BLUEHAT
SHANGHAI 2019

基于历史行为的异常检测

O365怎样反击内部恶意攻击

Lei He

Principal Engineering Manager, Microsoft Corporation

2019-05-30

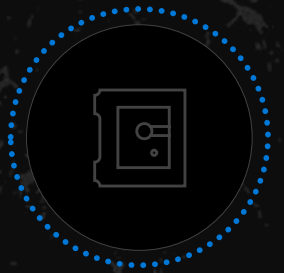
Office365安全要求

访问控制

- 无法使用Corp身份进行解密或访问，所有访问要求2FA
- 背景调查及安全培训
- 用户数据和运作中心隔离
- 零永久访问权限
- 客户密码箱和BYOK

安全监控

- 基于ETW的详细原始遥测技术，能够在<1天内测量新的遥测技术
- 集中处理会在15分钟内发出警报，以解决安全问题
- 每天至少1次攻击模拟服务以验证监视/响应
- 能够在<15分钟内触发安全响应工作流程，并在<1天内检测新工作流程



密钥管理

- 所有秘密必须存放在安全的容器中
- 秘密永远不应该离开边界
- 暴露时应立即滚动秘密
- 数据受托人应该在更新环境中完全控制秘密

反病毒修补

- 每天都扫描所有产品终点
- 所有中等和更严重评级的漏洞都应该打补丁或免除
- 所有网络应用程序应每月扫描一次
- 中央报告和跟踪

* 客户密码箱入门只能用于访问客户数据的企业服务.

概览

问题

- 信息泄露/心怀不满的恶意内部人员是重大的安全威胁
- 经过监督的ML检测训练以检测"已知"模式; 需要覆盖未知模式

解决方案

- 基于历史行为的检测标记异常活动
- 对于O365数据中心安全，用户== DevOps
- 可以推广到其他实体配置文件

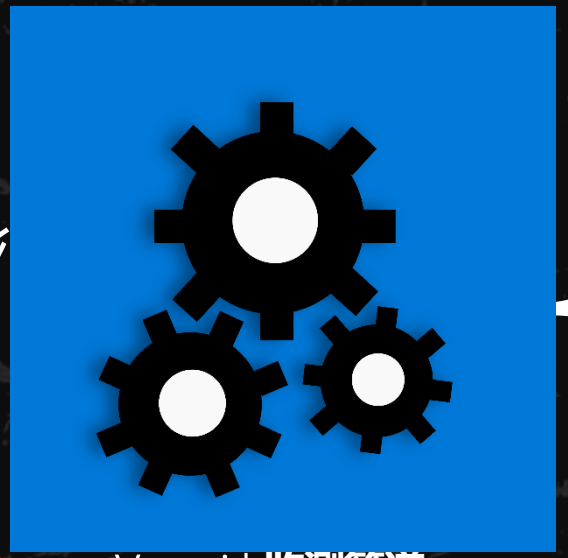
O365 数据中心监控

自动近实时多层检测和响应

在Kafka中流式传输数据源

- HostIDS ETW 事件
- Windows 事件日志
- Auth 日志
- 应用程序日志
- 服务器数据

O（1M）事件/秒



Vanquish**监测管道**

O（100K）**机器评估**

O（1k）**用户评估**

Spark**上的近实时（NRT）多层处理：**

<15分钟内的寻呼警报（包括基于ML的警报）

分析工具和仪表板

在收到警报时以近乎实时的方式交互式查看结果

警报和自动化

24 x 7，寻呼警报和自动响应。

模型特征选择

观察：DevOps活动展示模式

登录活动：

- 用户从哪里登录?
- 用户什么时候登录?
- 用户登录后做了什么?

及时提升：

- 用户请求了什么类型的权限提升?
- 谁批准了权限提升?

操作：

- 用户执行了哪个工作流程?
- 用户启动了哪些进程?
- 用户触发了哪些检测?

特征：

- 登录的机器
- 机器类型
- 容量单位范围
- 登录的IP
- 连接到的IP
- 其他检测触发
- 提升到何种权限
- 提升目的
- 批准者
- 特定的时间
- 流程和工作流程

模型

1. **产生每个用户的完整历史行为总结**
   a) 每个要素都是{ Value: Occurrence }的列表
2. **每隔2分钟，评估用户过去6个小时活动行为**
3. **将每个当前的活动行为与用户的历史活动行为进行比较**
   a) 针对会话中的值计算特征相似性得分。 **历史上发生的越高，越相似/正常**

