智慧运营 纵深监测与响应

张志鹏 斗象科技安全顾问

TCC——斗象科技能力中心（Tophant Competence Center）

专注于以下安全领域：

- Web安全研究，0-Day挖掘，技术分享
- 突发事件，应急响应技术支持
- IoT智能硬件，包含固件安全、逆向分析、无线协议、智能APP等安全研究
- 机器学习，突破现有技术的不足，提升安全能力
- 企业级安全产品的安全研究和研发

— 提供前沿安全技术的研究与能力支撑

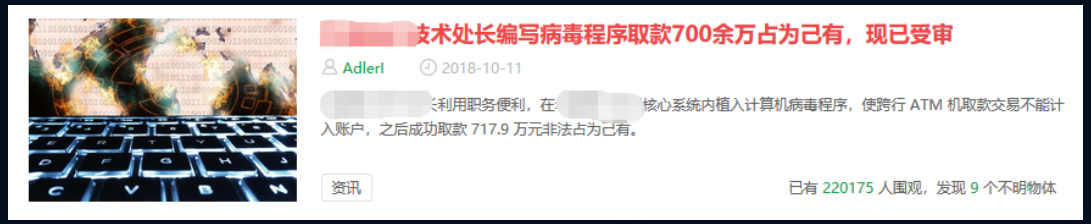
目录

近期的一些安全事件

外部入侵

12月---国外知名问答社区XXX遭黑客入侵，近一亿用户信息泄露；
11月---XXX酒店集团遭遇超大规模数据泄露，波及近5亿用户数据；
10月---美国运通XXX分公司数据库曝光，致70万人信息泄露；
10月---XXX航空数据泄露，940万乘客受影响。

内部风险

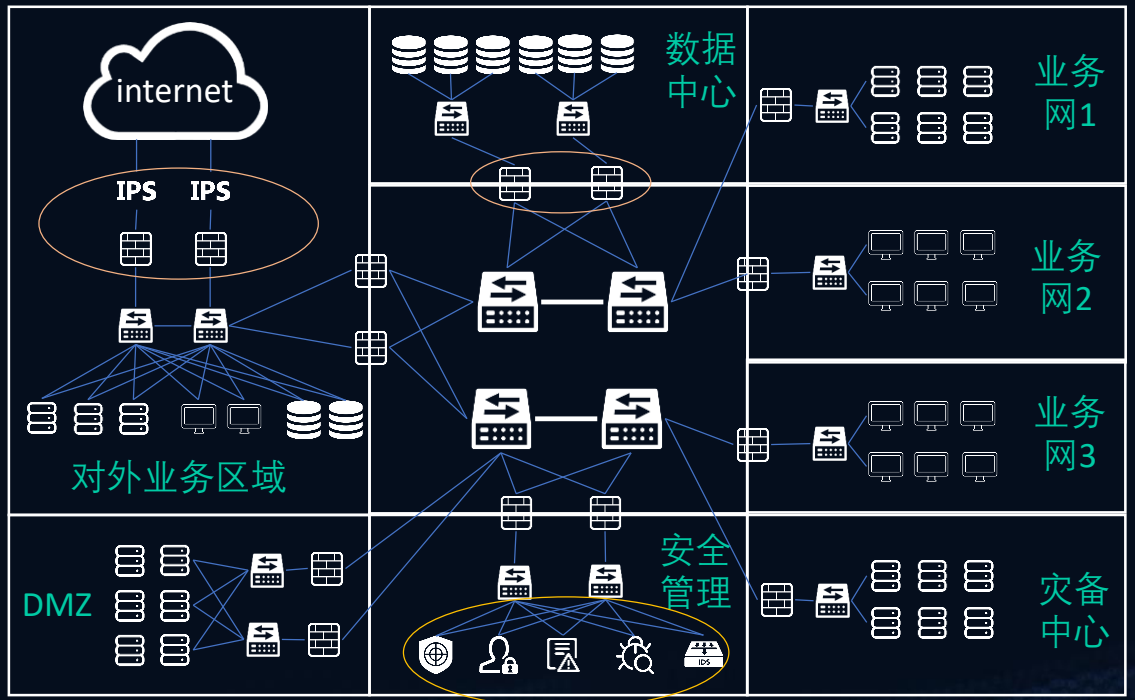


病毒木马

- 警惕Rotexy移动木马，三个月内已发起超过70000次攻击；
- “Satan”勒索病毒新变种在国内传播；
- KoiMiner挖矿木马变种入侵，超5000台SQL Server服务器被控制。

