金融企业如何正确实施 DevSecOps 策略

引言

包括银行、证券、保险在内的金融服务机构一直面临着巨大压力，他们需要不断增强网络安全水平，加快软件发布速度。乍一看，这两个目标似乎相互矛盾。但有一种方法可以帮助金融企业一举两得，协调并实现这些看似相互冲突的目标，答案就是DevSecOps。

DevSecOps 是指开发、安全和运维团队在整个软件开发生命周期（SDLC）过程中进行端到端协作，自动完成各自的任务，从而快速、安全地发布为数字业务提供支持的软件——包括移动应用、网络服务、API、物联网网络等。

在本份电子书中，我们将介绍：

- 金融企业在致力提高其软件开发生命周期的安全性和敏捷性时面临哪些主要挑战
- DevSecOps 如何保护这些公司的数字业务快速发布上线并为其带来竞争优势
- 为什么二进制制品管理是 DevSecOps 策略的关键，以及软件物料清单 (SBOM) 对于了解二进制文件的组成有何关键作用

金融行业面临的挑战

尽管所有垂直行业的企业都在努力提高其软件管道的发布速度和安全性，但金融服务公司面临的挑战更为独特，并且解决起来更有难度。

网络诈骗的重灾区

银行和其他金融服务公司持有大量宝贵的个人和财务数据，因此成为网络犯罪分子的主要目标。黑客入侵银行系统一旦得逞，就能窃取有关个人和商业客户、银行流程、财务记录等宝贵的机密数据。因此，金融机构面临的威胁来自四面八方，不法分子的手段多种多样，包括最新、最复杂的攻击技术。

无时无刻，银行都可能成为 DDoS（分布式拒绝服务）攻击、勒索软件攻击、网络钓鱼、零日漏洞、高级持续性威胁 (APT)、恶意软件感染、中间人黑客、跨站脚本、物联网入侵和供应链漏洞的攻击目标。

监管力度大

金融服务是监管最严的行业之一，全球各地都为此制定了大量复杂的行业规则和政府法规。显然，DevOps 团队必须确保他们向员工、客户和合作伙伴发布的所有软件均符合公司业务所在国家和地区的法律规定，这些法规不仅数量繁多、条款复杂，而且往往不够直白，新的法规层出不穷。未能遵守这些法规可能导致巨额罚款、承担法律责任、声誉受损和蒙受业务损失。

其中包括：

- **强客户身份验证 (SCA)**，欧洲法规要求金融应用至少提供两种用户身份验证形式
- **支付卡行业数据安全标准 (PCI DSS)**，旨在保护持卡人数据收集、存储、处理和传输的全球行业标准

- **金融工具市场指令（MiFID）**，旨在保护投资者的欧洲法规
- **修订后的支付服务指令（PSD2）**，一项旨在提高电子支付安全性和透明度的欧洲法规
- **萨班斯-奥克斯利法案**，一项美国联邦法律，旨在阻止和惩罚公司和会计欺诈及腐败，保护工人和股东的权益
- **多德-弗兰克法案**，一项美国联邦法律，旨在加强对整个金融服务业的监管，促进美国金融体系的稳定和监督
- **通用数据保护条例（GDPR）**，一项并非具体针对金融业的欧洲法规，旨在保护欧盟居民的隐私和个人数据
- **白宫关于改善国家网络安全的行政命令**，该行政命令并非针对金融公司，旨在加强对影响美国政府和美国私营部门的网络事件的预防和补救

数字环境高度受限

与其他行业相比，金融服务行业 IT 基础设施的特点是受到严格限制，因此敏捷性较差，包括：气隙系统；加强访问控制；非必要不进行跨团队协作；变更管理和审批缓慢；严格的审计和治理；开发人员的灵活性有限。

使问题更加复杂的是，金融行业的 IT 基础设施往往具有复杂、大型和异构的特点，既有传统的本地数据中心，也有采用**微服务架构和容器**的现代混合云部署。它们还必须支持广泛多样的终端，如智能手机、ATM 和 POS 机。

技术颠覆带来的压力

金融企业承受的压力有增无减，他们需要跟上业内各种眼花缭乱的技术创新，还要在与颠覆性初创企业和老牌企业的竞争中保持领先优势。最近的“金融科技”成果包括机器人咨询、纯数字银行、加密货币、区块链、基于人工智能的服务定制和 P2P 交易。

这意味着金融服务企业必须经常发布新的软件并及时更新，以不断增强其数字服务。有趣的是，早在十年前，他们一直在避免这种频繁改变，因为这会增加部署包含漏洞、错误配置或其他安全和合规漏洞的软件的风险。

客户需求不断提高

对于金融服务提供商提供的数字体验，客户的期待越来越高。他们希望通过数字渠道，使用手机、个人电脑和平板电脑便捷地处理银行业务、股票交易、支付、管理退休账户，等等。他们希望这些服务越来越个性化，功能越来越丰富，速度越来越快，并且随时可用。当然，他们还希望所有的数字交易都是安全的。

由于金融服务的数字化，客户更换银行和其他金融服务提供商的流程比以往都要容易，这种竞争压力增加了这些公司不断改善客户数字体验的紧迫性。

利用 DevSecOps 保护并加速您的软件开发生命周期（SDLC）

如何应对这些挑战？如何在不牺牲安全性的前提下保持软件发布速度和创新？无论您的 IT 环境是部署在本地、云端还是两者兼有，您的重点都是确保软件开发生命周期（SDLC）流程的灵活性和安全，而 DevSecOps 可以让这一切成为可能。

通过采用 DevSecOps 实现人员、流程和技术变革，金融服务机构可以：

- 在参与 SDLC 的所有团队和利益相关者（主要是开发、运维和安全，但也包括 QA/测试、业务领导者、公司治理、风险管理及合规审查和高层管理者）之间建立一种开放沟通、协作和共同负责的文化

- 实现任务自动化（包括尽可能多的安全性和合规性检查），提高 SDLC 的速度和敏捷性，并从设计阶段开始，将自动化方法原生内置到每个步骤中，以便及早发现问题并及时修复

- 在整个软件开发生命周期（SDLC）中对软件二进制文件进行精细化管理和跟踪，这样，如果发现它们包含严重的漏洞或合规性问题，就可以查看它们的使用情况，了解它们的“爆炸半径”影响范围，并迅速修复问题

- 验证通过软件开发生命周期（SDLC）生成的每个工件的真实性，以便开发人员和操作人员确保流水线创建的构建不包含有问题的工件

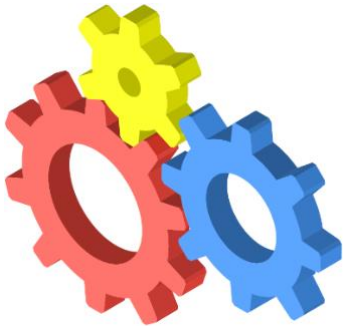
二进制文件管理是 DevSecOps 的核心

一旦源代码在构建阶段编译成二进制文件，二进制文件就会成为 DevOps 流水线中的主要资产，因为它们是开发人员构建、测试、推广软件和将其发布到生产环境的**单一数据源**。因此，管理二进制文件是确保软件构建的完整性和可重复性，进而确保应用程序质量和安全的关键。

要想实现快速、安全的发布软件，其核心是一个端到端、可扩展的 **DevOps 平台**，并以一个可处理所有类型软件包的存储库管理器为基础。该平台应能够通过 REST API 轻松与所有第三方 DevOps 工具集成，并应包含用于安全扫描、分发和监控生产中软件的组件。

DevOps 平台的存储库应存储所有二进制文件并为其分配唯一标准，无论它们是来自组织外部还是内部构建。这为金融服务公司提供了一个单一的数据来源，可用于匹配潜在威胁，并据此编写规则和策略，以触发针对这些二进制文件的特定行动，包括：

