

目
contents
录

01 AI 时代的 DevSecOps 变革

02 制品库的“多类型” & “大模型”管理实践

03 制品库的“软件供应链安全”管理实践

04 Demo & 案例

PART 01

AI 时代的 DevSecOps 变革

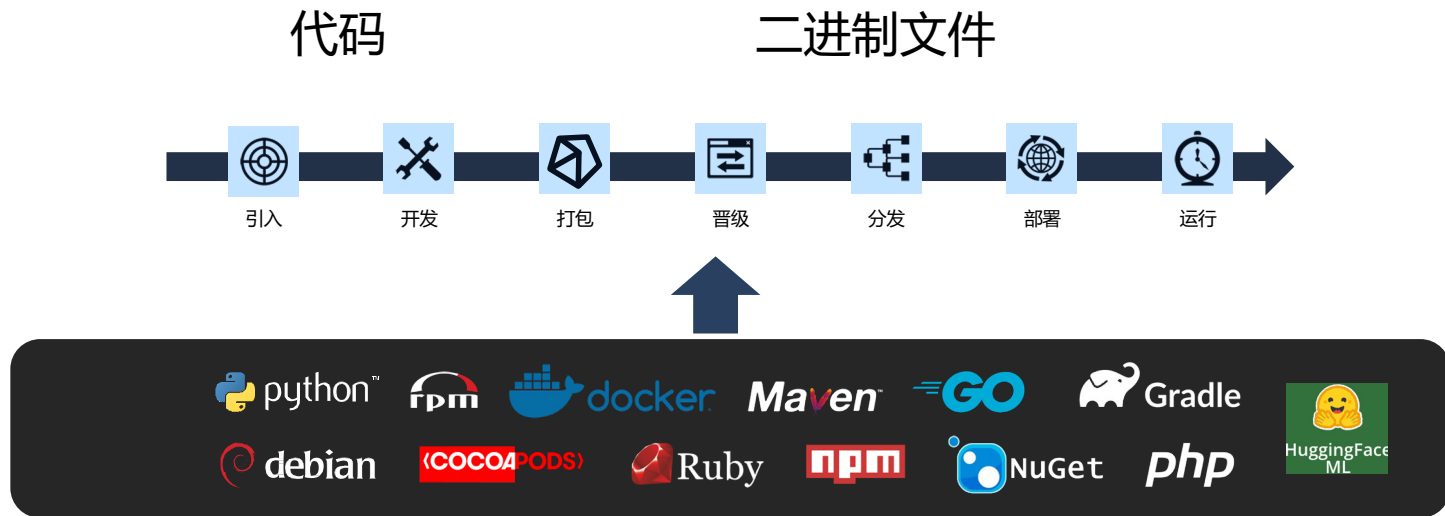
JFrog 软件供应链管理平台

- Artifactory (30+ 制品管理, Huggingface)
- Xray (18+ 制品扫描)
- Curation (OSS 引入管理)
- JFrog Advanced Security (SAST)
- Runtime Security (保持关注)





变革：世界仍在 OSS 上运行？



“我们正处于 AI 的起跑线上，每个行业都将被革命”

“苹果或因 AI 取消了电动汽车计划”

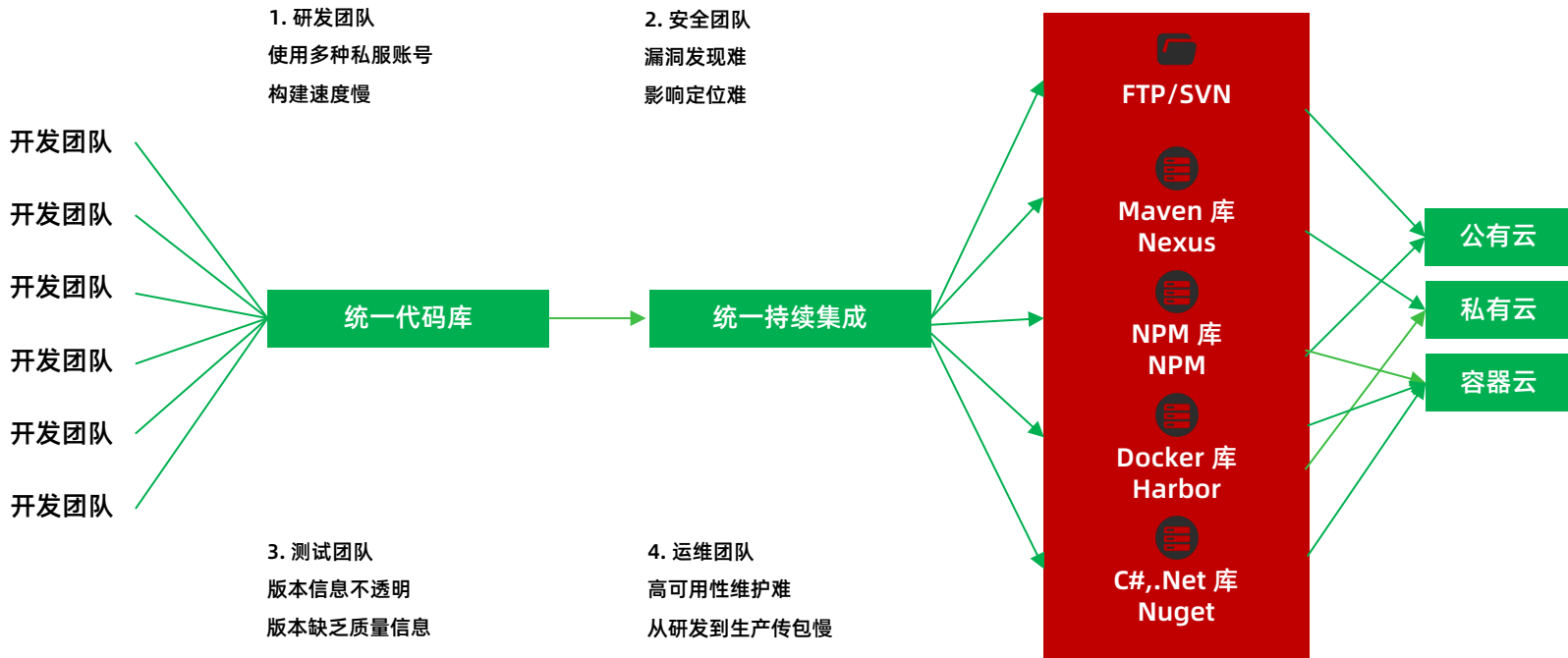
“DevSecOps 实践将为 AI/ML 开发和安全提供宝贵经验”

PART 02

制品库的“多类型” & “大模型” 管理实践



上一代软件管理方式











“最早的问题是 FTP/SVN，最新的问题也是”



为什么需要 Private Huggingface Hub

“类似于 Private Github、 Private Dockerhub，也需要 Private Huggingface Hub”

Before	After
 <p>Models and datasets aren't shared internally, no collaboration across teams.</p>	 <p>Share private models and datasets to collaborate within and across teams.</p>
 <p>Similar models are built from scratch across teams all the time.</p>	 <p>Model reusability across teams. Wheels don't need to be reinvented again.</p>
 <p>Unfamiliar tools and non-standard workflows slow down ML development.</p>	 <p>Familiar tools and standardized workflows accelerate your ML roadmap.</p>
 <p>Waste time on Docker/Kubernetes and optimizing models for production.</p>	 <p>Don't worry about deployment, spend more time building models.</p>

