CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Cloud Native Security 101: Building Blocks, Patterns and Best Practices

Rafik Harabi

Who Am I?

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

- Senior Solution Architect at Sysdig, Cloud Security Advocate
- Focus on Cloud Native Security and Observability
- Previously working on go to Cloud programmes

rafikharabi

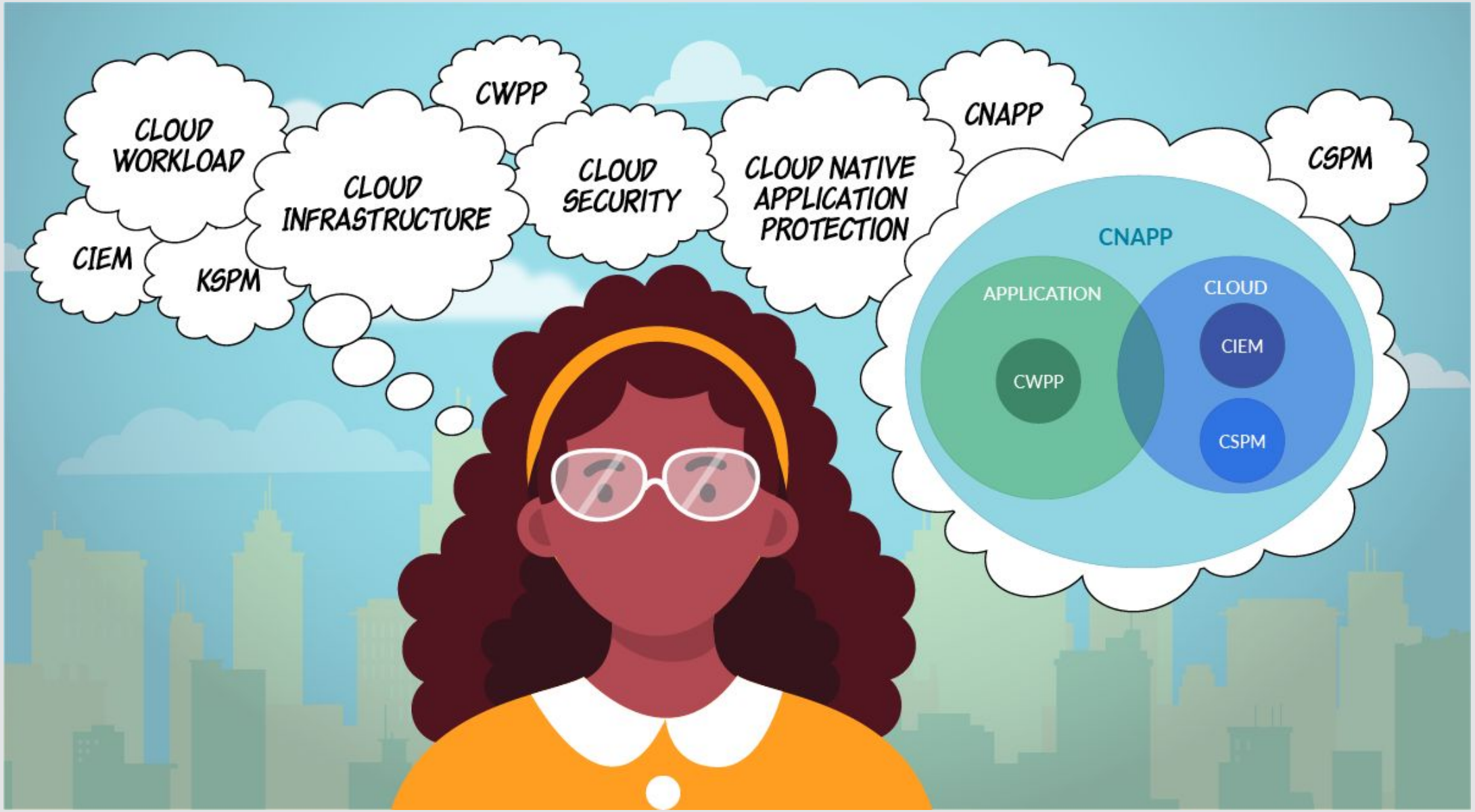
@rafik8_

Who are you?

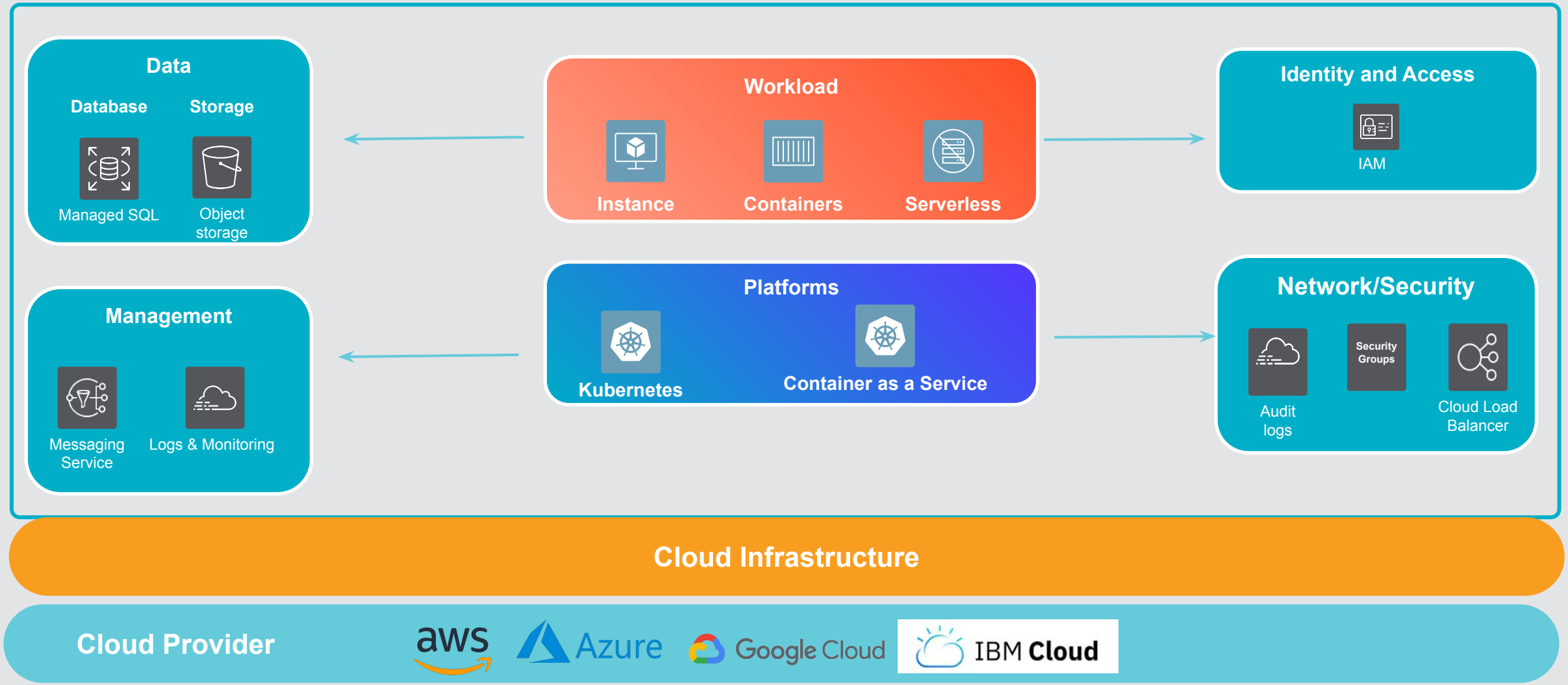
- Who is here for the first time?
- Who knows one of those acronyms: **CWPP, CSPM, KSPM, CIEM, CNAPP, CDR**?
- Who knows two of them?
- Who knows three?
- All of them?

Agenda

- Cloud Native Security acronyms
- Anatomy of Cloud Native application
- Lifecycle of Cloud Native application
- Cloud Native Security Platform building blocks.
- Attack vectors.
- Patterns & Best Practices.
- Personas and Workflows.


CLOUD WORKLOAD
CIEM
KSPM
CLOUD INFRASTRUCTURE
CWPP
CLOUD SECURITY
CLOUD NATIVE APPLICATION PROTECTION
CNAPP
CSPM
CNAPP
APPLICATION
CWPP
CLOUD
CIEM
CSPM

Anatomy of Cloud Native Application

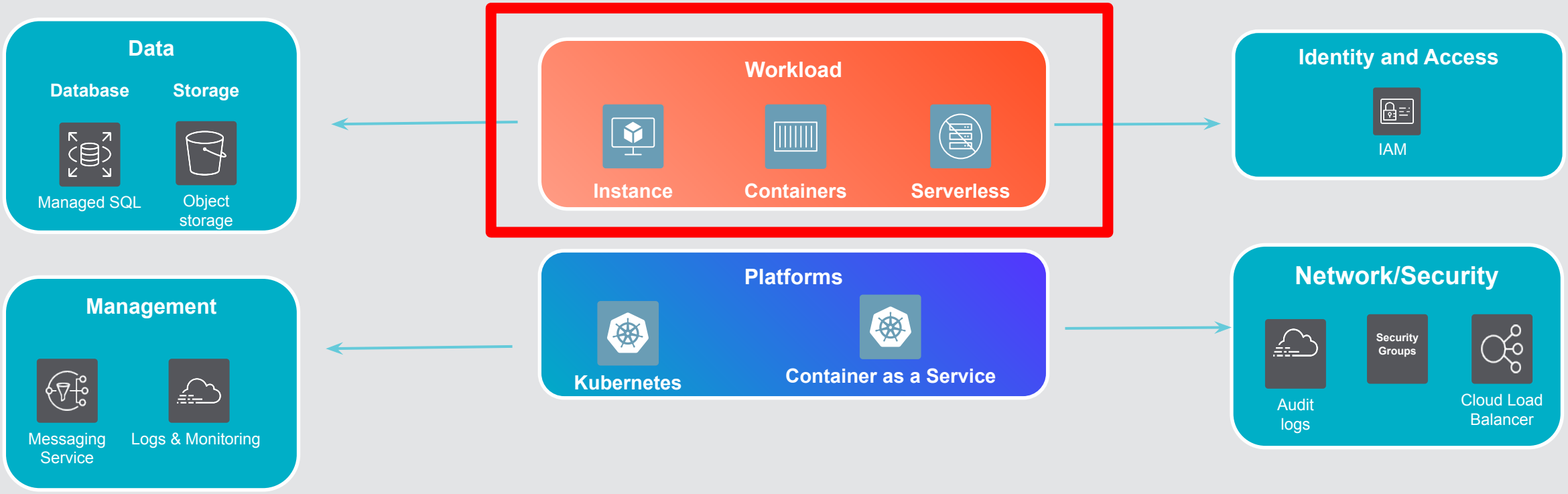


Cloud Native Acronym

CWPP

Cloud **W**orkload
Protection **P**latform

Workload and application security (Container, VM, Serverless).

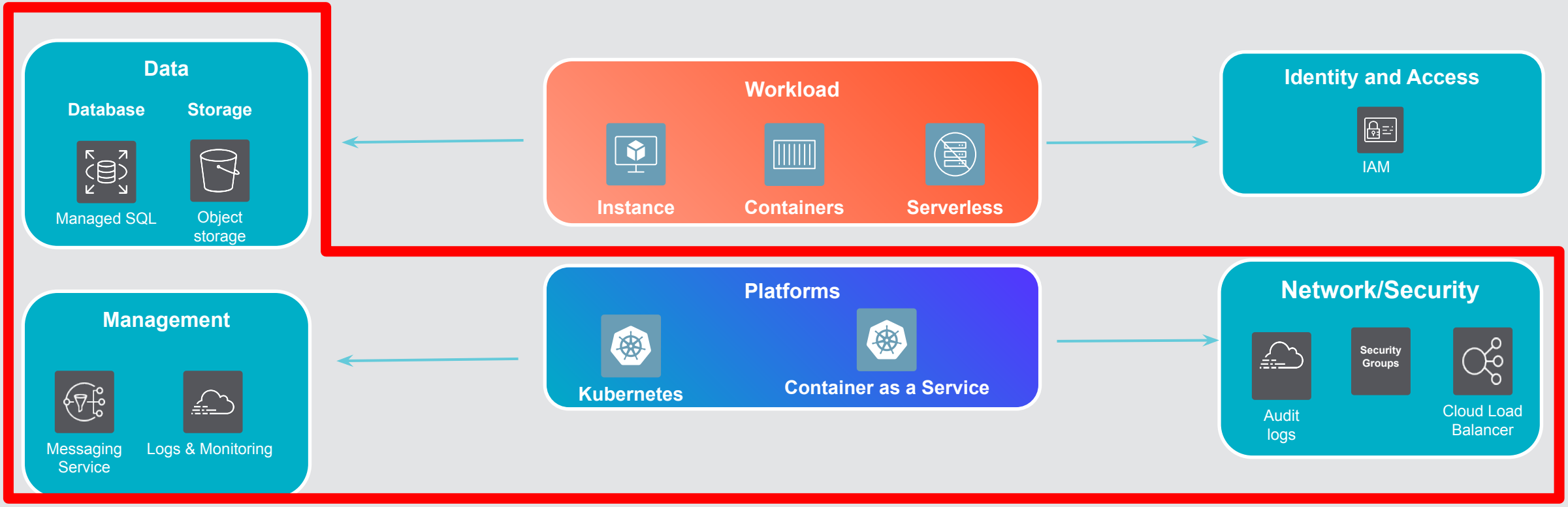


Cloud Native Acronym

CSPM

Cloud Security **P**osture **M**anagement

Cloud assets configuration security: Protect the cloud control plane, basically tracking cloud resources and verifying the static configuration of the cloud



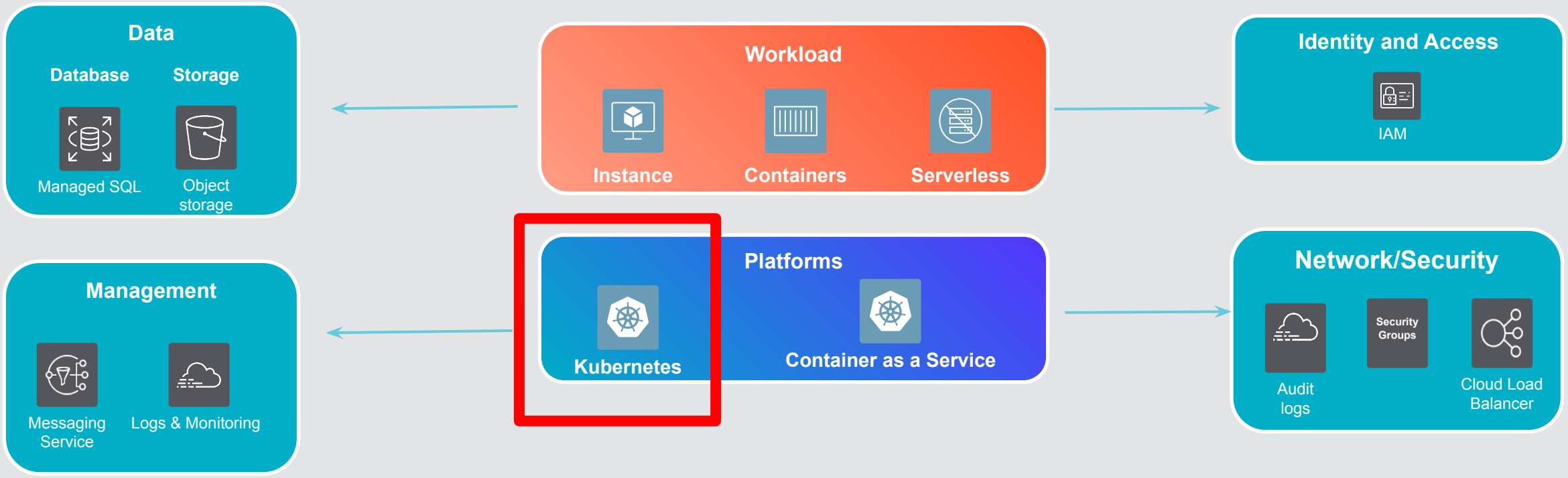
Cloud Native Acronym

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

KSPM

Kubernetes Security
Posture **M**anagement

Security configuration assessment for Kubernetes.

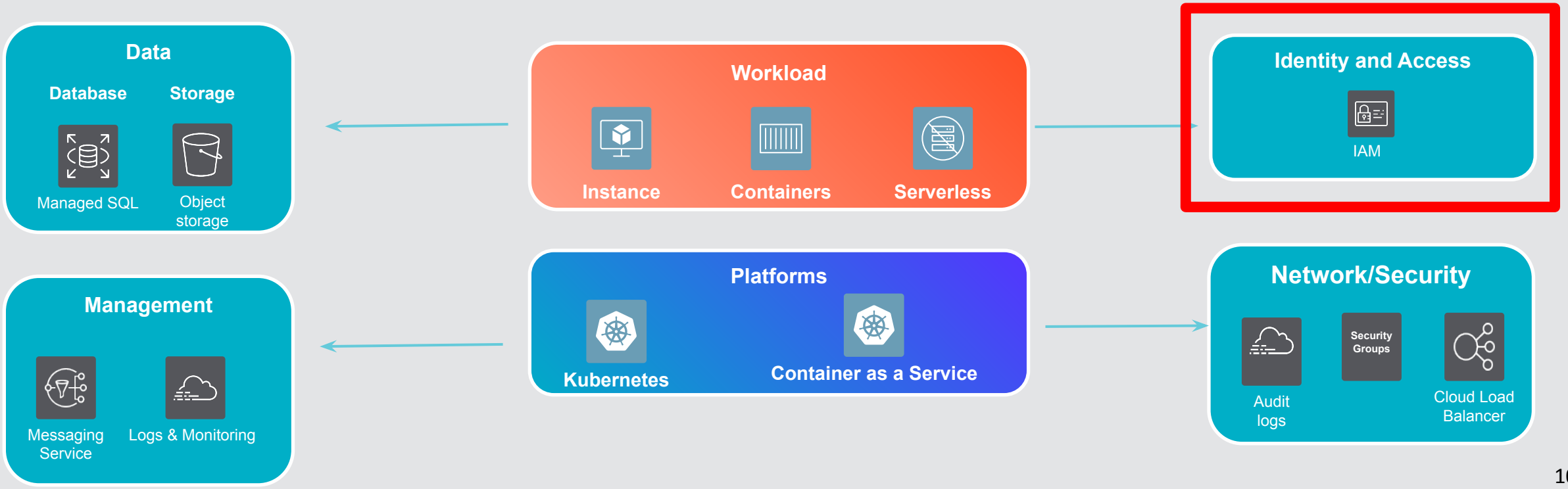


Cloud Native Acronym

CIEM

Cloud **I**nfrastructure
Entitlement **M**anagement

Manage identity and access security for both humans and services. Reducing the risk of excessive permissions and entitlement in the cloud.

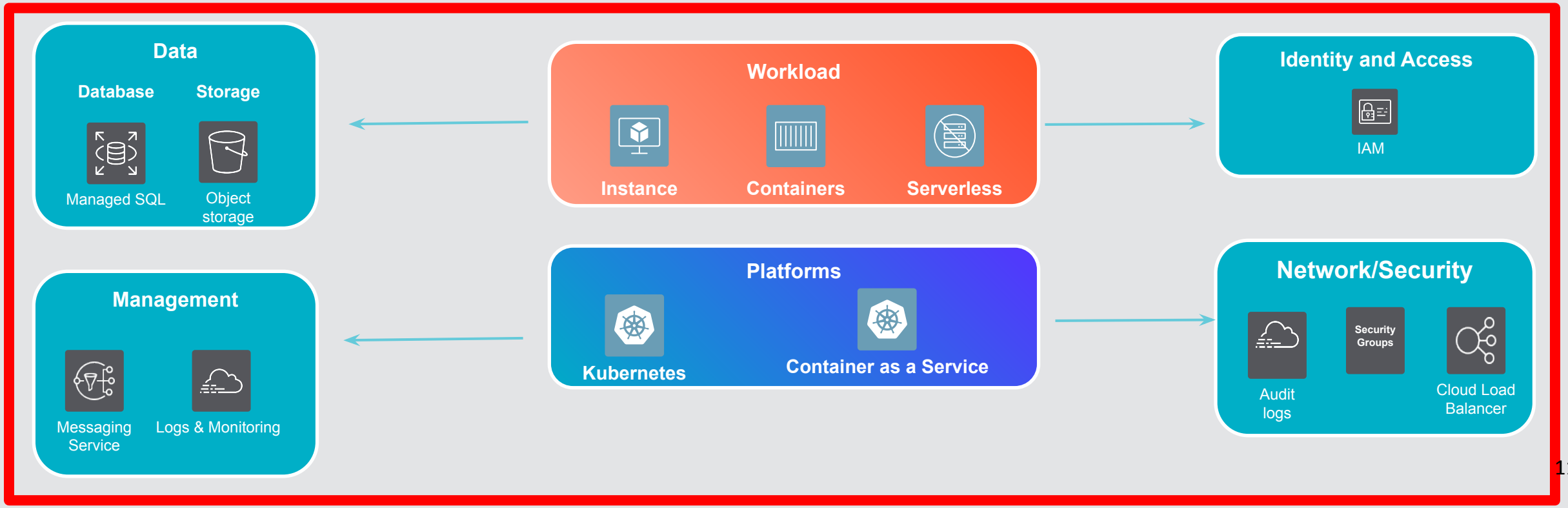


Cloud Native Acronym

CDR

Cloud **D**etection and **R**esponse

Threat Detection and Response for Cloud Assets and Workloads.

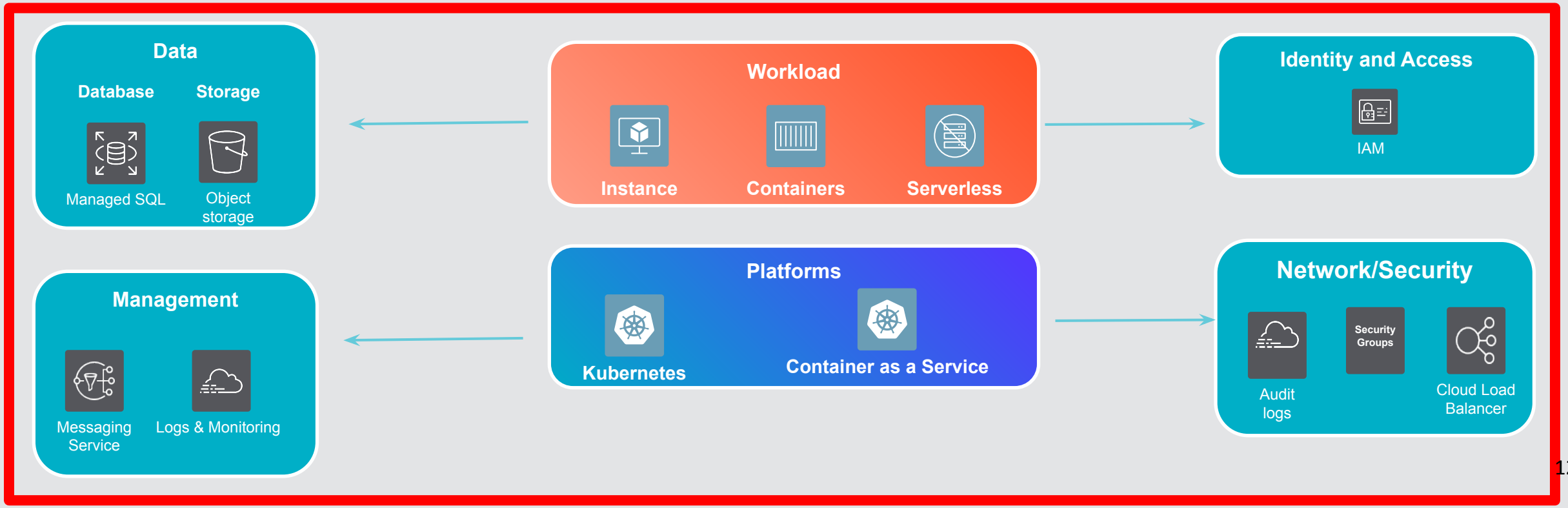


Cloud Native Acronym

CNAPP

Cloud **N**ative
Application **P**rotection
Platform

A platform that combine CSPM, CIEM, CWPP and CDR.



CNAPP Building Blocks

CSPM (& KSPM)

- Vulnerability Management
- Cloud Misconfigurations / IaC
- Cloud Inventory
- Cloud Threat Detection
- Compliance

CIEM

- Cloud IAM: Identities and Permissions
- Detect excessive permissions

CNAPP

CWPP

- Vulnerability Management
- Container / K8s Runtime Security
- Serverless Security
- Host/Container Threat Detection

CDR

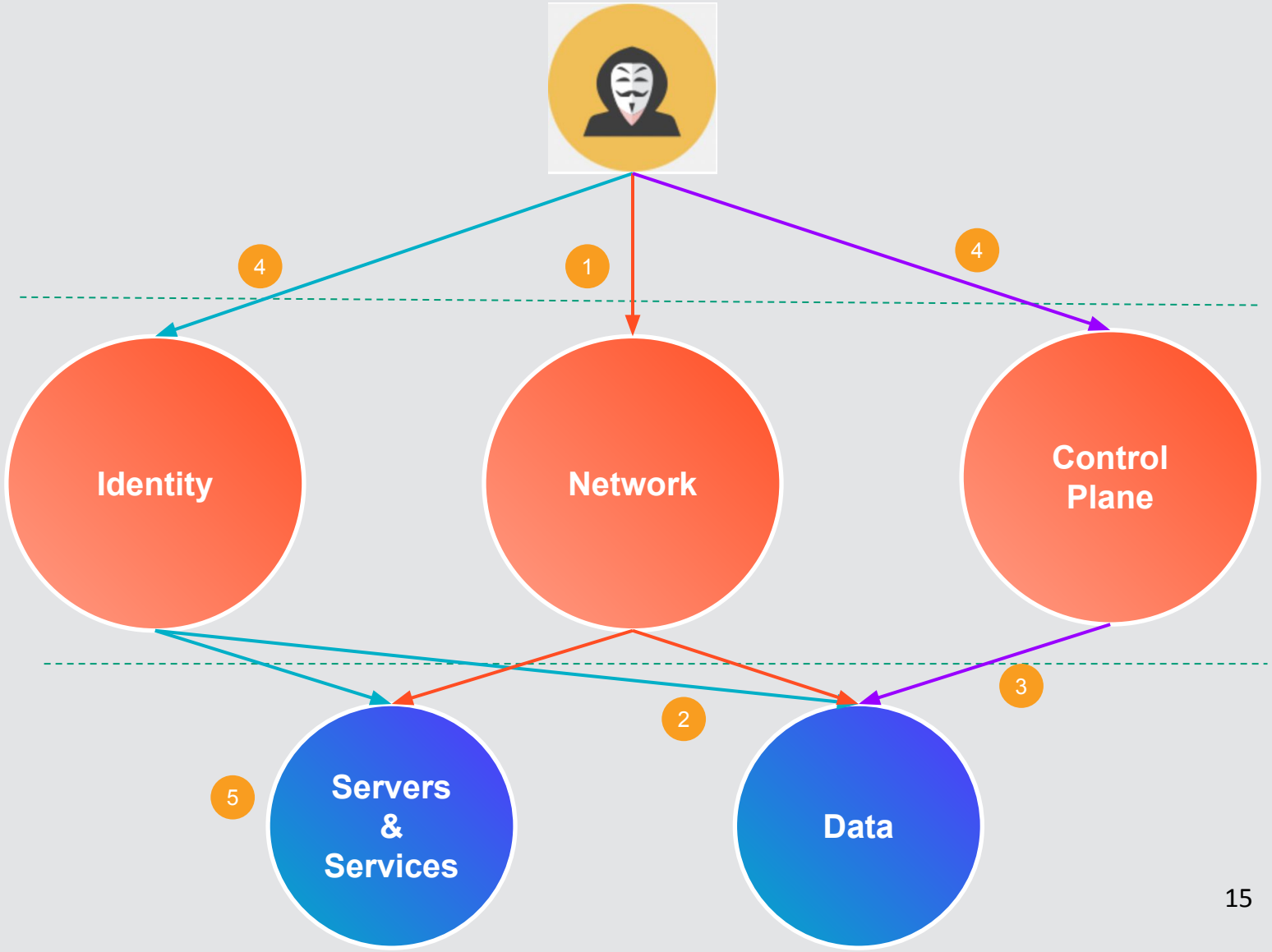
- Cloud Threat Detection
- Container / K8s Runtime Security
- Host Threat Detection

Attack Vectors

Cloud Attack Vectors

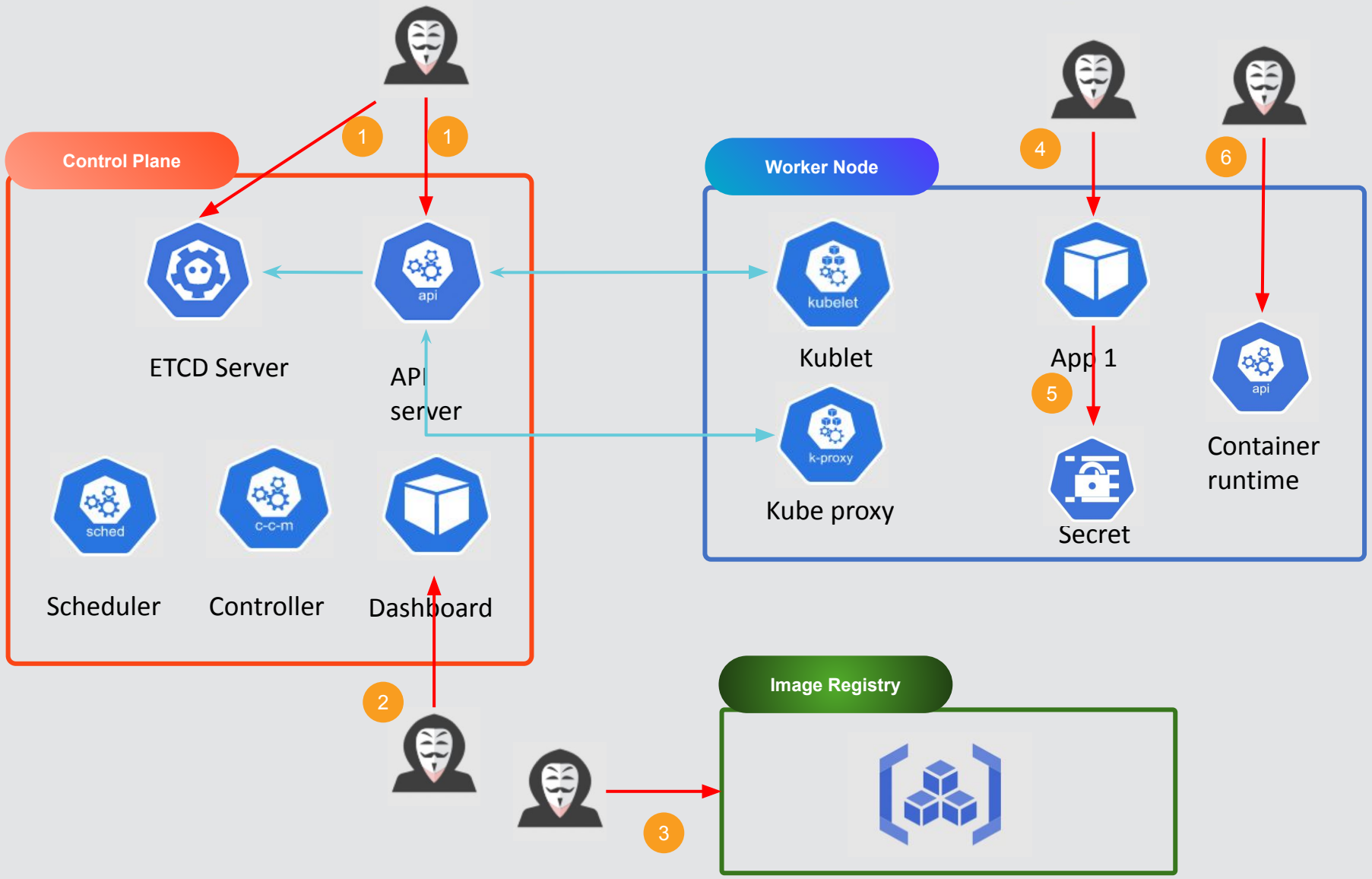
CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

1. Cloud network breaches
2. Unauthorized resource access
3. Cloud data exfiltration
4. Cloud security misconfiguration
5. Vulnerability exploits



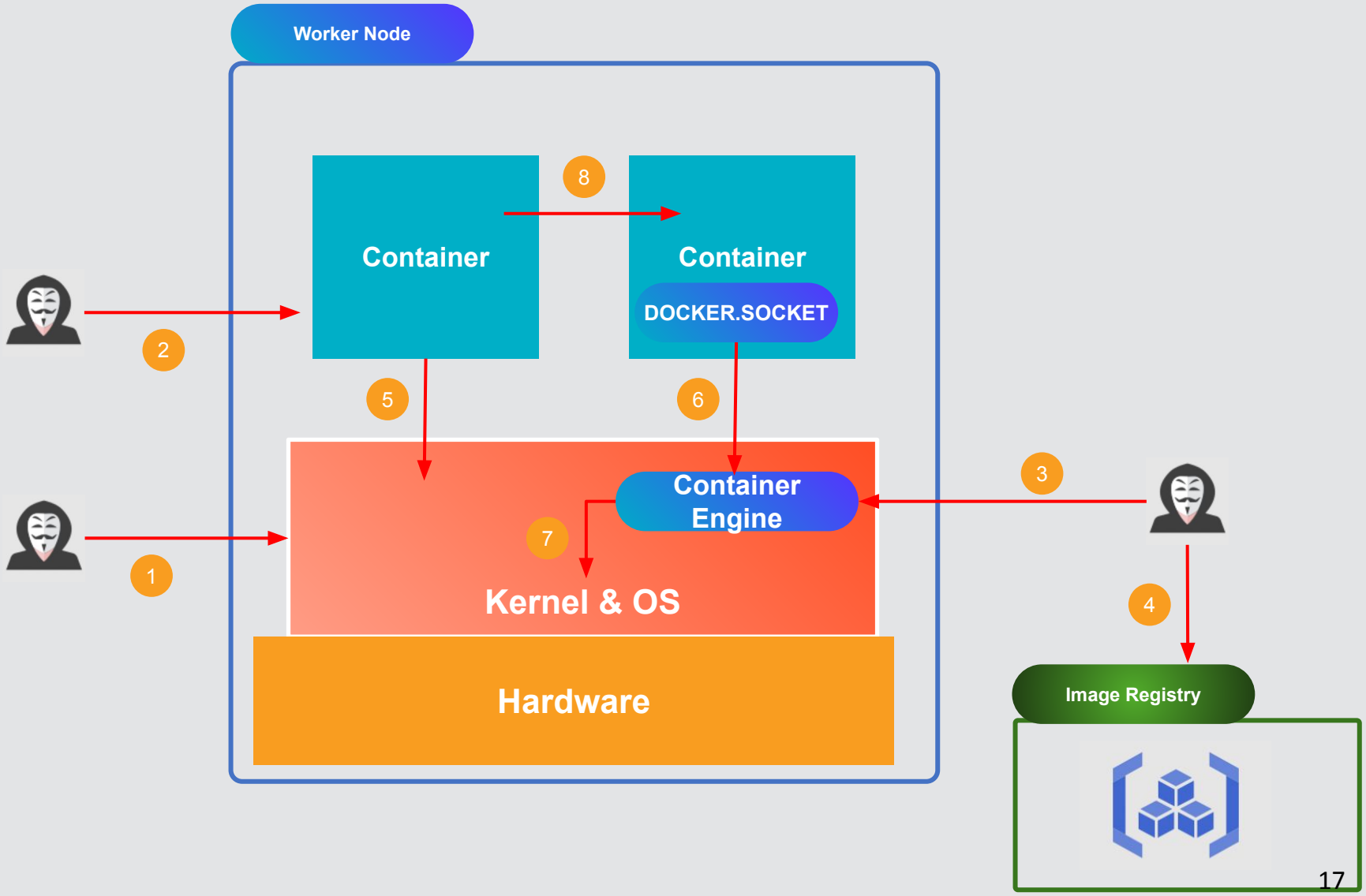
Kubernetes Attack Vectors

1. Access K8S API Server / ETCD API
2. Dashboard misconfiguration
3. Malicious container image in registry
4. Application with exploitable vulnerability
5. Gain access to secrets
6. Docker daemon misconfiguration



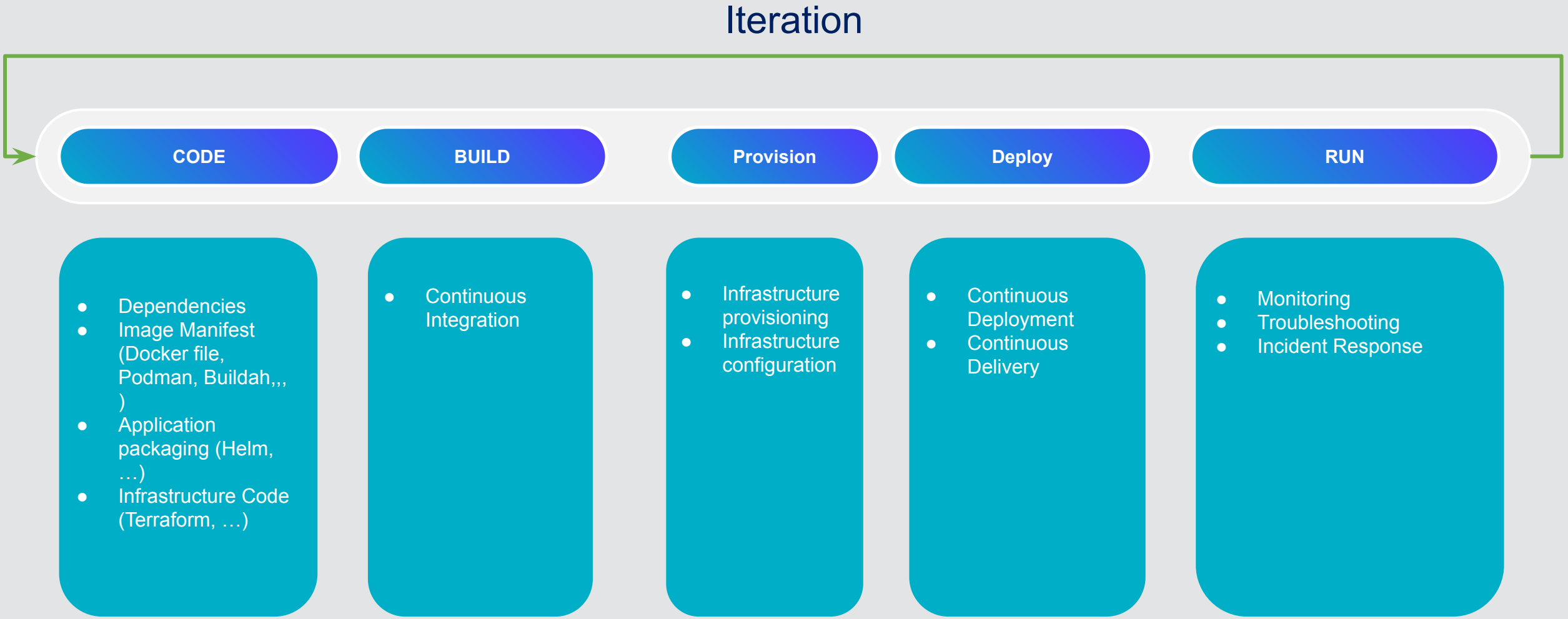
Container Workload Attack Vectors

1. Vulnerable OS/Container engine
2. Vulnerable application
3. Exposed Container engine
4. Insecure image registry
5. Privileged containers
6. Misconfigured container
7. Privilege escalation on host
8. Insufficient Network isolation



Patterns & Best practices

Lifecycle of Cloud Native Application



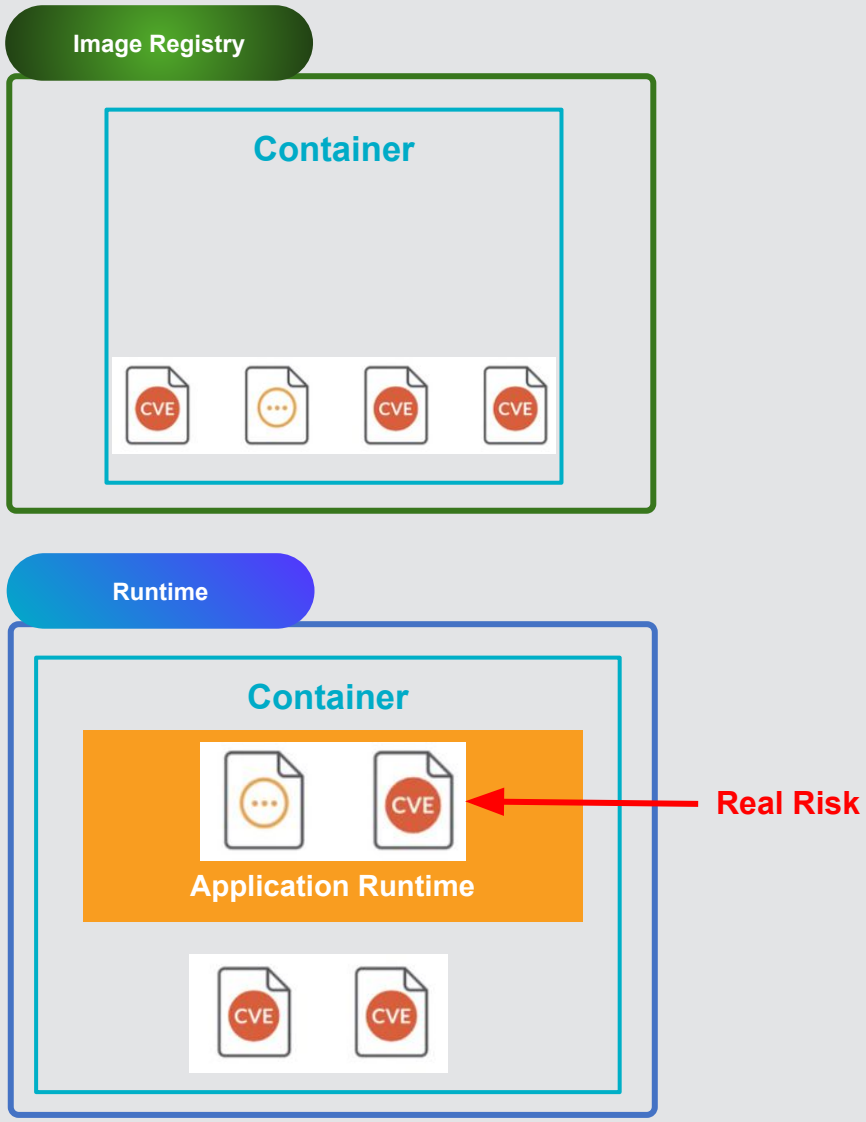
Secure Cloud Native Application

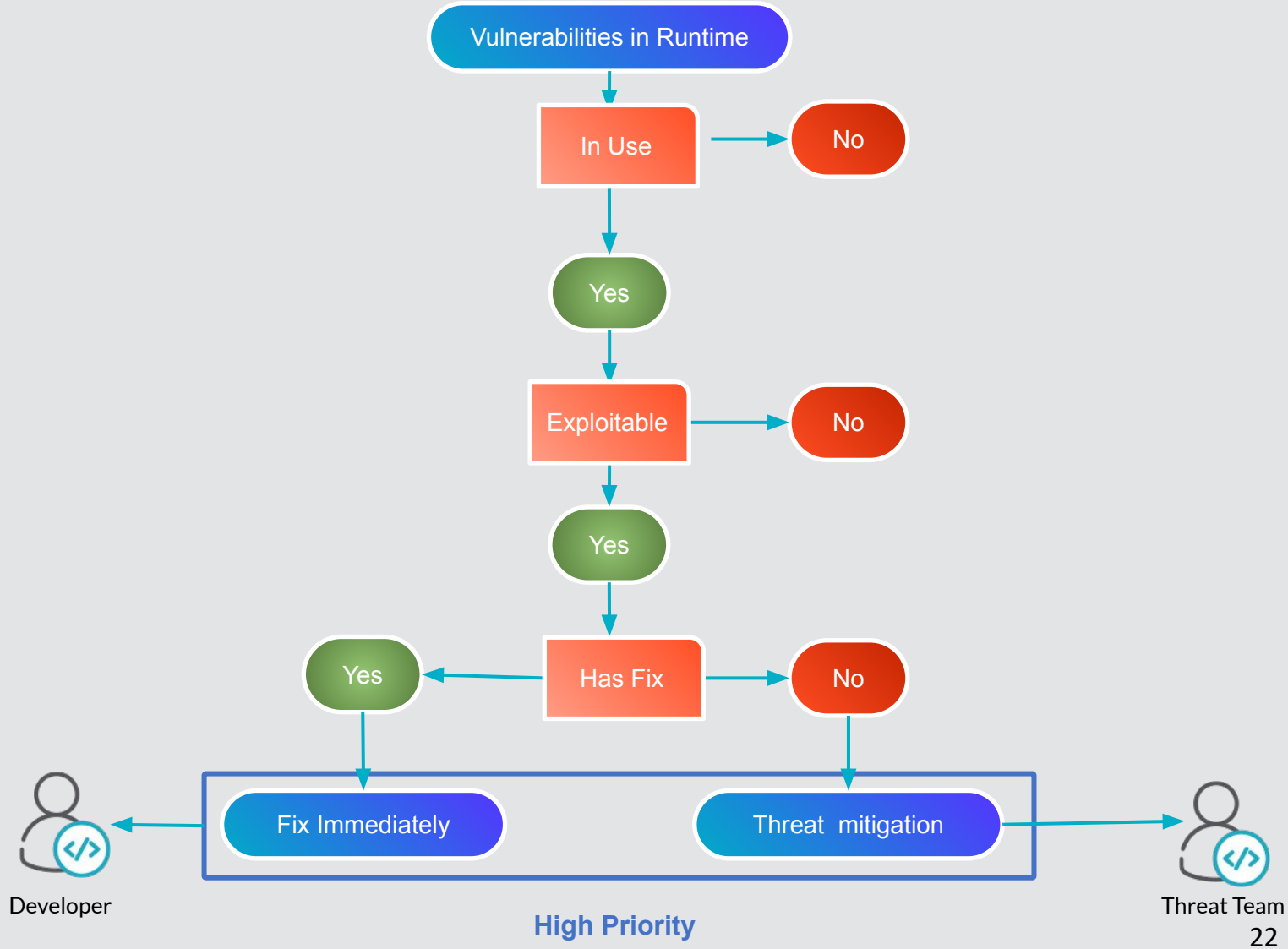
CODE	BUILD	Deploy	RUN			Respond & Forensics
Infrastructure as Code Validation	**Vulnerability Management**	**Admission**	**Configuration Management**	**Identity and Access Management**	**Threat Detection**	**Incident Response**
• Drift prevention • Block risky configs	• CI/CD pipelines, registries, and hosts • Prioritization based on in-use vulns	• Block risky images • Block risky config	• CSPM / cloud misconfigurations • Cloud Inventory	• CIEM / least privilege • Prioritization based on in-use permissions	• Cloud threat detection • Workload runtime security	• Capture detailed record for forensics • Block malicious containers / processes

Container In-Use vulnerabilities Prioritization

- **Pattern**: Prioritize images to be fixed based on packages that are really in use
- **Why**: Image contains usually many packages that are embedded but never used/loaded
- **Result**: Focus on what really matter to proritze and fix (avoid engineers fatigue)
  - multi-level vulnerabilities focus:
    - *In use ?*
    - *Exploitable ?*
    - *Has fix ?*
- Both for containers and Kubernetes hosts

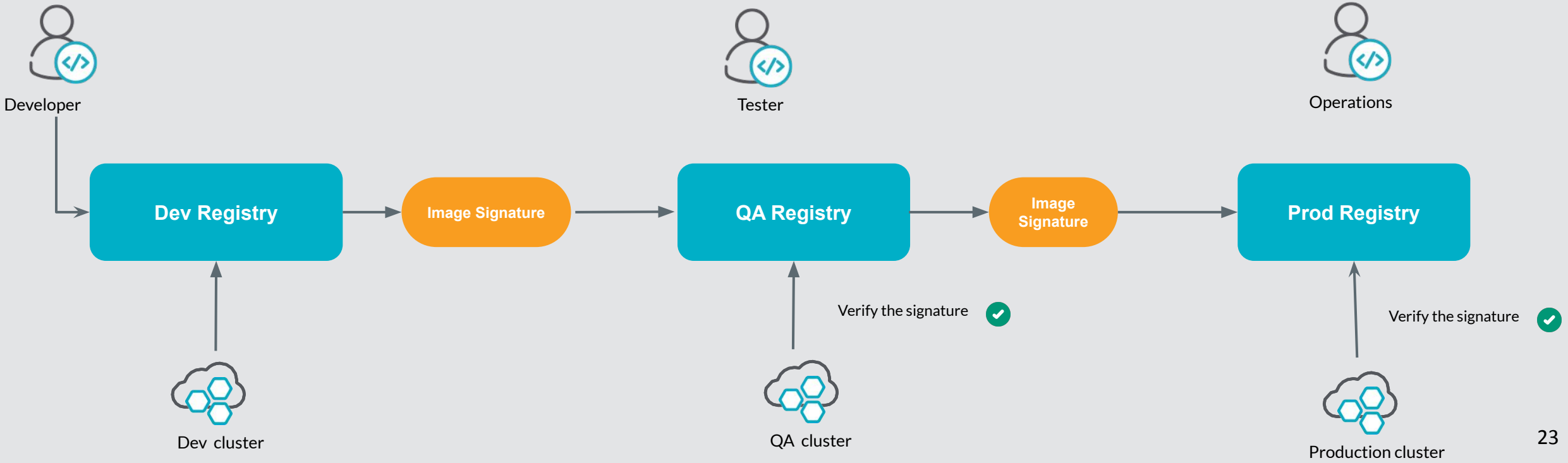
Container In-Use vulnerabilities Prioritization





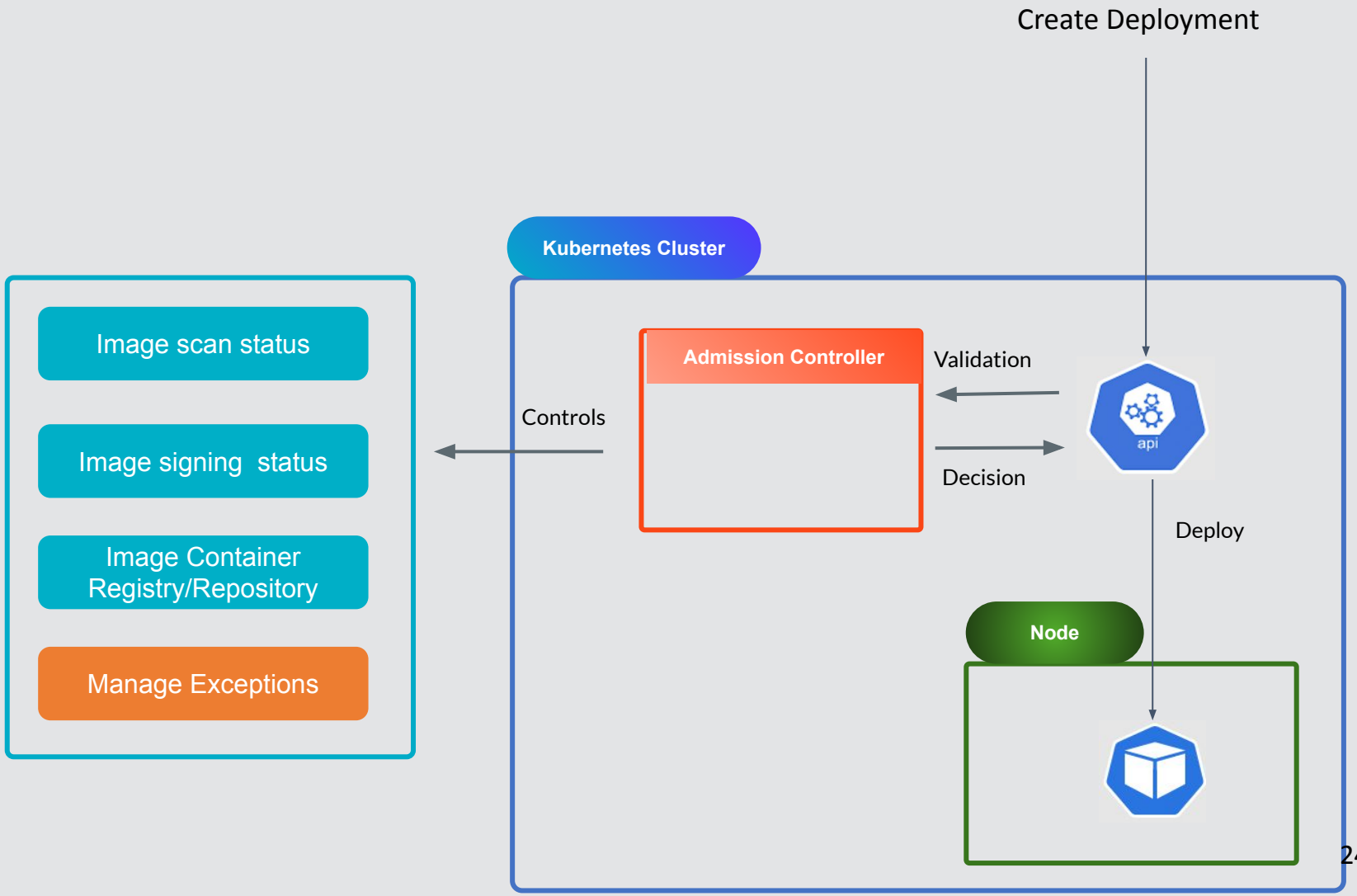
Container Image Signing

- **Risk**:
  - Deploy and run non-compliant/trusted image
- **Benefits**:
  - Container image integrity
  - Images are from a trusted source
  - Safe handover (from development to production)



Gatekeeper pattern (AC)

- Based on Kubernetes Admission controller
- **Risk**:
  - Vulnerability Image
  - Image from non trusted source
  - Compromised Image
- **Benefits**:
  - Avoid deploying and running non compliant workloads

