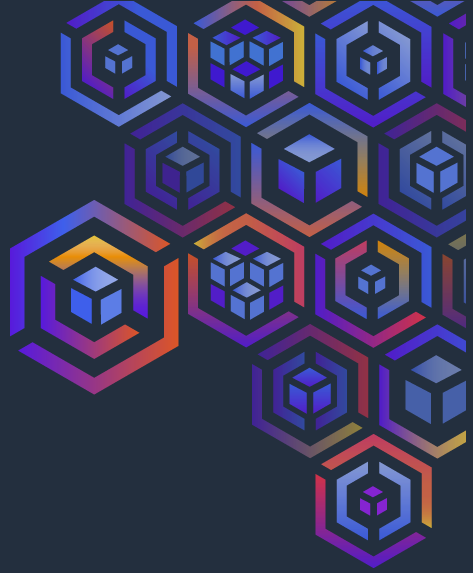

Nordea
knowit
NITOR
alma
CLOUD²
aws
COMMUNITY DAY
NORDICS
2023
Nordea Vallila Campus Helsinki

aws

COMMUNITY DAY

NORDICS



Securing AWS Estates at Scale

Nick Jones | 2023-04-20

Nordea knowit NITOR alma CLOUD²

aws

COMMUNITY DAY

aws sts get-caller-identity

Nick Jones – @nojonesuk

- Principal Consultant @ WithSecure
- AWS Community Builder
- Previously presented at:
  - fwd:cloudsec
  - RSA Conference
  - Disobey, CitySec Mayhem, T2.fi
  - +++

aws
COMMUNITY DAY

Agenda

- Common Misconceptions
- Real World Breach Scenarios
- What We See
- Key Security Controls
- Getting The Most From External Security Testing

