How to Avoid Security Breaches in the Cloud

Nick Jones – Telia Digital Hub 2023

WITH secure

About Me

Nick Jones

- Principal Consultant @ WithSecure
- Cloud Security Consulting Lead
- AWS Community Builder
- Focus on:
  - Security automation
  - Attack detection
  - Security as an enabler for engineering

Agenda

- What are the common breach scenarios in modern cloud infrastructure?
- Which attack vectors are organizations most vulnerable to?
- What are the key security controls to implement for a robust cloud defense?
- How can organizations future-proof their cloud security?

Common Breach Scenarios

WITH secure

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

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

A Note on Cloud Zero Days

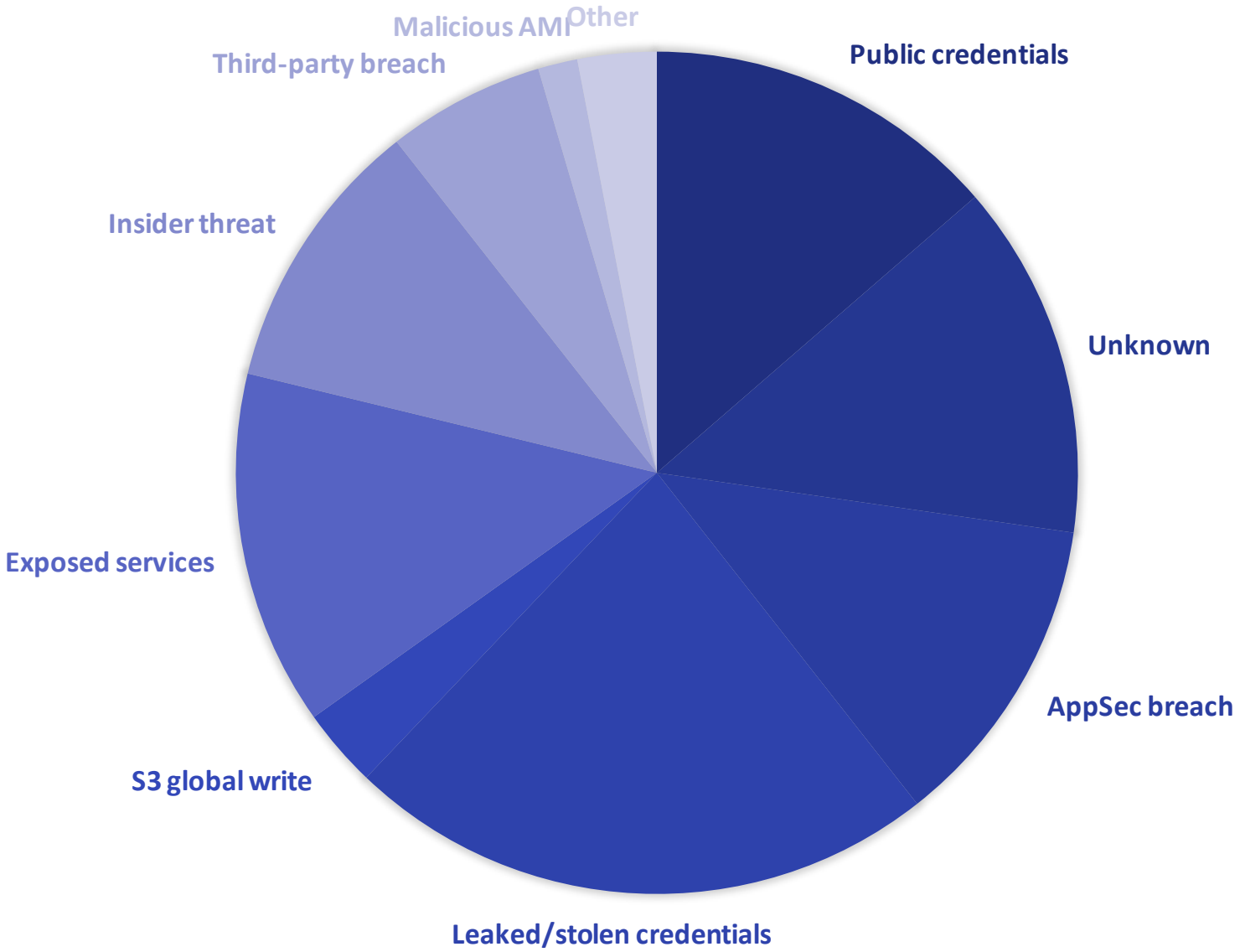
Cool but mostly irrelevant

- CloudVulnDB tracking >120 vulns
- One exploited in the wild, no breaches reported
- https://www.cloudvulndb.org

