



云原生应用供应链安全的最佳实践

查益 Senior PM (Microsoft)
张诗威 Principal SE Manager (Microsoft)

2023.4.8

目录

CATALOGUE

1

软件供应链安全

2

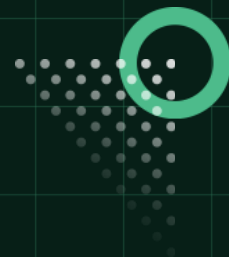
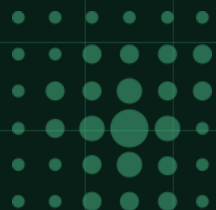
最佳实践

3

演示

4

总结



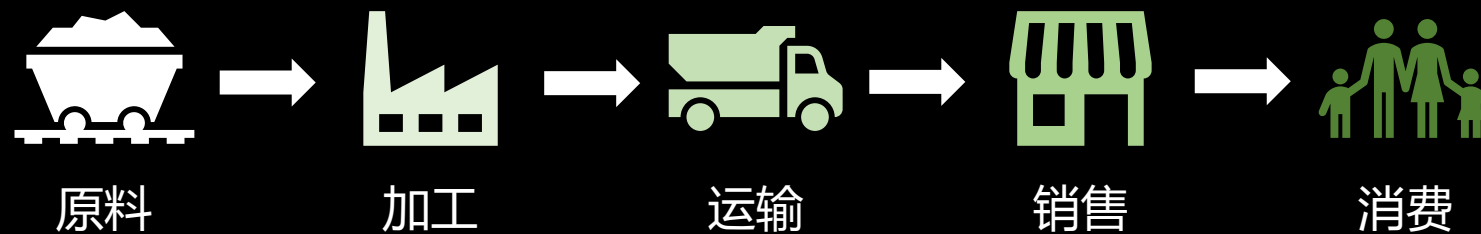


00

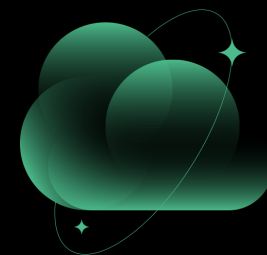
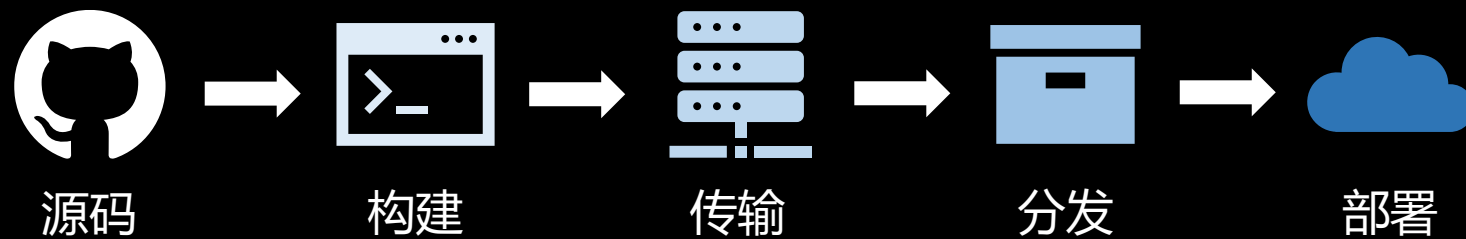
软件供应链安全

软件供应链 (Software Supply Chain)

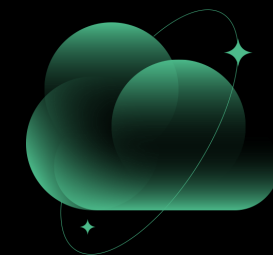
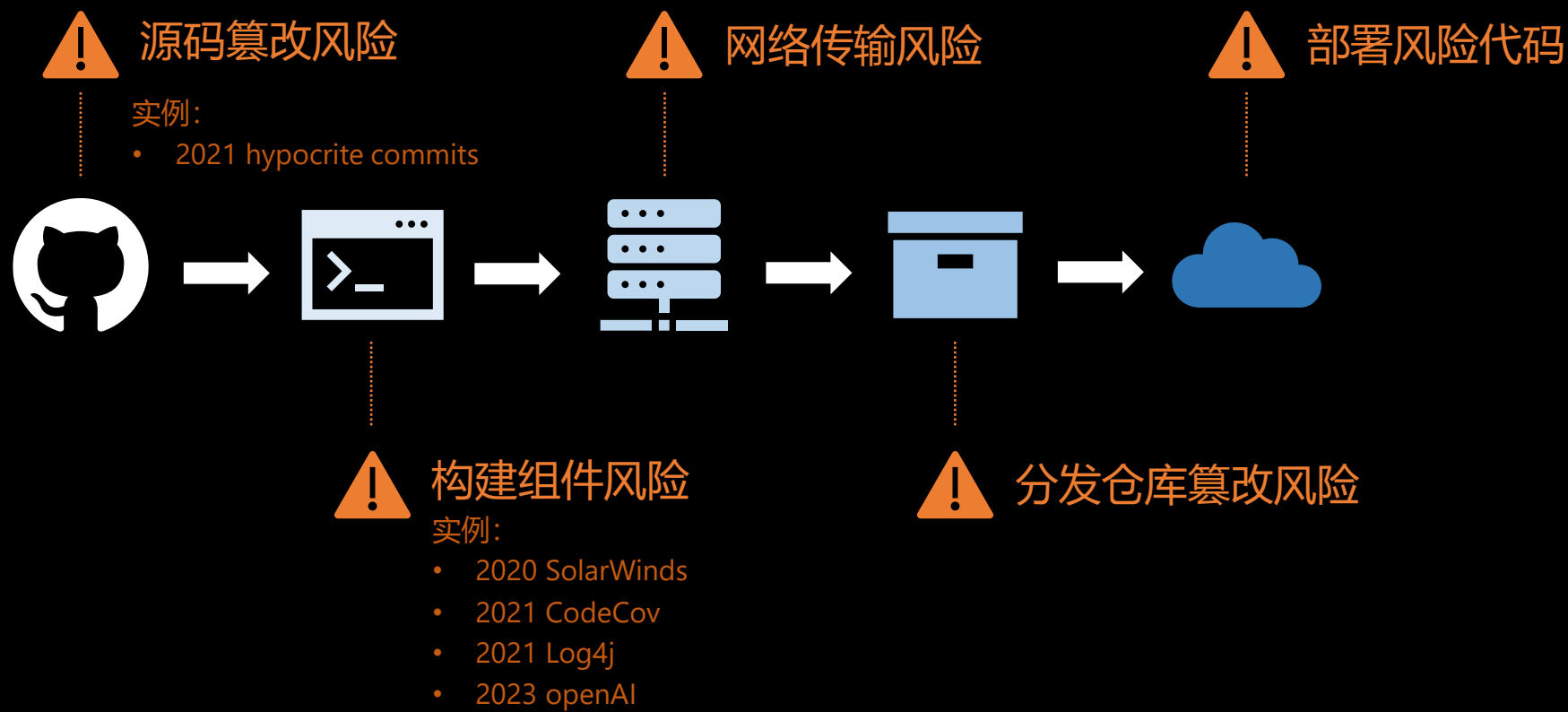
传统供应链

