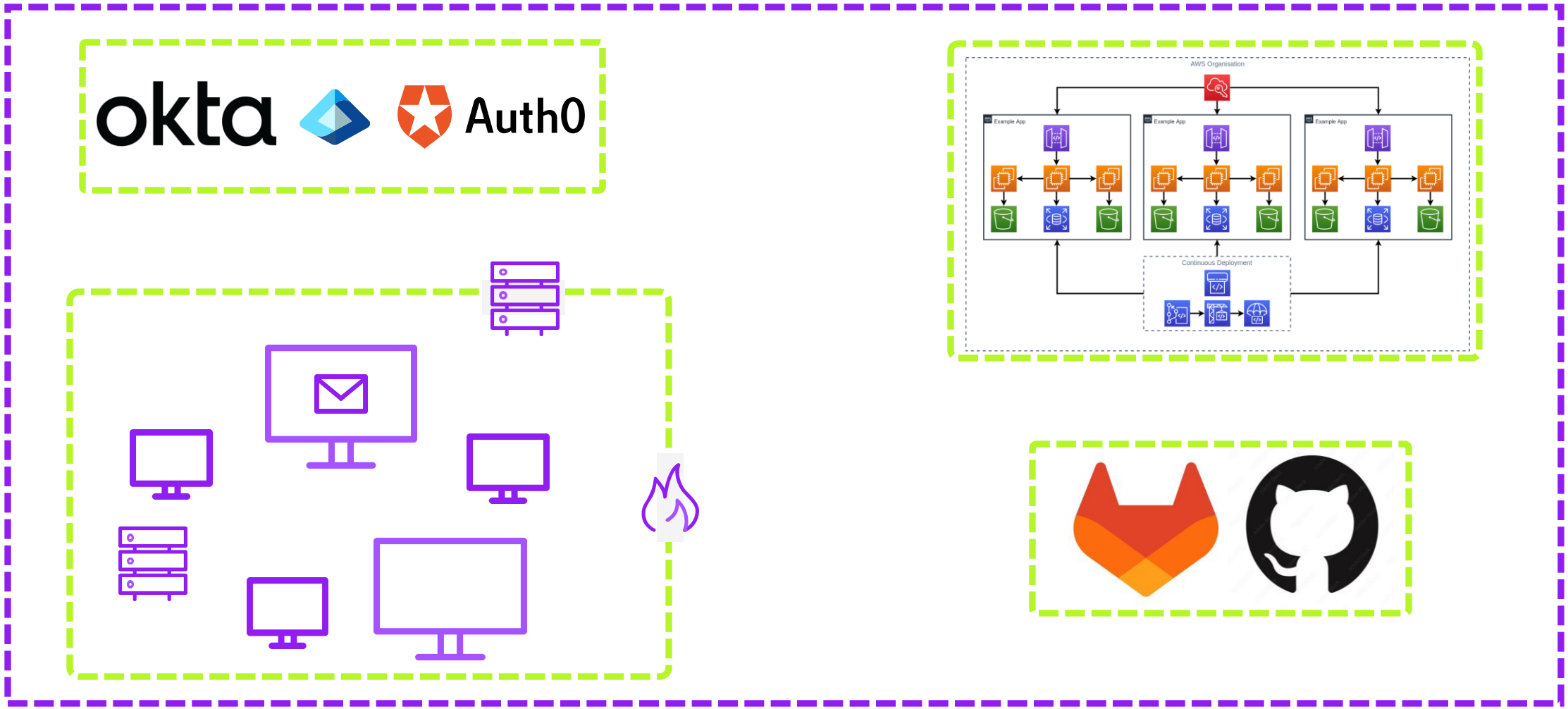
As per usual...

