唯品会 全球精选 正品特卖

唯品会安全应急响应中心 VIP Security Response Center

我要我的云安全

中小企业云上安全技术实践

千寻位置 Qianxun SI 傅奎

2018 唯品会第三届互联网电商安全峰会
2018 vip.com third Internet ecommerce Security Summit
2018-5-5 上海

因唯安全 所以信赖

唯与同行，智御未来

唯品会安全应急响应中心
VIP Security Response Center
VSRC

我要我的云安全

中小企业
云上安全技术实践

千寻位置 Qianxun SI

傅奎

唯品会安全应急响应中心
VIP Security Response Center

向先行者致敬

我要我的云安全——

但，

从来就没有什么银弹，

有的只是

血泪教训

和惨淡的经验……

云计算和企业上云是大势所趋

上了云就更安全了吗？

不存在的！

安全产品 · 云盾

- DDoS高防IP
- Web应用防火墙
- 游戏盾
- 安骑士
- 态势感知
- CA证书服务
- 内容安全
- 安全管家
- 堡垒机
- 加密服务
- 数据库审计
- 云防火墙
- 实人认证
- 安全加速 SCDN
- 混合云
- 网络漏洞扫描系统 NEW

安全解决方案

- 等保合规安全解决方案
- 政务云安全解决方案
- 新零售安全解决方案
- 混合云态势感知解决方案
- 互联网金融安全解决方案
- 游戏安全解决方案
- 社交/媒体spam解决方案
- 移动App推广欺诈解决方案
- 企业预防勒索解决方案

安全服务 · 先知

- 安全众测
- 等保测评
- 应急响应
- 漏洞扫描服务
- 安全培训
- 安全评估
- 代码审计
- 网站安全监测服务
- 安全加固
- 安全保障服务
- 现场值守服务
- 安全通告服务
- 安全应急演练服务
- PCI DSS合规咨询

安全公益

- 产业安全扶助计划

安全

- BGP 高防（网络安全）
- 网站管家 WAF（网络安全）
- 云镜（主机安全）
- Web 漏洞扫描（网络安全） NEW
- 活动防刷（业务安全）
- 登录保护（业务安全）
- 验证码（业务安全）
- 内容安全（业务安全）
- 应用安全（移动安全）
- 手游反作弊（移动安全）
- 专家服务
- 态势感知
- 数据加密服务

案例一：防 DDoS，稳稳的黑洞

2017年，某个深夜。

服务器被黑洞，而我们还在沉睡……

案例一：防 DDoS，稳稳的黑洞

事件类型：DDoS	受影响资产：(ECS)
事件描述：遭受峰值流量为3319M的DDoS攻击，持续时间30分钟	被攻击资产：(ECS)
开始时间：2017-06-24 22:21:37	结束时间：2017-06-24 22:51:41
攻击响应状态：清洗	防护建议： 购买

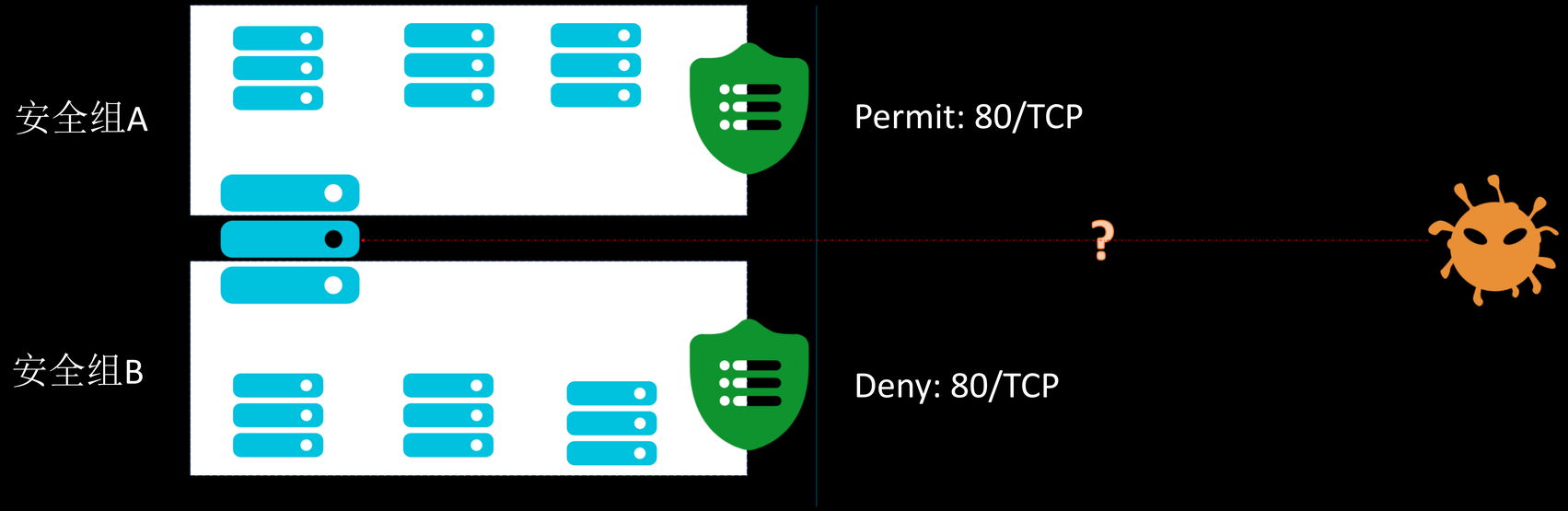
事件类型：DDoS	受影响资产：(ECS)
事件描述：遭受峰值流量为20450M的DDoS攻击，持续时间30分钟	被攻击资产：(ECS)
开始时间：2017-06-24 22:21:40	结束时间：2017-06-24 22:51:41
攻击响应状态：黑洞	防护建议： 购买，可有效防护DDoS流量攻击

案例二：薛定谔的安全组

“安全组”“不安全”

访问控制策略既是关闭的，也是开放的……

案例二：“薛定谔”的安全组



案例三：DPI了解一下？

“我也想做流量分析，问题是数据包在哪?”