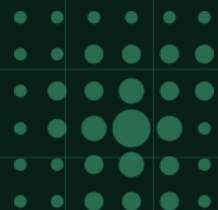


软件供应链



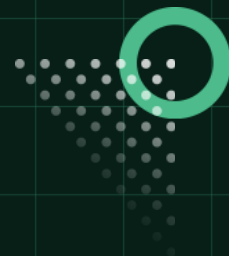
软件供应链的风险





01

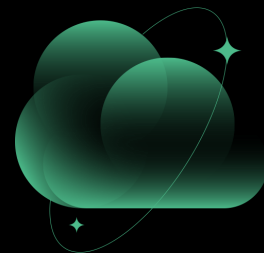
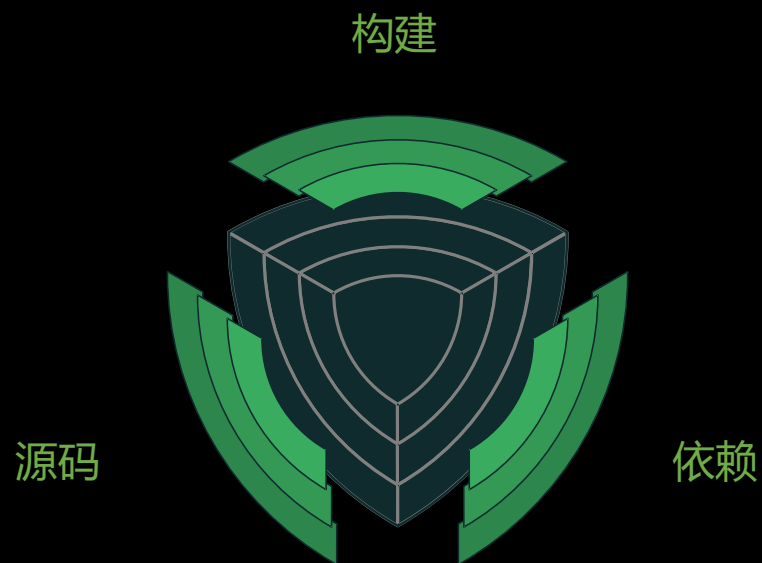
最佳实践



软件供应链消费框架 (S2C2F)







软件制品的供应链级别 (SLSA)



软件供应链消费框架 (S2C2F)

2023

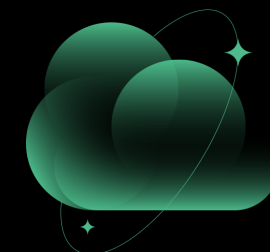
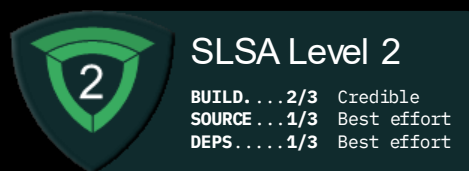
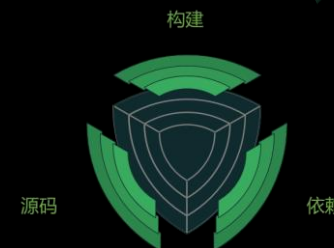


