LOS 10 EVENTOS DE SEGURIDAD MÁS IMPORTANTES QUE SUPERVISAR EN AZURE AD Y OFFICE 365

Identifique las deficiencias de las herramientas de auditoría nativas y supérelas.

Quest

Realmente ¿es su organización más segura ahora que utiliza aplicaciones en la nube?

Más eficaz, probablemente. Pero ¿más segura?

Los usuarios aún pueden llevar a cabo acciones de alto riesgo en la nube, y las credenciales de la cuenta todavía pueden verse comprometidas. Microsoft ha advertido a los administradores durante años de que decenas de millones de cuentas de AD son el blanco de ataques cibernéticos cada día.[1] Además, el 34 % de las infracciones de datos involucran a alguien que ya está dentro de la red.[2]

Lamentablemente, las herramientas nativas de auditoría de Office 365 y Azure AD dejan mucho que desear en lo que respecta a la auditoría de cambios en roles, grupos, aplicaciones, uso compartido y buzones de correo. Sus capacidades de búsqueda son limitadas y retienen los eventos de auditoría en los registros solo por un tiempo limitado.

Office 365 y Azure AD ofrecen capacidades de búsqueda limitadas y retienen los eventos de auditoría solo por un tiempo limitado.

Este libro electrónico destaca diez eventos de seguridad que los administradores siguen de cerca para mantener seguros sus entornos Azure AD y Office 365. Analice la información de auditoría que estos pueden encontrar utilizando herramientas y consolas nativas, e identifique los escollos con los que es más probable que se topen al extraer los informes de auditoría de forma nativa. Finalmente, ofrece una visión sobre una solución que puede ayudarles a superar algunas de estas limitaciones de la auditoría nativa.

1 Fontana, John, "Active Directory czar rallies industry for better security, identity", ZDNet, junio de 2015, https://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/.

2 "2019 Data Breach Investigations Report", Verizon, mayo de 2019, https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/.

Figura 1: Registro de auditoría unificado (para la búsqueda de registros de auditoría de Office 365)

¿Cómo funciona la auditoría en Azure y Office 365?

La gestión y seguridad de un entorno de nube comienza con la posibilidad de seguir los eventos de inicio y cierre de sesión de un usuario.

Para obtener esta información sobre las instalaciones, los administradores de sistemas que intentan hacer un seguimiento de los usuarios deben examinar varios registros en cada controlador de dominio de Windows y correlacionar los eventos de auditoría entre los registros de varios servidores.

En la nube, los administradores deben correlacionar de una manera similar a través de dos registros en Azure AD: el registro de auditoría, que contiene todos los eventos de cambio, y el registro de inicio de sesión, que contiene todos los eventos de autenticación (véase la figura 1). Pueden acceder a los registros a través del Azure Portal o de PowerShell.

En cuanto a Office 365, cada aplicación (Exchange Online, SharePoint Online, OneDrive para la Empresa, etc.) escribe en lo que se convertirá en el registro de auditoría unificada de Office 365, que contiene todos los eventos de administrador y usuario. El registro de auditoría unificado también incluye eventos del registro de auditoría de Azure y del registro de inicio de sesión.

Los administradores saben qué tipo de datos se almacenan en los registros. Pero extraer esos datos y utilizarlos para gestionar y proteger su entorno es otra cuestión.