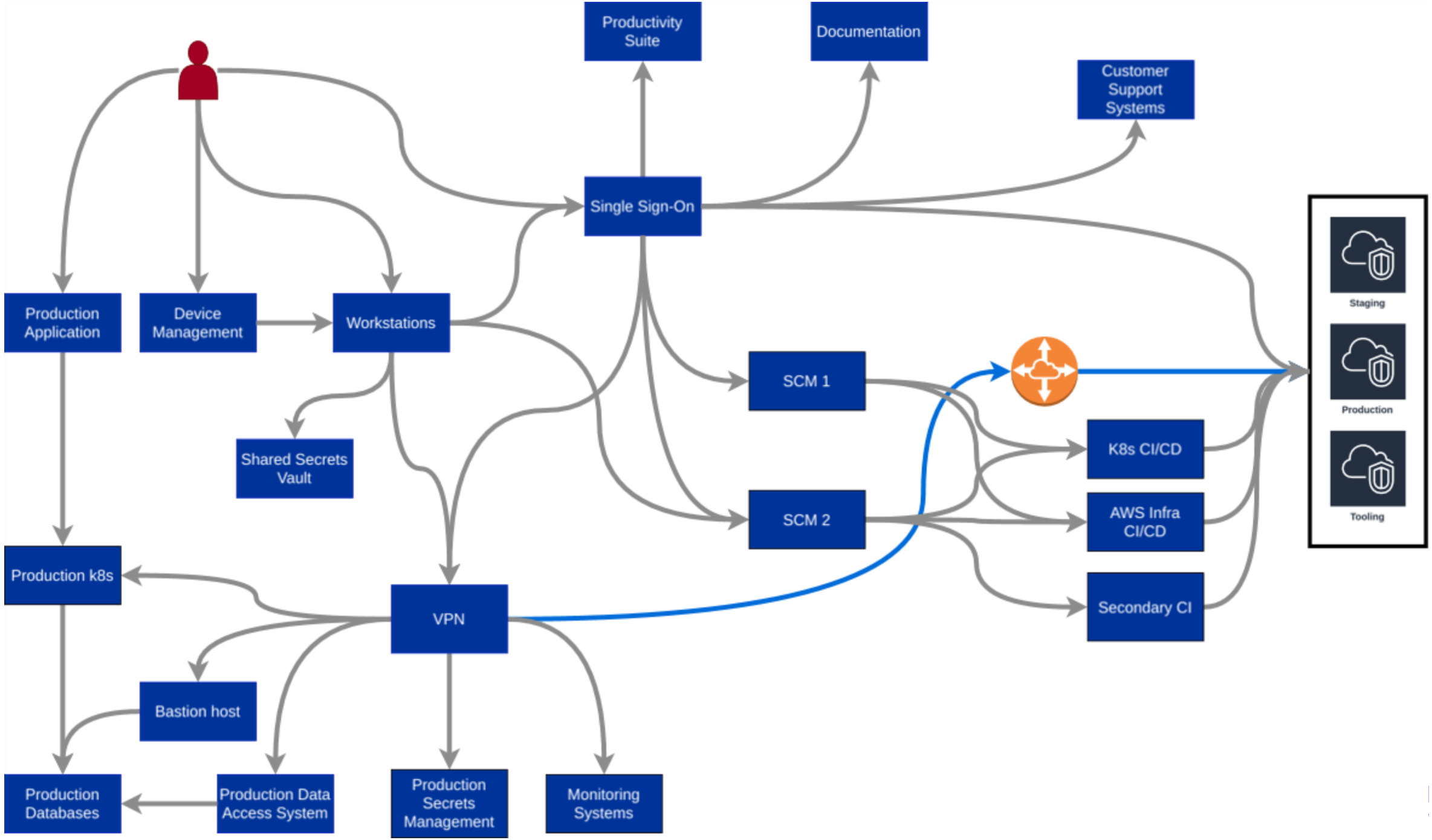
- No budget, no engineers
- We have security consultants!

Agenda

- How do people get breached?
- Where are most organisations weak?
- What should you prioritise?

The Reality of Cloud Security




Productivity Suite
Documentation
Customer Support Systems
Single Sign-On
Production Application
Device Management
Workstations
Shared Secrets Vault
SCM 1
SCM 2
K8s CI/CD
AWS Infra CI/CD
Secondary CI
Staging
Production
Tooling
Production k8s
VPN
Bastion host
Production Databases
Production Data Access System
Production Secrets Management
Monitoring Systems

Attack Vectors

Cloud Native Management Services

Native SSH/RDP aren't great

- Network level access to manage
- Overhead of separate authentication systems
- Harder to log & audit

Cloud Native Admin Tools are *mostly* better

- (Usually) easier identity management, fewer networking concerns
- Caveat: It joins two previously separate security domains
- Your IAM/permissions model needs to be solid!

Cloud Native Phishing

Identity Platforms / SSO

- Okta, Ping, OneLogin, Auth0...
- Single point of access
- Supply chain risk too

Interesting security properties

- Multi Factor Authentication, Conditional Access Policies etc.
- Often poor session management
- Get the session token, get access to ***everything***