Expect this to change

- Big focus on this from several research teams
- fwd:cloudsec 2022 keynote from Wiz is a good overview

Breach Causes



W / T H secure

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

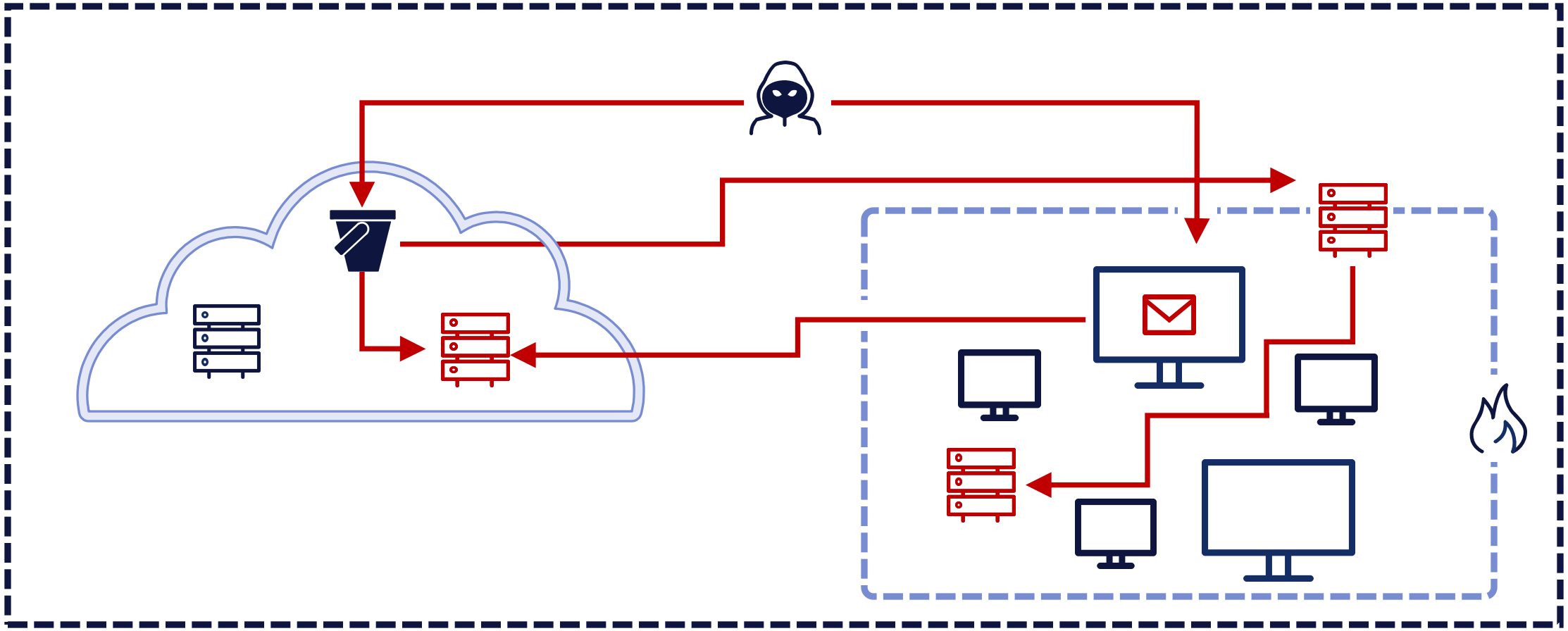
You **probably** won't get breached by:

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

Other Attack Vectors

WITH secure

Attackers Target Everything



W/TH secure

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***

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!

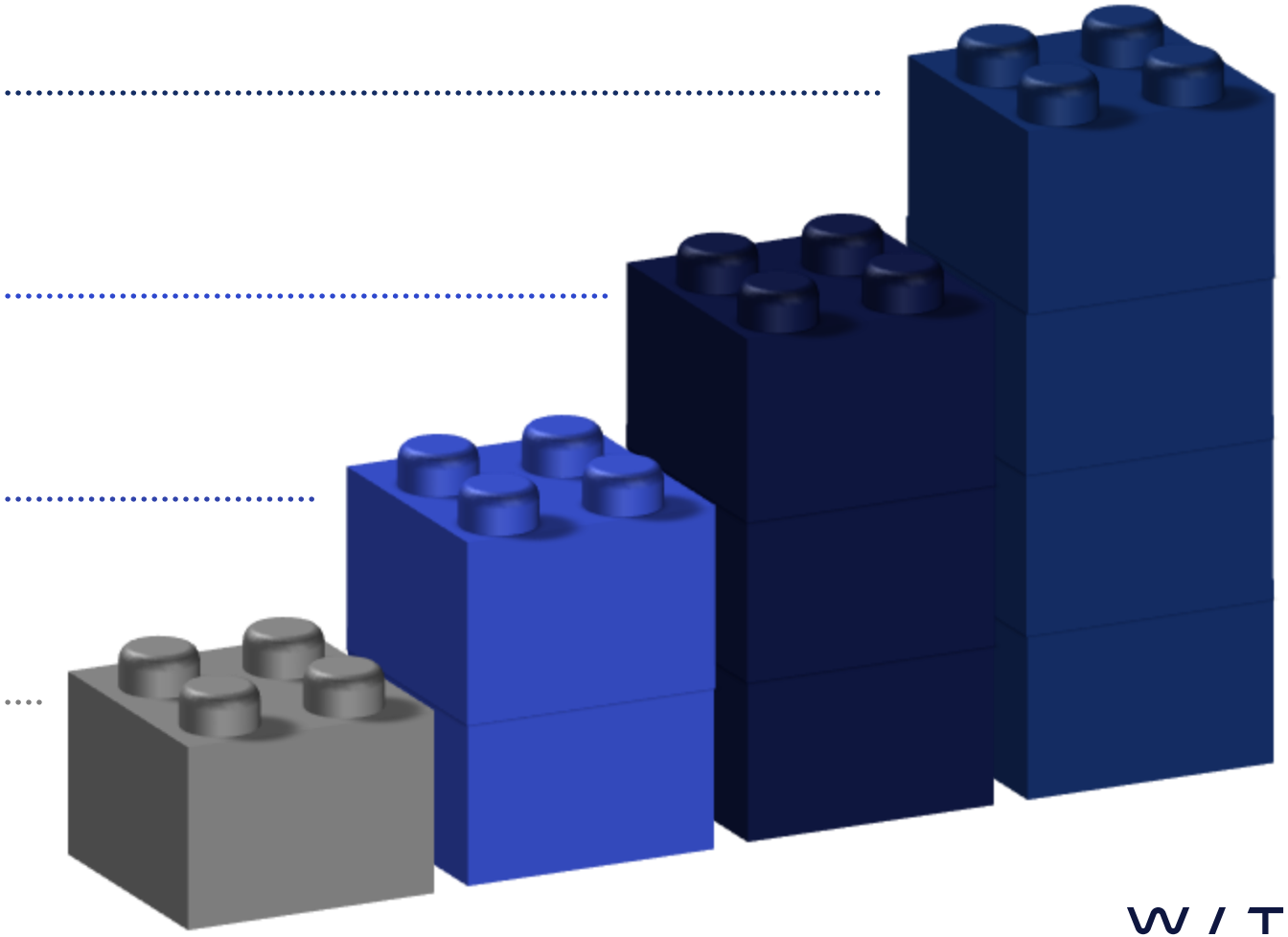
Exploiting Development Workflows

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 devs to move at speed 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?



W/TH secure

Key Security Controls

WITH secure

Strong Identity Controls

01 Enforce Multi-Factor Authentication (MFA) everywhere

02 Apply principle of not-very-much privilege

03 Eliminate long-lived credentials

04 Use provider-backed authentication where possible

05 Automate credential management and rotation

WITH secure

Production Access Control

1

Reduce the Need for Human Production Access

Design systems to reduce or eliminate the need for humans to access production systems and data, by providing robust production logging capability and CI/CD that allows emergency fixes to be deployed without human intervention