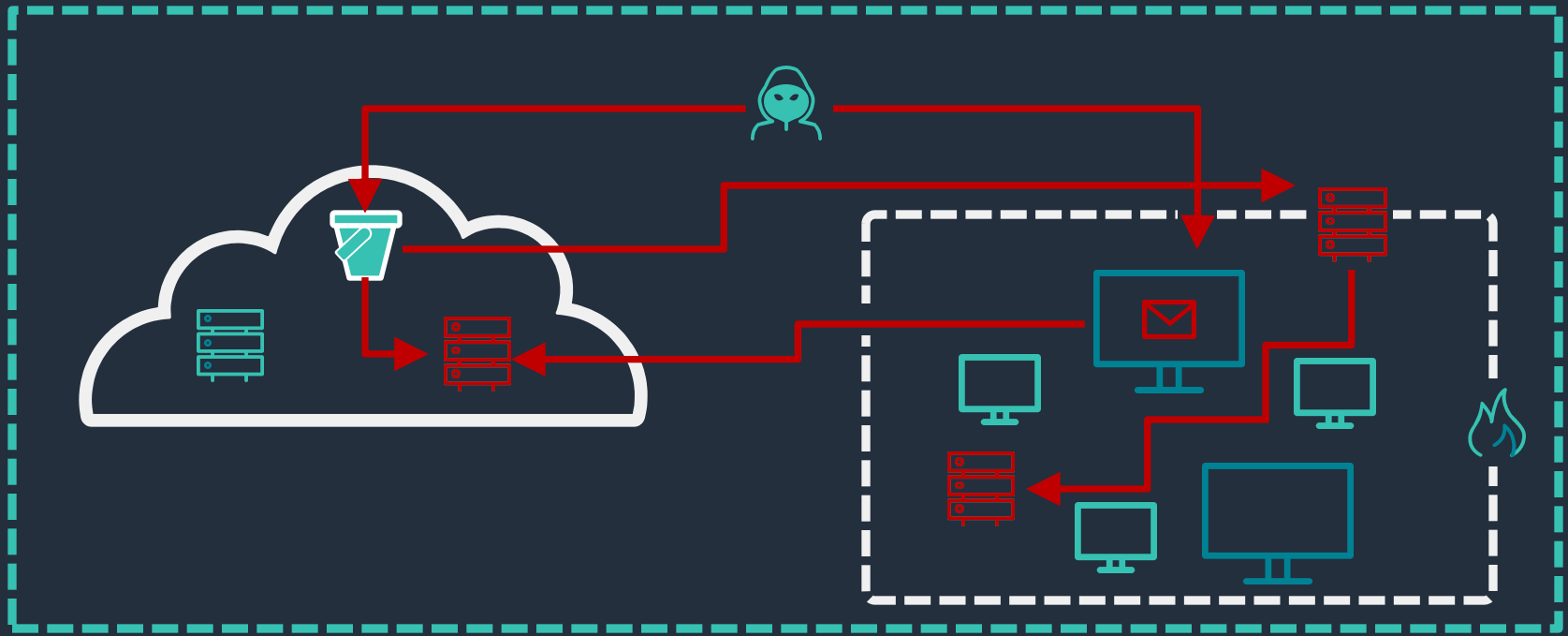
aws

COMMUNITY DAY

Security's Idea of Cloud

aws

COMMUNITY DAY



aws
COMMUNITY DAY

Real World Security

Attackers look for the easiest path	Most people get screwed by basics:	You p**robably** won't get breached by:
• Most attacks are opportunistic • The basics helps stop APTs	• **Public S3 buckets** • Forgotten AWS accounts • Leaked credentials • AdministratorAccess everywhere	• Encryption at rest • Not using the Nitro Enclaves etc • Zero days • AWS Insider threat

Real World Breach Scenarios

aws

COMMUNITY DAY

NORDICS

Breach Dataset

Rami McCarthy's Breach Dataset

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

Highlights

- 45 breaches back to 2014
- 21 incident reports
- Ignores S3 buckets – too many to count!

aws
COMMUNITY DAY

Inherently Flawed Data

- Not all breaches get spotted
- Providers hate talking about it
- Focus on low hanging fruit

aws
COMMUNITY DAY

A note on Zero Days

Cool but mostly irrelevant

- >120 vulns, 1 exploited ITW, no breaches reported
- https://www.cloudvulndb.org

Expect this to change

- Wiz, LightSpin, Orca + others doing lots here
- Watch fwd:cloudsec 2022 keynote from Wiz

aws
COMMUNITY DAY

Open S3 buckets

The perennial problem

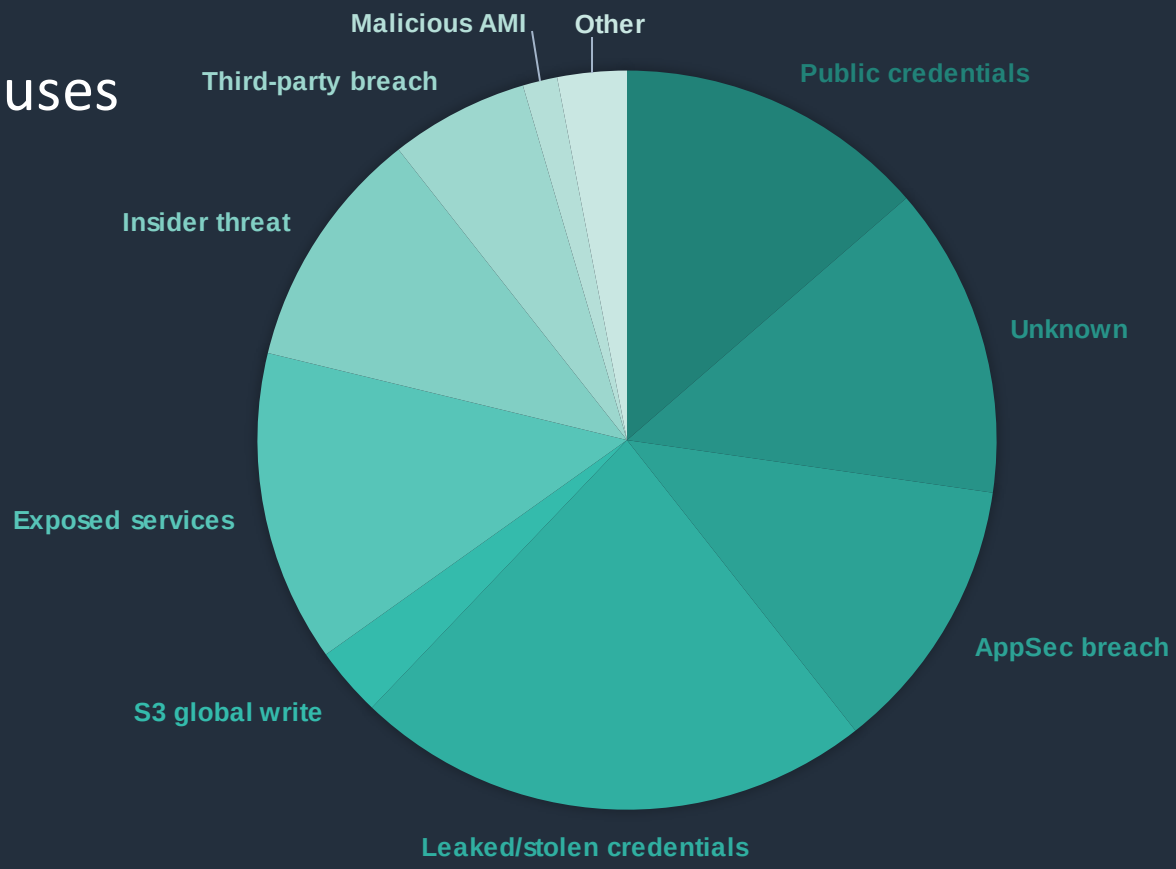
- Biggest source of breaches
- Trivial to find and exploit