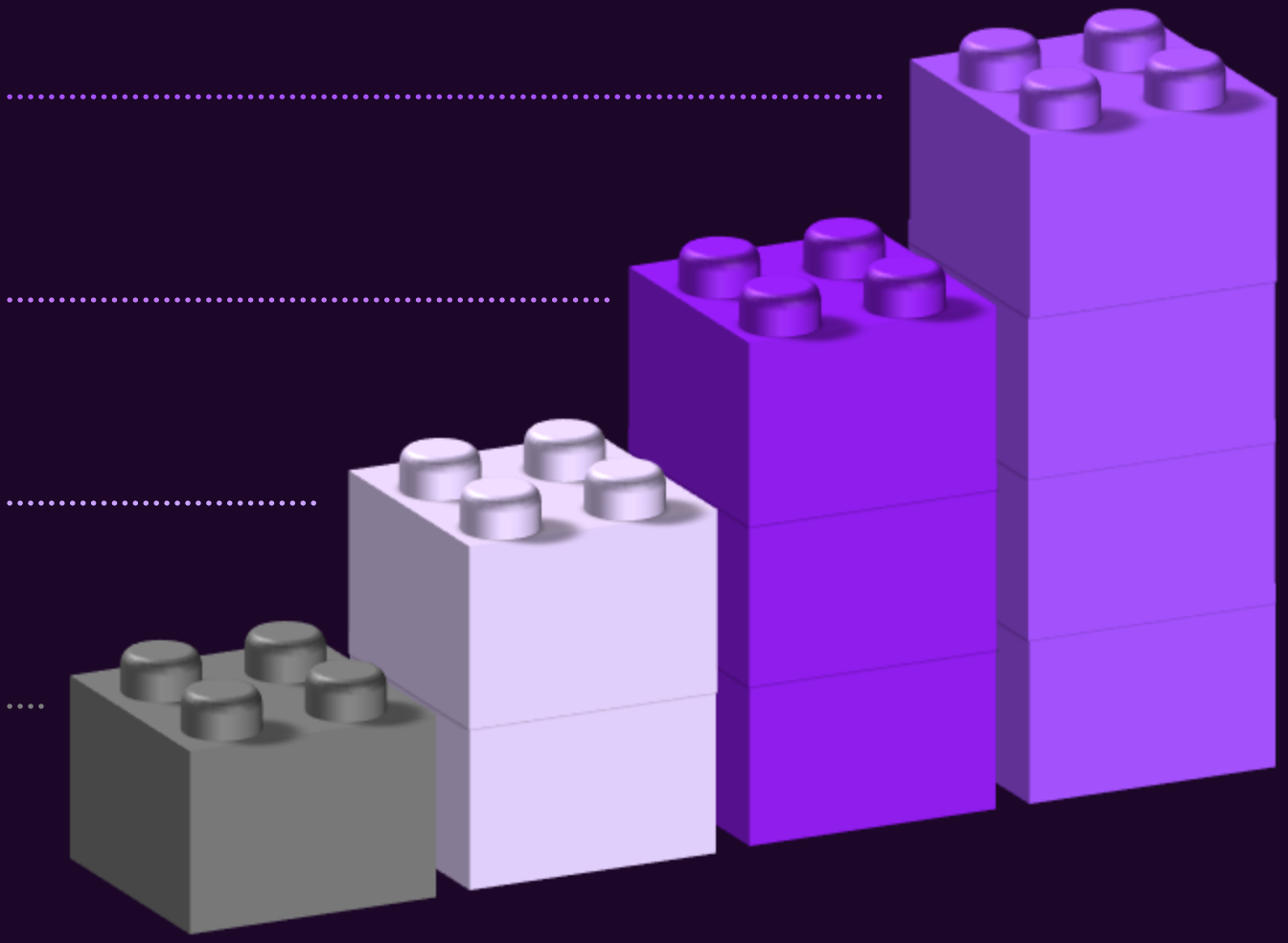
Exploiting Development Workflows

Source Code Management
Everyone uses GitHub or similar to develop and collaborate on their code

CI/CD
Continuous integration & delivery to automate testing & deployment of cloud workloads

Dev Usability > Security
Enabling devs to move at speed often means system architectures & controls are not hardened

Automatic IaC Deployments
IaC changes often automatically deployed after merging – can we bypass approvals process?



Terraform Cloud Exploitation

Pull Request

Opening a GitHub Pull Request triggers Terraform Cloud actions

Terraform Plan

Terraform Cloud runs **terraform init** + **terraform plan**, executing all Terraform code in the process. Posts plan results back to GitHub pull requests as a comment

Code Exec

external resource type references a bash script, which is executed by **terraform plan**

Steal Creds

Bash script can steal and exfiltrate credentials to attacker. Common to find credentials in:

- Environment vars
- Metadata service

OIDC Trust Exploitation

OpenID Connect

Common Method to authenticate external systems (e.g. CI/CD) to AWS

Common to see it misconfigured

Missing “aud” or “sub” condition keys

Broadly scoped “sub” condition keys

Configure own repository to assume role -> gain access

Real World Breaches

Breach Dataset

Inspired by Rami McCarthy's Breach Dataset

- Curated dataset of AWS related security incidents
- https://github.com/ramimac/aws-customer-security-incidents

Highlights

- >60 breaches back to 2014
- >50 incident reports
- Ignores S3 buckets – too many to count!