2

Use Production Access Control

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

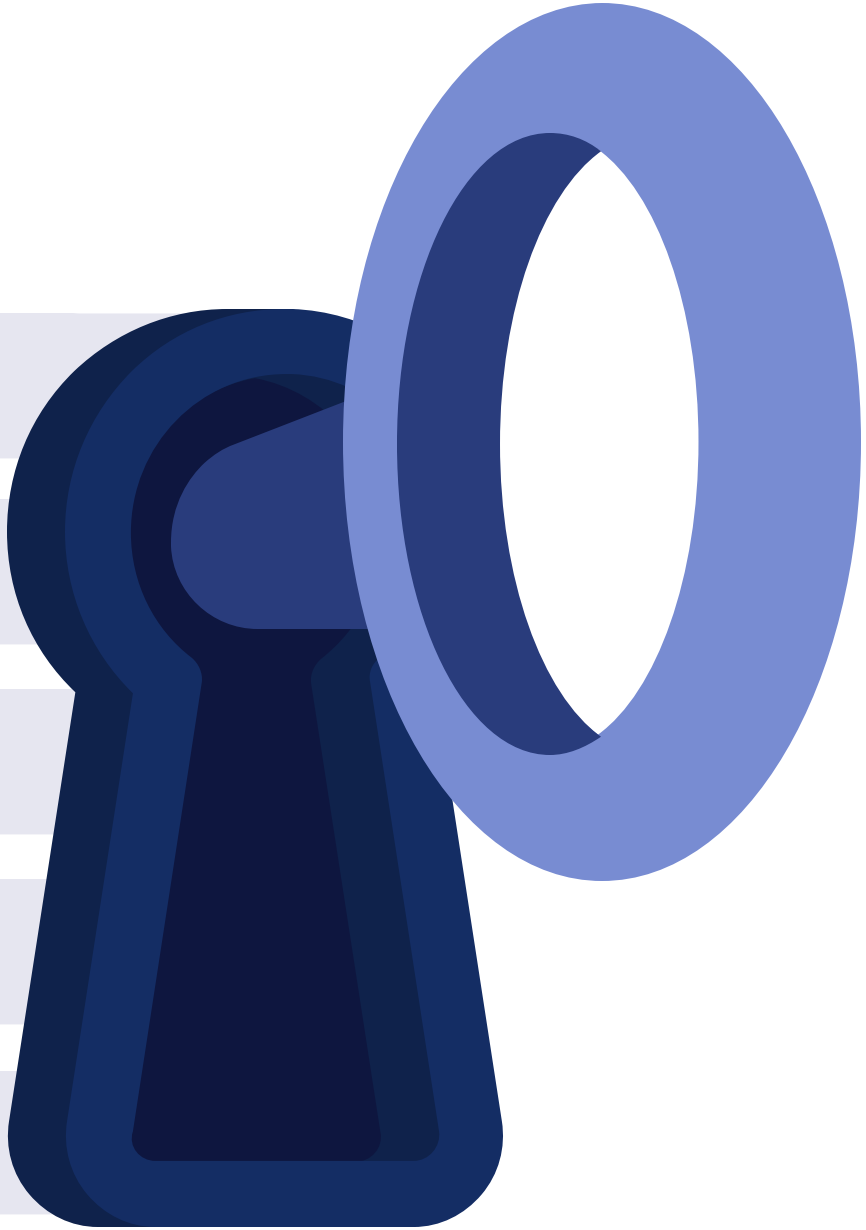
3

Feed PAC logs into your SIEM

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

Secrets Management

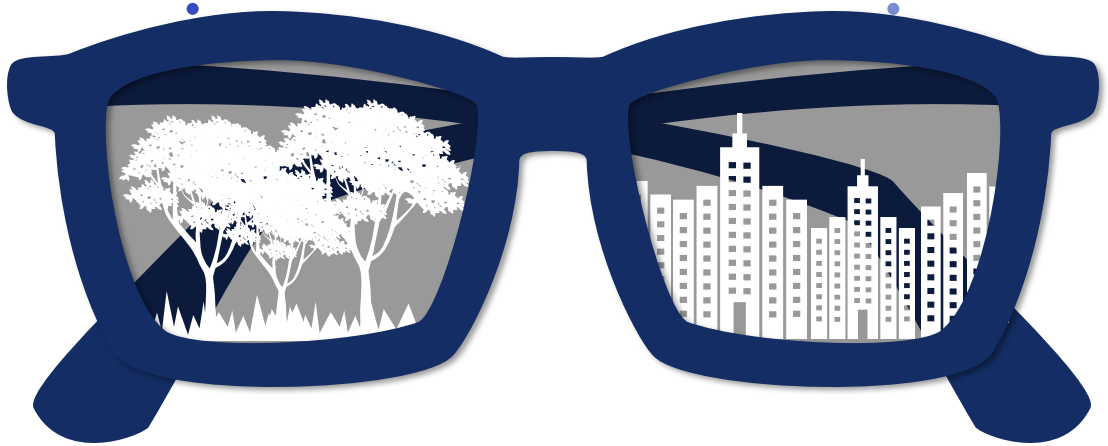
- Often the key point of failure
- Where do applications store their secrets?
- How are credentials shared and rotated?
- How do you know when secrets are leaked?
- Use your CSP’s secrets storage services!



Future-Proofing Your Cloud Security

WITH secure

Two Key Focus Areas



Automate

Leverage automation to drive as much security as possible

Leverage

Human-led work to cover automation gaps, validate end-to-end, and improve processes

WITH secure

Security Automation

04 Secrets Scanning

Scan repositories for keys, certificates etc.