Situation is Improving

- AWS offers options to prevent
- **Enable block public buckets everywhere!**

aws
COMMUNITY DAY

Breach Causes



aws

COMMUNITY DAY

NORDICS

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!

aws

COMMUNITY DAY

NORDICS

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

aws

COMMUNITY DAY

44%*

Breaches involving IAM users

* At least, given ambiguity of dataset

aws

COMMUNITY DAY

Other Interesting Attack Vectors

aws
COMMUNITY DAY

Identity Platforms / SSO

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

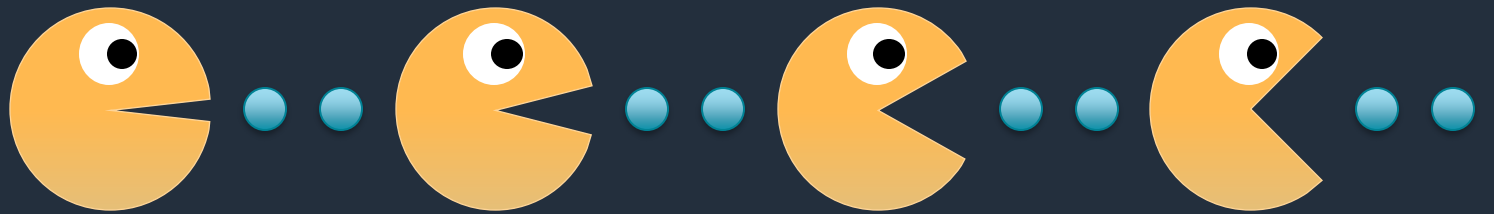
Interesting security properties

- MFA, Conditional Access Policies…
- Often poor session management
- Get the session token, get ***everything***

aws

COMMUNITY DAY

Cloud Style Shell Popping!



Phish a Developer
Steal their SSO session token

Login to AWS
Use the session token to authenticate

Recon
What services is the target using? SSM!

