字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY

字节跳动安全事件运营体系建设

字节跳动安全中心
陈明

实战攻防

关于我

- 目前在字节跳动安全中心团队负责安全事件运营工作
- 曾在腾讯云先后负责DDoS防护产品和云平台安全
- 10年信息安全从业经验
- CISSP、CISA、CCSK

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

大纲

安全事件运营体系介绍

01

安全运营做什么
安全运营怎么做

运营落地思路

02

痛点和难点
如何应对

未来展望

03

从繁琐的运营工作中抓住本质

实战攻防

Empower Security
Enrich life

PART 01

安全事件运营体系介绍

安全事件运营做什么

负责公司反入侵相关安全事件的运营，包括告警和规则运营、分析研判、溯源取证、调查整改，并为结果负责

涵盖国内各类业务

覆盖主要安全产品和能力

服务器：HIDS
网络：NTA、WAF、防火墙、IOC情报
终端：防病毒、EDR
数据：DLP、代码泄露监测
应用：行为分析和异常检测、邮件安全、身份认证、RASP

应急响应和HVV

主导开展应急响应
组织HVV防守工作

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全事件运营体系

流程阶段

资产监控 → 风险发现 → 风险隔离 → 取证溯源 → 复盘加固

梳理资产，增加监控组件

动态策略，感知风险

切断入侵路径，及时止损

查找蛛丝马迹，寻找入侵源头

降低风险面，提高安全门槛

运营支持

- **服务器:** HIDS
- **网络:** NTA、WAF、FireWall、IOC
- **终端:** 防病毒、EDR
- **数据:** DLP、代码泄露监测
- **应用:** 行为分析和异常检测、邮件安全、身份认证

资产要覆盖全

- 可视化检测
- 机器学习
- 关联分析
- UEBA
- 资产定位

策略要完善

终端: 样本查杀、EDR、MDM
网络: DNS、FireWall、WAF、VPN
应用: SSO及下游系统、邮件、账号、IM系统、权限回收

调查分析
- 样本上下文关联分析
- 文件、帐号触碰记录
- 横向移动记录
- 样本行为分析

安全加固
- 更新监控策略
- 部署拦截规则
- 清理“暗”数据
- 修复漏洞

告警单量
- 关键威胁展示
- 事件跟踪处理
- 事件归档

告警单要运营

入侵溯源
- 样本指纹库检索
- MitreATT&CK作战图
- 商业、开源情报检索
- 社工分析

平均检测时间 MTTD

平均响应时间 MTTR

实战攻防

Empower Security
Enrich life

难点和痛点

漏水

资产覆盖、规则完整度
有效的检测和防御

海量告警

如何找到真实有效的告警
如何找到最需要关注的告警

速度（MTTD、MTTR）

和攻击者的赛跑，事后发现几乎无济于事
运营成本高，分析和处置繁琐

PART 02

运营落地思路

运营思路

基础安全能力的覆盖

确保各项基础安全能力的全覆盖

优先关注内网告警事件

相比外网，需要优先关注内网环境的告警

重点环节设防、保护核心资产

针对入侵中的关键环节和核心资产重点保护

红蓝对抗，以攻促防

通过持续不断的红蓝对抗去暴露和发现防守中的薄弱点，持续改进

借鉴业界成熟框架，查漏补缺

参考att&ck、killchain框架，确保每个ttps都能覆盖

专项收敛风险，从根源解决风险

共性问题通过专项形式推动收敛，从源头入手，规避风险产生

实战攻防

基础安全能力的覆盖

持续建设和完善

从源头和关键节点入手，四两拨千斤

上线卡点，高风险资产重点覆盖

重点环节设防、保护核心资产

边界突破

网络：私搭wifi治理、wifi认证
异常（非常用设备、IP、多终端、多地域）、VPN盗用
EDR：终端入侵检测、钓鱼、水坑攻击
互联网暴露面：收敛对外暴露的高危端口和服务

横向移动

ueba：账号、IP行为基线（网络行为、各类应用系统操作、身份认证）
敏感系统操作：跳板机、代码平台、数据分析平台、任务管理系统

围绕数据和核心系统

数据：有哪些敏感数据、触碰数据的路径有哪些、针对数据库的操作审计、本地sql工具直连、后台系统操作监控、通过票据定位到人

核心系统重点保障

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

策略实现不难，难的是如何运营

通过wifi、vpn接入身份和sso身份比对发现账号盗用

user_login_risk

序号	ip	账户异常标签 ...	源用户登录时间 s...	网络持有人登录时...	盗用源用户名 src...	源用户部门 src_dep	源用户序列src_seq	网络持有人 dst_u...	网络持有人部门 dst_dep
1	[redacted]	sso_wifi	2021-07-03 19:...	2021-07-01 17:2...	[redacted]	[redacted]	技术	[redacted]	[redacted]
2	[redacted]	sso_wifi	2021-07-03 16:...	2021-07-01 23:0...	[redacted]	[redacted]	技术	[redacted]	[redacted]
3	[redacted]	sso_vpn	2021-07-03 13:...	2021-07-03 12:0...	[redacted]	[redacted]	技术	[redacted]	[redacted]

需要通过告警降噪，从技术和管理两个维度去持续优化

实战攻防

Empower Security
Enrich life

如何做告警降噪

1

告警量小，不是影响MTTR的关键原因则无需降噪

2

告警数据分析
规则分析
基于已知的特征降噪
多数据源关联打分
ueba、机器学习

3

告警产生的根本原因
能否不让告警产生

举例：NTA告警降噪

办公网nta两周告警量在40万条以上，单日告警量接近3万

数据分析：占比最大的为其它攻击利用（主要为矿池域名访问）、Sql注入（内部黑盒扫描）、信息泄露（未按目标系统聚合）
检测逻辑：部分规则只检测请求，未关联响应
降噪思路：
1、规则优化，关联响应及会话
2、针对不同规则的检测逻辑做告警聚合
3、内部扫描加白
4、恶意域名封禁，阻断访问并给予引导
5、关联终端、网络等其它数据
6、ip行为建模，挖掘更高优的告警

专项收敛风险

共性和经常发生的问题不能只是处理单个case，需要进行根因分析并对症下药

案例：发现内网出现大量存在远程代码执行的系统

根因分析：1、由于办公网到生产网的网络隔离，部分研发为了方便操作线上服务器，自行搭建webshell平台 2、部分研发同学认为在内网很安全，不清楚此举对公司的危害

应对方案：联合运维、安全培训、研发团队启动专项 1、加强安全意识宣贯，让研发同学意识到危害 2、完善制度，加入安全红线 3、加强检测，定期通报违规 4、优化跳板机体验

从根源着手，更加前置的解决问题

通过安全意识宣贯提升员工的敬畏之心，
收敛利用公司资源挖矿的行为

通过接入SSO认证、使用身份凭据的
方式解决弱密码问题

优先关注内网告警

内网不安全

- 员工会普遍认为内网很安全，反而放松警惕，认为内网安全问题不重要
- 外网系统有严格的上线卡点（SDLC），每天遭受大量攻击（SRC、黑客等）
- 以上两点导致内网的安全问题更多

依赖人的安全一定会漏水

- 依赖员工安全意识的防护体系一定会漏水
- 安全意识培训仍需要做，可以把及时反馈也做为目标之一

ROI更高

- 会涉及更为敏感的系统和数据
- 相比外网告警更好治理
- 整体量级更少

红蓝演练，以攻促防

定期演练

尽量使用不同的
攻击手法

针对性演练

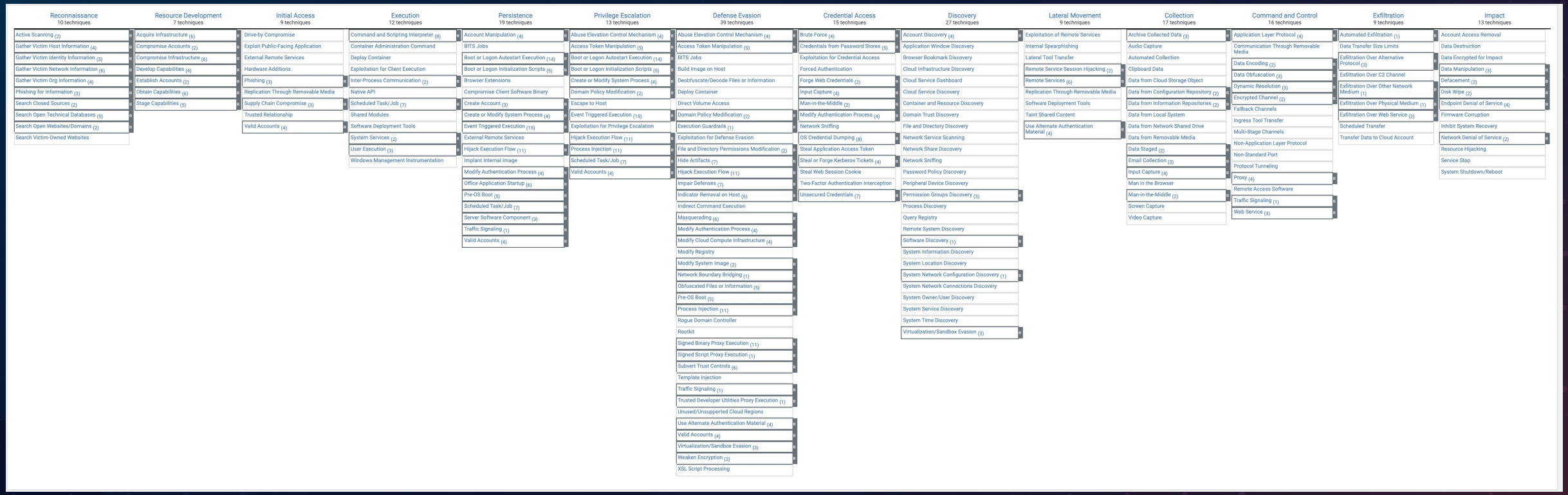
对补齐的能力点
针对性检验

持续改善

确保改进措施落地

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

借鉴业界成熟框架，查漏补缺



实战攻防

Empower Security
Enrich life

PART 03

未来展望

从繁杂的工作中抓住本质

安全能力的持续覆盖

持续完善各类安全产品和能力的资产及策略覆盖，持续提升单点检出及防御能力

运营效率的持续提升

持续关注MTTD、MTTR，提升运营团队综合作战能力

风险的持续收敛

持续不断的分析根因，从根源收敛风险

平台的持续建设

结合业务和运营需求，持续完善SOC平台能力，为运营做好支撑

THANK YOU FOR READING

实战攻防

字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY