MWR InfoSecurity

Protection and Detection in the Cloud

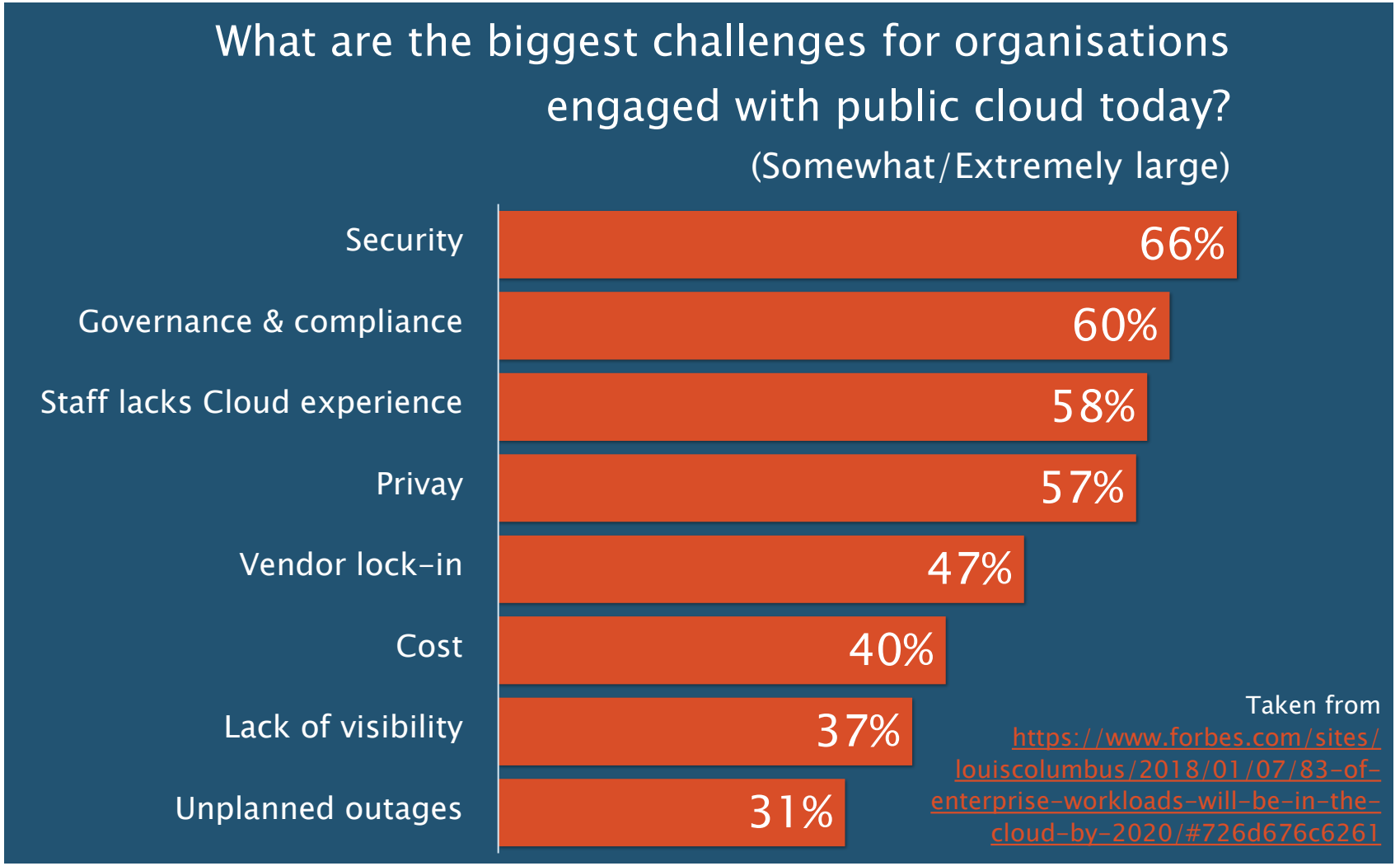
Nick Jones

31st January 2019

Cloud Computing

Forbes: 83% Of Enterprise Workloads In The Cloud By 2020

MWR: >50% of IR cases last year involved the cloud



Takeaways

MWR INFOSECURITY

Where traditional assurance falls short in the cloud

How to automate cloud assurance to:

- Remediate issues faster
- Scale security efforts
- Reduce costs

How to detect attacks in the cloud

Who Am I?

MWR InfoSecurity

- Nick Jones
- Consultant for >4 years, previously a software developer
- Research interests:
  - Cloud
  - DevOps/Automation
  - Attack Detection

*aaS

MWR INFOSECURITY

Bare Metal

IaaS

Virtual machines in the cloud

PaaS

Managed services – databases, app hosting, storage etc.