Pop Shells
Use our access to get shells on EC2 instances

Objective
Root an EC2 instance full of data

aws

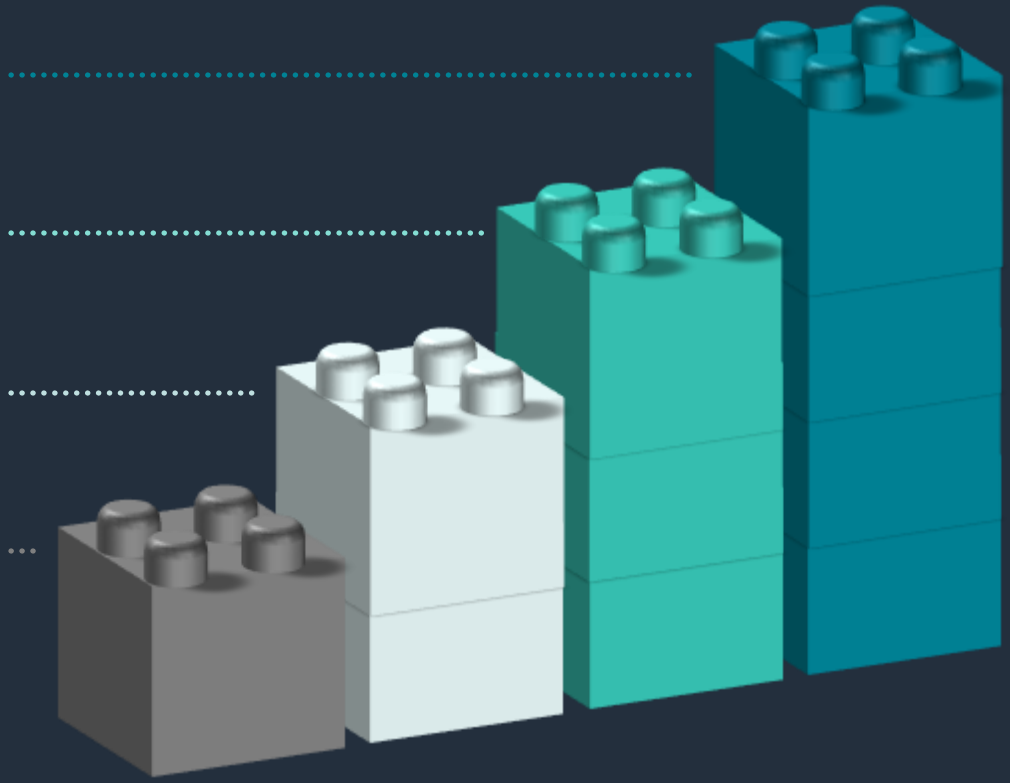
COMMUNITY DAY

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

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

Dev Usability > Security
Enabling dev velocity often means system architectures and controls are not well hardened