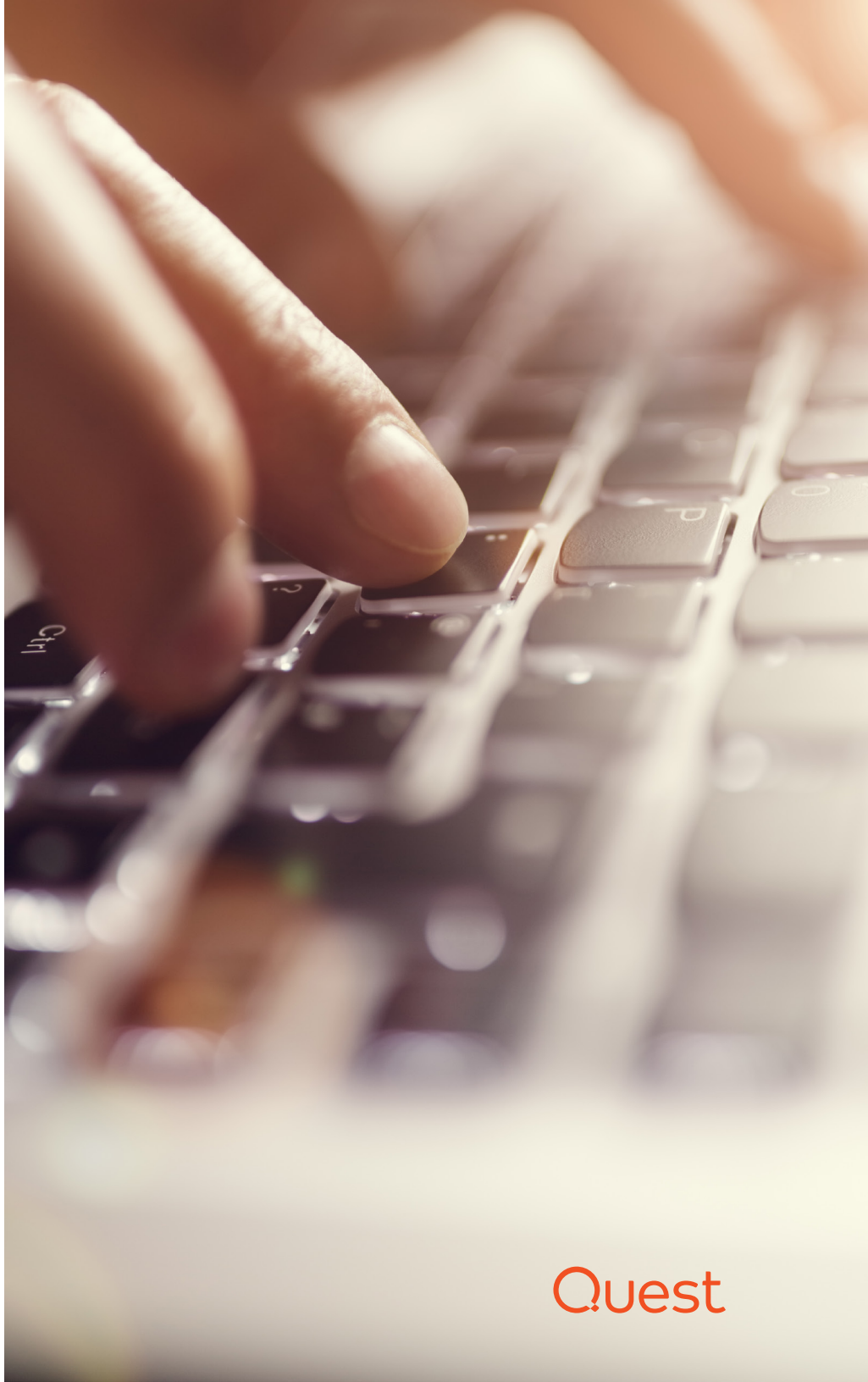
Quest

Los administradores saben dónde están los registros y qué tipo de datos se almacenan en ellos. Pero extraer esos datos y utilizarlos para gestionar y proteger su entorno es otra cuestión.

LOS BRECHAS DE AUDITORÍA DE LAS HERRAMIENTAS NATIVAS

Auditar en Azure y Office 365 tiene varias limitaciones.

- Para las organizaciones con entornos híbridos, no es posible buscar la actividad de auditoría en las cargas de trabajo locales y en la nube de un solo vistazo.
- Del mismo modo, las políticas de auditoría para las cargas de trabajo locales deben configurarse aparte de las de las cargas de trabajo en la nube. Además, no hay forma de supervisar las políticas de auditoría si cambian o las deshabilitan otros administradores.
- Puede haber una demora de 24 horas o más en el procesamiento de algunas de las entradas de los registros de auditoría y en su adición al registro de auditoría unificado.
- Los registros en Azure se conservan durante intervalos de tiempo que varían, según la carga de trabajo y el tipo de suscripción. Esto puede ser un factor restrictivo cuando el departamento de TI investiga los incidentes. También puede ser demasiado incierto para algunos requisitos reglamentarios.
- Los eventos se formatean de forma diferente dependiendo del tipo de evento y de si se produjo de forma local o en la nube. Sin un formato normalizado, los registros visibles a través de consolas nativas son difíciles de interpretar.
- Es posible acceder a los eventos de auditoría de Azure y Office 365 a través de PowerShell. Además, tanto Azure como Office 365 ofrecen un portal web para acceder a los eventos de auditoría. Sin embargo, el portal muestra solo 15 eventos a la vez, y la demora en el procesamiento se traduce en que no todos los eventos de auditoría relevantes están necesariamente presentes a la vez.



1. Cambios a roles importantes

En la infraestructura local, se consideran importantes varios grupos dentro de AD, como administradores de dominio, operadores de cuenta y administradores de servidor, debido a los derechos avanzados que otorgan. En la nube, eso también se aplica a los roles en el inquilino de Azure.

El problema es que, con el tiempo, usuarios como los administradores, los operadores, los gerentes y los técnicos del servicio de asistencia técnica adquieren gradualmente muchos más derechos de los que deberían tener. Por lo tanto, una gestión cuidadosa incluye la capacidad de informar y alertar sobre los cambios que tienen lugar en esos grupos y roles.

El problema es que, con el tiempo, usuarios como los administradores, los operadores, los gerentes y los técnicos del servicio de asistencia técnica adquieren gradualmente muchos más derechos de los que deberían tener.

ENCONTRAR ROLES EN EL REGISTRO DE AUDITORÍA DE AZURE

En la nube, el primer paso es identificar roles importantes en el portal de Azure. En la sección **Registros de auditoría**, bajo Azure Active Directory, una búsqueda en el servicio **Core Directory** y en la categoría **RoleManagement** devuelve todos los cambios a los roles del inquilino, como se muestra en la figura 2. Lamentablemente, esto no permite la búsqueda directa solo de los roles que se consideran importantes. Los administradores deben examinar cada evento de auditoría por separado para saber qué rol se modificó.

Quest

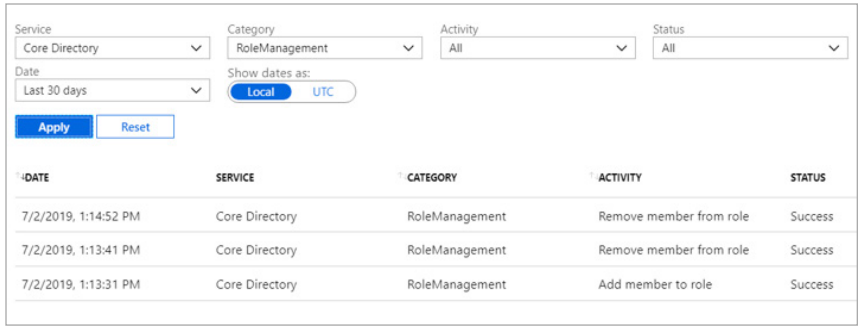


Figura 2: Búsqueda de roles en el portal de Azure

Otra opción es exportar y analizar los resultados como una hoja de cálculo de Microsoft Excel. Esto requiere una suscripción no solo a Office 365 sino también a Azure.

ENCONTRAR ROLES EN EL REGISTRO DE AUDITORÍA UNIFICADO

La información también se puede recopilar a partir de una búsqueda en el registro de auditoría unificado a través del Centro de seguridad y cumplimiento de Office 365. (Estas búsquedas se comparan con los registros de Azure AD, además de los registros de todas las herramientas de Office 365, como se ha descrito anteriormente. Pueden llevar más tiempo que las búsquedas en el registro de auditoría de Azure solo).

Las búsquedas devuelven todas las actividades individuales relacionadas con la administración de roles en un intervalo de fechas determinado (véase la figura 3), lo que es una ventaja sobre la búsqueda en el registro de auditoría de Azure.

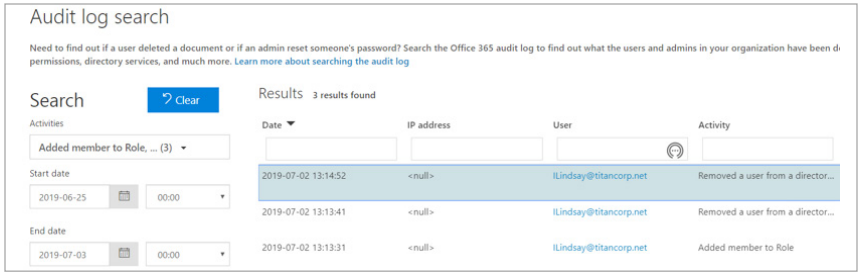


Figura 3: Búsqueda de registro de auditoría unificado

Aquí, sin embargo, todo el detalle de la auditoría se encuentra en un formato de texto JSON integrado, por lo que identificar el rol modificado significa examinar todos los detalles. Es posible exportar los datos a una herramienta como Excel, pero como se muestra en la columna AuditData en la figura 4, el formato JSON dificulta el filtrado de los roles modificados.

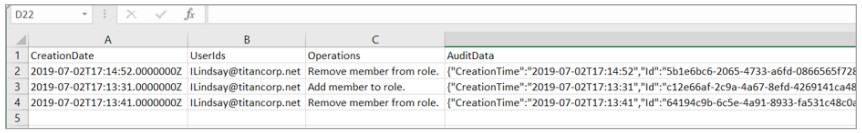


Figura 4: Resultados de búsqueda vistos en Microsoft Excel

Quest

2. Cambios a grupos

Los grupos de AD han sido durante mucho tiempo la clave para garantizar el acceso a los recursos. En la nube, eso sigue siendo cierto con algunas complicaciones.

- Azure permite más tipos de grupos. Por ejemplo, los usuarios pueden crear grupos a través de aplicaciones como Outlook y Teams.
- Los grupos de Office 365, como los creados a través de Teams, generan otros recursos de Azure para respaldar la aplicación.[3]
- Azure AD B2B facilita la creación de grupos para la colaboración con clientes y proveedores. Pero conlleva el riesgo de que un usuario conceda un acceso no intencionado a un tercero.

Azure AD B2B facilita la creación de grupos para la colaboración con clientes y proveedores. Pero conlleva el riesgo de que un usuario conceda un acceso no intencionado a un tercero.

3 Para obtener más información, consulte el libro electrónico "Frequently Asked Questions: Office 365 Groups", https://www.quest.com/whitepaper/frequently-asked-questions-office-365-groups81344485/.

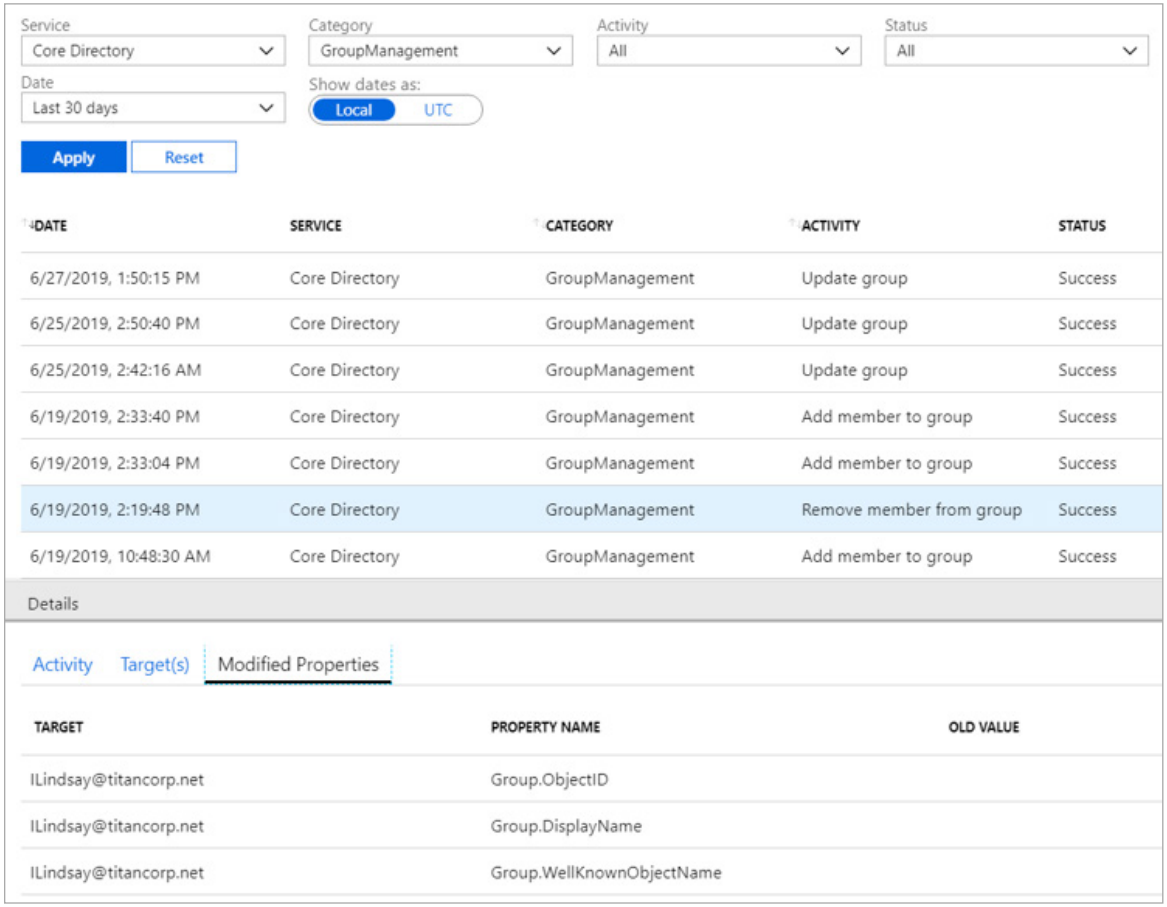


Figura 4: Búsqueda de roles en el portal de Azure

ENCONTRAR GRUPOS EN EL REGISTRO DE AUDITORÍA DE AZURE

Al igual que con los cambios de roles, el portal de Azure es el primer paso lógico para mantener un seguimiento de los grupos. En la sección **Registros de auditoría**, bajo Azure Active Directory, una búsqueda en el servicio **Core Directory** y en la categoría **GroupManagement** devuelve todos los cambios a los grupos del inquilino (parte superior de la figura 4). Nuevamente, sin embargo, esto no permite la búsqueda directa solo de los grupos que se consideran importantes. Además, el grupo modificado no se muestra inicialmente, por lo que los administradores deben examinar los detalles del evento de auditoría en la pestaña Propiedades modificadas (parte inferior de la figura 4) para encontrar el grupo modificado.

Otra opción es exportar y analizar los resultados como una hoja de cálculo de Microsoft Excel, que requiere suscripciones no solo a Office 365 sino también a Azure.

Quest

ENCONTRAR GRUPOS EN EL REGISTRO DE AUDITORÍA UNIFICADO

Al igual que con los cambios de roles, la información sobre los cambios de grupo también se puede recopilar en el Centro de seguridad y cumplimiento de Office 365 (véase la figura 2) de una búsqueda de registros de auditoría en todas las **actividades de administración de grupos de Azure AD**. Una búsqueda en **Se ha agregado un miembro al grupo** y **Se ha quitado un miembro del grupo** (véase la figura 5) muestra los cambios en la suscripción.

Pero ese procedimiento todavía no permite búsquedas directas solo en los grupos deseados; es necesario buscar cambios en todos los grupos y, luego, examinar los datos. Y, de nuevo, todo el detalle de la auditoría está en un formato JSON integrado, por lo que identificar el grupo modificado significa tener que examinar todos los detalles. Es posible exportar los datos a una herramienta como Excel, pero el formato JSON dificulta el filtrado de los grupos modificados.

Figura 5: Propiedades modificadas en el registro de auditoría unificado

Quest

3. Cambios a aplicaciones

Azure AD permite la configuración simplificada de muchas aplicaciones SaaS y el acceso a aplicaciones locales.

Aunque las aplicaciones SaaS no son difíciles de configurar, pueden romperse fácilmente si los cambios no se realizan de manera adecuada. Además, los cambios sin documentar se traducen en pérdida de tiempo, productividad y ganancias a medida que se resuelven los problemas. Por lo tanto, poder realizar un seguimiento de los cambios en las aplicaciones es un imperativo empresarial.

Poder realizar un seguimiento de los cambios en las aplicaciones es un imperativo empresarial.

ENCONTRAR CAMBIOS DE APLICACIÓN EN EL REGISTRO DE AUDITORÍA DE AZURE

En el portal Azure, el primer paso para encontrar cambios en una aplicación individual es en Azure Active Directory en la sección **Registros de auditoría** para la aplicación individual. El problema es que se requiere mucho análisis manual y repetitivo para encontrar cambios.

Quest

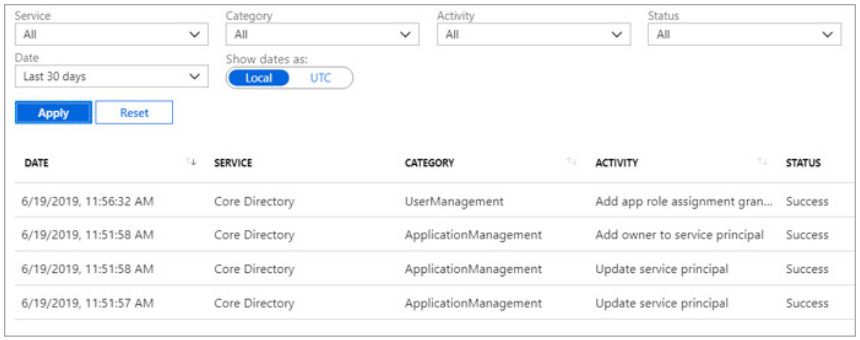


Figura 6: Cambios en la aplicación listados en el registro de auditoría de Azure

Como se muestra en la columna Categoría de la figura 6, los eventos de auditoría provienen de **ApplicationManagement** y **UserManagement**.

Al profundizar en la categoría **ApplicationManagement**, se obtiene la lista que se muestra en la figura 7.

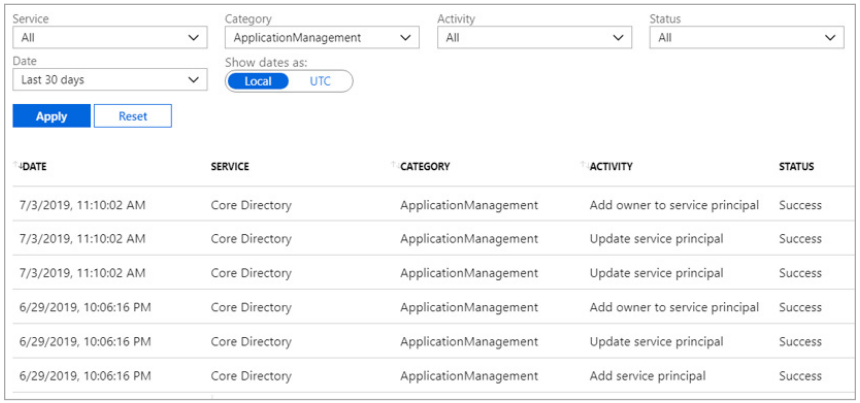


Figura 7: Buscar en la categoría ApplicationManagement

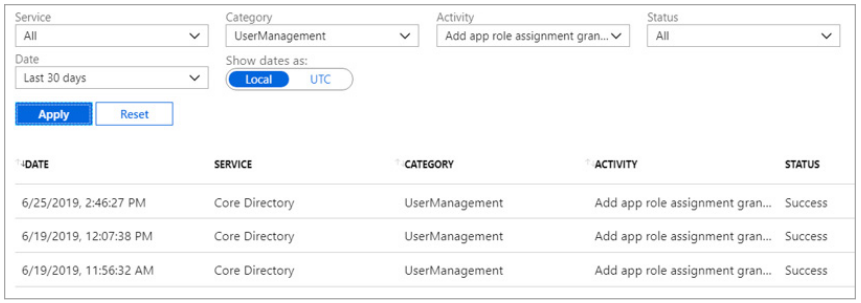


Figura 8: Buscar en la categoría UserManagement

Para profundizar en los cambios de la aplicación relacionados con **UserManagement**, es necesario cambiar a esa categoría y, a continuación, seleccionar cinco actividades diferentes del menú desplegable **Actividad**:

- Añadir la concesión de asignación de roles de la aplicación al usuario (véase la figura 8)
- Crear contraseña de la aplicación para el usuario
- Eliminar contraseña de la aplicación para el usuario
- Eliminar la asignación de roles de la aplicación del usuario
- Revisar la asignación de aplicaciones

Por lo tanto, no hay una manera fácil de buscar todos los cambios en la aplicación o generar una lista que contenga los cambios deseados.

4. Creación de recursos

Casi cada migración a la nube se traduce en la creación de recursos, algunos de los cuales (como un sitio de Microsoft Teams) crean su propio conjunto de recursos, tales como grupos de Office 365 y recursos de SharePoint. Ser capaz de hacer un seguimiento del tipo y el número de recursos creados ayudará a los administradores a reducir la costosa y lenta carga de administrarlos.

ENCONTRAR RECURSOS CREADOS EN EL REGISTRO DE AUDITORÍA DE AZURE

Tenga en cuenta los recursos asociados con la creación de usuarios y grupos. El mejor lugar para descubrir los recursos consumidos (adiciones, eliminaciones, actualizaciones, cambios de licencias o asignaciones de roles de la aplicación) es en el registro de auditoría de Azure Active Directory en el portal de Azure.

Lamentablemente, solo se puede buscar en una única categoría (**UserManagement**; véase la figura 9 y, después, en **GroupManagement**) a la vez, por lo que los administradores deben ejecutar múltiples consultas para recopilar información.

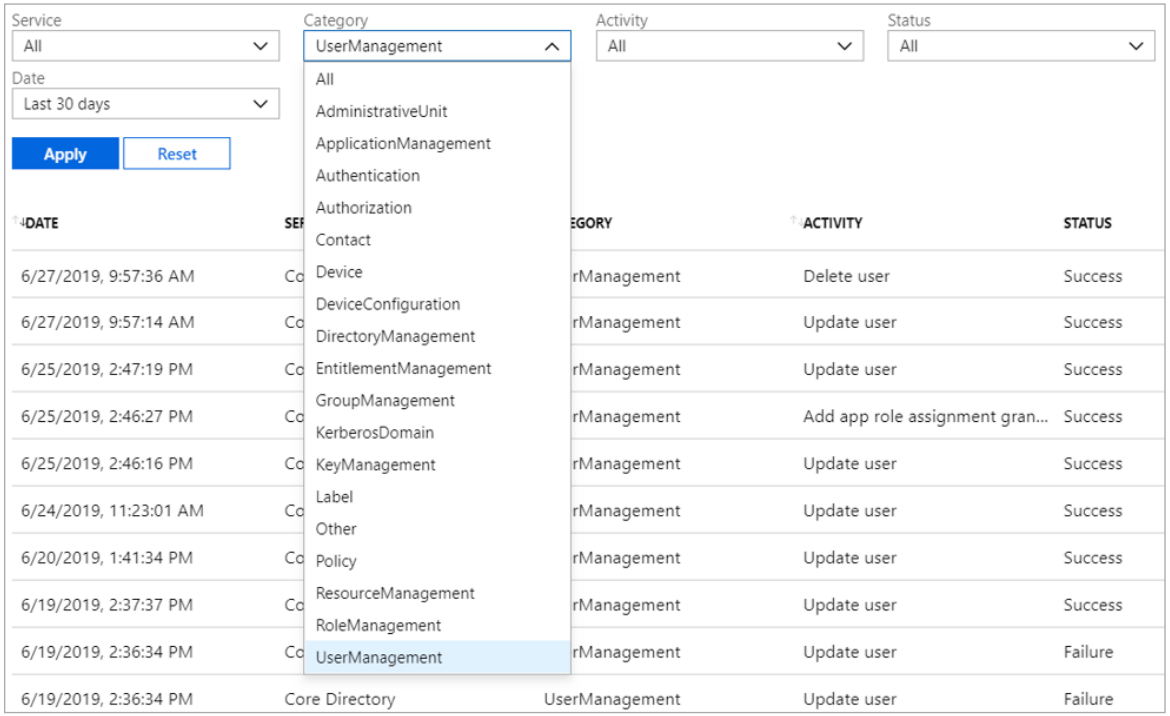


Figura 9: Recursos creados listados en el registro de auditoría de Azure

Ser capaz de hacer un seguimiento del tipo y el número de recursos creados ayudará a los administradores a reducir la costosa y lenta carga de administrarlos.

Quest

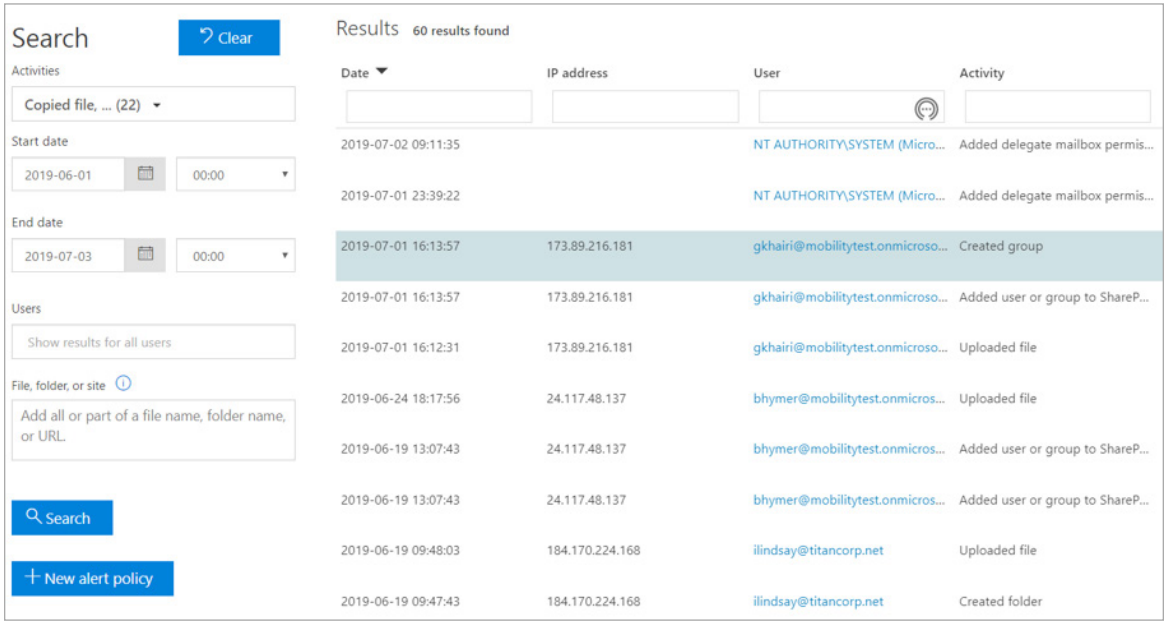


Figura 10: Recursos creados listados en el registro de auditoría unificado

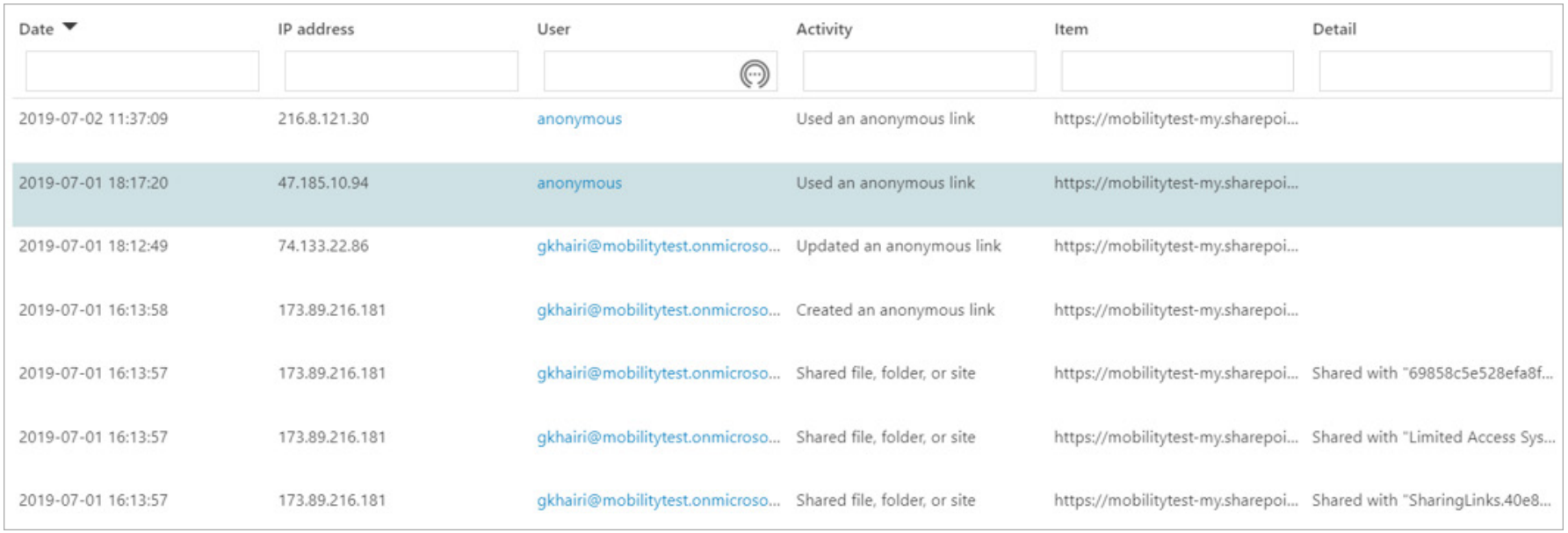
ENCONTRAR RECURSOS CREADOS EN EL REGISTRO DE AUDITORÍA UNIFICADO

La búsqueda de registros de auditoría en el Centro de seguridad y cumplimiento de Office 365 (véase la figura 10) ofrece una vista de múltiples recursos:

- Archivos: Copiado, movido, cargado, renombrado o restaurado
- Carpetas: Creada, renombrada, movida o restaurada
- Sitios de SharePoint: Lista creada, elemento de lista creado
- Permisos de Site: Se agregó el administrador de la colección de sitios, se agregó un usuario o grupo al grupo de SharePoint, se creó un grupo
- Exchange: Elemento del buzón de correo creado, permisos del buzón de correo agregados
- Sway: Sway creado
- Teams: Equipo creado, pestaña añadida, conector añadido, canal añadido, miembros añadidos, bot añadido

Obtener una imagen completa de todos esos recursos requiere múltiples consultas. Y, como ocurre con cualquier otra búsqueda de eventos de auditoría de Office 365, los detalles estarán en el JSON integrado, lo que los hace menos accesibles que el simple resultado de una consulta.