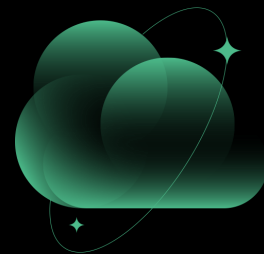
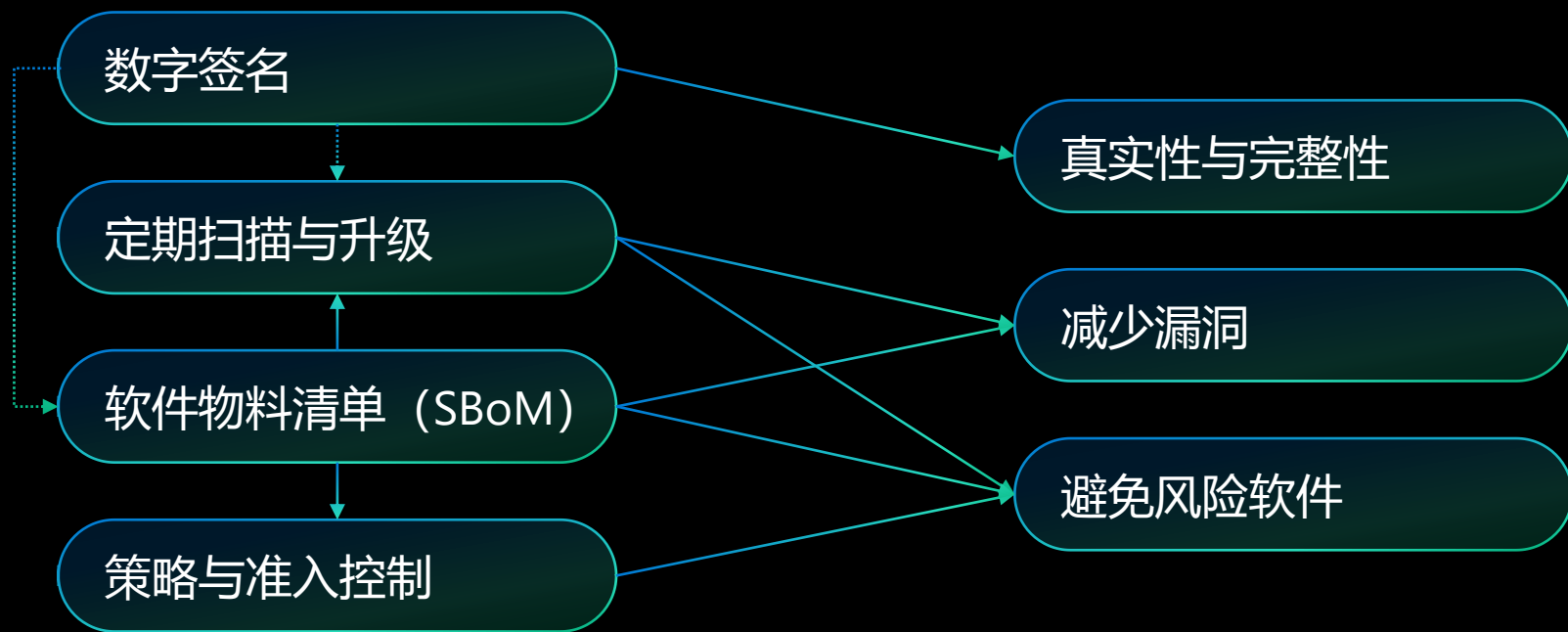
Level 1	Level 2	Level 3	Level 4
 Minimum OSS Governance Program <ul style="list-style-type: none">• Use package managers• Local copy of artifact• Scan with known vulns• Scan for software licenses• Inventory OSS• Manual OSS updates	 Secure Consumption and Improved MTTR <ul style="list-style-type: none">• Scan for end life• Have an incident response plan• Auto OSS updates• Alert on vulns at PR time• Audit that consumption is through the approved ingestion method• Validate integrity of OSS• Secure package source file configuration	 Malware Defense and Zero-Day Detection <ul style="list-style-type: none">• Deny list capability• Clone OSS source• Scan for malware• Proactive security reviews• Enforce OSS provenance• Enforce consumption from curated feed	 Advanced Threat Defense <ul style="list-style-type: none">• Validate the SBOMs of OSS consumed• Rebuild OSS on trusted infrastructure• Digitally sign rebuilt OSS• Generate SBOM for rebuilt OSS• Digitally sign protected SBOMs• Implement fixes

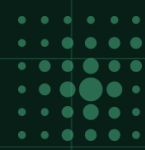


软件制品的供应链级别 (SLSA) v0.1

1. 构建过程必须全自动执行并生成来源文件
 - 例：未签名的来源文件
2. 要求版本控制并使用托管构建服务来生成可认证的来源文件
 - 例：托管源码/构建、已签名的来源文件
3. 源码和构建平台符合特定标准以保证源码可审计性和来源完整性
 - 例：主机安全控制、不可伪造的来源文件
4. 所有修改需要双人审阅，并要求构建过程密闭可重现
 - 例：双人审阅、密闭构建

