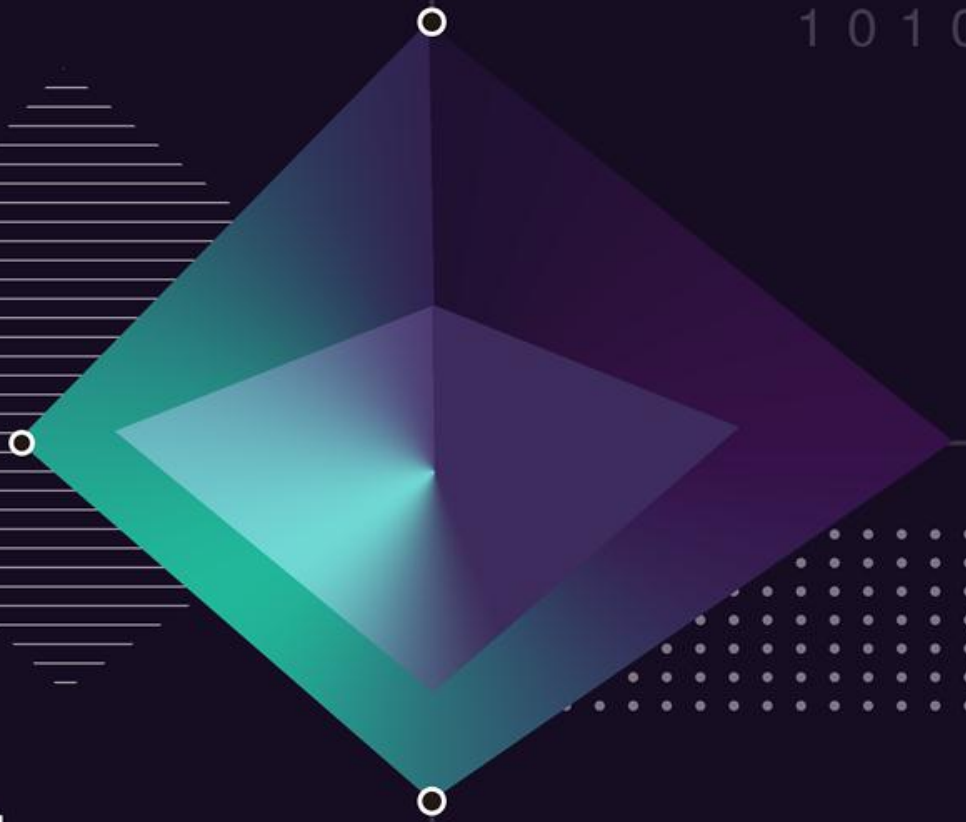
FREEBUF | 企业安全 俱乐部

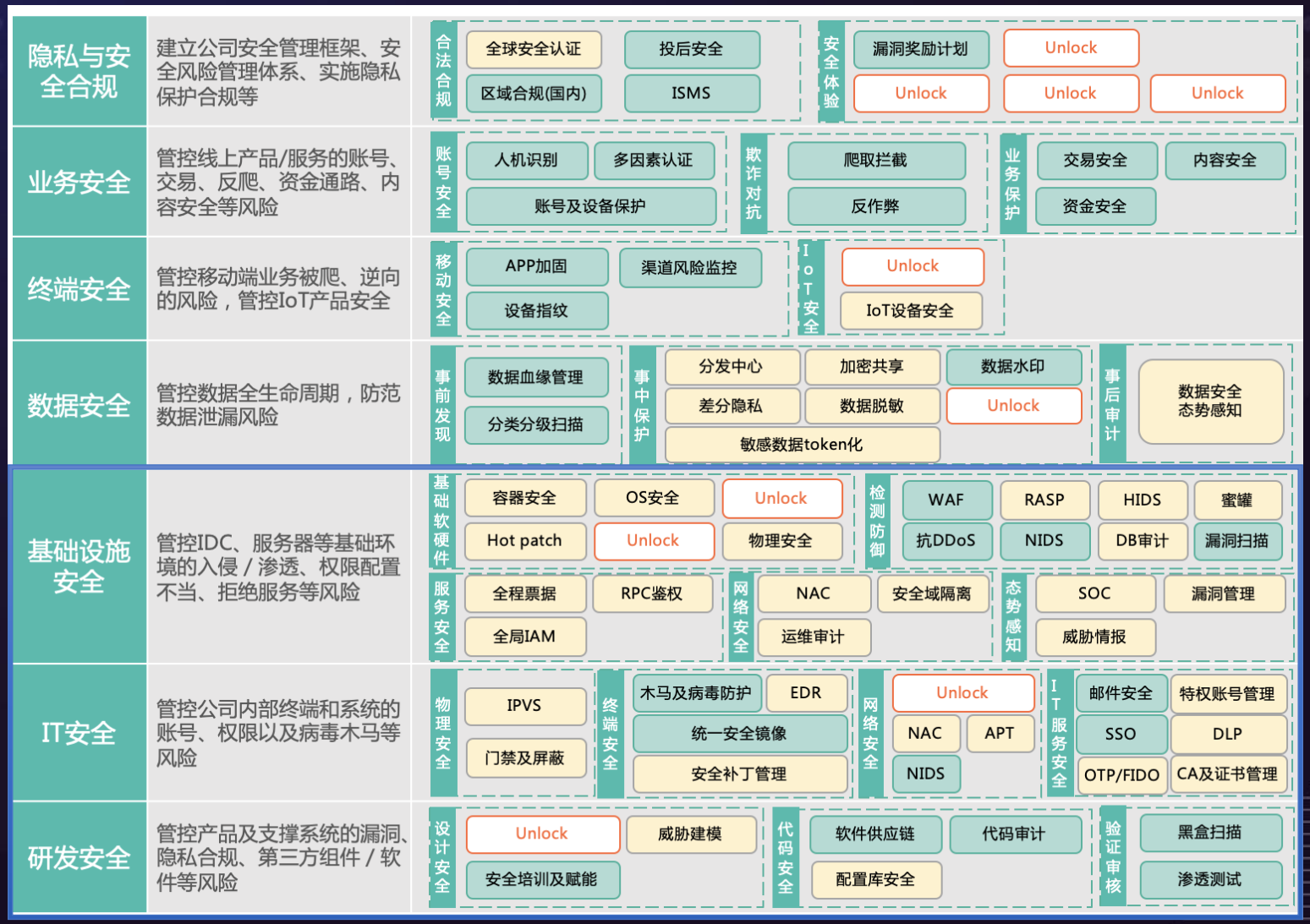
美团基础安全运营实践

演讲人：赵弼政
Title：美团基础安全负责人



2019 | 企业安全俱乐部
数据治理专场

基础安全范围


隐私与安全合规
建立公司安全管理框架、安全风险管理体系、实施隐私保护合规等
合法合规
全球安全认证
投后安全
区域合规(国内)
ISMS
安全体验
漏洞奖励计划
Unlock
Unlock
Unlock
Unlock
业务安全
管控线上产品/服务的账号、交易、反爬、资金通路、内容安全等风险
账号安全
人机识别
多因素认证
账号及设备保护
欺诈对抗
爬取拦截
反作弊
业务保护
交易安全
内容安全
资金安全
终端安全
管控移动端业务被爬、逆向的风险，管控IoT产品安全
移动安全
APP加固
渠道风险监控
设备指纹
IoT安全
Unlock
IoT设备安全
数据安全
管控数据全生命周期，防范数据泄漏风险
事前发现
数据血缘管理
分类分级扫描
事中保护
分发中心
加密共享
数据水印
差分隐私
数据脱敏
Unlock
敏感数据token化
事后审计
数据安全态势感知
基础设施安全
管控IDC、服务器等基础环境的入侵 / 渗透、权限配置不当、拒绝服务等风险
基础软硬件
容器安全
OS安全
Unlock
Hot patch
Unlock
物理安全
检测防御
WAF
RASP
HIDS
蜜罐
抗DDoS
NIDS
