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

云原生安全规划与实践

小佑科技 袁曙光

CAICT 中国信通院

目录

不可变的基础设施

物理机

- 单个应用
- 物理服务器作为扩展单元
- 以年为单位的生命周期

虚拟主机

- 硬件虚拟化
- 虚拟机作为扩展单元
- 以月为单位的生命周期

容器

- OS 虚拟化
- 应用/服务为控制单位
- 以分钟级别的生命周期

Serverless

- 应用运行时虚拟化
- 资源作为扩展单位
- 以秒级别为生命周期

防护边界变化

传统IDC

- 以物理位置或者设备为边界
- 主要以MAC/IP为标识

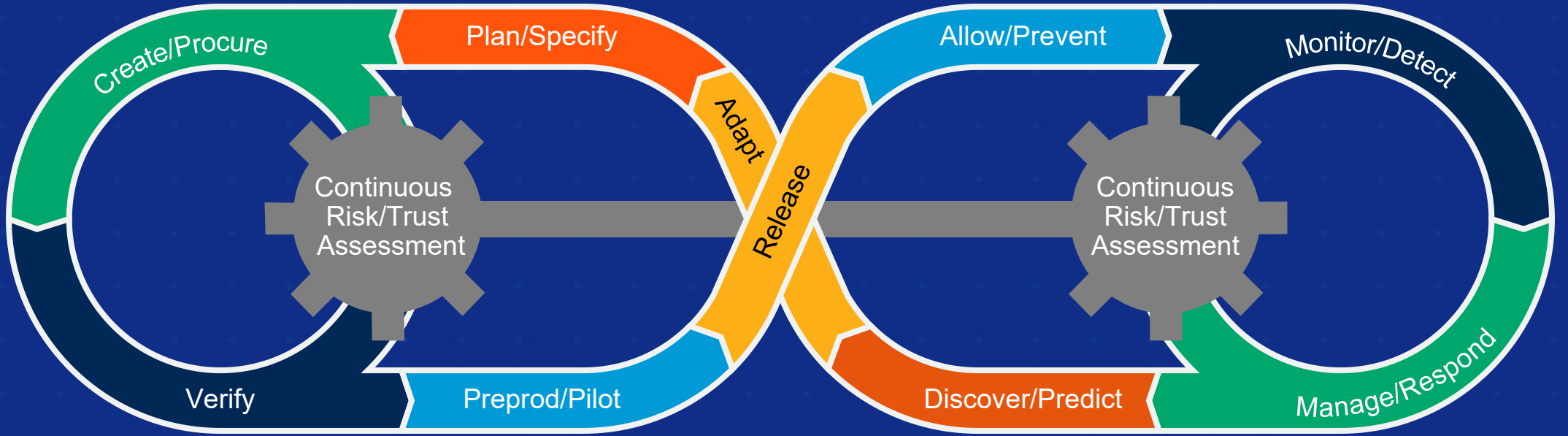
VM云计算

- 以虚拟机为边界
- 主要以IP为标识

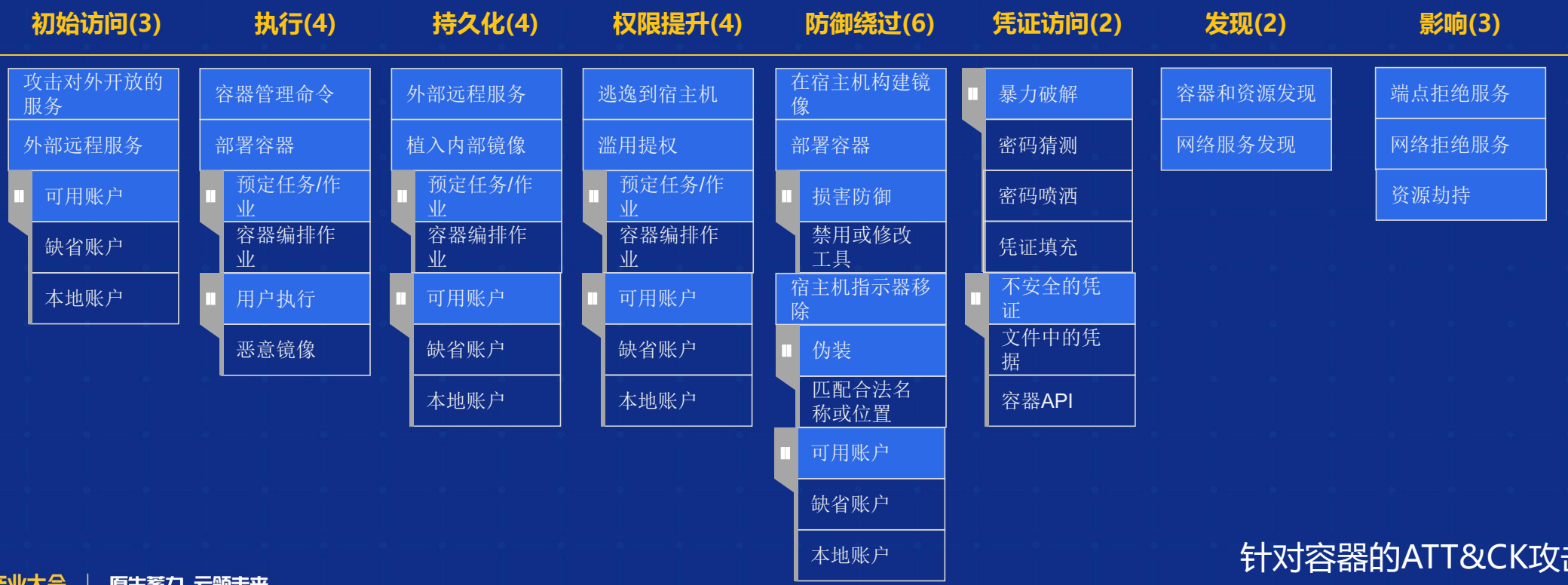
云原生

- 以服务或应用为边界
- 主要以标签为标识

高度自动化的流程


Create/Procure
Plan/Specify
Allow/Prevent
Monitor/Detect
Adapt
Release
Continuous Risk/Trust Assessment
Continuous Risk/Trust Assessment
Verify
Preprod/Pilot
Discover/Predict
Manage/Respond

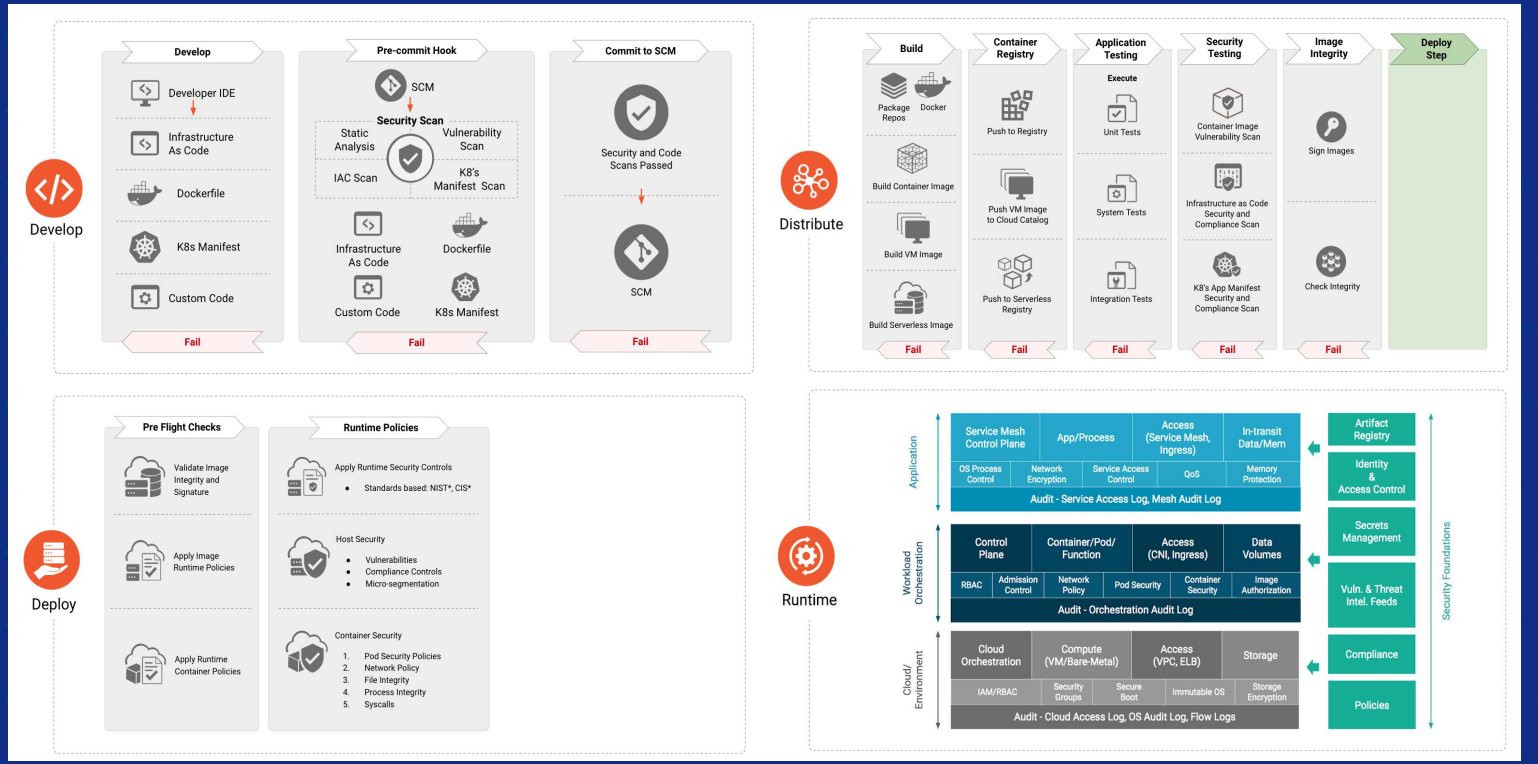
全新的攻击手段



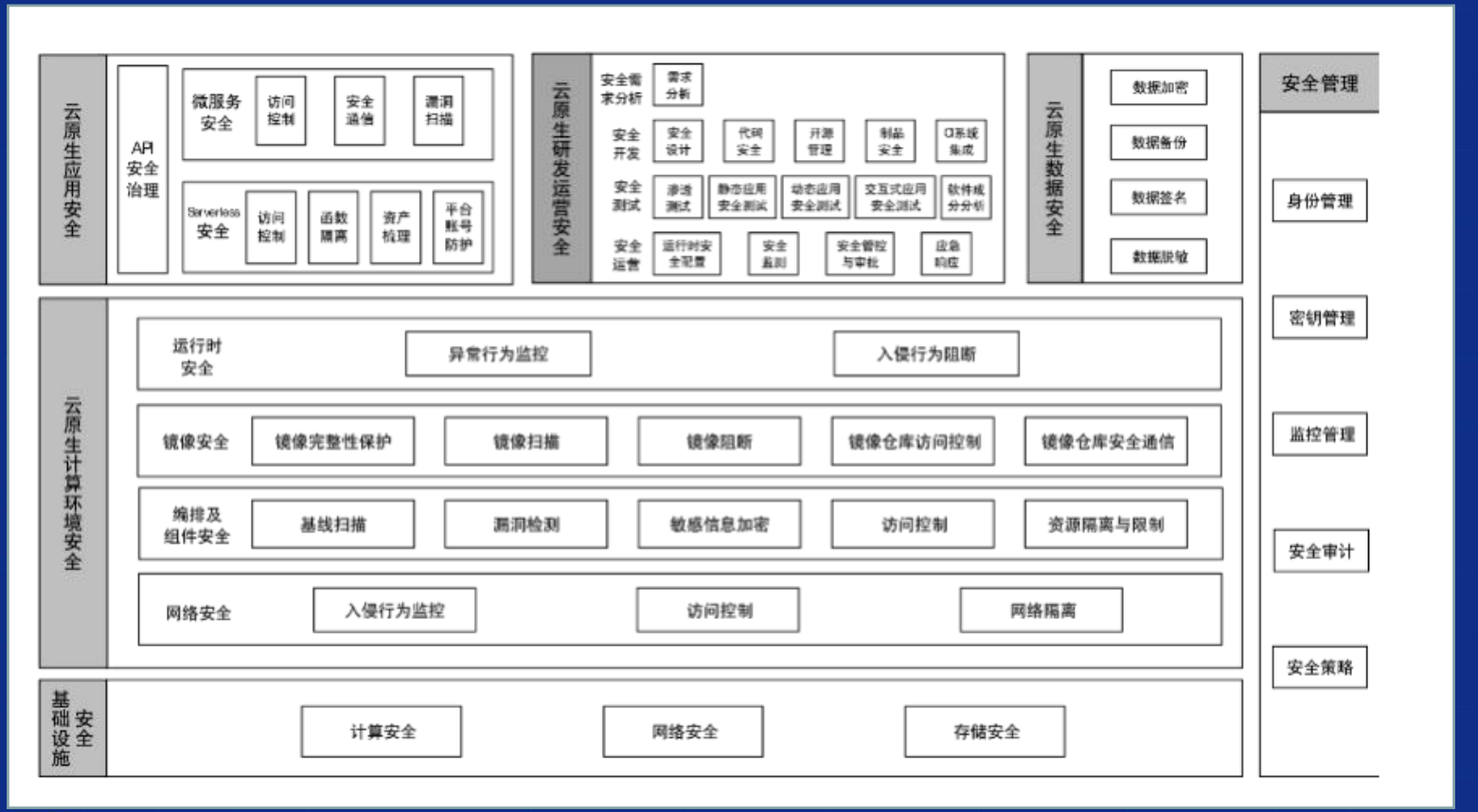
针对容器的ATT&CK攻击模型

目录

应用生命周期视角下的云原生安全体系



IT架构视角下的云原生安全体系



云原生关键安全的四大支柱

容器安全

编排工具（集群）安全

微服务安全

DevSecOps

云原生安全建设的规划

容器/集群

- 镜像安全
- 容器运行时安全
- 集群安全
- 网络层访问控制

微服务

- 应用安全
- 微服务API安全
- 服务网格化安全
- 应用层访问控制

无服务

- RASP

安全运营

- 事件检测
- 事件响应
- 事件处理

云原生安全建设需要注意的几个关键点

01

云原生安全策略先行，结合实际，建立基线及准入机制

02

全面的考虑云原生安全整体架构

03

根据云原生的建设节奏，逐步完善

04

贴合云原生技术演进方向，防止建设完不能用或者没有用

05

贴合云原生的特点，使用符合云原生特点的解决方案

目录

整体解决方案

安全策略调整

- 安全策略的自动机器学习
- 自动调整安全策略

运行环境的检测

- 主机安全合规基线扫描
- 容器安全合规基线扫描
- 编排工具合规基线扫描
- 网络安全策略配置

安全监控

- 容器/主机内进程行为监控
- 容器/主机内文件行为监控
- 容器/主机内网络行为监控
- 容器系统调用监控
- 编排工具日志审计

安全扫描

- 镜像模板文件安全扫描
- 镜像软件漏洞扫描
- 镜像恶意文件扫描
- 镜像敏感文件扫描
- 镜像开源许可扫描
- 阻断镜像构建

安全验证

- 镜像安全验证
- 基础镜像验证
- 镜像签名验证
- 镜像来源验证
- 阻断镜像运行

安全风险处理

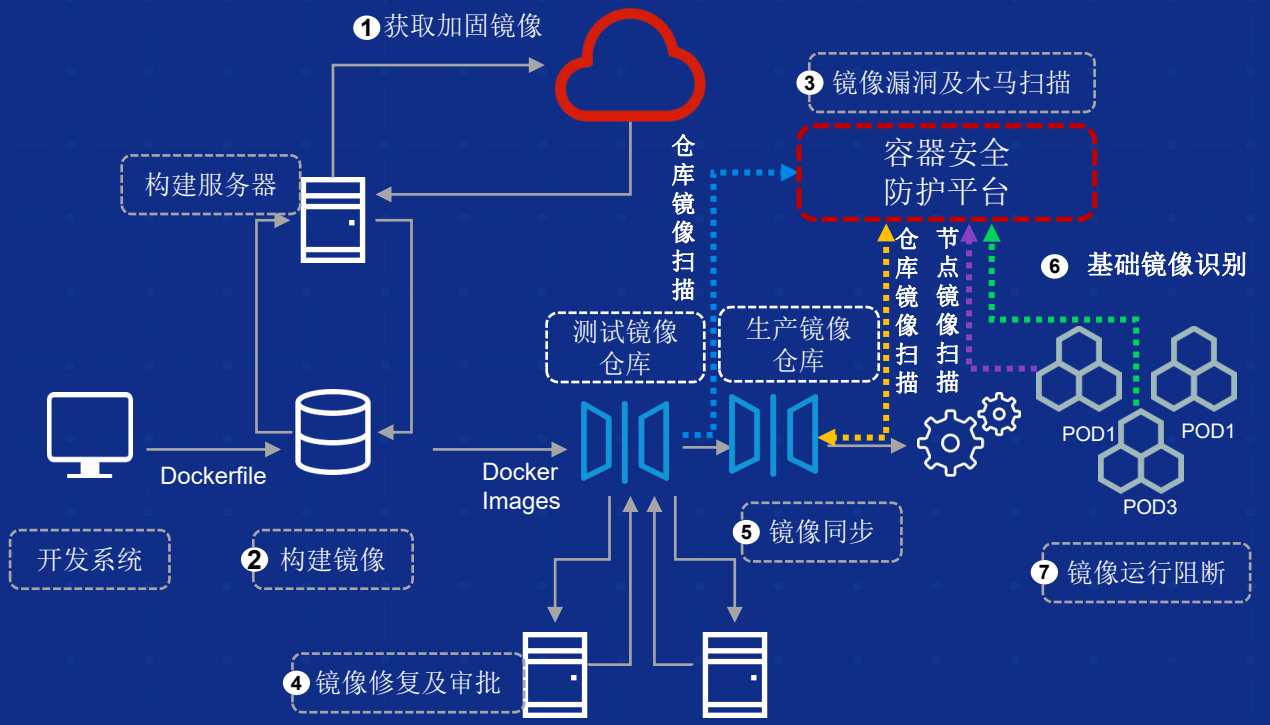
- 恶意镜像禁止运行
- 容器内恶意行为阻断
- 安全事件关联分析处理

合规基线的自动检测

技术合规基线

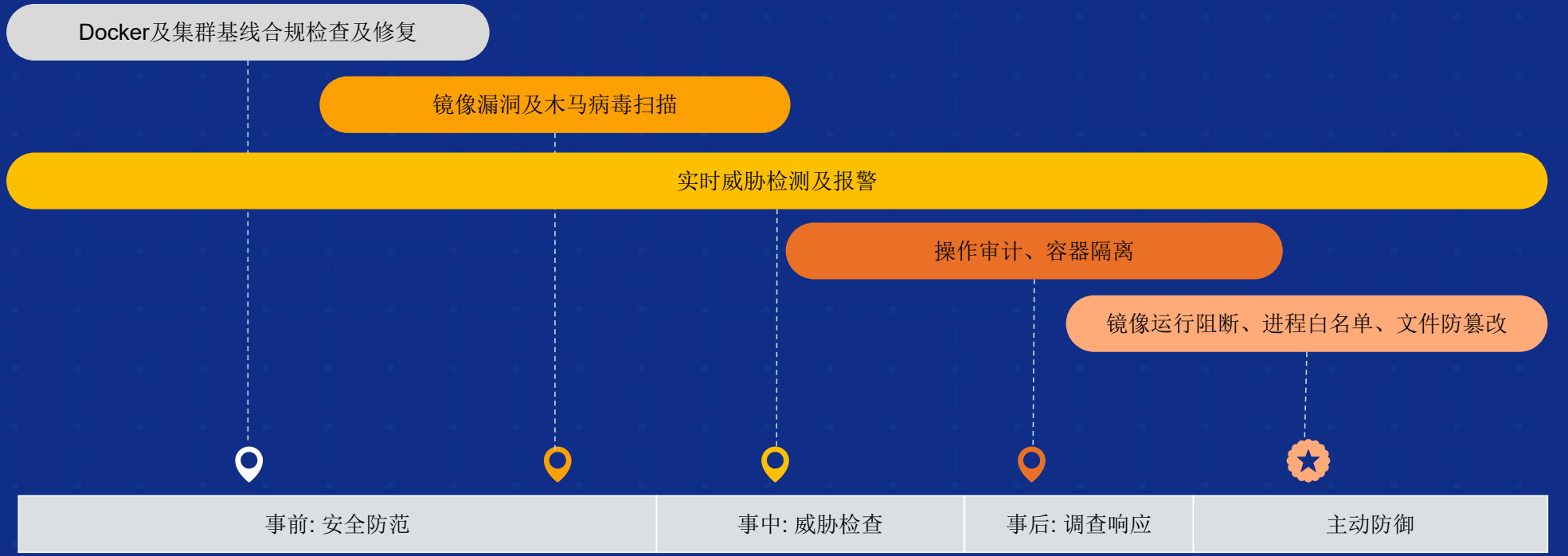
- CentOS、Ubuntu 等OS合规基线
- Kubernetes、Openshift合规基线
- Docker合规
- 企业自定义合规

