F-Secure | LABS

SECURING YOUR AWS WORKLOADS AT SCALE

Nick Jones

LABS

THIS PRESENTATION WILL COVER...

What does your cloud security landscape actually look like?

How will an attacker target your workloads?

What’re the key controls to have in place?

$ whoami

NICK JONES

Senior Security Consultant, Cloud Security Lead @ F-Secure Consulting

AWS Community Builder

Presented at DEF CON, fwd:CloudSec, RSA, t2, DevSecCon etc

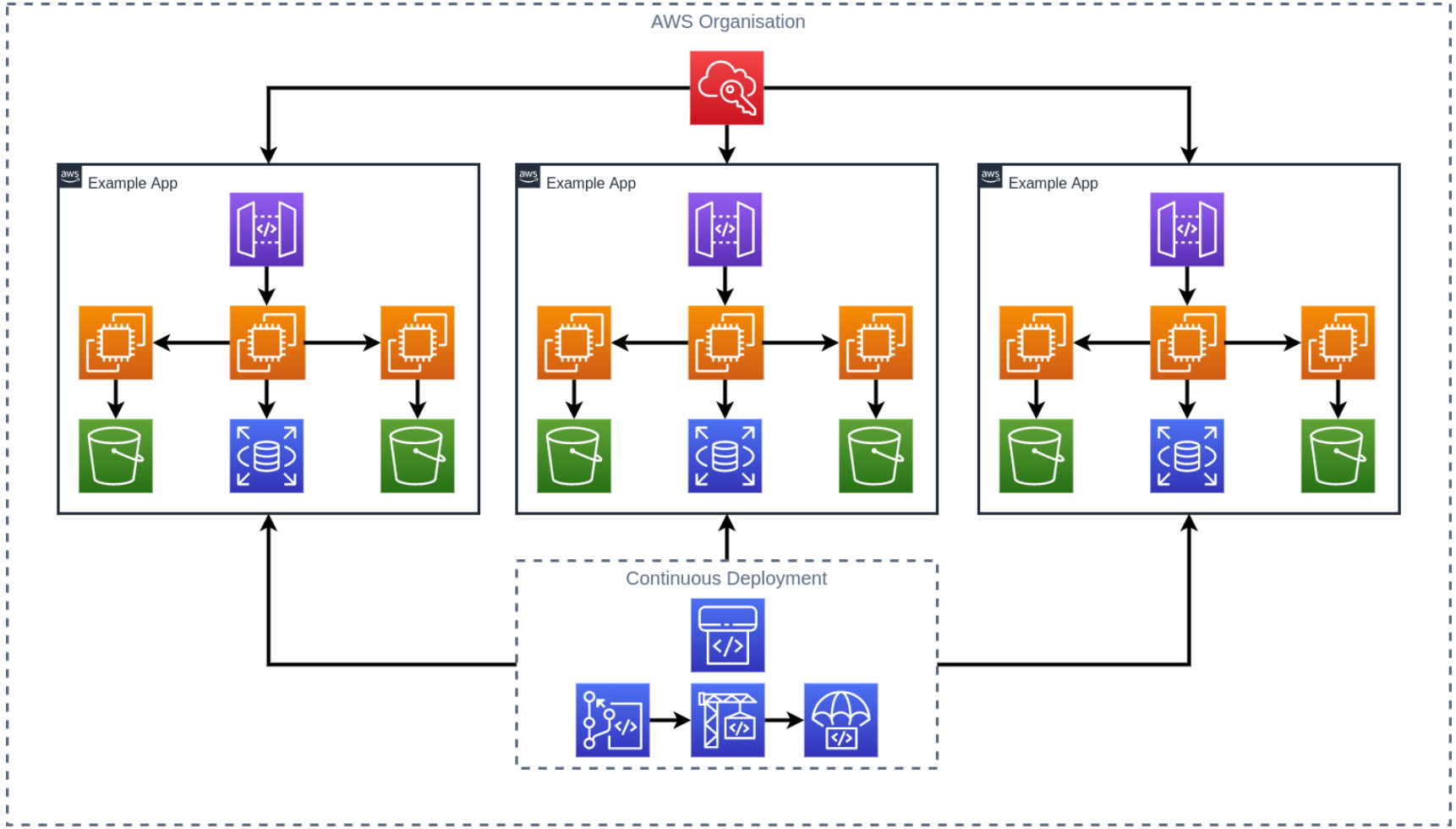
Lead Developer on Leonidas - https://github.com/fsecurelabs/leonidas

F-Secure | LABS

YOUR CLOUD SECURITY LANDSCAPE

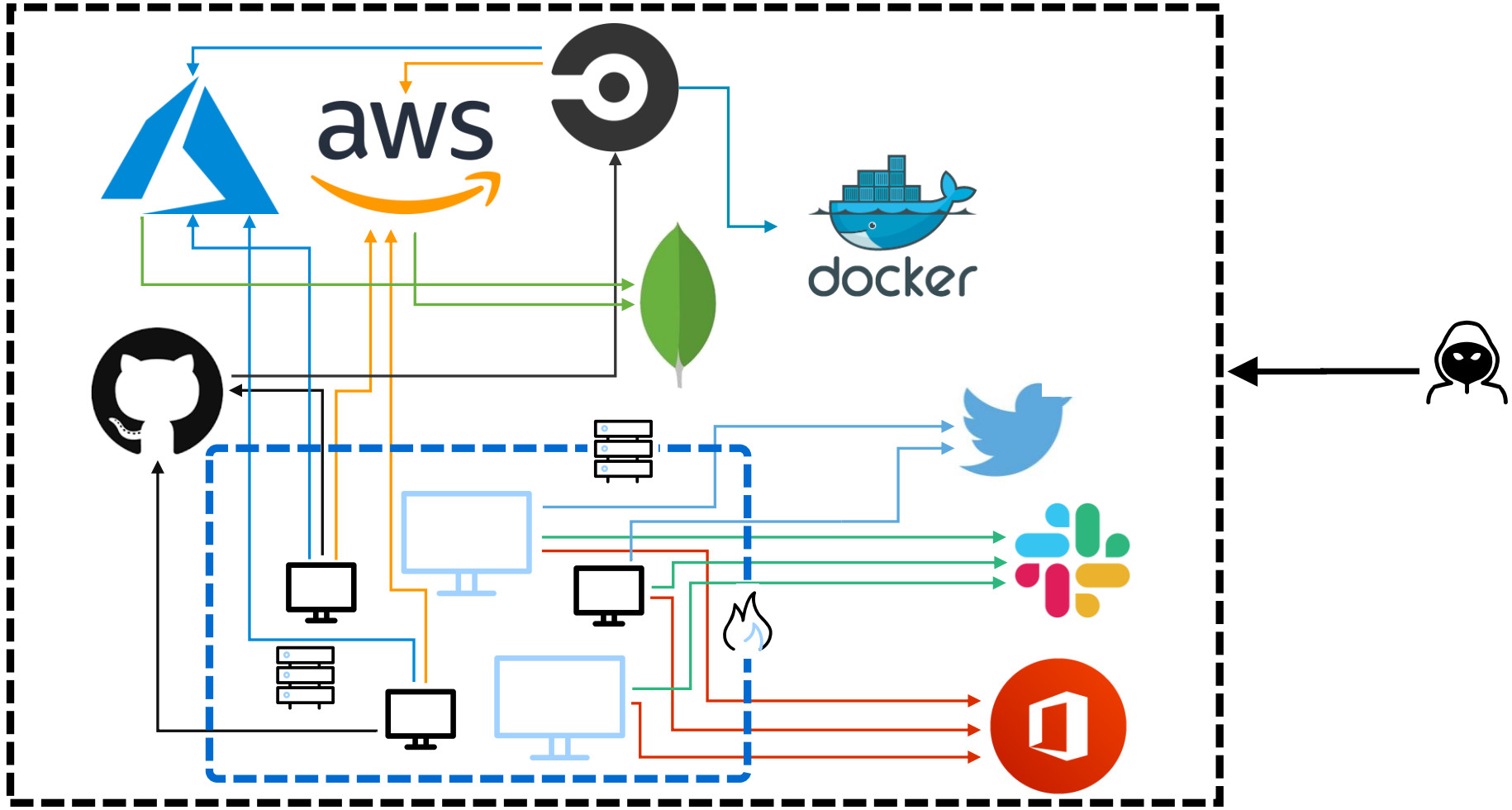
LABS

THE SCOPE OF MOST PEOPLE'S THINKING



LABS

THE REALITY



F-Secure | LABS

HOW ATTACKERS OPERATE IN THE CLOUD

COMMON MYTHS DISPELLED

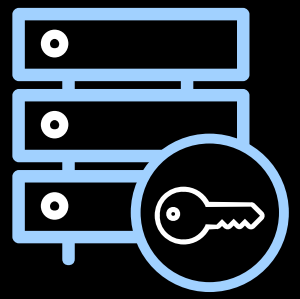
LABS

Attackers look for path of least resistance	Most people get screwed by the basics:	The following **probably** won't be how you get breached:
• Most attacks are opportunistic • Getting the basics right helps stop APTs too	• Forgotten AWS accounts • S3 buckets with public access • Leaked credentials • Admin rights granted to stupid things	• Insufficient/misconfigured encryption at rest • Not using the latest Nitro Enclave/Shiny AWS Security ServiceTM • Some insane AWS 0-day • A disgruntled engineer at AWS