Inherently Flawed Data

Human Error

Not all breaches get spotted. Missing telemetry, misconfigured alerts etc

Low Hanging Fruit

It's easier to spot well known TTPs and low sophistication attacks than novel/advanced TTPs

Provider Malaise

AWS, Azure, Google, Oracle etc all hate talking publicly about breaches customers suffered while using their services

Open S3 Buckets

The perennial problem

- Biggest source of breaches for years now
- Trivial to find and exploit

Situation is Improving

- AWS providing good options to prevent
- Enable block public buckets everywhere!

Credentials

Most common cloud breach scenario

- Verizon DBIRs say ~70% of cloud breaches

Some fun options:

- Credentials in public repositories
- Insider threat / former employees
- Phishing!

Credential Management

People Problems

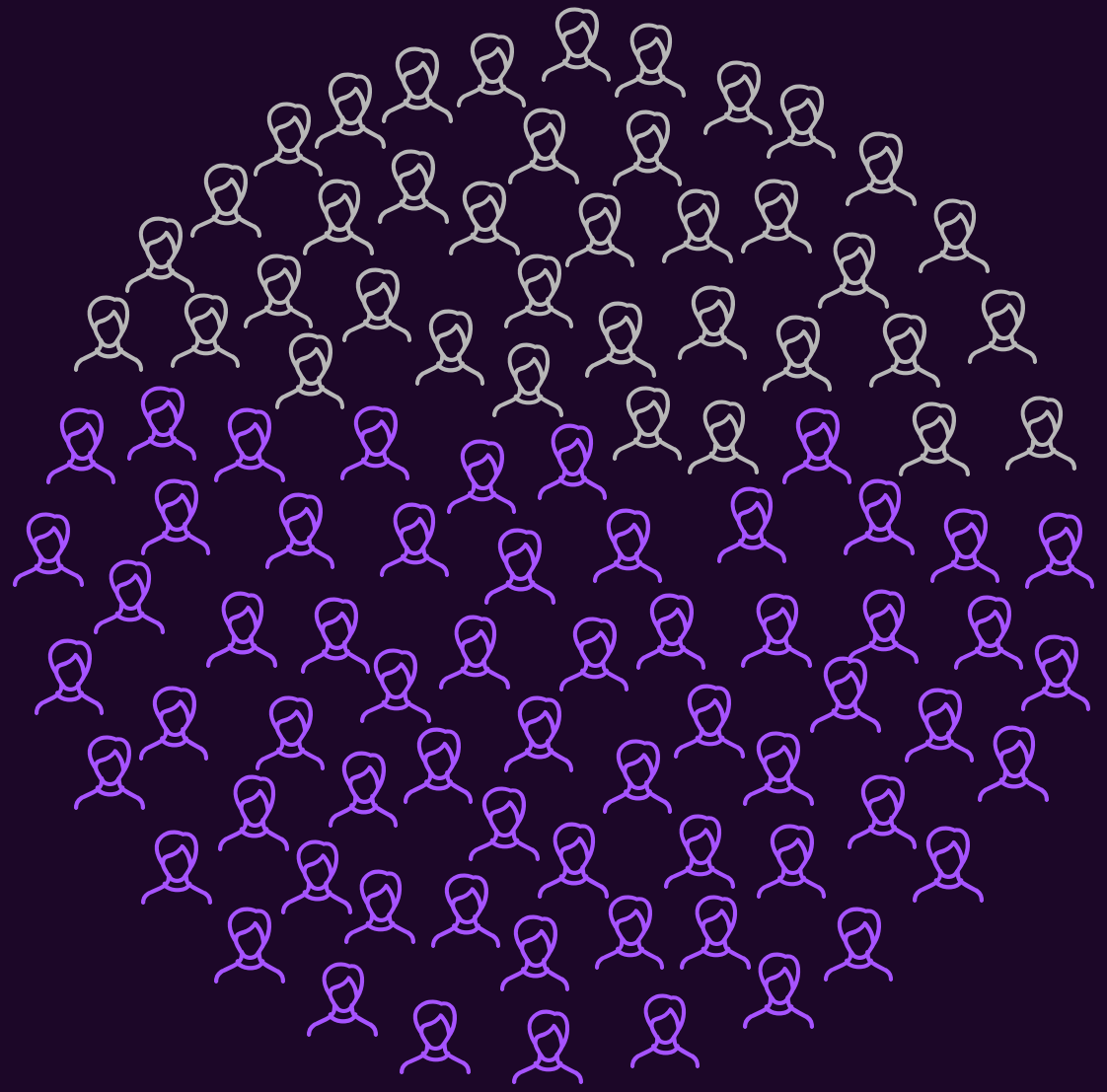
- Disgruntled current/former employees/contractors
- Hard to prevent insider threat
- Proper leaver management **really** important!