镜像的漏洞管理



1. 获取黄金镜像
2. 基于黄金镜像构建业务镜像
3. 上传测试仓库并扫描漏洞和病毒
4. 镜像漏洞修复及上线审批
5. 审批通过后将镜像同步到生产仓库
6. 节点镜像的扫描及基础镜像的识别
7. 配置镜像运行策略并进行阻断

容器运行时的动态检测与防护



编排工具的安全检测

安全检测

对Kubernetes集群的Api Server及节点模拟黑客攻击进行安全检测，发现安全漏洞

日志分析

对Kubernetes的日志进行安全分析，以发现不符合安全策略的POD、服务等创建、删除等

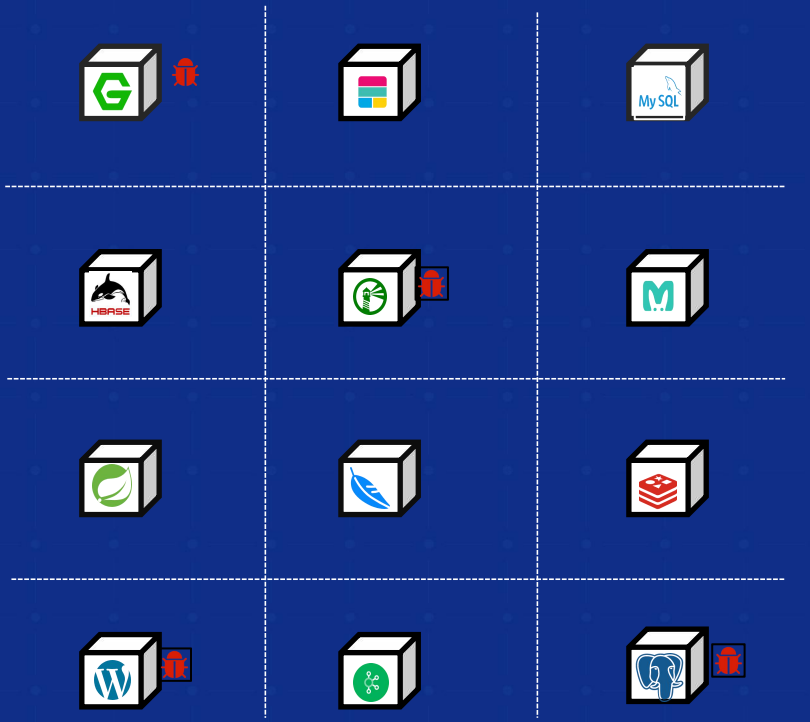
配置审计

对Kubernetes的Yaml文件进行审核，发现不符合安全策略的配置