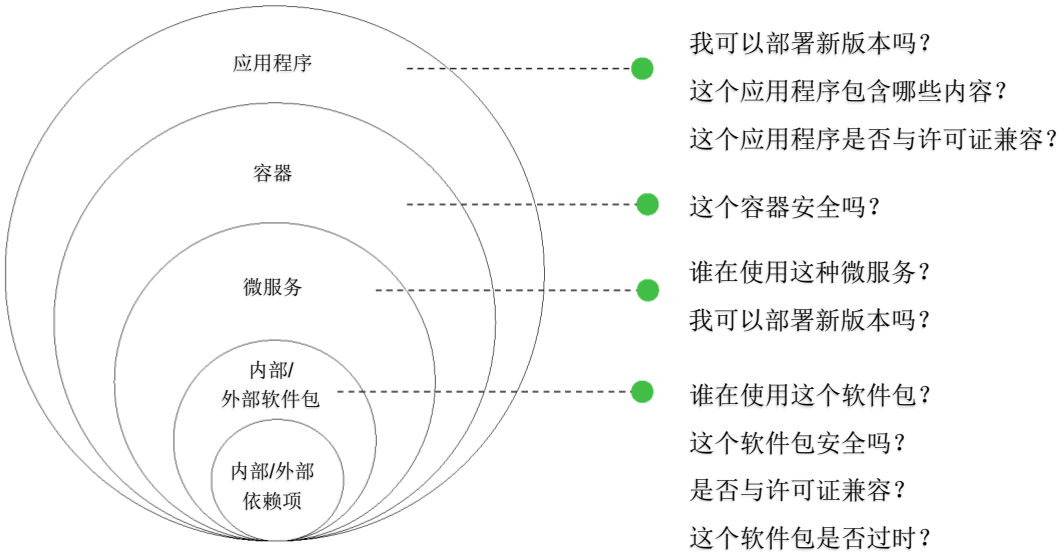
- 阻止文件使用
- 进行标记
- 为其添加新的元数据
- 启动二级进程
- 通知适当的团队成员



金融行业 DevOps 团队的一项重要职能是**隔离环境**，即无法连接到互联网的系统。通常情况下，开发组织会访问 Docker Hub 等远程公共资源来下载用于构建的依赖项。但是，金融机构通常有更严格的安全要求，不能将其业务连接到互联网，因此，拥有一个支持这种隔离环境的 DevOps 平台至关重要。

金融服务企业还需要深入、详细地了解其二进制文件，包括其第三方传递依赖，尤其是开源组件，这些组件通常占应用程序代码库的 90% 以上，包括 API 库、基础操作系统等。

为了解二进制文件的组成，您的 DevOps 平台应为您构建、分发和部署的所有软件生成一份**软件物料清单 (SBOM)**。SBOM 包含构成软件的所有“成分”的列表，包括库和模块（无论它们是开源的还是专有的），以及在构建过程中使用的开发工具和 CI 环境的相关信息。

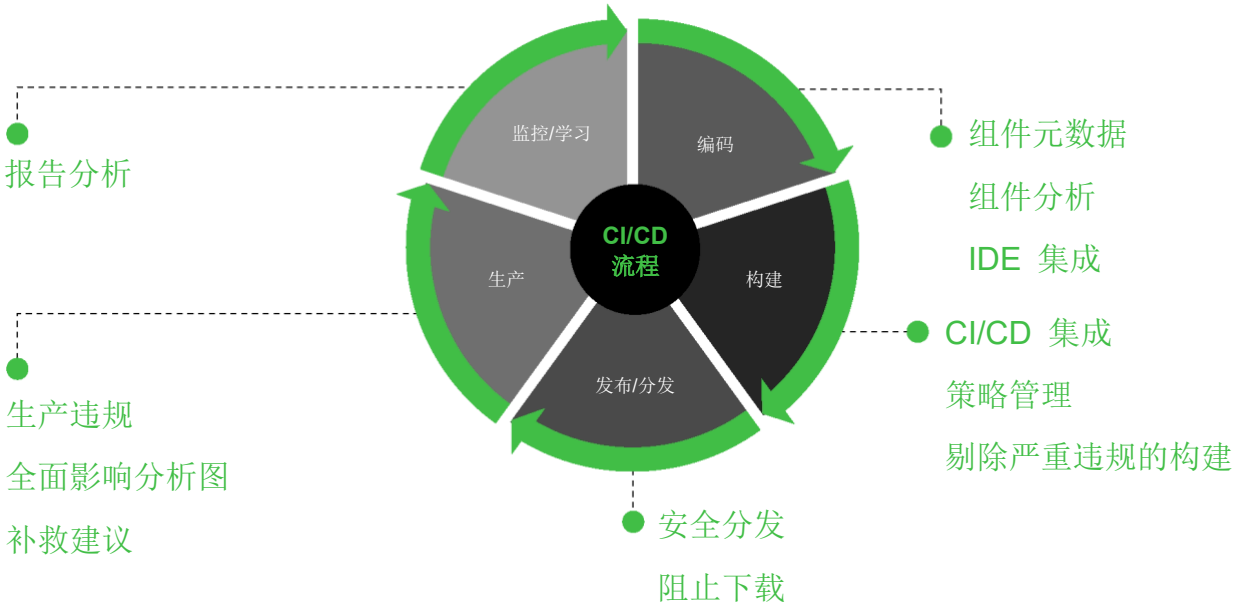


SBOM 还可以概述软件的构建时间、经历了哪些 SDLC 阶段（开发、质量保证、试运行、生产），以及发现并修复了哪些**安全性和合规性**问题。

这些信息有助于推进 DevSecOps 的工作，并有助于维护各种用例的安全性和合规性。例如，SBOM 详细说明了应用程序中使用的所有上游组件及其各种版本。这样，当发现影响应用程序的漏洞时，就可以轻松检测到哪些版本受到影响以及具体产生了什么影响。

该平台还应在整个 SDLC 阶段持续扫描所有软件组件，以检测和修复漏洞、许可证合规性问题和其他问题，具体涵盖以下阶段：

- 编码，包括捕获组件元数据、执行组成分析以及与组织的集成开发环境 (IDE) 集成
- 构建，包括与 CI/CD 系统集成、执行策略管理以及剔除出现严重违规的构建
- 发布/分发，包括确保安全分发软件和阻止下载
- 生产，包括检测生产违规行为，创建完整的影响分析图，并提供修复建议
- 监控，包括创建报告和生成分析



总之，**端到端 DevOps 平台**具有原生的安全和合规功能，可帮助金融服务机构对其二进制文件进行全面问责、追溯和审计。因此，如果二进制文件出了问题，他们可以进行精确、快速的根本原因分析，并采取适当的措施。

结论：

在本电子书中，我们解释了金融服务机构必须采用 DevSecOps 的原因。DevSecOps 可帮助他们在不减慢软件发布速度的前提下妥善保护其 SDLC。

DevSecOps 为银行和其他金融服务提供商带来的主要好处包括：

- 端到端的 SDLC 保护
- 加速软件发布
- 提高开发、运维和安全团队的生产力
- 增强跨团队沟通与协作
- 提高数字服务的质量、性能、可靠性和创新性
- 推动业务增长和扩展，包括：
  - 增加营收
  - 更好地留住客户
  - 降低成本
  - 增强客户体验

想进一步了解如何在金融服务中成功采用 DevSecOps？**联系我们查看演示！**

JFrog DevOps 平台拥有所有必备的功能，可帮助您部署端到端的 DevOps 流水线，快速、频繁地发布安全、合规的软件。

JFROG PLATFORM