Secrets management

- Credentials in repositories
- Shared passwords

44%*

Breaches involving IAM users



* At least, given ambiguity of dataset


NUKE IT FROM ORBIT
ITS THE ONLY WAY TO BE SURE
memegenerator.net

Other Common Themes

AppSec

Application weaknesses out of the OWASP Top 10

Compromised CI/CD

Pivoting in via compromised CI/CD platforms

Phishing an Engineer

Phishing still a major risk, even in the cloud space

S3 Global Write

Somehow, people allow the whole world to write to their S3 buckets

Summary

Attackers look for the easiest path

- Most attacks are opportunistic
- Your org is likely not a priority target
- The basics helps stop APTs too

Most get breached by the basics:

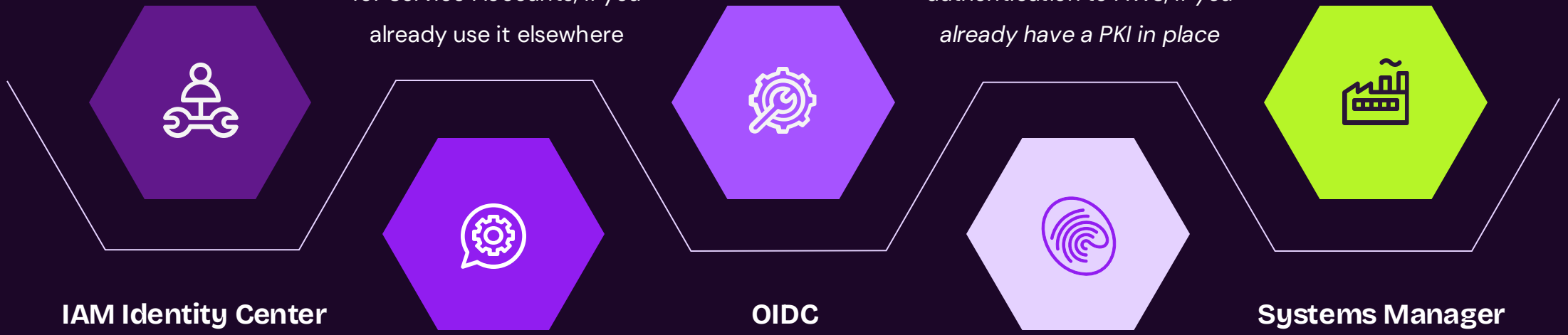
- **Public Storage Accounts**
- Forgotten accounts
- Leaked credentials
- Bad leaver handling

You **probably** won't get breached by:

- Encryption at rest
- Not using *[insert shiny security feature]*
- Zero days
- CSP Insider threat

Doing Good Security in AWS

Replace your IAM Users



IAM Identity Center

For human access. Ideally backed by your main SSO - Entra, Okta, Auth0 etc

EKS Pod Identities

For Kubernetes – IAM Roles for Service Accounts, if you already use it elsewhere

OIDC

OpenID Connect, for cross-cloud & systems authentication to AWS

IAM Roles Anywhere

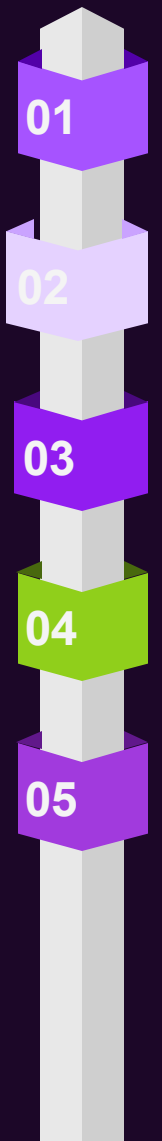
For on premises authentication to AWS, *if you already have a PKI in place*