合规审计

使用CIS等合规标准对Kubernetes进行合规审计

微服务安全



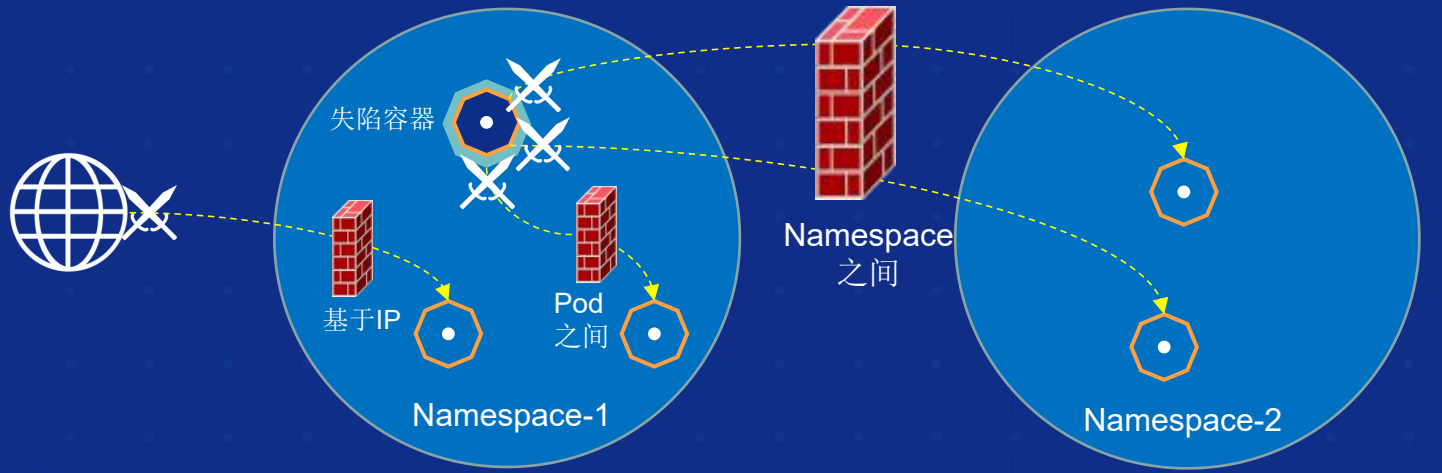
云原生网络安全

容器网络可视化

- 感知网络流量
- 识别失陷容器与恶意行为（规则、机器学习）

容器网络微隔离

- 匹配不同CNI插件
- 支持不同控制粒度（集群/namespace/service/Pod/IP）

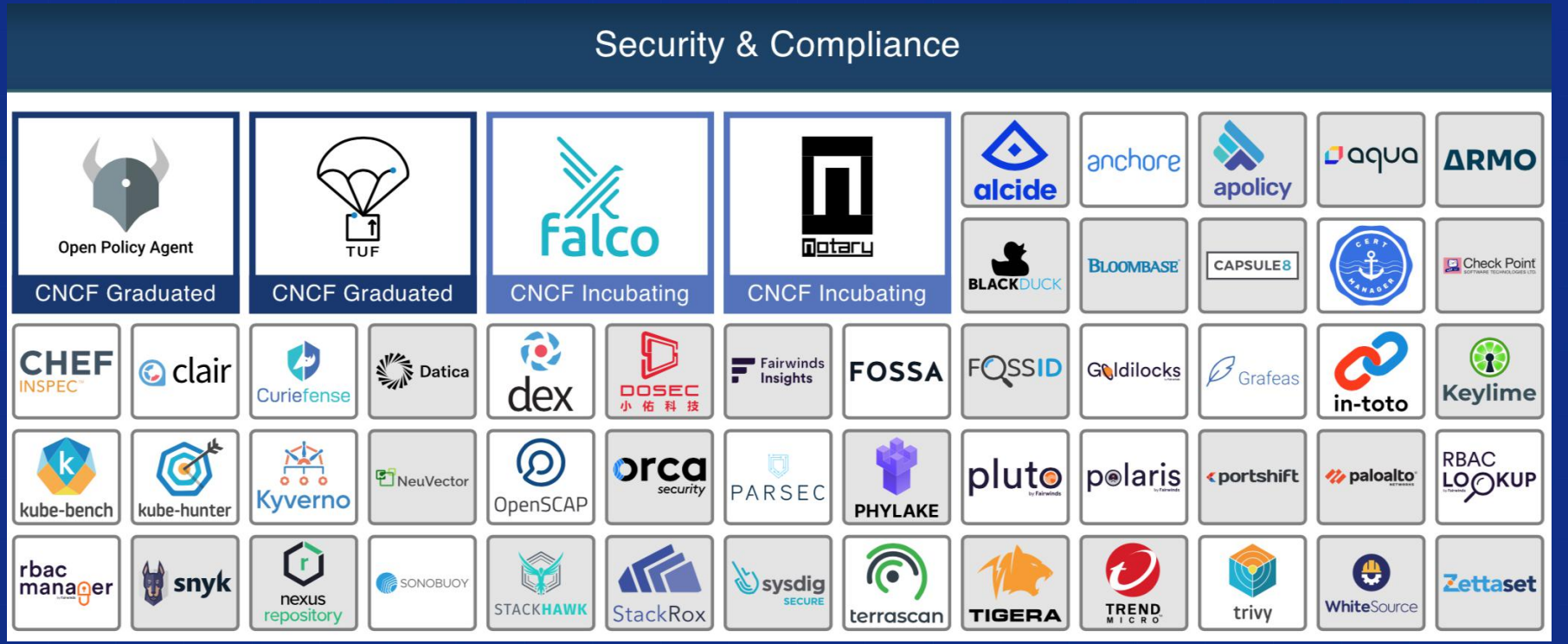


处置措施

- 隔离失陷容器
- 阻断攻击流量

攻击流量

可参考技术-CNCF安全与合规象限



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