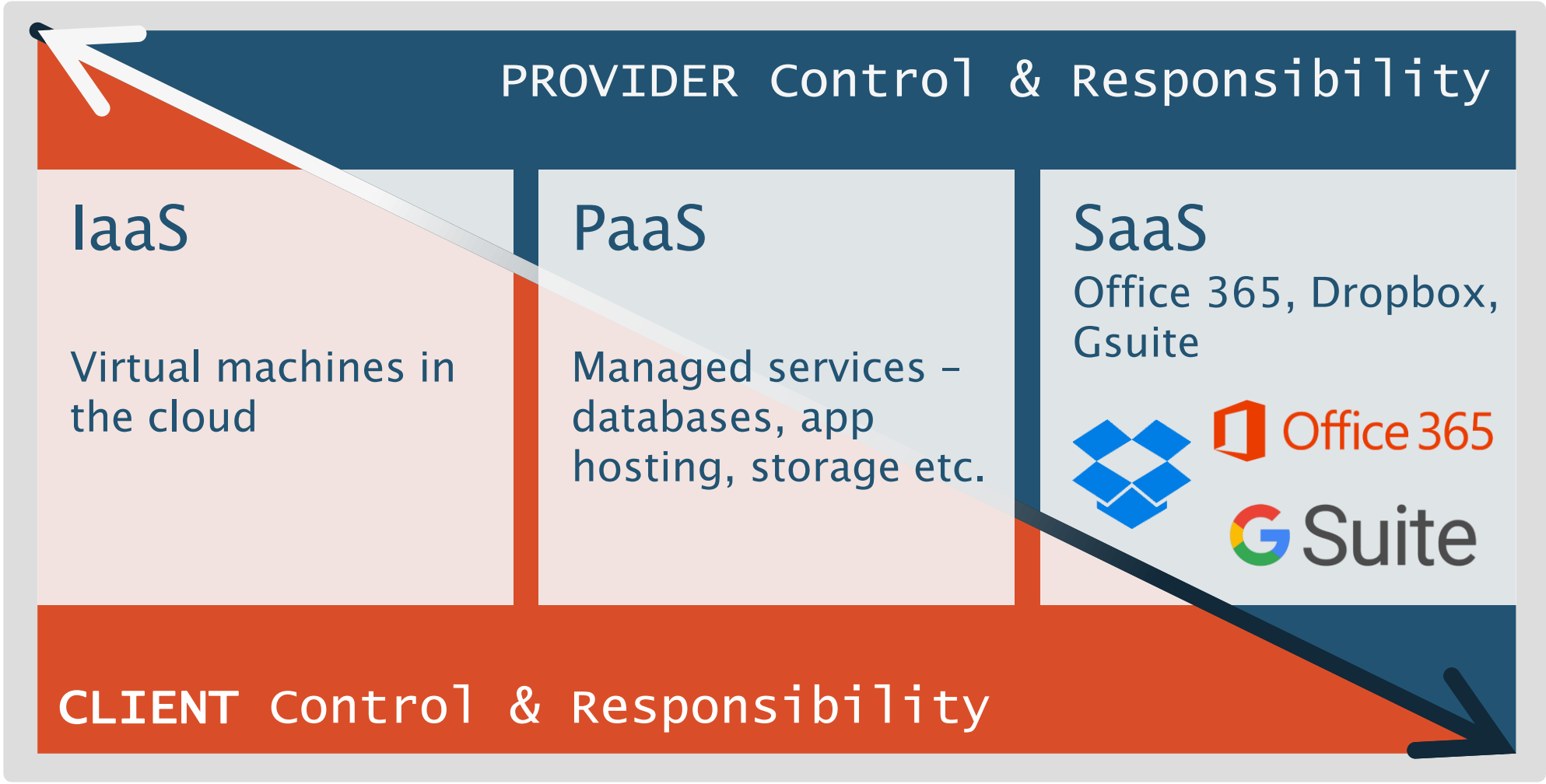
SaaS

Office 365, Dropbox, Gsuite

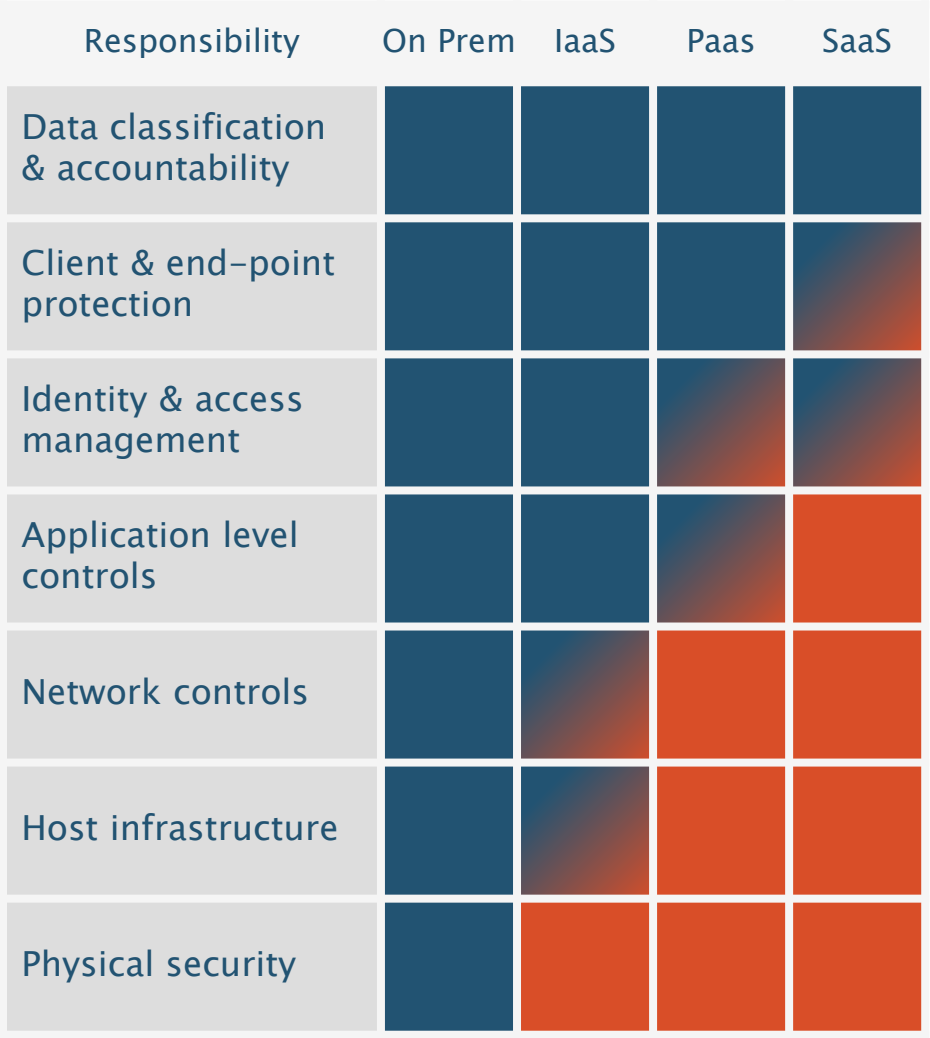
Office 365

G Suite

*aaS


PROVIDER Control & Responsibility
IaaS
Virtual machines in the cloud
PaaS
Managed services – databases, app hosting, storage etc.
SaaS
Office 365, Dropbox, Gsuite
Office 365
G Suite
CLIENT Control & Responsibility

Shared Responsibility Model



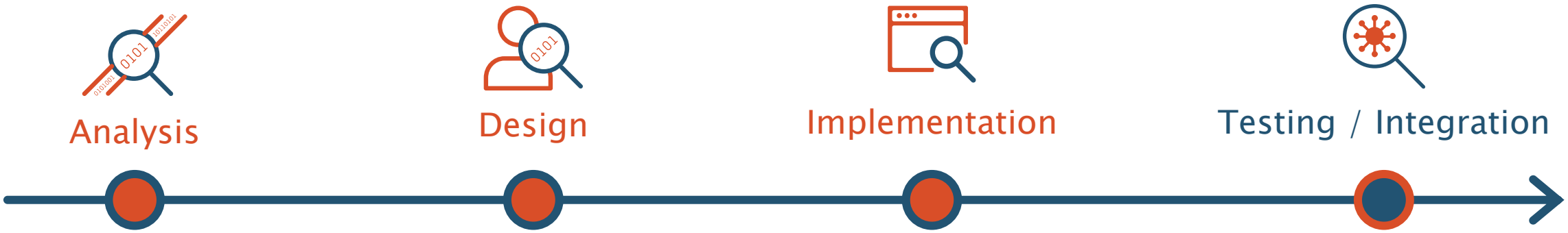
- Outlines who is responsible for securing what
- Varies depending on IaaS vs Paas vs SaaS
- Rules out traditional security assessment techniques for many cloud resources
- Security mindset shift
  - Vulnerabilities -> misconfigurations

Cloud Customer

Cloud Provider

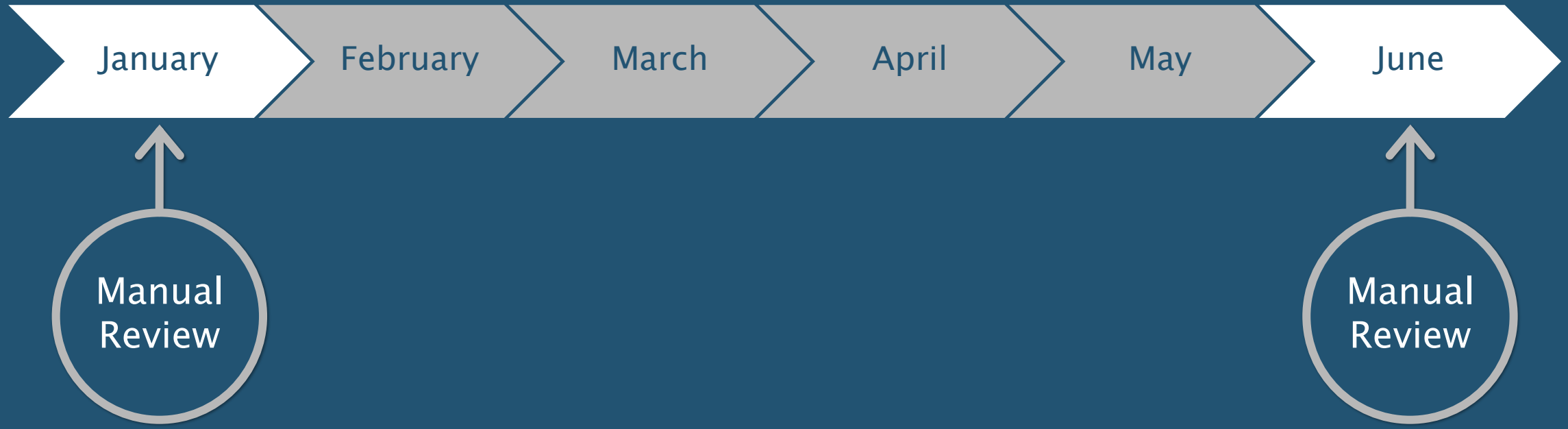
Image taken from https://blogs.msdn.Microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