LABS

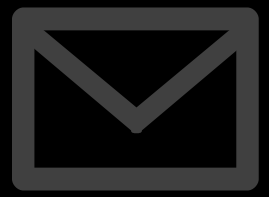
INITIAL ACCESS

Public Storage



Web App Vulnerabilities

Exposed Credentials



Targeted Attacks

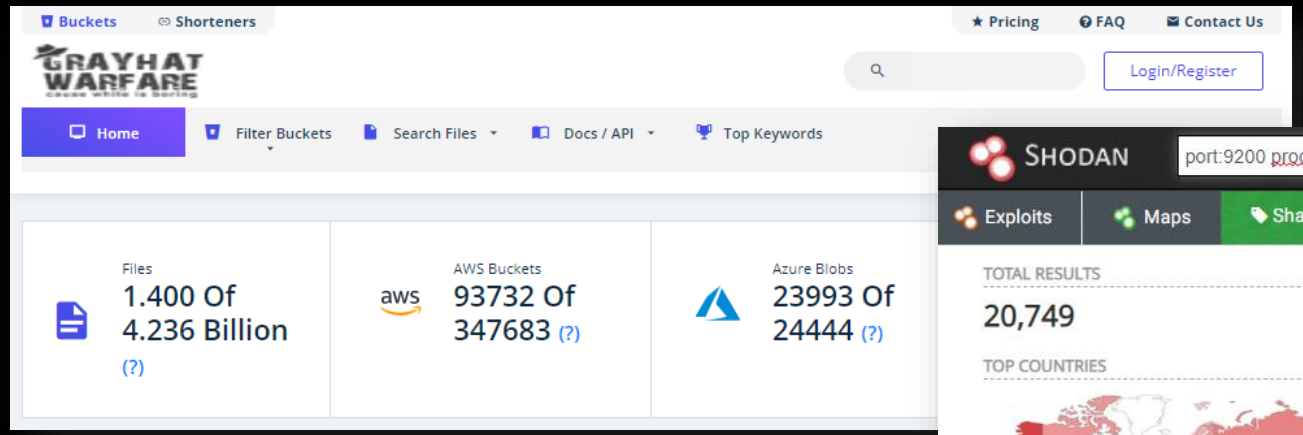
LABS

PUBLIC STORAGE

Sensitive data exposure from public storage is alive and well!

Leaky AWS S3 bucket once again at centre of data breach

Prestige Software exposed millions of records after failing to pay attention to the security of its cloud instances



Home » Security Bloggers Network » Another S3 Bucket Leads to Breach of 50k Patient Records

Another S3 Bucket Leads to Breach of 50k Patient Records

by Dennis Sebayan on March 15, 2021

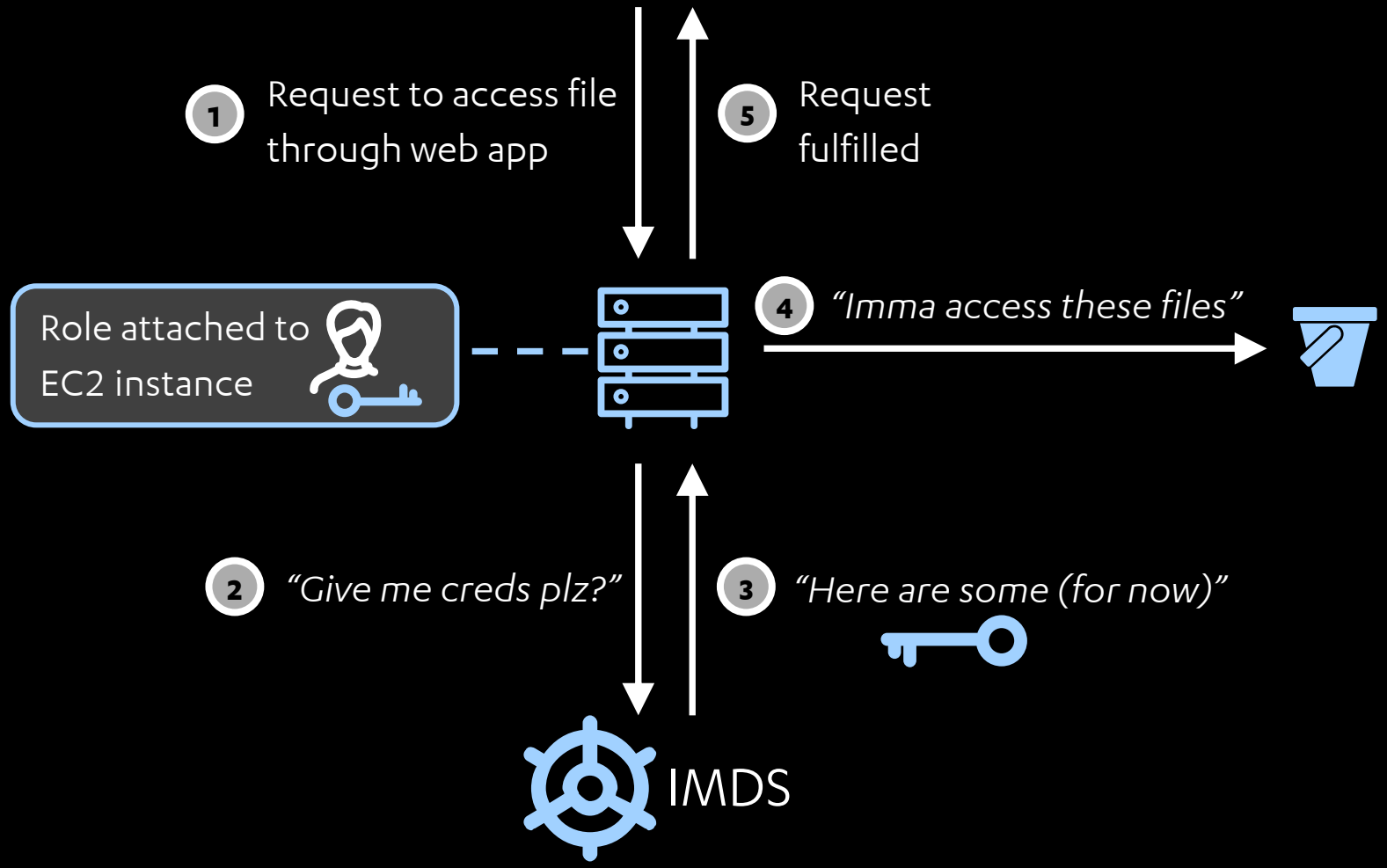
Data of millions of eBay and Amazon shoppers exposed