TruffleHog
detect-secrets

02 IaC Scanning

Scan Infrastructure as Code in pipelines

Checkov
TFLint

IAM 03

Identify IAM misconfigurations

Cloudsplaining
StormSpotter
BloodHound
IAMSpy

01 Configuration

Assess resources for configuration issues

Prowler
ScoutSuite

WITH secure

Human-led reviews

WITH secure

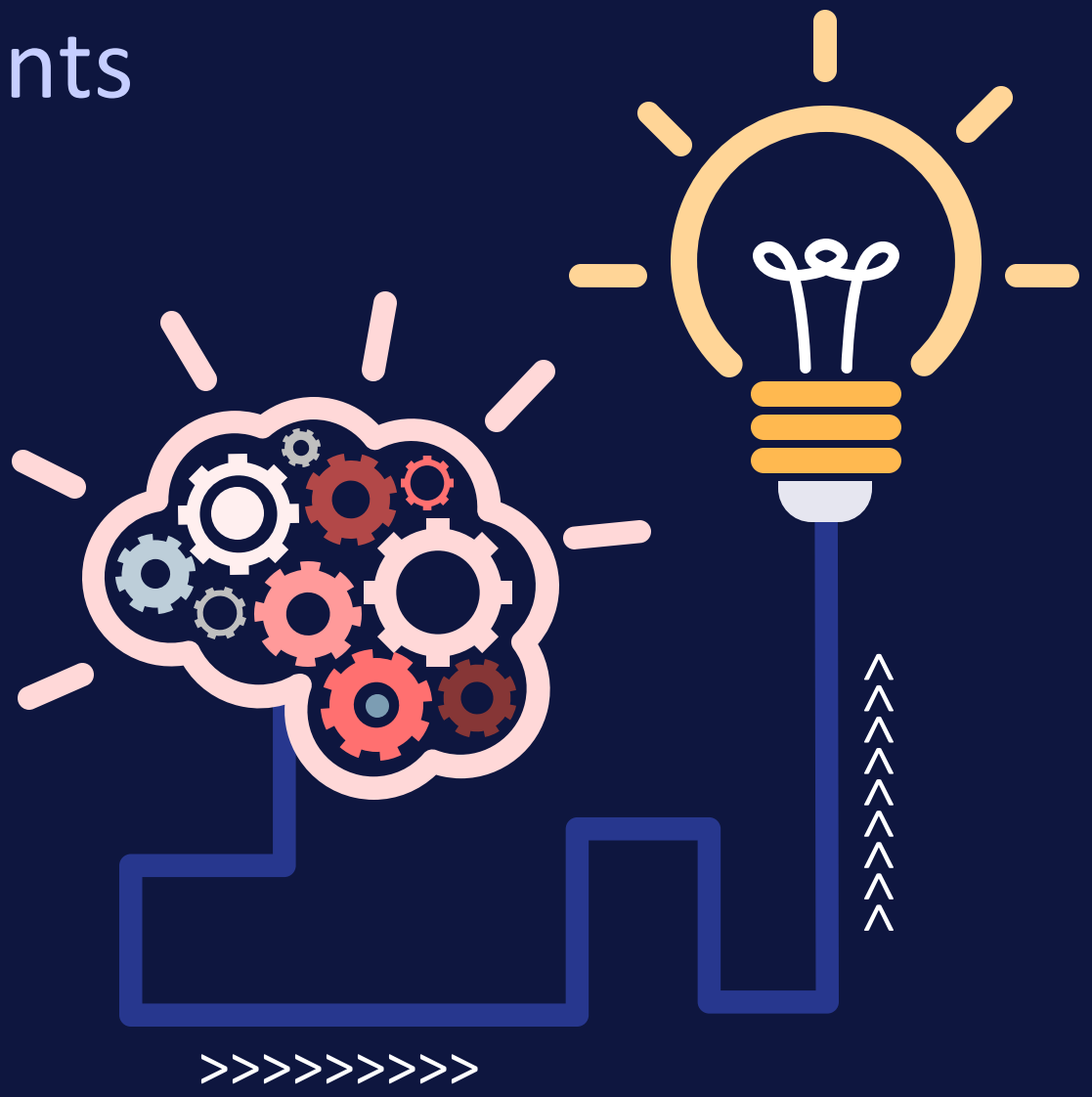
Objective-Driven Assessments

Business targets

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

Realistic starting points

- Leaked access keys
- Compromised developer
- Other insider threat
- Application compromise



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

Thanks for listening!

Twitter/X: @nojonesuk

Blog: www.nojones.net

WITH secure

WITH®

secure