Systems Manager Hybrid Activation

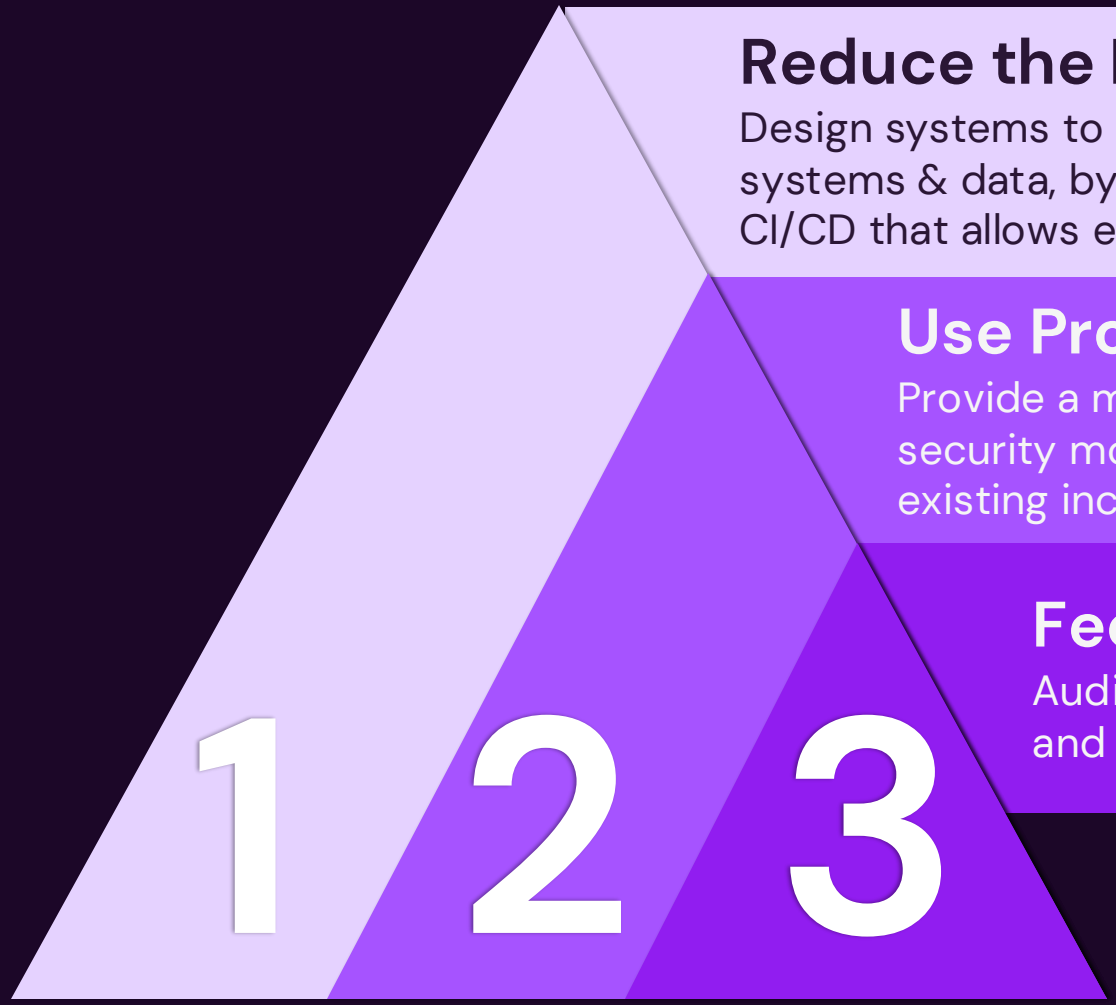
For on premises authentication to AWS, if you don't have PKI deployed

Strong Identity Controls

- Enforce Multi-Factor Authentication (MFA) everywhere
- Apply principle of not-very-much privilege
- Eliminate long-lived credentials
- Use provider-backed authentication where possible
- Automate credential management and rotation



Production Access Control



Reduce the Need for Human Production Access

Design systems to reduce the need for human access to production systems & data, by providing robust production logging capability and CI/CD that allows emergency fixes to be deployed automatically

Use Production Access Control

Provide a means to gain production access that provides a robust security model, audit logs, and an approval workflow that ties into existing incident management processes and systems

Feed PAC logs into your SIEM

Audit logs from PAC should be monitored by security team, and activity tracked against the appropriate incident ticket

Pipeline Hardening

01 Code Scan IaC

Analyse IaC for malicious code on pull request before triggering TFC

02 Four Eyes Checks

Enforce approval on all merges into master

03 Pipeline Assessments

Treat SCM and CI/CD as crown jewels, threat model and pentest accordingly

04 Reduce Attack Surface

Standardise tooling, disable unneeded components

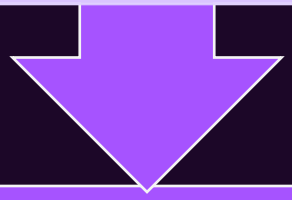
Secrets Management

- Often the key point of failure
- Where do applications store their secrets?
- How are credentials shared and rotated?
- How do you know when secrets are leaked?
- Use Secrets Manager / SSM Parameter Store!

Security Testing Done Right

“Penetration Testing” in AWS

App Assessment/Pentest		
OWASP Top 10	Business logic flaws	API flaws



Cloud configuration review / “pentest”		
Configuration mistakes	IAM permission review	Network layout/SG hardening etc

“Penetration Testing” Mostly Sucks

Basic config audits often called “pentests”

Driven by audits, not threats

Cloud engineering moves too fast

Low return on investment

Usually ignores critical supporting systems

What To Do Instead?

Automate

Leverage automation to drive as much security as possible

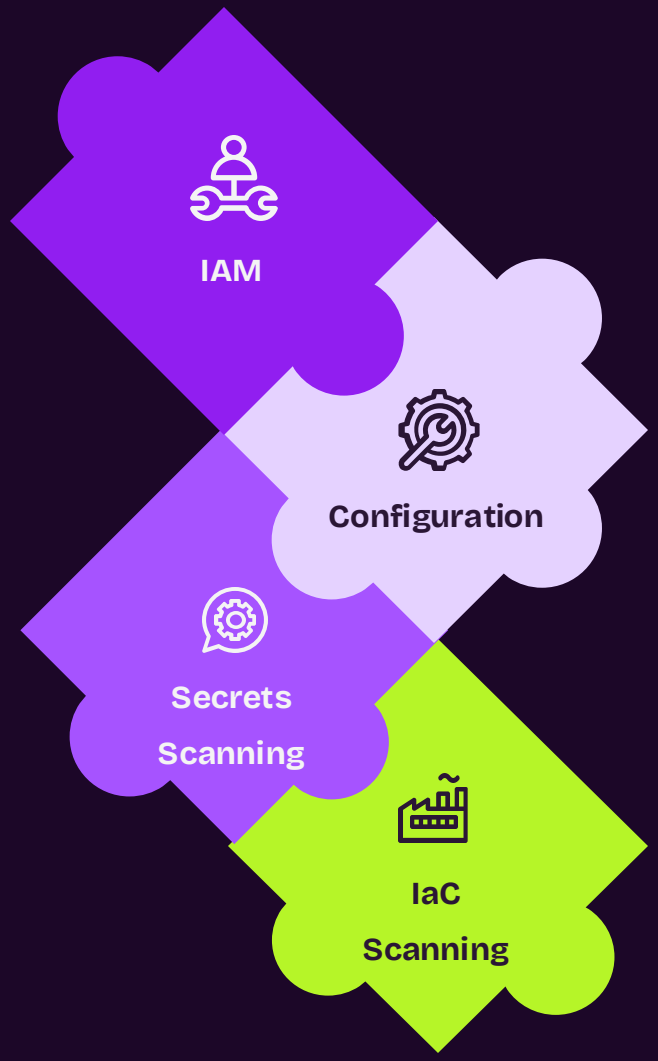
Assess

Use humans to find the rest, and simulate attackers

AI for CloudSec

- Explosion of new AI tools – security no different
- As ever, issues with hallucinations and misunderstandings
- Lot of potential, though – watch this space!
- For now, treat like a junior engineer on steroids

Security Automation



IAM

Identify IAM misconfigurations

Cloudsplaining, pmapper, iamgraph, IAMSpy, cloudfox

Configuration Analysis

Look for common/basic misconfigurations

Prowler, scoutsuite

Secrets Scanning

Spot secrets when they're committed/leaked so you can rotate them

Trufflehog, detect-secrets

IAC Scanning

Spot configuration mistakes before deployment

Checkov, tflint, tfscan

Human-Led Reviews

Objective-Driven Assessments

Business targets

- Steal key data/IP
- Move money
- Deploy malicious code to prod

Realistic starting points

- Leaked access keys
- Compromised dev/insider threat
- Application compromise

Don’t buy a “Red Team”

You probably don’t need one

- All about stealth, validating detection and response
- Depth, not breadth

Red Teaming is the final step

- Confirm and harden your attack surface
- Build your detection and response
- Test hardening, detection & response collaboratively
- … **then** maybe a red team!

Collaborating with Security Consultants

If You're Going to Buy a Penetration Test...

Make it work for you

- Fit their testing and reporting into your workflows
- Push for deep advice and long-term solutions
- Ensure what they propose to do addresses your concerns

Find a good partner

- Do they understand AWS/Cloud/DevOps?
- Can they show you relevant and novel R&D?
- Use engineers to vet providers' technical knowledge

Help Us Help You!

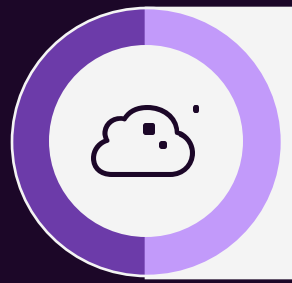
Access

- Give us read access to the AWS accounts
- If you're using IaC, show us that too

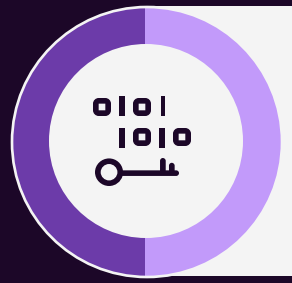
Work with us

- Help us understand what you've built
- Show us problems, help us design solutions
- Stay engaged and communicative with testers