12 MAR 2020 7

Data loss

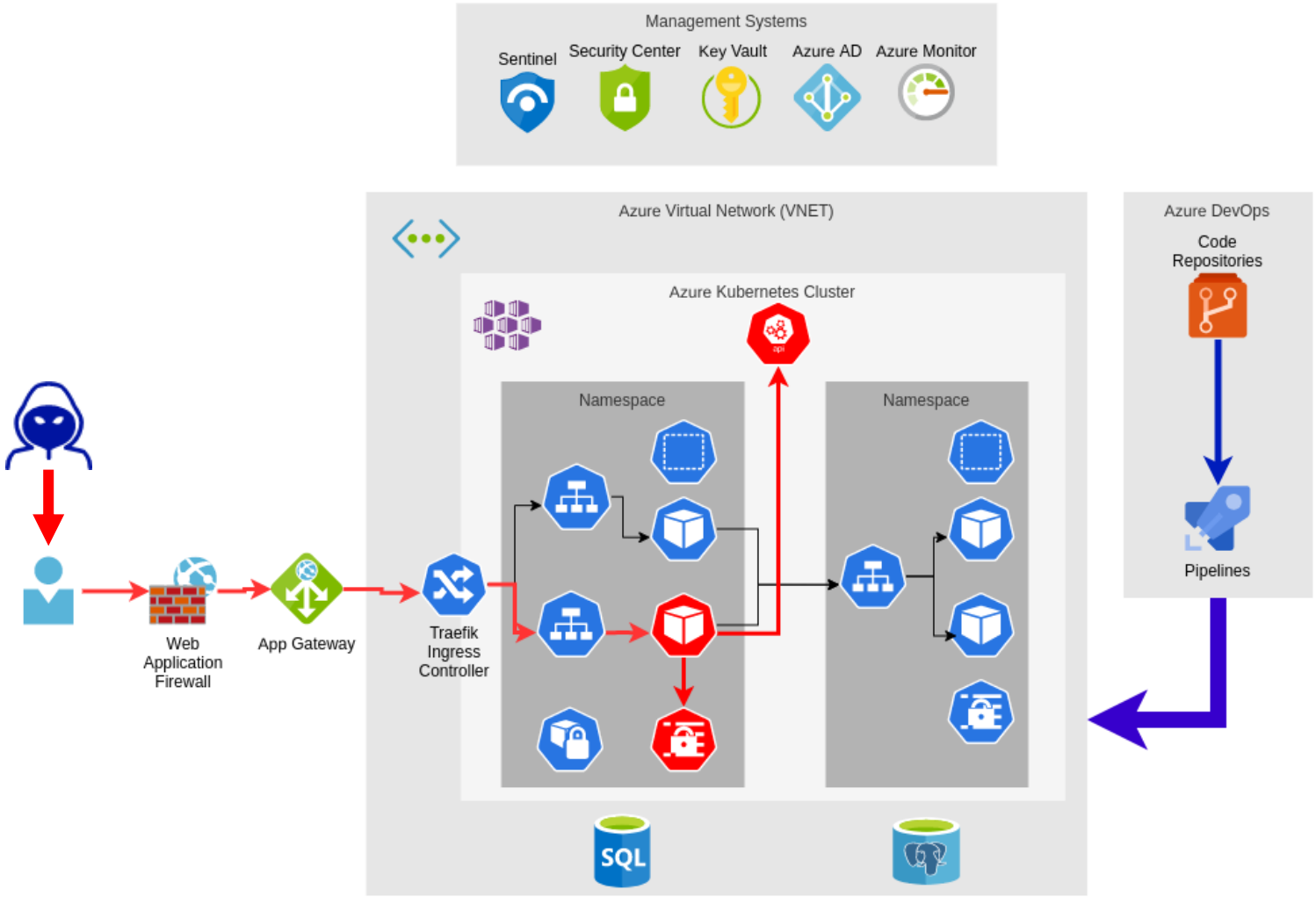
LABS

WEB APP VULNS



LABS

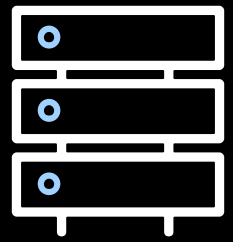
WEB APP VULNS



LABS

TARGETED ATTACKS

Identity Management

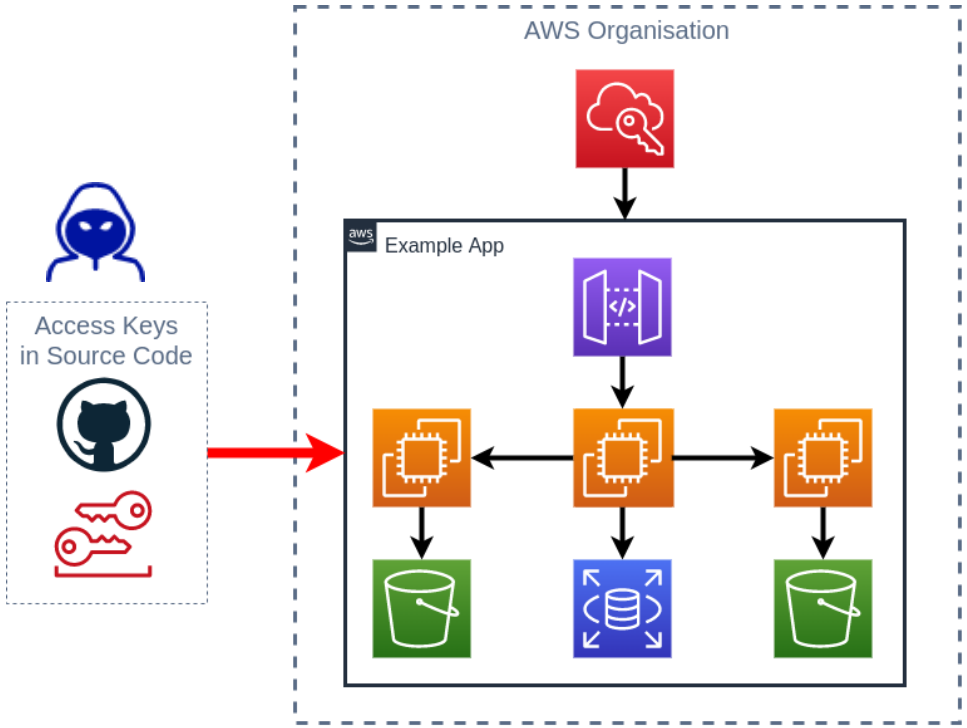


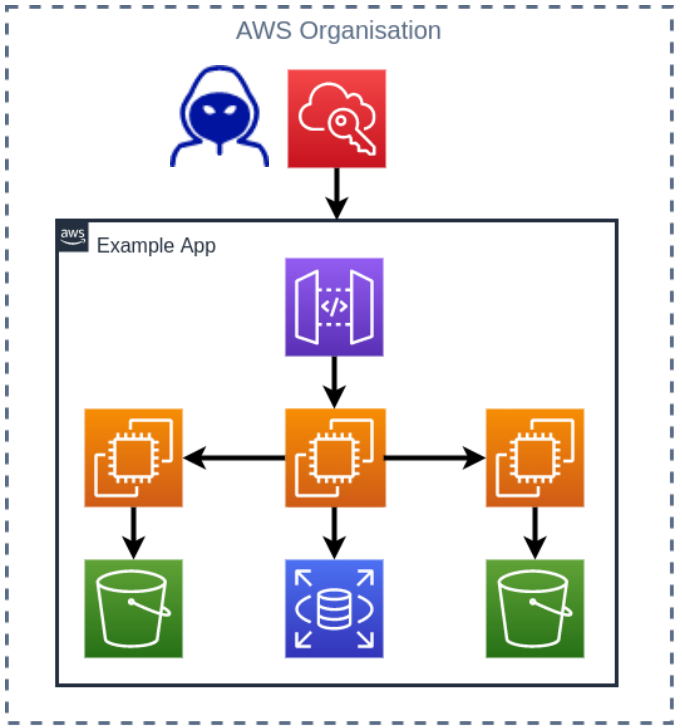
Lateral movement between environments

SCM and CI/CD

LABS

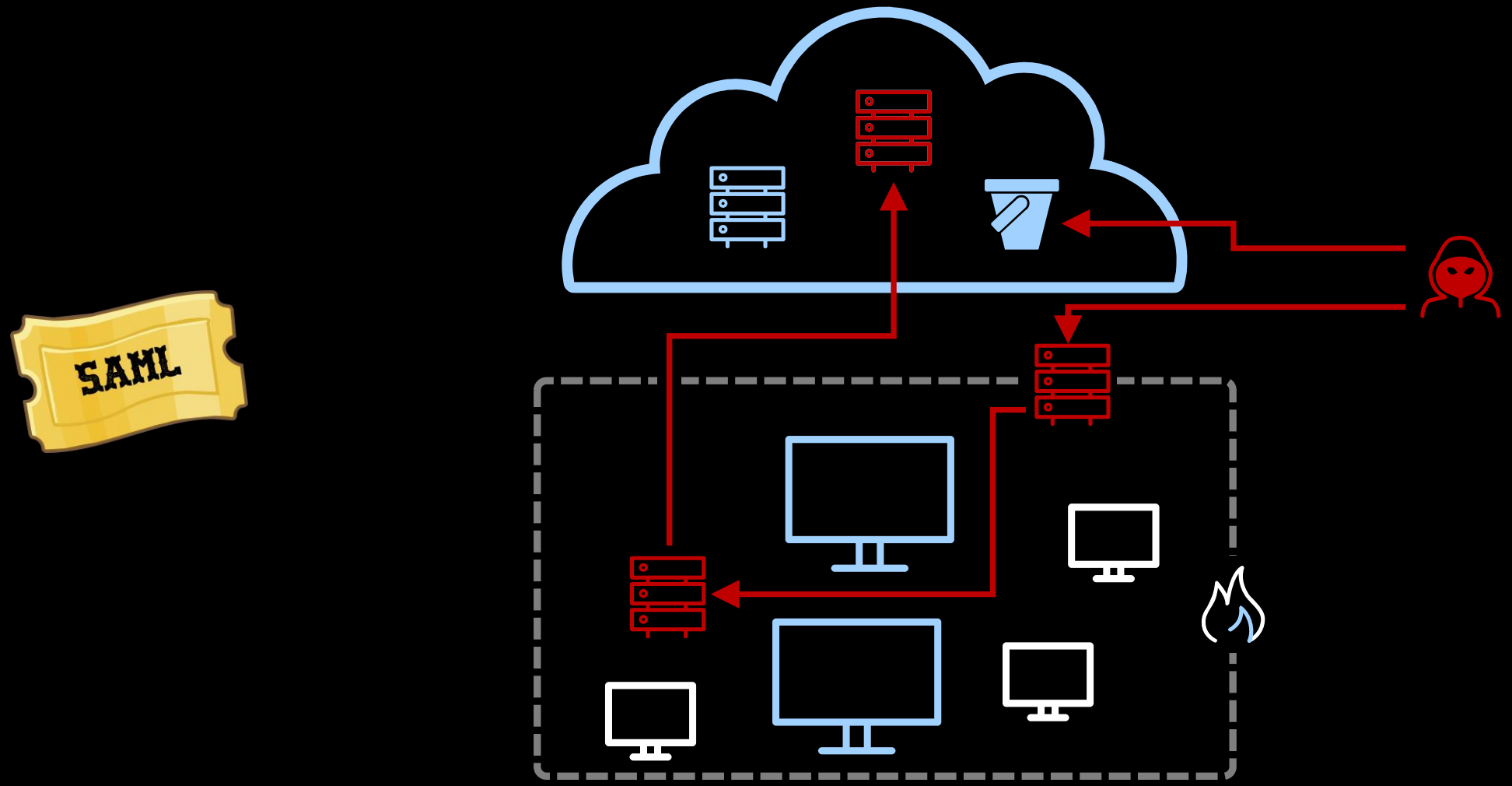
IDENTITY MANAGEMENT





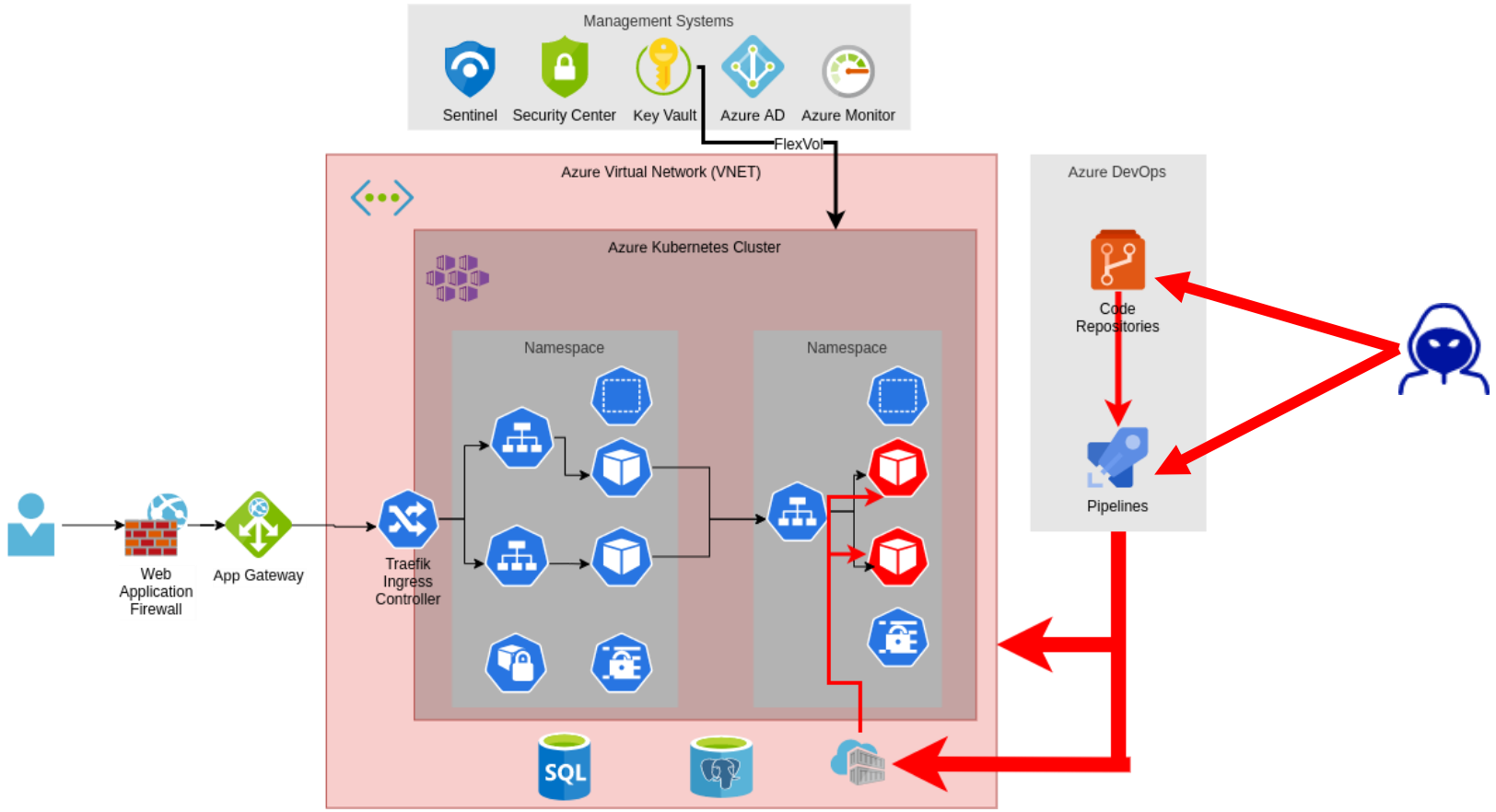
LABS

LATERAL MOVEMENT



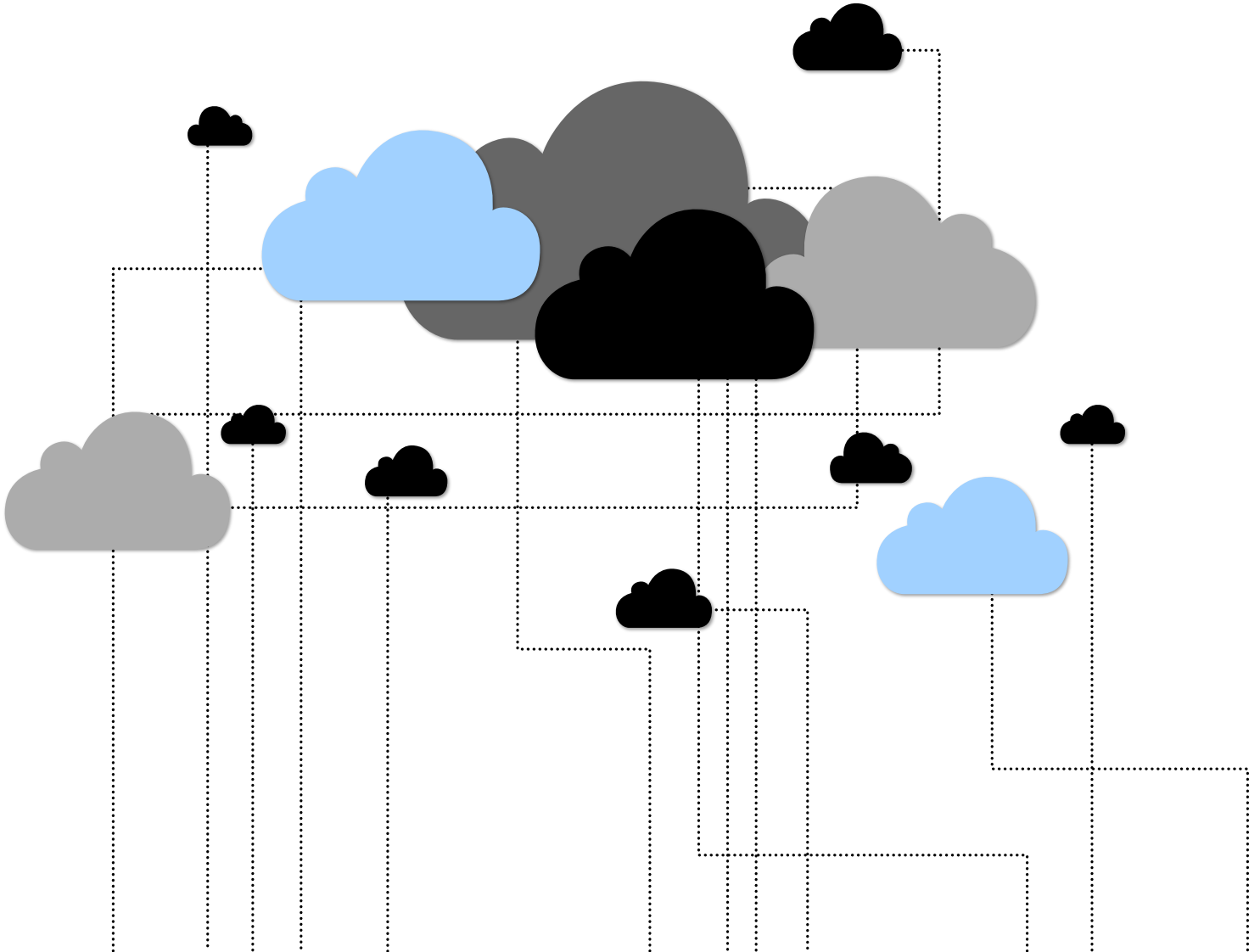
LABS

SCM / CONTINUOUS DELIVERY



LABS

KEY SECURITY CONTROLS



LABS

STRONG IDENTITY CONTROLS

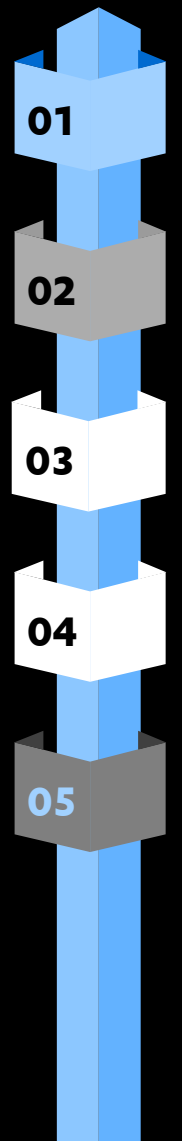
Enforce Multi-Factor Authentication (MFA) everywhere
Importance of this cannot be overstated - hardware tokens > TOTP apps > SMS

Apply principle of least privilege to all roles/policies
Easier said than done in most environments – use cloudsplaining/awspx

Reduce or eliminate long-lived credentials, especially IAM users!
This applies to SSH keys etc for production too

Use instance roles, IAM roles tied to resources wherever possible

Automate credential management and rotation
PAM solutions will often support auto-rotation after use



