

Change Auditor for Logon Activity

Alert and report on AD logon and logoffs and Azure AD sign-in activity

Increasing compliance regulations and security concerns make automated, reliable and complete tracking of user logon and logoff activity essential today. But most third-party tools are cumbersome to implement and don't provide the level of auditing required to ensure adequate accountability of user actions, whether on premises or in the cloud. Meanwhile, native tools also have serious drawbacks when it comes to visibility, alerting, auditing and data security.

With Change Auditor for Logon Activity, you can promote better security, auditing and compliance in your organization by

capturing, alerting and reporting on all AD logon/logoff and Azure AD sign-in activity. Track Kerberos, NTLM and ADFS authentications to help proactively identify vulnerabilities.

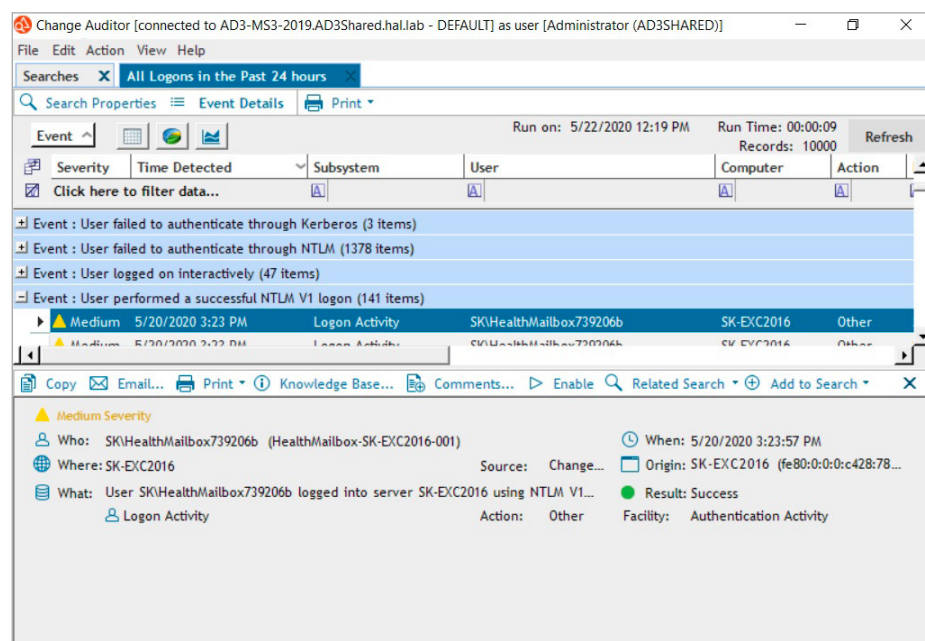
FEATURES

NTLM authentication auditing — Detect applications that are still using less secure NTLM authentications.

Golden Ticket detection — Detect and alert on common Kerberos authentication vulnerabilities used during Golden Ticket / Pass-the-ticket attacks.

“When something goes wrong, managers always ask IT for a report on what changed, and they need it now. Native tools didn't enable us to respond to those requests quickly, especially since we are a limited IT staff. But with Change Auditor, we can start pulling up reports right away. That's really critical for us.”

John Eckard, Server Team Manager, Howard County



Change Auditor [connected to AD3-MS3-2019.AD3Shared.hal.lab - DEFAULT] as user [Administrator (AD3SHARED)]

File Edit Action View Help

Searches X All Logons in the Past 24 hours

Search Properties Event Details Print

Event Severity Time Detected Subsystem User Computer Action

Click here to filter data...

Run on: 5/22/2020 12:19 PM Run Time: 00:00:09 Records: 10000 Refresh

Event : User failed to authenticate through Kerberos (3 items)

Event : User failed to authenticate through NTLM (1378 items)

Event : User logged on interactively (47 items)

Event : User performed a successful NTLM V1 logon (141 items)

Medium 5/20/2020 3:23 PM Logon Activity SK\HealthMailbox739206b SK-EXC2016 Other

Copy Email... Print Knowledge Base... Comments... Enable Related Search Add to Search

Medium Severity

Who: SK\HealthMailbox739206b (Health/Mailbox-SK-EXC2016-001)

Where: SK-EXC2016

What: User SK\HealthMailbox739206b logged into server SK-EXC2016 using NTLM V1... Logon Activity

Source: Change...

Action: Other

When: 5/20/2020 3:23:57 PM

Origin: SK-EXC2016 (fe80:0:0:0:c428:78...

Result: Success

Facility: Authentication Activity

Track hybrid logon/logoff and sign-in activity with detailed session information. Group, sort and filter the data to find out who's logging in remotely and from where.

BENEFITS:

- Captures, alerts and reports on all AD logon/logoff and Azure AD sign-in activity
- Tracks both Kerberos and NTLM authentications to help identify vulnerabilities
- Provides enterprise-wide visibility into sessions and logon/logoff and sign-in activity (including the start and end time), as well as all critical information about change events (who, what, when, where, and origin/workstation)
- Automates the collection of multiple disparate and cryptic logon events
- Provides simple, consolidated reports for security and auditing purposes
- Send real-time alerts to email and mobile devices to prompt immediate action, even while you're not on site
- Reduces security risks with the ability to alert on failed logons
- Integrates with SIEM solutions to forward Change Auditor events to Splunk, ArcSight or QRadar

SYSTEM REQUIREMENTS

For complete system requirements, please refer to the Installation Guide, available at support.quest.com/technical-documents/change-auditor.

Complete user activity auditing —

Audit the entire timeline of an administrator's activity, from logon to logoff and all actions they take in between (when combined with other Change Auditor modules).

Hybrid security awareness — Report on AD user logons and logoffs, and correlate with Azure AD sign-ins to help identify suspicious activity across your hybrid cloud environment. Information captured includes the type of logon, the IP address and geographical origin, the application being authenticated to, and whether the attempt was successful.

Normalized 5W audit details — Translate cryptic native logs into a simple, normalized format highlighting the who, what, when, where and workstation details and before and after values.

Related searches — Provides instant, one-click access to all information on the event you're viewing and all related activity, eliminating guesswork and unknown security concerns.

Security threat timelines — Enables viewing, highlighting and filtering of logon activity and related change events over time for better forensic analysis of events and trends.

Real-time alerts on the move — Sends critical alerts on both successful and failed logons via email and mobile devices to enable fast response to security threats, even while you're off site.

Compliance-ready reporting —

Simplifies collection of logon activity for major external regulations and internal security policies.

Integrated event forwarding — Easily integrates with SIEM solutions to forward Change Auditor events to Splunk, ArcSight, QRadar or any platform supporting Syslog. Additionally, Change Auditor integrates with Quest® InTrust® for 20:1 compressed event storage and centralized native or third-party log collection, parsing and analysis with alerting and automated response actions to suspicious events.

Hosted dashboard— View all AD user logons/logoffs, Azure AD sign-ins and Office 365 activity together in On Demand Audit, a SaaS dashboard with flexible search and data visualization.

ABOUT QUEST

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.