Face the challenge,Embrace the best practice

EISS-2021
企业信息安全峰会

北京站

2021.04.23
BEIJING，CHINA

安世加

云环境安全检测挑战与机会

江 虎

腾讯数据安全架构师

2021.5.14

安世加

自我简介

- 江虎
- 腾讯数据安全架构师
- 《互联网企业安全高级指南》作者之一
- 一线大厂十多年安全从业经验
- 专注入侵检测、取证、攻防技术研究

安世加

目录

安世加

云环境-攻击面

Overlay

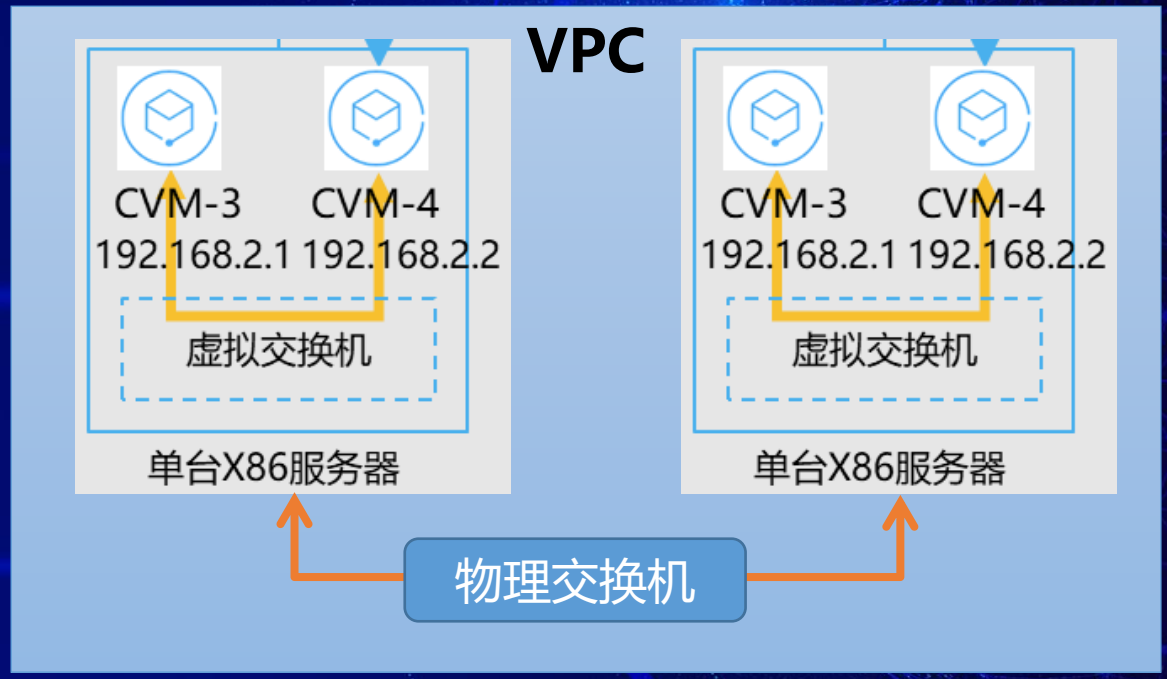
- 业务
  - PaaS\SaaS\FaaS...
- 云控制台
  - API
- 混布
  - Vpc\kvm\docker

Underlay

- 宿主机\物理机
- 裸金属
  - 智能网卡
- 网络设备
  - 可编程交换机
  - ...

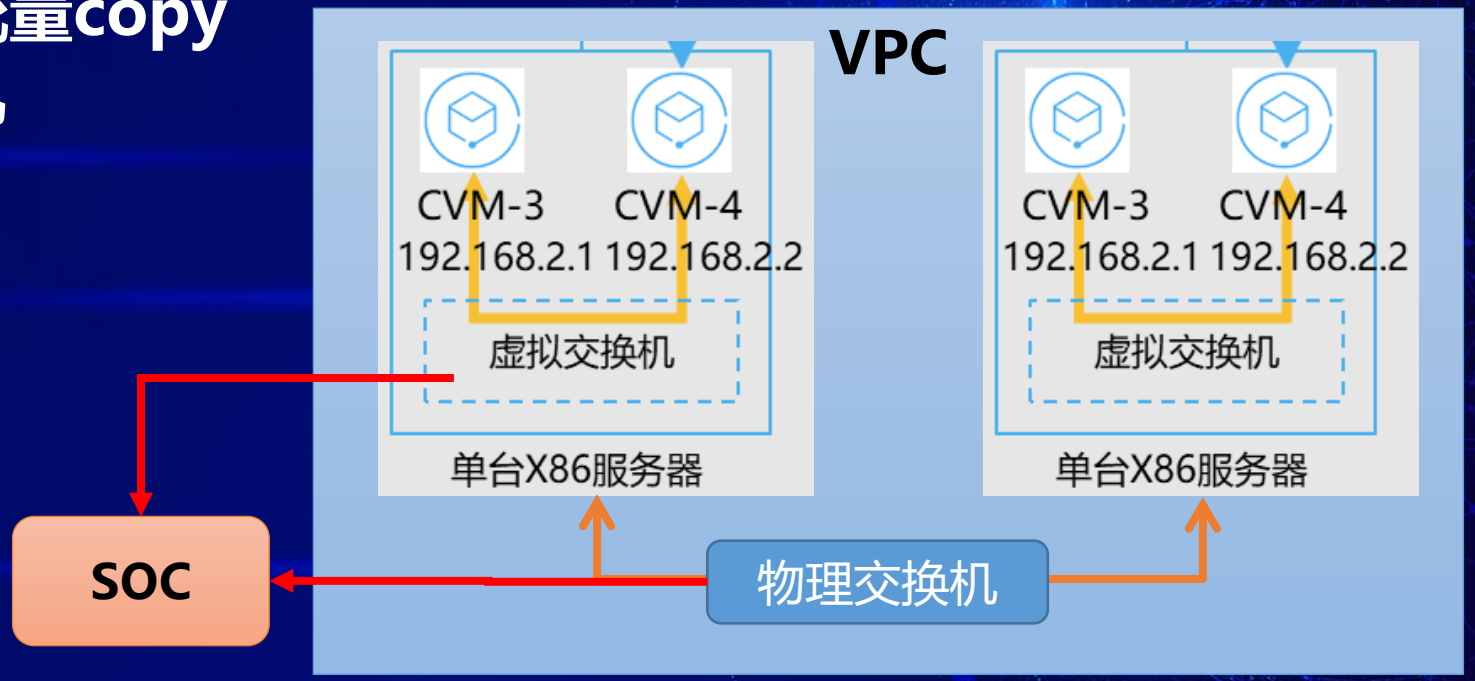
模糊的网络边界

- 传统的流量安全产品部署在机房出入口
- 云架构混布下的流量监测盲点
  - 同城VPC之间
  - 同VPC的CVM之间
  - 流量转发\隧道\“代理”



更细粒度的东西向流量监测

- 传统的流量安全产品+智能网络设备流量转发
  - 同宿主机-**裸金属设备流量copy**
  - 同城VPC-**可编程交换机**



四顾不暇的EDR

容器

- 轻量
- 生命周期短

非标物理机\虚机

- 非标系统
- 各类版本kernel

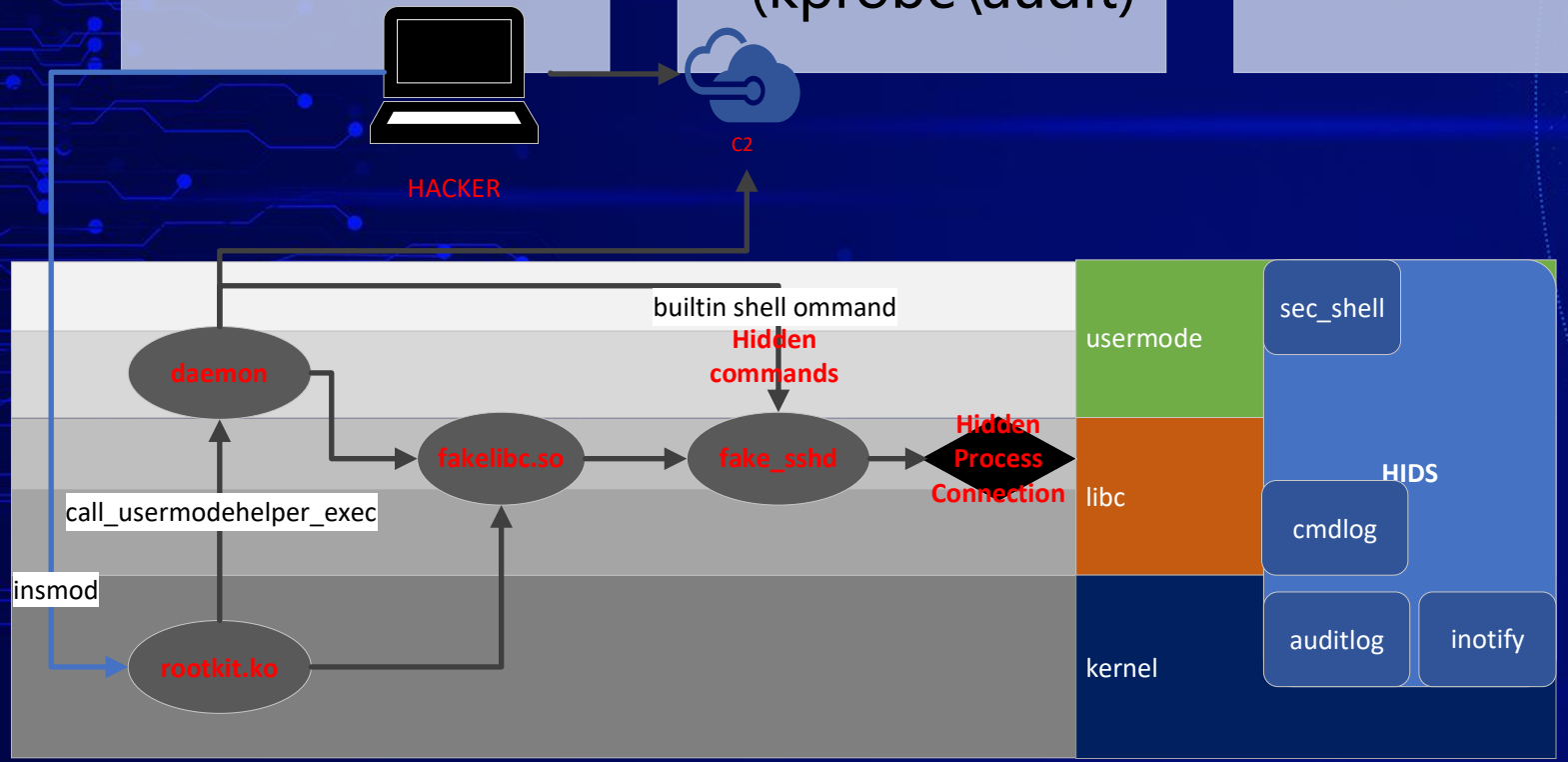
智能网络设备

- 可编程交换机
- 智能网卡

安世加

全栈主机EDR

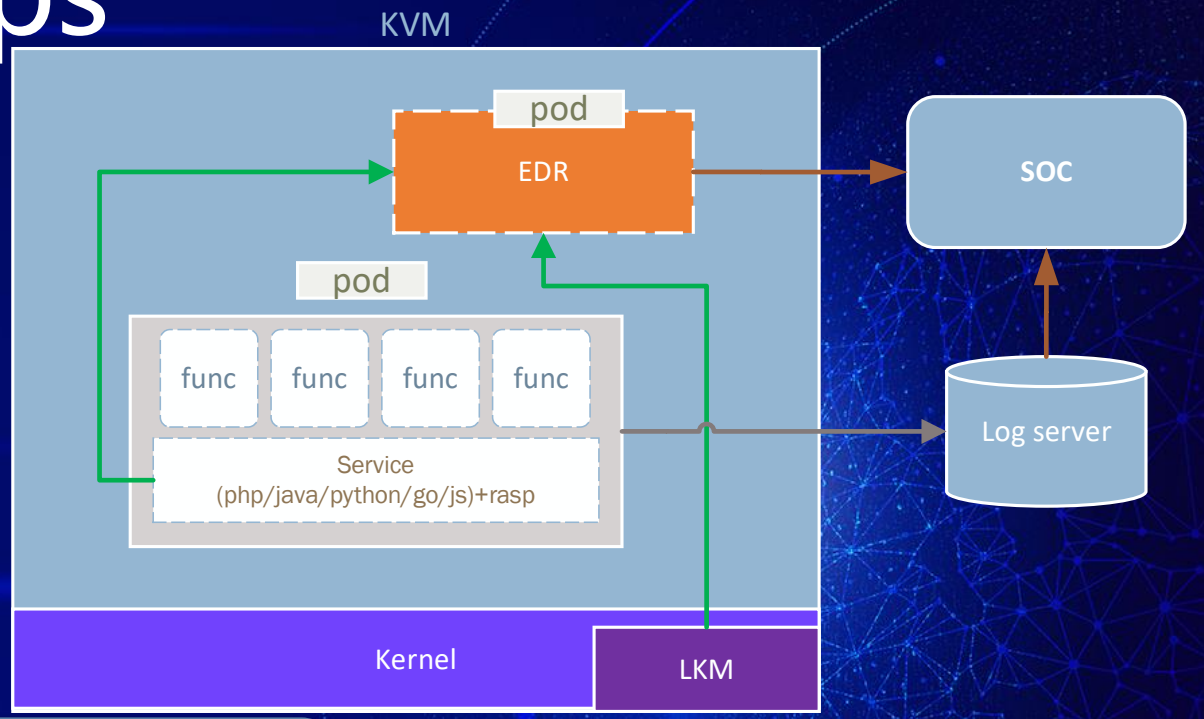
智能(网络)设备	非标物理机\虚机	容器
• 多平台版本支持	• 兼容性较好的内核方案(kprobe\audit)	• 云原生 • 容器化部署



更敏捷（碎片化）的应用发布

Serverless+devsecops

- IAST代码安全扫描嵌入发布流程
- Soar+DAST
- Docker(image\file)+RASP



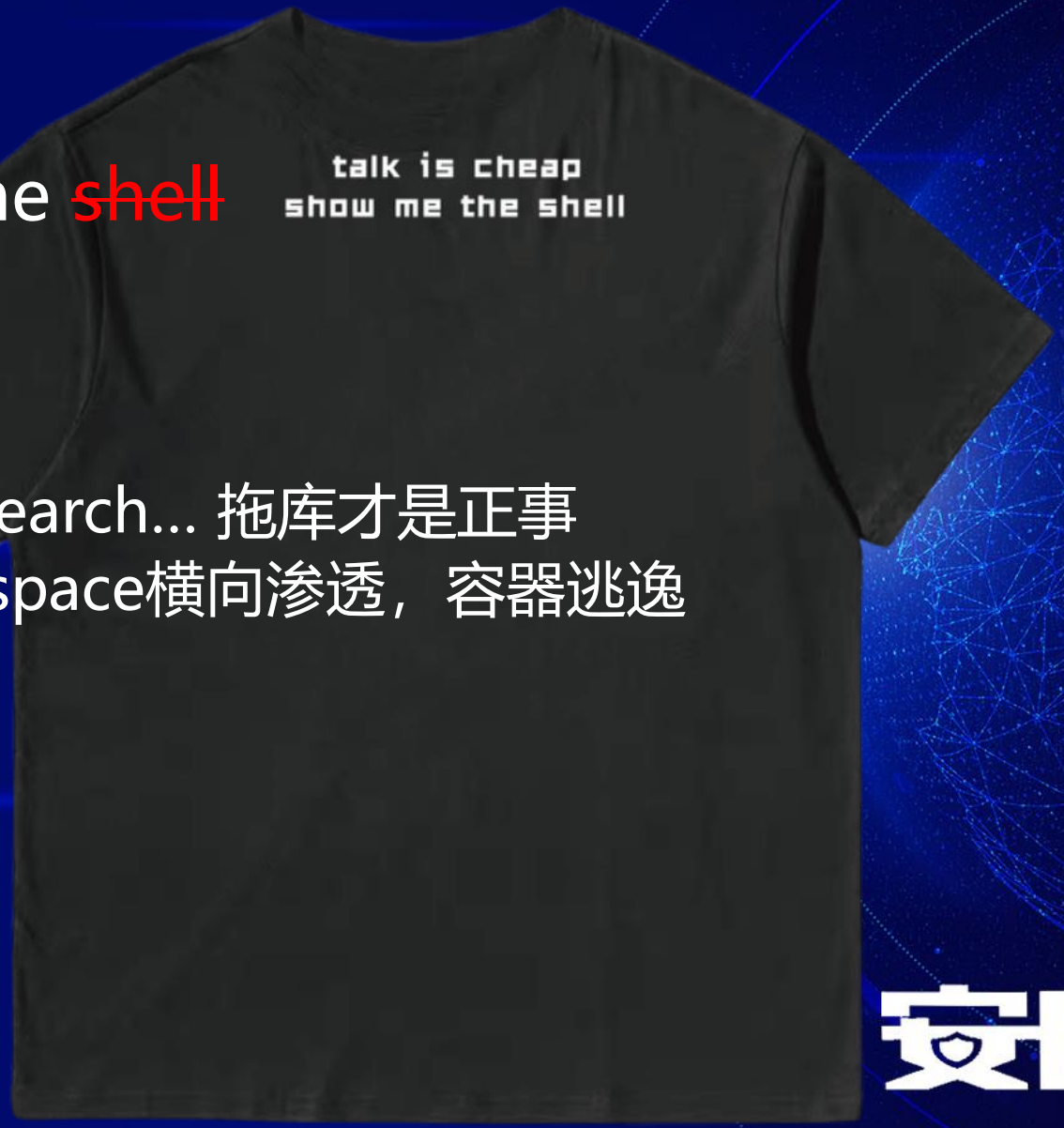
Devsecops

Kona JDK

DAST&SAST	IAST	RASP+onionEDR	+soar
安全左移	默认安全	运行时安全	安全服务自动(助)化

攻防维度下沉

- Talk is cheap,show me the ~~shell~~
  - AK\SK
  - Environment，AK\SK
  - Kubecongfig，AK\SK
  - API，redis\mysql\elasticsearch… 拖库才是正事
  - Namespace，k8s同namespace横向渗透，容器逃逸
  - …