LABS

LIMIT BLAST RADIUS

Separate Projects

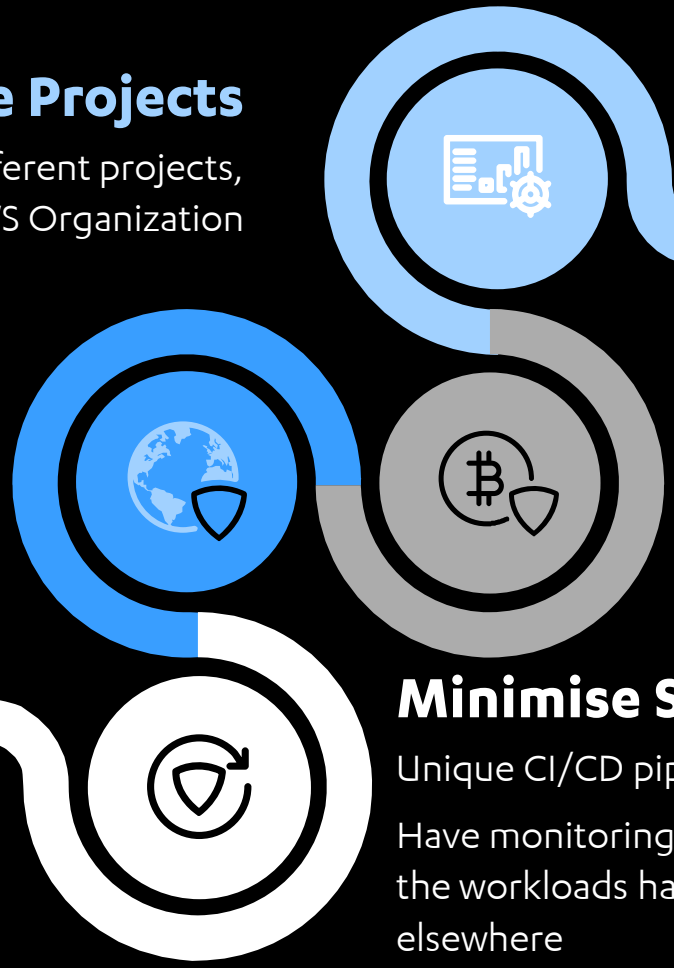
Use separate AWS accounts for different projects, organised under an AWS Organization

Segregate at the Network Level

Enforce strong network boundary controls

Avoid VPC peering (especially with third parties)

Think carefully before exposing network routes between environments



Separate Environments

Keep development, QA/test and production environments in separate accounts

Run security tools in their own accounts

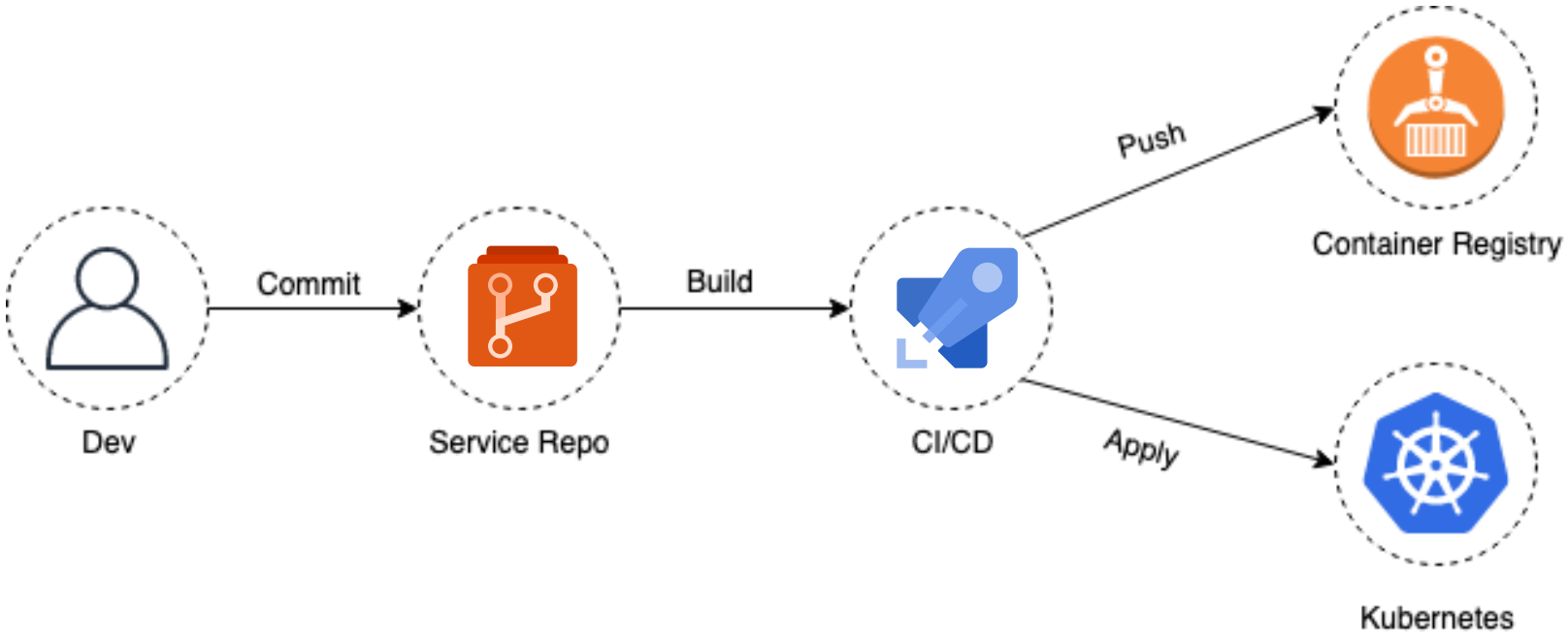
Log centrally to a hardened logging account

Minimise Shared Service Access

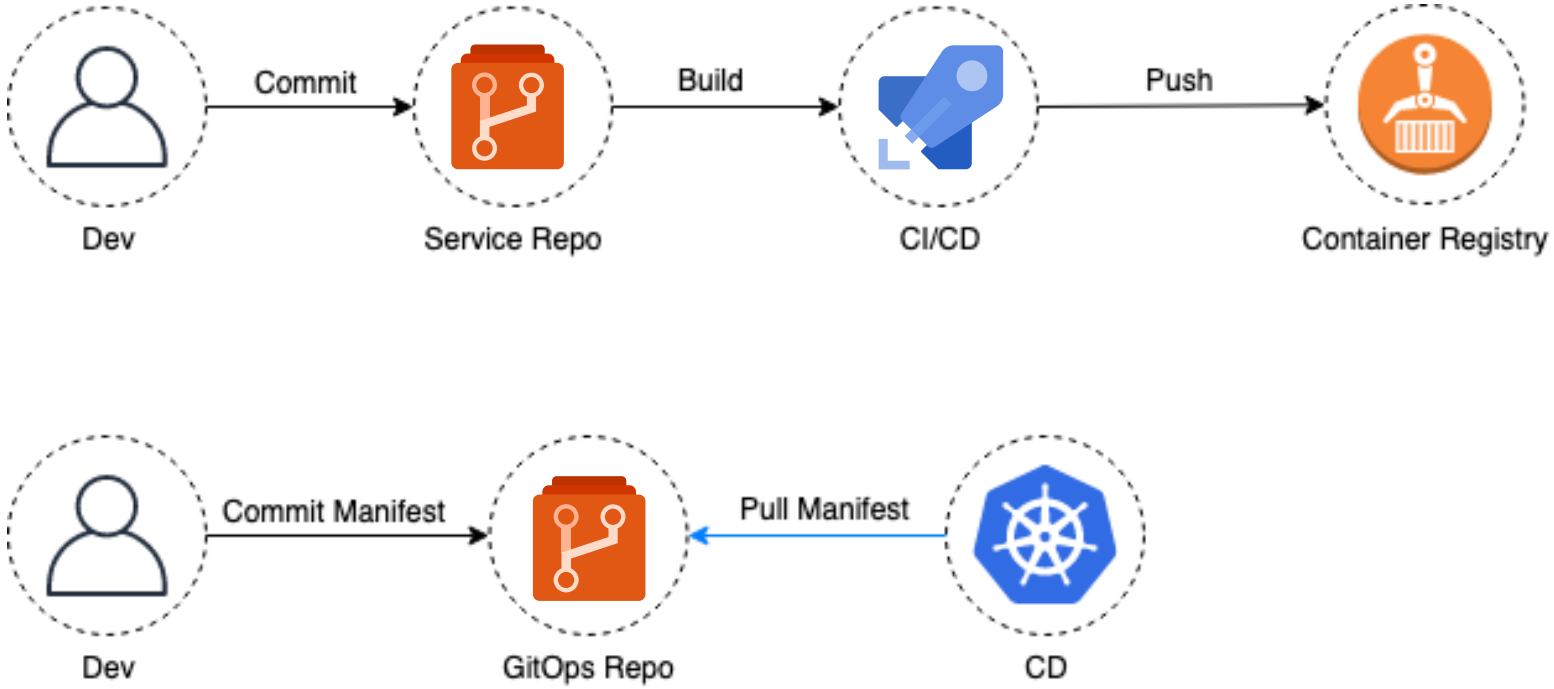
Unique CI/CD pipelines per environment

Have monitoring tools reach into the account rather than the workloads having permissions to write data out elsewhere

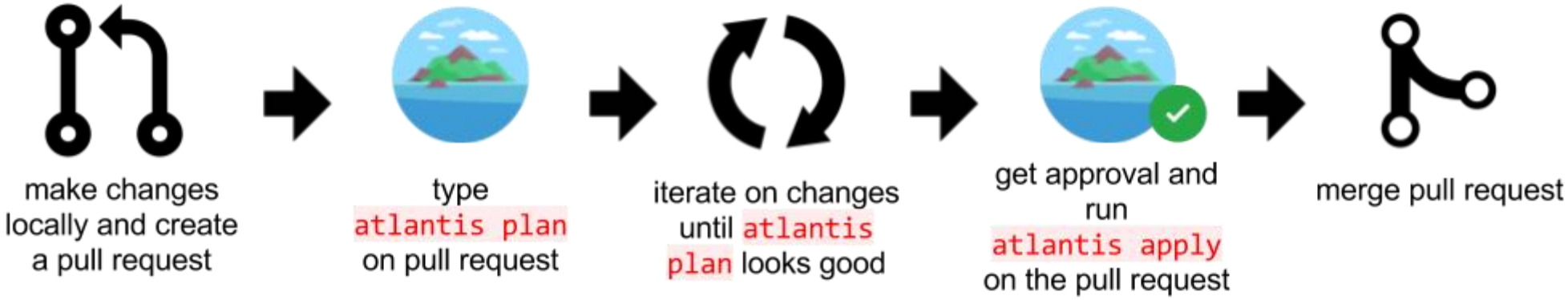
PUSH-BASED CI/CD



PULL-BASED CI/CD



ATLANTIS


make changes locally and create a pull request
type atlantis plan on pull request
iterate on changes until atlantis plan looks good
get approval and run atlantis apply on the pull request
merge pull request

LABS

AVOID PEOPLE IN PRODUCTION

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

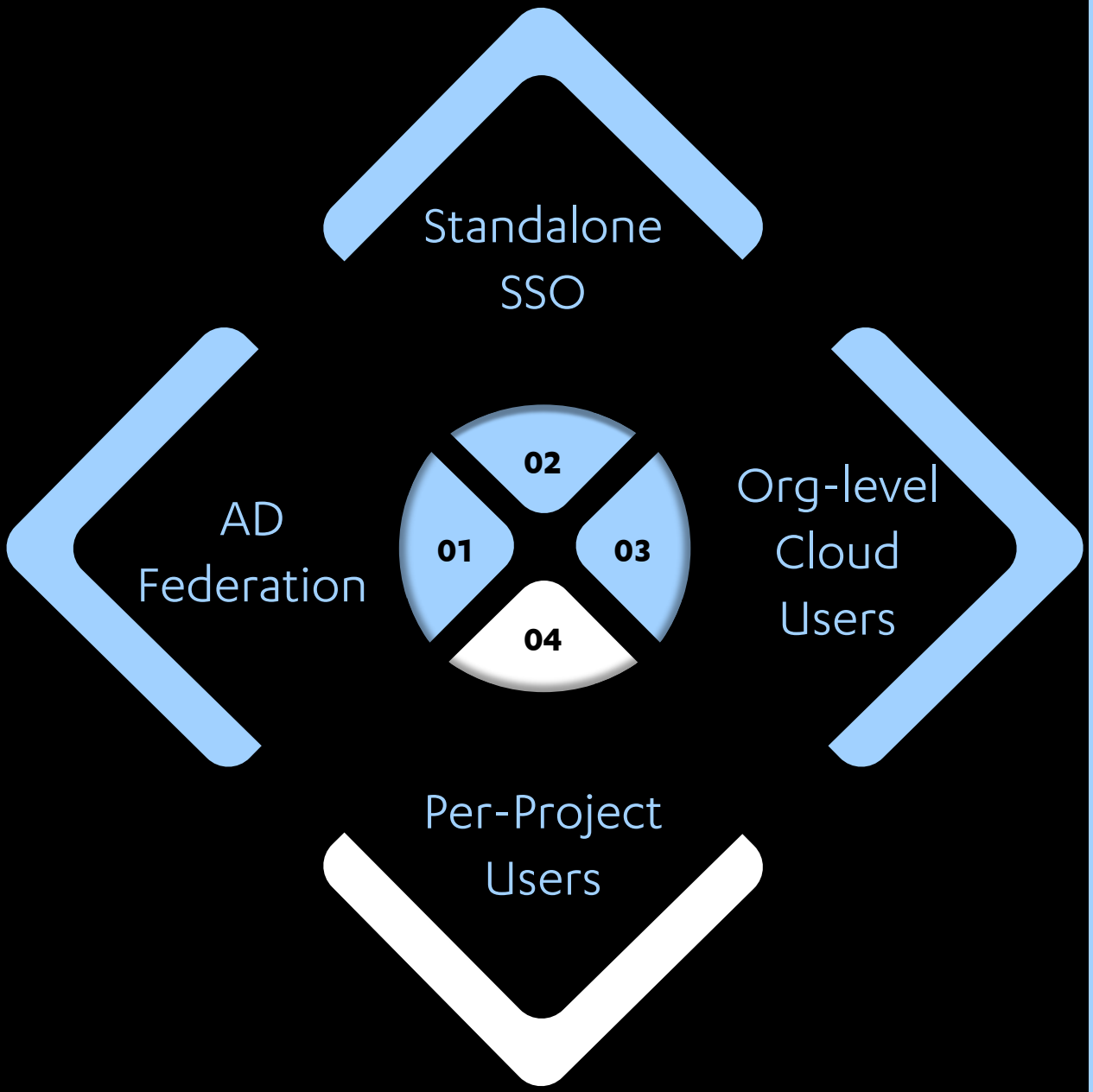
Use Production Access Control

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

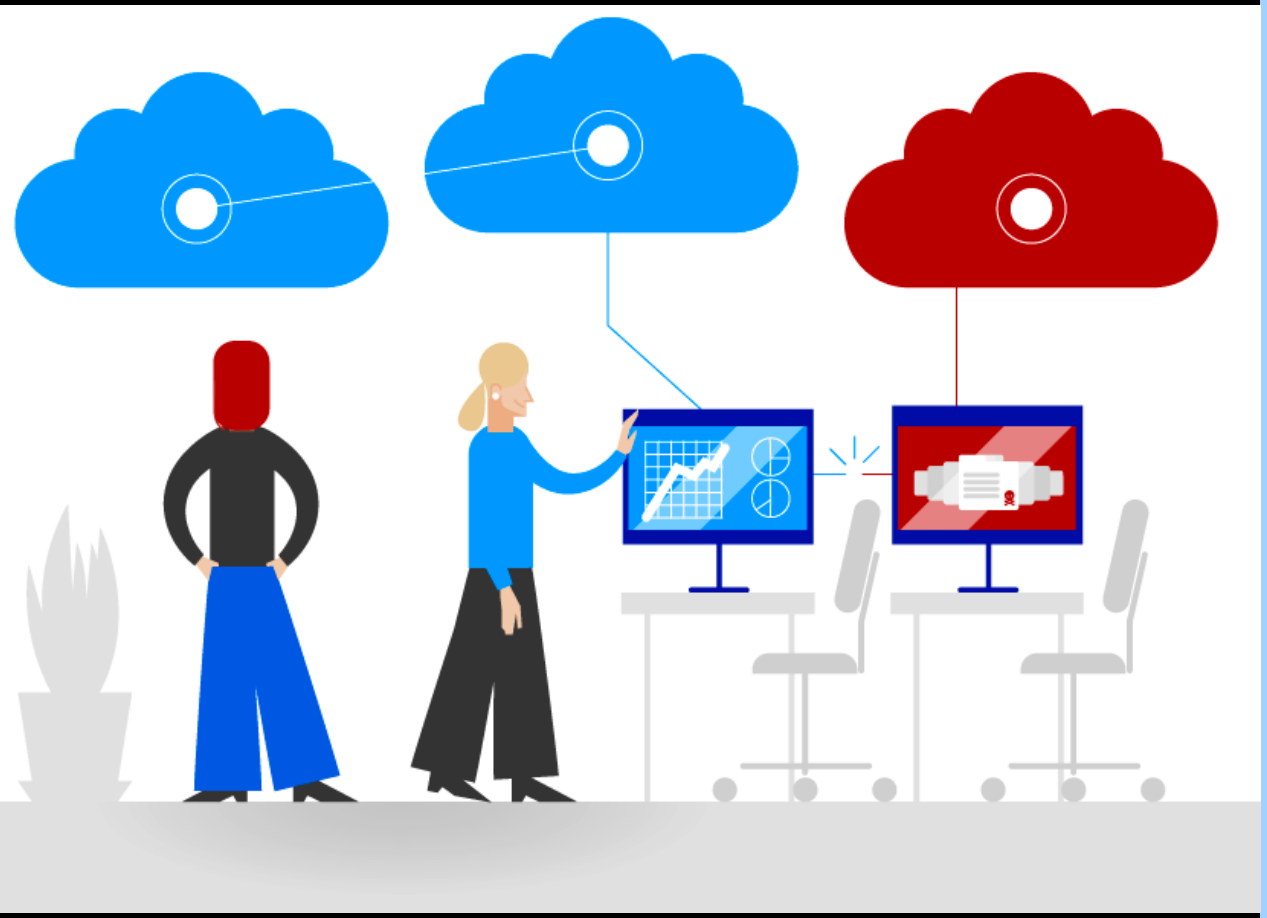
Audit logs from PAC should be monitored by security team, and activity tracked against the appropriate incident ticket



AUTHENTICATION APPROACHES

1. Easy to manage, but expands blast radius of on premise breaches.
2. Breaks the link with on-premise AD, single place for user management across multiple clouds
3. No dependence on external systems, but per-cloud, more long-term management overhead than an SSO
4. Everything is isolated, but adds a lot of management overhead

SECRETS MANAGEMENT



One of the key failings in most cloud environments

Consider:

- Where applications store their secrets
- How credentials are shared between systems
- How secrets are rotated
- How to identify when secrets are leaked – scanners in CI/CD systems, monitoring internal file shares and knowledge bases