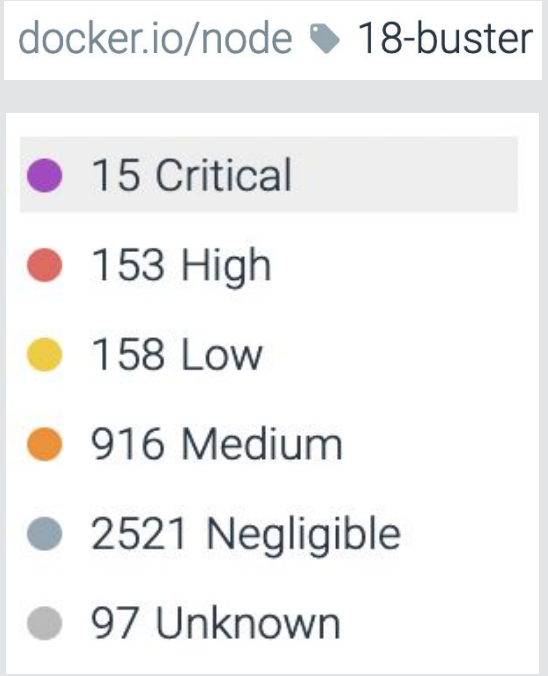


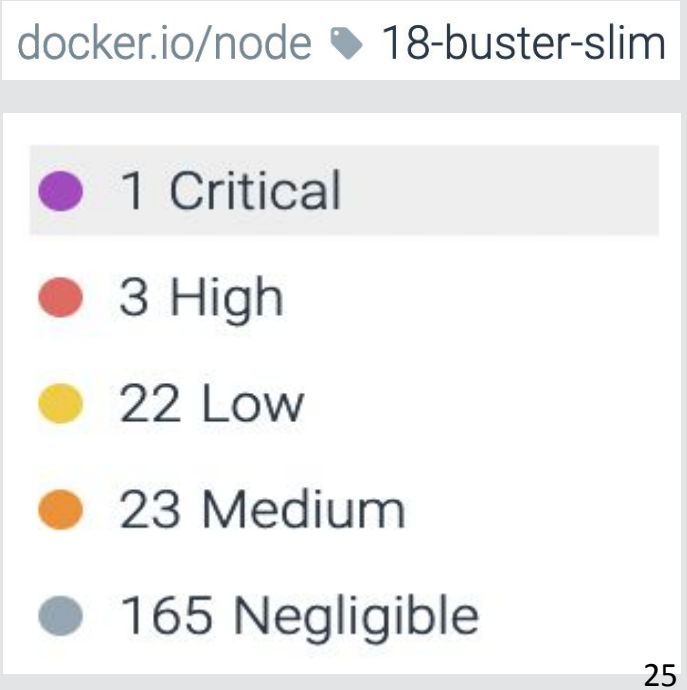
Base Image & Layer Analysis

- Use a library of base images from a trusted source

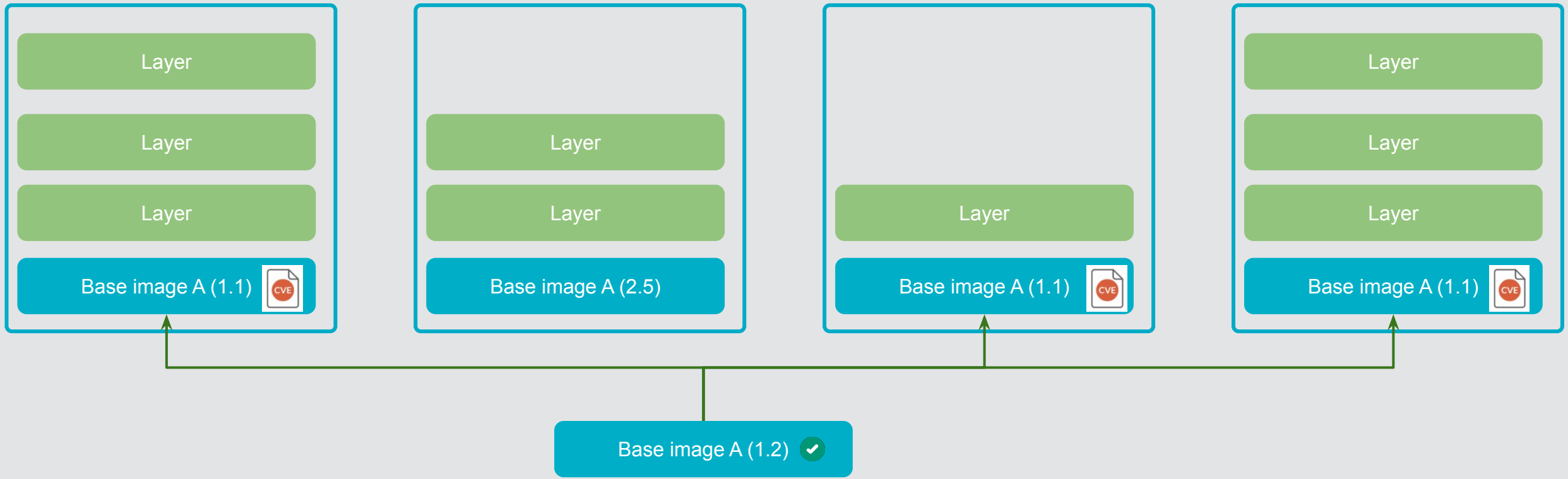
- Start with a minimal base image

Red Hat Ecosystem Catalog



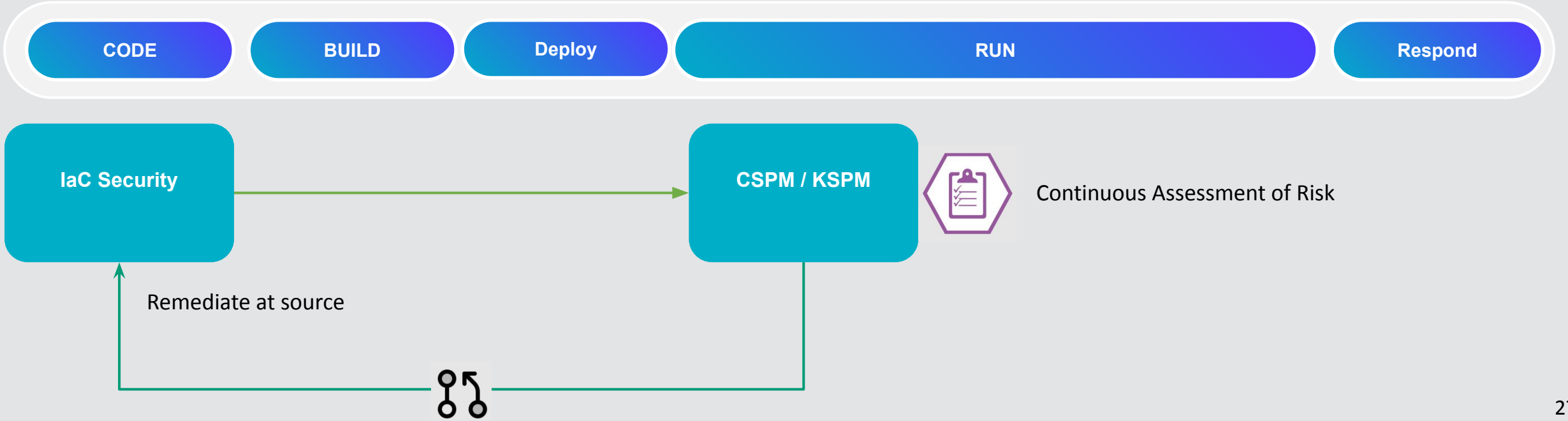


Base Image & Layer Analysis

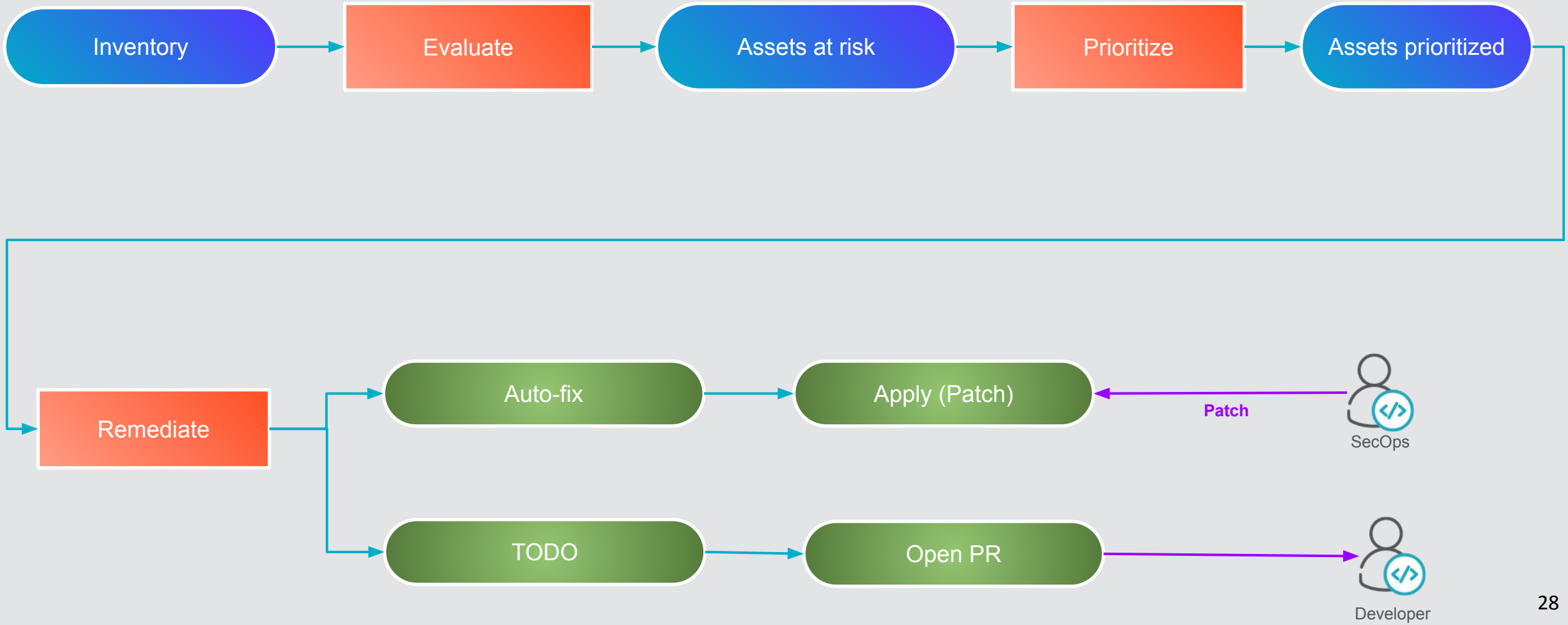


Continuous & Actionable Compliance

- Continuous CSPM: all misconfiguration are flagged, addressed in an automated and continuous way
- Configuration Drift detection and remediation



Risk Assessment and Prioritization



Personas & Workflows

Cloud Security Personas

Developer

- Build secure application
- Fix Vulnerability

Platform Engineer

- Building Platform using IaC
- Platform troubleshooting

DevOps

- Automation
- Continuous Integration
- Continuous Delivery

DevSecOps

- Automation
- Continuous Integration
- Continuous Delivery
- Vulnerability Management
- Policies implementation

