# Change Auditor Threat Detection

针对Microsoft环境的前瞻性用户威胁检测

绝大部分企业主要通过Active Directory (AD)进行身份验证和授权，这也使其成为黑客、网络恐怖分子和心怀不满员工的主要攻击目标。但是各个企业可能尚未意识到对其AD系统造成更为直接威胁的因素其实是内部人员在工作中有意或无意的行为。更为糟糕的是，AD结构复杂，很难在威胁出现时对其进行确认。基于规则的传统用户威胁检测方法会生成很多警报，因此您无法对它们进行全面调查；您会面临忽略真正威胁的风险，使您的企业面临数据安全违规的风险。您如何实时分析您的环境中发生的所有用户活动，以避免您的企业出现中断情况?

Change Auditor Threat Detection通过对用户个人行为模式建模来提供独特的用户威胁检测方法，从而检测可能表示可疑用户或受攻击帐户的异常活动。Change Auditor Threat Detection借助专用高级学习技术、用户和实体行为分析(UEBA)和成熟的评分算法来分析用户活动，从而确定贵企业中风险非常高的用户，发现潜在的用户威胁并减少误报造成的干扰。您最终可以弥补本地审核工具留下的缺口，确保环境安全。

## 特性

### 实时审核日志分析

实时高效地分析大量审核数据，包括AD变更、身份验证和文件活动。在这些原始活动事件的基础上构建用户基准并前瞻性地检测用户何时存在异常行为，以便您可以立即发现潜在可疑的活动。


*Change Auditor Threat Detection可帮助您快速轻松地检测可疑用户活动，为您的环境和用户提供持续保护。*

## 优势：

- 基于用户行为模式前瞻性地检测威胁
- 减少基于规则的威胁检测产生的海量警报
- 结合上下文查看安全警报，以快速轻松地确定其严重性
- 根据用户行为基准轻松检测到出现异常行为的用户
- 根据您的现有审核数据发现威胁，以降低对您的基础架构的影响

## 使用情形：

Change Auditor Threat Detection可让您快速轻松发现威胁，包括：

- 异常AD活动
- 滥用特权帐户
- 暴力破解攻击
- 数据渗漏
- 不当访问系统或资源
- 恶意软件
- 权限提升
- 横向移动

## 系统要求

### CHANGE AUDITOR协调程序

（服务器端组件）

**处理器**：等效于四核英特尔酷睿i7或更高配置的处理器

**内存**：最低：8 GB RAM或更高配置；建议：32 GB RAM或更高配置

### CHANGE AUDITOR客户端

（客户端组件）

**处理器**：等效于双核英特尔酷睿i5或更高配置的处理器

**内存**：最低：4 GB RAM或更高配置；建议：8 GB RAM或更高配置

### CHANGE AUDITOR代理

（服务器端组件）

**处理器**：等效于双核英特尔酷睿i5或更高配置的处理器

**内存**：最低：4 GB RAM或更高配置；建议：8 GB RAM或更高配置

如需查看系统要求的最新详细列表，请访问support.quest.com/change-auditor

### 自动化的用户行为分析(UEBA)

无需任何管理员输入或配置即可为用户活动模式建模。用户行为基准是通过无人监管的高级机器学习技术自动创建的，能够为各个方面的用户活动（包括其登录模式、管理活动以及文件和文件夹访问）建模。

### 成熟的异常行为检测

通过自动将每个用户操作与相关用户的行为基准进行比较来发现异常用户活动。成熟的威胁指标检测和多级别风险评分确保只会突出显示非常严重的异常情况，这表示风险性非常高的用户行为。

### 基于模式的用户威胁检测

只有在检测到异常用户行为的关联模式时，才会发出SMART用户威胁警报。不依靠规则来检测特定活动，而是通过成熟的用户行为模式检测自动分析发生的所有用户活动并发现环境中非常可疑的用户。成熟的全局建模技术可确保仅突出显示非常关键和相关的用户行为模式，显著减少孤立活动和误报带来的干扰。

### 高保真用户分析

Change Auditor创建审核日志以作分析之用，因此用于前瞻性检测您环境中威胁的所有原始事件数据从一开始就包括以下宝贵信息：

- 更改执行者
- 更改内容
- 更改时间
- 更改位置
- 发起更改的位置的IP地址或工作站

与本机Windows事件日志不同，Change Auditor可确保不会错过任何重要的用户操作，避免在用户行为分析中产生严重的缺口。

### 结合上下文的安全警报

查看作为警报一部分发现的威胁指标上下文中的所有可疑用户活动警报。每种行为异常都会在用户的基准活动上下文中显示，且随附触发该警报的所有原始事件，既可以清晰表明发出警报的原因，又可以简化调查和后续跟进过程。

### 轻量级用户威胁检测

利用您的现有Change Auditor基础架构和审核数据为用户行为建模，这样就不用额外部署不必要且复杂的代理和服务器。单个虚拟设备是启用高级用户威胁分析所需的唯一附加基础架构。

## 关于QUEST

Quest的宗旨是通过简单的解决方案解决复杂的问题。为实现此宗旨，我们秉持注重卓越产品和优质服务的理念，并且追求易于合作这一总体目标。我们的愿景是提供技术来避免在效率与有效性之间做出取舍，从而使您和您的企业可以减少用于IT管理的时间，并将更多时间用于业务创新。

Quest
www.quest.com/cn
如果您不在北美洲，可以在我们的网站上找到本地办公室信息。



DataSheet-ChangeAuditorThreatDetection-US-KS-zh_CN-WL-32855