

# 源于社区 服务社区

中国DevOps社区峰会 2023 · 广州



## 为金融企业解锁下一代安全产品库

JFrog 解决方案架构师 - 张鹏





# 目录

- 1 软件供应链安全背景
- 2 金融行业需求特点和实践案例分享
- 3 JFrog 解锁新一代供应链加速和安全功能特性



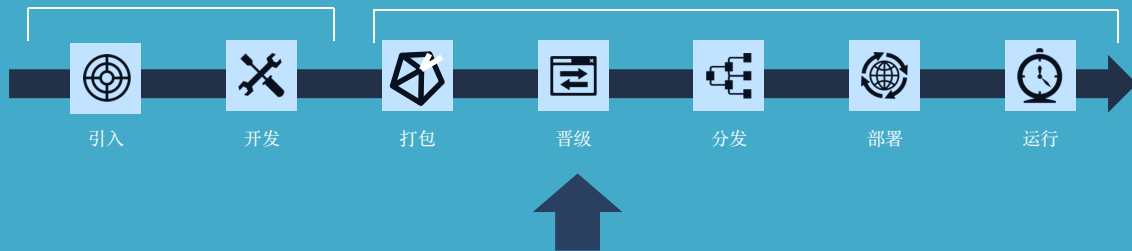


# 1. 软件供应链安全背景



代码

二进制文件



世界在 OSS 和第三方组件上运行  
贯穿 SDLC 的每个阶段





软件供应链攻击  
上涨 100 倍





# 开发者 是其明确目标

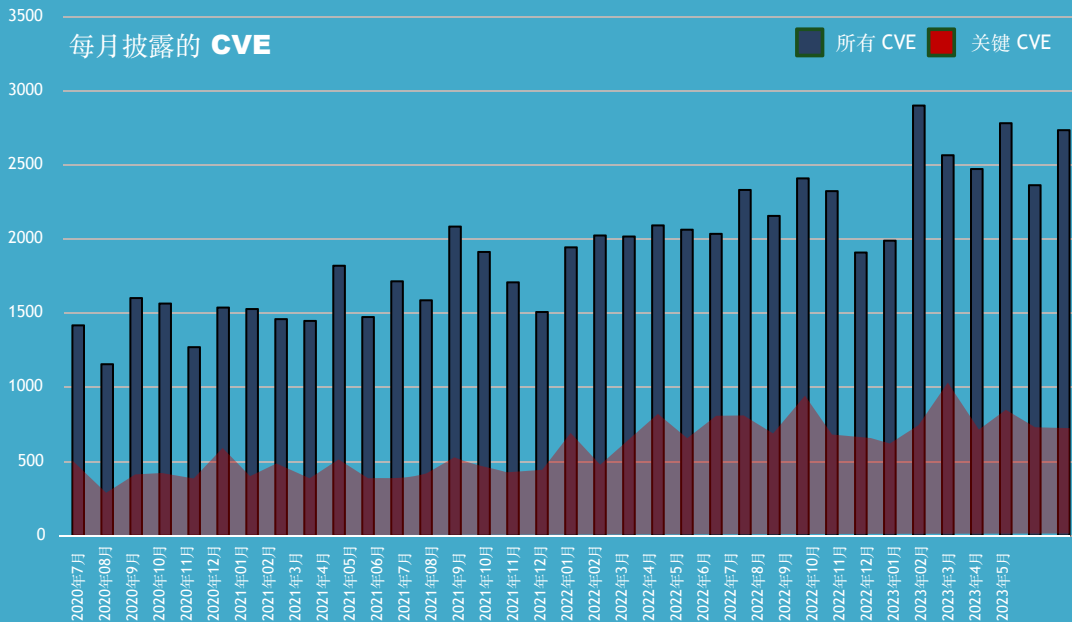


但他们厌倦了安全



CVE 的发布率正在增加

对开发和安全团队产生  
持续压力







然而通用组件中的**关键 CVE**

可以没有真正的安全影响





然而  
关键 CVE  
在通用组件中可以没有真正的安全影响

“

在这个星球上每个使用互联网的人  
几乎每天都以某种方式使用了 Curl

”

curl://



超过200亿安装





然而  
关键 CVE  
在通用组件中可以没有真正的安全影响



daniel:// stenberg://  
@bagder

CVE-2020-19909 is everything that is wrong with CVEs

Another 9.8 CRITICAL curl p

都编好了。

daniel.haxx.se/blog/2023/08/2...

漫长的4天后.....

Base Score: 9.8 CRITICAL

4:03 PM · Aug 25, 2023 · 338.3K Views

390 Reposts 41 Quotes 1,271 Likes 123 Bookmarks

### Current Description

**\*\* DISPUTED \*\*** Integer overflow vulnerability in tool\_operate.c in curl 7.65.2 via a large value as the retry delay. NOTE: curl reports that this has no direct security impact on the curl user; however, it may (in theory) cause a denial of service to associated systems or networks if, for example, --retry-delay is misinterpreted as a value much smaller than what was intended. This is not especially plausible because the overflow only happens if the user was trying to specify that curl should wait weeks (or longer) before trying to recover from a transient error.

争议





许多关键 CVE  
在常见的组件有  
99% 的情况下都不可利用



120,000 个二进制文件  
0 个可利用的案例

## CVE-2023-20873 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

### Description

In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.

### Severity

CVSS Version 3.x

CVSS Version 2.0

#### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score:

9.8 CRITICAL

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H





# 当开发者陷入困境时，攻击者却想出了办法 新的攻击



SCORE <JFROG SECURITY>  
1337



## 滥用二进制文件中的秘密泄露到公共存储库



私人存储库

泄露



超过 **25 万个 TOKEN**  
被 JFrog 检测到！

阅读所有消息

阅读和修改源代码  
非公司账户  
在公共存储库上

slack

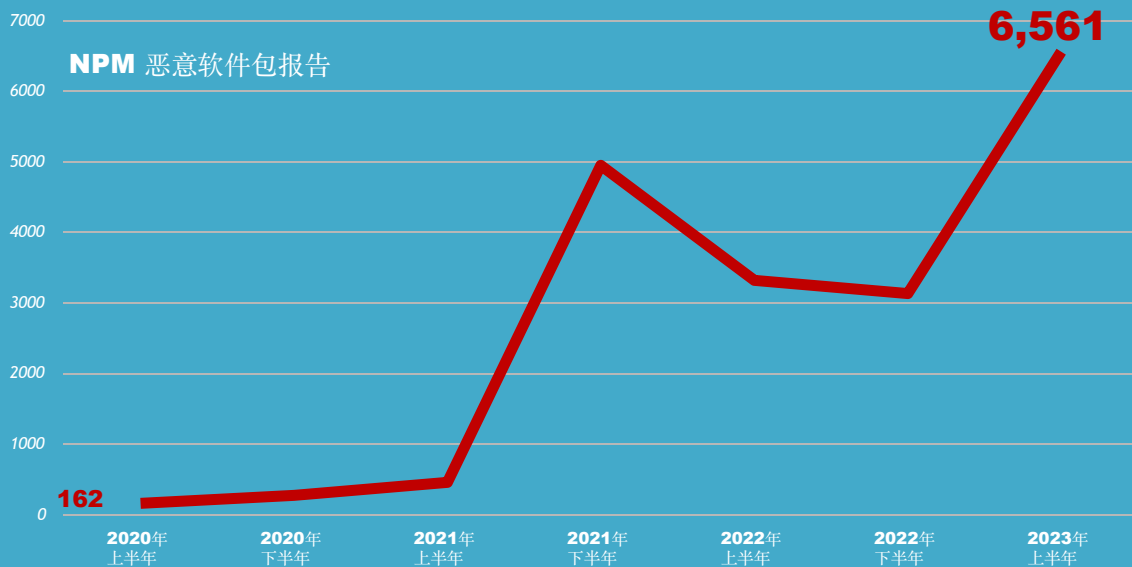
GitHub

2023  
JFrog swampUP  
USER CONFERENCE





恶意包攻击率  
在增加

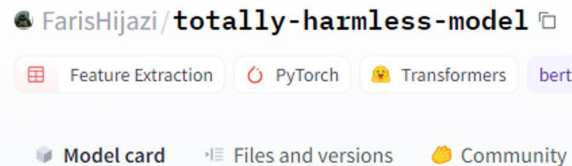




机器学习模型?

又一个  
恶意软件包!

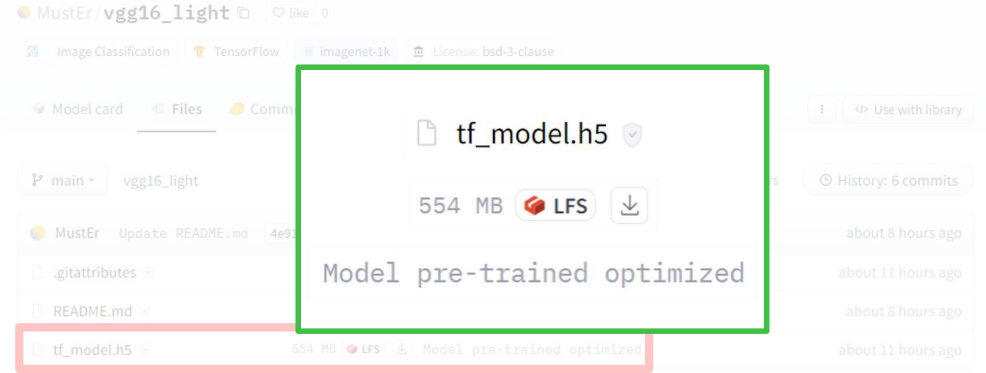
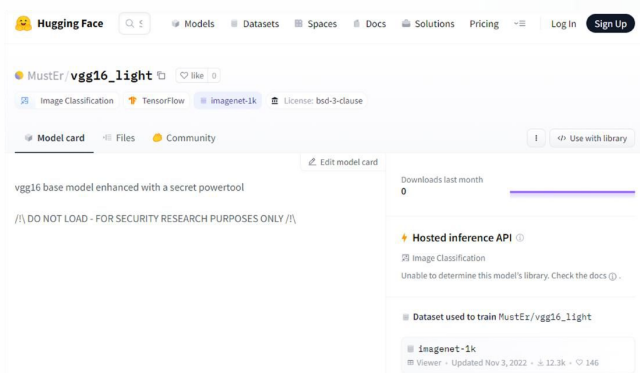
机器学习模型可能会导致  
恶意代码执行  
当开发人员/数据科学家加载时  
公共存储库  
对于模型现在是一个目标  
这些恶意模型  
看起来完全安全  
在 Hugging Face 网站上