Traditional Security Testing



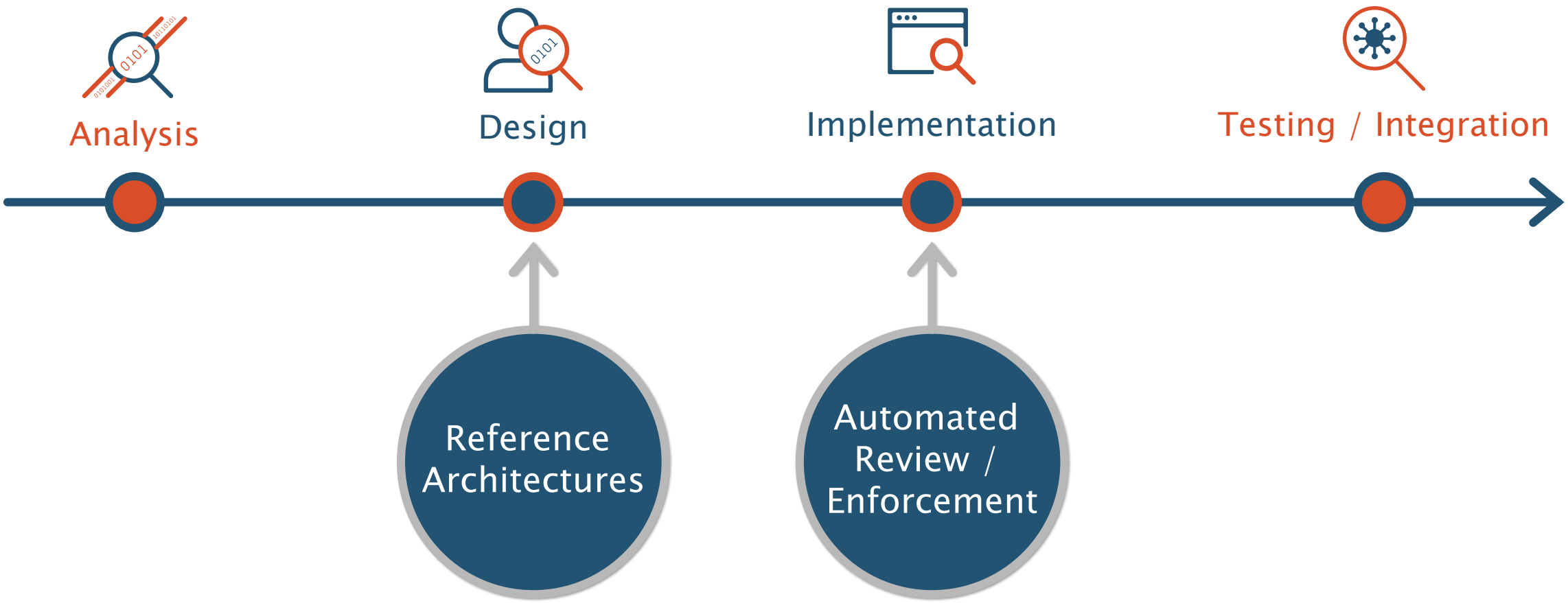
- IaaS – traditional network and application testing still applies
- PaaS – application assessment as before, configuration review for infrastructure

Cloud Configuration Review - Issues

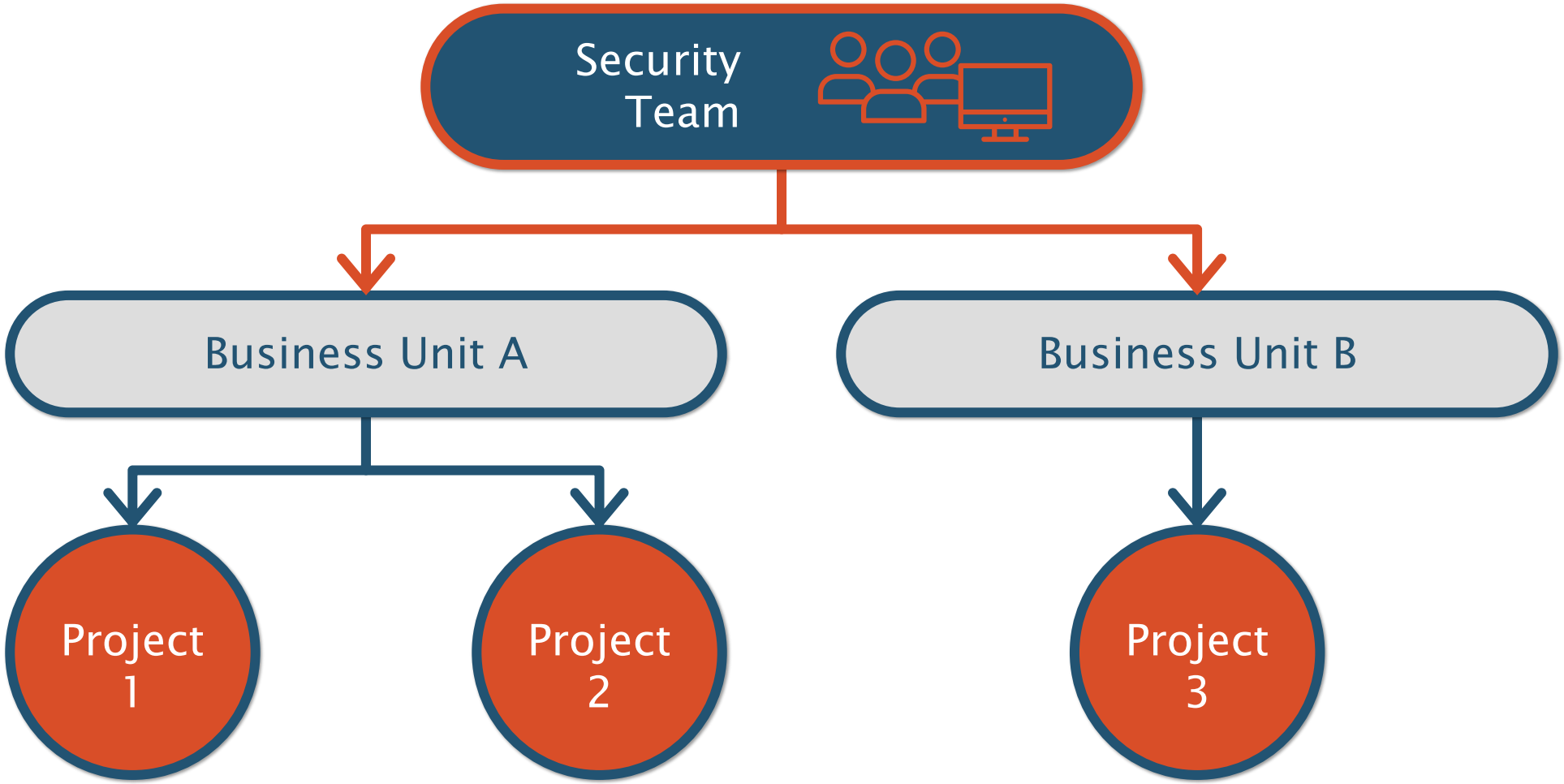


Cloud Configuration Review - Issues

Complements to Manual Review



Reference Architectures / patterns



Reference Architectures – How To

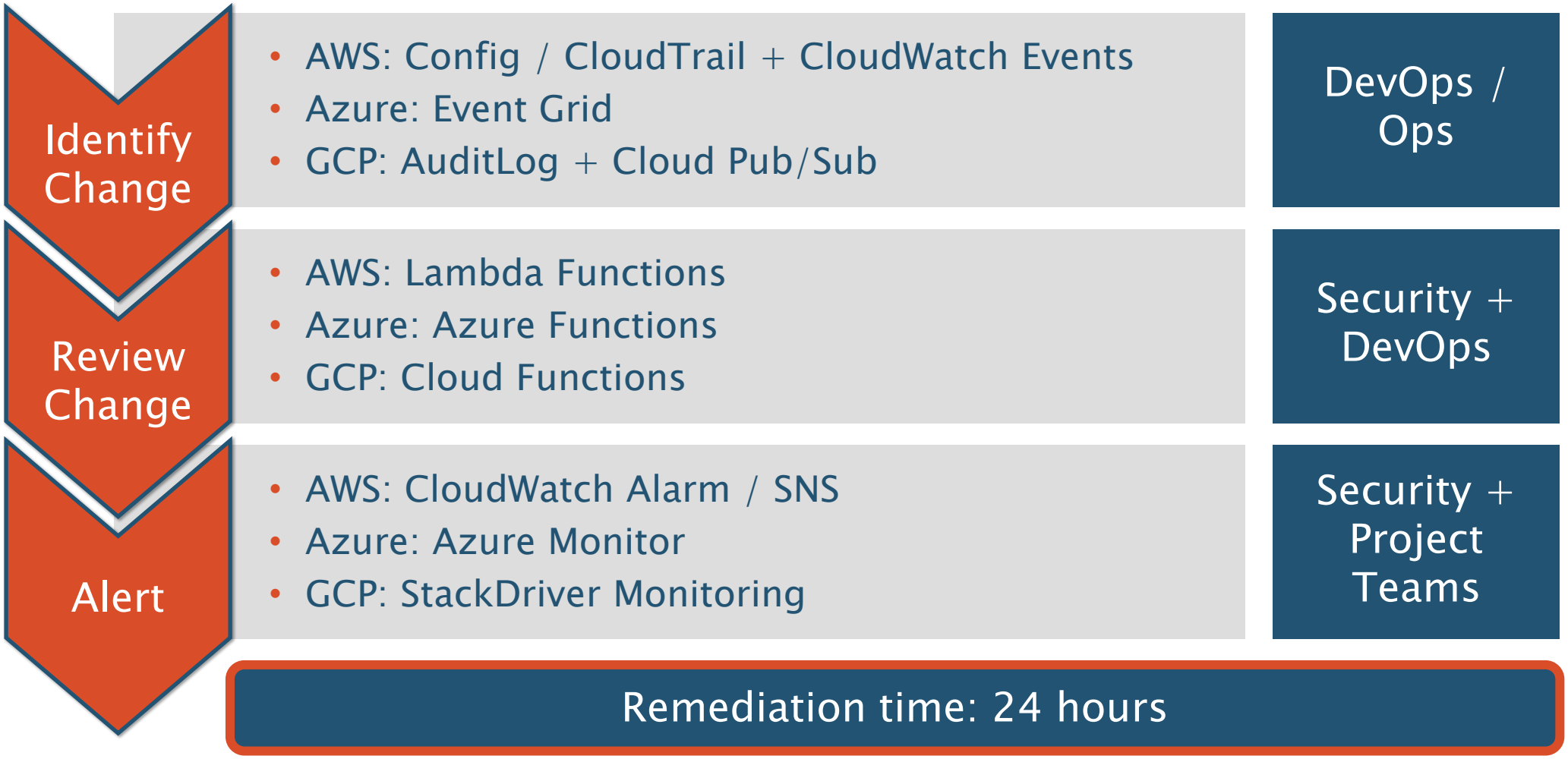
MWR InfoSecurity

Identify common services

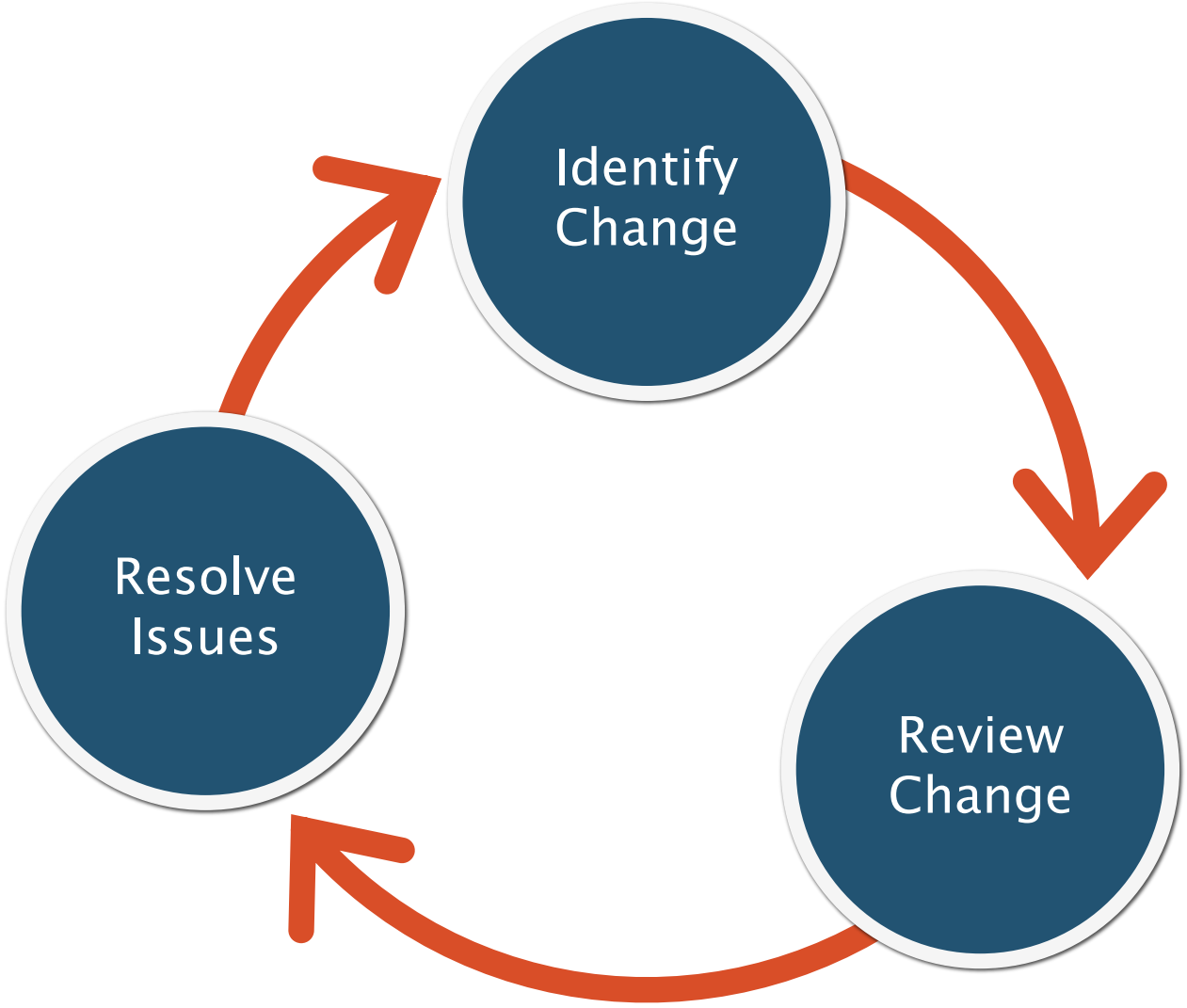
Review Internal/ External Guidance

Implement Architecture in IaC tool

Continuous Configuration Review



Continuous Configuration Enforcement



Remediation time: 30 minutes

Existing Work

MWR INFOSECURITY

- AWS Whitepaper – Automating Governance on AWS
- OSS Frameworks:
  - Cloud Custodian
  - Security Monkey
  - Forseti Security