“只有南北，无问西东？”

不要试图在云平台上自建 IDC……

十八般武器都玩不转了？

云平台不是万能的，怎么办？

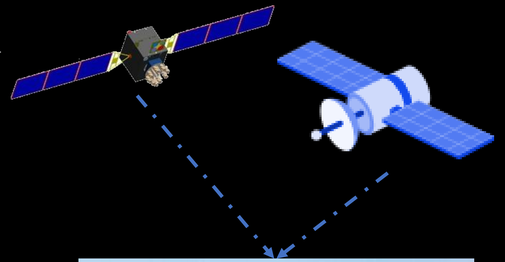
上了“贼船”你还能怎么样？

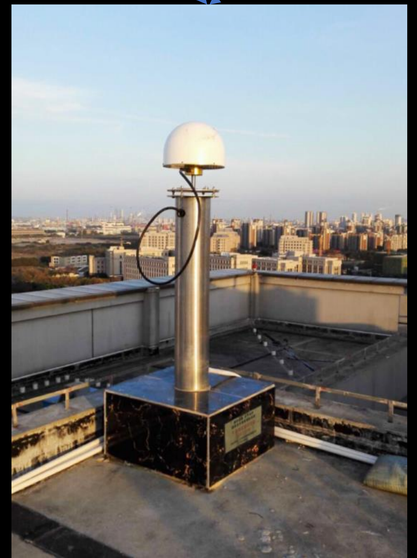
运行环境发生变化，

安全工作也要与时俱进

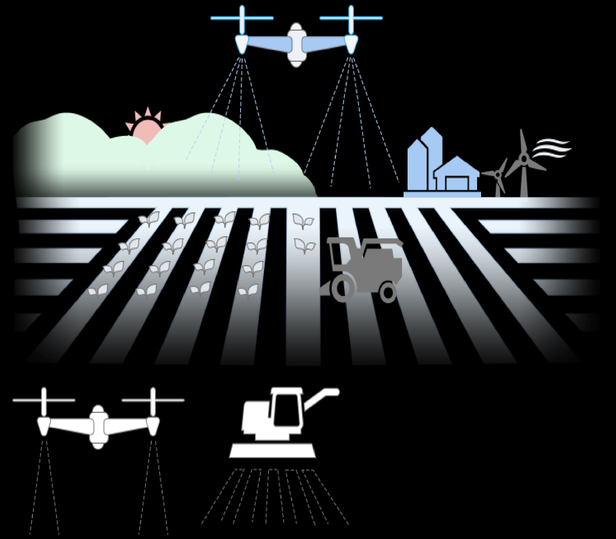
高精度位置服务在公有云上的安全防护实践

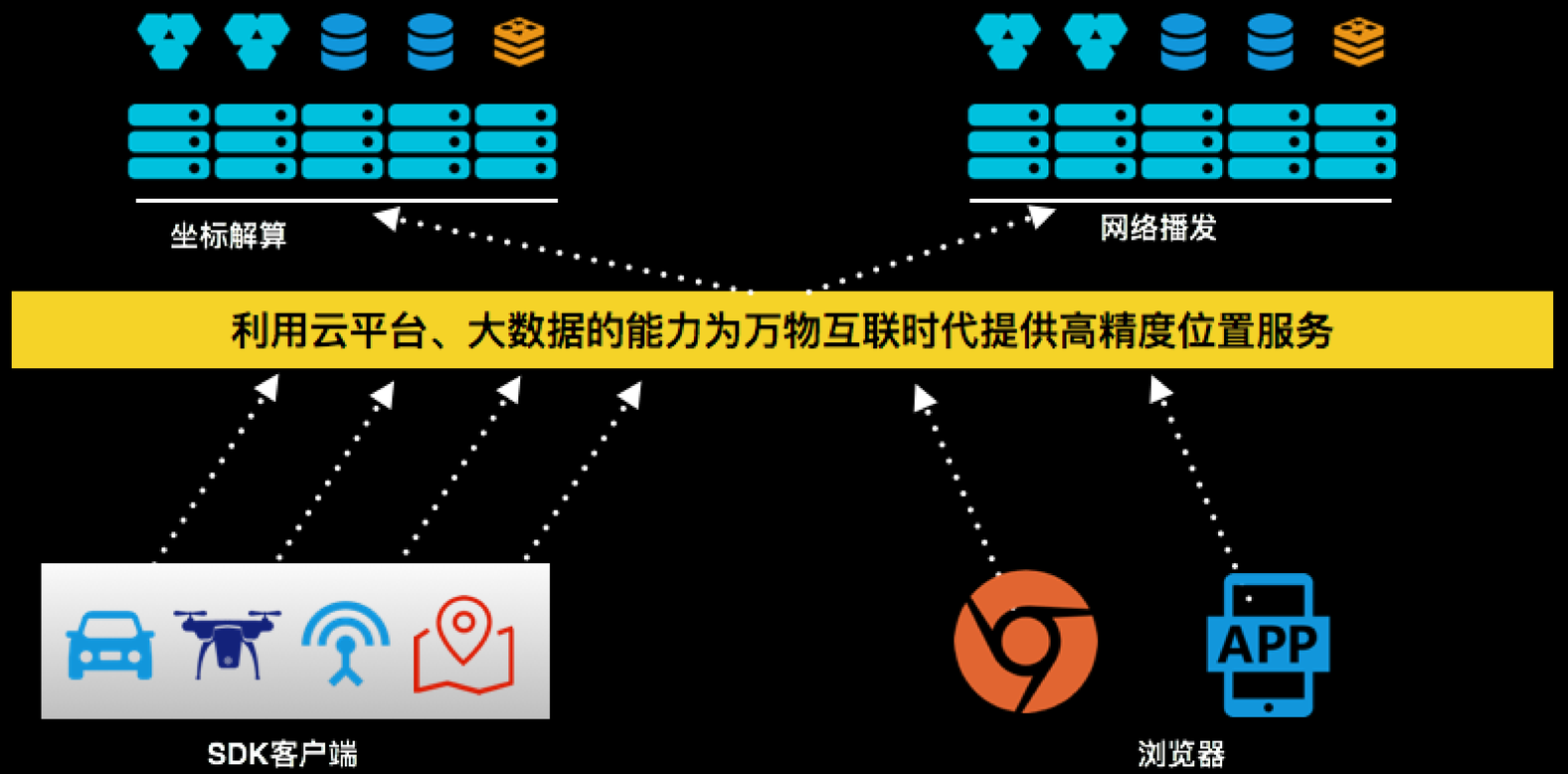
（基于阿里云）






基站总数：••••





全球服务

亿级用户

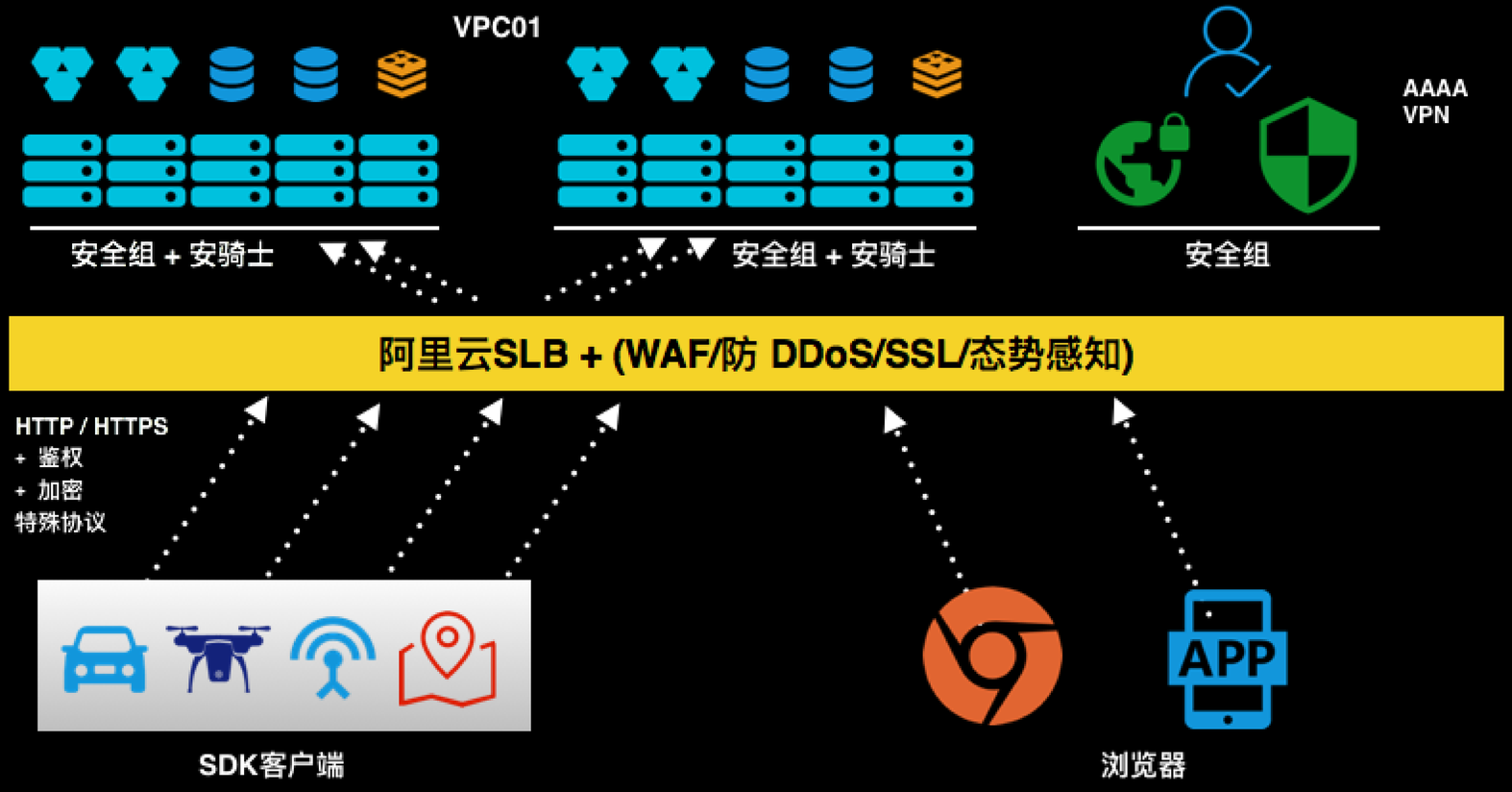
实时动态厘米级

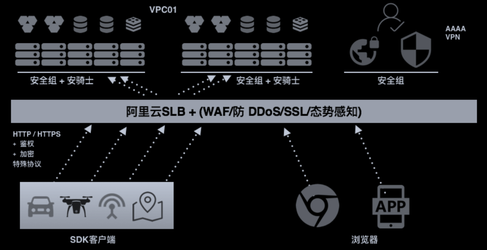
静态后处理毫米级

1）基础安全防护：

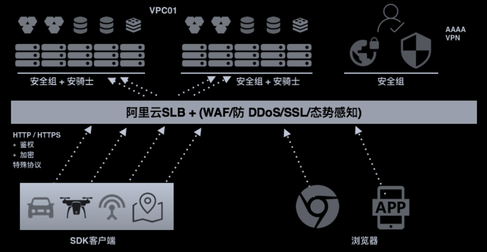
用好云平台基础产品，

识边界，扎篱笆。


VPC01
安全组 + 安骑士
安全组 + 安骑士
AAAA
VPN
安全组
阿里云SLB + (WAF/防 DDoS/SSL/态势感知)
HTTP / HTTPS
+ 鉴权
+ 加密
特殊协议
SDK客户端
浏览器
APP


VPC01
安全组 + 安骑士
安全组 + 安骑士
AAAA
VPN
安全组
阿里云SLB + (WAF/防 DDoS/SSL/态势感知)
HTTP / HTTPS
+ 鉴权
+ 加密
特殊协议
SDK客户端
浏览器
APP

多数据中心

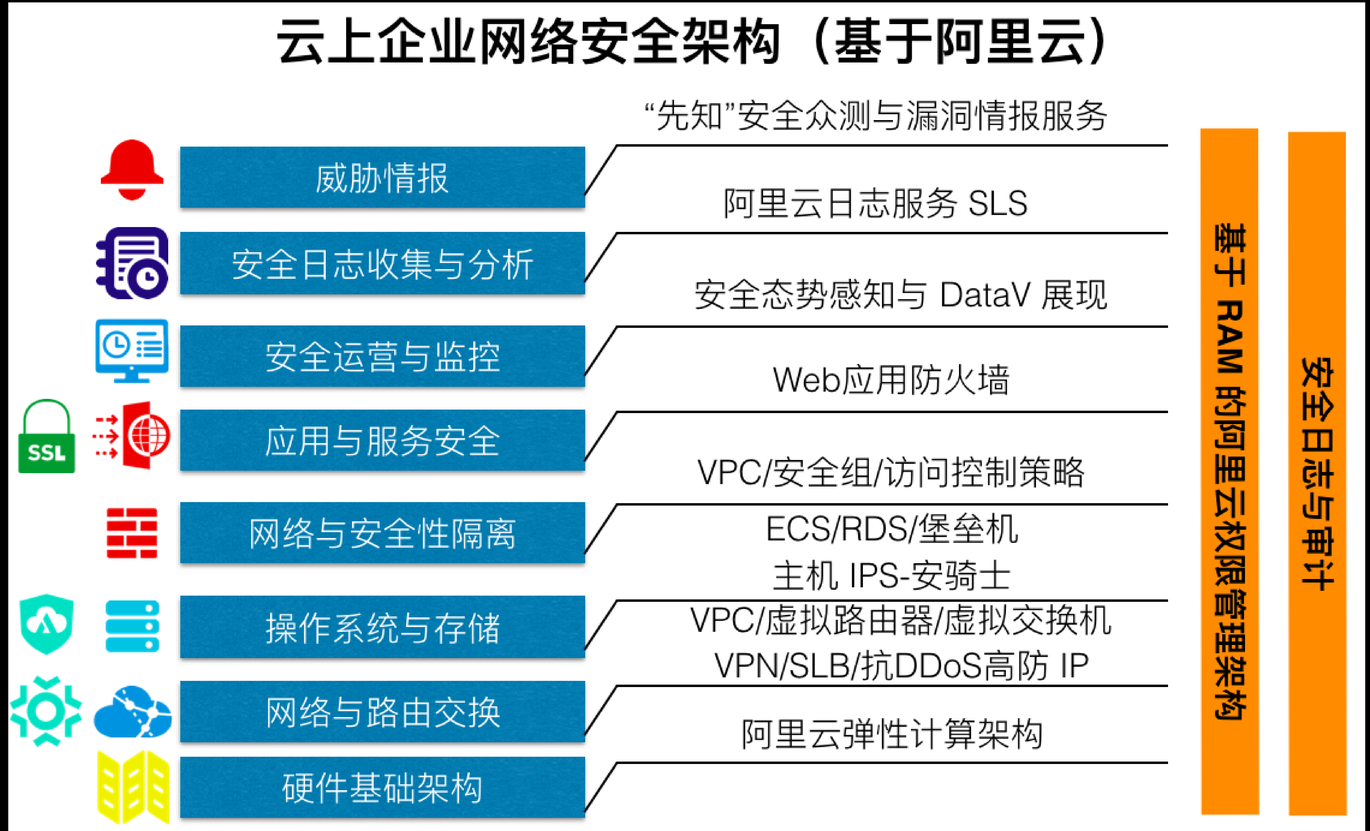

VPC01
安全组 + 安骑士
安全组 + 安骑士
AAAA
VPN
安全组
阿里云SLB + (WAF/防 DDoS/SSL/态势感知)
HTTP / HTTPS
+ 鉴权
+ 加密
特殊协议
SDK客户端
浏览器
APP

2）科学搭建云上安全防护框架：

深入理解云产品是前提，

不仅仅是安全产品。

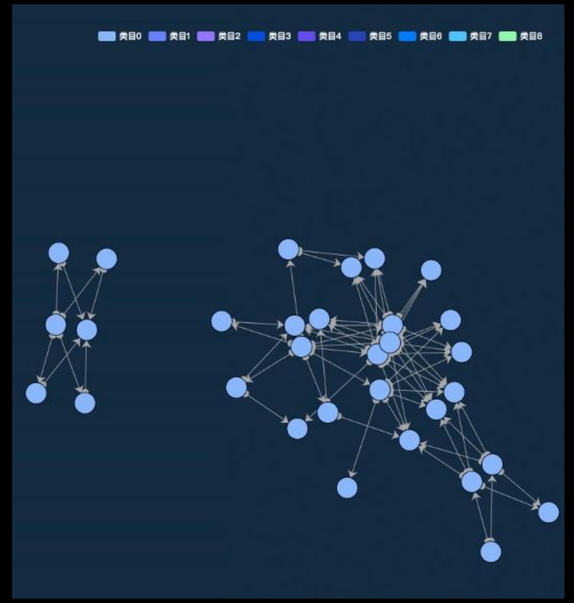
云上企业网络安全架构（基于阿里云）

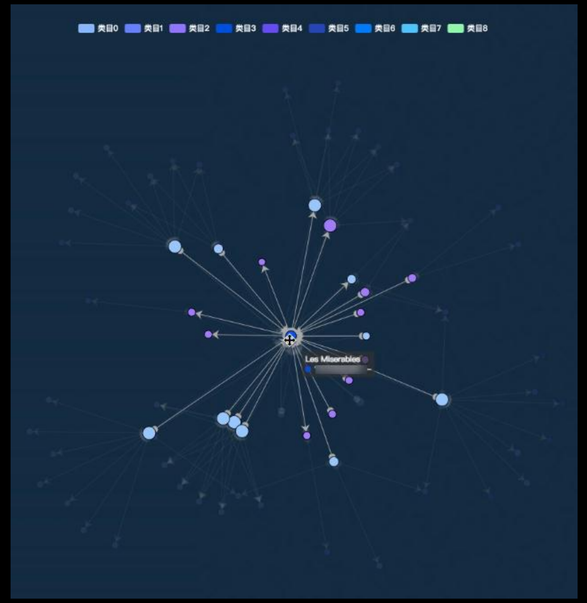


3）榨干云安全产品功能：

穷，就得物尽其用……

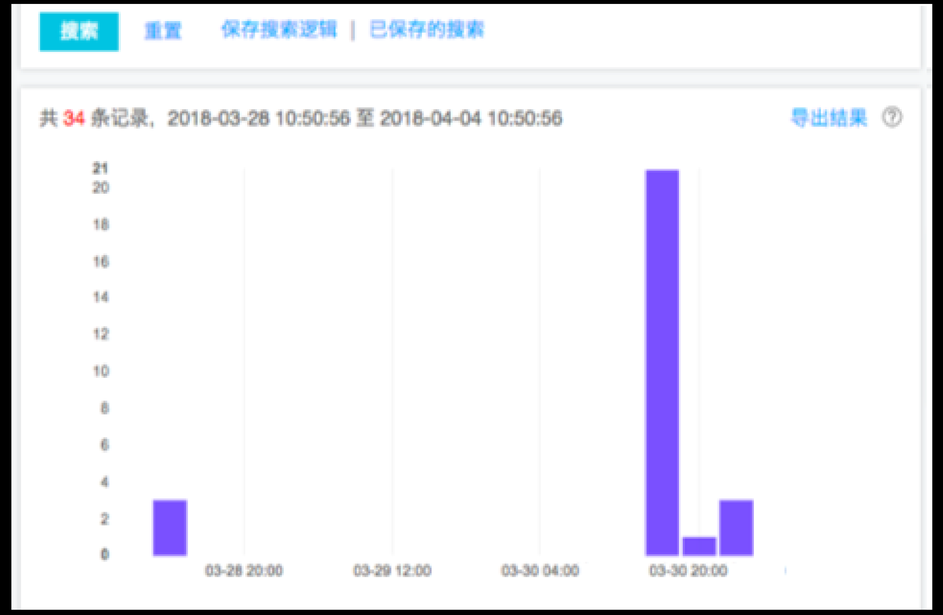
应用实践：态势感知DNS 日志分析

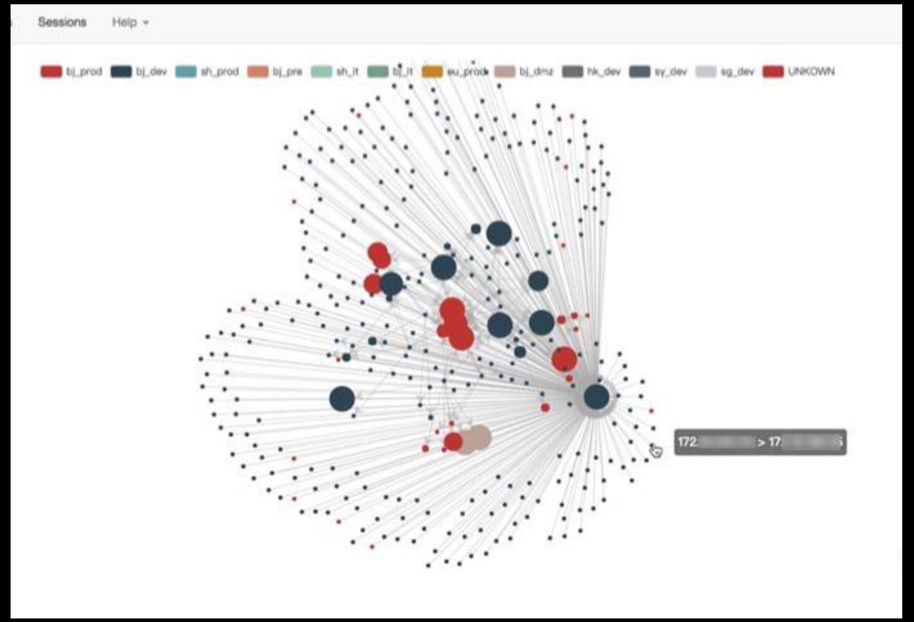




应用实践：网络会话日志分析

应用实践：网络会话日志分析





应用实践：换一种姿势检测“挖矿”行为

应用实践：借助 WAF 实现虚拟补丁

公司最后一名 PHP 工程师离职，

“0day”来了……

应用实践：借助 WAF 实现虚拟补丁

4）运营好云上安全产品：

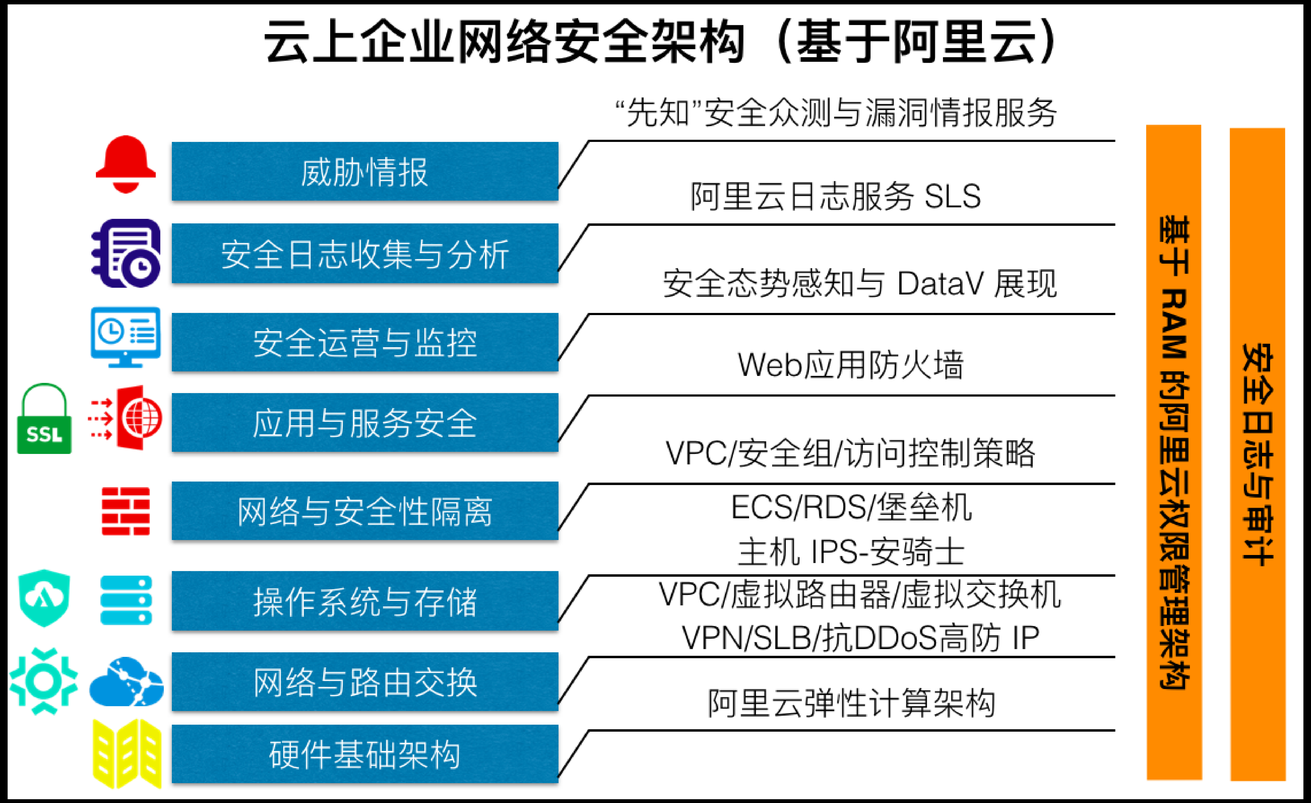
自己动手，弥补平台产品的不足

外网开放端口监测

Github 敏感信息监控

Gitlab 访问行为审计

云上企业网络安全架构（基于阿里云）

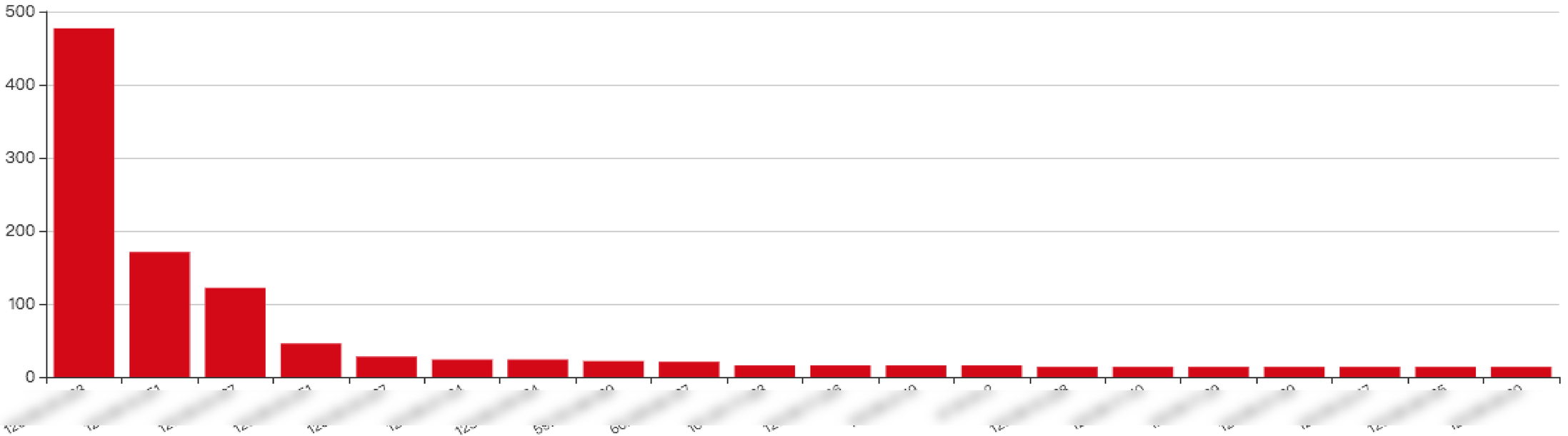


深度挖掘安全日志

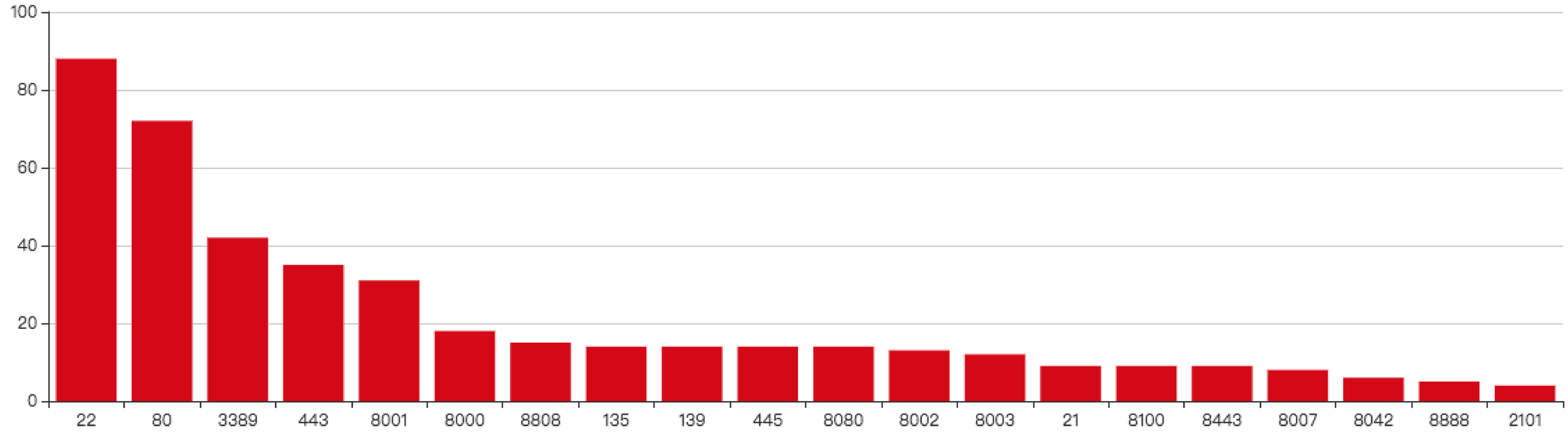
长期积累历史数据

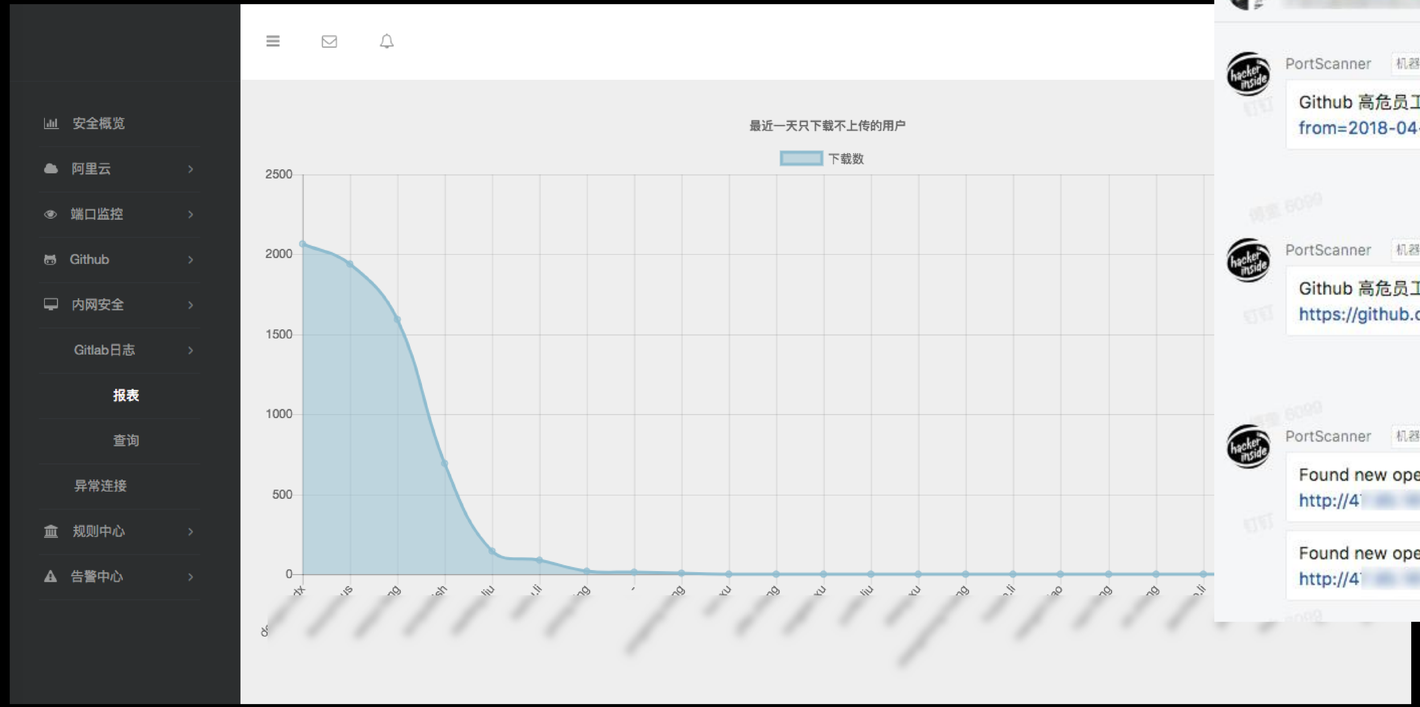
反向推动架构演进

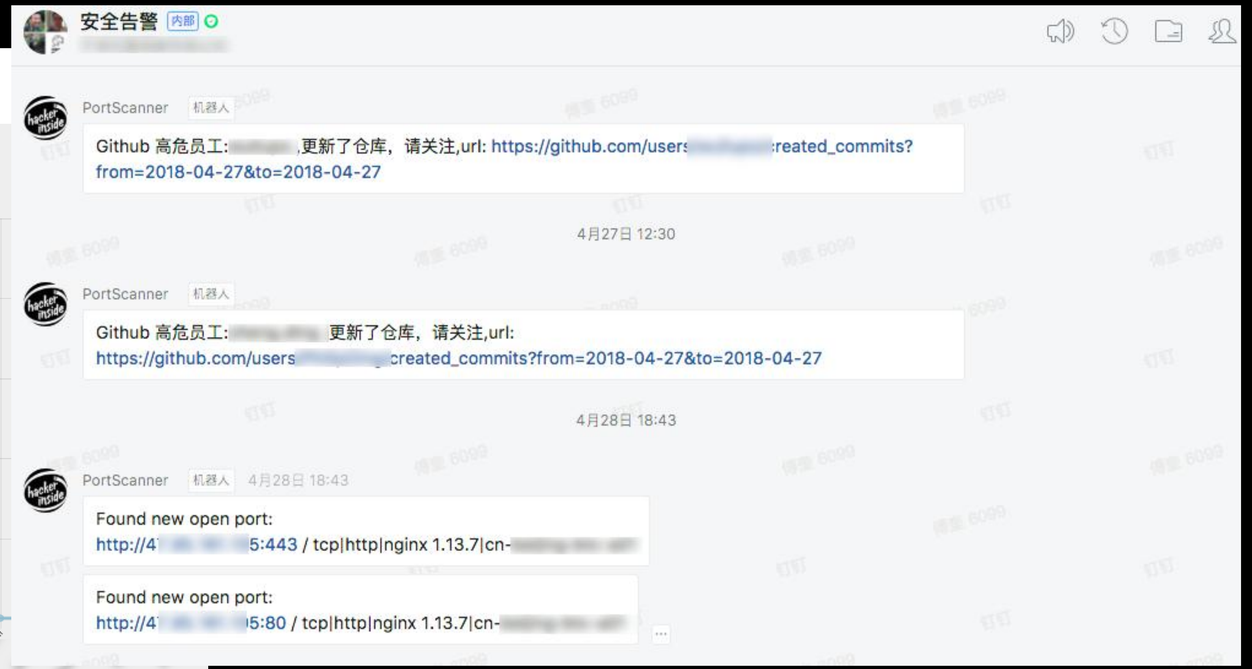
基于IP的端口开放统计



外网端口开放统计


100
80
60
40
20
0
22
80
3389
443
8001
8000
8808
135
139
445
8080
8002
8003
21
8100
8443
8007
8042
8888
2101


安全概览
阿里云
端口监控
Github
内网安全
Gitlab日志
报表
查询
异常连接
规则中心
告警中心
最近一天只下载不上传的用户
下载数
2500
2000
1500
1000
500
0


安全告警
内部
PortScanner
机器人
Github 高危员工:[redacted],更新了仓库，请关注,url: https://github.com/users[redacted]created_commits?from=2018-04-27&to=2018-04-27
4月27日 12:30
PortScanner
机器人
Github 高危员工:[redacted]更新了仓库，请关注,url: https://github.com/users[redacted]created_commits?from=2018-04-27&to=2018-04-27
