Supply chain security

Develop quickly without inviting The Nefarious

Ivan Milchev
ivan@mondoo.com

About me

mondoo

- Mondoo Kubernetes Operator
- Kubernetes, containers and Linux integration

PRODRIVE TECHNOLOGIES

- Architect of the in-house Manufacturing Execution System (MES)
- Created a Kubernetes scheduler extension for network-aware scheduling
- Developed a customized managed Kubernetes platform

Ivan Milchev
Senior Software Engineer
ivan@mondoo.com

Innovation

How did it start?

How did it start?

How did it start?

How did it start?

The Nefarious

Who are they?

Smart

Organized

Rich

Omnipotent

How do they operate?

Sales Quotas

Playbooks

Customer Support

Affiliate Programs

What do they want?

The defense line

How you think it is?

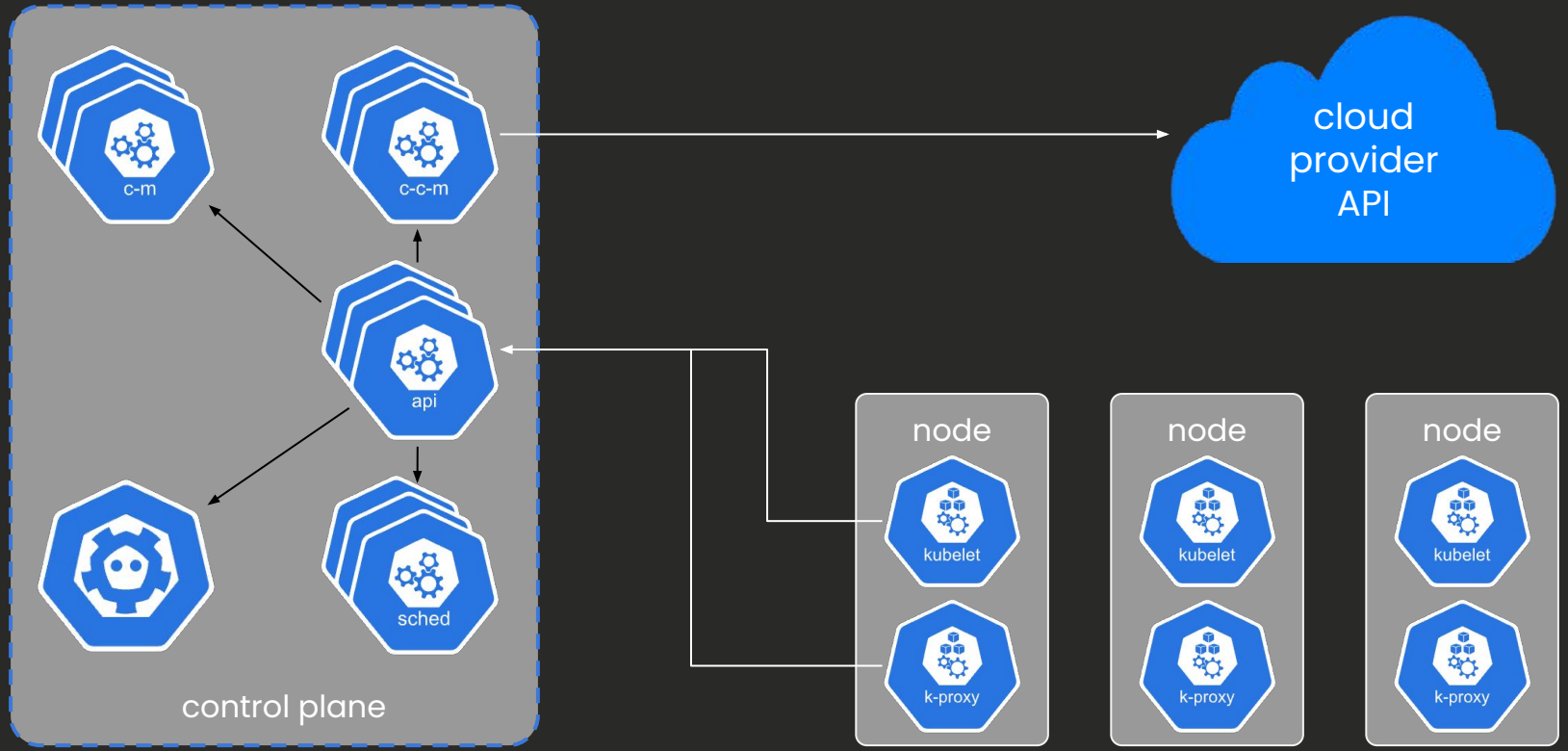
How the CTO thinks it is?

How the security engineer thinks it is?

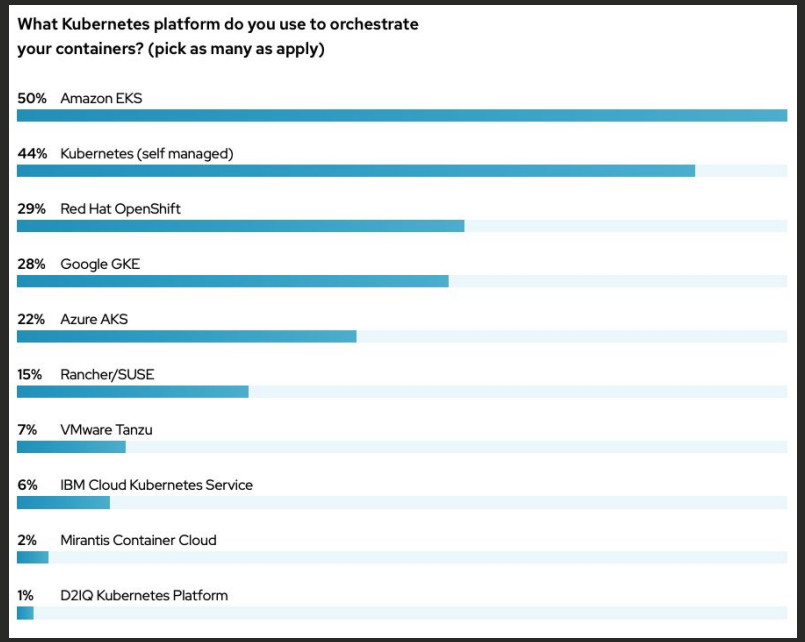
How it really is?

But seriously…

Kubernetes is complex



Businesses are choosing the cloud for K8s

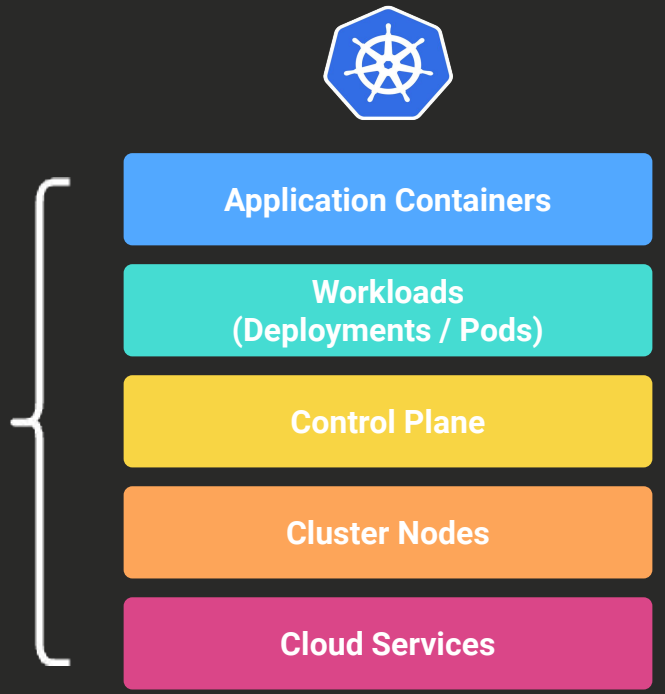


2022 RedHat State of Kubernetes Security

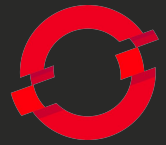
Securing Kubernetes

Security for Kubernetes runtime

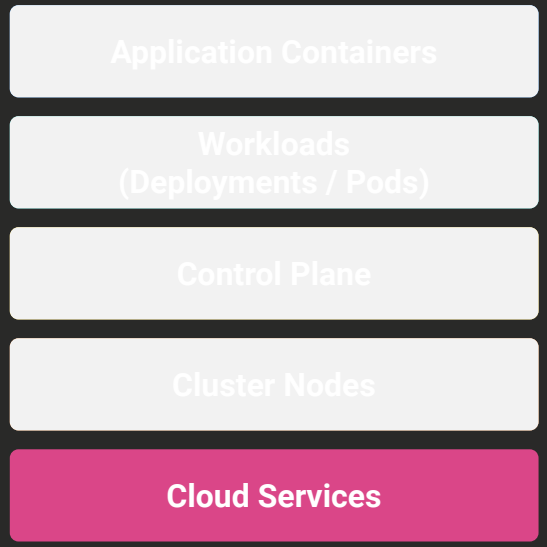
Kubernetes is a complex system requiring deep inspection across multiple layers of infrastructure and services to ensure security



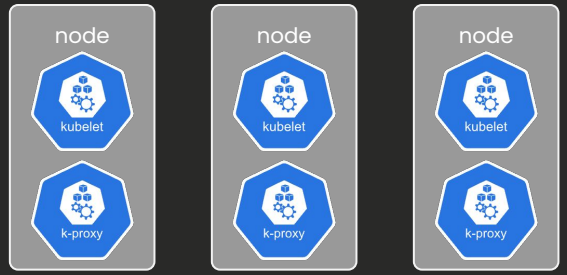
Cloud Services



- Identity and access management
- Network and compute security
- Storage security
- Encryption keys and certificates
- Logging



Cluster Nodes



Are my cluster nodes secure?

- Operating system end-of-life?
- Operating system patched?
- Operating system hardened?
- Is the container runtime hardened?
- Is the Kubelet hardened?

Application Containers

Workloads
(Deployments / Pods)

Control Plane

Cluster Nodes

Cloud Services

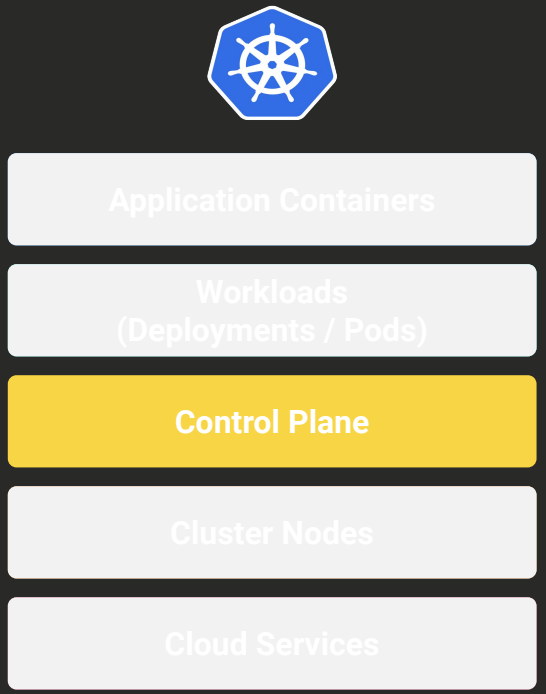
Control Plane

Is the Kubernetes API secure?

- Use TLS for all API traffic
- API authentication
- API authorization
- Audit logging

Is etcd secure?

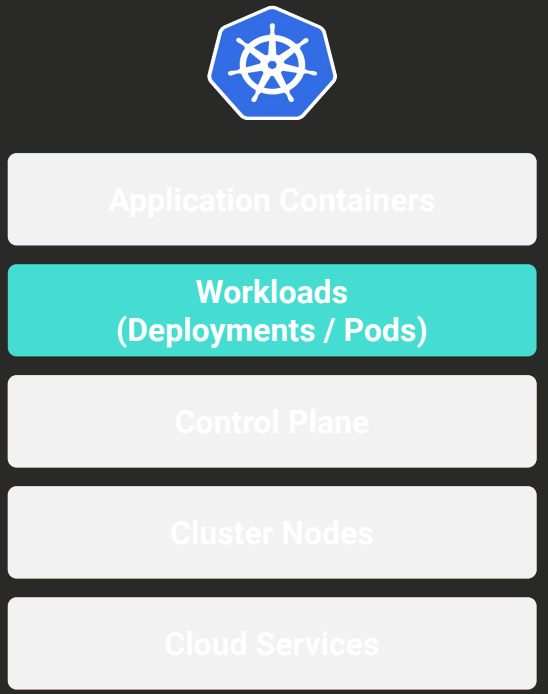
- Restrict access to etcd
- Encryption at rest



Workloads

Are the Kubernetes workloads secure?

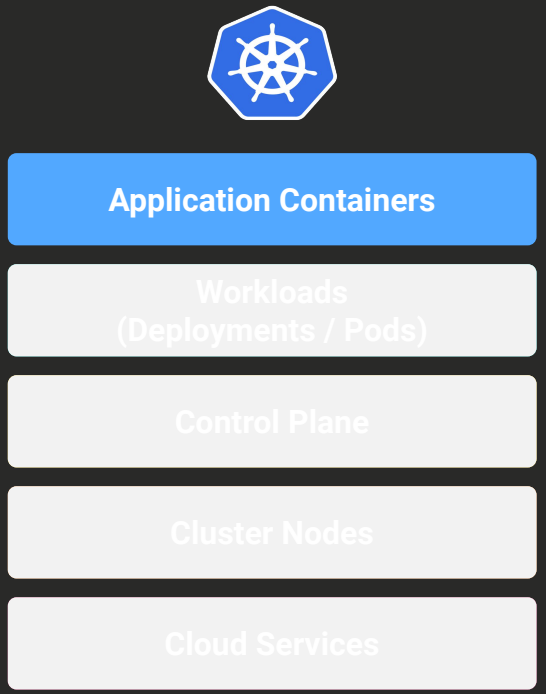
- Limiting resource usage on a cluster
- Limit privileges
- Restrict network access



Application Containers

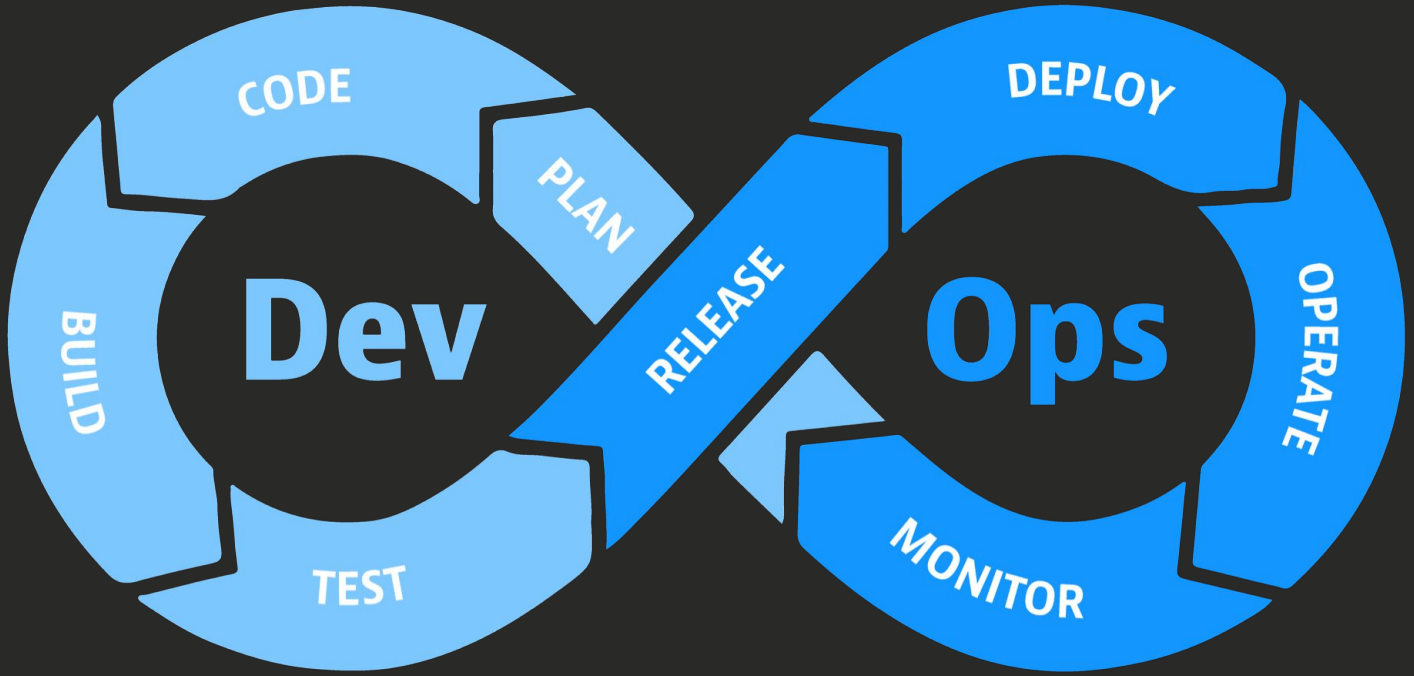
Are the containers running in Kubernetes secure?