The Other View of Security Enforcement

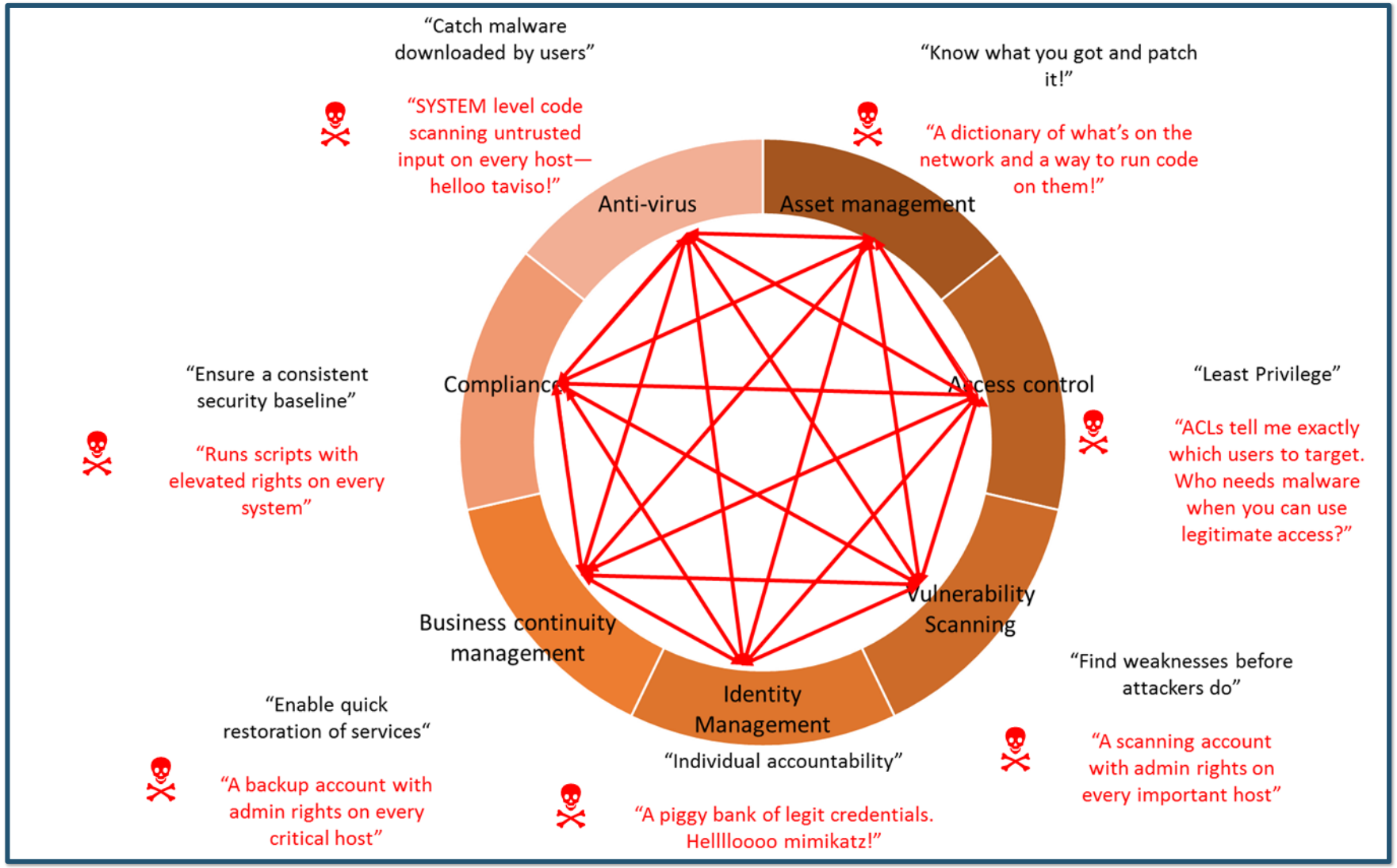
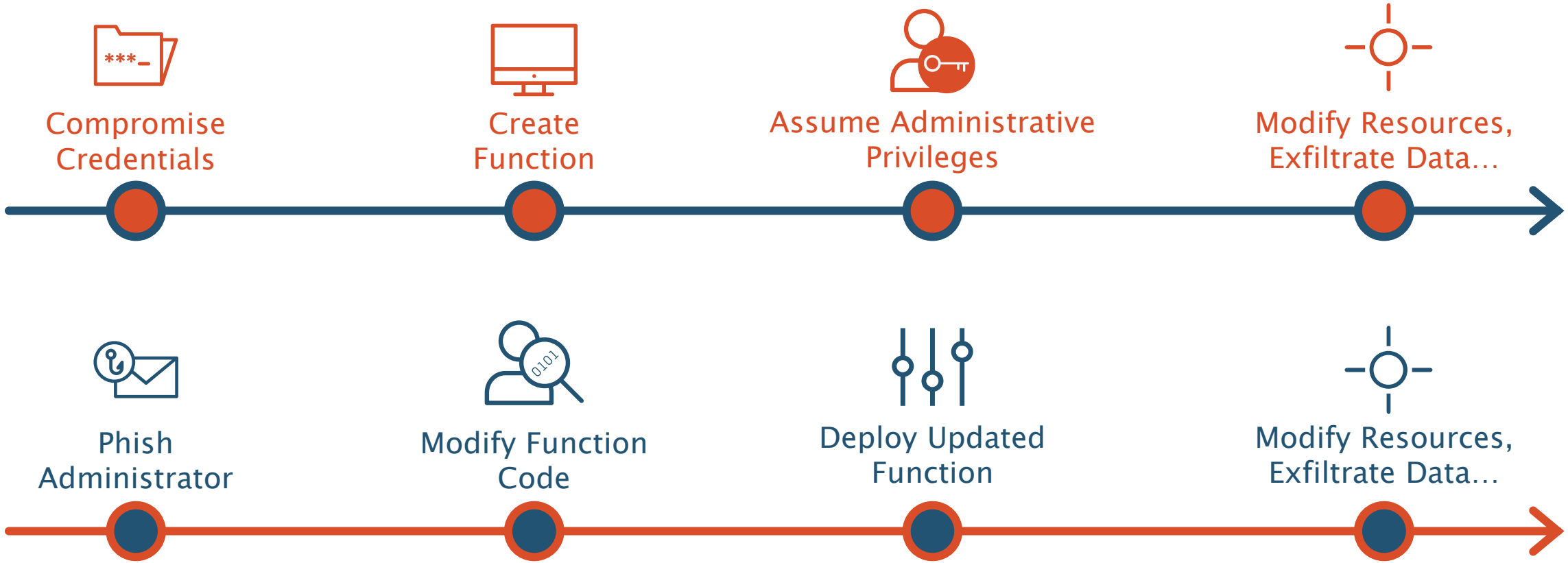


Image taken from John Lambert
https://twitter.com/johnlatwc/status/699304590500634625

