Change Auditor for Logon Activity

针对AD登录和注销以及Azure AD登录活动发出相应警报并进行报告

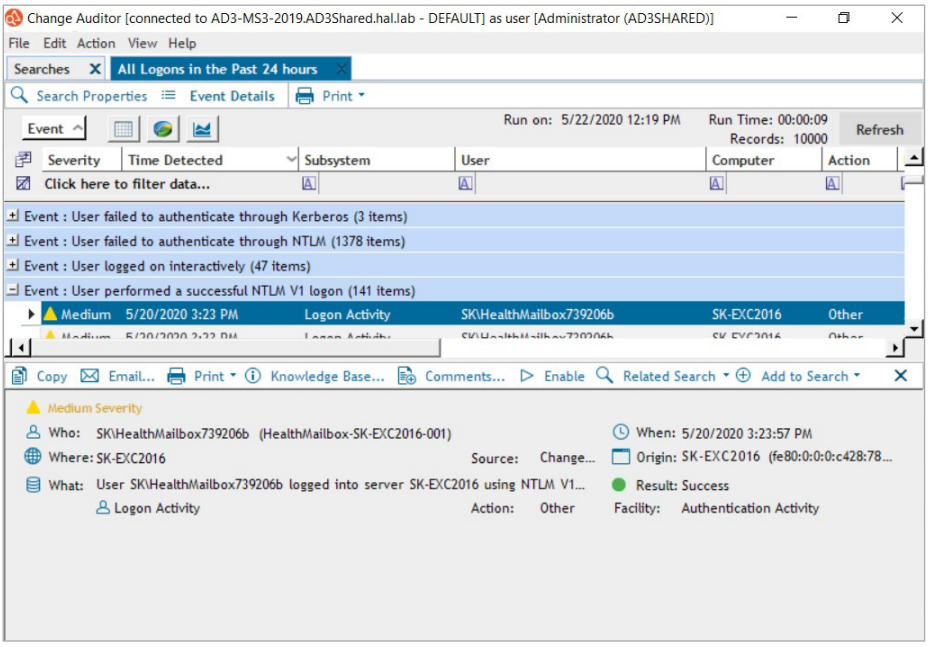
如今，不断增加的合规性法规和安全问题使得自动化、可靠且全面地跟踪用户登录和注销活动变得不可或缺。但是，无论是在本地还是云中，大多数第三方工具的实施过程都非常繁琐，而且无法提供所需的审核级别来确保对用户操作的充分问责。同时，原生工具在可见性、警报、审计和数据安全方面也有严重的缺陷。

借助Change Auditor for Logon Activity，您可以通过捕获所有AD登录/注销和Azure AD登录活动并提供相应警报和报告，来提高企业的安全性与合规性并优化审核。跟踪Kerberos、NTLM和ADFS身份验证，以帮助前瞻性地发现漏洞。

功能

NTLM身份验证审核 — 检测仍在使用安全性较低的NTLM身份验证的应用程序。

黄金票据检测 — 检测在黄金票据/票据传递攻击期间使用的常见Kerberos身份验证漏洞，并发出相应警报。



通过详细的会话信息跟踪混合登录/注销和登录活动。对数据进行分组、排序和筛选，找出谁在远程登录以及从哪里登录。

> “当出现问题时，经理总是要求IT立即报告所更改的内容。原生工具无法使我们快速应对这些请求，尤其是在我们的IT员工非常有限的情况下。但是，借助Change Auditor，我们可以立即开始创建报告。这对我们来说真得至关重要。”
>
> *John Eckard，霍华德县服务器团队经理*

优势：

- 捕获AD登录/注销以及Azure AD登录活动、发出相应警报并进行报告
- 跟踪Kerberos和NTLM身份验证，以帮助发现漏洞
- 提供对会话、登录/注销和登录活动（包括开始和结束时间）的企业级可见性，以及关于变更事件的所有关键信息（人员、事件、时间、地点和来源/工作站）
- 自动收集多个不同且加密的登录事件
- 为安全和审核目的提供简单、整合的报告
- 向电子邮件地址和移动设备发送实时警报，让您即使不在现场也能收到相应提醒，以便立即采取措施
- 能够在登录失败时发出警报，从而降低安全风险
- 与SIEM解决方案相集成，将Change Auditor事件转发到Splunk、ArcSight或QRadar

完整的用户活动审核 — 审核管理员活动的整个时间表，从登录到注销以及其间执行的所有操作都包括在内（与其他Change Auditor模块结合使用时）。

混合安全意识 — 报告AD用户登录和注销，并与Azure AD登录相关联以帮助发现混合云环境中的可疑活动。捕获的信息包括登录类型、IP地址和地理位置、获得身份验证的应用程序以及登录尝试是否成功。

规范化5W审核详细信息 — 将加密的本机日志转换为简单的规范化格式，突出显示人物、事件、时间、地点、工作站详细信息以及事件前后的值。

相关搜索 — 只需单击一下，便可立即访问关于您所查看事件的所有信息以及所有相关活动，避免无谓的猜测和未知安全隐患。

安全威胁时间表 — 支持查看、突出显示和筛选随时间推移顺次发生的登录活动及相关更改事件，以便更好地对这些事件和趋势进行取证分析。

随时随地获得实时警报 — 通过电子邮件和移动设备发送有关成功和失败登录的关键警报，以确保即使您在异地也可以快速对安全威胁做出响应。

合规性就绪报告 — 简化登录活动收集，以符合主要外部法规和内部安全政策。

集成的事件转发 — 轻松与SIEM解决方案相集成，将Change Auditor事件转发到Splunk、ArcSight、QRadar或任何支持Syslog的平台。此外，Change Auditor与Quest® InTrust®相集成，实现20:1的压缩事件存储，集中化的原生或第三方日志收集、解析和分析，以及针对可疑事件的警报和自动响应操作。

托管控制板 — 在On Demand Audit（具有灵活搜索和数据可视化功能的SaaS控制板）中查看所有AD登录/注销、Azure AD登录以及Office 365活动。

系统要求

有关完整的系统要求，请参考support.quest.com/technical-documents/change-auditor中的安装指南。

关于QUEST

Quest提供软件解决方案，在越来越复杂的IT环境中带来新技术的优势。从数据库和系统管理到Active Directory和Office 365管理，以及网络抗风险能力，Quest都可帮助客户在当下解决其面临的下一个IT挑战。Quest Software。未来与现在的碰撞。

Quest
quest.com/cn
有关当地办事处信息，请访问 (quest.com/cn-zh/locations)

DataSheet-ChangeAuditorLogonActivity-US-LR-zh_CN-WL-64108