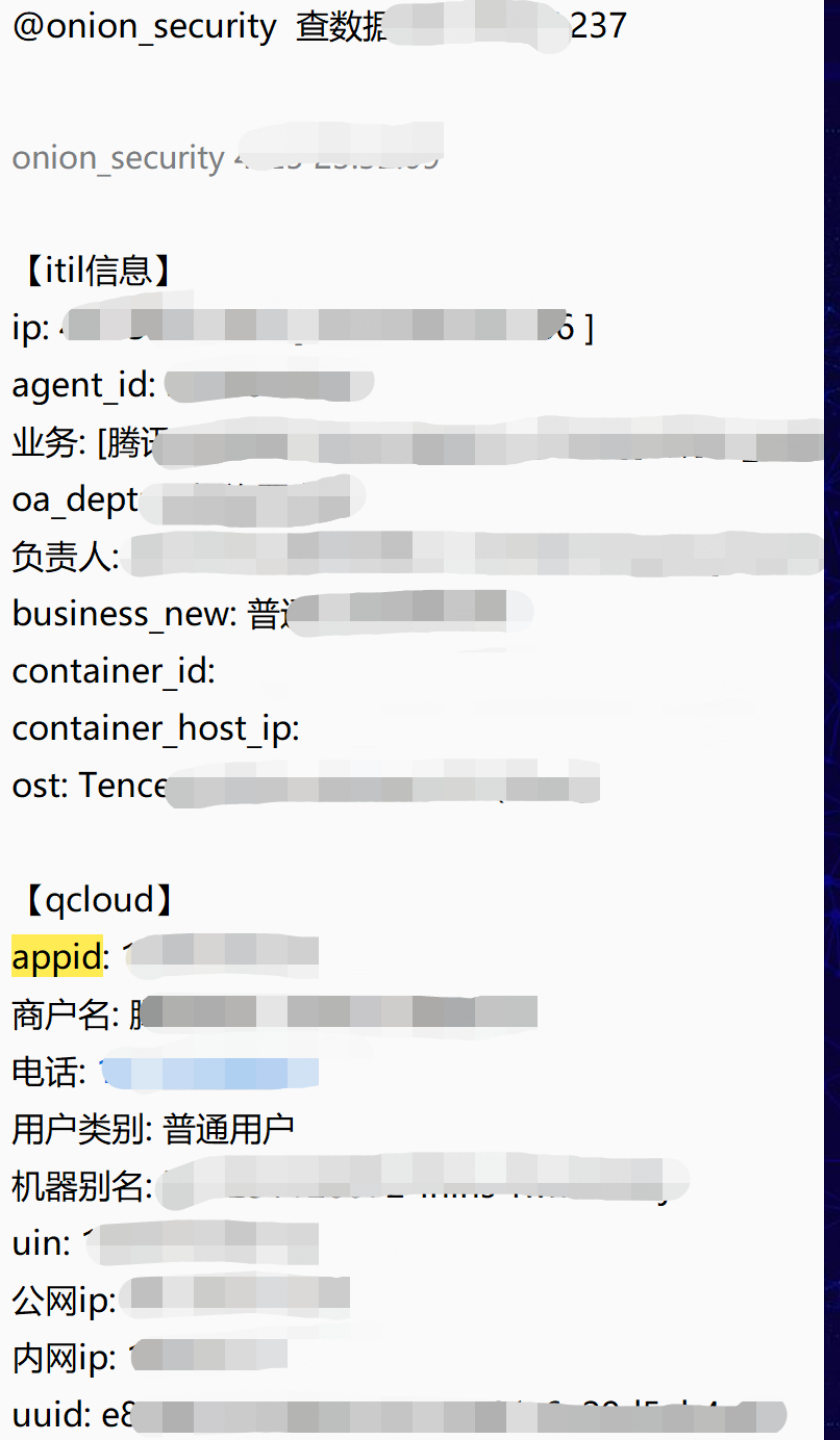
PaaS\SaaS\FaaS维度的战场

- 云环境 ‘fileless’ 攻击
  - 没有木马
  - 没有webs hell
  - 不需要也不存在**持久化**
- 云上的 “宝藏”
  - *aas的能力， “白嫖CDN” 、代理...
  - 资源：计算、流量、存储
  - 资产：数据

安世加

数据运营更细粒度

- *aaS审计能力
  - 风险识别，漏洞检测
  - 数据使用\盗用审计
  - 历史“现场还原”
- SaaS\FaaS:资产识别粒度必须更细
  - 宿主机
  - 容器
  - APPID
  - 风险出现在的代码行



总结

融入云架构

- cwpp**云原生**落地
- dev**SEC**ops

切换风险视角

- 保护**云资产**
- 聚焦云**服务风险**

安世加

Thanks

专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站:

https://www.anshijia.net.cn

微信公众号:

asjeiss

安世加