- Container vulnerability scanning
- Provenance and attestation
- Disallow privileged users

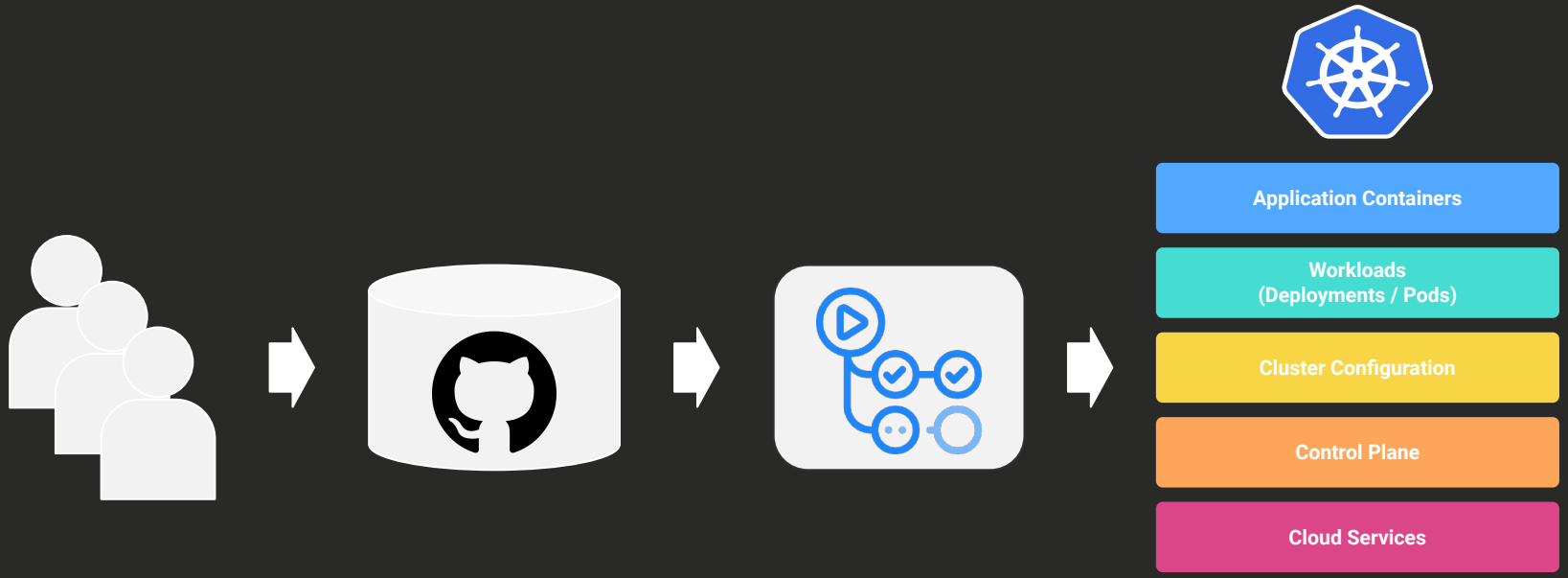


Secure Development