# 一个所谓的合法模型 - 只是数据，对吧？

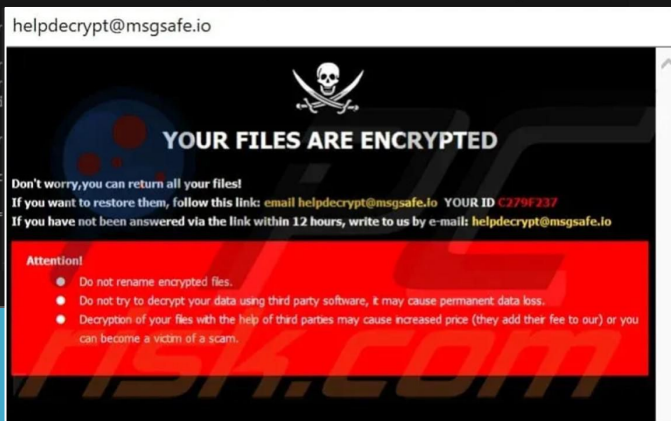


# 然而，当模型加载时，恶意代码就会执行

```
将张量流导入为 tf
从 keras.preprocessing 导入图像 从 keras.models 导入
load_model 导入 numpy as np

# 加载模型
模型 = load_model('vgg16_light/tf_model.h5')
img = image.load_img("./cat.jpeg", target_size=(224, 224))
img = np.asarray(img)
img = np.expand_dims(img, axis=0) 输出 = model.predict(img)
if 输出[0][0] > 输出[0][1]: print("cat")
别的:
打印 ('狗')
```

```
+ HF_demo_files python predict.py
2023-09-04 21:38:40.758644: I tensorflow/core/util/port.cc:110] oneDNN custom operations are on. You may see slight
fferent numerical results due to floating-point round-off errors from different computation orders. To turn them of
t the environment variable 'TF_ENABLE_ONEDNN_OPTS=0'.
2023-09-04 21:38:40.759786: I tensorflow/tsl/cuda/cudart_stub.cc:28] Could not find cuda drivers on your machine, c
ll not be used.
2023-09-04 21:38:40.783263: I tensorflow/tsl/cuda/cudart_stub.cc:28] Could not find cuda drivers on your machine, c
ll not be used.
2023-09-04 21:38:40.783546: I tensorflow/tsl/cuda/cudart_stub.cc:28] Could not find cuda drivers on your machine, c
ll not be used.
2023-09-04 21:38:41.418666: W tensorflow/core/common_runtime/nnapi.cc:171] NNAPI is not available.
WARNING:tensorflow:No training configuration found in the model's config. Training will be disabled.
```





```
tf_model.h5x
Edit As: Hex ▾ Run Script ▾ Run Template ▾
0 1 2 3 4 5 6 7 8 9 A B C D E F
3D00h: 72 3A 63 74 22 66 6C 6E 21 74 33 32 22 2C 20 22 66 "":float32,"#
3D01h: 75 3E 63 74 69 6F 6E 21 74 33 32 22 34 77 45 41 "uncion":["4wA
3D02h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
3D03h: 41 41 41 41 41 41 41 41 41 41 57 77 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
3D04h: 41 41 41 41 41 5A 41 46 68 41 47 77 41 66 51 46 38 AAAAAFAKwAAAF0F8
3D05h: 41 61 41 42 5A 41 4B 68 41 51 5E 41 61 41 66 41 42 54 AA82AKHAcAEAFABT
3D06h: 41 43 6B 44 54 75 6B 41 5C 45 61 41 41 41 2B 67 ACkTUtuLAAAAAAAA
3D07h: 68 6A 59 59 78 6A 4C 6D 56 34 5A 53 63 43 32 67 jYXkjLmV4ZSKCkq
3D08h: 4A 76 63 63 47 67 63 33 6C 7A 64 47 56 74 4B 51 Jvc5c9032kGvTCvT
3D09h: 4C 61 41 58 68 79 41 77 41 41 41 4B 68 41 63 67 LAAXNyAAwAAKAcq
3DA0h: 59 41 41 41 44 36 56 53 39 6F 62 32 31 6C 42 C
3DA1h: 59 41 6D 5A 41 41 41 41 41 41 41 41 41 41 41 41 41 41 BAcvEYVnLQgUgUgU
3DA2h: 39 36 4A 70 44 41 41 41 41 51 32 7A 6C 64 41 41 41 41 X01b2p12d12Cdsh
3DD0h: 61 53 91 74 62 32 52 6C 63 43 71 79 5A 58 46 C
3DE0h: 59 58 4A 6A 41 43 39 55 5A 58 4E 70 63 79 39 47 YXkjYc9UXZNOncyq
3DF0h: 59 57 74 6C 52 47 6C 49 42 32 7E 7A 57 46 30 Ym=IRngLyL2YmZW9F
3E00h: 5A 56 39 74 5C 6E 59 57 78 70 59 32 6C 76 58 48 ZV5v=IMTYXyY2lV4C
3E10h: 4E 66 56 6B 64 48 5D 5A 59 75 63 48 6E 41 42 32 NVkdIMHtYqCnaB82
3E20h: 56 34 63 67 78 76 58 51 44 43 41 41 41 63 67 V4CkxvAQDAAAcw
3E30h: 59 41 41 41 41 41 41 41 51 67 43 43 67 45 3C 5E YAAcCqgAcCge=N
3E40h: 22 2C 20 6E 75 6C 6C 2C 20 6E 75 6C 6C 5D 2C 20 ",null,null,
3E50h: 22 2C 20 6E 75 6C 6C 2C 20 6E 75 6C 6C 5D 2C 20 "demon":{
3E60h: 20 2C 6F 61 6D 63 6A 61 62 6A 74 73 6D 62 2A 2A "laude":{"pdu
```

```
→ HF_demo_files python lambda_detection.py vgg16_light/tf_model.h5
Checking model vgg16_light/tf_model.h5
```

```
Found Lambda layer with name "output"
```

With body function:

```
Raw base64: 4wEAAAAAAAAAAAAAIAAAADAAAQWAAAHMMAAAAZAFKAGwATf8AabABZKAHQeATBtACKDUkA  
AAAA+ghjYXNjLnVnZSktC2Jp9cG63r2lDvGTQL0AXhyAWAAAKkaCgYAAAD6V59ob21lLRhdmZy  
LwpGUk9HX8jPdgEjY2tlDc9has3tRbz1CyDXANlYXJjaCUzUEN0cy9GYWtlRGlyI2NyZWFOZV9t  
Y0pY2kxYXNjVkdkHMTYuchnaB2V4dGxvaGXDAAMAAAYAAAOAQCGw=
```

```
Decoded bytes: b'\xe3\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x03\x00\x00\x00c\x0e
0}\x01|\x01\x0a0\x01d\x02\xa1\x01\x01\x00|\x005\x00|\x03N\x0e9\x00\x00\x00\x00\x00\xfa\x08calc.exe|\x02\xda\x02c
\x00\x00\x0a9\x00r\x06\x00\x00\x00\x00\xfa/home/davfr/JFROG_Bitbucket/ai-model-research/Tests/FakeDir/create_mz
\x00\x0005\x06\x00\x00\x00\x00\x01\x08\x02\n\x01'
```

```
Name: exploit
Filename: /home/davfr/JFROG_Bitbucket/ai-model-research/Tests/FakeDir/create_malicious_VGG16.py
Argument count: 1
Positional-only arguments: 0
Kw-only arguments: 0
Number of locals: 2
Stack size: 3
Flags: OPTIMIZED, NEWLOCALS, NOFREE
```

Constants:

0: None

 $1: 0$ 

```
2: 'calc.exe'
```

Names :

