MITRE ATT&CK 实践入门

文章结构

- 围绕4个关键用例
  1. 网络威胁情报
  2. 检测与分析
  3. 对手模拟与红队
  4. 评估与工程
- 以3个层次讲述
  - 第一层：资源少的初始团队/新手
  - 第二层：走向成熟的中等安全团队
  - 第三层：拥有高级安全团队和更多资源的组织机构

1 网络威胁情报

- 第一层：
  1. 查询已映射ATT&CK的开源报告
  2. 查询每个威胁组织的TTP和检测、缓解措施
- 第二层：将自己的情报映射至ATT&CK，映射的具体步骤：
  1. 理解ATT&CK（结构、定义）
  2. 找出指标与行为
     - e.g. 原子指标：IP
     - e.g. 行为：建立Socks5通讯
  3. 研究行为
  4. 将行为转译为战术(Tactics)
  5. 确定行为里所应用的技术(Techniques)
  6. 对比其他分析师的结果
- 第三层：
  1. 从更多数据源处进行映射
     - 事件响应数据
     - OSINT情报源
     - 威胁情报订阅源
     - 实时告警信息
     - 组织历史信息
  2. 根据映射的ATT&CK信息来规划防御步骤

2 检测与分析

- 第一层：
  1. 了解组织内拥有的数据源。可以对照ATT&CK中的DataSource部分进行收集。重要的一些数据源包括：
     - 进程及命令行监控
     - 文件及注册表监控
     - 身份验证日志
     - 网络数据包捕获
  2. 收集数据并输入至SIEM
     - 测试数据集可参考：Splunk Botsv2
     - 测试环境搭建可参考：DetectionLab
  3. 观察他人创建的分析，应用到自己的数据上
     - 适合初学者的分析案例：CAR-2016-03-002
     - 从分析到检测的完整流程：
       1. 分析攻击技术
       2. 得出检测伪代码
       3. 编写SIEM查询语句
       4. 自动化
- 第二层
  1. 编写自己的分析来扩展覆盖面，包括两方面：
     - 理解攻击机制
     - 发现攻击在数据中的反应
  2. 具体实施
     - 进行模拟攻击　使用工具：Atomic Red Team
     - 收集攻击的日志数据　使用工具：DetectionLab
     - 寻找指标并编写搜索语句
  3. 迭代分析流程：
     1. 编写搜索语句检测恶意行为
     2. 修正搜索以减少误报
     3. 同时确保恶意行为的检出
- 第三层
  1. 进行真实的红蓝对抗
  2. 在对抗中完善对不同攻击技术的检测策略
  3. 追踪检测策略的覆盖情况
     - 使用工具：ATT&CK Navigator
     - 例如使用颜色标注：
       - 红色：未覆盖
       - 黄色：一定程度的覆盖
       - 绿色：高完成度的覆盖
- 相关资源
  - 网络分析库 (CAR):MITRE 的分析库
  - EQL: Endgame 的开源分析库
  - Sigma: 一种工具无关的分析格式，附带按此格式编写的分析库
  - 威胁猎手战术手册: 在日志数据中查找 ATT&CK 技术的策略库
  - 原子红队 (Atomic Red Team)
  - 检测实验室 (Detection Lab)
  - BOTS: Splunk的Boss of the SOC数据集，含背景噪音和红队攻击
  - BRAWL Public Game: MITRE 的红队数据集
  - ATT&CK Navigator: ATT&CK 矩阵数据可视化工具

3 对手仿真与红队

注：对手仿真(Adversary Emulation)与渗透测试等其他红队形式不同的是，前者在预先构造的场景下，使用特定的TTP、针对特征防御面进行攻击，模拟特定对手组织

- 第一层
  - 使用对手仿真工具模拟红队攻击
    - 原子红队
    - CALDERA
  - 执行原子测试的周期：
    1. 选择一个ATT&CK技术
    2. 选择一个针对该技术的测试
    3. 执行测试过程
    4. 分析检测过程
    5. 提高对抗能力
- 第二层
  - 阶段建议：当团队/组织具备红队功能时，将技术映射至ATT&CK
  - 重要案例：APT3对手模拟手册
  - 使用工具：Cobalt Strike / Empire已经映射到ATT&CK中
- 第三层
  - 阶段任务：与CTI团队合作，创建对手仿真任务
  - 对手仿真的五个步骤
    1. 收集威胁情报
       - 基于自身组织机构选择一个对手，与CTI团队合作分析该对手的TTP
    2. 抽取技术
       - 将红队操作映射至ATT&CK，便于红队进行攻击操作
    3. 分析与组织
       - 基于对手及其操作方式的大量情报，抽取出对手的操作流程图
    4. 开发工具和程序
       - 在知道红队做什么、怎么做之后，需要确定如何实现
    5. 模拟对手
       - 红队与蓝队开始紧密合作，仿真对手TTP进行
  - 相关资源
    - APT3对手模拟手册

4 评估与工程

- 第一层
  - 阶段建议：相比全面评估，更建议从小处入手。
  - 做法：选择一种技术，确定对此技术对覆盖率，进行适当工程强化后，开始检测此技术
- 第二层
  - 阶段建议：扩大技术的评估，使用ATT&CK覆盖热度图进行追踪
  - 做法：
    - 技术覆盖度可分为高中低置信度
    - 对检测工具进行迭代：
      - 工具在哪里运行：边界还是端点?
      - 工具检测的原理：静态指针还是行为检测?
      - 工具所监视的数据源：数据源类型可以推断所能检测的攻击技术
    - 提升覆盖率主要过程：
      - 创建短期内需重点关注的技术列表
      - 确保拉取正确数据以供分析
      - 开始构建分析并更新覆盖图
- 第三层
  - 阶段建议：纳入缓解措施以强化评估
  - 做法：参照ATT&CK缓解措施（Mitigation）进行引入、实现
- 相关资源
  - ATT&CK Logging Cheat Sheet（可用于检测的Windows事件日志清单）
  - ATT&CK数据地图（Datamap）项目
  - Dett&CT框架
  - MITRE ATT&CK脚本
  - 基于ATT&CK分析发现网络威胁
  - ATT&CK缓解措施（ATT&CK Mitigation）