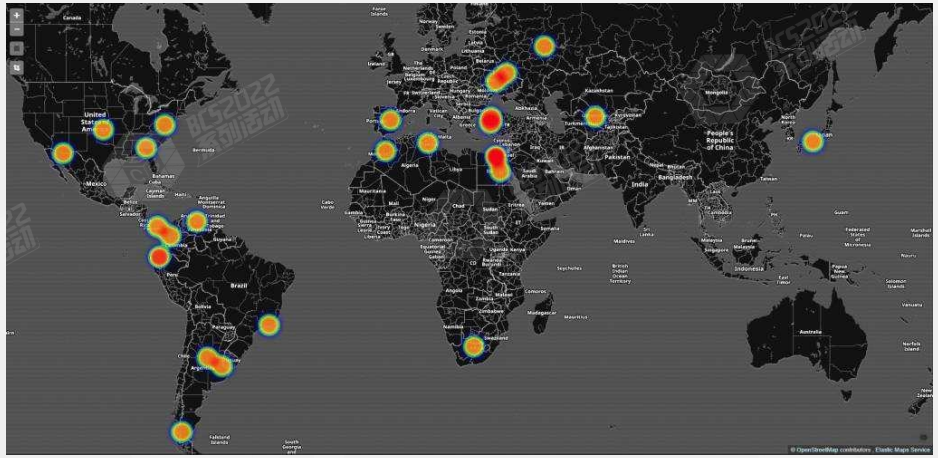
2022北京网络安全大会
2022 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音

自动化安全事件运营突破

北京国舜科技股份有限公司 - 董利伟

网络安全态势日趋严峻



BlackMoon僵尸网络事件

健康宝DDoS攻击事件

网络安全事件运营现状

威胁检测 | 分析研判 | 追踪溯源 | 处置响应

安全事件研判

每天成百上千条安全事件需要人工研判，大量无效告警造成运营难度提升

海量安全事件告警

每天来自众多不同类型的安全设备的安全事件告警

事件响应处置

是否针对有效告警进行处置以及加固?

众多安全设备

FW、WAF、IPS、ACM、NTA、APT... ...

事件溯源

针对安全事件进行有效溯源，复盘。

网络安全事件运营现状分析

- 数据覆盖广
- 数据来源多
- 数据量极大
- 数据异构性

- 安全设备告警检测逻辑不可见
- 海量数据中充斥的大量的误报
- 有效告警被淹没在无效告警中

- 孤立告警事件难于推理
- 重复低效的二次取证
- 不完备的资产实体库、研判过程缺乏知识指引

- 安全运营人员配备：
- 安全运营知识沉淀：

- 知识模型
- 知识交换
- 知识运用
- 知识迭代

- 度量的指标：围绕资产实体、围绕运营流程、围绕能力矩阵
- 如何选取度量指标

网络安全事件运营体系建设需求

严峻的安全现状

传统安全体系、安全架构遭遇瓶颈，需要进一步提升安全运营水平；合规性建设思想陈旧。

全新的安全形势

针对中国境内目标发动攻击的APT组织36个，处于活跃状态的APT组织至少有13个。

安全建设遇瓶颈

从现实中的网络安全建设看，多年来我们一直偏重于架构安全和被动型、防御型能力的建设

主动防御能力建设

传统的安全设备已无法提升安全能力，需要积极的开展主动防御能力的建设，网络安全建设要面向实战化

采集与检测

提供网络安全持续全面监控能力，及时发现各种攻击威胁与异常，特别是针对性攻击。

响应与处置

建立威胁可视化及分析能力，对威胁的影响范围、攻击路径、目的、手段进行快速研判，目的是有效的安全决策和响应。

预测与预防

建立风险通报和威胁预警机制，全面掌握攻击者目的、技战术、攻击工具等信息。

完善防御体系

利用掌握的攻击者相关目的、技战术、攻击工具等情报，完善防御体系。

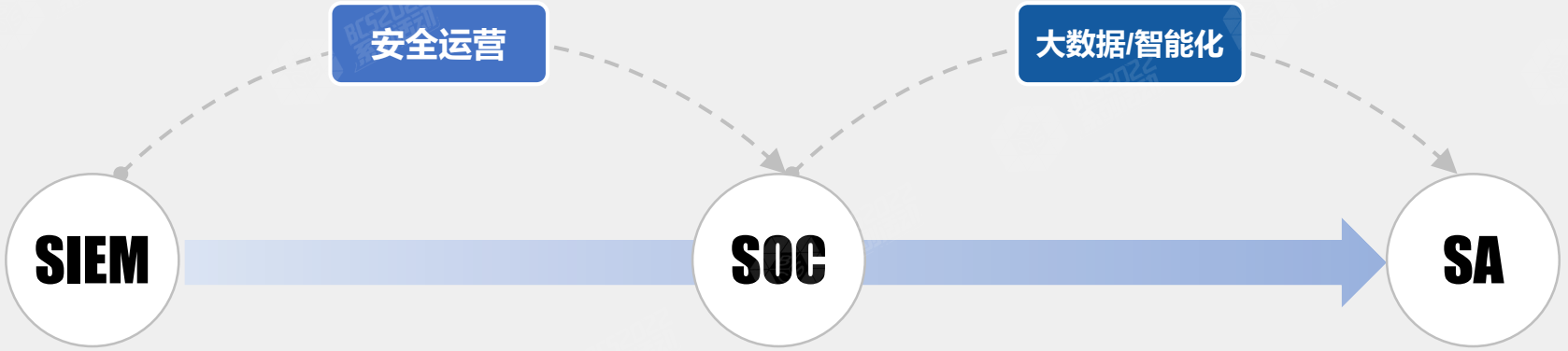
网络安全事件运营相关产品发展趋势

Endsley于1995年提出态势感知的概念：

- 定义：在一定时间和空间内观察环境中的元素，理解这些元素的意义并预测这些元素在不久的将来的状态。
- 目的：分析空战环境，快速判断当前及未来形势并作出反应。

业内标准：

态势感知是一种基于环境、动态、整体的洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应预警能力的一种方式，最终是为了决策与行动，是安全能力的可视化与落地。



安全信息和事件管理

负责从大量企业安全设备、企业应用和企业使用的其他软件中**收集安全日志数据，并进行分析和报告。**

安全运营中心

主要针对安全进行收集、分析和集中化管理，通过深度分析、统计和关联分析、及时反映相关资产的安全基线，能够为各类安全事件及时提供处理方法和建议。

态势感知

通过应用大数据技术，和智能化分析技术，体现了系统智能化的运维能力。使安全运营从数据采集、数据分析、响应处置完成闭环管理。

网络安全事件运营痛点分析

Alert ----------> Event ----------> Incident

安全告警

原始日志

SIEM/SOC/SA

关联分析

场景分析

场景分析

预警分析

分析研判

- 分析是什么攻击？
- 分析是否攻击成功？
- 分析攻击后的影响？
- 分析还原攻击过程？
- 应采取什么措施？

人工线下处理

处置响应

- 封堵IP地址
- 删除文件
- 禁用账号
- 卸载启动项
- .....

人工线下处理

MTTD

MTTR

网络安全事件运营体系完善思路

安全策略框架

- 覆盖所有的攻击行为
- 快速添加标准策略
- 策略进行灰度上线，满足可运营的标准

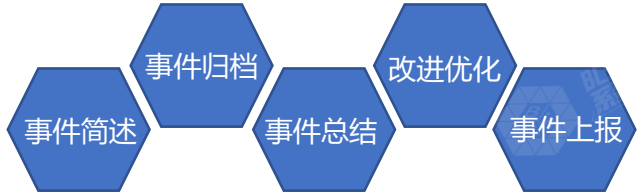
告警分析研判

辅助信息包含：受害资产的业务属性、漏洞情报、归属人；攻击资产的归属人、威胁情报、IP网段信息、资产登录信息、资产配置信息、资产日志信息、资产进程服务信息、资产联网信息

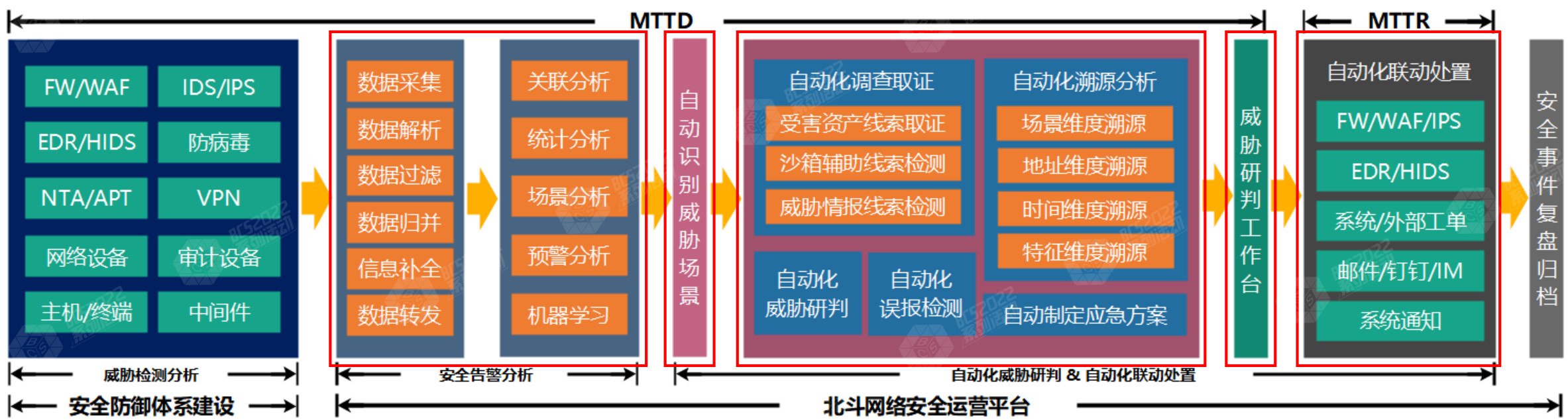
响应处置

复盘总结

事件简述、事件详情、事件归档；在事件总结中，反思不足和缺陷；对改进项进行排期、跟踪改进进度；完善现有运营体系



自动化网络安全事件运营方案



客户痛点

- 安全设备告警信息中的检测逻辑不可见，缺乏对安全告警逻辑的解释信息。对于安全告警的研判分析需要依赖大量额外的线索辅助分析。
- 安全事件分析研判、线索取证、定损评估、响应处置等过程完全依赖于安全运营值班人员的应急响应经验的网络安全知识储备。
- 网络中存在大量的误报告警信息，极大的消耗了安全运营人员对于告警的取证、分析研判的时间和精力。
- 安全事件溯源、拖线、复盘安全依赖人工下线处理，各部门协同作战存在很大挑战。

产品价值

- 通过自动化技术，完成安全告警的自动线索取证、自动威胁研判、自动误报分析、自动溯源分析、自动制定处置方案，从而极大程度提升安全告警研判和响应时间，**MTTD**从天级别降低至分钟级，**MTTR**从小时级降低至秒级。单个安全事件应急响应效率**提升50倍**。
- 将安全专家应急响应经验固化成剧本，通过平台的自动化技术，让“安全专家”7X24小时值守。
- 安全事件运营标准化、流程化，安全事件运营体系化、指标化。

THANKS