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



aws

COMMUNITY DAY

DevOoooops

Objective
Admin access over production

Malicious Insider
Default developer access

Access GitHub
Find some interesting IaC repositories

Malicious Pull Request
Exploit Terraform Cloud's operating model

Exfiltrate Credentials
Grab the credentials Terraform Cloud uses to deploy

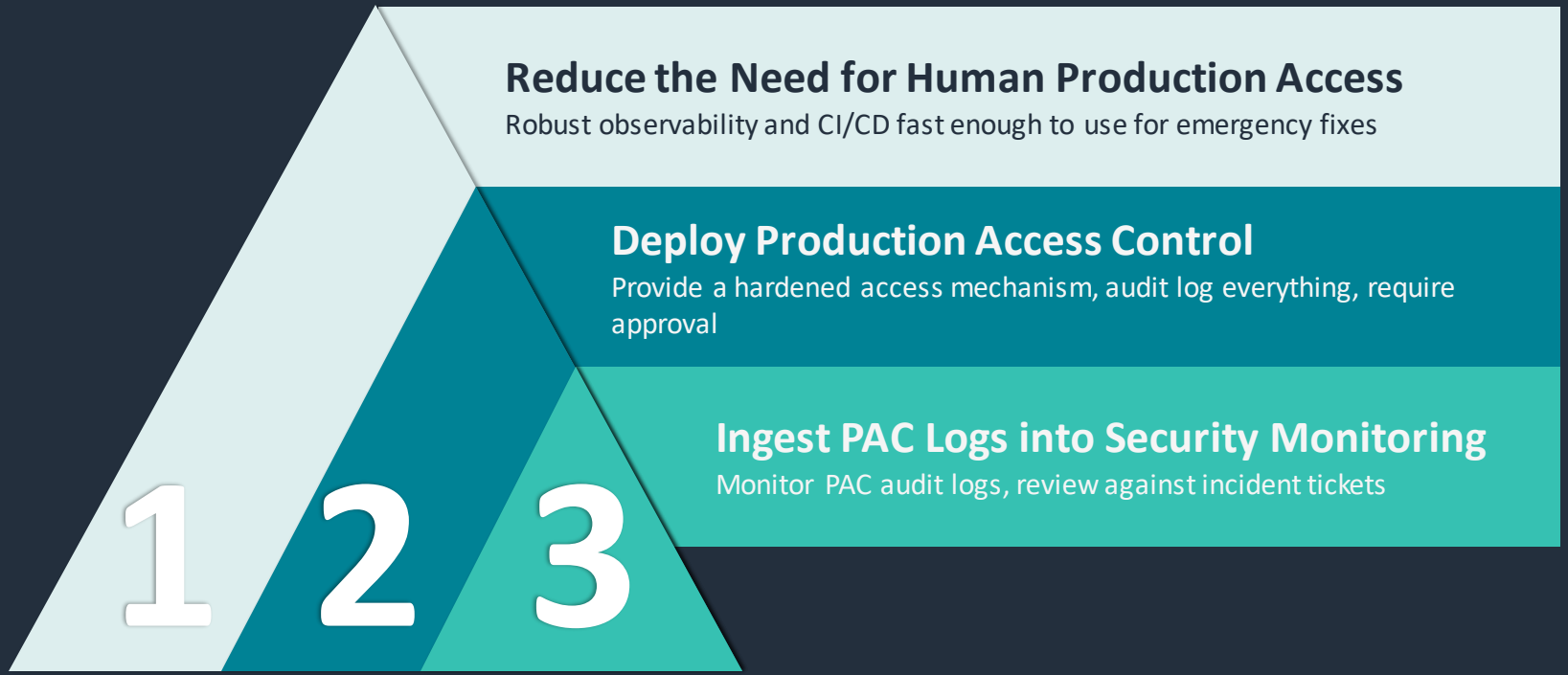
aws
COMMUNITY DAY

Identity Management

- Multi-Factor Authentication (MFA) everywhere
- Principle of not-very-much privilege
- Eliminate long-lived credentials (**IAM USERS!**)
- Use IAM Roles where possible
- Automate credential management and rotation

aws
COMMUNITY DAY

Production Access



aws

COMMUNITY DAY

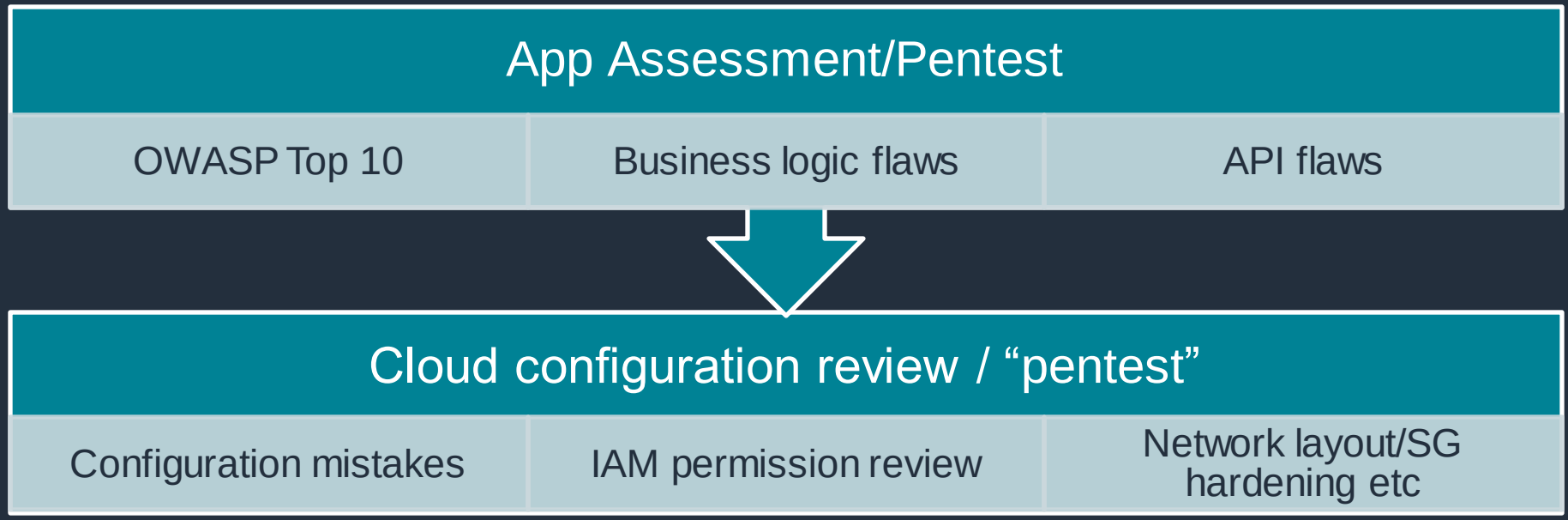
Secrets Management

- 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

aws
COMMUNITY DAY

“Penetration Testing” in AWS



aws

COMMUNITY DAY

NORDICS

“Penetration Testing” Mostly Sucks

- Driven by audits, not threats
- Cloud engineering moves too fast
- Low return on investment
- Ignores critical supporting systems

aws
COMMUNITY DAY

What To Do Instead?

Automate

Leverage automation to drive as much security as possible

Assess

Use humans to find the rest, and simulate attackers

aws

COMMUNITY DAY

02 IaC Scanning

Scan Infrastructure as Code in pipelines

Checkov
TFLint

01 Configuration

Assess resources for configuration issues

Prowler
ScoutSuite

Secrets Scanning 04

Scan repositories for keys, certificates etc

TruffleHog
detect-secrets

IAM 03

Identify IAM misconfigurations

Cloudsplaining
Pmapper
IAMSpy

aws
COMMUNITY DAY

Human-led reviews

aws
COMMUNITY DAY

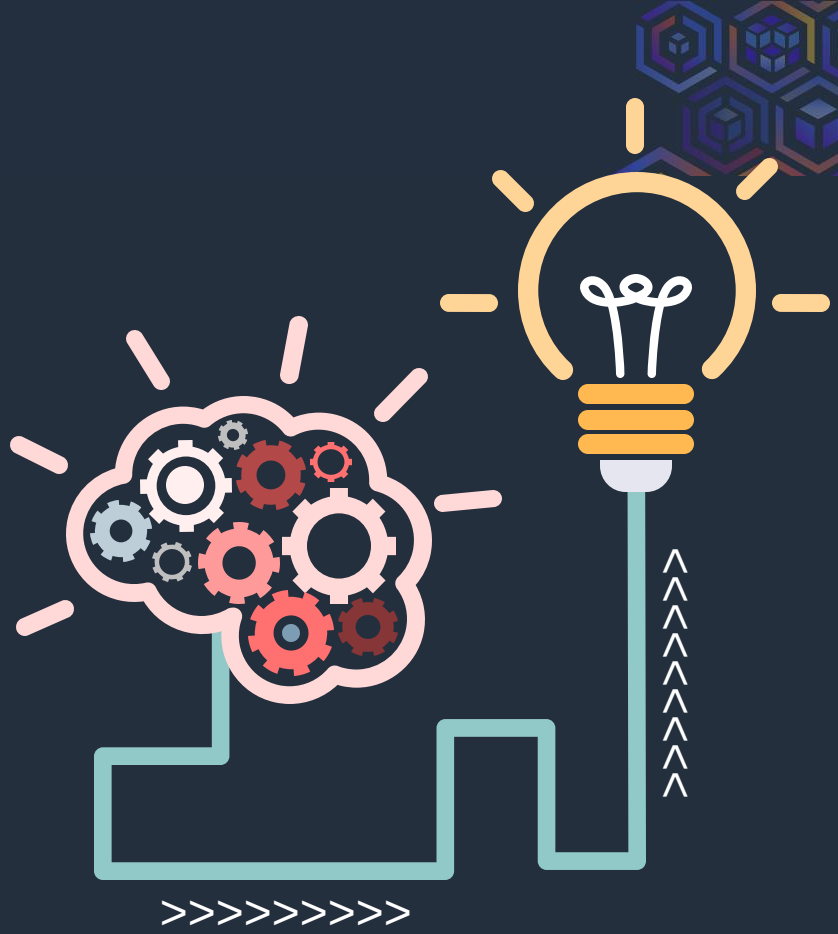
Objective-Driven Assessments

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



aws
COMMUNITY DAY

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

aws

COMMUNITY DAY

NORDICS

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

Find a good partner

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

aws

COMMUNITY DAY

NORDICS

Help Us Help You!