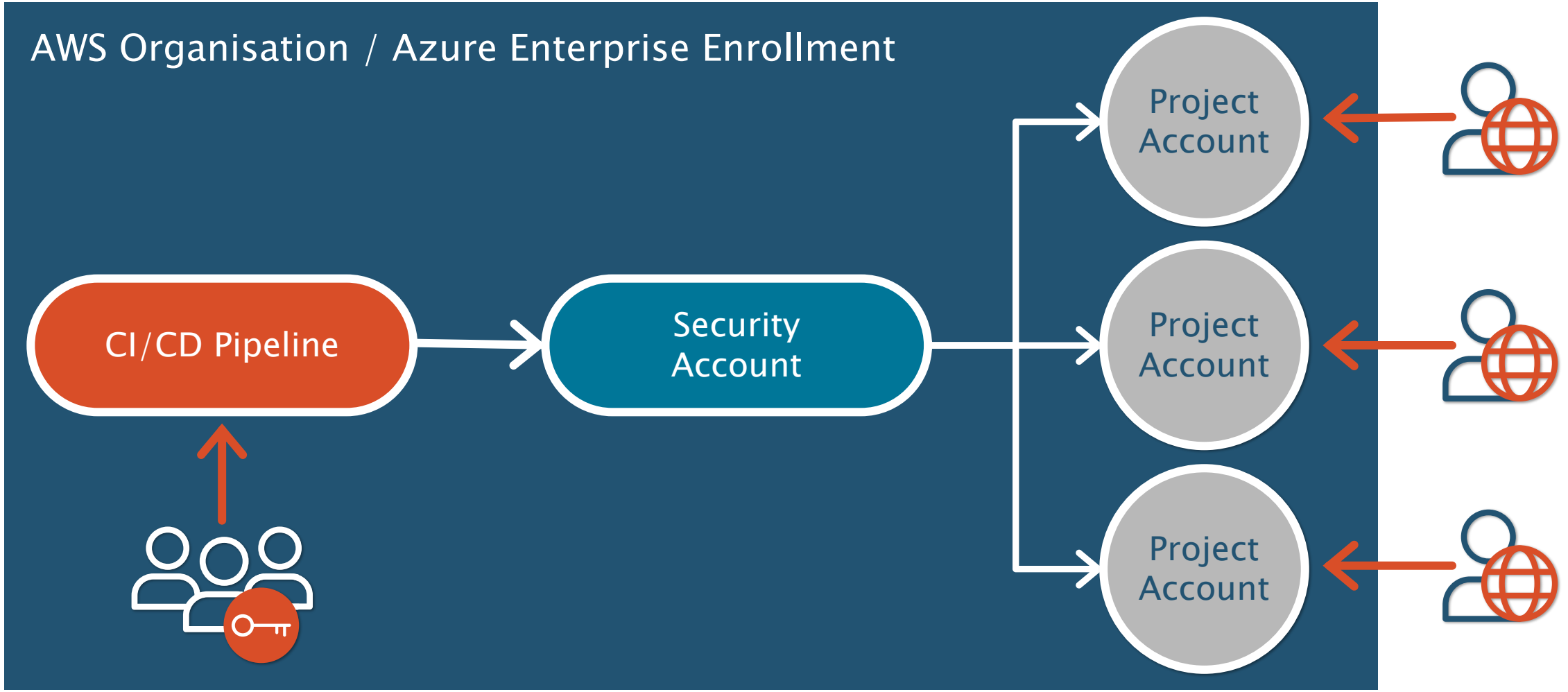
Attacking Continuous Enforcement

MWR INFOSECURITY

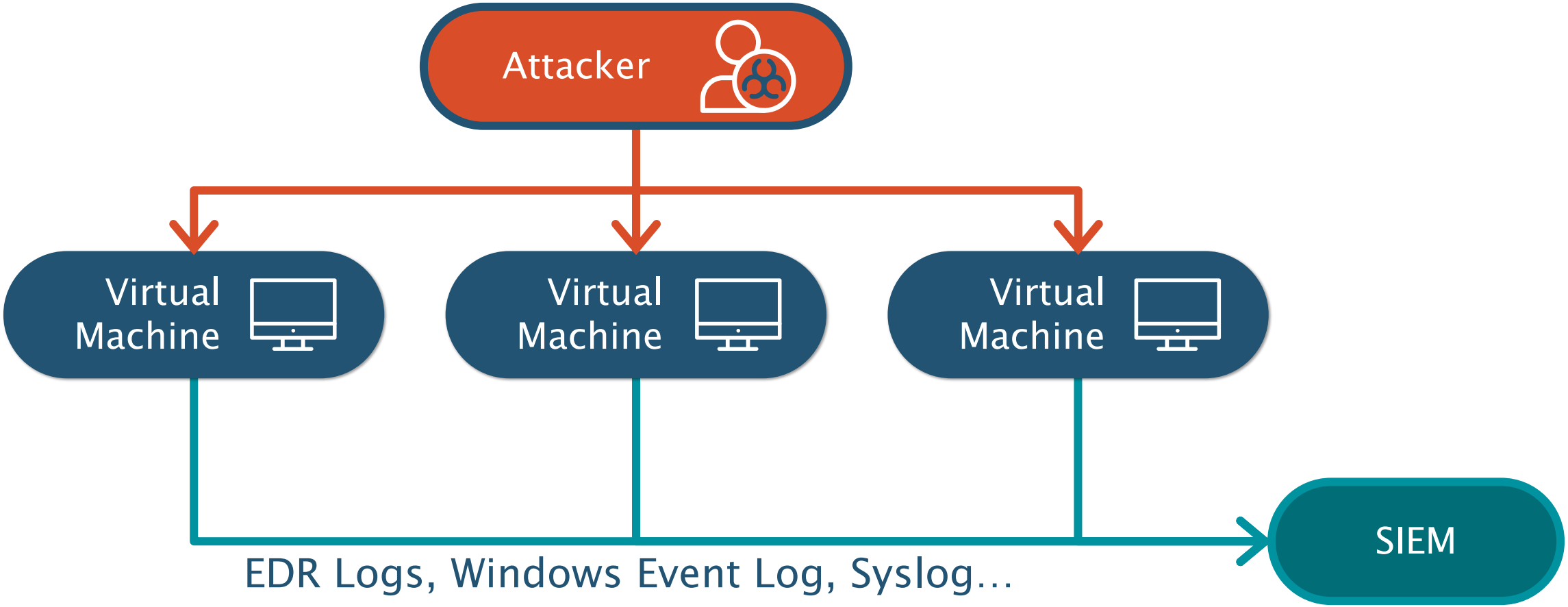
Enforcement functions often assigned lots of permissions



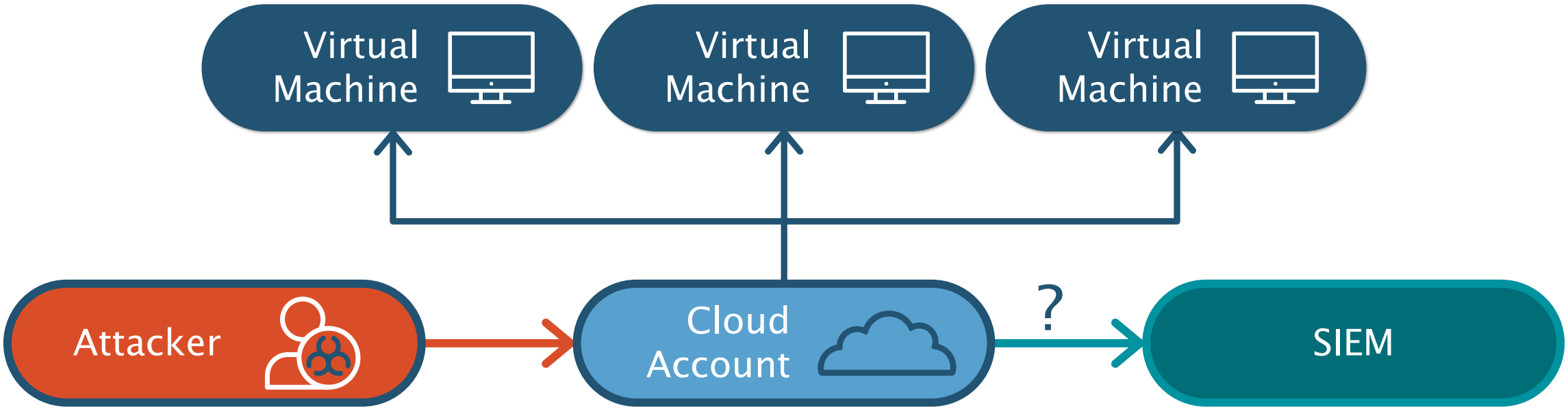
Reduce The Risk



What about Detection and Response?