DB审计
漏洞扫描
服务安全
全程票据
RPC鉴权
全局IAM
网络安全
NAC
安全域隔离
运维审计
态势感知
SOC
漏洞管理
威胁情报
IT安全
管控公司内部终端和系统的账号、权限以及病毒木马等风险
物理安全
IPVS
门禁及屏蔽
终端安全
木马及病毒防护
EDR
统一安全镜像
安全补丁管理
网络安全
Unlock
NAC
APT
NIDS
IT服务安全
邮件安全
特权账号管理
SSO
DLP
OTP/FIDO
CA及证书管理
研发安全
管控产品及支撑系统的漏洞、隐私合规、第三方组件 / 软件等风险
设计安全
Unlock
威胁建模
安全培训及赋能
代码安全
软件供应链
代码审计
配置库安全
验证审核
黑盒扫描
渗透测试

猎豹并不能长时间捕猎
为了速战速决，捕猎前必须会耐心的物色对象，匍匐靠近，等待时机。

捕猎很酷，
捕猎前的铺垫一点也不酷。
捕获猎物，
酷的和不酷的事情都得做。

酷与不酷

- APT一个较难的目标
- 挖知名大厂产品0day
- 守卫数亿用户
- …

以入侵漏报的N种理由看“不酷”的工作

虽然我能检测很多webshell，但这一种方式“刚好”漏了

误报太多了，看不过来，其实已经告警了

这台机器的HIDS似乎有bug，日志没回传

后台规则引擎“正好”没工作

我都跟进了，但是“疏忽”了

这一台机器“恰好”没安装HIDS

主动发现	时间	事件名	所属业务	漏报主因	
				策略	运营
×					×
×					×
×					×
×				×	
×				×	
×				×	
×					×