Security Engineer

- Vulnerabilities Reports
- Compliance Reports
- Implement Policies

Security Architect

- Threat Modeling & Attack Surface
- Security Posture
- Define Policies

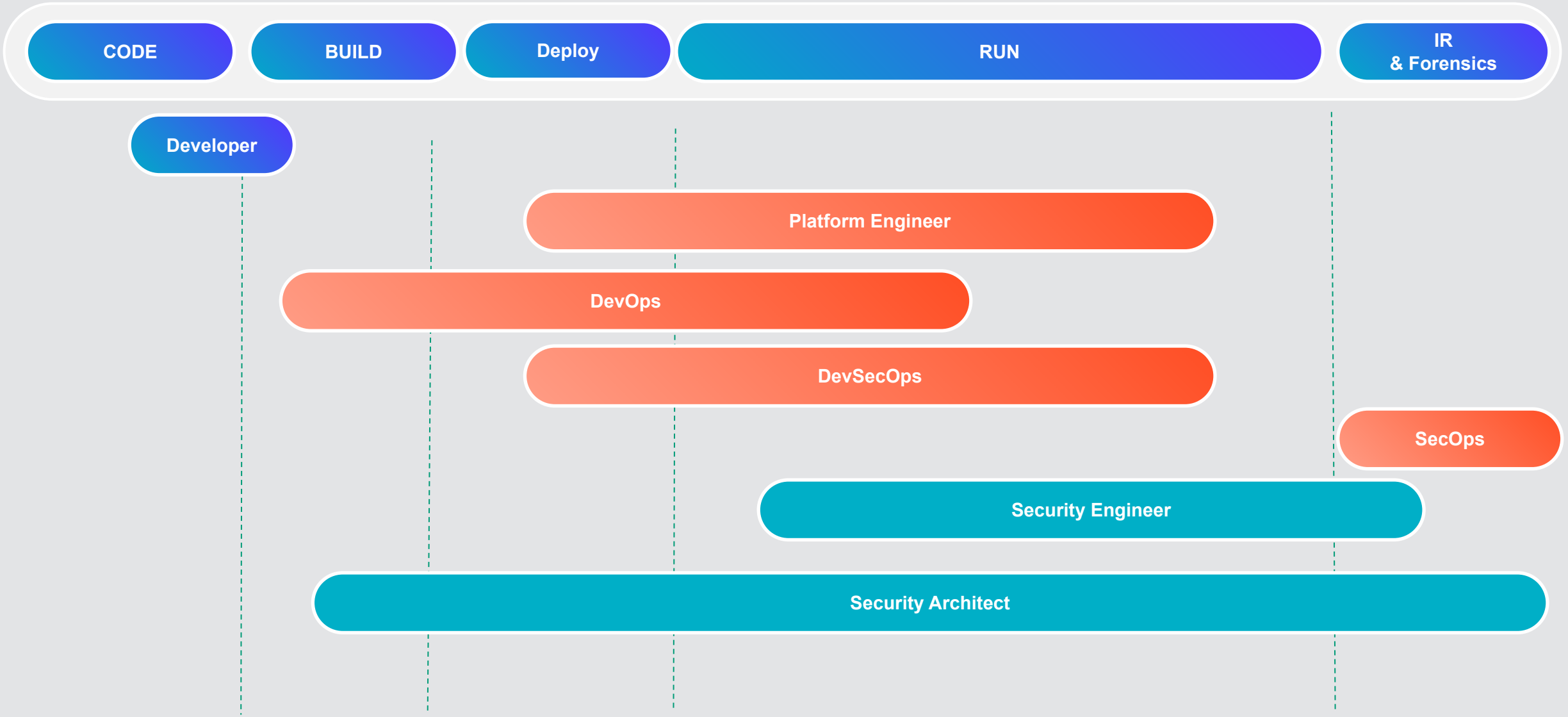
SecOps

- Threat Detection
- Forensics

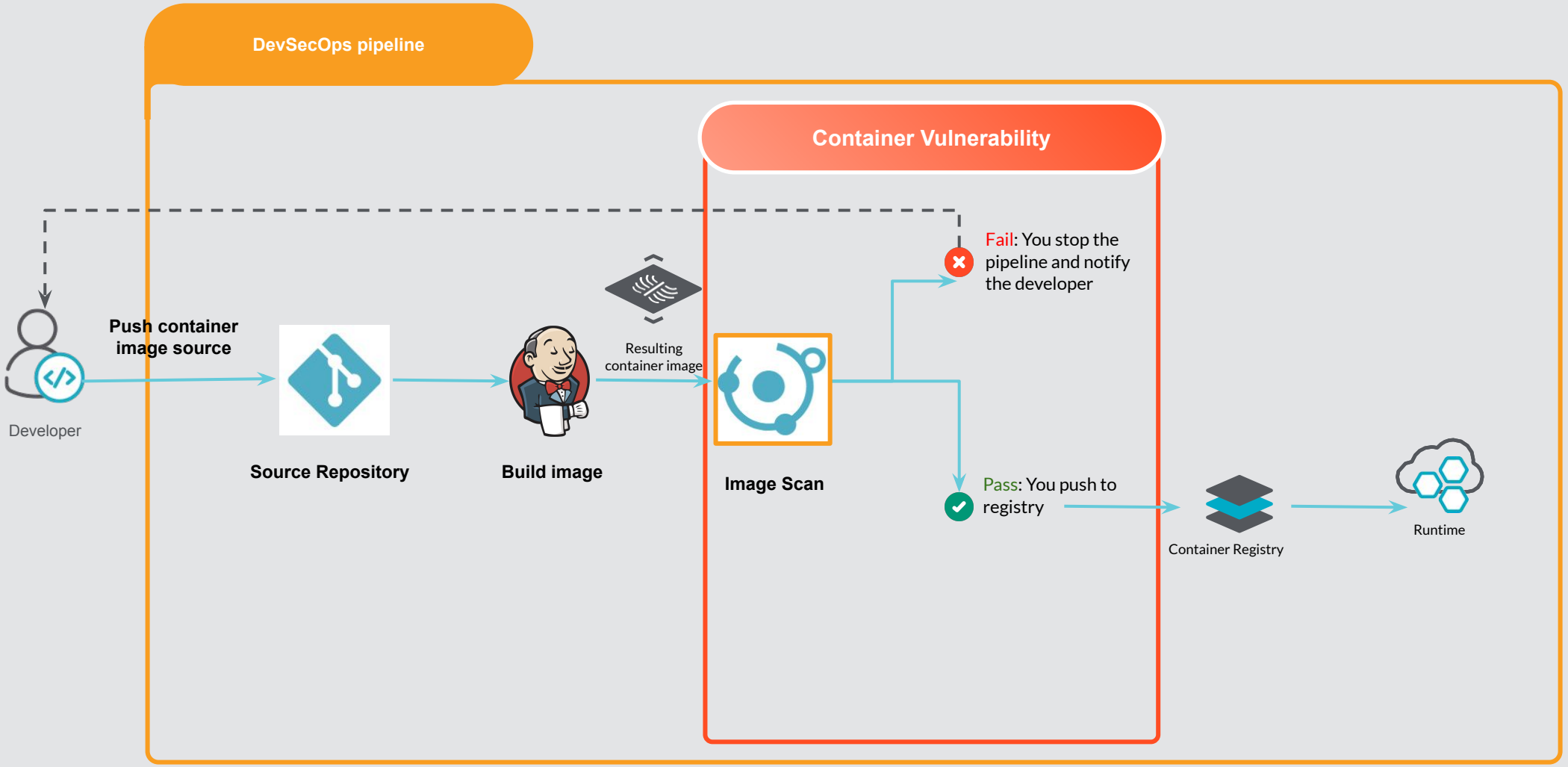
CISO

- Compliance
- Risk Governance

Cloud Security Personas

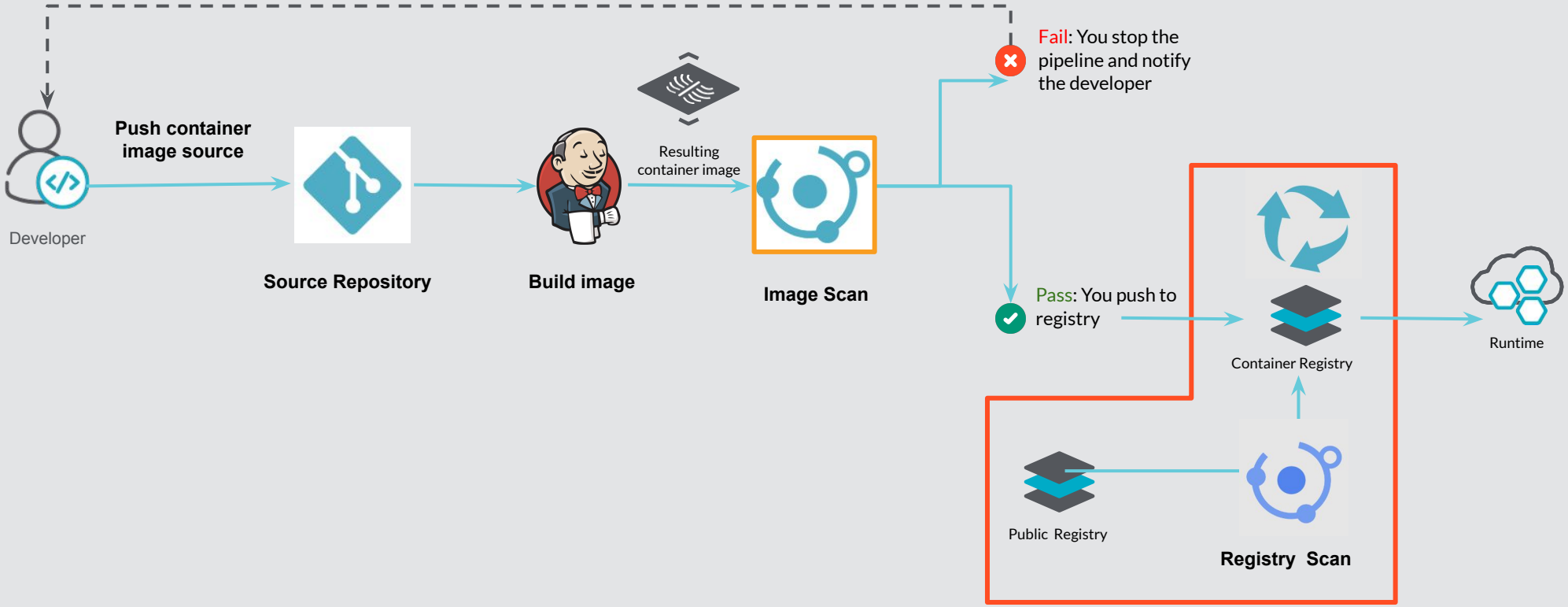


DevSecOps workflow (CI scan)

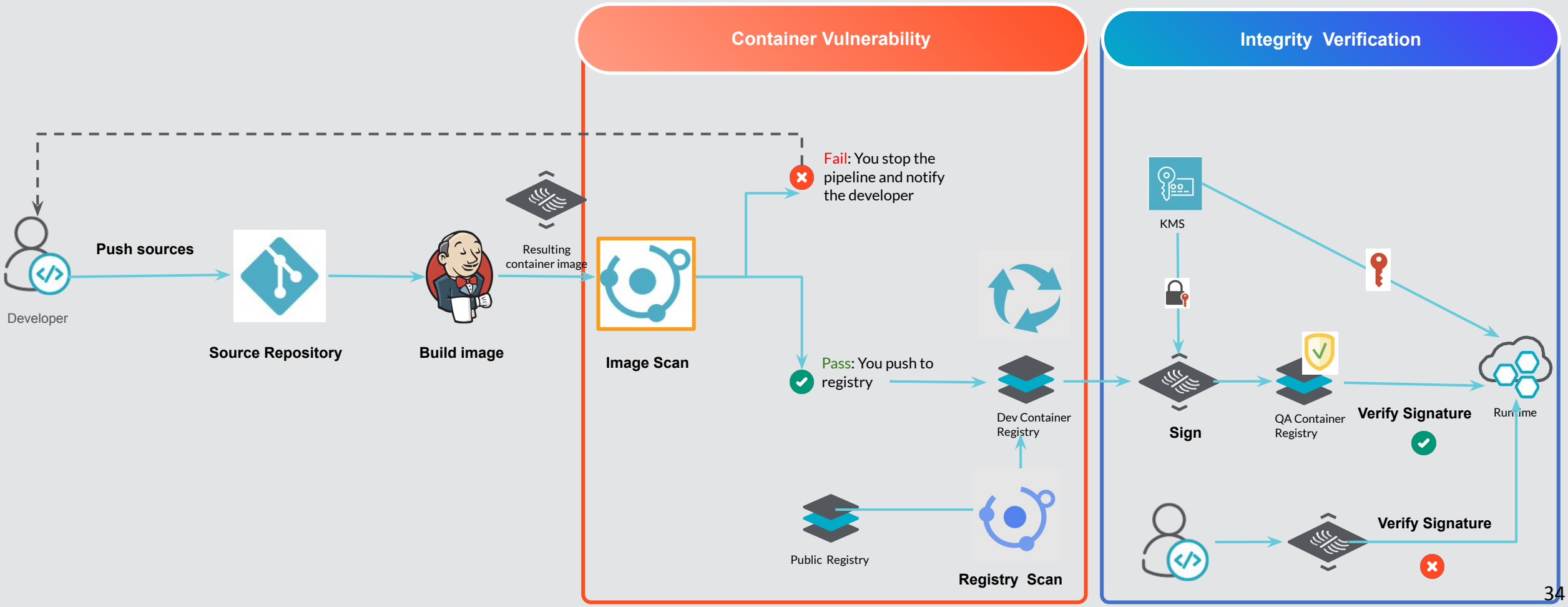


DevSecOps (Registry scan)

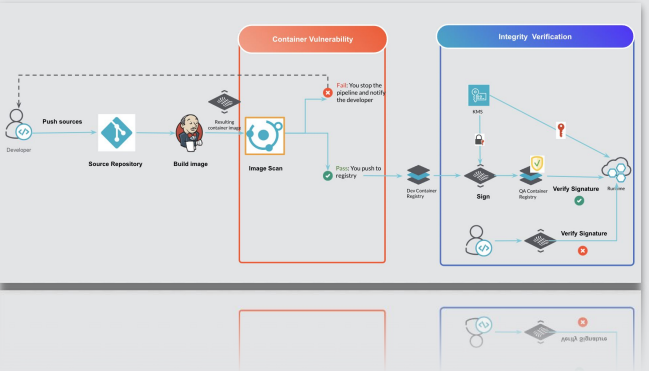
- **Risks**:
  - Skip CI pipeline
  - 0-day vulnerability in previously validated image
  - Pulling non validated image from public repository (introduce malware, cryptomining or high and critical vulnerabilities)
- **Pattern:** Continuously scan container registries.

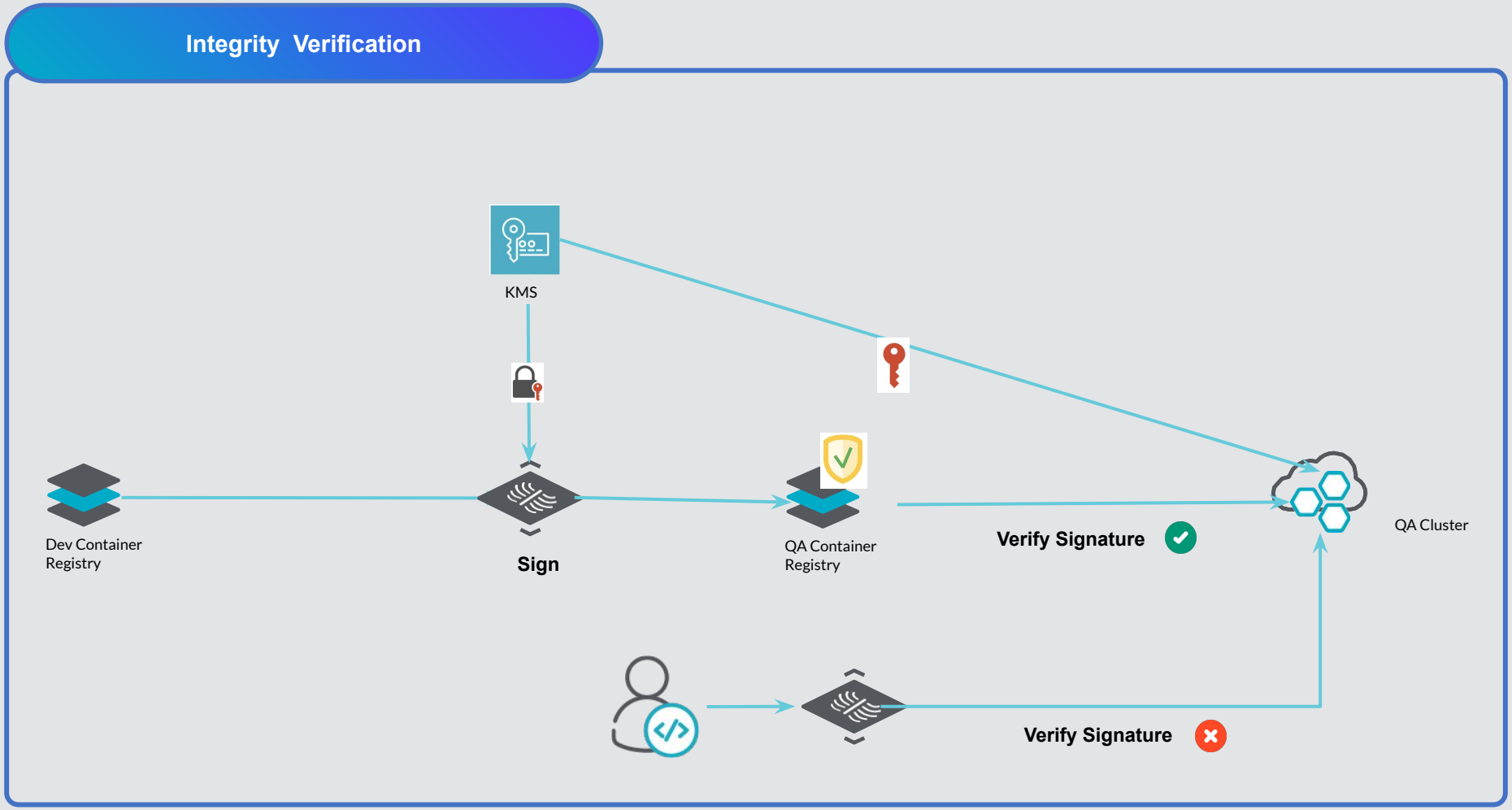


DevSecOps (workload integrity)

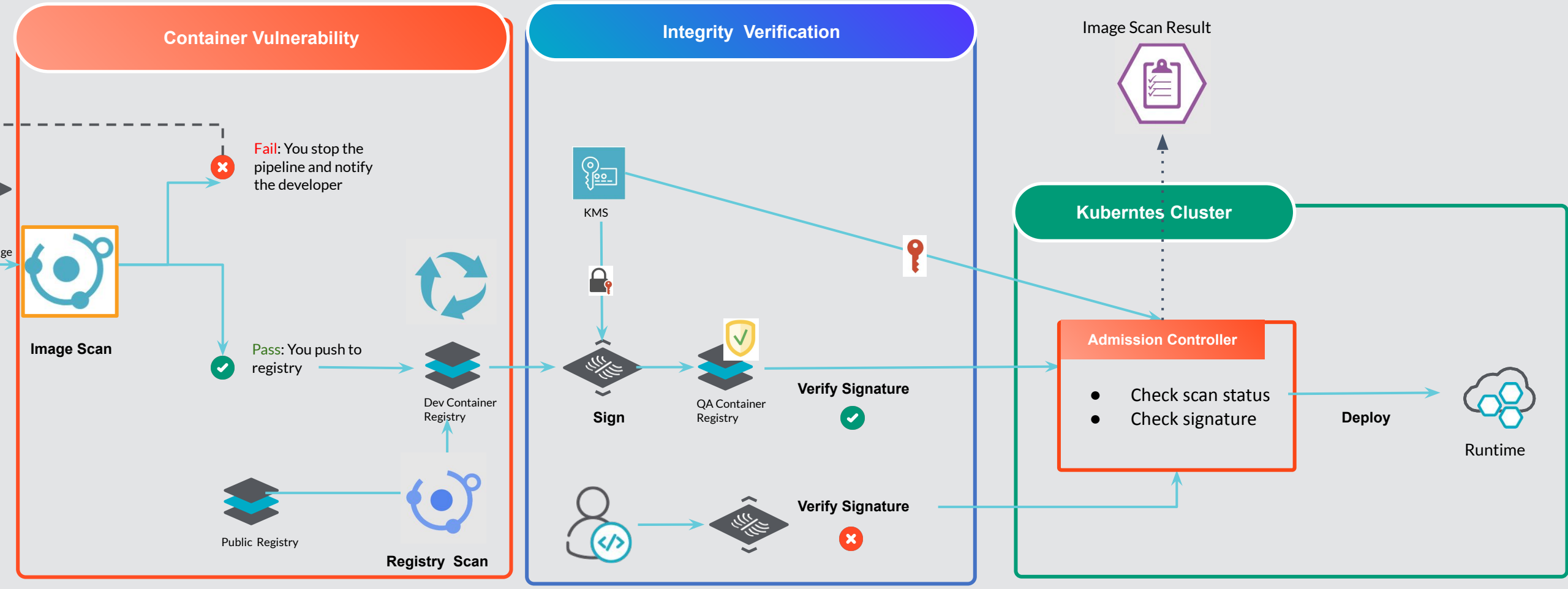


DevSecOps


Container Vulnerability
Integrity Verification
Push sources
Source Repository
Build image
Image Scan
Sign
Verify Signature
Verify Signature