DevOps lifecycle

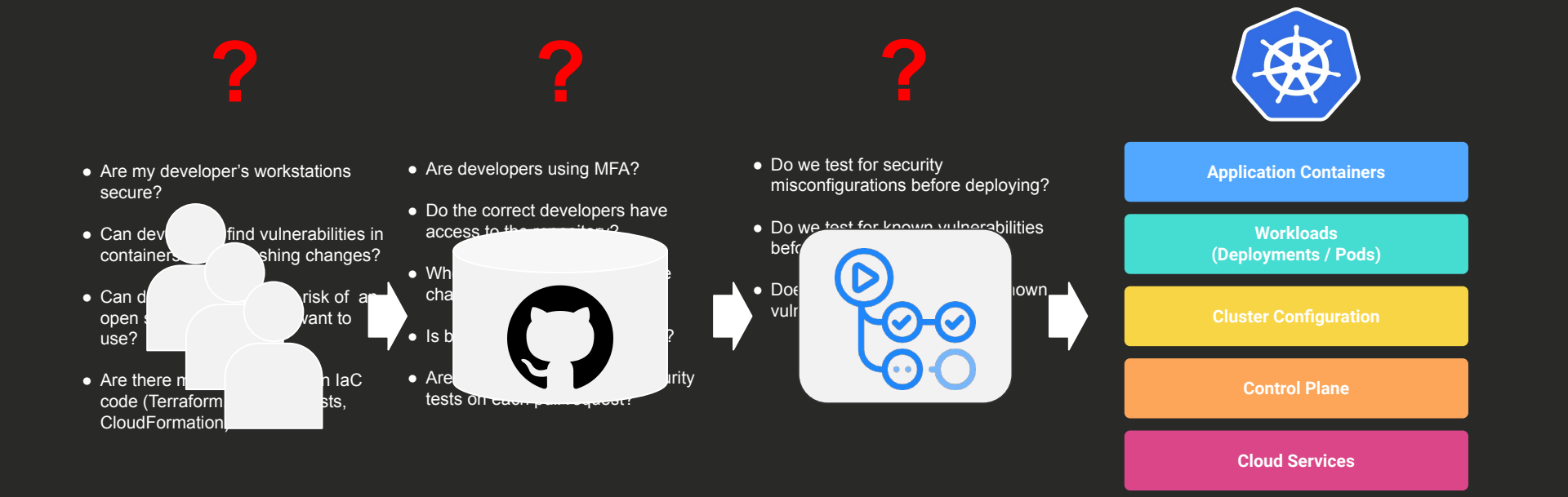


GitOps workflow



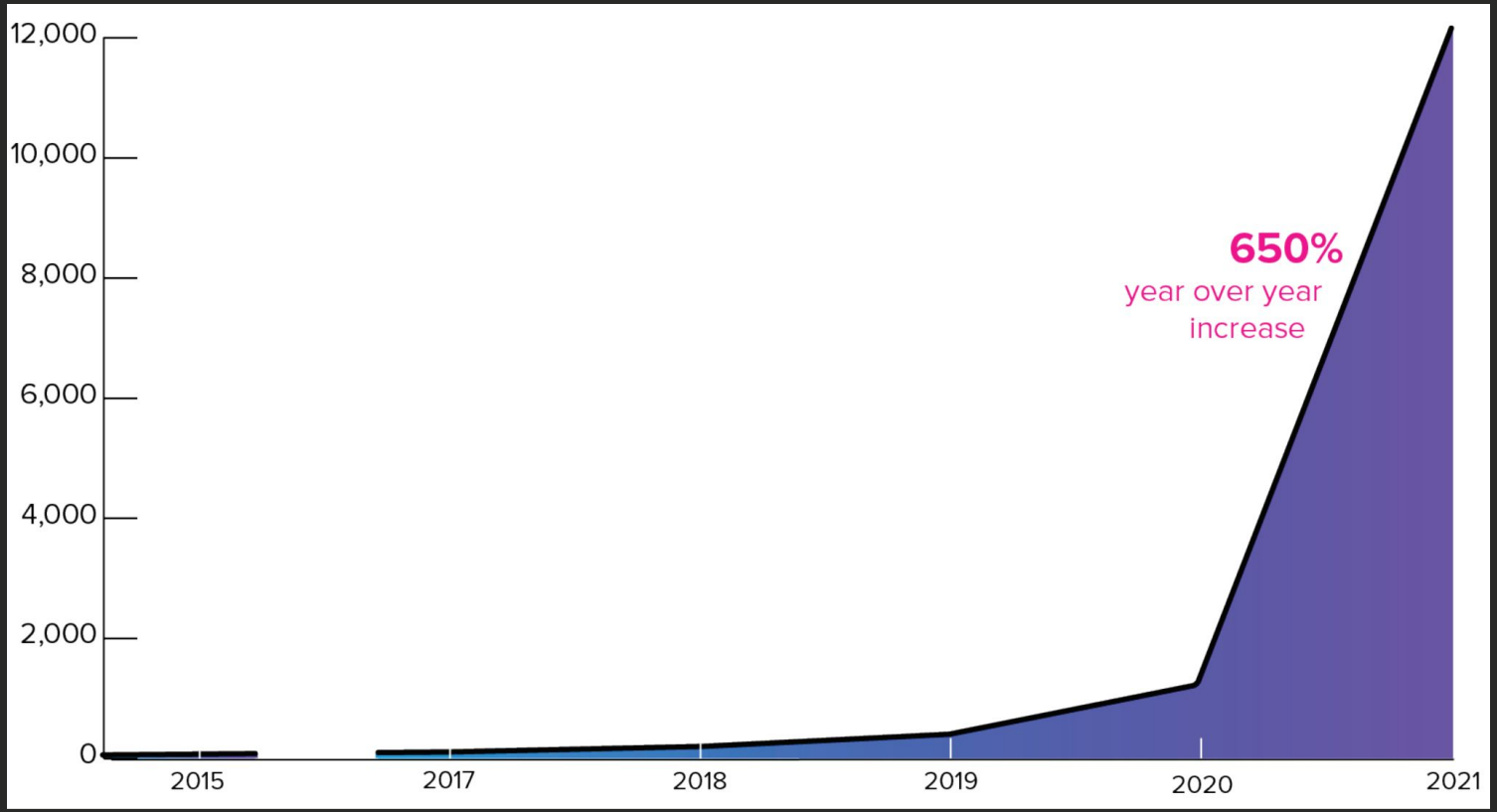
local development source control ci / cd runtime