$$Sim_i = MIN(Phis_0, Phis_1, Phis_j, \dots, Phis_k)$$

   b) 根据n个特征的相似性得分生成会话**异常分数**。

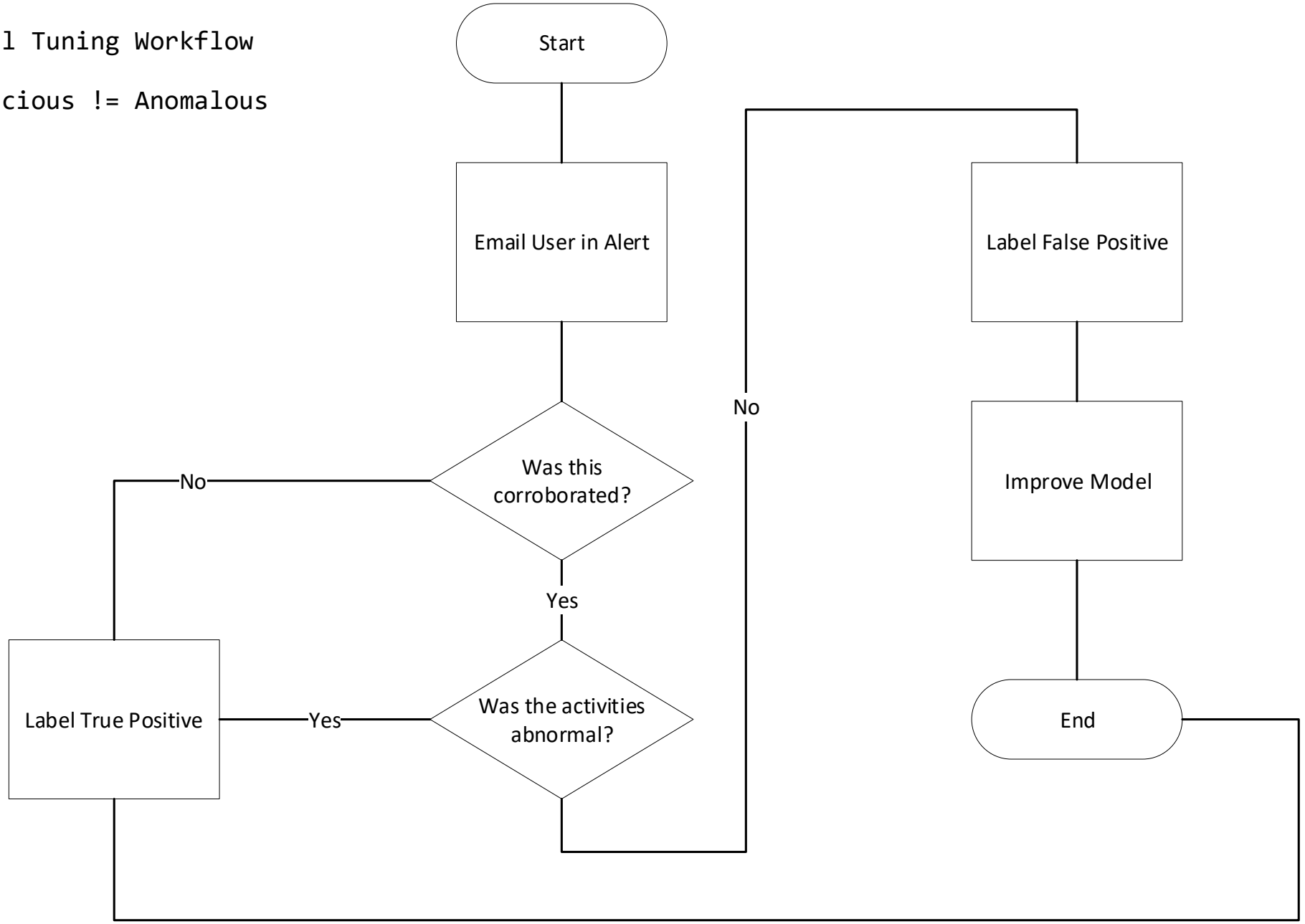
$$\text{Anomaly Score} = 1 - \text{AVG}(Sim_0, Sim_1, Sim_2, \dots, Sim_n)$$

4. **收集历史事件测试数据集以评估性能**
5. **根据警报次数容忍度来设置警报阈值（每周5次）**

模型调优

Model Tuning Workflow

Malicious != Anomalous



模型调优模式

新团队成员：

设置活动量的最低阈值

稀疏功能：

设置有效功能的最低阈值

双重计数：

删除自动生成的活动

换队伍：

使用团队资料

重命名命令：

不区分大小写的比较

高熵特点：

用{Capacity Unit, Capacity Type}替换目标计算机名称或IP

降低用户源IP的权重

降级自由文本功能（比如，提升权限）

模型性能

成功指标：警报次数

- 自2018年末发布以来，每周平均提供约5次警报

成功指标：精确度

- ~90%真阳性（上个月16/18）

真实积极的类型

- 渗透测试
- 一次性事件（“破碎玻璃”）或审计
- 操作流程违规
- DevOps 不良行为
- DevOps一次性测试或试验

行动起来

应用基于历史行为的异常检测深度防御！

- 从高质量数据开始
- 找到真实的恶意事件
- 做在线实施前首先执行离线分析
- 通过反馈循环持续调整
- 可解释的模型
- 警报有足够的补充信息

答疑

BLUEHAT
SHANGHAI 2019

基于历史行为的异常检测

Lei He

leih@Microsoft.com

www.linkedin.com/in/lei-he-security