What about Detection and Response?



Cloud Log Sources

MWR InfoSecurity

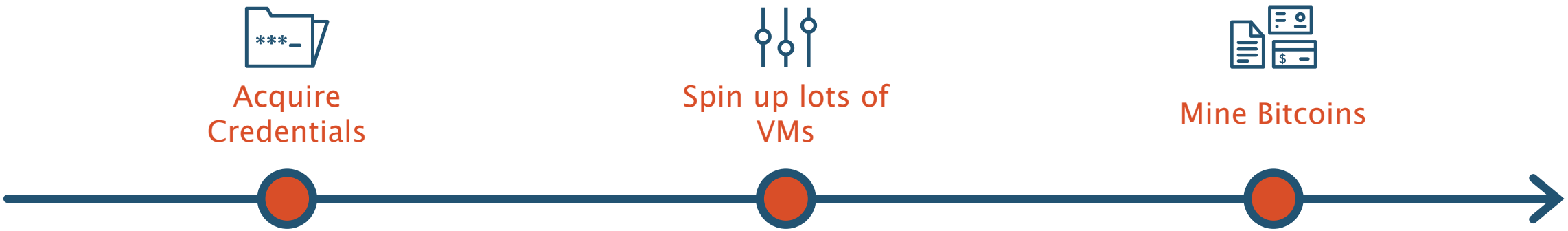
- Cloud API call logs (CloudTrail, Audit Log etc)
- Output from automated review and enforcement
- VPC/NSG flow logs
- Storage access logs
- System logs from any VMs
- Application logs from PaaS

what does an attack look like?

MWR INFOSECURITY

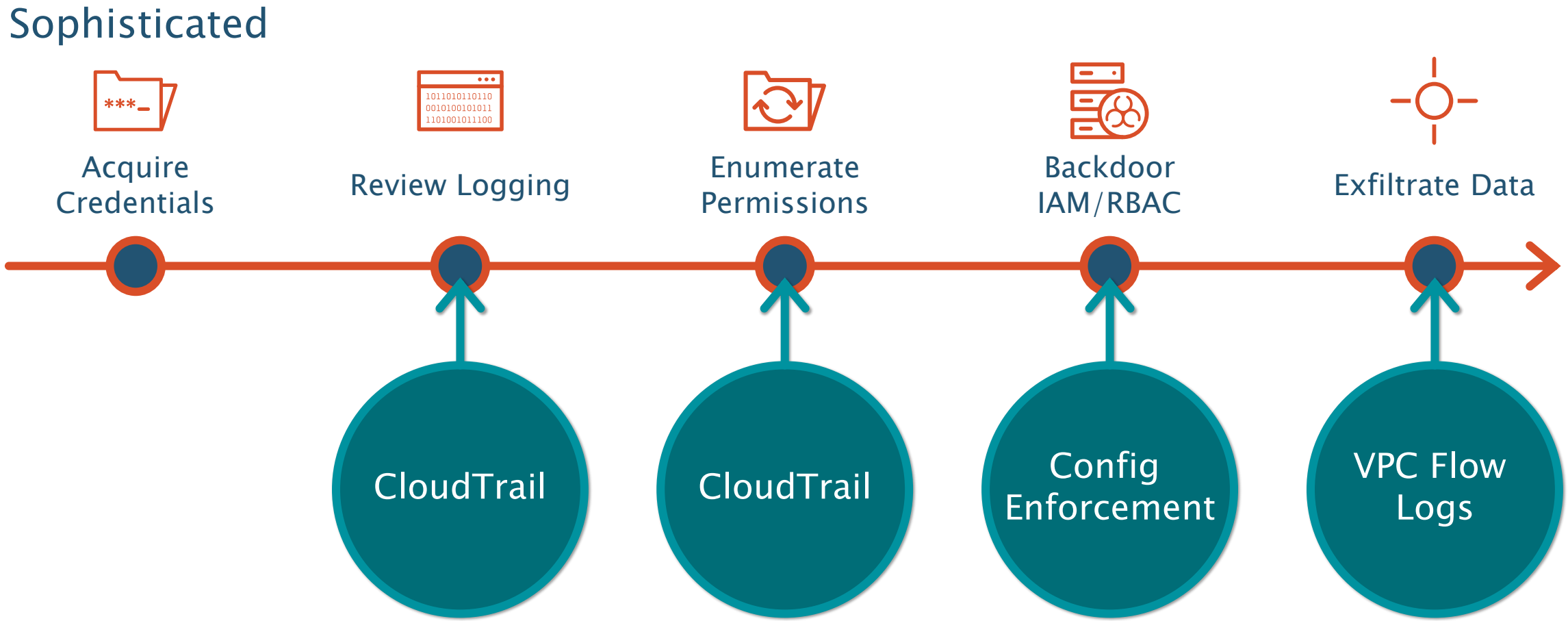
Sophisticated

Low skill/effort



what does an attack look like?

MWR INFOSECURITY

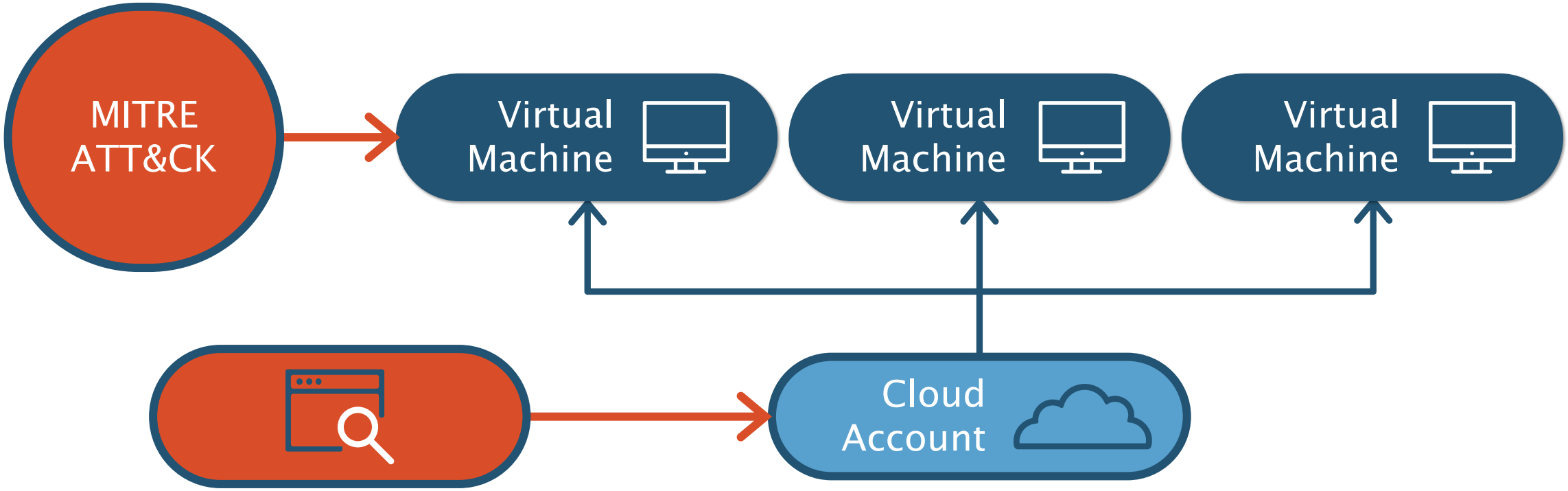


IoCs to Watch For

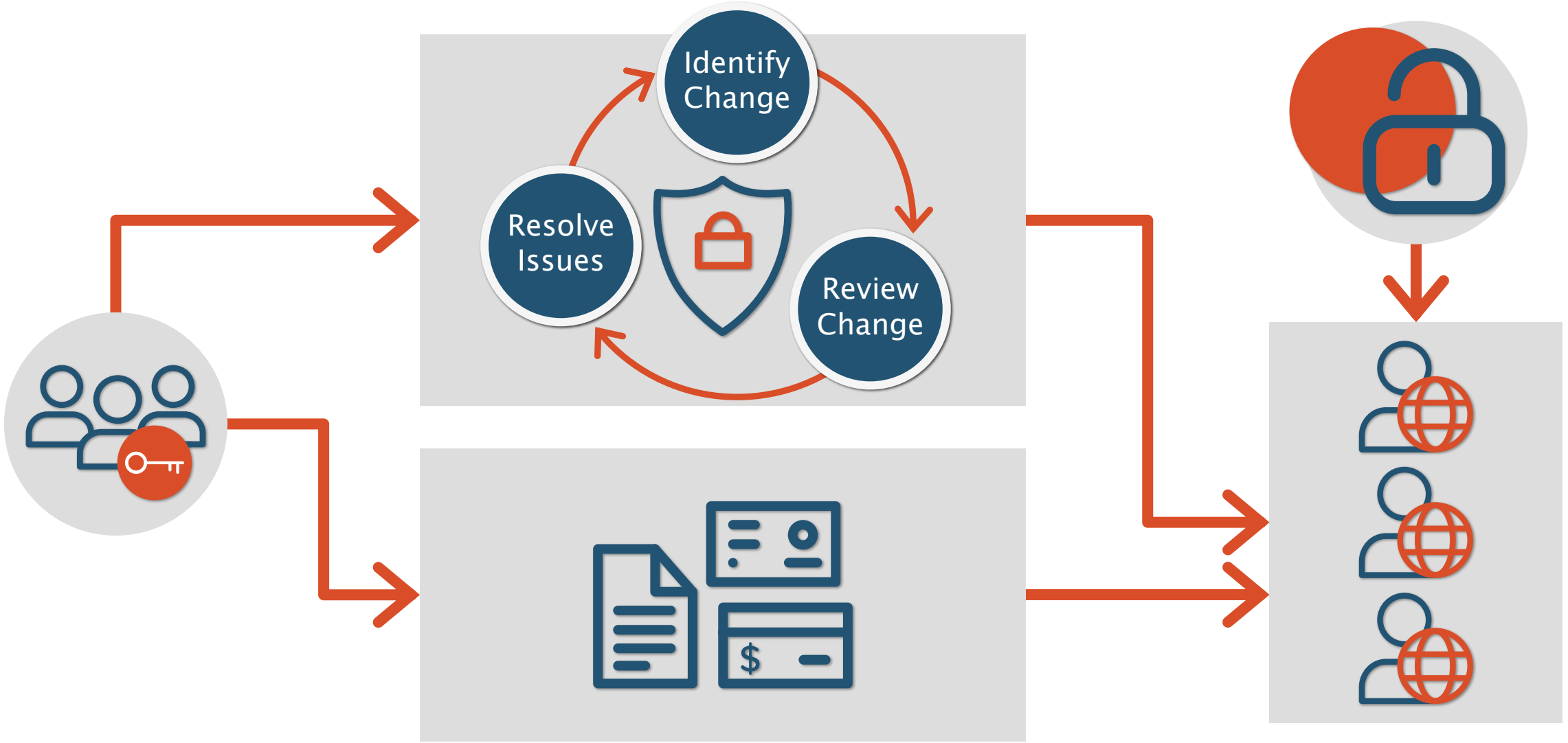
MWR InfoSecurity

- Use of credentials from unexpected locations
- Creation of resources in unused regions
- Repeated failed authentication attempts
- Creation of new IAM/AAD users
- Modifications of roles, policies, network security controls
- Outbound traffic to odd locations or in odd volumes

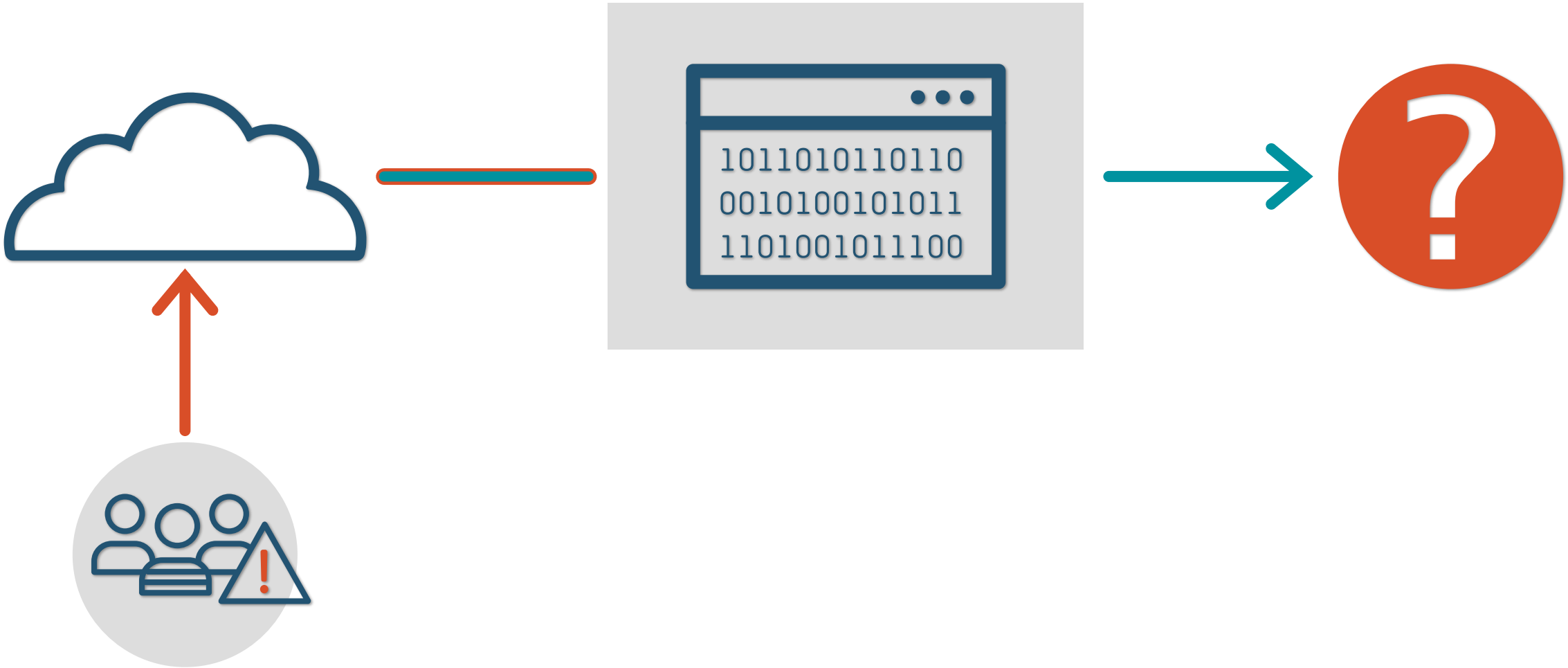
How do we Assess Detection In the Cloud?



Conclusions



Conclusions




Questions?
MWR
INFOSECURITY