KCon

2019

APT 攻守道

演讲人：何艺

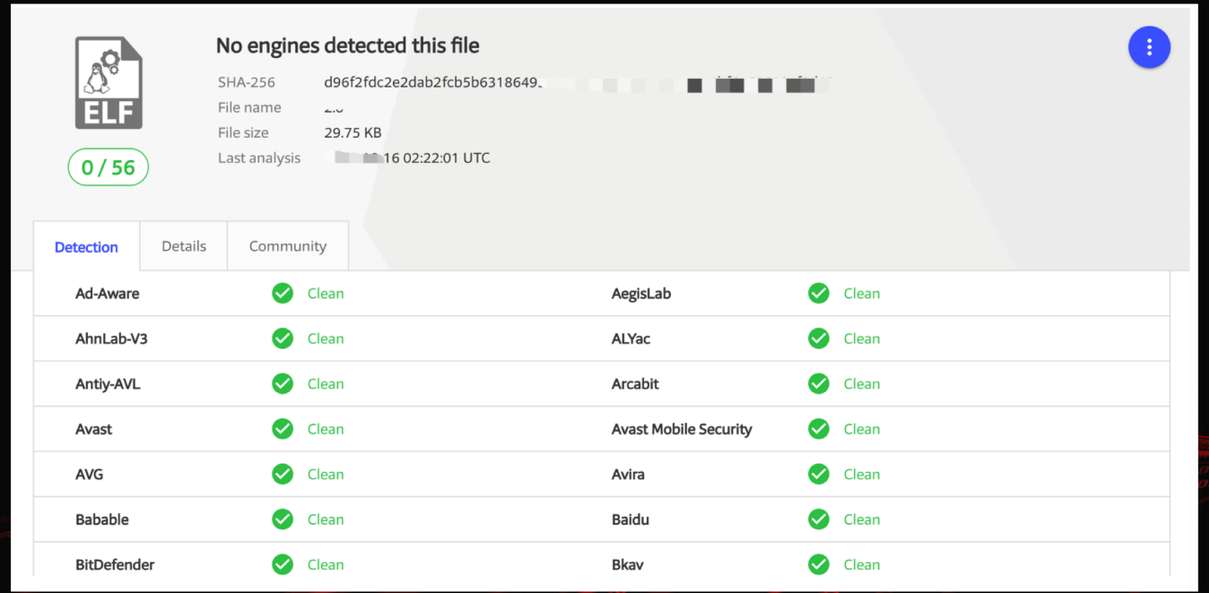
目录
CONTENTS

PART
01

APT 攻击：薛定谔的猫

APT 案例

APT 案例



- 免杀标配
- 无文件
- 无进程
- 无端口
- 无通信

APT 行为特点

- 明确的目标
- 情报收集准备
- 定制化攻击，精准钓鱼、社工投递

- 免杀、高隐蔽性后门
- 反追踪定制域名
- 干净的IP

- 隐匿行踪
- 谨慎操作
- 长期潜伏

甲方环境

- 永远有傻白甜的“人”
- 不知道谁在管理的海量“资产”
- 野蛮生长“业务系统”
- 任性的“权限”、离职的管理员
- 不出事要你何用，出了事要你何用的“安全人员”

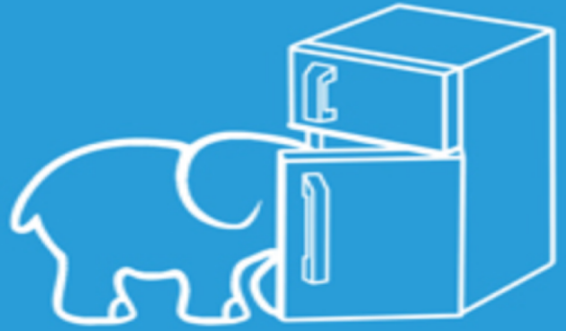
PART
02

APT 防护体系

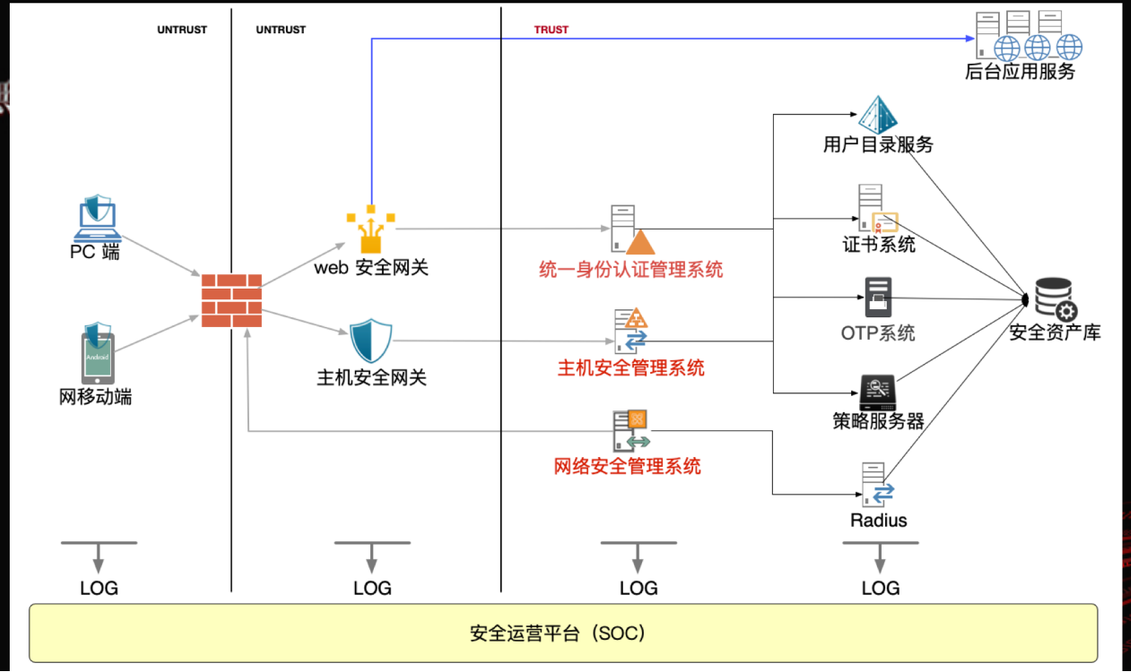
怎么做？

做好防御 1

做好监控 2



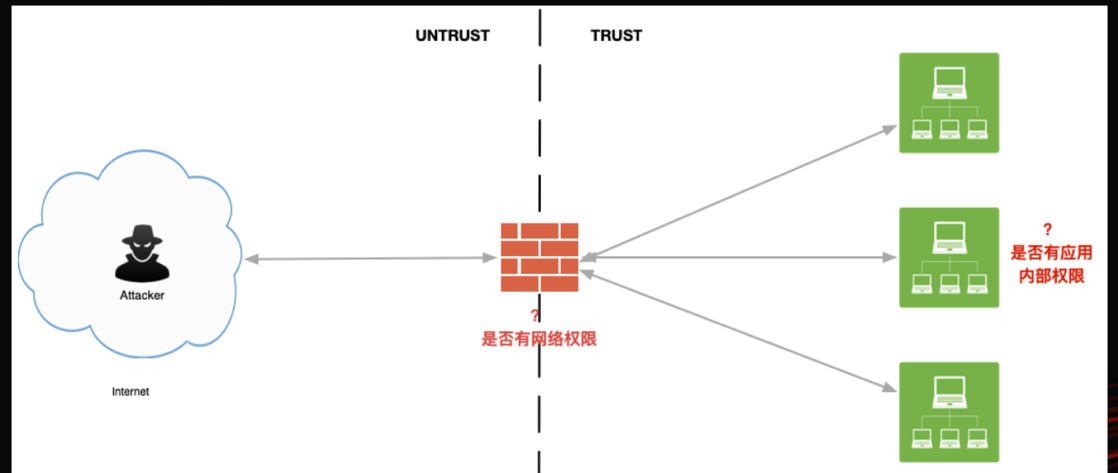
做好管理 3



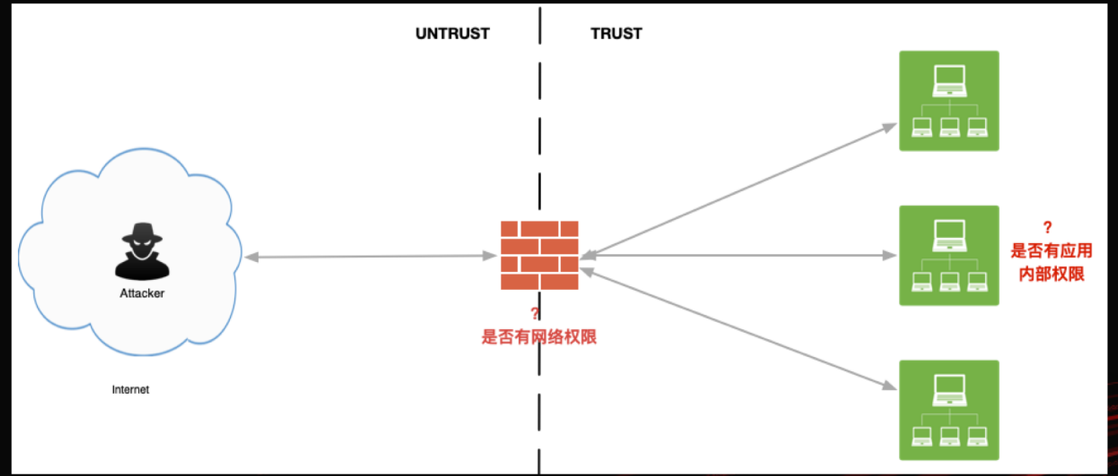
安全防护平台核心能力

- **平台化**：服务化输出能力
- **安全准入**：终端准入、业务准入、隔离机制
- **统一边界**：统一入口，减少攻击面
- **统一身份认证**：统一身份，多因素强认证
- **统一权限控制**：基于用户、设备、业务的最小化授权
- **资产数据整合**：**建立起人->资产->业务关系**

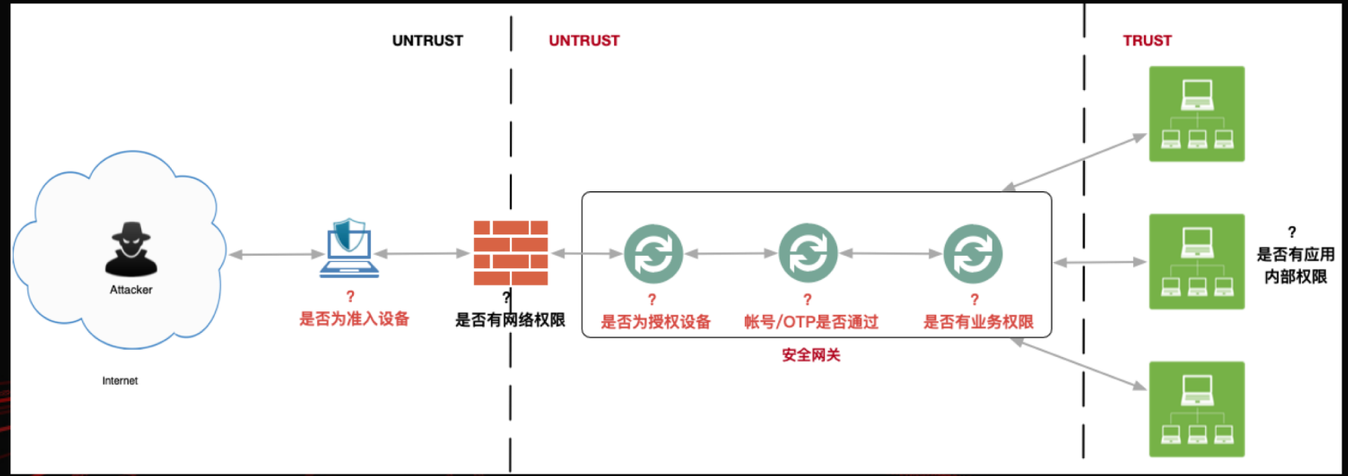
传统攻击路径



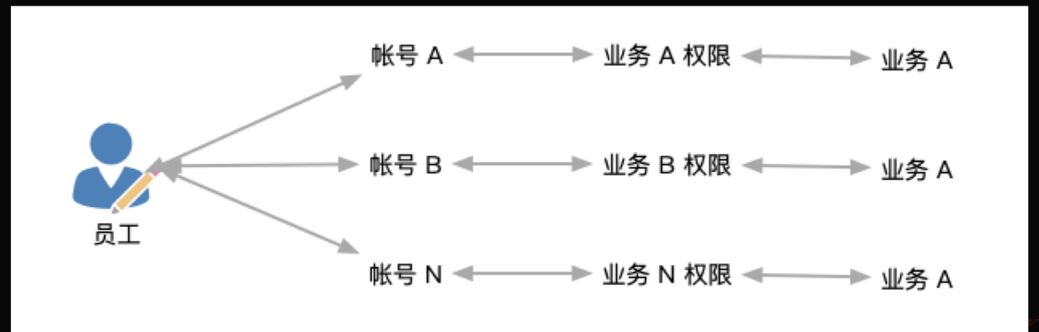
传统攻击路径



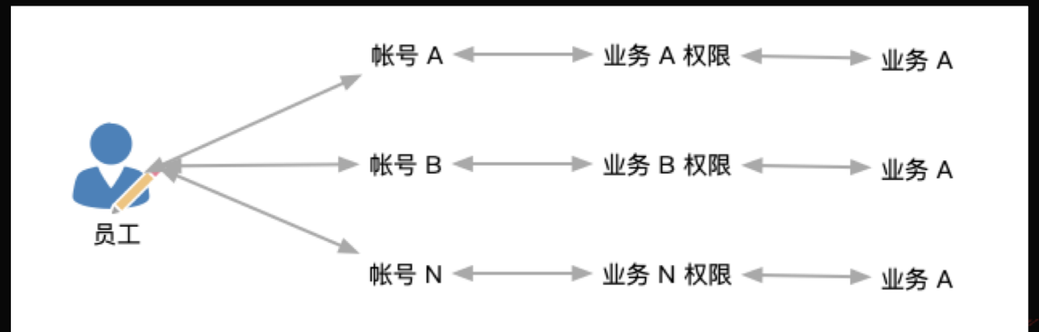
零信任攻击路径



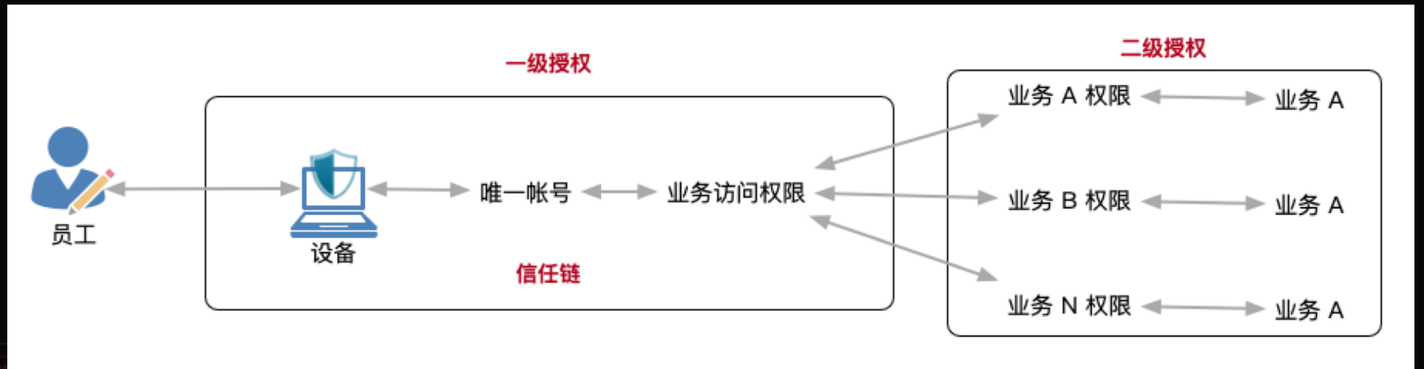
传统权限模型



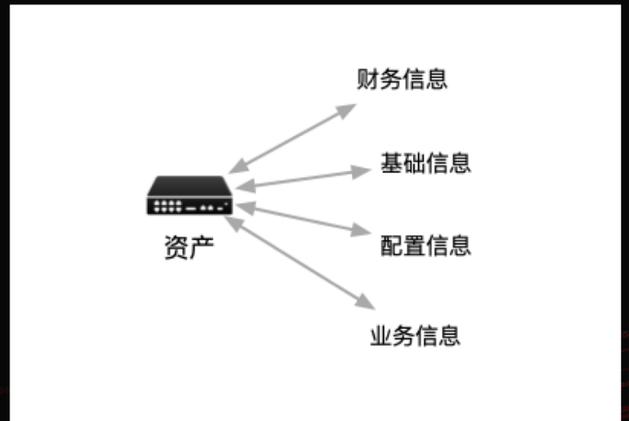
传统权限模型



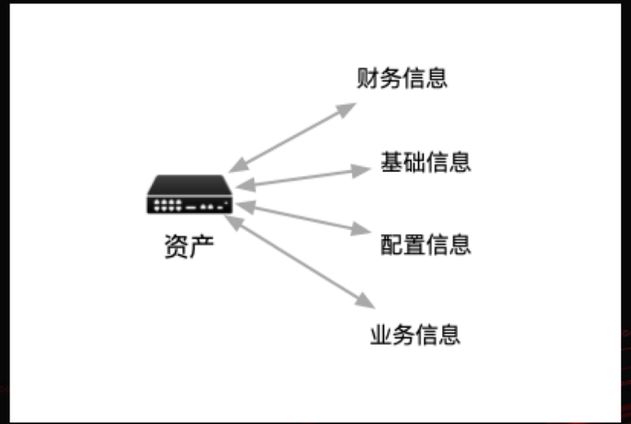
零信任权限模型



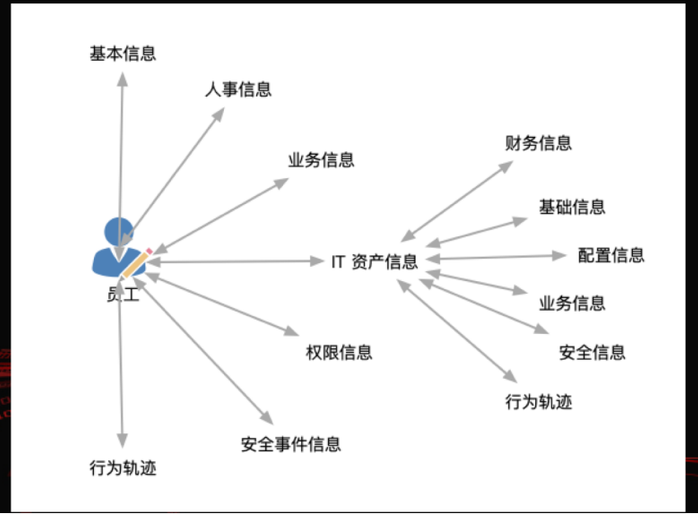
传统资产管理
（CMDB）



传统资产管理
（CMDB）



新的安全资产管理
（SADB）



APT是不是就搞不进来了？

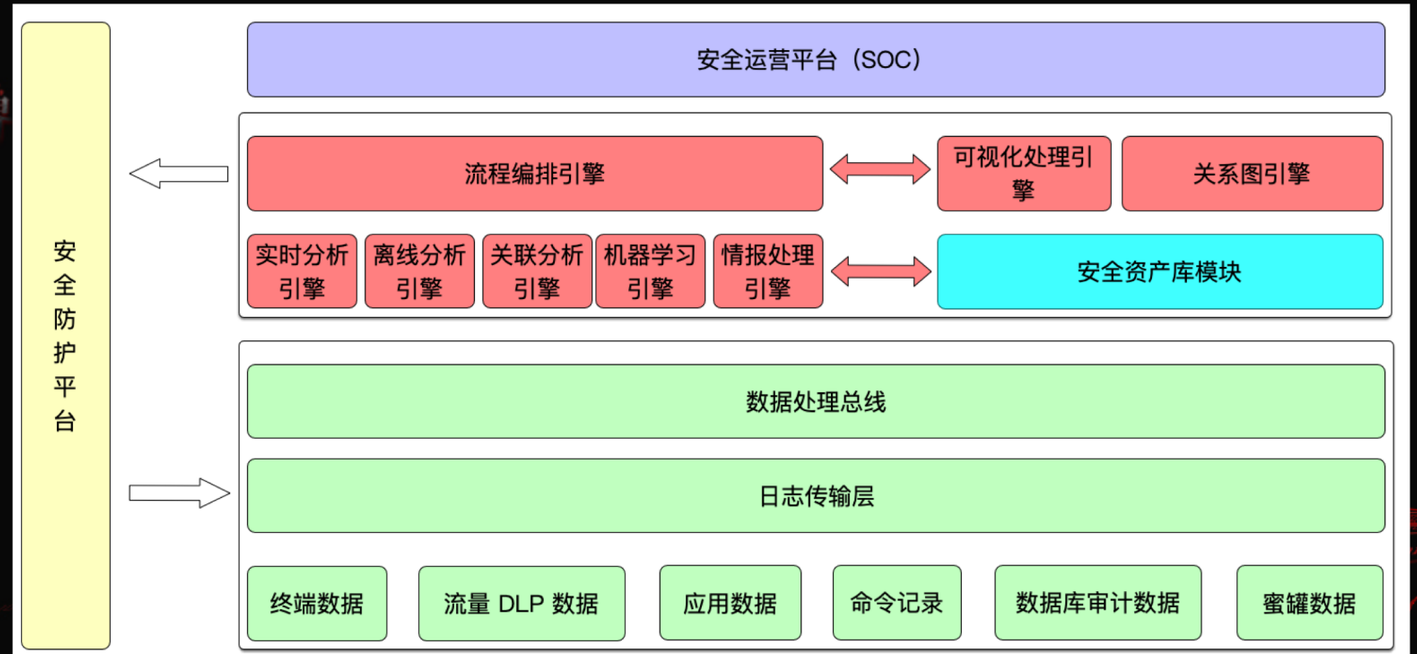
APT是不是就搞不进来了？

所有的防御手段只是提高入侵成本，以空间换时间！

PART
03

APT 检测架构

既然入侵一定会成功，那么发现时间和响应时间就至关重要了！



检测架构要解决的问题

- 数据质量，越精细越好
- 关键节点是否能监控到
- 处理能力和方式够不够
- 人永远不够用，需要自动化
- 灵活好用的分析工具
- 资产行为能否还原

如何解决高质量数据问题？

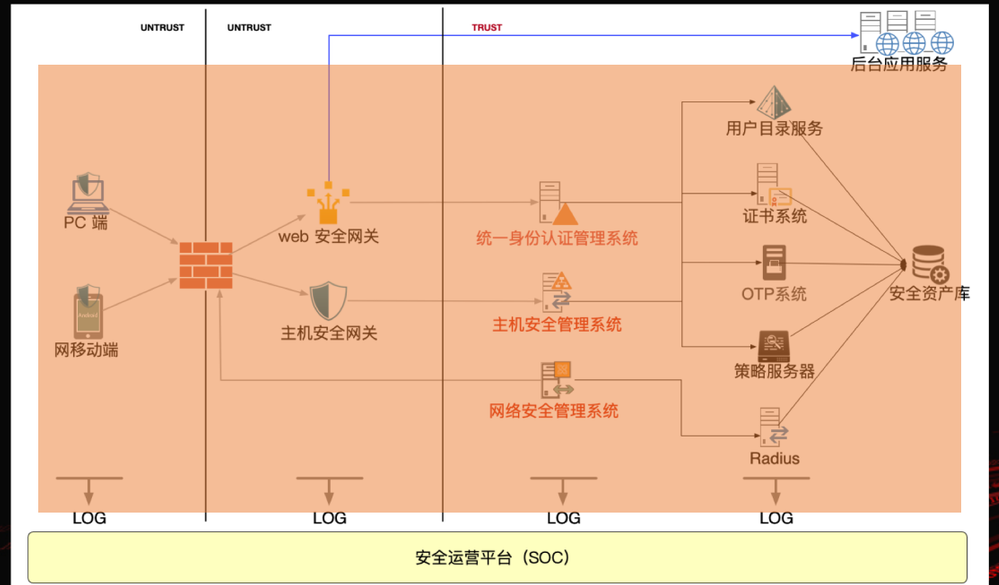
- 流量识别
- 应用/内容识别
- 用户识别

Time	src_ip	src_port	src_bytes	dst_ip	dst_port	dst_bytes	duration
Aug..276	10.	57,698	3,549	22[redacted]	443	32,260	1.105
Augu..4	11.[redacted]	37,806	683	221[redacted]	80	32,260	0.089

Time	src_ip	host	uri
August [redacted]49.000	10.[redacted]	mobi[redacted].net	/[redacted]eTable
August [redacted]49.000	1[redacted]	mobi[redacted].net	/[redacted]rtLog

src_ip	host	uri	user	user_empl_name	user_dept_name
10.[redacted]	mobi[redacted].net	/[redacted]ble	[redacted]	[redacted]	[redacted]品
10.[redacted]	mob[redacted].net	/[redacted].og	[redacted]	[redacted]	[redacted]品

如何解决关键节点监控问题？



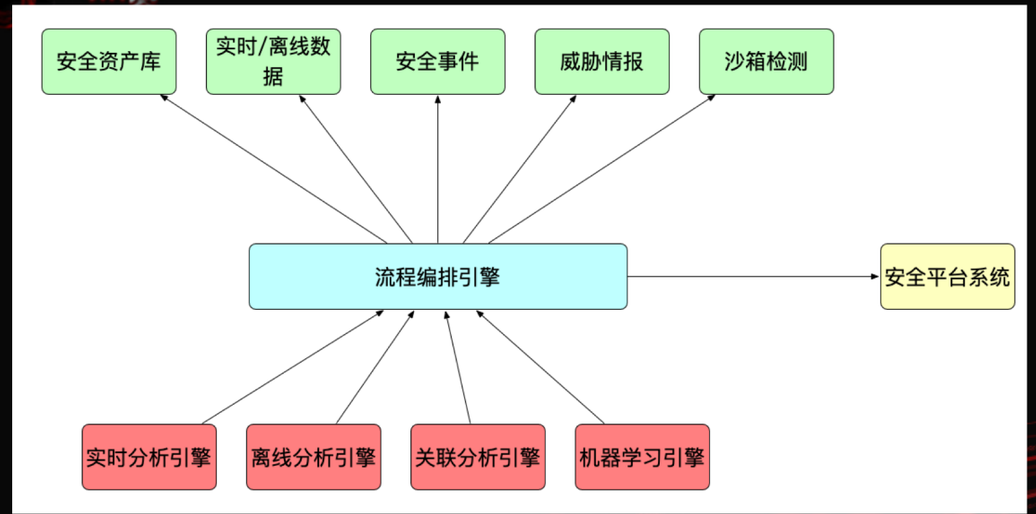
一定会漏报的情况下，覆盖节点越多机会越多！

- 网络层、主机层、应用层、用户层多纬度数据覆盖
- 数据进行分类和行为定义
- 基于身份信息来富化数据
- 能还原行为过程

如何让资产信息产生更多价值？

- 建立人与资产的关系
- 建立资产与业务的关系
- 整合资产的关联元数据
- 梳理资产的行为逻辑
- 关联资产的安全事件

如何提高事件处理能力？



- 放弃完美的引擎
- 适合自己场景的

- 流程编排可以承上启下

如何提高分析能力？

- 更直观的工具
- 允许进行大海捞针
- 通过“关系图”建立人、资产、事件和行为的联系
- 半自动化分析的探索

APT是不是就一定能发现了？

APT是不是就一定能发现了？

没有人用的工具，是没有价值的工具！

安全运营/管理挑战

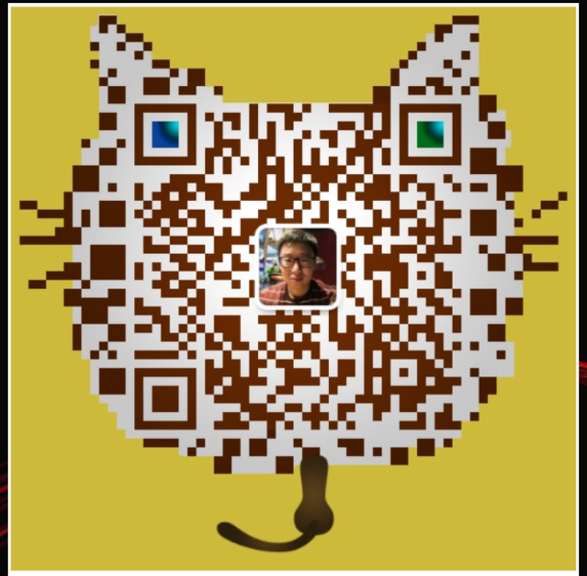
- 指标的覆盖和提高
- 如何判断APT事件
- 什么叫异常行为
- 还有多少种未知的场景

观点总结

1. 入侵一定会发生
2. 所有的防护措施均是提高成本，换取时间
3. 检测一定会漏，多纬度检测好于单一纬度
4. 对抗是系统工程，没有银弹
5. 线下打击能力是最后的防卫

谢谢观看

演讲人：何艺



扫一扫上面的二维码图案，加我微信

KCon