Alibaba Group 阿里巴巴集团 | 蚂蚁金服 ANT FINANCIAL

安全智能驱动的新一代SOC建设

谷安&安全牛 李华

1、ISOC的理念

2、ISOC能力建设

3、ISOC技术实现

4、ISOC建设难点

5、ISOC的市场分析

6、ISOC的主流厂商

传统SOC的问题

缺乏安全攻防对抗的能力

缺乏大数据处理的能力

缺乏安全智能分析的能力

缺乏有效响应协同的能力

缺乏专业人员运营的能力

新一代ISOC的理念

1、ISOC的理念

2、ISOC能力建设

3、ISOC技术实现

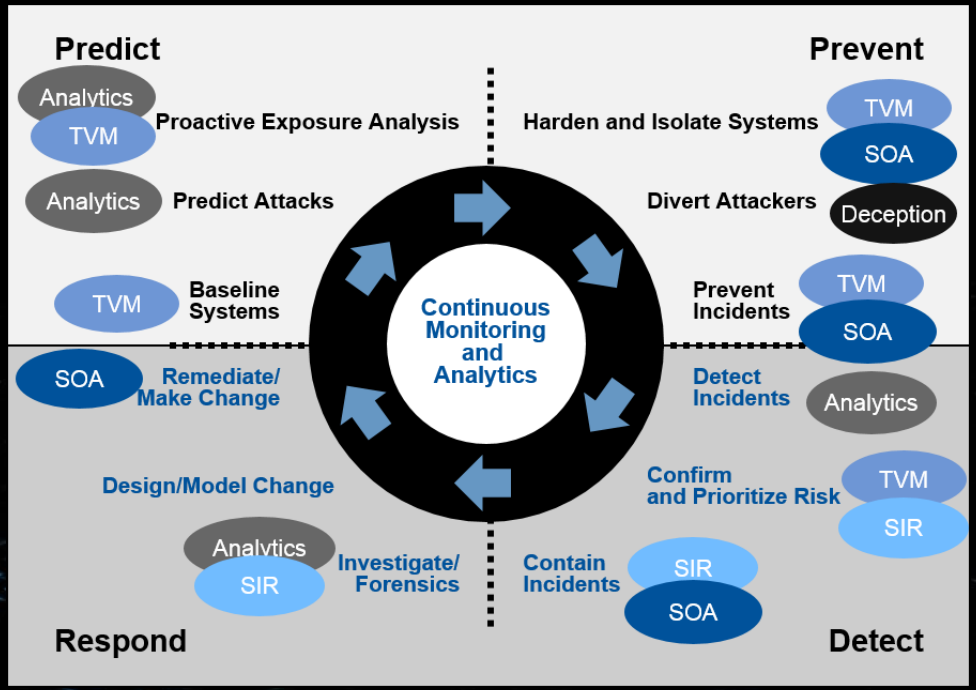
4、ISOC建设难点

5、ISOC的市场分析

6、ISOC的主流厂商

自适应安全架构

- 风险可见化：Visibility
- 防御主动化：Proactive
- 运行自动化：Automotive



安全防御

在新一代SOC体系中，SOC将为安全设备提供安全智能引擎和情报数据，采用深度防御策略，自动化协同安全能力，并逐步实现安全策略的可视化。

安全检测与持续监控

新一代SOC的
安全监测能力将

- 采用大数据平台架构
- 增加网络流量分析（NTA）
- DNS访问数据（pDNS）分析
- 采用用户与实体行为分析（UEBA）
- 增加终端检测和响应（EDR）
- 采用威胁情报平台（TIP）技术和产品
- 人机交互分析工具

快速响应

新一代SOC的快速响应能力建设包括：

- 采用事件响应平台（IRP），收到安全报警后可实现自动化编排响应行动，提供有价值的情报和事件上下文，并能对复杂的网络威胁作出自适应响应；
- 应能与各类SIEM、IT Help Desk系统集成，自动或手动触发响应工单，实现安全策略变更和控制，如关闭漏洞、关闭网络端口、升级系统配置、修改用户权限或者提升信息防护的强度等；
- 逐步做到与安全设备联动，自动化分发安全策略，实现自动响应。

溯源取证

新一代SOC将重点打造威胁追捕（Threat Hunting）的能力。

使用威胁追捕平台提高了高级威胁的检测能力、增加了寻找威胁的新方式、发现了他们之前没有发现过的威胁、减少了调查时间等。威胁追捕平台的特点是使用机器学习方法来进行自动决策，调查取证和自动分析。

威胁追捕类型	描述
假设驱动	这种类型的威胁溯源是先基于一个假设，比如假设攻击者是一个已知黑客团体的TTP，或者某个竞争对手
IOC驱动	根据攻击的数据和相关IOC，从已知攻击者IOC库中进行深入调查和分析
分析驱动	采用高级分析技术、机器学习、人工智能等技术来辅助识别

风险预警

新一代SOC的风险预警能力建设将包括：

主动风险评估、预测威胁

持续设定安全基线

持续漏洞跟踪，预测重大漏洞可能引起的攻击

通过威胁情报共享，及时发现同行业的攻击行为，关注黑客市场和新闻

1、ISOC的理念

2、ISOC能力建设

3、ISOC技术实现

4、ISOC建设难点

5、ISOC的市场分析

6、ISOC的主流厂商

ISOC的平台主要功能模块

ISOC整体架构示意图

1、ISOC的理念

2、ISOC能力建设

3、ISOC技术实现

4、ISOC建设难点

5、ISOC的市场分析

6、ISOC的主流厂商

ISOC建设难点

- 产品化与定制化（甲方与乙方）
- 大数据平台如何构建（安全与业务）
- 运营团队如何建设（自建与外包）
- 数据采集标准缺乏（乙方厂商）
- 情报共享机制缺乏（国家、行业、厂商）

主要内容

1、ISOC的理念

2、ISOC能力建设

3、ISOC技术实现

4、ISOC建设难点

5、ISOC的市场分析

6、ISOC的主流厂商

ISOC的市场分析

当前市场状况

2017年10亿左右

未来市场规模

2020年50-100亿

行业应用状况

金融、政府、运营商、能源

客户认知情况

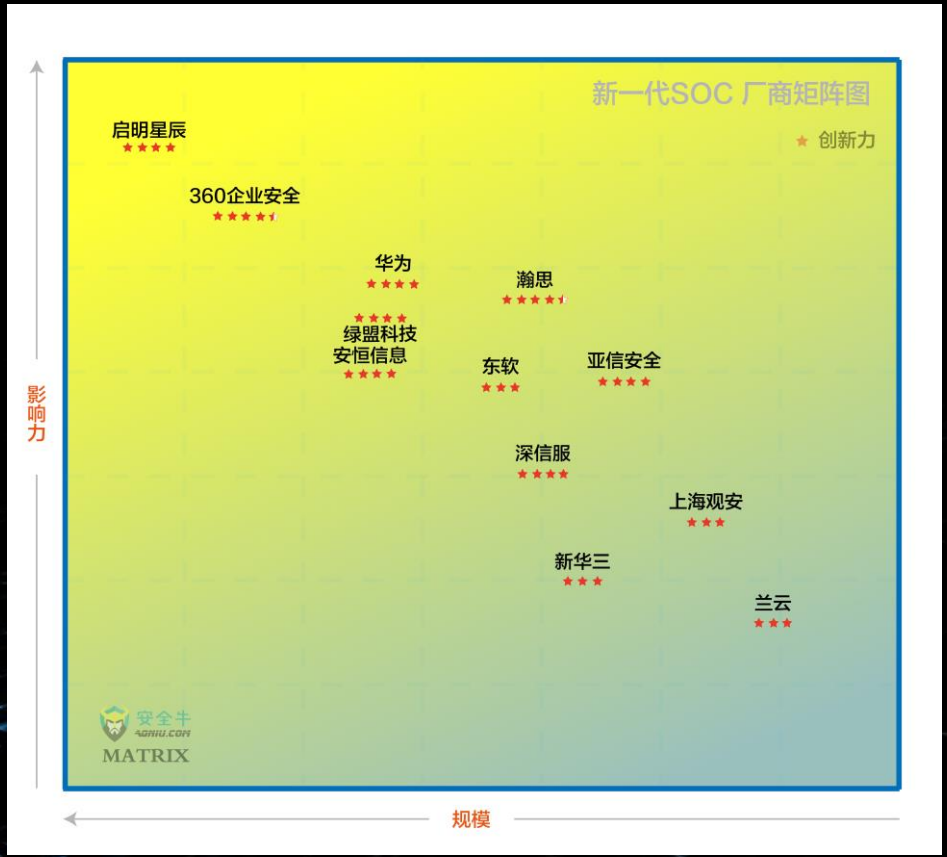
特定行业认可

技术成熟度

典型用户已取得验证

ISOC主流厂商

- 启明
- 360
- 安恒
- 东软
- 瀚思
- 华为
- 兰云
- 绿盟
- 观安
- 深信服
- 新华三
- 亚信



Thank you