Securing the GitOps workflow



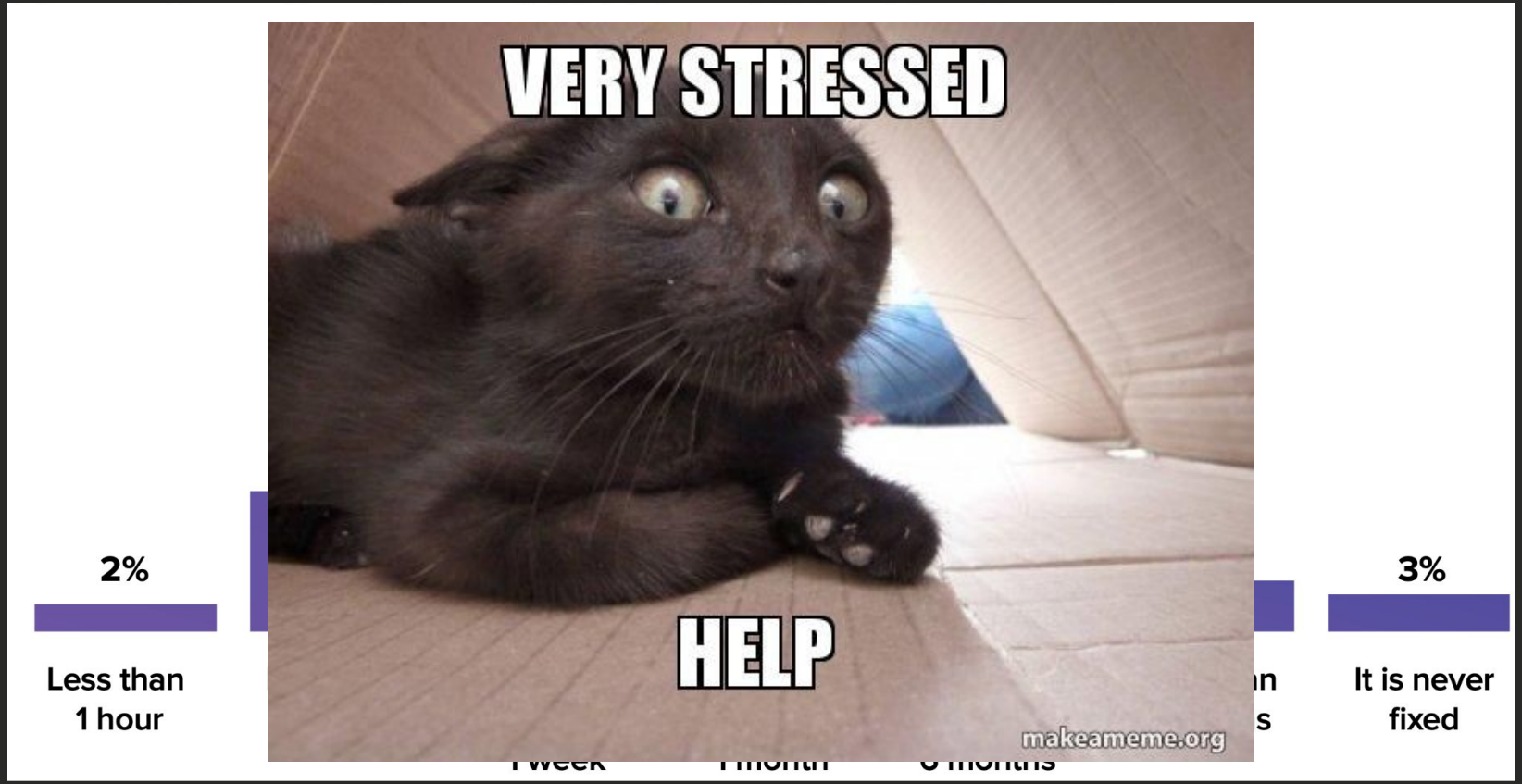
The current situation in numbers

Software supply chain attacks (2015–2021)



State of the Software Supply Chain by Sonatype - 2021

Time to remediate OSS vulnerabilities



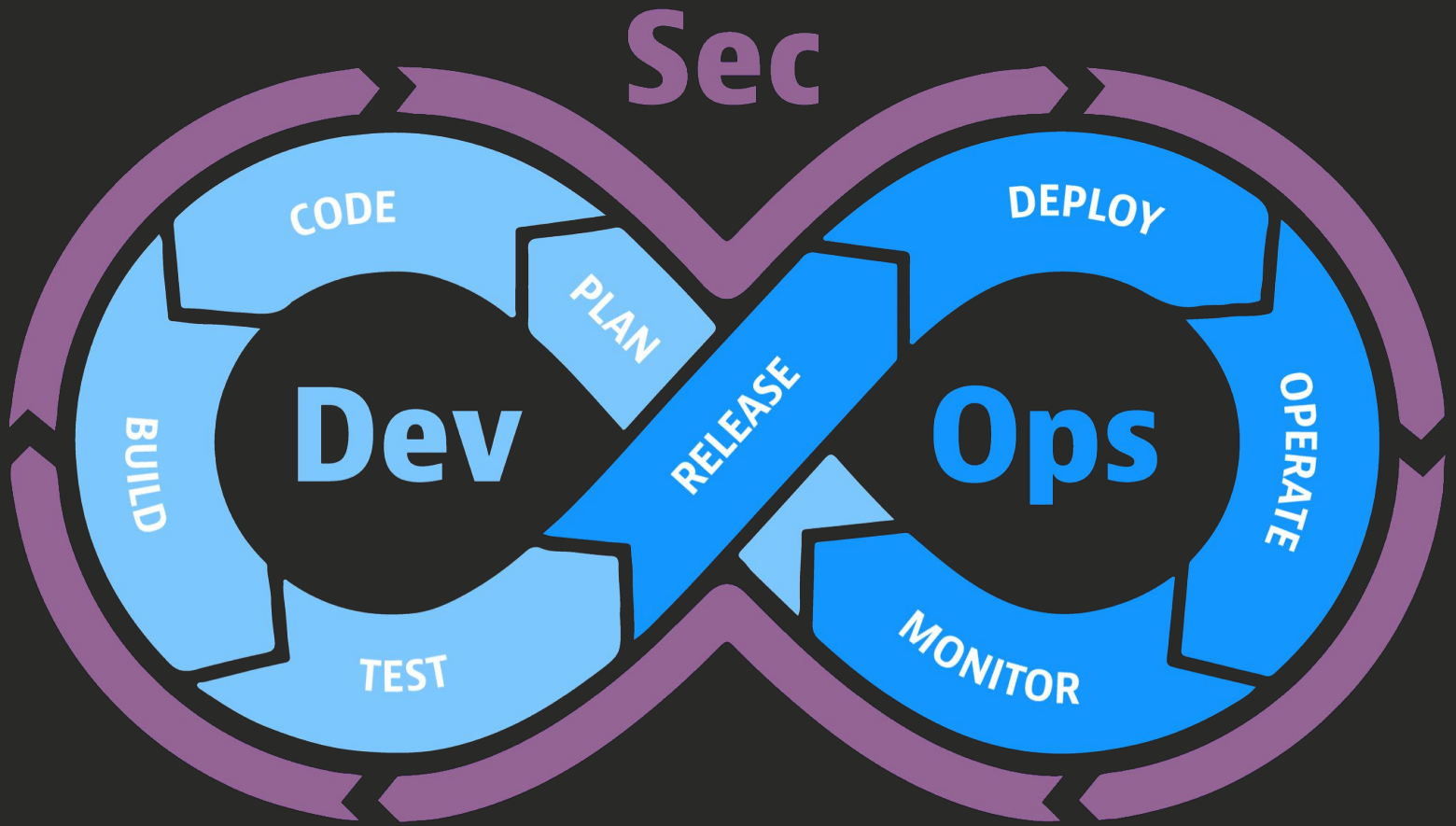
State of the Software Supply Chain by Sonatype - 2020

The solution

~~The solution~~

The improvements

DevSecOps lifecycle



Check automatically and continuously

?

