



结果导向的安全运营

赵弼政/职业欠钱
美团基础安全负责人

目录

安全运营

如何评价安全工作好坏

怎么做

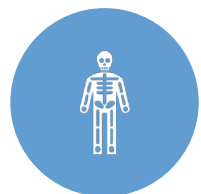
安全运营的一些心得

如何评价安全工作好坏



入侵检测的评价

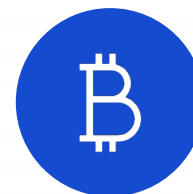
- 技术沙盘的完备性?
 - 蜜罐、HIDS、NIDS、EDR、WebIDS、RASP
- 技术/概念的先进性?
 - 用户态 vs 内核态 特征工程 vs 机器学习
- 攻击场景的覆盖度?
 - ATT&CK
- 酷炫的地图炮?
 - 态势感知、威胁情报、SOAR、NG-SOC



自研/开源黑白
灰盒组件/SDK



CVE/Paper/CTF



主动发现的数量
/比例高



外报漏洞少



人均代码多



培训的次数多

可手段并不是目标啊

入侵：反正就是发现不了

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

后台规则引擎“正好”没工作

这台机器的HIDS似乎有bug，
日志没回传

误报太多了，看不过来，其实
已经告警了

看过了当成误报了

这一台机器“恰好”没安装
HIDS



又来告警了



看看是怎么被入侵的



看看是怎么被入侵的

安全运营死亡三连

URL不在库中

爬虫引擎bug

Post 类URL不敢扫

Cookie认证不通过

调度引擎Bug了



插件异常

最大的遗憾并非失败而是本可以



评价好坏看跟谁比

GFAA厂很牛但是不可复制不可参考啊

AT很牛但我们人不如他们多啊

同梯队其他公司也就这水平，我们差不多啊

我们是小厂做不好很正常啊



安全没有绝对

并不影响我们追求“本可以做到的更好”

说服老板安全需要投入更多的人和资源，也是安全运营工作之一

同等人力，ROI是否已足够高

方法论是业界最佳实践么

我真的尽力了么？

态度问题 or 能力问题？

示例1：

某安全产品发布新版本

因Bug导致线上事故

业务问责并排斥继续部署，负责人转岗

示例2：

推广某产品部署/扫描器上线

业务抗拒/拖延/反复打扰

导致事实上公司不具备该安全能力



安全专家的能力模型

- 安全技术：擅长漏洞研究、攻防（Web/iOS/Android/二进制...）
- 安全管理：了解业界实践、合规要求，擅长解决方案
- 安全开发：擅长Coding，跟专业开发有时略有区别
- 安全算法：建模、开发，机器学习、AI
- 安全运维：擅长“使用”和“维护”
- 安全架构：顶层设计
- SRC“运营”：外联、品牌、市场活动
- ...

资源/HC 不足，安全专家被迫全栈



安全人才

渗透测试&数据分析专家
挖洞&扫描器技术专家
算法专家
应急响应安全专家
IT安全专家

VS

待解决的问题

覆盖、丢数据、高可用
漏URL (覆盖)、调度、Cookie
甄别误报
情报处理、修复慢
业务不肯/拖延部署

缺失的技能栈影响目标的达成

真*重视安全 = 目标不妥协 = 尊重技术客观挑战但质疑真的尽力了么?

结果导向的评价与激励模式催生安全运营

为了实现安全目标，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源解决问题并持续迭代优化的过程

——《我理解的安全运营》

运营就是对运营过程的计划、组织、实施和控制，是与产品生产和服务创造密切相关的各项管理工作的总称。从另一个角度来讲，运营管理也可以指为对生产和提供公司主要的产品和服务的系统进行设计、运行、评价和改进的管理工作。

——百度百科

跟传统安全工程师的区别：对目标负责，而不仅是对技术痴迷

有强烈的对目标负责和结果导向意识，并且极具技巧的达成了目标，就是一个有运营意识和能力的安全工程师并不是非得专门设置一个安全运营岗位

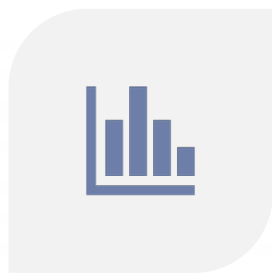
醉心攻防技术本身不愿意为最终结果负责，只想提供核心技术的专业人才同样值得尊重
只是需要有人配合完成他不愿意、不擅长完成的部分，共同达成目标

安全运营怎么做

- 说得清要达成的目标，解决的思路，符合逻辑
- 量化出评价的方式，跟踪趋势
- 分析得清主要矛盾
- 坚持复盘、迭代优化



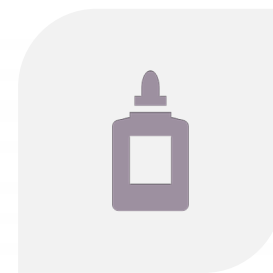
目标管理



量化评价



主要矛盾



迭代优化

1. 对互联网开放的服务被利用：SSH/RDP、Redis、Jenkins/Tomcat/OpenFire/、VPN、代理
2. Web应用漏洞：RCE、上传漏洞、SSRF、命令执行/注入漏洞
3. （钓鱼、水坑、社工）员工账号失窃、设备感染恶意木马
4. 供应链攻击（Xcode、Xshell、Putty、Pip、CCleaner、供应商/开发商/外包/客服）
5. 公共存储平台泄露内网接入信息（GitHub、网盘、知识管理工具）
6. WiFi、有线网络
7. 边界网络设备、影子系统（IoT、嵌入式设备）

以入侵检测为例：解决思路的逻辑

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

1. 加固：减少攻击面
2. 入侵感知：数据采集、模型建设告警 / 部署商业产品
3. 欺骗防御：蜜罐



合作伙伴
投后公司
生态合作
公有云

数据采集：

HIDS
WAF
NIDS
RASP
EDR
DB Audit
AD Log
Mail Log
SSO
VPN
Application



1. 禁止一切非业务端口对外开放

- 公网扫描 (Zmap/Masscan) 公司全量IP、全量端口
- NIDS 流量分析高危协议
- 注册制, 非授权不得对外开放

问题:

IP范围不全 —— 责令资产管理团队查漏补缺

识别协议不全 —— nmap默认协议、白名单备案模式

扫描速度慢 —— 增量/存量区分、并发

业务抗拒修复 (历史问题 or 各种困难) —— 红线制度配套、自上而下

海量咨询 —— 机器人/知识库

2. 安全域隔离

- 办公网、IT服务、stage/prod/dev、核心敏感业务、客服/外包/分支职

问题:

