2019第三届顺丰信息安全峰会

2019 THE 3rd SF INFORMATION SECURITY SUMMIT

“切尔诺贝利”之痛

-- 情报驱动的安全运营

李燕宏

深信服安服BG安全总监

关于我

- 深信服安服安全总监，MSSP 安全运营架构师，12年+ HP、 RSA、微软以及KPMG等安全运营咨询项目合作实施经验。致力于SOC安全运营领域的研究，主要研究领域包括威胁情报分析、NSM网络监控、安全大数据分析建模以及安全运营成熟度等。

- 先后主持参与华为、腾讯、盛大、招行等大中型企业的SOC安全运营中心的建设与运营管理。曾任华为MS首席安全运营架构师，先后为华为MS建立了第一个以 Follow the sun 模式运作的 7*24 安全运营中心。

- 译有《网络安全监控实践》（Chris Sanders，前美国防部NSM架构师；Jason Smith，麦迪安公司高级分析师 ）、《情报驱动应急响应》（ Rebekah Brown ，Rapid7情报总监，前美NSA网络战高级分析师；Scott J.Roberts，麦迪安公司高级分析师，SANS情报讲师）

“切尔诺贝利”的影响

切尔诺贝利核事故可能成为5年之后苏联解体的真正原因，其重要程度甚至要超过我所开启的改革事业。

-- 前苏联总统 戈尔巴乔夫

一组数字：

- 9.3万人死亡
- 27万人致癌，250万人身患各种疾病

- 灭火共出动3000架次直升机，“自杀式”投放5000吨硼沙铅混合物
- 10+个师24万军队，60万人参与隔离区清理工作

- 180亿卢布
- 后期消除影响耗费累计2000 亿美金；

“切尔诺贝利”事故过程复盘

堆芯毒素积累，
安全测试条件无法满足

带病测试失败，紧急按
下停机按钮，设计缺陷
导致堆芯爆炸

7分钟后，第一批消防官兵
抢险，无防备下仅少数幸存

专家组现场调查，
34小时后撤离小镇居民

外部侦测到核辐射对苏联施压，
67小时后官方才首次对外公告

“事故”对情报工作的启示

1. 技术操作层面：

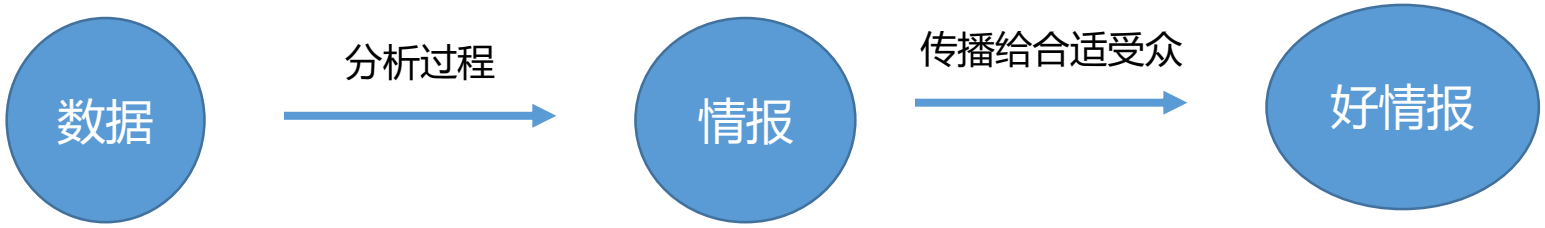
- 内部情报搜集不容忽视
- 情报传递的时效性
- 情报传播机制是否公开透明

2. 管理决策层面：

- 情报内部传播渠道是否通畅
- 外部情报对自身的影响

情报的概念

网络威胁情报（CTI）：



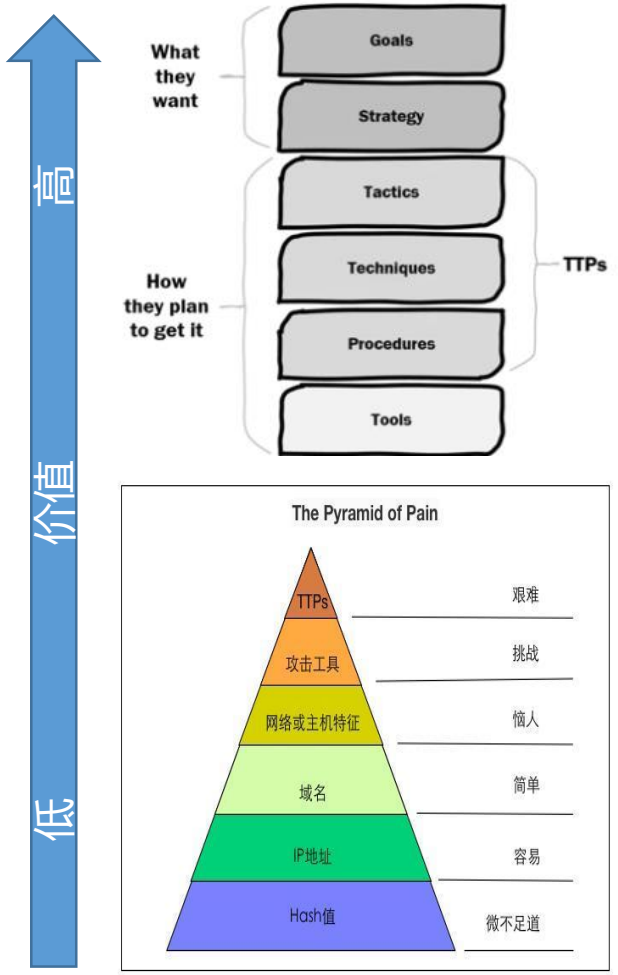
痛苦金字塔模型

1. **战术情报**：受众一般是安全运营中心（SOC）分析师或应急响应人员。通常是低等级的且极易过时的信息，比如IOCs特征、低阶TTPs（ Tactics/Techniques/Procedures）。

2. **作业情报**：受众包括高级数字取证和事件响应（DFIR）分析师和其他 CTI 团队。通常包括黑客攻击的相关信息和高阶TTPs内容。甚至包括有关指定威胁组织的特点、能力和意图等信息。

3. **战略情报**：支撑企业高管人员对风险评估、资源分配和企业战略做出正式决策。通常包括安全态势、威胁组织的动机和分类。

e.g. 一个漏洞利用情报的例子

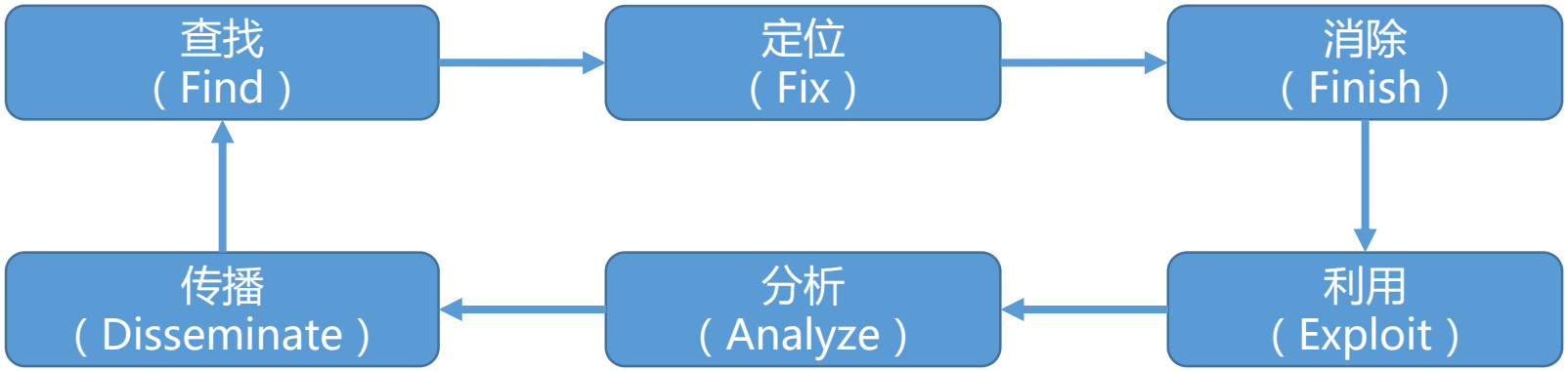


情报运作的 F3EAD 循环

1.目标：威胁方向
2.来源：内外/商业/开源
3.种类：战术/作业/战略

识别攻击者行为：可能针对的目标、通信渠道以及攻击方法

往往对接 IR 流程，进行威胁的遏制、缓解和消除



受众：
IR/溯源团队：战术/作业情报
管理层：战略情报
第三方：取决于目标、意愿

攻击者TTP总结，
制定时间表和killchain分析
深入的恶意代码分析

其它IOCs（ IP地址、URL地址、文件哈希值、反向DNS、邮件地址以及JA3指纹等）、Exploit代码、恶意代码、漏洞CVE、黑客组织研究报告等

情报驱动安全运营的理念

威胁为中心

- 利用所有数据源，结合情报分析攻击
- 注重对未知威胁的检测能力
- 制定应急预案并演练
- 循环流程

安全运营建设的框架体系

业务
Business

- 业务目标
- 绩效指标
- 内部支持
- 外部关系
- 业务交付
- 供应商管理

人员
People

- 人员架构
- 人员培训
- 职业认证
- 团队经验
- 技能评估
- 发展通道
- 管理能力

流程
Process

- 运营流程
- 分析流程
- 技术流程
- 业务流程
- 知识管理
- 内控

技术
Technology

- 技术框架
- 数据收集
- 监控分析
- 情报关联
- 数据建模
- 可用性保障

安全运营建设的业务痛点

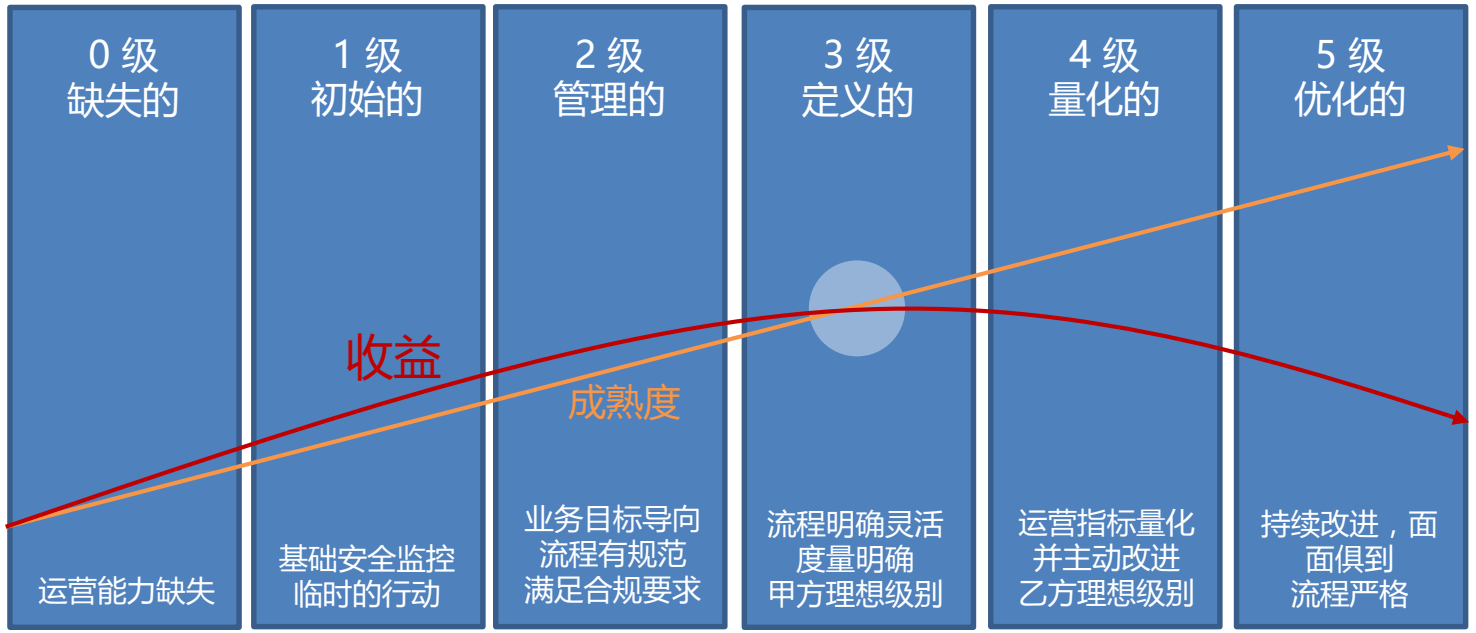
面对威胁变化的技术手段有限

- 项目产品上线交付了，后期运营跟不上
- 海量日志，关键事件无法冒泡
- 情报缺失，对于威胁事件无法精准识别
- 威胁处置无法形成闭环
- 缺乏固化的威胁处理流程

很难组建完整的安全人才梯队

- 人员技能短板很难补齐
- 缺乏足够的人力资源
- 高级安全人才流动性较大
- 安全人员的职业发展通道问题

安全运营建设的提升建议



考虑点：

1. **早阶SOC成熟度（0-1.5）提升较为明显，中阶SOC成熟度（1.5-3）能力爬坡则相对困难。**
2. **中小企业则可借助 MSSP 服务（Managed Security Service Provider）转移风险与成本，大企业可引入MSSP外部资源（例如：7X24 合作）来持续提升成熟度；**

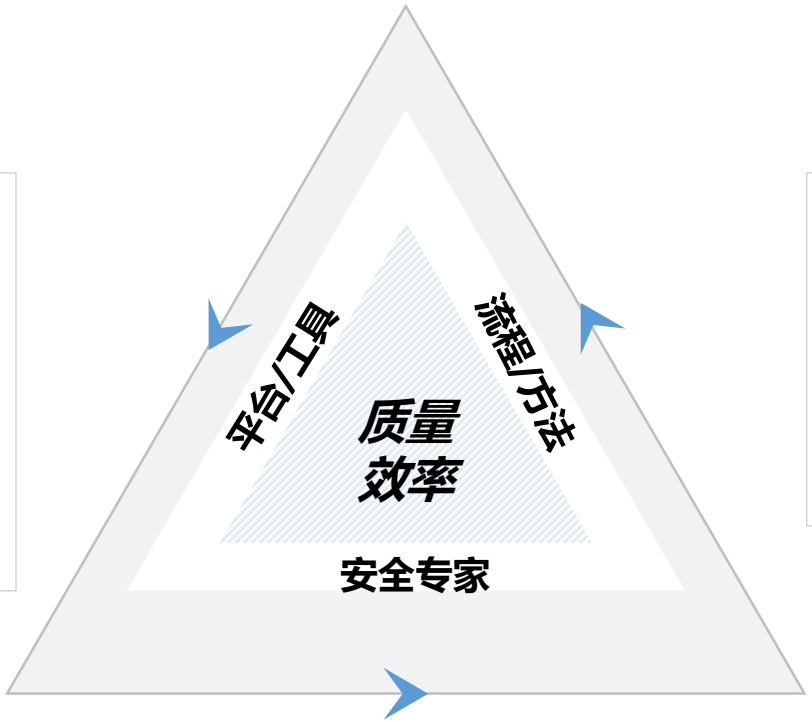
MSSP 联合安全运营模式

安全运营能力	漏洞预警响应　威胁监测与主动响应（DR）　事件响应（IR）
安全专家梯队	企业自建安全团队　驻场安全运营专家　远程安全运营专家
安全运营中心	安全设备日志　精准的威胁信息　外部威胁情报　需要保护的设备资产　AI引擎　Usecase 定制建模
安全产品模块	下一代防火墙　终端检测响应　漏洞扫描　安全感知平台　……

MSSP 服务的选择考虑

持续进化的平台/工具

- 安全运营平台的**大数据AI能力**；
- 漏洞管理平台的**威胁情报能力**；
- 安全能力成熟度评估工具；
- 安全风险评估工具；
- 半自动化渗透测试工具；
- 应急响应工具；



标准的流程与成熟的方法论

- 能否通过**客户服务监控大屏**保障服务流程的可视化；
- 能否通过**工单系统**保障服务流程的标准化；
- 是否具备成熟的**安全能力成熟度评估方法**，

持续监测与快速响应

- **7*24小时持续监测能力，精准预警；**
- **7*24小时安全专家值守，快速响应；**
- **服务工程师的现场支撑能力；**


THANK YOU