SECRETS MANAGEMENT IN AWS

LABS

Make use of AWS services to do the heavy lifting

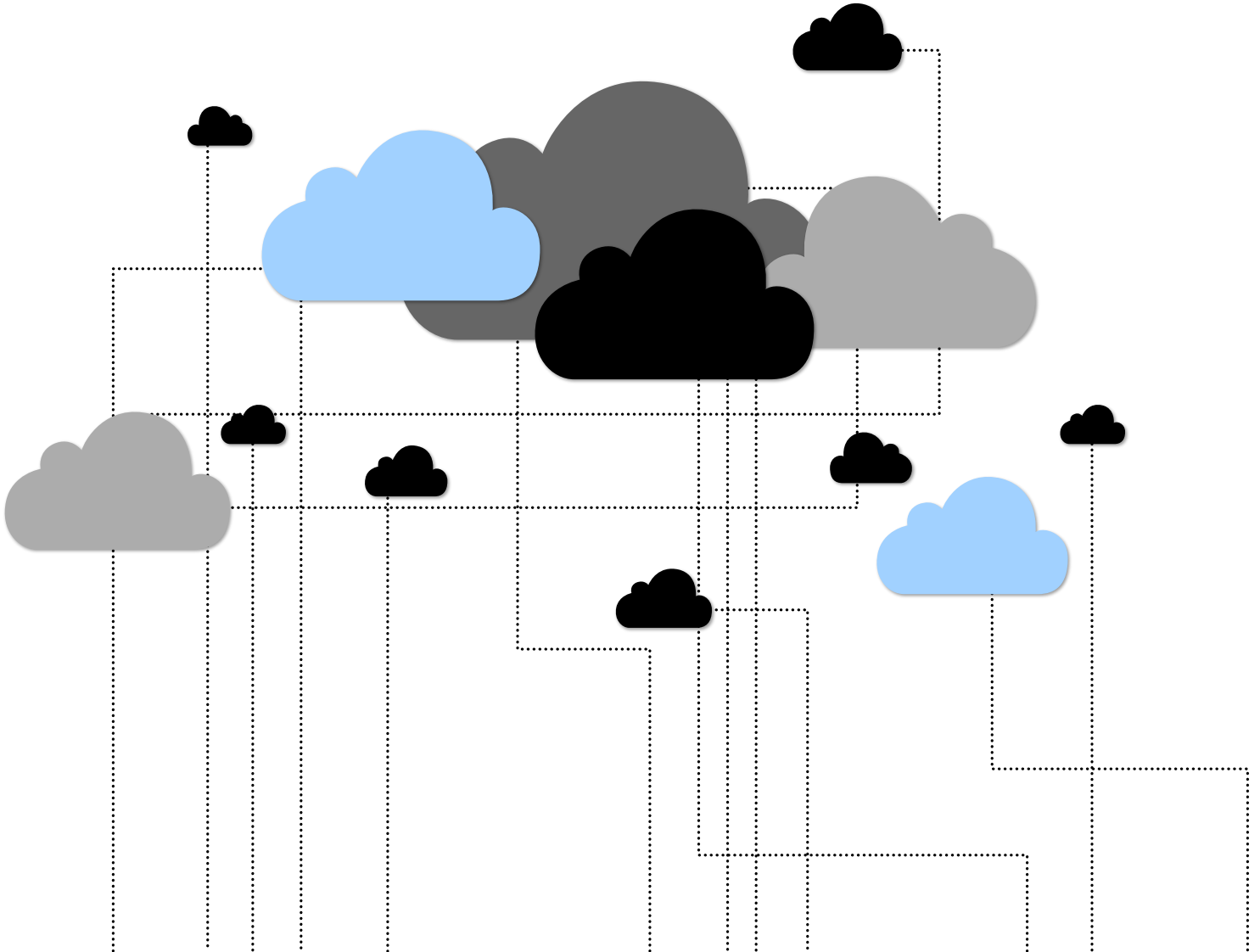
- Secrets Manager
- Systems Manager Parameter Store
- Hashicorp Vault or similar, if used with IAM authentication

Common places to find hardcoded secrets

- **EC2 USER DATA!**
- Cloudformation templates
- App source code
- Environment variables in Lambda configurations
- S3 buckets

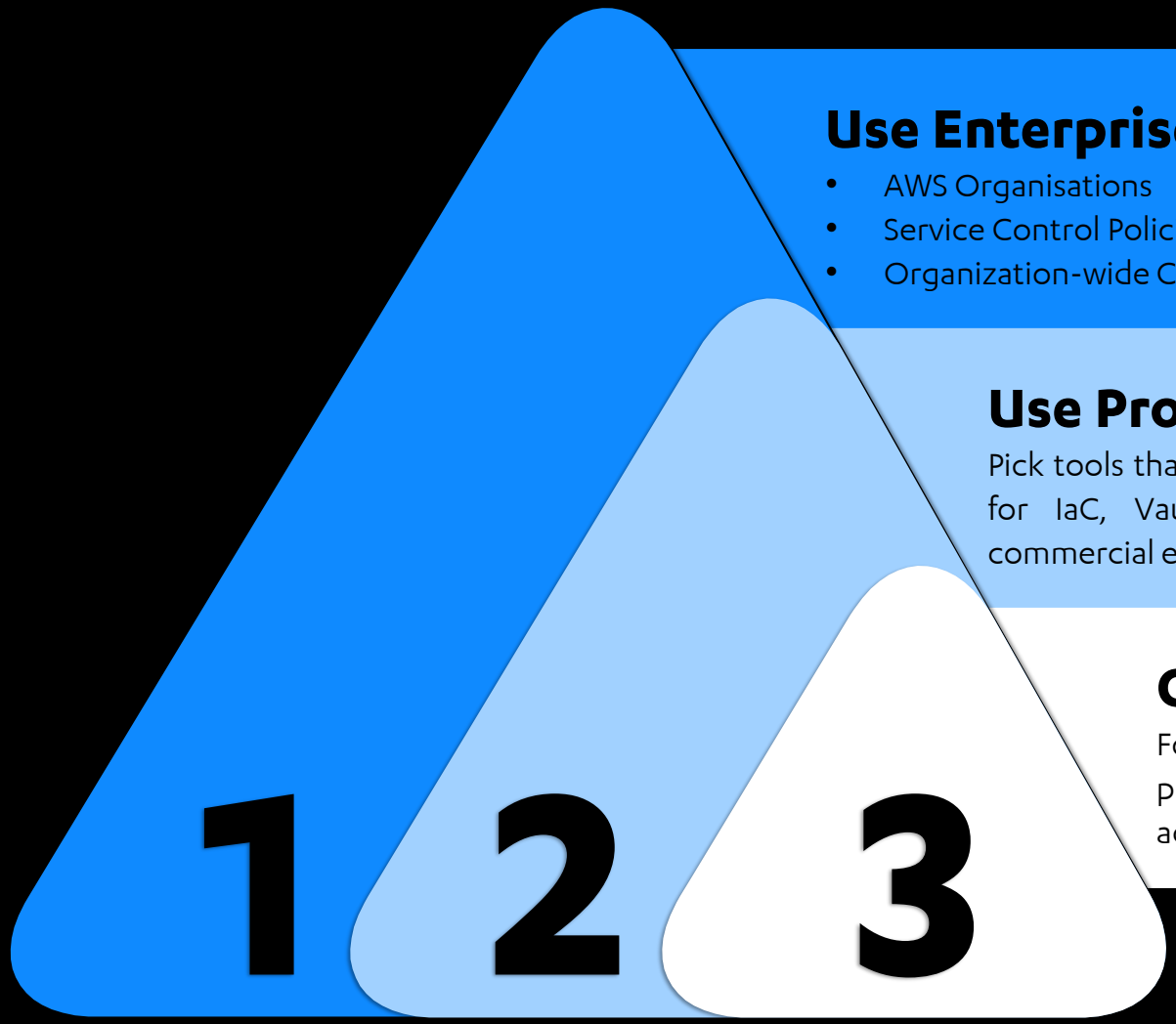
LABS

SCALING CLOUD SECURITY



CENTRALISING MANAGEMENT

LABS



Use Enterprise Management Features

- AWS Organisations
- Service Control Policies
- Organization-wide CloudTrail/GuardDuty

Use Provider-Agnostic Tooling

Pick tools that work across all the cloud providers you work with. Terraform for IaC, Vault/Conjur for secrets management, Cloud Custodian or commercial equivalent for configuration review and enforcement

Centralise Security Functions

For each provider, maintain a security account, subscription or project, and another for logs. Tightly restrict access to these accounts to only those users and systems who really need access

LABS

CENTRALISING MONITORING

SOURCE	BENEFIT
Control Plane audit logs (CloudTrail)	**Visibility of all administrative actions**
Service Specific Logs (S3 storage access logs, Lambda executions, KMS key access, etc.)	**Shows access and usage of specific resources and services, which may help to track lateral movement or actions on objective**
Cloud-native detection services	Detection of known bad activity
API Gateway/WAF Logs	Identify malicious requests to applications
VPC flow logs	Identify anomalous traffic by source and destination, volumes etc
System logs from any VMs	Grants OS-level visibility of potential attacker activity
Endpoint Detection and Response agents in VMs	Detects malicious activity within VMs as with on premise estates
Application logs	Provides app-specific contextual information

LABS

LOG SOURCES

CloudTrail

> *"CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services."*

From a security monitoring perspective, this is the **MVP**. Amongst other things, it can include API calls for IAM (user creation, modification, etc.) and service-level events like EC2 creation, S3 bucket creation.