海量咨询 —— 机器人/知识库、自助平台

特例 —— 高级管理者特批

只增不减 —— 服务树&有效期

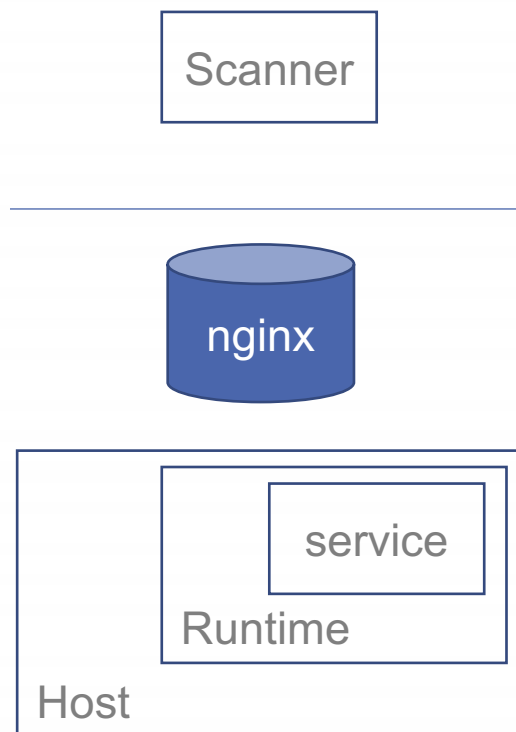
看起来毫无技术含量的工作



以入侵检测为例：主要矛盾

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



Scanner: 提前规避漏洞

NIDS: 明文攻击、木马检测

WAF or WebIDS: 缓解 or 感知

应用日志: 风控

RASP: 恶意调用

HIDS: 文件、进程、命令、日志



看上去很6

漏URL：NIDS+Nginx Log

商业/开源

自研

示例：
扫描触发告警、脏数据
引发业务投诉
甚至要求不要扫

不敢扫：业务自助

适配难

灵活性好

质量问题：竞品对比、监控

速度慢

漏洞库维护成本

误报高

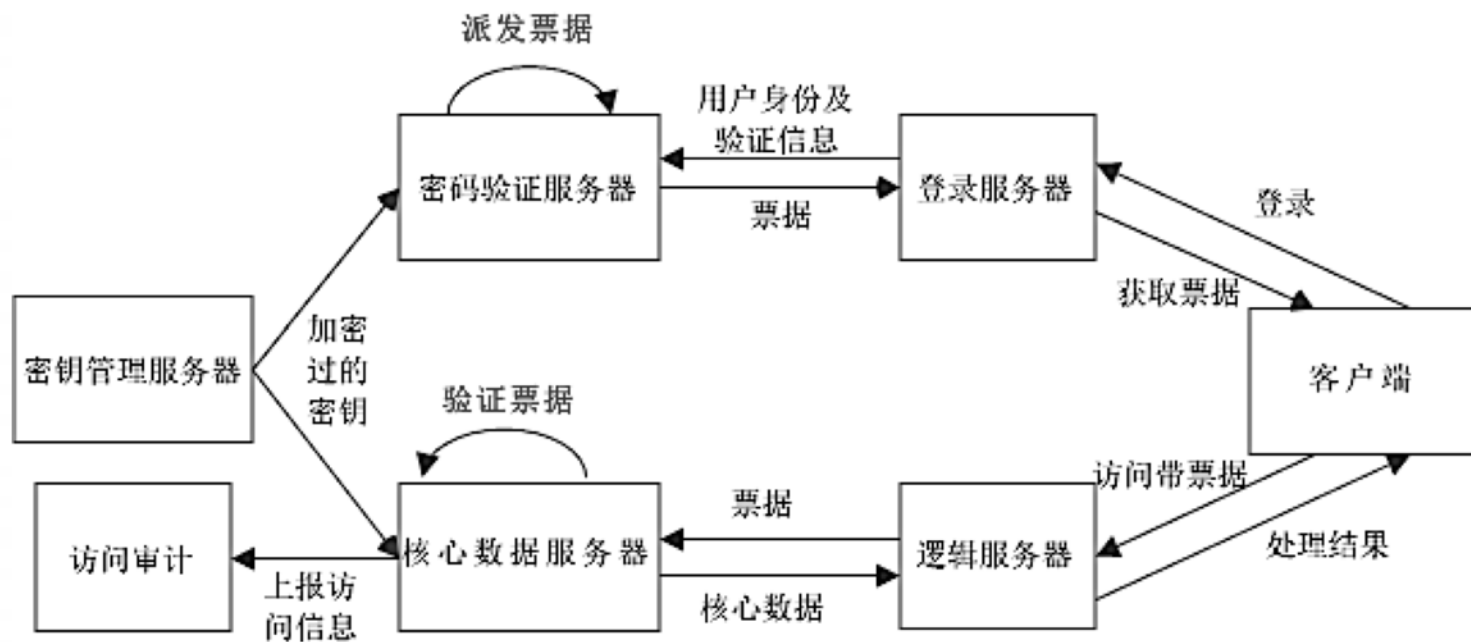
质量问题

成熟

payload维护成本

应对：
1. 首次扫描走变更流程
2. 允许业务自助报备、扫描


水平越权漏洞治理：同类漏洞下降85%



一些心得总结

安全运营的一些心得

- 安全责任归属：业务是安全主责
- 安全推动配合度问题：区分态度和能力问题、数据晾晒
- 正确表达安全诉求：说人话
- 安全高层支持：对标最佳实践
- 事件驱动的利弊：塞翁失马焉知非福
- 安全宣导：以终为始、全民战争

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that create a sense of depth and movement, resembling a grid or a series of overlapping planes.

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE