云原生产业大会 2021 CLOUD NATIVE INDUSTRY CONFERENCE 2021/05/26 × 中国 / 北京 原生蓄力 云领未来

云原生安全理念、风险与快速实践路径

张嵩　青藤云安全技术副总裁

CAICT 中国信通院　青藤云安全

云原生安全挑战

云原生代表了一系列新技术，包括容器编排、微服务架构、不可变基础设施、声明式API、基础设施即代码、持续交付/持续集成、DevOps等，且各类技术间紧密关联。

- **技术挑战**

云原生引入了大量基础设施新技术，导致安全工作者理解难度增加， 云越来越像个黑盒，过去的安全工作多数只是围着核心业务外围转

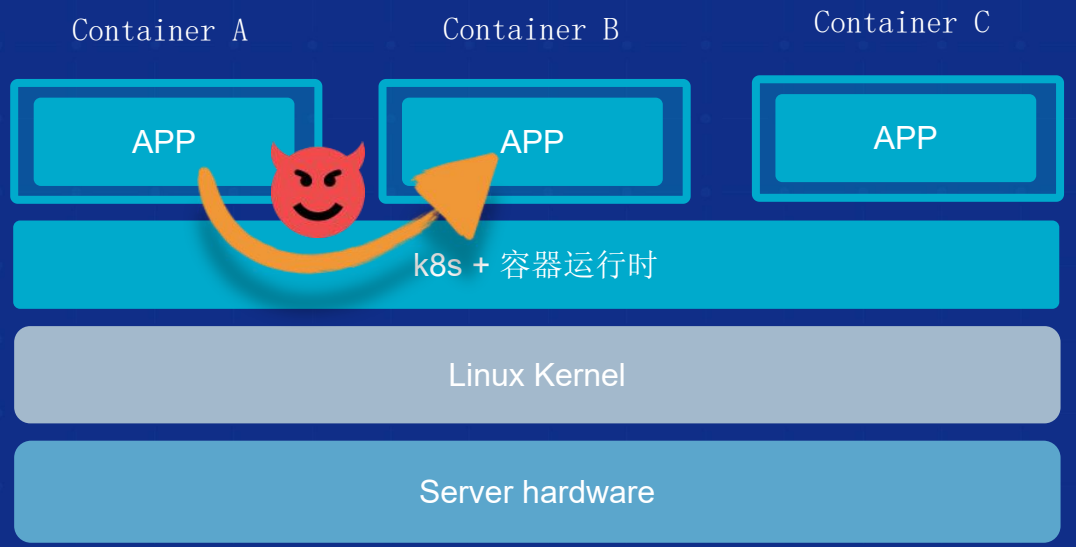
- 组织挑战

安全建设和云基础设施关系紧密，导致安全职责需要重新考虑，安全组织和信息化其他组织的关系无法简单定义为谁主管、谁建设、谁负责

云原生安全风险-容器逃逸

青藤云安全

容器的「逃逸问题」，直接影响到了承载容器的底层基础设施的保密性、完整性和可用性。



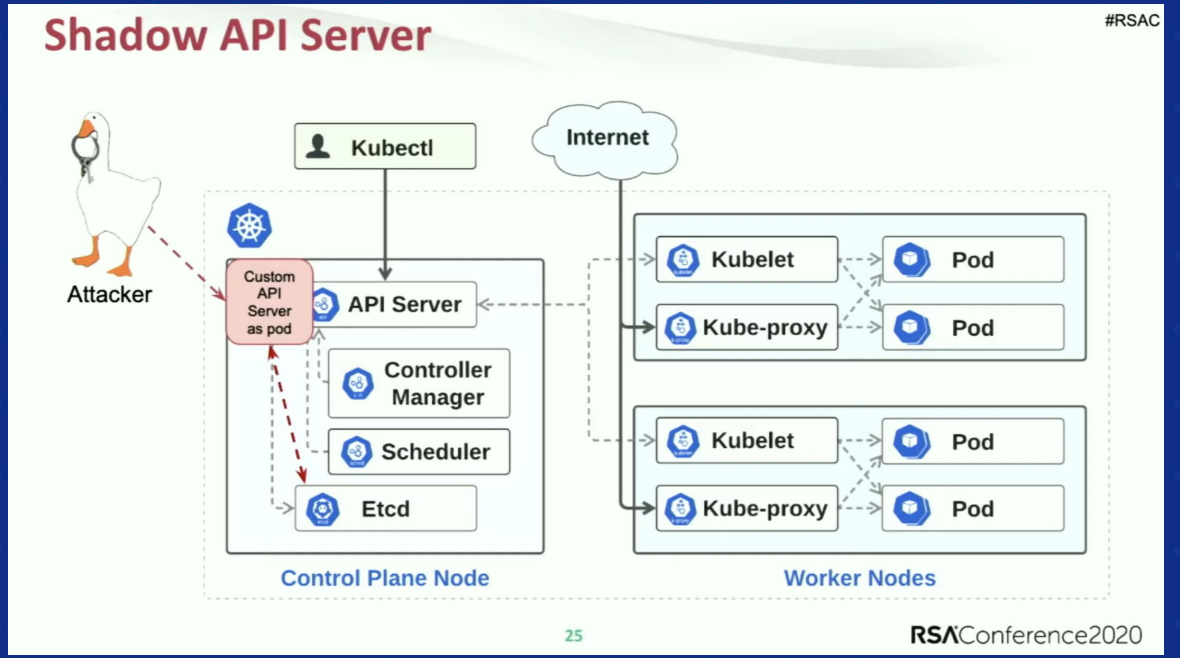
用户层：用户配置不当导致逃逸。如：开启特权容器、不安全的目录挂载、敏感的权限

服务层：Docker 、k8s自身的漏洞/不安全配置导致的逃逸，如CVE-2019-5736 runC漏洞导致容器逃逸

系统层：漏洞导致的逃逸，如 “脏牛” 漏洞-CVE-2016-5195

云原生安全风险-编排风险

由于编排环境中组件的漏洞、不安全配置、不恰当的授权等问题，导致编排环境中存在可被利用薄弱点。



研究人员在 “RSAC 2020: Advanced Persistence Threats: The Future of Kubernetes Attacks” 提出一种针对K8s集群的隐蔽持续控制通道。

1. 拿到了master node的create pod权限的前提之下，
2. 创建一个具有API Server功能的Pod
3. 后续命令通过新的“shadow api server”下发。新的api server创建时可以开放更大权限，并放弃采集审计日志，且不影响原有api-server功能，日志不会被原有api-server记录，从而达到隐蔽性和持久控制目的。

云原生安全风险-容器风险

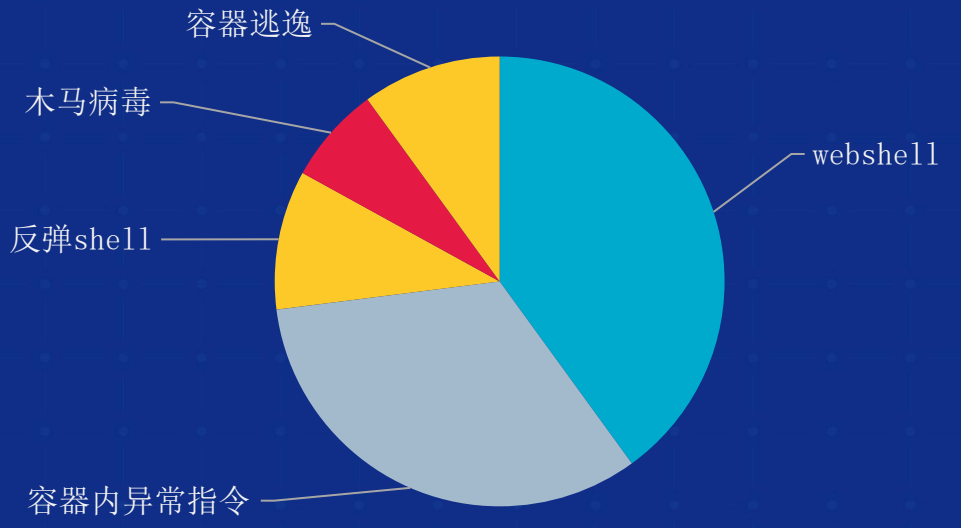
青藤云安全

在2021年攻防对抗中，青藤发现来自容器中的攻击数据如下。

30
覆盖客户

5w+
发现风险镜像

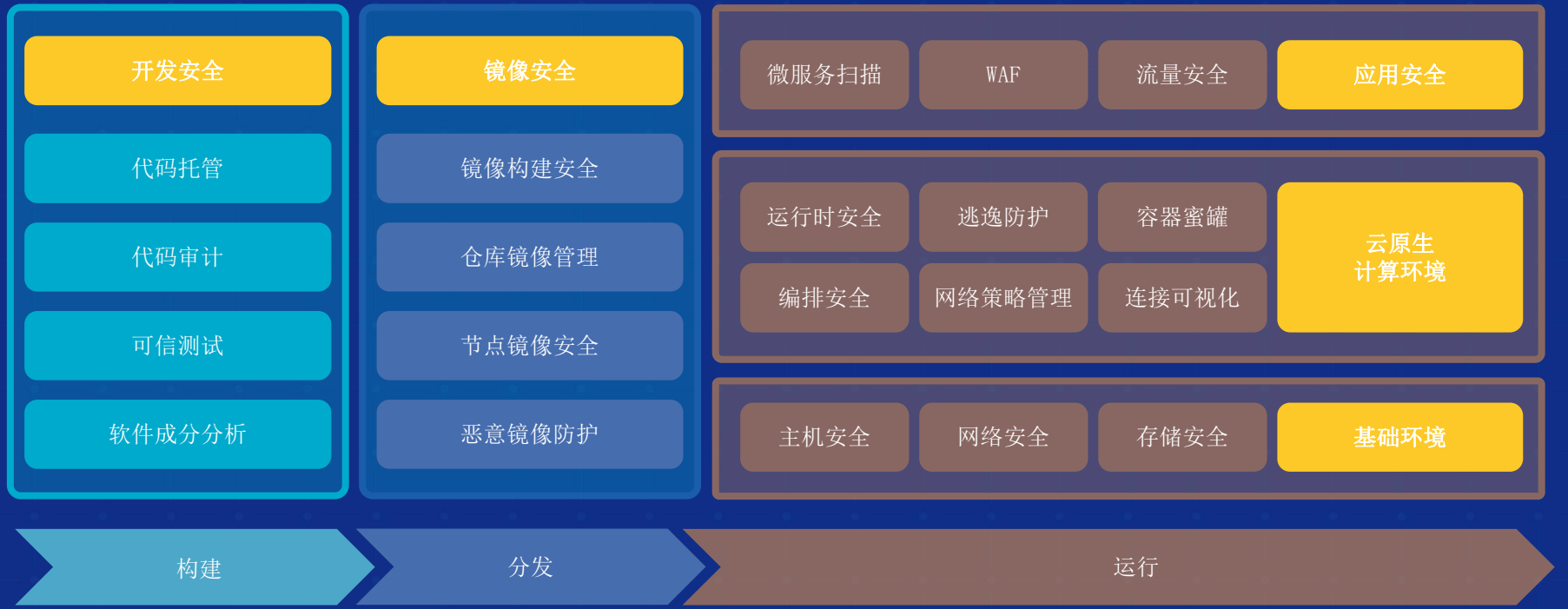
100+
发现红队攻击



2021年重保容器内事件分布

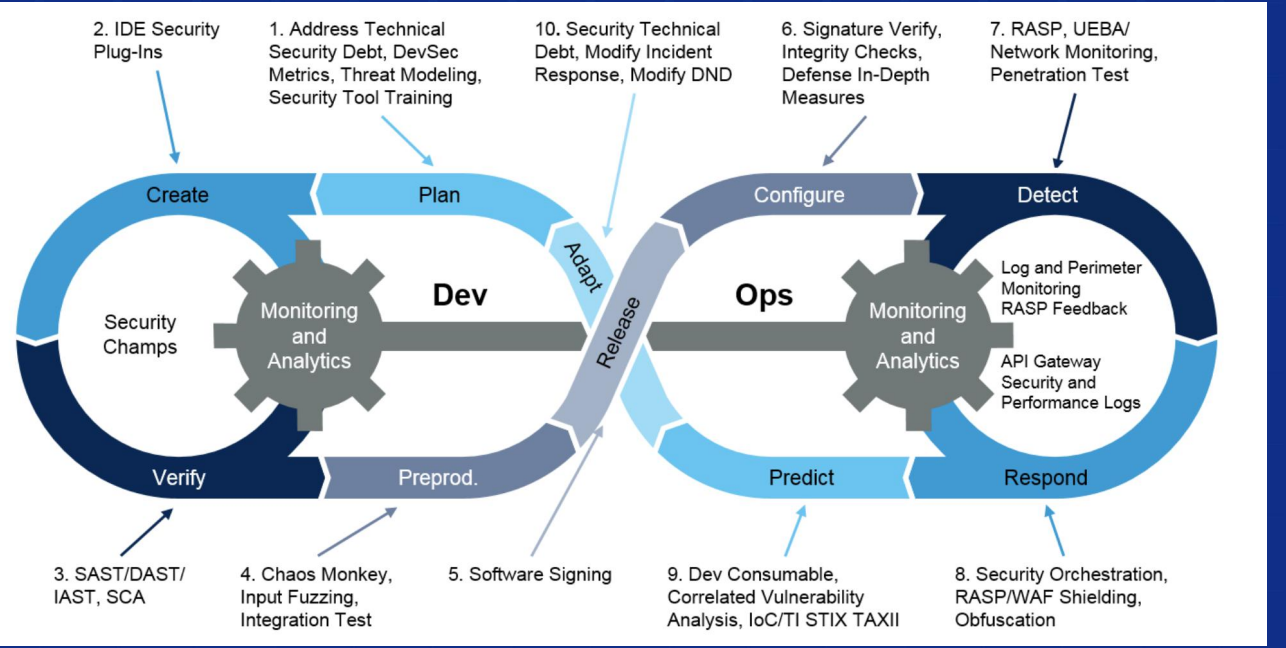
云原生安全框架

青藤云安全



云原生安全理念-DevSecOps

DevSecOps是将安全性尽可能无缝和透明地集成到敏捷IT和DevOps开发中。理想情况下，这样做不会降低开发人员的敏捷性或速度，也不会要求他们退出开发工具链环境，目的是为了实现安全地快速生产。



Gartner DevSecOps安全开发工具链模型

云原生安全理念 - 建设原生安全性

旨在依托云原生平台，建设更完善的云原生安全框架。

合理使用云原生平台提供的安全能力

- 权限管理
- 安全配置
- 网络隔离策略
- ….

深入与云原生环境集成

- 镜像安全深入集成到构建流水线中