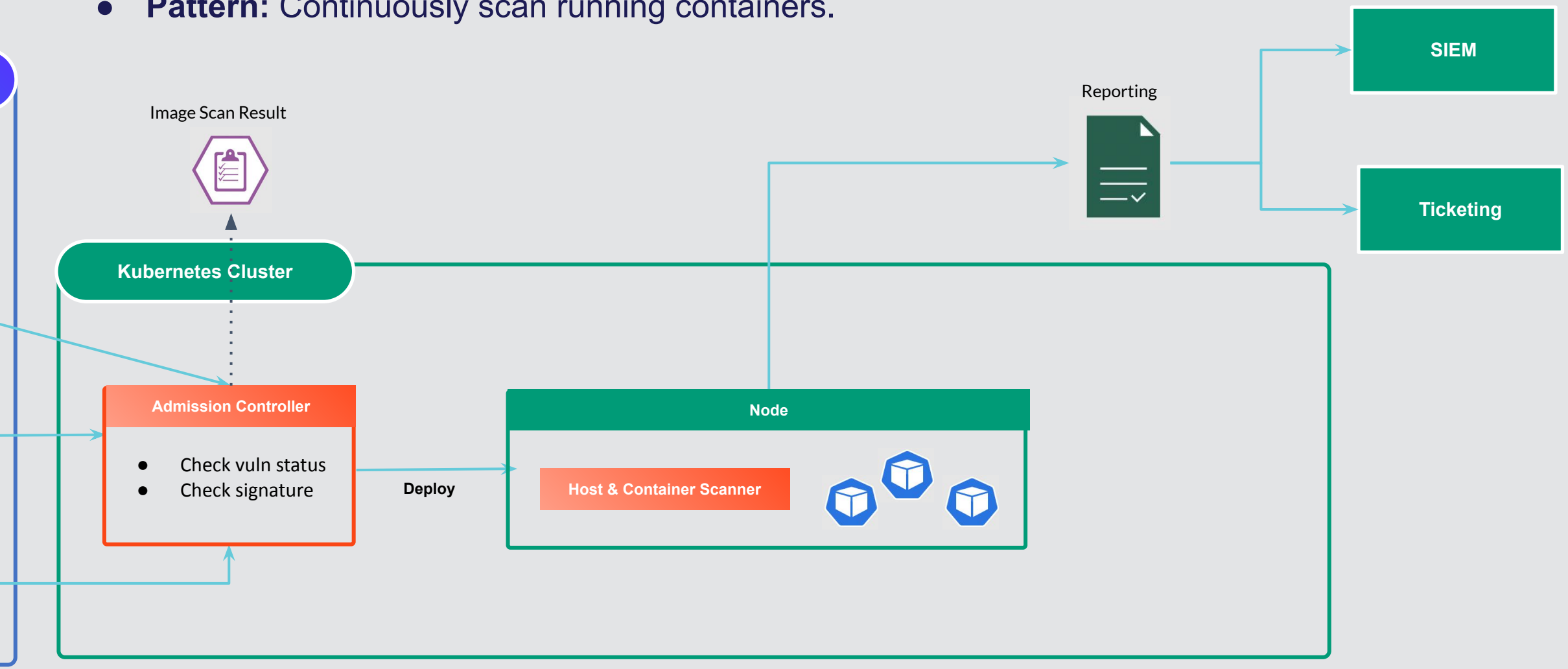

Integrity Verification
KMS
Dev Container Registry
Sign
QA Container Registry
Verify Signature
QA Cluster
Verify Signature

DevSecOps (Admission Controller)

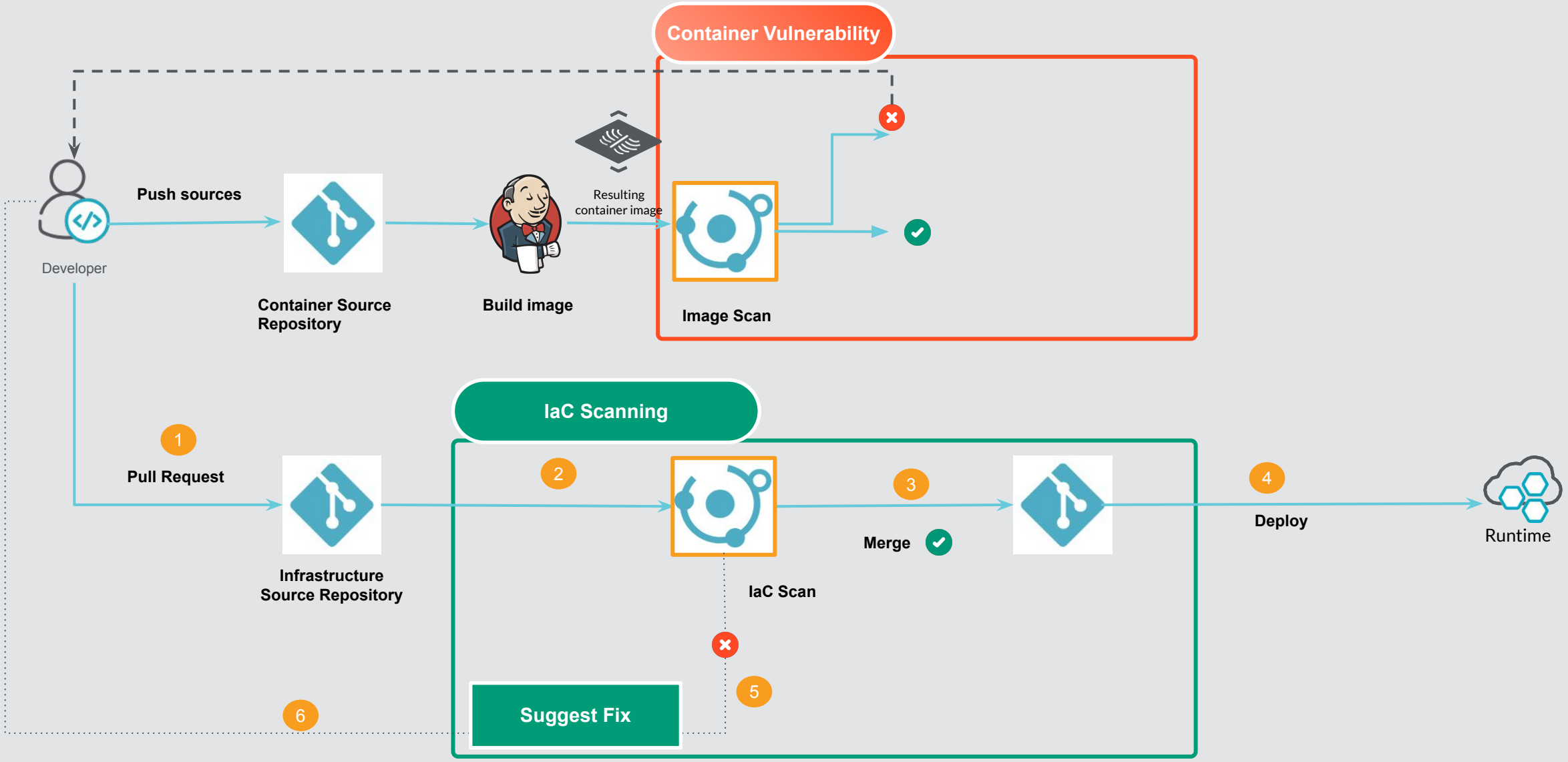


DevSecOps (Runtime scan)

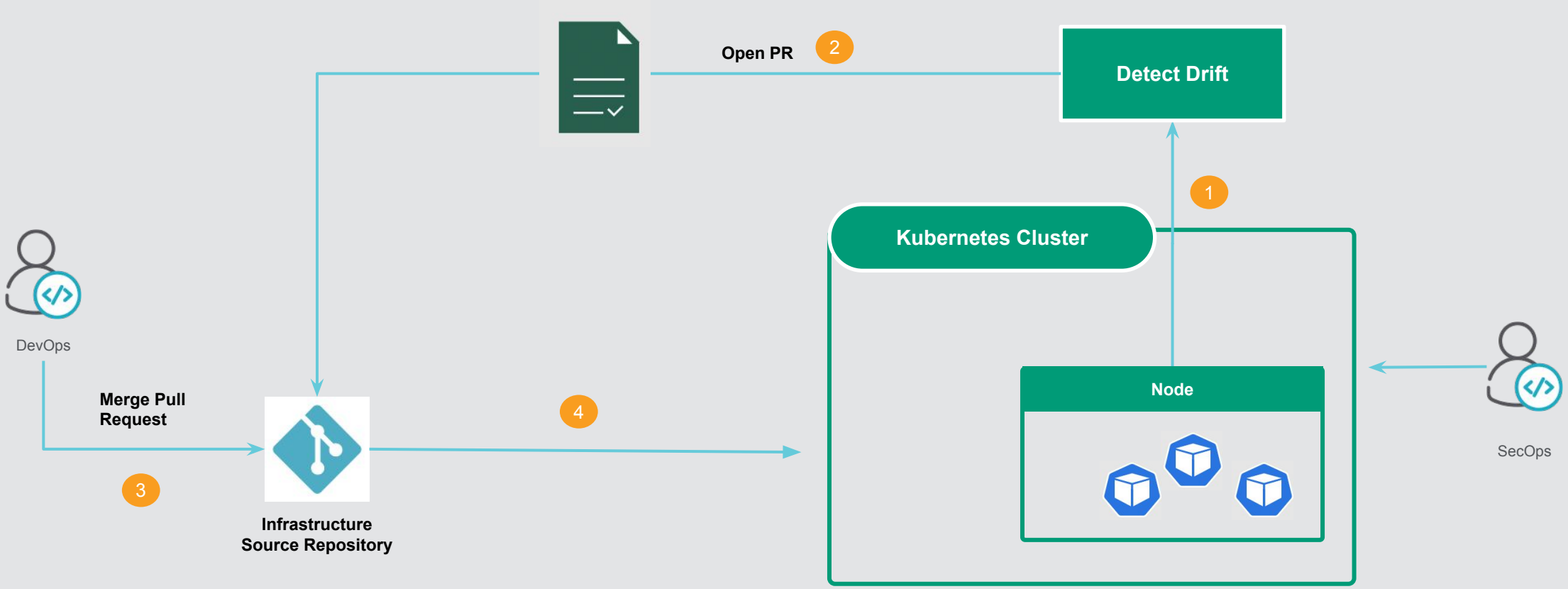
- **Risks**:
  - 0-day vulnerability in running images (Log4shell …)
- **Pattern:** Continuously scan running containers.



IaC security (build phase)



IaC security (run phase)



Takeaways

- Cloud Native security implementation is a team and collaboration matter.
- Cloud native security should be adopted gradually:
  - It depends on your cloud journey stage.
  - Always start with the most important use cases for your business.

Further reading

- CNAPP Cloud Security:
  https://sysdig.com/blog/cnapp-cloud-security-sysdig/
- Google Cloud Podcast:
  EP94 Meet Cloud Security Acronyms with Anna Belak
- Gartner:
  Innovation Insight for Cloud-Native Application Protection Platforms
- MITRE ATT&CK Matrix for Containers:
  https://attack.mitre.org/matrices/enterprise/containers/

Thank you! Any questions?

Don’t forget to rate the session and provide your feedback please 🙂


CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023