Access

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

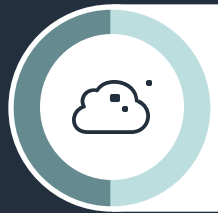
Work with us

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

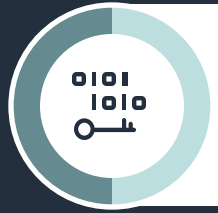
Conclusions

aws

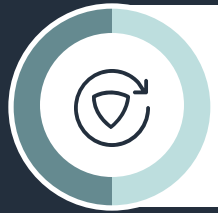
COMMUNITY DAY



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



Focus on IAM (especially users!), secrets management and CI/CD

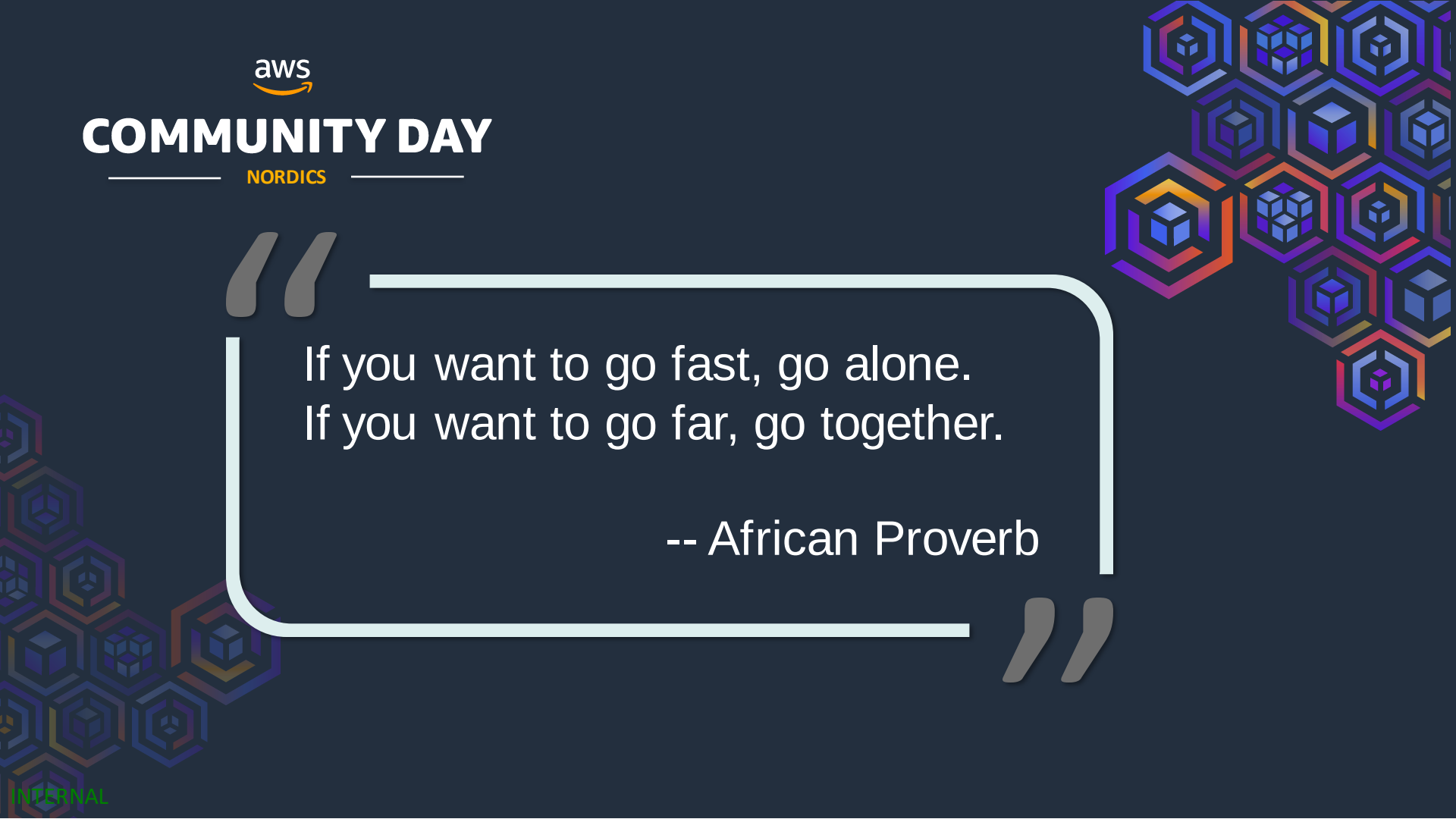


Leverage automation and be smart about how you use humans

aws

COMMUNITY DAY

NORDICS

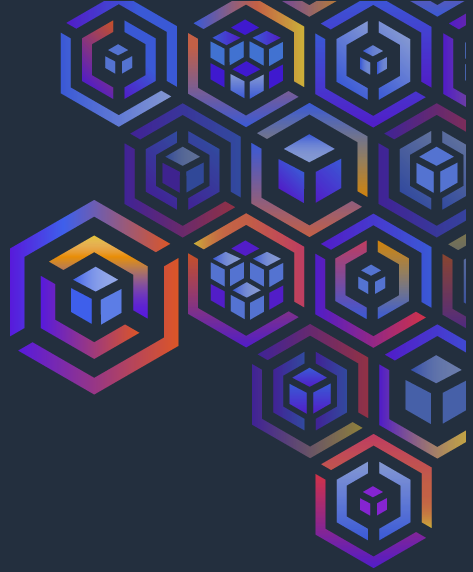


> If you want to go fast, go alone.
> If you want to go far, go together.
>
> -- African Proverb

aws

COMMUNITY DAY

NORDICS



Thank you!

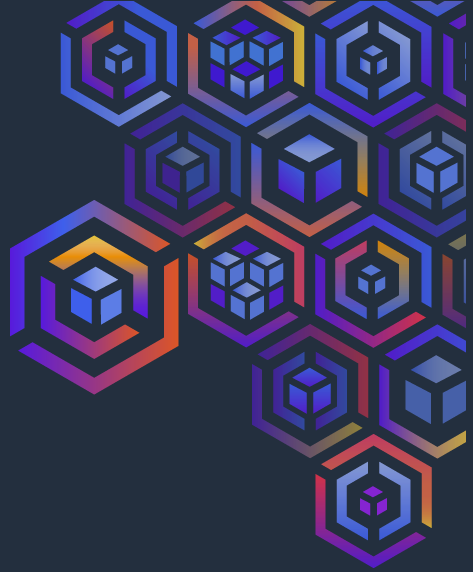
https://twitter.com/nojonesuk + https://www.nojones.net

Nordea knowit NITOR

aws

COMMUNITY DAY

NORDICS



This is a simple title slide

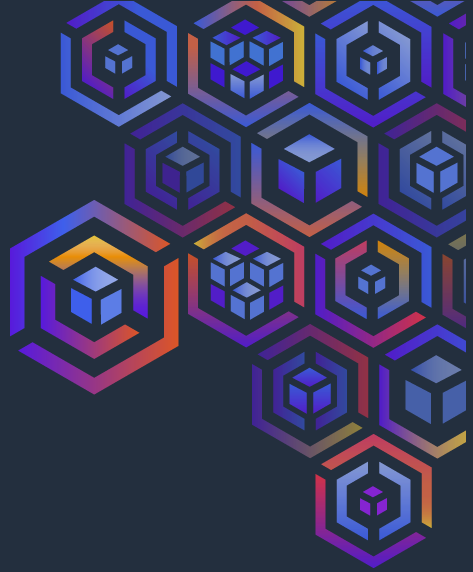
PRESENTER | DATE

aws

COMMUNITY DAY

NORDICS

Title + Content



aws

COMMUNITY DAY

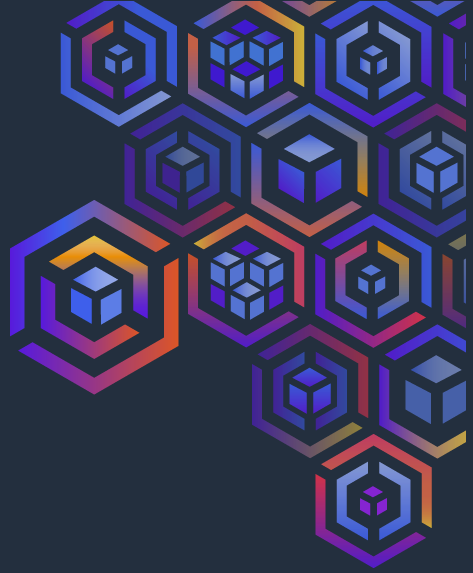
Alt title + content 1

aws

COMMUNITY DAY

NORDICS

Code Snippet



Section Title

aws

COMMUNITY DAY

Two columns

aws

COMMUNITY DAY

Comparison

aws

COMMUNITY DAY

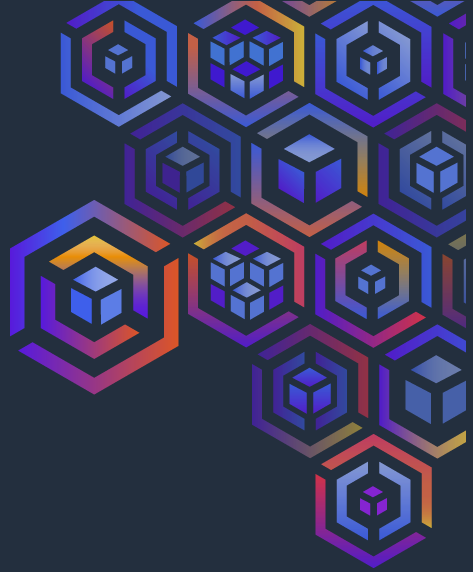
Three column

aws

COMMUNITY DAY

NORDICS

Four column with graphics



aws

COMMUNITY DAY

Six section with graphics