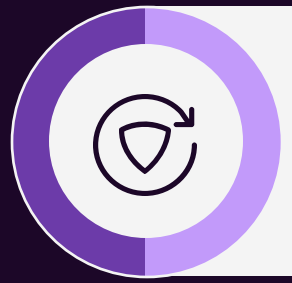
Conclusions



Security of the cloud extends to include a lot of external factors



Focus on identity, secrets management and CI/CD



Leverage automation and be smart about how you use humans

Staying Up To Date

Social Media

Twitter still king, sadly. See https://www.nojones.net/cloud-security-resources for some names to get you started

Slack

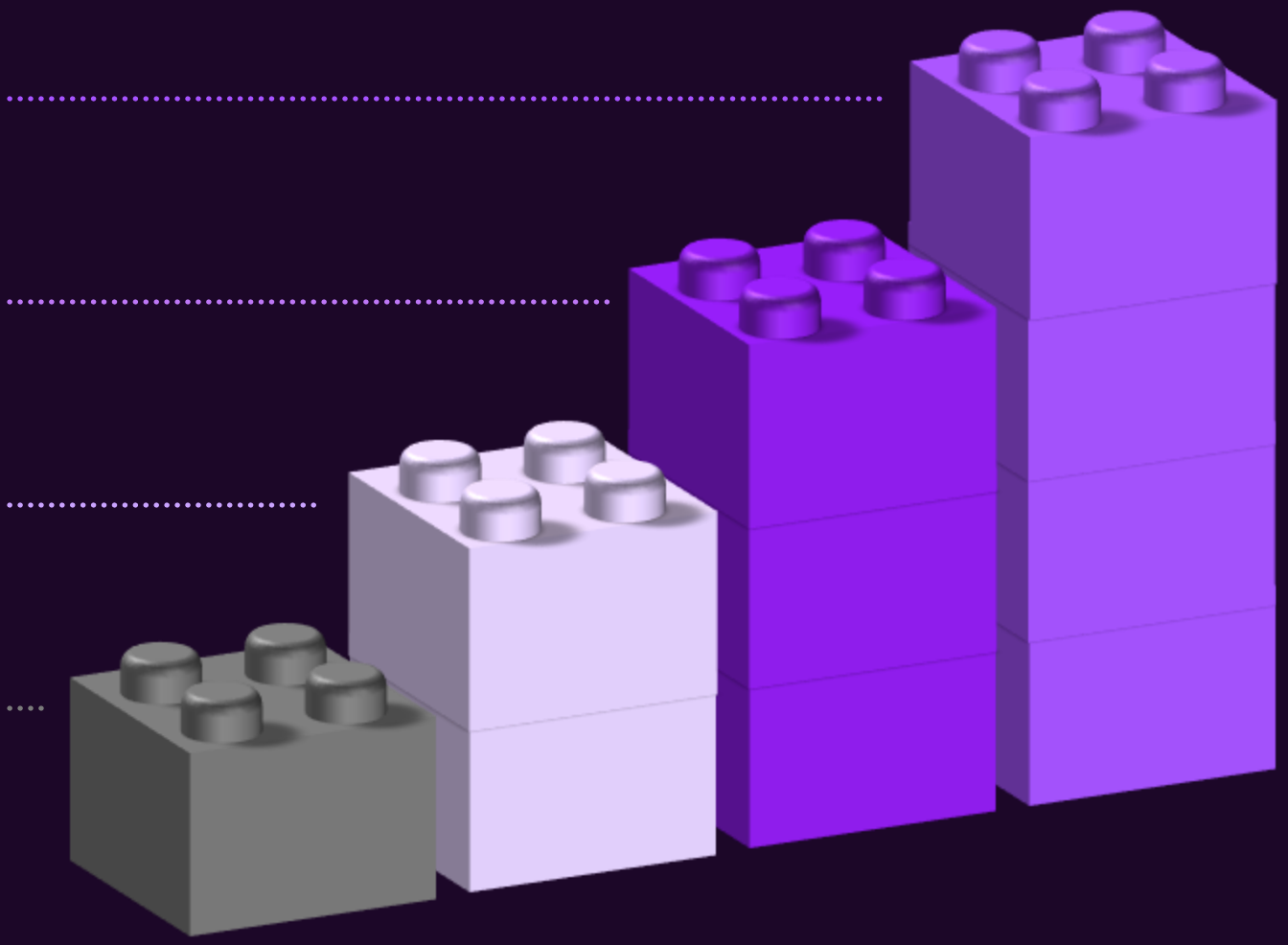
Fwd:cloudsec slack workspace: https://fwdcloudsec.org/forum/

Conferences

Fwd:cloudsec NA + EU years ahead of the others, generally. DEF CON Cloud Village, Black Hat, etc. *sometimes* good

Local Meetups

AWS User Groups, Cloud Security Alliance Norway, OsloSec, BSides Oslo etc



Thanks for Listening!

https://www.nojones.net
Cloud Security Forum Slack: @Nick Jones
X: @nojonesuk
https://www.linkedin.com/in/nickojones/