- Are my developer's workstations secure?
- Can developers find vulnerabilities in containers before pushing changes?
- Can developers evaluate risk of an open source project they want to use?
- Are there misconfigurations in IaC code (Terraform, K8s manifests, CloudFormation)?

local development

?

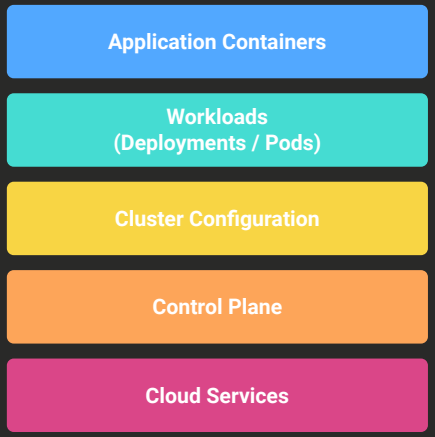
- Are developers using MFA?
- Do the correct developers have access to the repository?
- Who can review/approve/merge changes to the code base?
- Is branch protection configured?
- Are we running automated security tests on each pull request?

source control

?

- Do we test for security misconfigurations before deploying?
- Do we test for known vulnerabilities before deploying?
- Does our CI/CD tooling have known vulnerabilities?

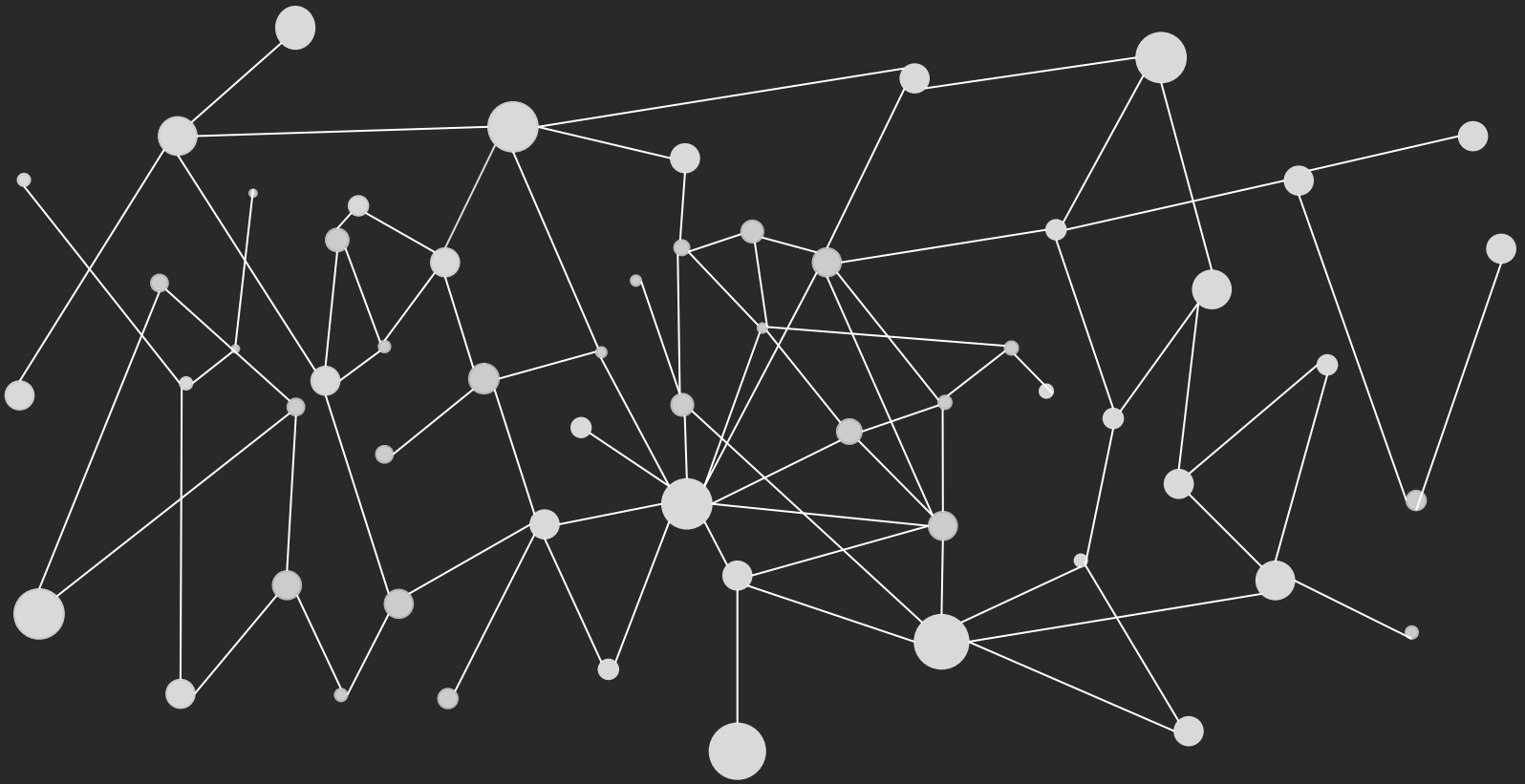
ci / cd



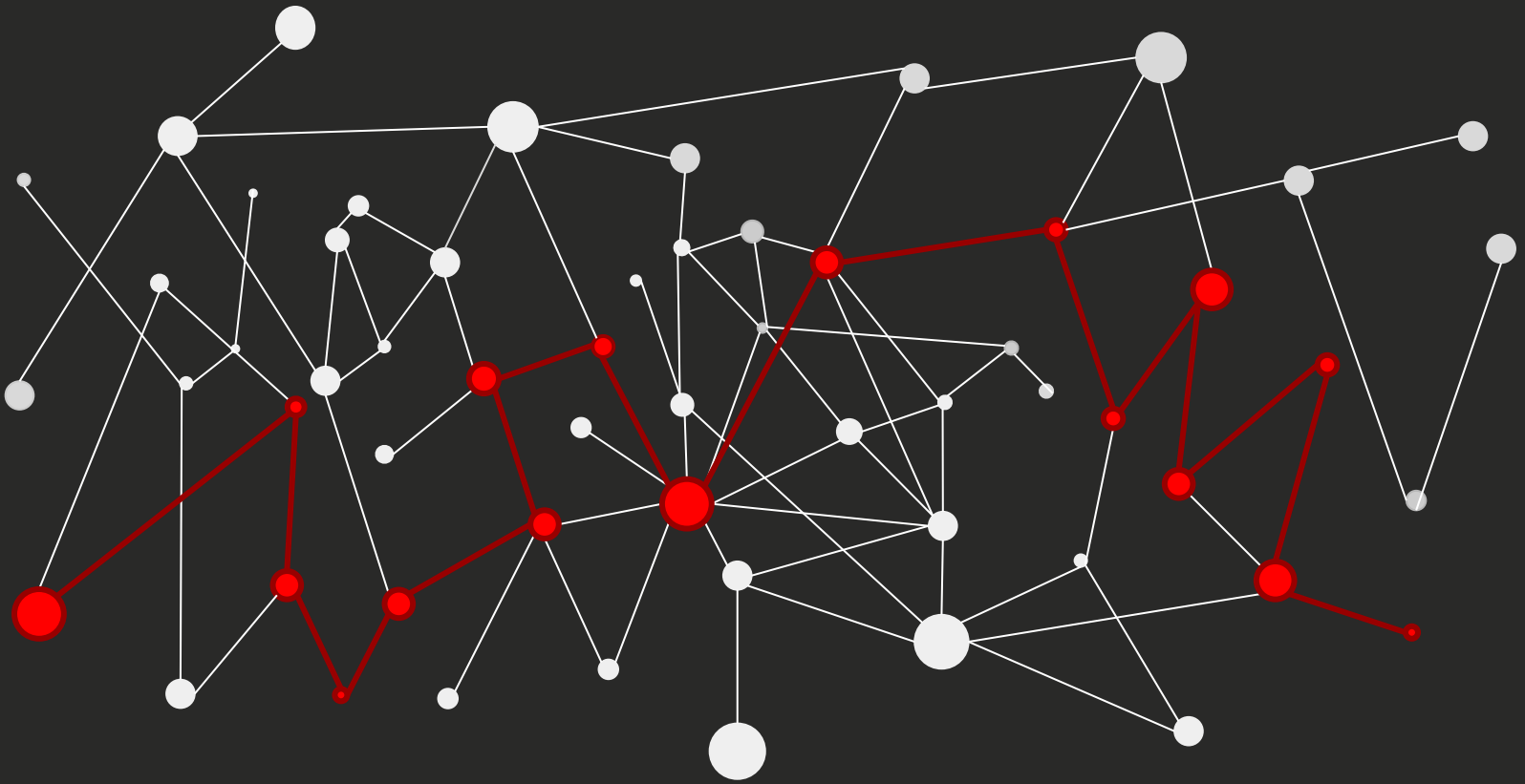
runtime

Conclusion

Security is complicated

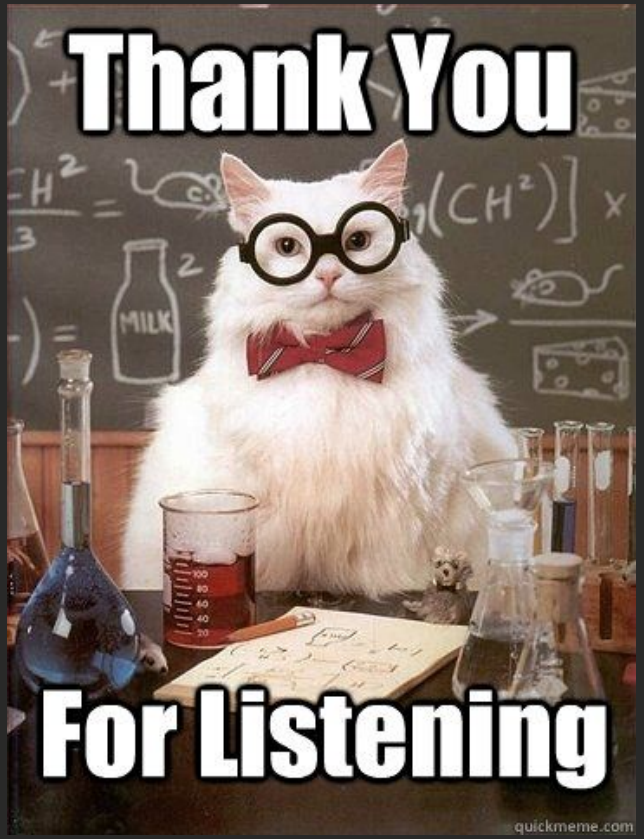


Security is complicated



Security is a shared responsibility

Validate everything


Thank You
For Listening
MILK
quickmeme.com