LABS

LOG SOURCES

Service-specific Object-level / Data Events

Whereas CloudTrail gives us an ***account-level*** view, several services provide enhanced logging, e.g. S3's ***Data Events*** logging.

Whereas a `ListBuckets` event is logged by default in CloudTrail, a `ListObjects` or `GetObject` event is not. Similar comparisons exist across other services like DynamoDB.

Further, services like AWS GuardDuty output their 'Findings' to CloudWatch which can be forwarded, used to trigger subsequent actions, etc.

When enabled, object-level data events are logged to CloudTrail too

DECENTRALISED SECURITY SKILLS

LABS

Range of technologies too broad for an individual to build skills in all areas

Engineers are the SMEs, security should collaborate closely with them for best effect

Security teams should include automation specialists – ex-cloud/devops engineers ideal here.

Expect to invest heavily in this area –cloud security people are scarce, and thus expensive

DECENTRALISED SECURITY PROCESSES

LABS

Central security teams will not have the bandwidth to secure everything

Train and empower your engineering teams to:

- Do their own threat modelling
- Build and extend relevant security automation

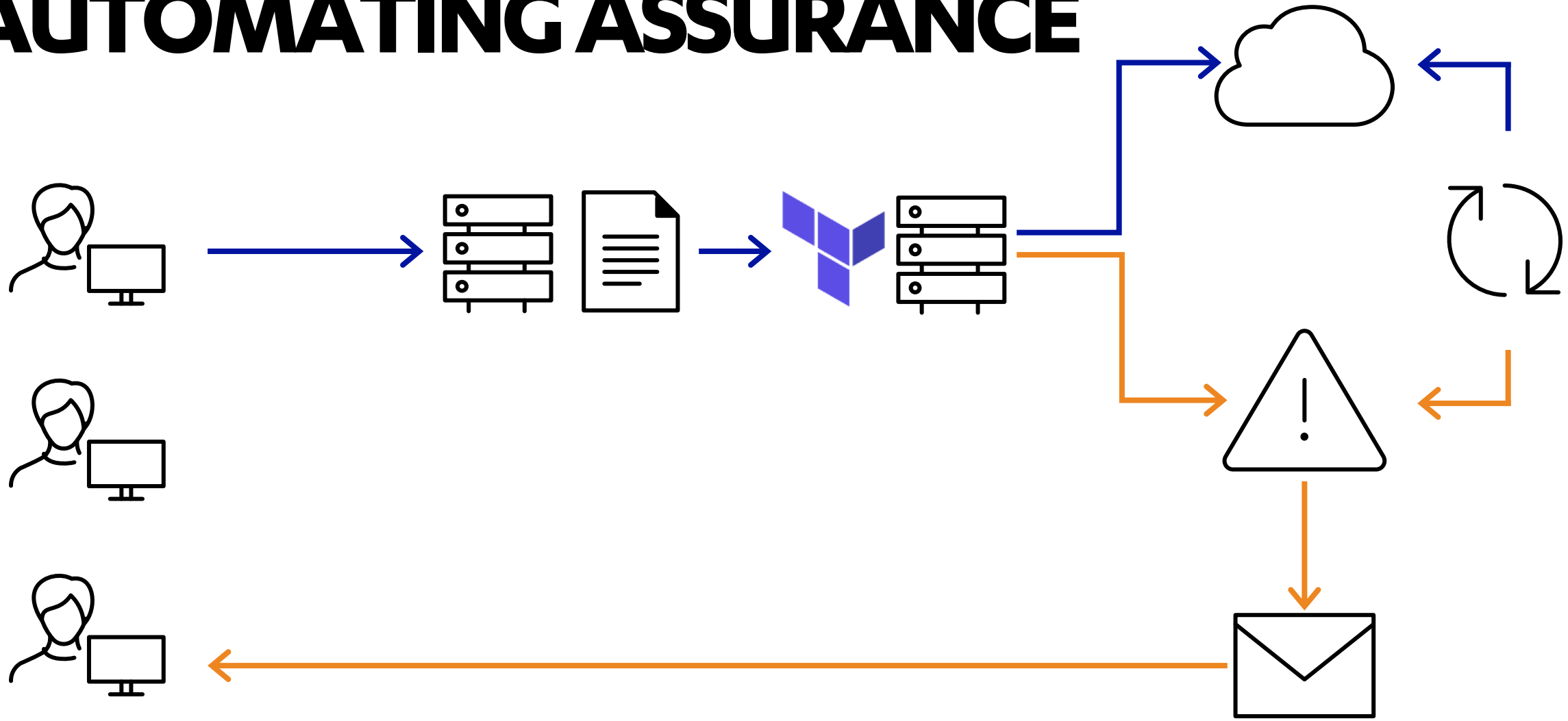
Make security expertise available to individual teams throughout the development lifecycle

Cheaper to fix security issues earlier in the process

Have a triage process to prioritise security work

LABS

AUTOMATING ASSURANCE

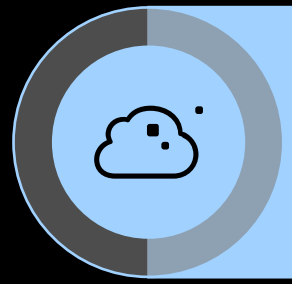


F-Secure | LABS

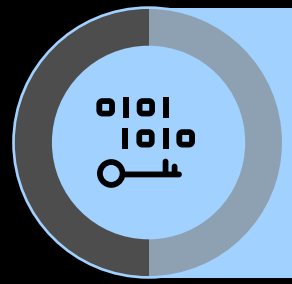
CONCLUSIONS

CONCLUSIONS

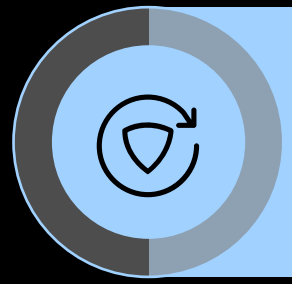
LABS



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

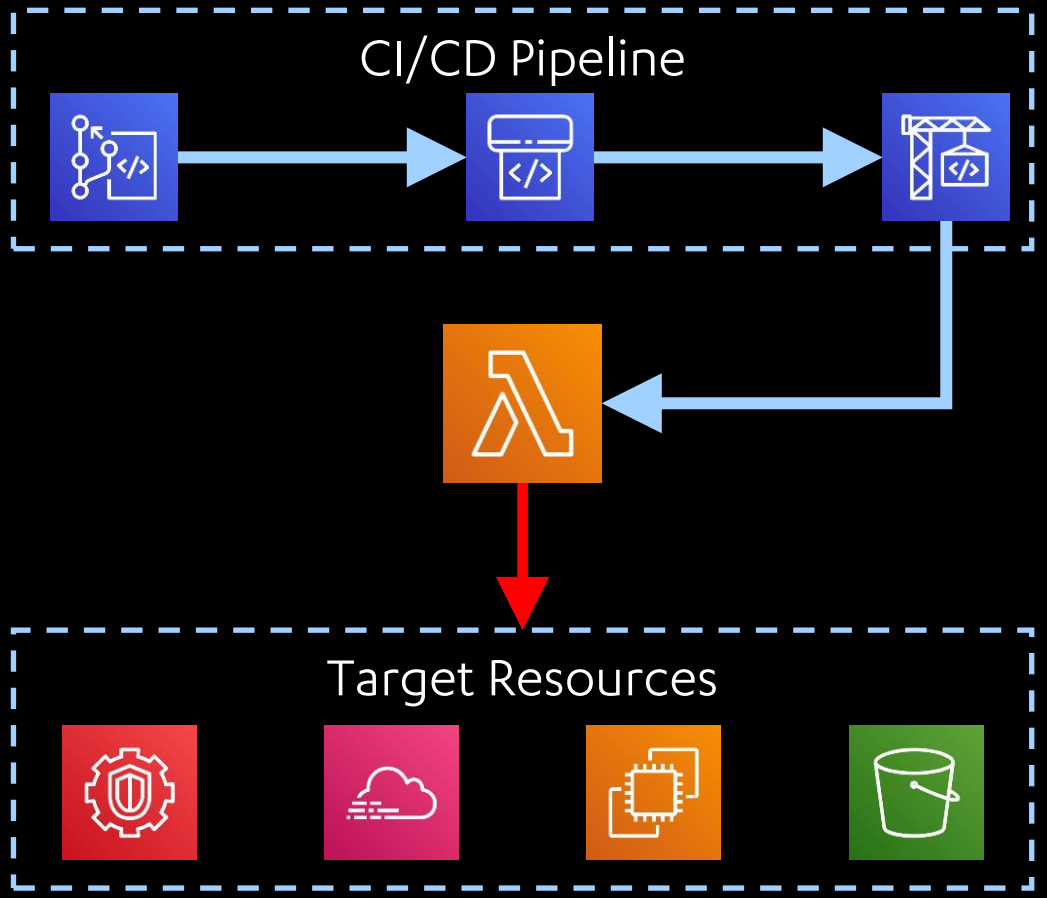


Focus on IAM, secrets management, environment segregation and CI/CD



Leverage automation and empower engineers to scale company-wide

LEONIDAS



- Automate attacker actions in the cloud
- Both test and detection cases
- AWS support now, Azure/GCP on the roadmap
- 45 test cases - more to come
- https://github.com/fsecurelabs/leonidas


F-Secure
LABS