天空卫士内部威胁防护
Skyguard Insider Threat Protection

天空卫士CTO 陈少涵

技高一筹 HIGH-TECH FOR TECH HIGH

以人工智能 护数据资产

ITP - Insider Threat Protection

什么是ITP？ - What

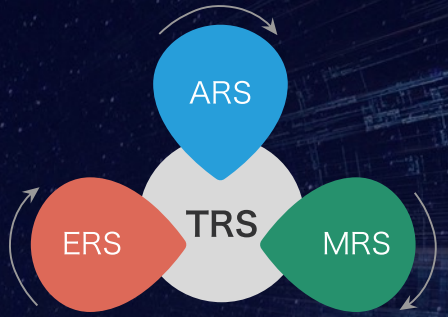
- 策略增强、具有深度内容感知能力的UEBA
  - 安全策略+行为双擎融合：UCS内容安全策略引擎+ITM行为分析引擎
  - 深度内容感知能力
  - 终端+网络多协议监控
- 基于深度学习和统计分析技术的行为分析
  - 智能地解读、关联、和预警风险行为
  - 捕捉异常行为
  - 回溯严重的违规事件，寻找具有相似行为的用户和终端
- 开放的架构支持多方合作
  - 标准的syslog日志接口
  - 基于REST API的Config接口

为什么要ITP？ - Why

- 误报率和检出率的矛盾（FP .vs. Coverage）
  - 更严格的安全策略能够降低误报率，但也会降低检出率
  - 需要更智能、更细粒度的策略来减低误报率并同时提高检出率
- 缺乏对安全事件的回溯和概括能力
  - 无法追溯有同类行为的用户或终端
  - 无法有效检测通过对内容加密或编码逃脱内容检测的行为
  - 需要智能的事件回溯机制
- 无法对已知风险模式进行概率匹配
  - 无法将专家知识共享给安全网关
  - 需要可持续更新的机制来分析已知风险模式，并同现有用户行为进行概率匹配

功能要点 - How

- **异常行为检测：**
  - 对每个用户或IP得到异常风险分值ARS（Anomaly Risk Score）
- **精准威胁行为模式预测：**
  - 对每个用户或IP得到模式相似分值MRS（Model Risk Score）
- **对已知的风险模式的检测：**
  - 对每个用户或者IP的行为根据已知的风险模式进行概率预测得到专家风险分值ERS（Expert Risk Score）



ITP：Next Steps

- 集成下一代防火墙、威胁情报、数据库安全等兄弟厂商
- 支持CASB和Gator Cloud的Cloud ITP
- 整合移动DLP
- 模拟人体获得性免疫（Adaptive Immunity）的自动防御体系

Thanks.