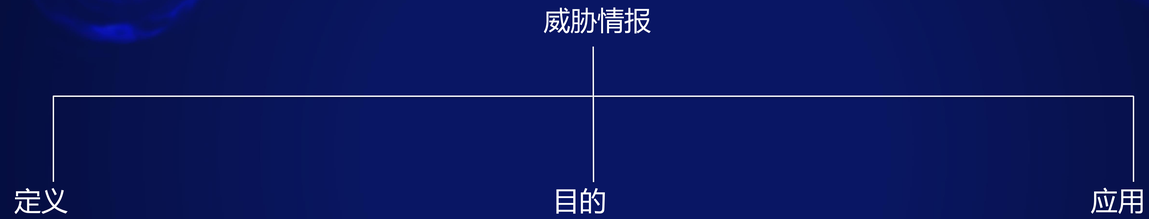
CTIC 2019网络安全分析与情报大会

CYBER THREAT INTELLIGENCE CONFERENCE 2019

威胁情报的实践应用

潘盛合
顺丰集团•信息安全与内控处信息安全负责人


威胁情报
定义
目的
应用

01.什么是威胁情报?

Gartner（2014）：一种基于证据的知识，包含**场景、机制、指标、影响**和**可操作建议**。描述了现存的、或即将出现针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

01 场景

3月1日，发现某团伙使用**IP、**工具对我司会员系统进行攻击

02 机制

在**处没有进行**验证导致攻击者可以对此进行攻击

03 指标

对业务系统进行长达3个小时的攻击

04 影响

影响了该系统的可用性

05 可操作建议

建议将其IP封禁后及时修复这方面的漏洞

02.使用威胁情报的目的?

减少不确定性

除企业内部信息外，引入外部威胁情报可降低自身风险不确定性

预测潜在威胁

基于外部数据，建模预测内部潜在威胁

支撑安全决策

通过对外部威胁，内部潜在威胁评估作出进一步安全决策

03.威胁情报的应用

情报集市　场景应用　情报运行　问题探讨　方法尝试

情报集市


传统安全
IP位置
IP代理库
IP真人度
IP信誉
恶意DNS
恶意软件
恶意URL
漏洞情报
业务安全
失信名单
被执行状态
诉讼信息
欠税数据
工商信息
企业存续
竞争对手
业务产品
SOOPAT专利
国家专利查询
招聘数据
经营数据
手机黑卡
手机小号
外卖手机
手机归属地

场景应用 - 传统安全


防护
检测
响应
预测
系统加固
隔离系统
攻击防护
异常检测
事件风险评估
事件缓解
修复矫正
策略变更
事件调查
风险评估
威胁预测
基线调整

场景应用 - 业务安全

人资线

招聘准入
员工流失

财务线

月结风险
代收风险
采购风险

市场线

营销活动
同业竞争

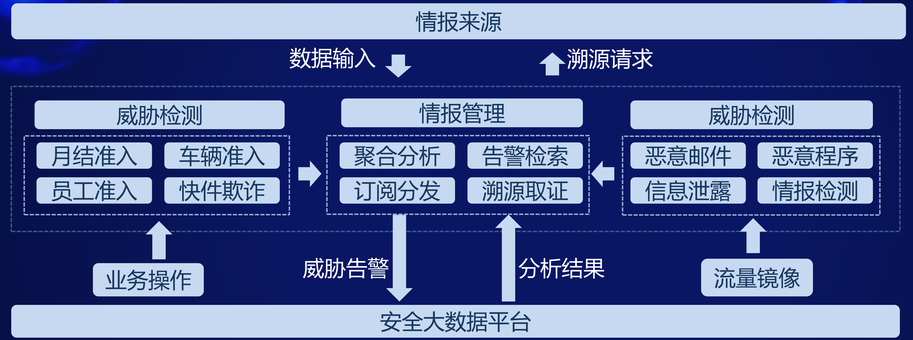
营运线

供应商风险
快件欺诈

运力线

承运商风险
车辆风险

情报运行


情报来源
数据输入
溯源请求
威胁检测
月结准入
车辆准入
员工准入
快件欺诈
情报管理
聚合分析
告警检索
订阅分发
溯源取证
威胁检测
恶意邮件
恶意程序
信息泄露
情报检测
业务操作
威胁告警
分析结果
流量镜像
安全大数据平台

问题探讨

场景匹配度低

情报更新频率

情报合法合规

情报质量不一

方法尝试

多家交叉验证

丰富场景数据

隐私脱敏加密

加快更新频率

畅想未来-“四更”

更广情报范围

更低情报花费

更快检测威胁

更好响应事件

THANK YOU