



GOPS 2020  
Shanghai

# GOPS

2020 全球运维大会  
- AIOps 风向标



指导单位：



主办单位：



大会时间：2020年11月27日-28日

大会地点：上海中庚聚龙酒店



# 碎片化运维场景下的DevSecOps实践

龙凡 腾讯游戏 运营安全负责人



# 龙凡

腾讯游戏 运营安全负责人

10年腾讯游戏运营安全工作经验，负责了多个重要安全项目建设，涉及游戏运营风险审计、数据安全、应用安全、身份与访问管理等多个安全领域。

CONTENTS

# 目录

①

背景

②

历程

③

现状

④

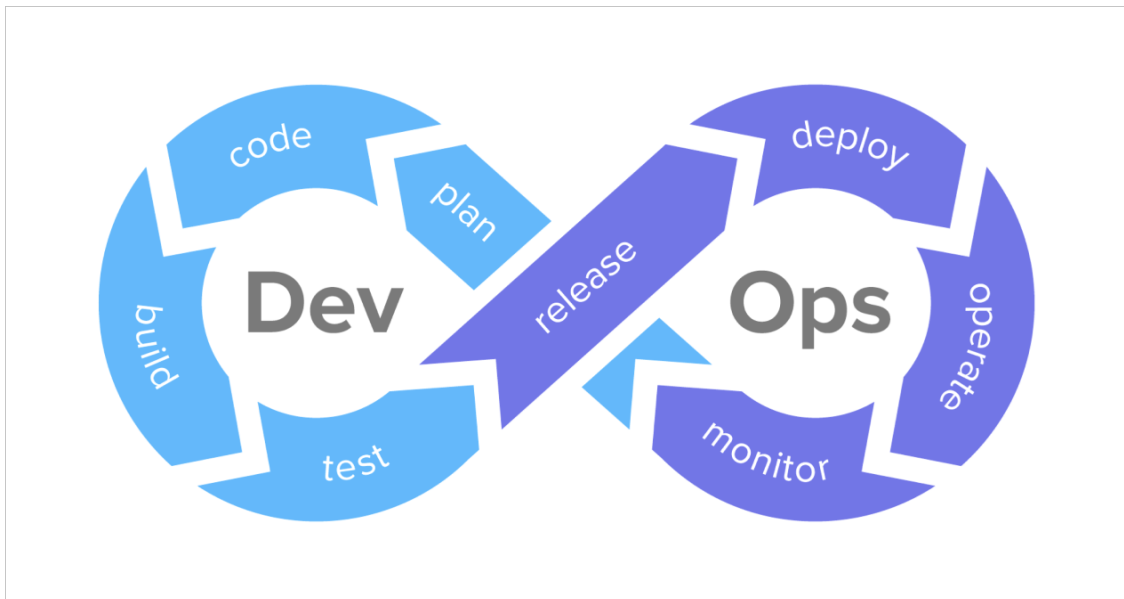
展望



# 背景



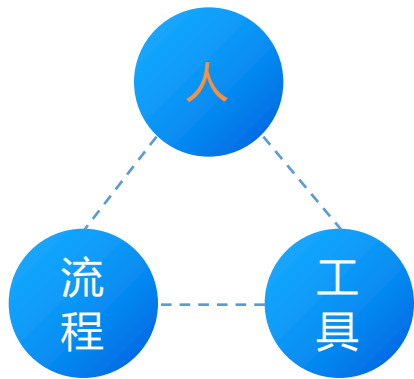
# 一个观点：碎片化运维操作难以消除



- **碎片化操作**：指无法完全通过自动化完成的运维操作，比如测试环境代码调试、现网环境故障排查等；或者在将手工操作转换为自动化过程中需要进行的操作



# 一个原则：DevSecops实施的关键是适应用户



## 12 Things to Get Right for Successful DevSecOps

Published: 19 December 2019

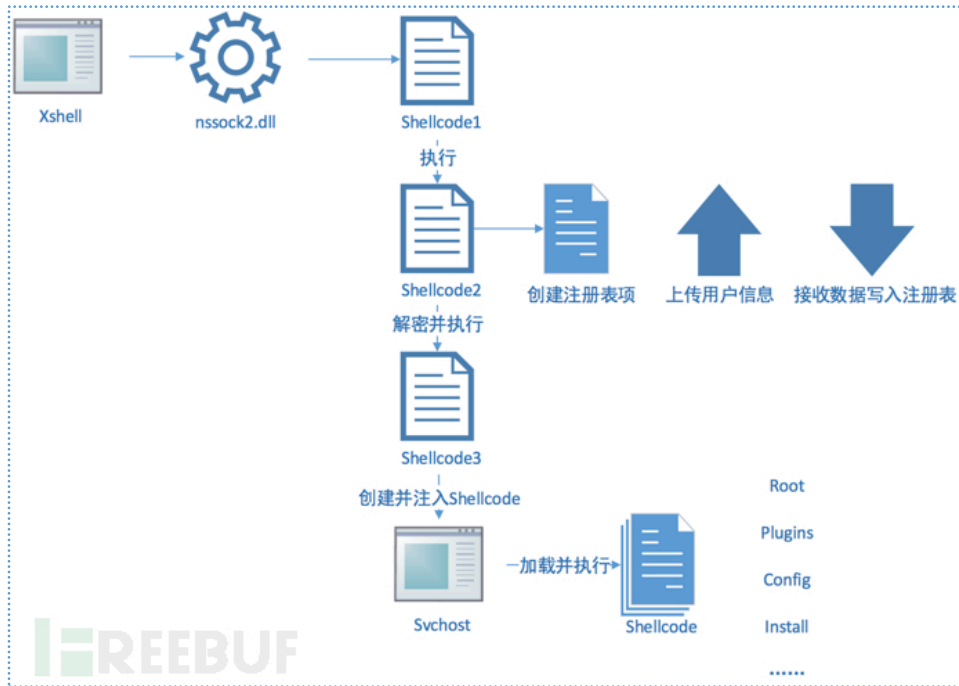
ID: G00450792

### Analysis

- Adapt Your Security Testing Tools and Processes to the Developers, Not the Other Way Around