- 与云原生各类工具、组件集成，如service mesh、镜像仓库、容器运行时等。

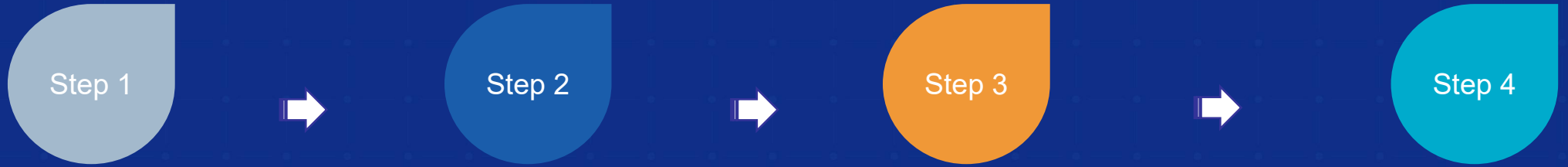
补齐云原生平台缺失的安全能力

- 容器运行时监控
- 镜像阻断
- 开发安全

企业在构建容器云平台时，安全的快速实践路径是怎样的？

云原生安全快速实践路径

面临新技术带来的新安全风险，云原生安全快速实践路径如下。



建设平台基础设施安全&平台网络安全

集群环境安全加固

与DevOps进行集成，全流程监控应用本身的安全问题

构建全景资产视图，进行持续监控与响应，实现集群风险可见、可控。

Step1：建设平台基础设施安全

容器平台上线之前，需对节点进行加固，并做好网络边界的划分。

网络安全

- 构建基础的网络边界，如平台与公网的边界、物理网络与云主机的网络边界等。
- 搭载流量检测产品，实时检测流量层的入侵行为

节点安全

- 不安装没有必要的软件包，减少可被攻击面
- 制作Golden image，尽可能确保节点操作系统的统一化、标准化
- 上线前对节点进行加固。使用风险扫描工具对节点上的漏洞、弱口令等脆弱点进行加固
- 在主机层安装HIDS，实时检测主机层的入侵行为

存储安全

- 存储产品需要具备充分的备份和数据恢复能力
- 需具备存储加密和数据传输加密能力

Step2：集群环境安全加固

1） 合理划分集群应用权限

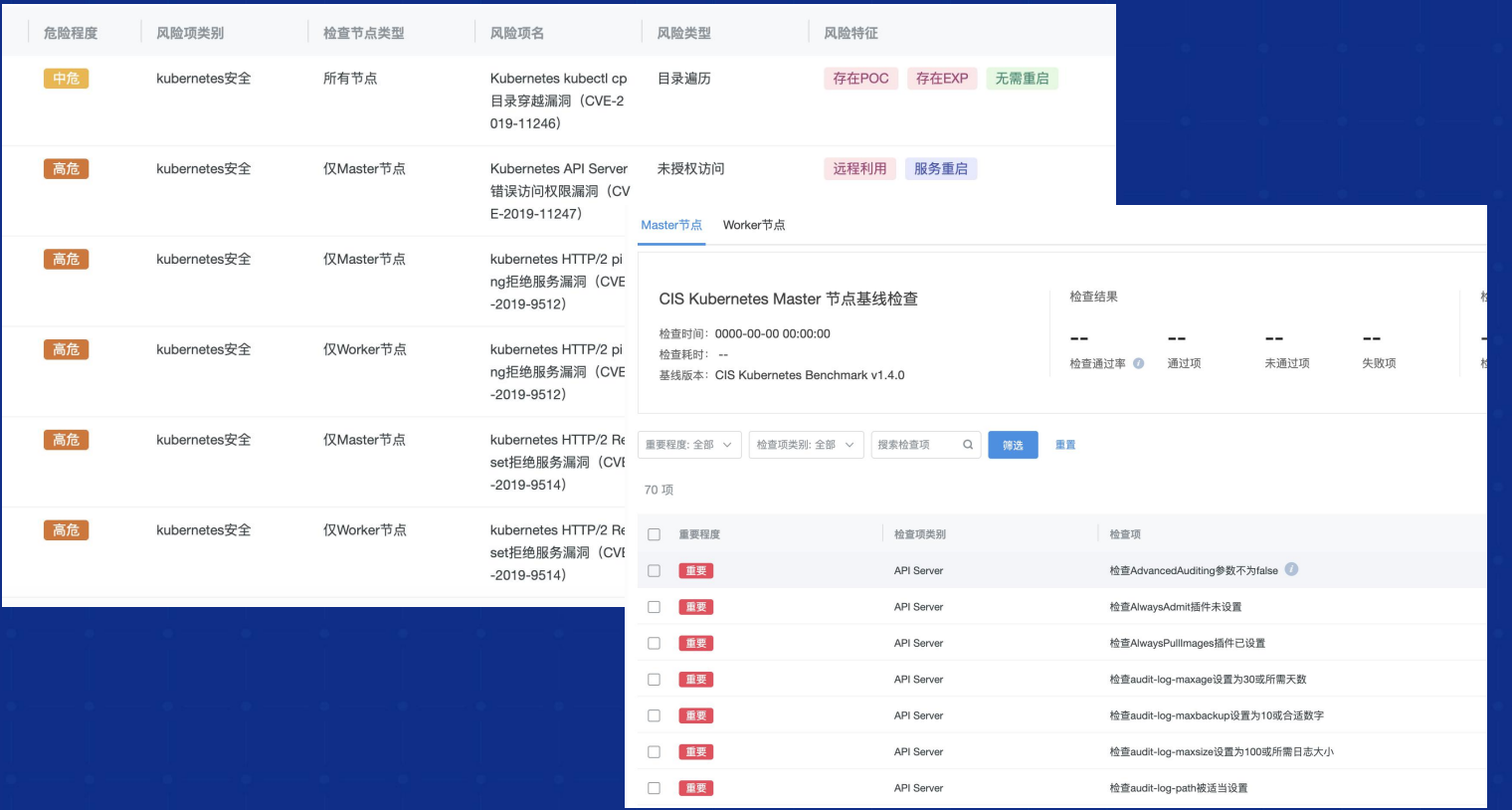
例如k8s集群中应按照rbac策略，合理划分权限，避免授予过大的高风险权限；某个业务的仓库项目应仅限于由业务方管理。

2） 为集群的配置建立统一的安全基线

使用安全基准线（如CIS K8S 基线）对集群进行检测，确保上线的集群满足最基本的安全基准。

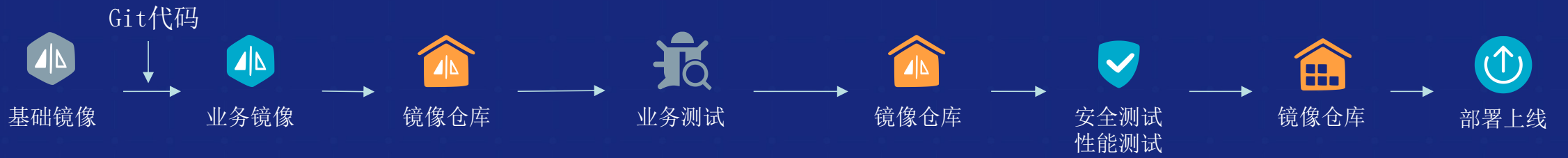
3） 使用风险扫描工具发现集群组件漏洞，并进行加固

发现k8s、docker、service mesh等集群组件的安全漏洞问题，并进行加固。



Step3：容器应用安全

进一步，需关注镜像构建过程及其运行时的的安全问题。



基础镜像安全检查

- 恶意文件
- 敏感信息
- 应用漏洞

业务镜像构建过程检测&阻断

- 镜像配置合规性检测:Dockerfile、yaml文件的合规性
- 业务镜像安全检测
- 阻断不合规的业务镜像

测试仓库镜像安全检查：

- 检查镜像安全性

微服务安全漏洞扫描

生产仓库镜像检查：

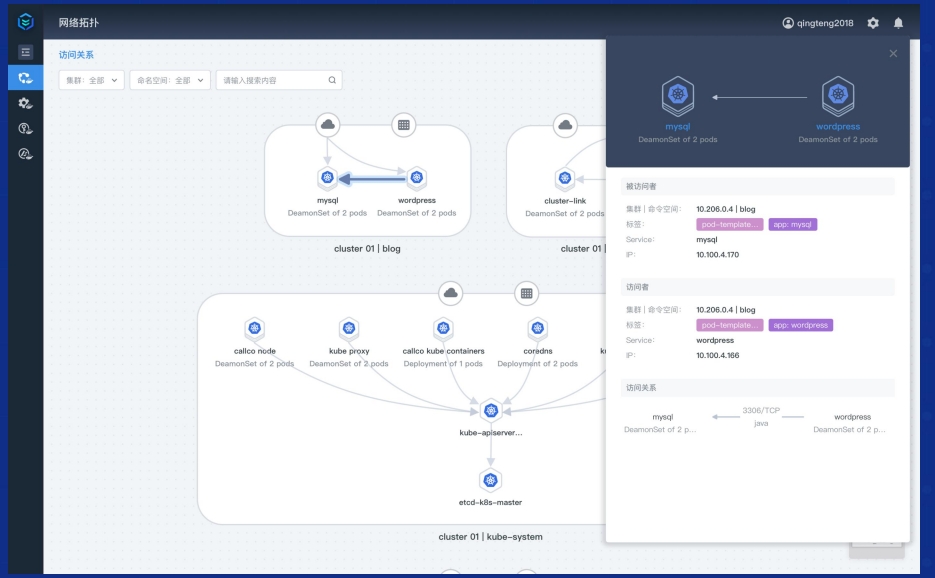
- 软件使用合规性
- 检查不必要的软件应用
- 检查是否来源基础镜像

运行时监控：

- 不安全镜像运行阻断
- 运行时安全监控
- 运行时业务隔离

Step4：构建持续的安全监控与响应能力

构建全景资产视图，进行持续监控与响应，实现集群风险可见、可控。



云原生 产业大会
2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

THANKS!

CAICT 中国信通院

青藤云安全