内忧外患

传统安全部署架构



懂安全，知需求，想做事

但

投入越多，设备越多，数据越多

报警来不及分析；
信息来不及关联
事件来不及响应；
数据来不及整理；

安全运营？

累

安全运营还要做什么？

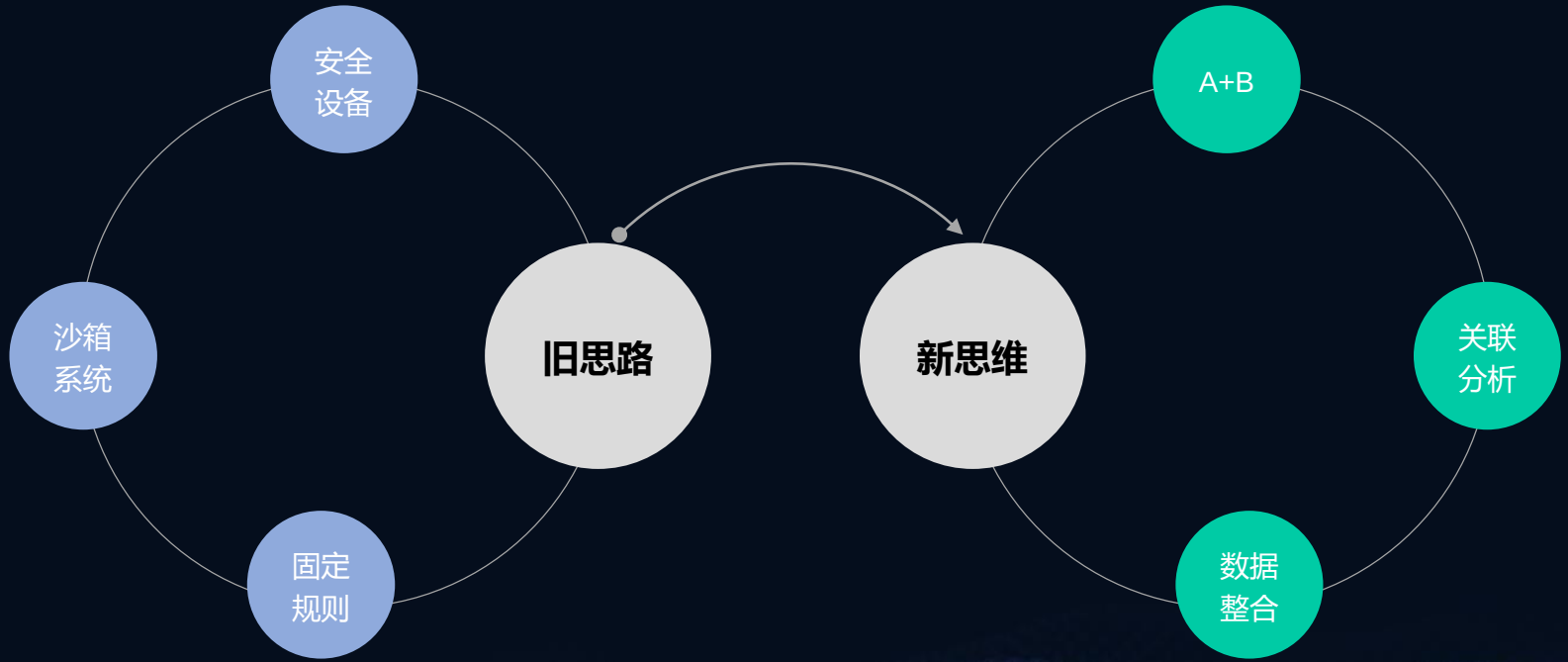
快 —— 应急事件响应速度要快

准 —— 数据监测能力要准

狠 —— 面对问题处理要狠

用一套解决方案实现解决问题快速定位、分析和解决的闭环流程，让安全应用简单、方便。

技术理念



如何做到多层监测及快速响应？

用机器语言代替人为判断

用全量数据代替局部分析

用关联分析代替固定规则

解决方案流程

原始数据

- 通信流量
- 设备日志
- 威胁情报
- ……

数据管理

- 数据提取
- 数据转换
- 数据加载

安全能力

- 入侵检测能力
- 漏洞分析能力
- 安全建模能力
- 安全情报能力
- ……

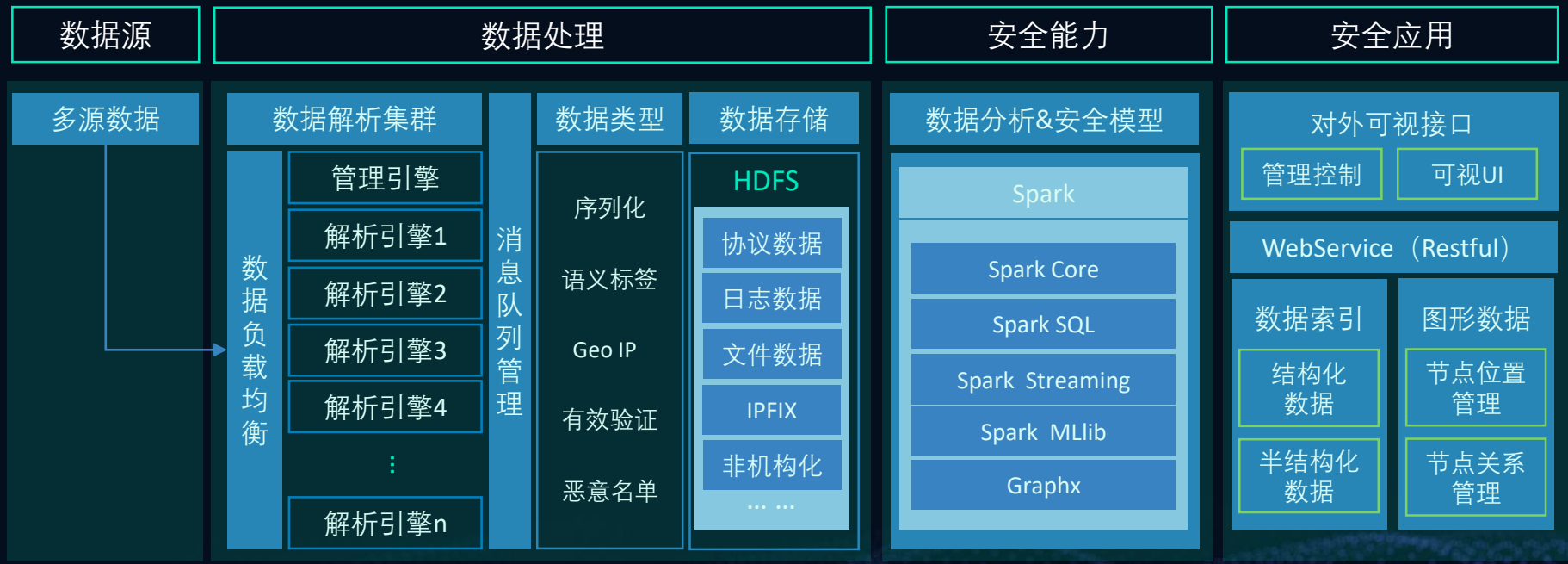
安全应用

- 事件关联分析
- 安全场景化
- 攻击溯源
- 安全态势可视
- ……

对多源数据进行统一管理，利用大数据分析及机器学习等技术，构建安全场景监测模板，多级关联，准确定位

多源数据如何管理？安全监测能力如何全面？安全场景如何关联？

大数据处理架构


数据源
数据处理
安全能力
安全应用
多源数据
数据解析集群
数据负载均衡
管理引擎
解析引擎1
解析引擎2
解析引擎3
解析引擎4
解析引擎n
消息队列管理
数据类型
序列化
语义标签
Geo IP
有效验证
恶意名单
数据存储
HDFS
协议数据
日志数据
文件数据
IPFIX
非机构化
... ...
数据分析&安全模型
Spark
Spark Core
Spark SQL
Spark Streaming
Spark MLlib
Graphx
对外可视接口
管理控制
可视UI
WebService （Restful）
数据索引
结构化数据
半结构化数据
图形数据
节点位置管理
节点关系管理

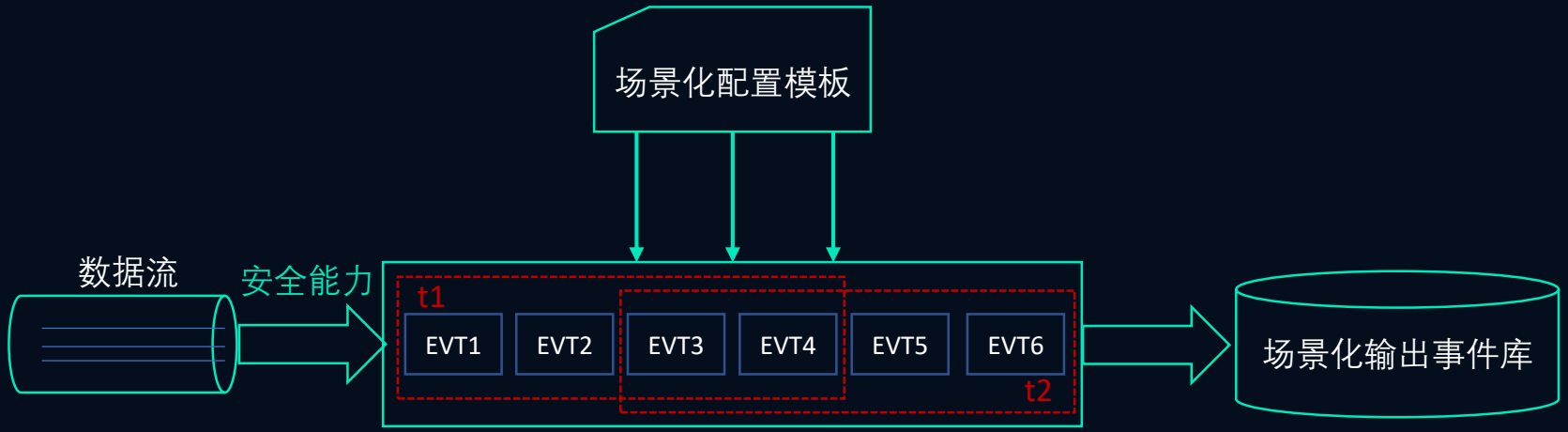
数据处理过程

数据解析	数据标签	数据去重	数据格式
将不同格式的数据，按照数据的类型进行内容识别工作，数据拆分成平台能识别的最小元素。	将解析后的数据进行标签化管理，例如资产的类型、协议数据的内容等。	将入资产库的数据进行去重处理，使得平台系统仅有唯一的一份可用资产数据。	将数据按照系统可读格式进行转存处理。

安全事件识别


格式化数据
基于规则的识别
格式化数据
基于统计的识别
格式化数据
基于模型的识别
暴力破解
弱口令
Web漏洞
扫描行为
爬虫行为
信息泄露
内网渗透
DB恶意事件
通用应用
特定资源访问频率
特定资源访问间隙
用户行为分析
.....
隐蔽隧道
恶意文件
恶意IP
WEBSHELL
恶意域名
.....
EVT1
EVT2
EVT3
EVT4
EVTn

事件场景化与关联分析


场景化配置模板
数据流
安全能力
t1
EVT1
EVT2
EVT3
EVT4
EVT5
EVT6
t2
场景化输出事件库

场景模板

基础信息

场景名称　场景描述　场景唯一ID　KC属性

场景事件威胁度　场景事件可信度　场景输出的事件类型

关联分析配置

关联事件逻辑分析　关联时序分析

事件检出配置

检测时间宽度　滑窗宽度　超时时间　事件属性　详情属性

归并关键key　归并聚合字段　归并更新字段　场景分析主题

案例分析-webserver漏洞攻击与利用（JavaDescRCE）

场景描述：企业Web应用服务器存在反序列化漏洞，被攻击者成功利用并反弹shell

安全场景模板

关联关系：　时序

逻辑关系：　or

事件：
- Java反序列化特征1-10
- Ongl表达式注入1-6
- Windows WMIC 命令行特征的出站通信流量

- Struts2注入攻击1，2
- Window cmd命令行特征
- Window powershell命令特征
- DNS隐蔽隧道通信

合并字段：　Dst IP

案例分析-木马病毒感染上线

场景描述：企业某台服务器感染病毒，并在内网肆意传播

安全场景模板

关联关系：　时序

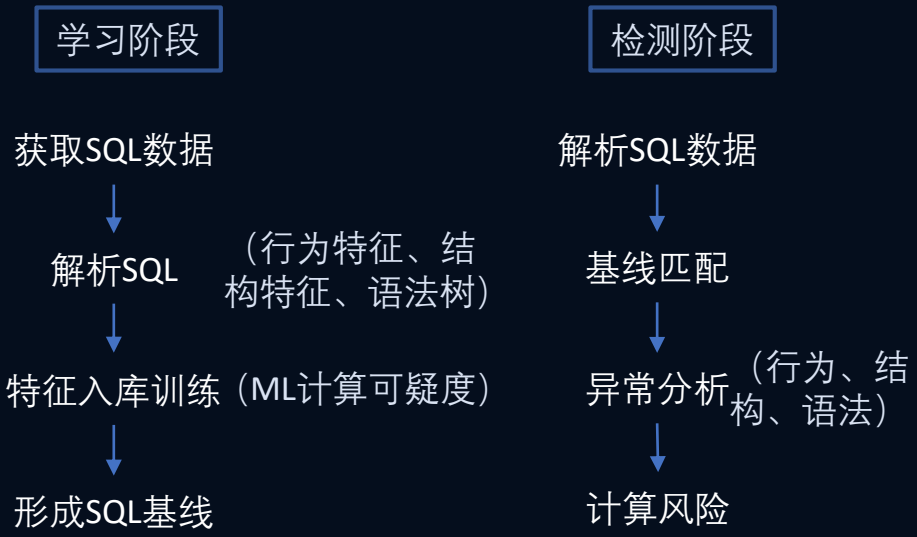
逻辑关系：　or

事件：
- 访问异常目标
- 流量中带有恶意文件
- 访问异常目标
- 隐蔽隧道通信（DNS/ICMP）

合并字段：　Dst IP

案例分析-SQL异常监测

- 监测流程



- SQL异常案例

```
select column_name from wp_column where id=35 and 1=2 union select
TABLE_NAME from information_schema.TABLES where
TABLE_SCHEMA=0x7770 limit 14,1;
```

Tabel&Command分析

[{wp_column=Select,**true**}, { information_schema.tables=Select, **false**}]

sqlField分析

[{wp_column.column_name,**true**}, {wp_column.id,**true**}, {information_schema.tables.table_name,**false**}, {information_schema.tables.table_schema,**false**}]

sqlRiskValue:110,疑似风险

案例分析-资产异常监测模型

信息安全的核心是保护资产的安全，随着资产变更而引入的风险更是繁多：未审批服务器上线；管理端口对外开放；新增的未授权端口、生产内网违规新增测试系统等。

- 资产归类细化

基本元素	(IP，主机名，操作系统，端口，MAC地址)
应用视角	(服务应用，应用组件，框架，开发语言，版本，域名等)
用户视角	(账号，常用登陆时间区间，地理位置)
访问关系	终端与服务的访问关系，账号与服务的访问关系，服务应用访问次数统计等

- 资产异常监测模型

资产识别	根据资产分类对多源数据进行资产识别、去重、管理
建立资产档案	对资产进行建模训练，建立资产管理基线
资产风险监测	异常新增端口、未授权IP访问、 账户活跃异常、异常外连行为、新增资产、异常访问源、异常时间访问等
资产动态管理	资产变更管理及可视化展示

优势与思考

FIT 2019

凡战者，以正合，以奇胜

FREEBUF | FIT

THANKS