<https://huggingface.co/blog/introducing-private-hub>

通过与 ML/Data Sci 团队的数千次对话，有了对构建 ML 面临的最常见问题和挑战的独特视角：

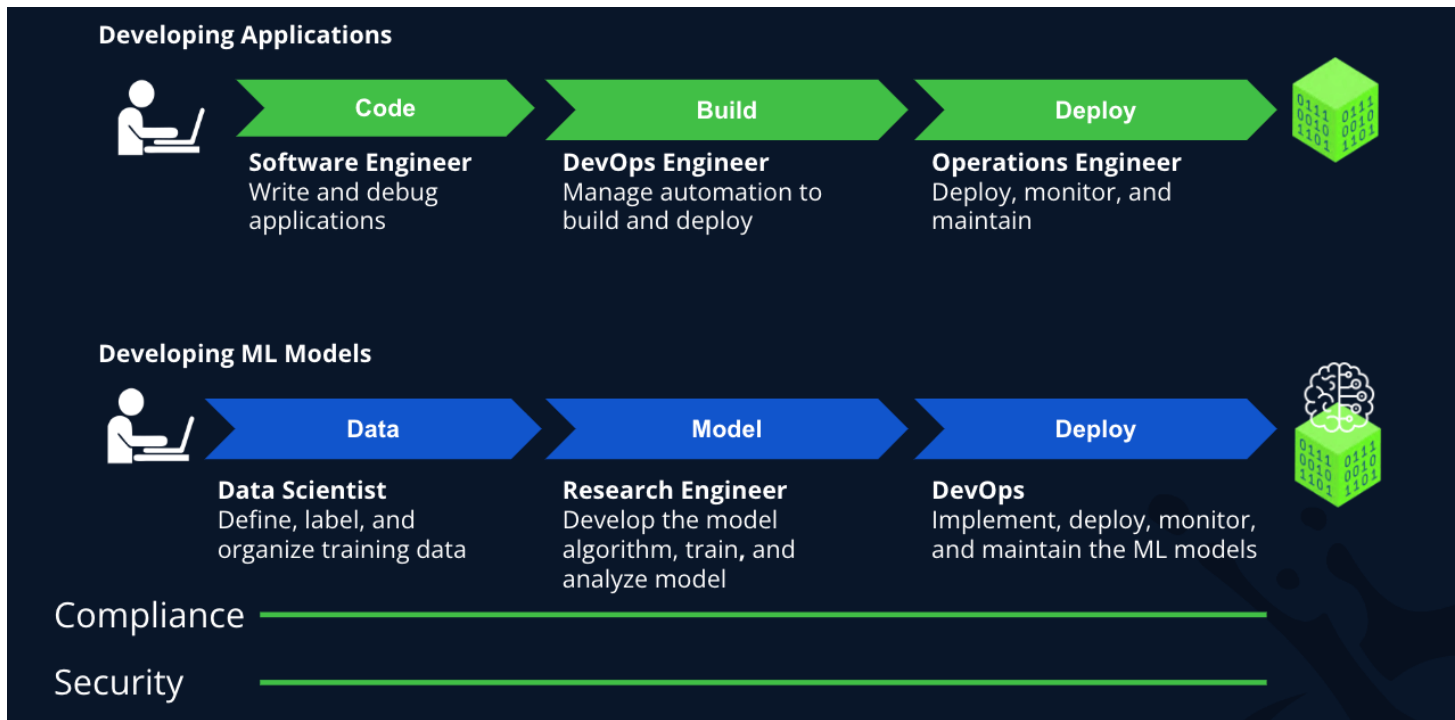
重复的工作、不良的反馈循环、跨团队协作的高摩擦、非标准流程和工具以及生产模型优化困难。

我们不再提供 Private Hub 本地部署。



AI/ML 与传统软件研发的异同

角色不同，目标一致，并行“构建”过程与“结果”，带来版本管理的复杂性和 ML 效率问题



<https://jfrog.com/blog/ml-model-versioning/>



如今 AI/ML 模型版本管理的问题

- 使用 S3 存储桶

这会让数据科学家自行命名每个上传，这通常会导致命名不一致、
File_Name_Final_Final_Final 难题，甚至丢失文件。

- 使用 Git

数据科学家和工程师只需在 Main 分支上堆叠 Commit，利益相关者可以看到以前的提交，但没有简单的方法可以知道他们每次提交会得到什么，因为名称只是一组随机字符。

“基于 **FTP/SVN** 的手工作坊又回来了”

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/568003046034006071>