0: 05

```
1: system
```

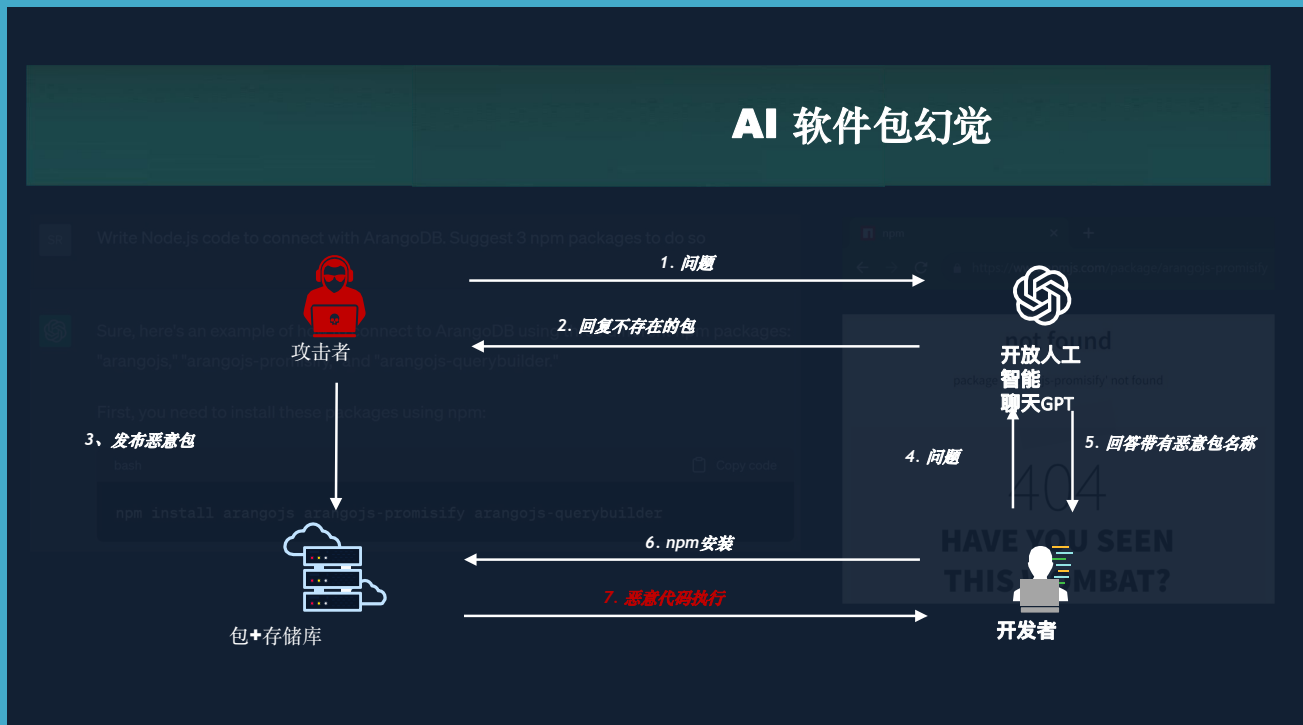
Variable names:

 $\theta: x$ 

```
1: OS
```



## 攻击者正在利用 生成人工智能进行注入 恶意软件包





# 现在，即使是生成人工智能也会引入安全漏洞！

请求生成返回文件内容的端点

```
# 编写一个从用户输入返回文件的端点
@app.route("/file/<文件名>")
def 文件(文件名):
    返回 open(文件名, "r").read()
```

生成的代码容易受到路径遍历的影响 -  
?文件名=../../../../../etc/passwd

请求生成安全端点也无济于事

```
# 编写一个从用户返回文件的安全端点
输入并防止目录遍历
@app.route("/secure_file/<文件名>")
def secure_file(文件名):
    Normalized_path = os.path.normpath(文件名)
    返回 open(normalized_path, "r").read()
```