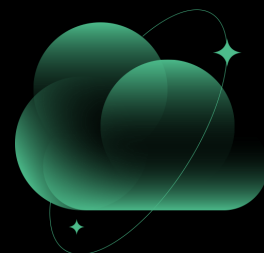
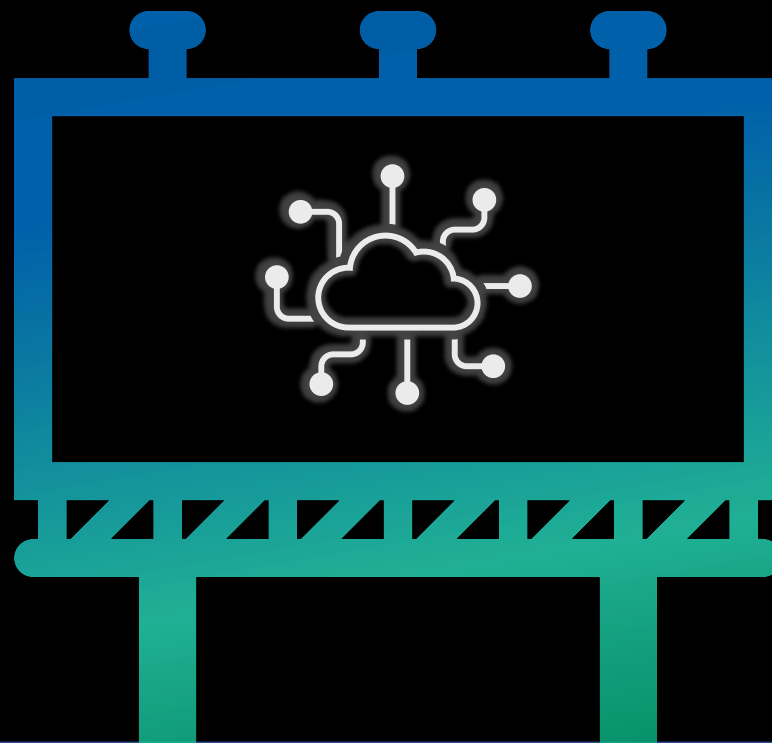


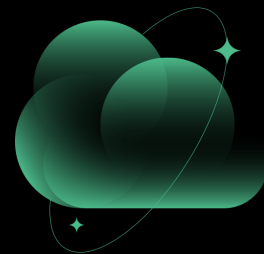
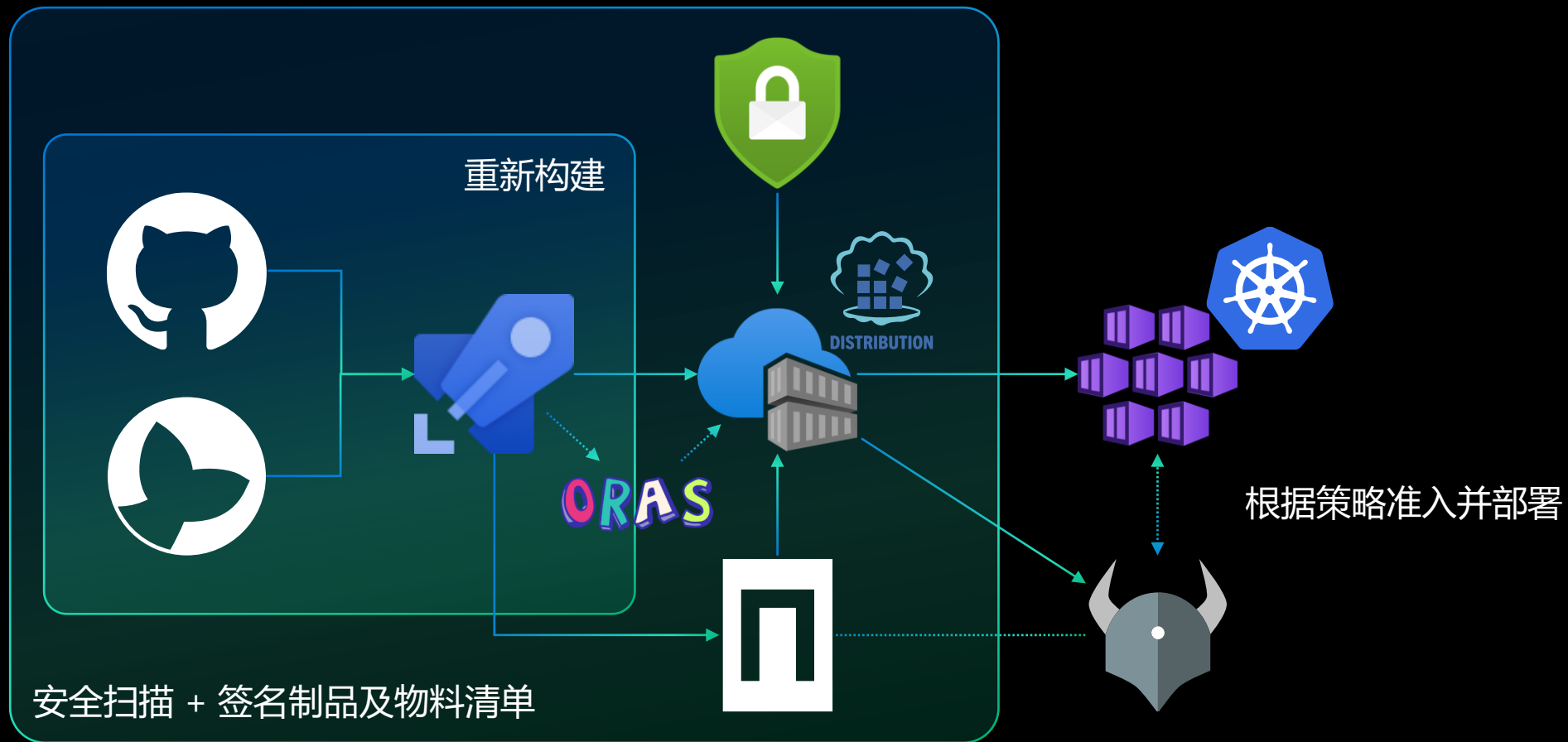


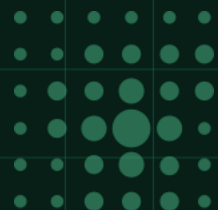


- 容器镜像及制品签名
 - Notation
 - Cosign
- 容器镜像及制品分发管理
 - ORAS, regctl, skopeo
- 软件物料清单生成
 - Microsoft sbom-tool
 - Syft
- 软件来源及变更证明
 - in-toto attestation
- 容器镜像安全扫描
 - Trivy

- 开放策略代理 (OPA)
 - Gatekeeper
 - Kyverno
- 适用于K8S集群的验证引擎
 - Ratify







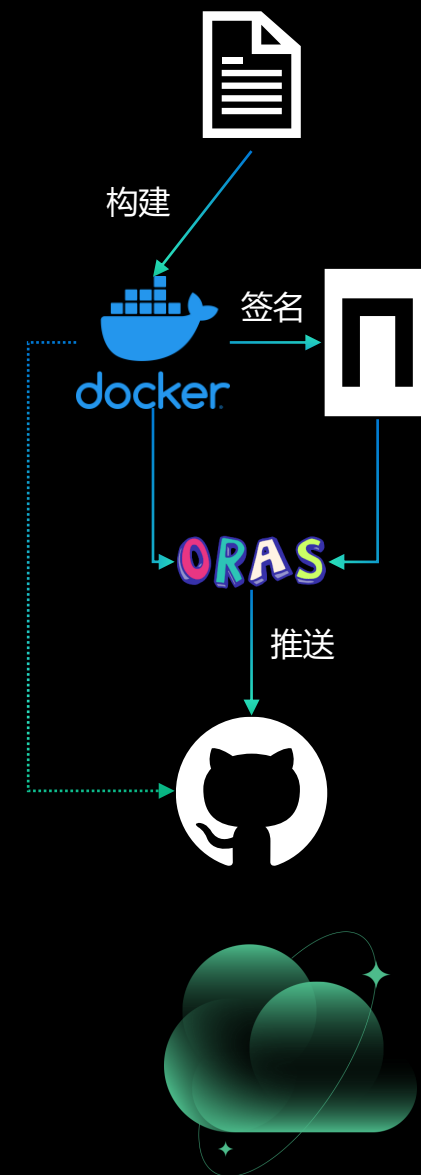
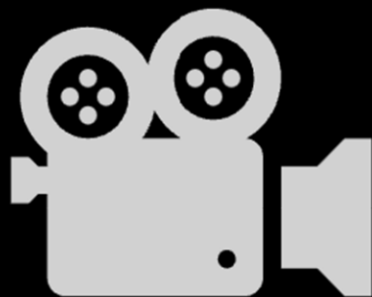
10