新概念不解决工程化问题

One man army 可以用新名词做一个Demo
在实战中，也能会发挥一定的作用

但是在大规模组织面前，有时只是一个玩具
举个例子：
1个人的反爬、业务安全 vs 上百人的团队
1个人的HIDS vs 几十人的入侵检测团队
1个机器学习的demo vs 几十人的AI实验室
1个人的威胁情报爬虫 vs 爬虫、算法、卧底

工程化的背后全是赤裸裸的钱

挖出1个安全漏洞
审核1段代码找出所有漏洞

找出1个攻击

扫出一些漏洞

VS

20亿行代码/20w个项目/日均2000次迭代
找出所有漏洞

24*7*365 任意时段数十万任意机器5分钟内捕获到每一个类似的攻击并积极响应闭环

没有/很低误报的情况下把漏洞描述、修复方法、验证方法自动化的发给研发还不能漏掉

长期稳定全覆盖的产出要求HC、钱、时间、经验、组织化保障

非不能也，实不为也

大规模系统的问题，都有现成方法论
给专业RD、SRE、QA、PM、数据分析资源都能解决

- 稳定性、兼容性与覆盖率
- 数据对账
- 支撑工具
- 高可用
- 质量
- 资产管理设施
- 发布管理设施
- 基础设施的安全特性
- 安全开发框架
- …

安全运营：做真正对安全结果负责的人

酷与不酷的事情都做

拿到结果收获回报

按效果付费
按结果激励
vs
按技术付费

催生安全运营为主的细分岗位

“对问题进行分析、诊断，发现症结后，协调资源，实现目标的持续过程，称为（安全）运营”。

——《我理解的安全运营》

评价安全运营的好坏

实例

- 不评价，看老板心情

  没有数据量化，无法衡量进步

- 罗列“原始”数据或事迹

  罗列数据，不等于衡量好坏

  共计挖掘严重漏洞2个，高危漏洞61个，中危漏洞24个，低危漏洞 35个。挖掘漏洞总计122个

- 主观打个分数

  从30分提升到了60分

  技术沙盘新增了AI、ML、UEBA，比原来多3项

  技术的领先，不等于结果的好坏

解决方案：

设计指标，客观描述能力好坏，对齐目标，鼓励期望行为

开启指标评价之前，正确的认识指标的局限性

核心指标： 评价工作好坏的唯一标准
辅助指标： 必要非充分条件，描述趋势

警惕：
考核什么，很容易得到什么，但未必是期望的结果。
如果确定自己在做正确的事，有时可以忽略短期的指标数据。
指标不一定是正确的，应开发自动化系统积累数据。

领域	子领域	项目	指标
入侵对抗	预防	高危端口	**入侵事故** 止损时长
	缓解	WAF	覆盖率 拦截开启率 **漏拦截次数** **误拦截次数**
	检测	HIDS	**检出率** 覆盖率 健康度 数据完整度 **策略覆盖度**
		NIDS	**检出率** 覆盖率 可用性 数据完整度 **策略覆盖度**

HIDS运营经验分享

不同阶段，使用不同的指标驱动描述
挑战1： 架构合理性
挑战2： Bug、Bug，还是Bug
挑战3： 覆盖率
挑战4： 数据完整度
挑战5： 模型、误报
挑战6： 检出、策略覆盖度

研发安全填坑分享

SDL人尽皆知，做到的没几个

人工审计：个体差异大、覆盖率低

自研扫描器：不敢扫、URL覆盖、Poc

白盒审计： 1万个告警，4个有效漏洞

考核指标：外报高危漏洞

应急响应填坑分享

坑1： 来活就干，未关注情报准确性，紧急度
坑2： 默默救火，没知会到合适的决策者，不会讲“人话”
坑3： 慢慢救火，责任心被质疑
坑4： 情报慢人一步，应急全靠朋友圈
坑5： 应急过程不维护TimeLine
坑6： 复盘松散不深刻，疲于奔命反复救火

考核指标：止损时间、根因重犯

总结

基础安全涵盖了主要的安全攻防对抗领域。

做得不好时，外报漏洞、事件会时刻提醒管理层。
做得好时，则成为组织幕后英雄，无人问津。

身为安全工作者，拿人钱财替人消灾。
酷与不酷的工作，都要做好，才能实现目标。

规模较大的公司，受限于安全人员规模，工程化是最大的挑战。
使用数据量化的方式，持续驱动主要矛盾收敛。

安全运营人员，是无数血泪事故培养出来的真正为结果负责的英雄。

THANKS