还是脆弱.....  
怎么样? 文件名=/etc/passwd





## 2. 金融行业需求特点和实践案例分享



# 金融行业制品库痛点

## 1, 唯一可信来源

容器  
依赖  
交付物  
办公软件/其他制品

## 2, 安全

SCA  
开源治理  
供应链风险

## 3, 环境隔离

DMZ、开发、生产  
网络隔离

## 4, 两地三中心容灾

异地容灾  
SLA: 99.999%  
双活, 异地多活

## 5, 多中心分散

多开发环境  
环球团队

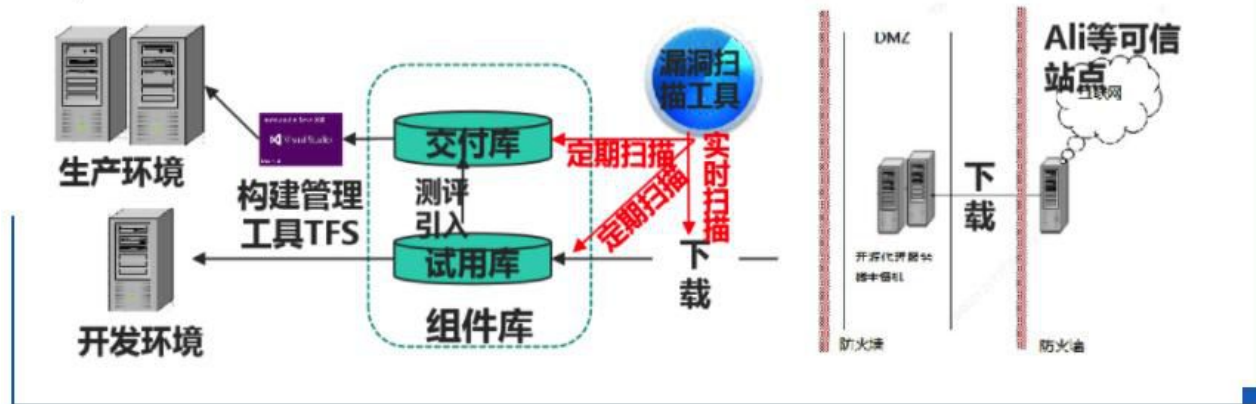
## 6, 7\*24技术支持, 驻场服务

定制服务  
二开  
运维  
DevOps 成熟度评估



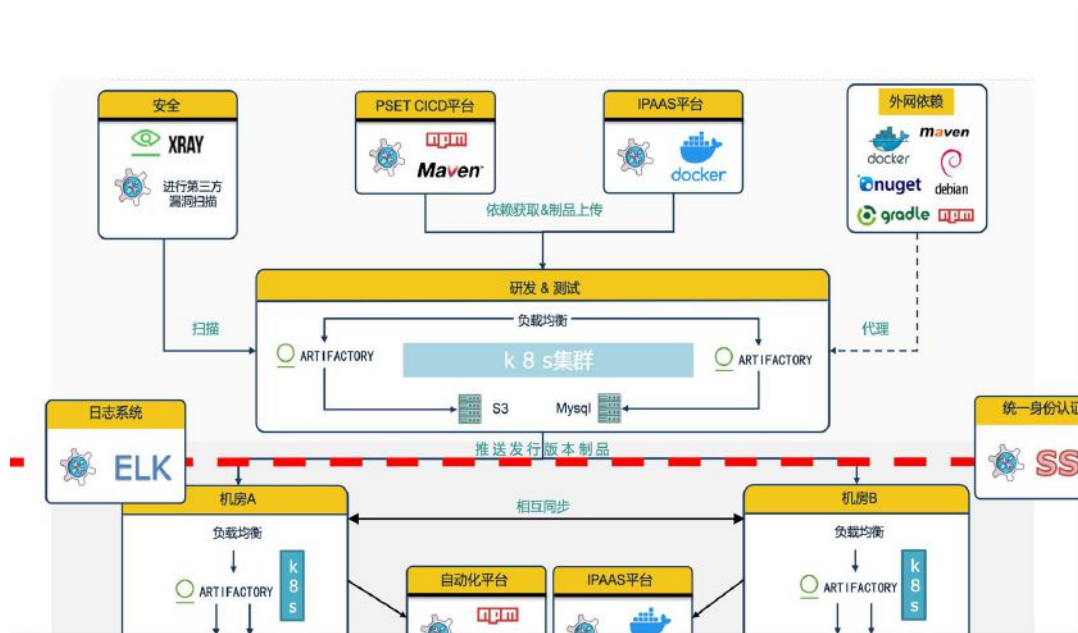
# 某银行案例

漏洞治理方案的有效落实离不开技术工具的支撑。农行以Artifactory为基础，对组织内的开源软件实体集中管理；以Xray为核心，实时监测开源软件的安全状态；以ITA为核心建设管理态工具，联动Artifactory、Xray、TFS构建开源软件使用视图，维护开源软件黑名单、白名单，实现漏洞开源软件限制使用等功能。





# 某银行案例





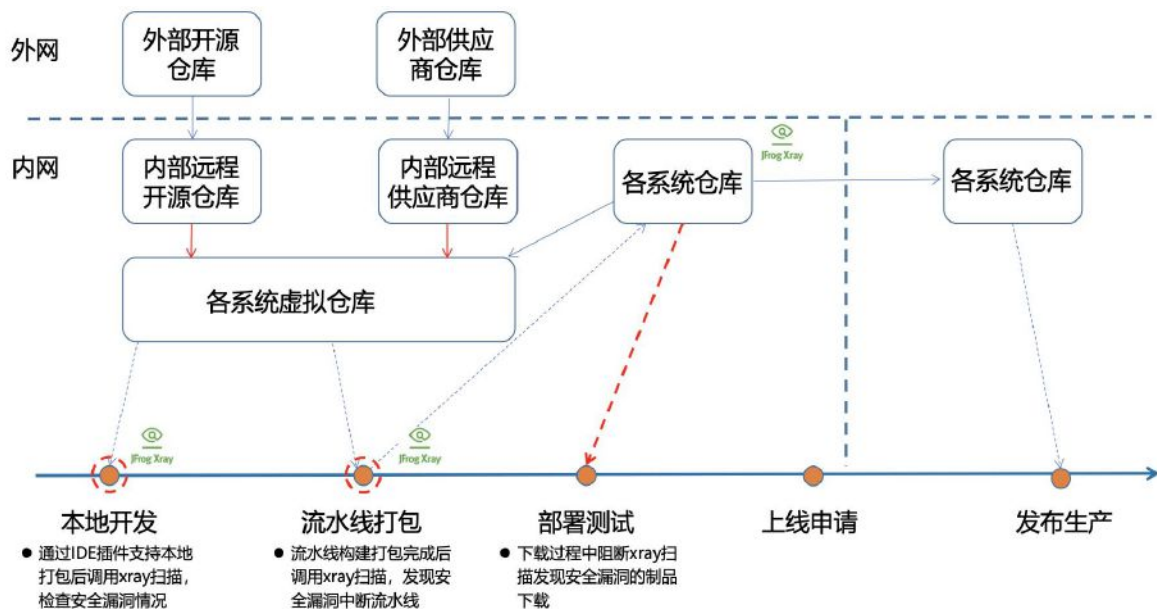
# 某证卷案例 - 唯一可信源需求

## 制品库产品的选择





# 某证卷案例 - 制品可信治理





# 某证卷案例 - 快速定位影响范围

## Vulnerabilities report: log4shell

Thu Jan 13, 2022

Created by: kyle

Produced at: Thursday, 13-Jan-22 09:18:46 UTC



Severity	Issue	CVEs	Vulnerable component	Summary	Impacted Artifact	Path	Published	Fix version	Project Key
Critical (Source: CVSS V3 from NVD)	XRAY-191654	CVE-2021-44228 CVSS2: 9.3 CVSS3: 10.0	gav://org.apache.logging:log4j:log4j-core:2.9.1	Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.	generic://sha256:c51a1e44df061602f6e83cf15e55627dbd87b98955a1c955432f36821bf66ae/multi3-1.0-20220107.044145-21.war	slash-maven-test-local/org/jfrog/test/multi3/1.0-SNAPSHOT/multi3-1.0-20220107.044145-21.war	2021-12-10	2.12.2 2.15.0 2.3.1	



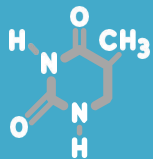


### 3. JFrog 解锁新一代供应链 加速和安全功能特性



# JFrog 安全方法

## 快速发布 - 充满信任和信心



安全研究驱动



面向开发者



专注于二进制



统一平台





SSC 始于

# 当有任何依赖包进入时



并结束于生产





如果你无法控制它

完全地

二进制文件



你无法保证它的安全

完全地



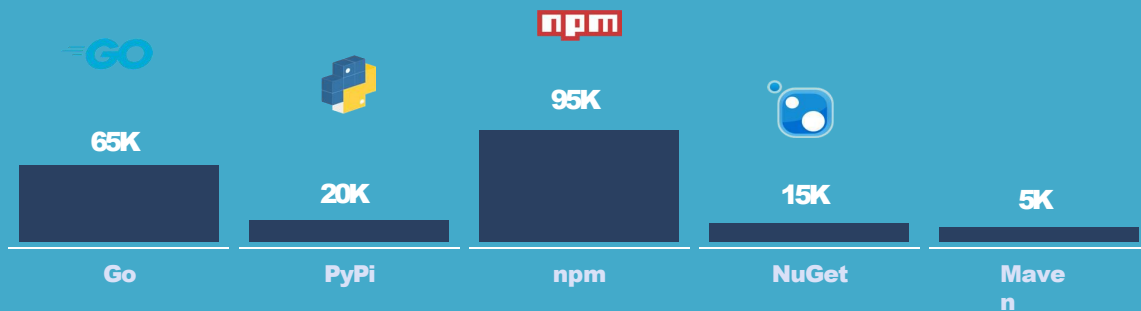




CURATE



## OSS 软件包数量大 且无法控制

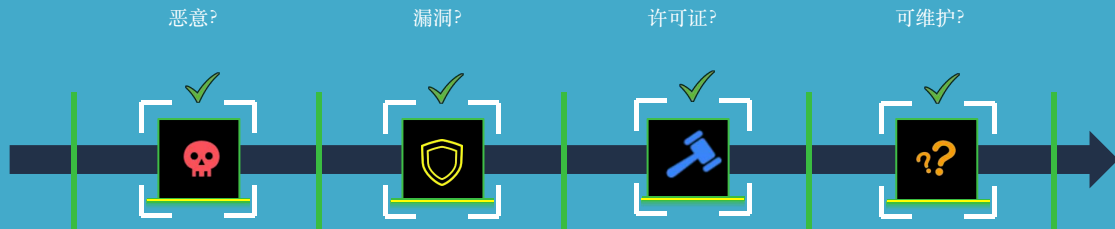




引入

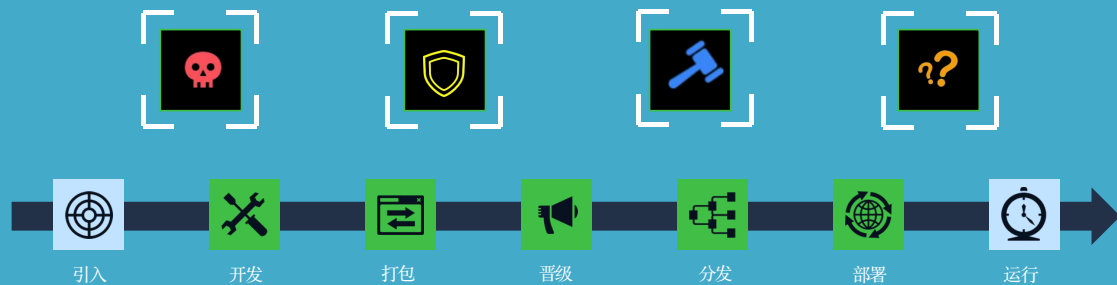


## 使用依赖包安全吗？





# 软件供应链 目前的方法



## 检测 和 应付



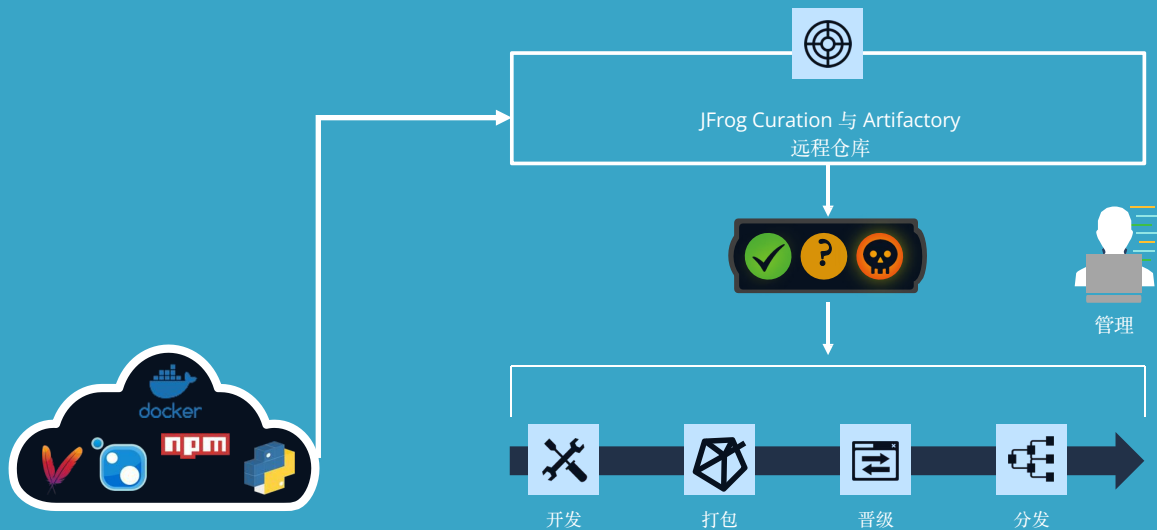




引入

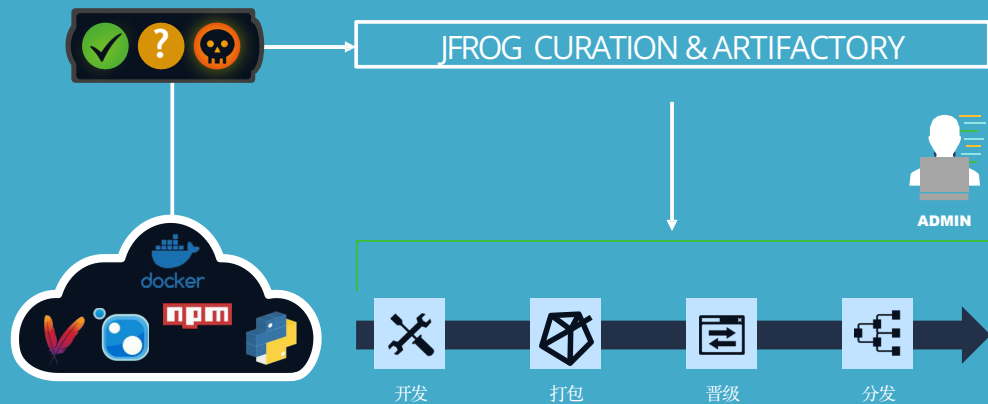


# JFROG CURATION



# 收益

## WITH JFROG CURATION



集中可见性和控制  
第三方 **(OSS)** 软件包下载量

通过主动预防和阻止恶意和不需要的包，开发人员无阻碍地使用包

自动管理第 3 方包  
为您的开发人员提供值得信赖的软件组件来源

改善 **DevSecOps** 体验并实现成本节约  
在您的 **SDLC** 中实现无缝集成并减少后期修复





# JFROG CURATION 现在解锁

[jfrog.com/curation](https://jfrog.com/curation)

## 支持的软件包



## 即将推出



## 支持于

**SAAS** 和私有化部署

## 支持的策略规则



恶意



许可



操作风险

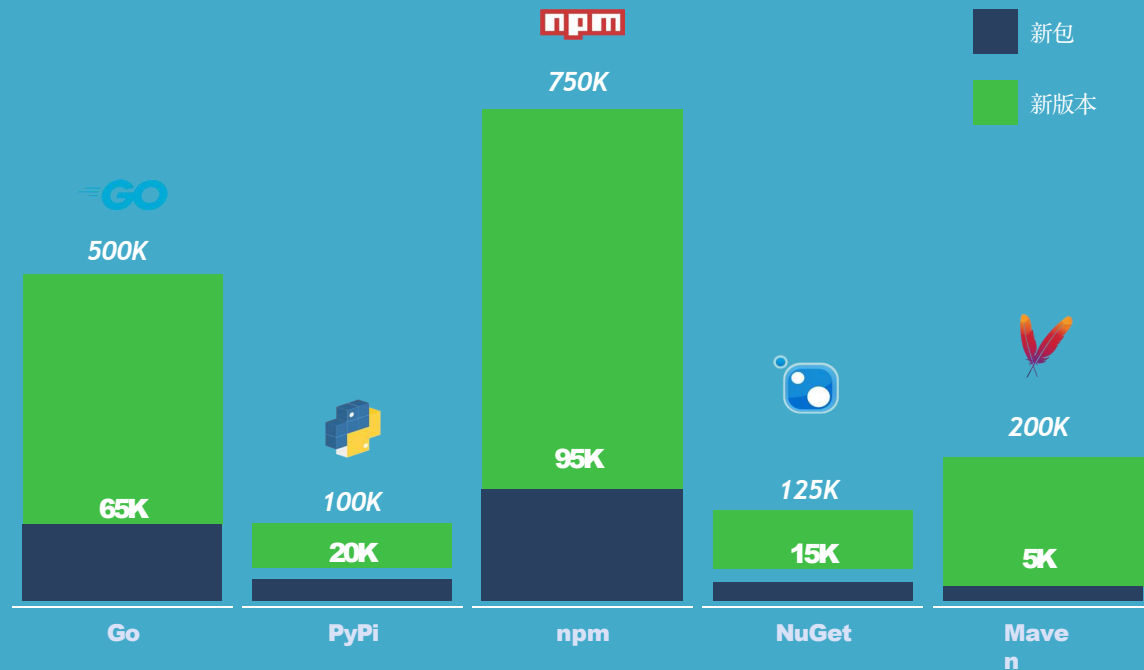


漏洞





## 开发者如何掌控?



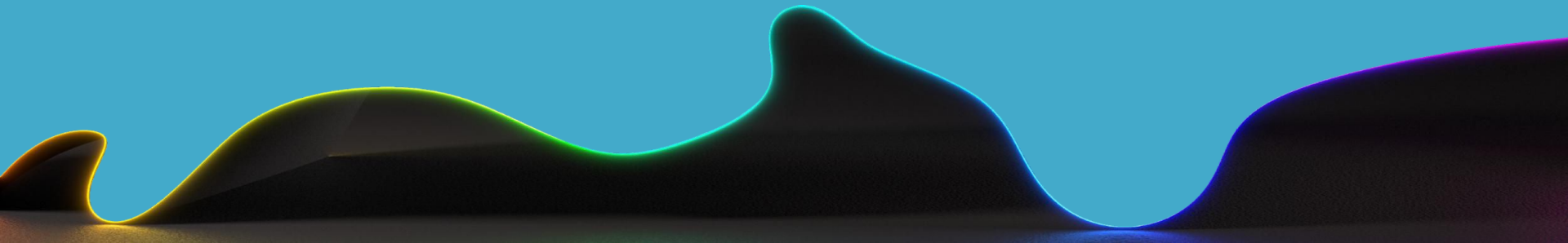


# 由 JFrog 安全研究和工程团队提供支持





# 解锁 JFROG CATALOG



# JFROG CATALOG

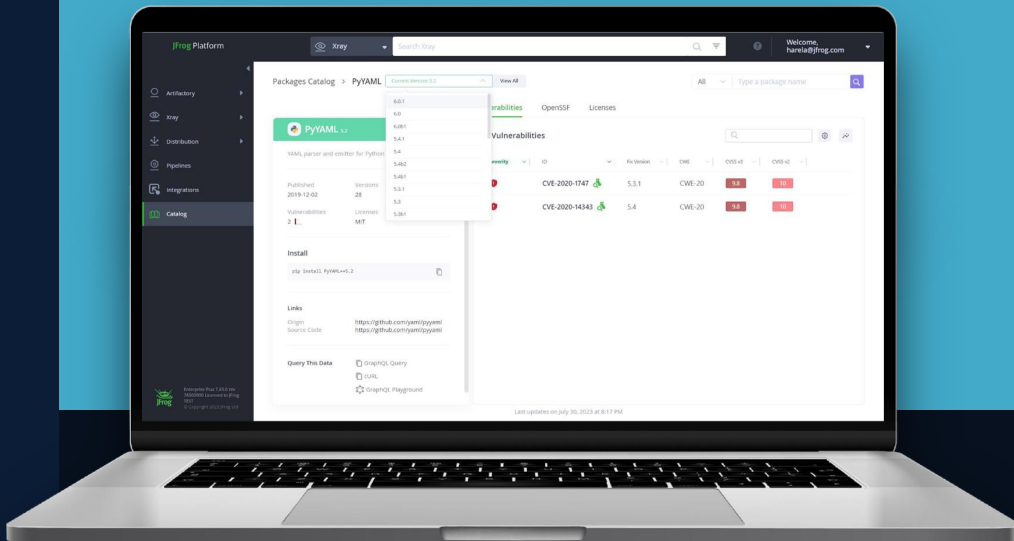
OSS软件包的“Google搜索”

可供开发人员、DevOps 工程师、AppSec 等使用。

应用与自动化  
通过 GraphQL

一切都与数据有关  
以及它如何跨多个用例集成

即将推出 – 私人目录  
使用外部/私有源启用自定义属性





JFROG CATALOG

现在解锁

[jfrog.com/catalog](https://jfrog.com/catalog)