# 一个风险：供应链攻击防不胜防



tombkeeper

10-12 11:56

2012 年，putty、WinSCP、SSH Secure 等软件的汉化版被植入后门。

2017 年，XShell、Xmanager 官方发布版被植入后门。

所以，TeamViewer 这事儿可不新鲜，未来一定还会发生。

对大多数人来说，面对远程访问软件的官方发布版被植入后门这种威胁，没有太好的办法。唯一可行的应对措施是：除非有严重漏洞，否则别随便升级。

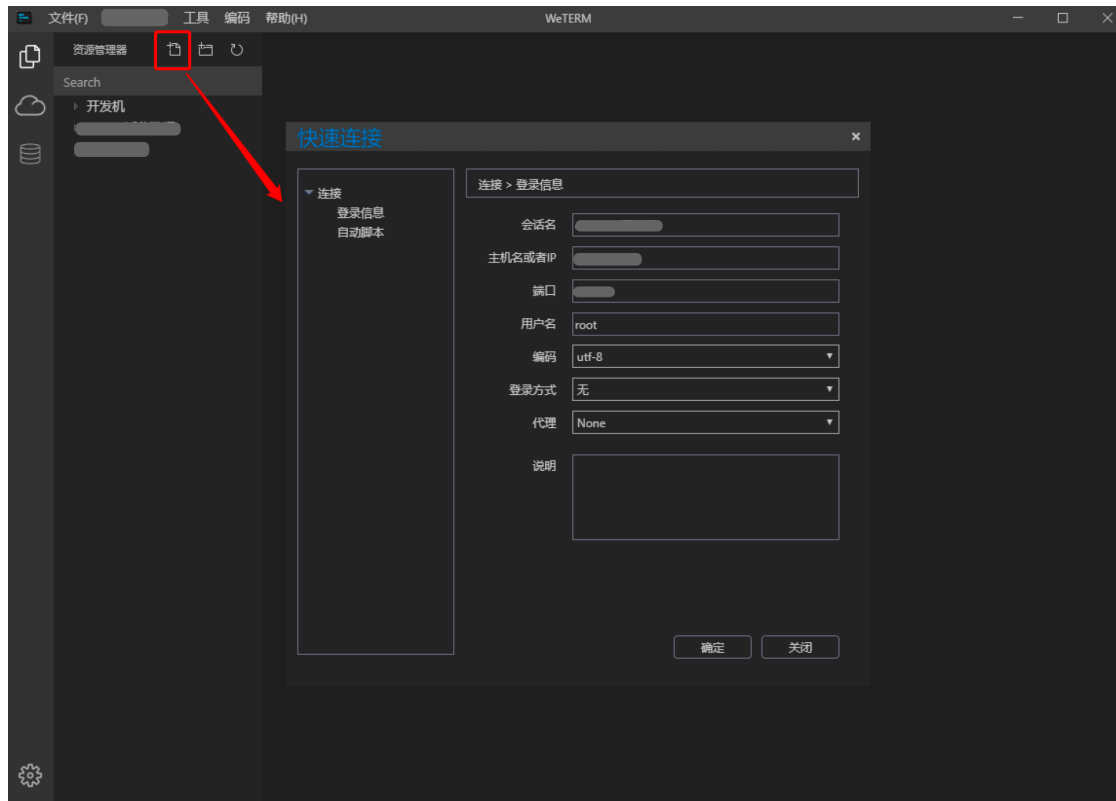




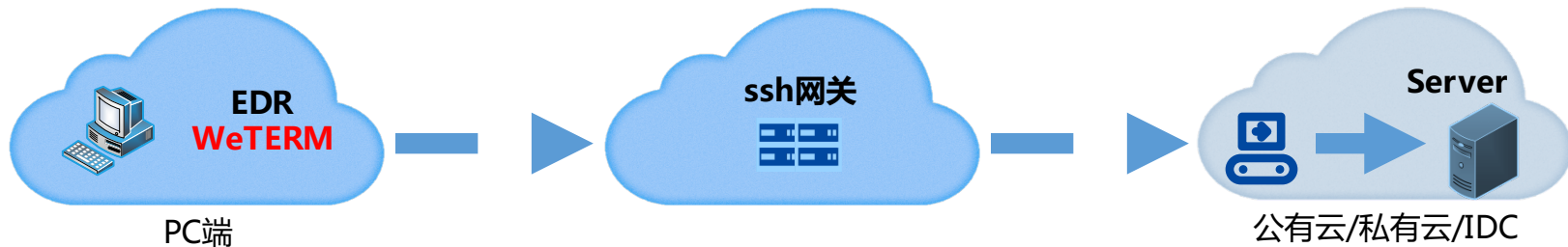
# 历程



# 从一个ssh工具开始-WeTERM



# 场景一：服务器安全的结合-零信任



✓ 可信ssh客户端

✓ 身份传递



## 场景二：应用安全的结合-软件部署

【安

作者：七夜

近日，  
库，所  
在此建

0x

11月1  
木马、

分享

于PyPI官方仓  
的原则，TSRC

侵，并实施种植

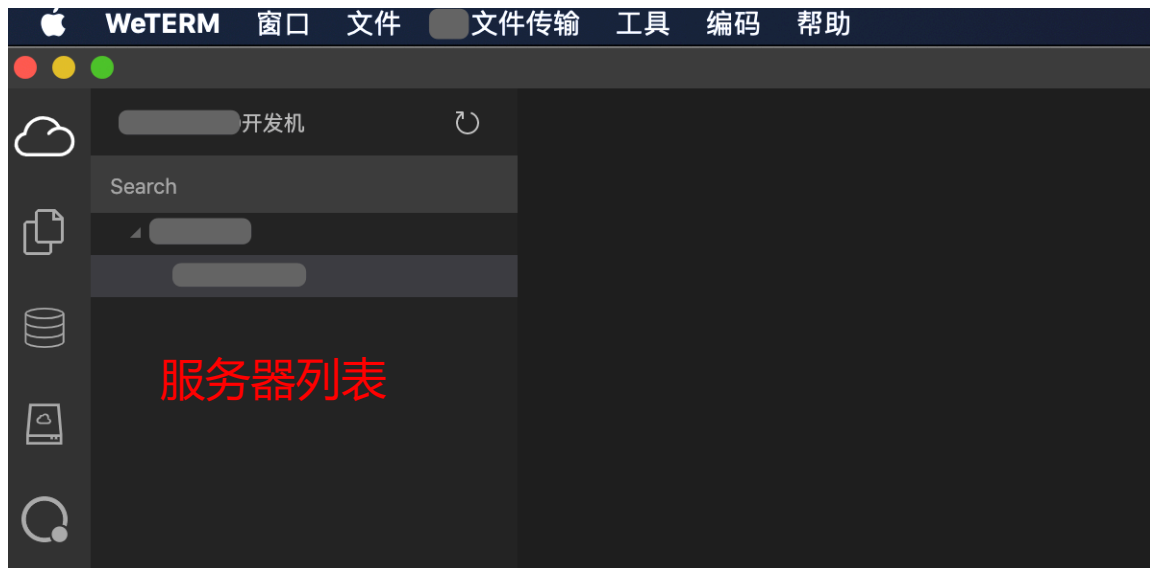
正常 covid 包的功能是获取约翰斯·霍普金斯大学和worldometers.info提供的有关新型冠状病毒的信息，每天的安装量上千次。在新冠疫情在世界流行的大背景下，covid包因输入错误的包名而被安装到系统中，covid包的数量将会不断增加。

✓ 可靠软件源

✓ 交互简化



## 场景三：效率提升的结合-资源申请



✓ 流程串联

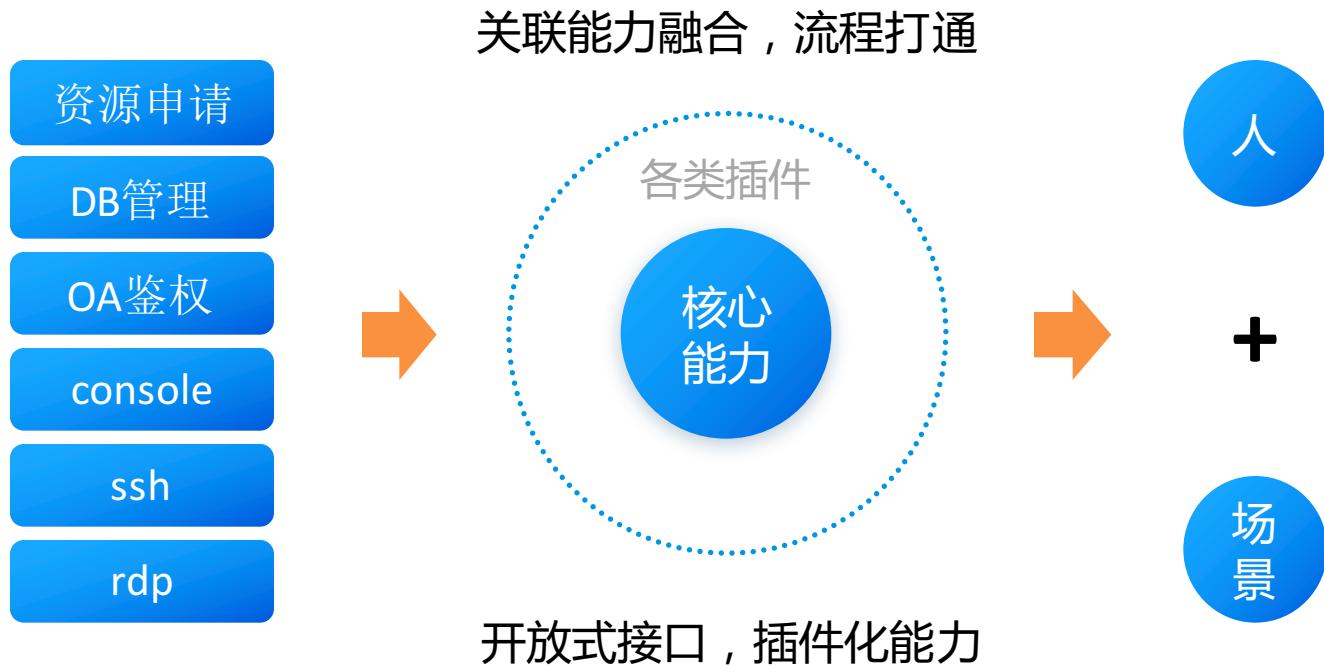
✓ 用户体验



现状




# 从工具到连接器的进化









# 收益，不仅限于安全

- 
- 结合网关能力的零信任服务器安全
  - 组件安全、终端工具安全

- 
- 免密登录
  - 复杂命令的前端简化
  - 常用脚本、代码的保存及分享
  - 多种自定义功能



- 
- 不同环节的流程打通
  - 服务器间传输文件
  - 开发服务器环境自动配置
  - 本地PC脚本、配置等同步

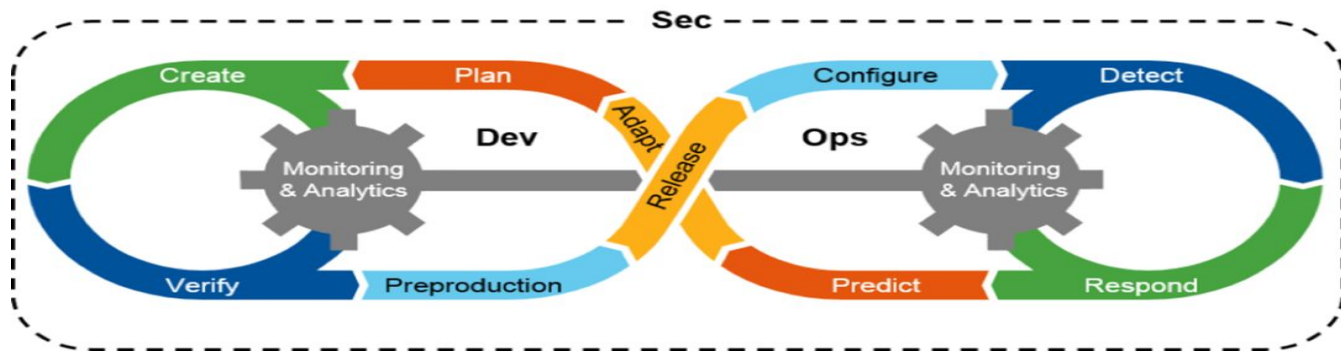
- 
- 节省商业终端工具授权费用



展望



# DevSecOps架构下的探索



碎片化操作 + DevSecOps



- 安全覆盖
- 流程连接
- 内嵌

# 期待后续的交流



公众号：腾讯游戏运营安全



龙凡个人微信号



# Thanks

高效运维社区  
开放运维联盟

荣誉出品