演示

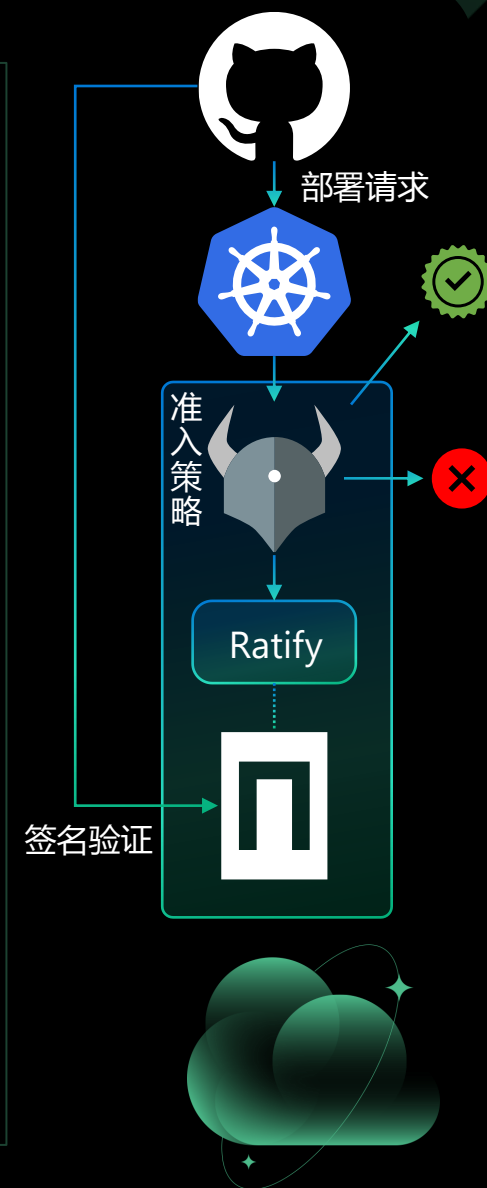
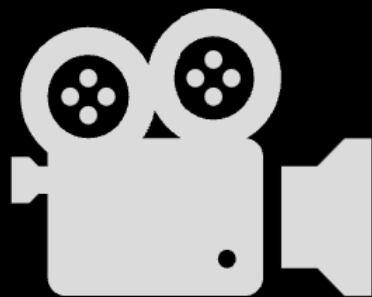
K8S集群上安全的部署容器镜像

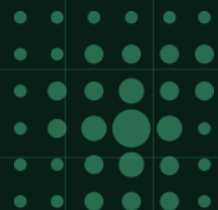


演示-发布签名的容器镜像到ghcr.io



演示-K8S集群安全部署容器镜像





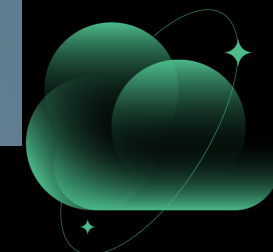
11

总结



总结

- 云原生应用供应链安全
- 最佳实践
 - 软件供应链消费框架 (S2C2F)
 - 软件制品的供应链级别 (SLSA)
- 核心技术以及开源解决方案
 - Notation: <https://notaryproject.dev>
 - ORAS: <https://oras.land>
 - Ratify: <https://github.com/deislabs/ratify>
- 企业级的解决方案请联系微软Azure团队





Thanks