4月28日 18:43
PortScanner
机器人
4月28日 18:43
Found new open port:
http://4[redacted]5:443 / tcp|http|nginx 1.13.7|cn-[redacted]
Found new open port:
http://4[redacted]5:80 / tcp|http|nginx 1.13.7|cn-[redacted]

5)构建良好的问题沟通机制：

云上安全的运营也是

企业与云平台共同协作关系的运营

5) 构建良好的问题沟通机制：

- **关注平台技术演进和发展方向**
- **与云平台建立良好的沟通机制**
  - 合作交流群
  - 聆听平台
  - ACE 活动
  - MVP 渠道
  - 云栖社区

总结：云上安全成功运营的关键：

深入理解
平台架构

灵活运用
平台产品

持续运营
不断进步

关键时刻还得靠平台……

最后：一些感悟和观点

观点：

- 没有百分之百的云
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

观点：

- 没有百分之百的云
- 上云就是自废武功
- [illegible]
- [illegible]
- [illegible]

观点：

- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- [illegible]
- [illegible]
- [illegible]

观点：

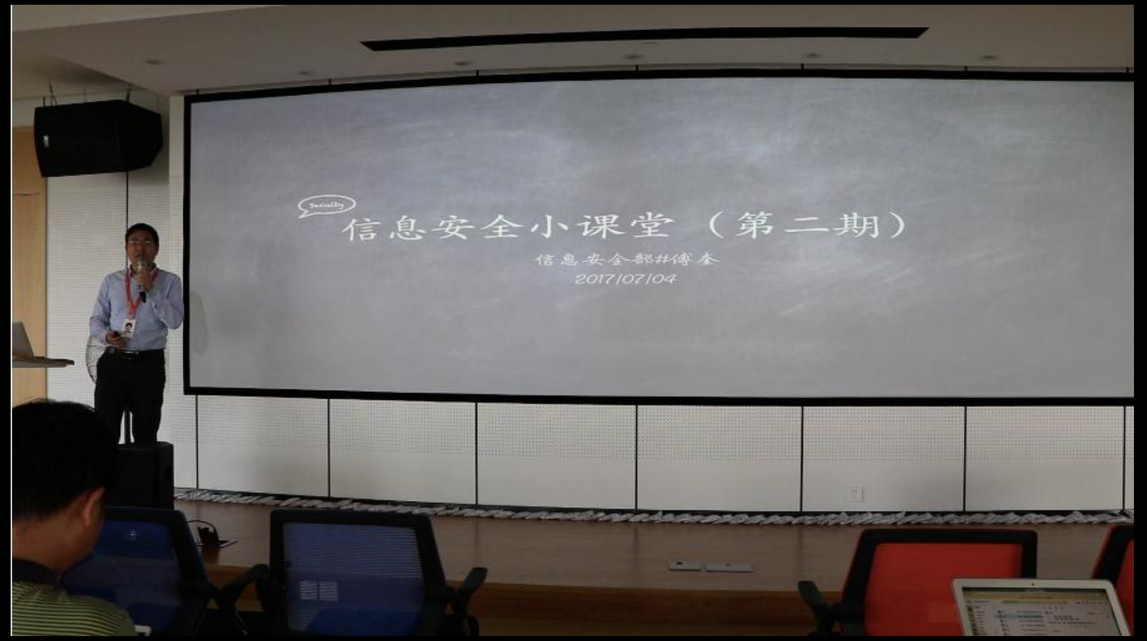
- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- 与平台共同进步
- [illegible]
- [illegible]

观点：

- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- 与平台共同进步
- 安全厂商正被挑战
- [illegible]

观点：

- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- 与平台共同进步
- 安全厂商正被挑战
- 死都死在密码上



专项安全开发培训

距离卓越开发者还有最后一公里

信息安全部

唯品会安全应急响应中心
VIP Security Response Center

定目标 组团队
识边界 扎篱笆
上规范 走流程
多监控 少干预
收日志 做审计
出数据 反馈
斗产品 练开发
靠平台 入联盟
调测试 撩运维
摸石头 勤复盘
云计算 更安全
上云就上阿里云

共同捍卫企业云安全

谢谢！

千寻位置 Qianxun SI