Red Hat

开发人员应采用的 6 个 DevSecOps 最佳实践

1 降低应用依赖项风险

用于构建应用的软件组件中可能存在漏洞，需要您进行妥善管理。您可以使用软件组成分析（SCA）工具来降低软件供应链风险，尤其是在使用开源软件组件时。应寻找具备以下能力的 SCA 工具：

- 扫描应用依赖项，确保它们不含已知的漏洞。
- 通过识别组件及其许可证并标记或许不兼容的许可证，帮助自动实现软件许可合规性。
- 确认应用依赖项是最新的，并且来自于依旧活跃并在提供更新的社区。
- 成为应用构建过程中的自动化部分，融入到开发环境中。这使开发人员有机会在集成之前解决问题，从而减少应用构建失败的次数。

2 统一代码和配置管理

GitOps 模式在 Kubernetes 和容器化环境中比较流行，它包括的多种实践可助您从开发阶段开始极大改善安全态势：

- 将源代码管理（SCM）开发最佳实践应用于配置。使用相同的登记、合并和批准控件，能够追踪到对基础结构配置作出变更的特定人员和时间。
- 开发人员不应依赖 Ops，而应在流程中尽早考虑配置，并确立对应用的预期生产环境的构想。在开发、测试和生产中使用相同类型的环境与安全控制，从而更轻松地在整个生命周期中管理配置。
- 利用自动化构建管道来构建容器镜像和二进制工件，实现持续集成 / 持续交付（CI/CD）。将这些镜像部署到生产环境中时，应当不需要进行临时更改。
- 不在 SCM 系统中存储敏感数据。利用工具来扫描配置和容器镜像，确保它们不含嵌入的机密。

3 保护应用机密

在整个应用生命周期中，管理身份和机密（如密码、令牌和密钥）非常重要。对 SCM 系统、容器镜像仓库和二进制存储库的访问需要受到控制。供应用用于访问数据库和服务的凭据，以及自动化构建和测试过程所需要的凭据，也需要得到保护。如果机密存储在 SCM 系统或配置文件中，则有可能会被意外泄露。采取以下措施来保护应用机密：

- 在生命周期早期建立身份管理和访问控制基础架构。
- 考虑使用机密保管库或硬件安全模块（HSM）来管理和保护静止和传输中的秘密。机密保管库通常是软件解决方案，而 HSM 则使用专用硬件来提供更高级别的保护。应选择其中任一项来集成到身份管理基础架构中。

4 使用可信的基础镜像

容器基础镜像是高度精简化的 Linux® 发行版。其中可能会预装数百个软件包，或许含有潜在的漏洞。采取以下措施来降低容器镜像风险：

- 选择可信的镜像，其应当具有安全可靠、定期发布并经过充分测试的更新。调查镜像来源和可用的支持选项。
- 利用镜像工具检查有无已知漏洞。还应扫描镜像，以验证其配置是安全的，并且不含嵌入的机密。
- 删除可能在被攻击时利用的不必要的二进制文件（包括操作系统工具），从而减少攻击途径。

5 尽早解决合规性和审计问题

为了减少转入生产时的延迟，务必在开发的早期阶段了解所需的合规框架和技术控制。可以在构建管道中嵌入自动化检查，以执行法规遵从性和安全性要求。

主动开始记录文档，因为规程和策略文档可能在审计中至少占 50%。策略文档应包括访问控制、变更控制、备份和数据保留。记录规程时应包括安全检查，如应用安全测试和 SCA。

6 从强大的平台和生态系统着手

随着安全威胁不断增多，使用一个具有综合性安全生态系统的平台来提供集成和受支持的解决方案变得至关重要。红帽 ® OpenShift® 是一个企业级 Kubernetes 平台，具有广泛的功能来支持开发和运维。红帽 OpenShift 中强大的构建和部署管道提供了一个理想的平台来实施自动化安全检查和控制。从将源代码构建为镜像，到之后的生产部署，流程中的任何阶段都可插入安全检查。

红帽拥有一个由安全防护合作伙伴组成的生态系统，可以增强和扩展红帽 OpenShift 的安全防护功能。这些合作伙伴与红帽通力协作，提供受支持的解决方案来与红帽 OpenShift 集成。您可以从一系列解决方案中挑选，满足所在企业和机构的独特安全要求。

红帽 CodeReady Workspaces 是一个在红帽 OpenShift 上运行的 Kubernetes 原生开发环境，能够加快基于容器型应用的开发。红帽通用基础镜像和红帽运行时可奠定一个坚实的基础，让您的应用具有可靠的来源。

红帽 DevSecOps 框架

全面了解安全防护生命周期，了解开发安全功能如何与红帽 DevSecOps 框架相辅相成。访问 red.ht/DevSecOps。

查找开发安全防护解决方案

观看红帽和红帽安全防护合作伙伴提供的网络培训课堂，了解如何在整个应用生命周期中纳入安全防护。

关于红帽

红帽帮助客户跨环境实现标准化，支持他们开发云原生应用，并利用红帽一流的支持、培训和咨询服务，实现复杂环境的集成、自动化、安全防护和管理。

红帽官方微博

红帽官方微信

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编: 100020
8610 6533 9300

cn.redhat.com
#F29682_0921