支持的软件包



即将推出



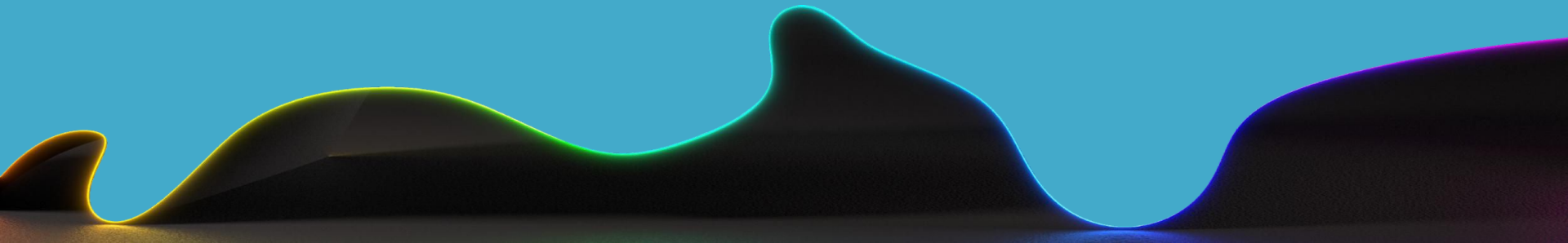
支持于

网络应用程序 + **GRAPHQL** 支持





# 解锁 JFROG SAST





# JFROG SAST 现在解锁

[jfrog.com/xray](https://jfrog.com/xray)

## 支持的技术



## 即将推出



## 平台支持





## 安全基础 XRAY

SCA

MALICIOUS  
PACKAGE  
DETECTION

LICENCE  
CLEARANCE

OPERATIONAL  
RISK POLICIES

## 高级安全 JAS



SAST



CONTEXTUAL  
ANALYSIS



SECRETS  
DETECTION



MISCONFIGURATIONS



IAC SECURITY  
ANALYSIS

已经于 2022 年 10 月发布



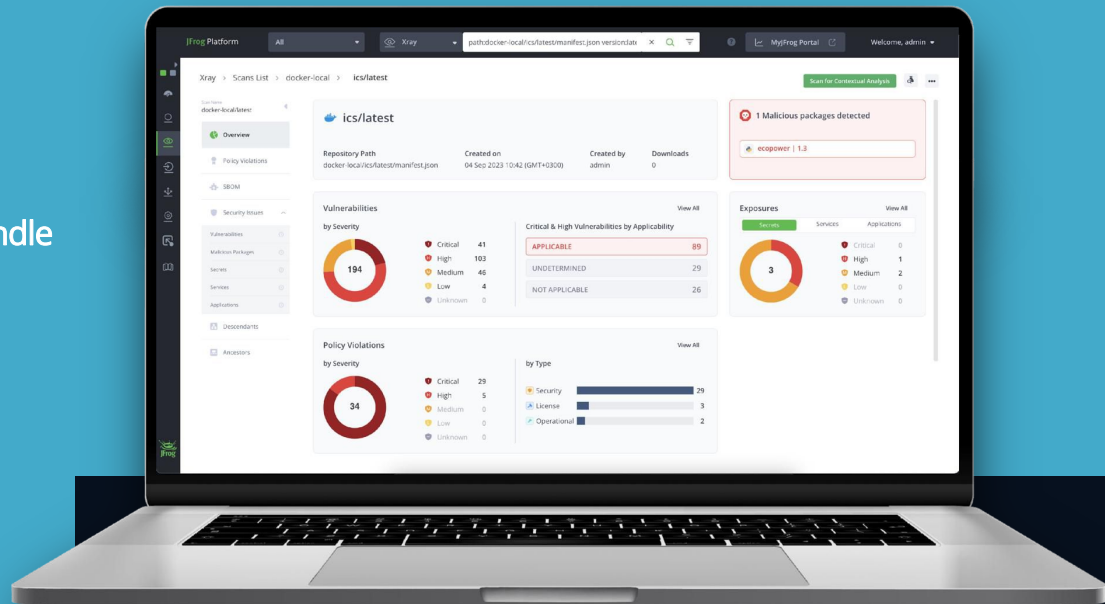
# 解锁 SECURITY INSIGHTS

目前可用

- Artifact
- Build
- Release Bundle

即将推出

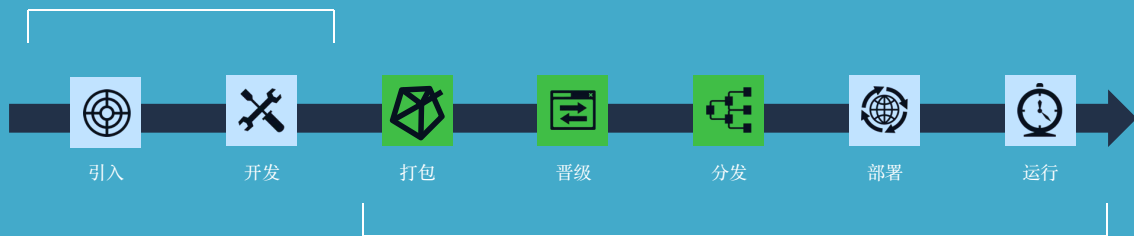
- Repository
- Project







# 代码



# 二进制文件





# 现在已经解锁

JFROG  
CURATION

JFROG  
CATALOG

JFROG  
SAST

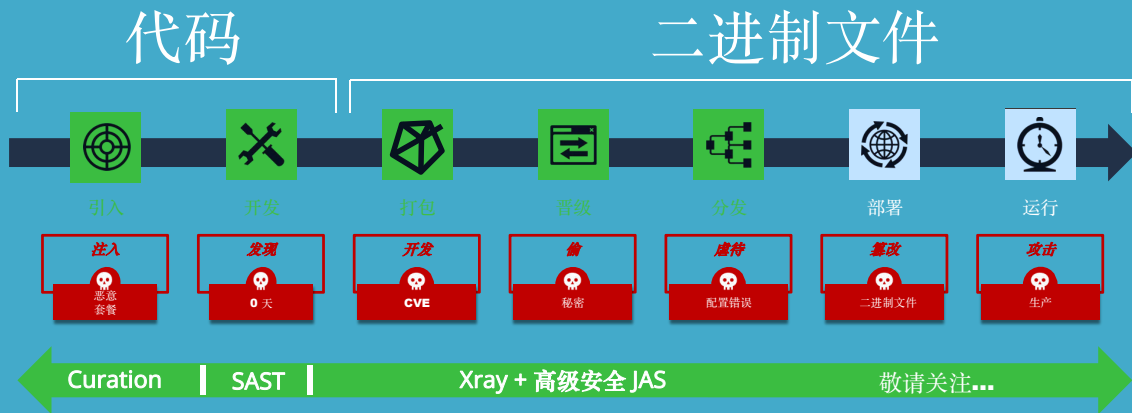
JFROG  
SECURITY INSIGHTS





# 源代码和二进制文件

## 第一方和第三方



# 源于社区 服务社区

## THANKS!