Quest



Date	IP address	User	Activity	Item	Detail
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "69858c5e528efa8f...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "Limited Access Sys...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "SharingLinks.40e8...

Figura 11: Actividad de uso compartido que figura en el registro de auditoría unificado

5 y 6. Uso compartido: archivos importantes y datos anónimos

La migración a SharePoint Online y OneDrive para la Empresa introduce nuevos tipos de riesgo, especialmente en lo que respecta al uso compartido de datos. Como se mencionó anteriormente, los usuarios pueden compartir datos confidenciales de forma involuntaria incluyendo, sin darse cuenta, a un usuario B2B de otra empresa. Por ejemplo, un usuario no autorizado que obtenga un enlace de uso compartido libre a los datos de OneDrive puede acceder al archivo de forma anónima.

El aumento del riesgo es la desventaja de un mayor intercambio de información. Para el departamento de TI, poder generar informes de

Un usuario no autorizado que obtenga un enlace de uso compartido libre a los datos de OneDrive puede acceder al archivo de forma anónima.

Azure AD sobre el uso compartido de datos es aún más importante a medida que las empresas se migran a la nube. Las empresas tienen razones de peso para bloquear o controlar estrictamente el uso compartido de tipos de archivos específicos.

ENCONTRAR SOLICITUDES DE ACCESO Y USOS COMPARTIDOS EN EL REGISTRO DE AUDITORÍA UNIFICADO

La búsqueda de registros de auditoría en el Centro de seguridad y cumplimiento de Office 365 devuelve información sobre archivos, carpetas y sitios compartidos. La figura 11 representa los resultados de

una búsqueda en las **actividades de solicitud de acceso y uso compartido.**

El problema es que la consulta devuelve todos los datos de esas actividades. Una consulta más eficaz y útil limitaría los resultados a las extensiones de los archivos compartidos, como CER, DER, CRT, PEM, PFX, P7B, P7C, P12, PPK, PUB, SPC, STL, CRL, SSH, EVT, EXE, BAT y PIF. O bien podría reducir los resultados a extensiones de archivo de Microsoft Office, PPT, PPTX, XLS, XLSX, DOC, DOCX, etc. La búsqueda de registros de auditoría no lo permite.

Otra opción es exportar el superconjunto de datos del campo **AuditData** del registro de auditoría unificado a un formato de hoja de cálculo. No obstante, es necesario manipular algunos datos para limitar los resultados a las partes cuestionables.

Las acciones anónimas, que son de particular interés, son más fáciles de consultar introduciendo la palabra “anónimo” en el filtro de actividad, como se muestra en la figura 12.

Cambiar el filtro de usuario a “anónimo” devuelve cualquier archivo al que se haya accedido de forma anónima. Se obtienen resultados similares al filtrar las columnas **UserIds** u **Operations** en los eventos de auditoría exportados.

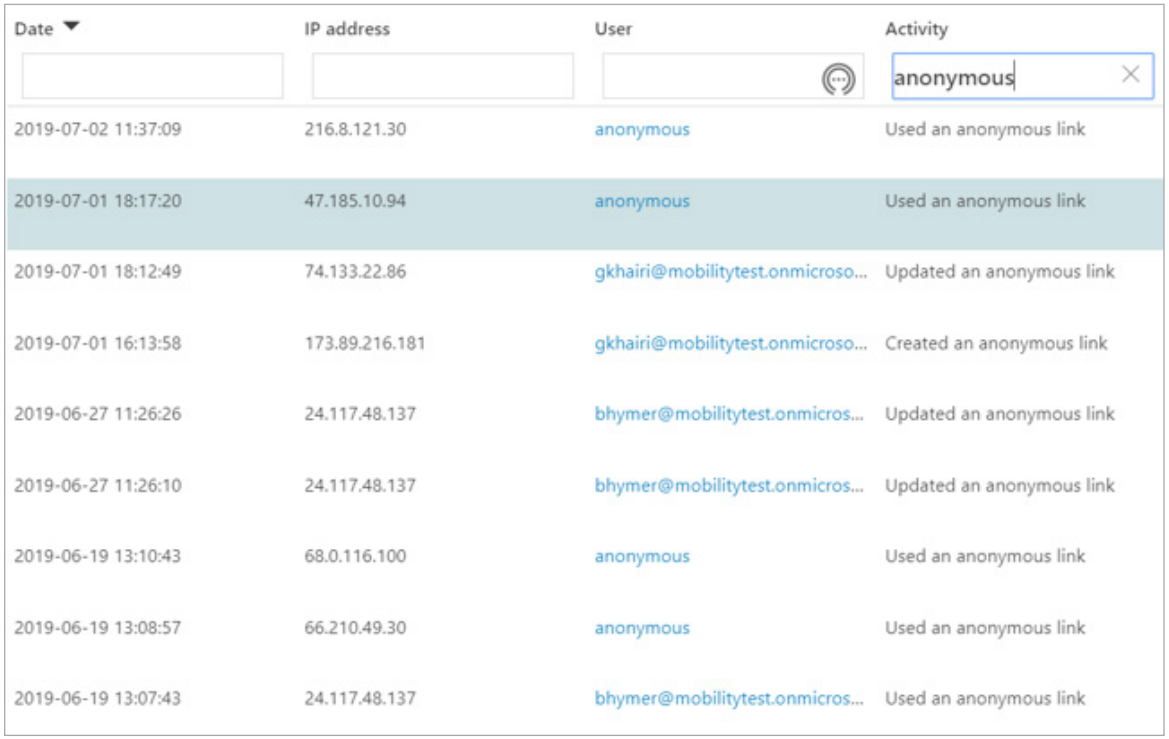
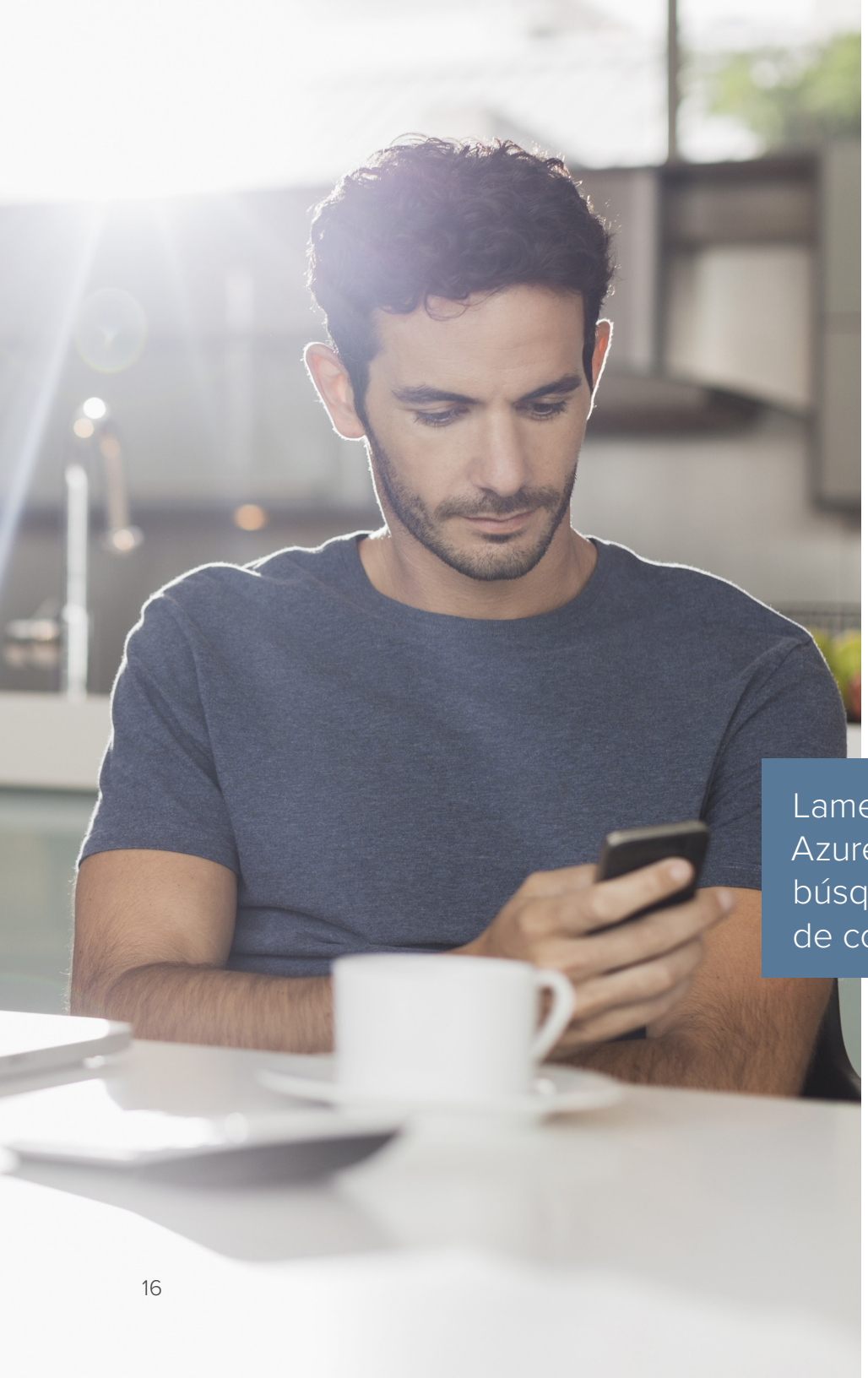


Figura 12: Resultados de la búsqueda en la actividad de uso compartido anónima

Quest



7. Correo electrónico: reenvío de mensajes entrantes

Por sí mismo, el reenvío de correo electrónico entrante a otros destinatarios no es ni bueno ni malo. Es posible que los destinatarios necesiten compartir información en un mensaje con proveedores o clientes externos. Los consultores y contratistas *in situ* pueden preferir reenviar mensajes y consolidar todo su correo electrónico en una sola cuenta. Los usuarios pueden reenviar el correo electrónico manualmente, además un usuario (a través de ForwardSMTP) o un administrador (a través de ForwardAlias) pueden configurar el reenvío automático en un buzón de correo.

El reenvío automático podría ser perfectamente inofensivo, pero los administradores inteligentes mantienen un ojo en los cambios que implican el reenvío de correos electrónicos para impedir aquellos que sugieren una actividad maliciosa.

Lamentablemente, los registros de auditoría en Azure Active Directory y Office 365 no permiten búsquedas directas sobre los cambios en los reenvíos de correo electrónico.

Lamentablemente, los registros de auditoría en Azure Active Directory y Office 365 no permiten búsquedas directas sobre esos cambios. En su lugar, es necesario exportar el registro completo para cambios en Exchange Online, y luego buscar los eventos de auditoría exportados con **{“nombre”:“DeliverToMailboxAndForward”,“valor”:“True”}** en el campo Parámetros del detalle de auditoría con el fin de que se devuelvan los eventos deseados.

Quest

8. Correo electrónico: actividad no propietaria

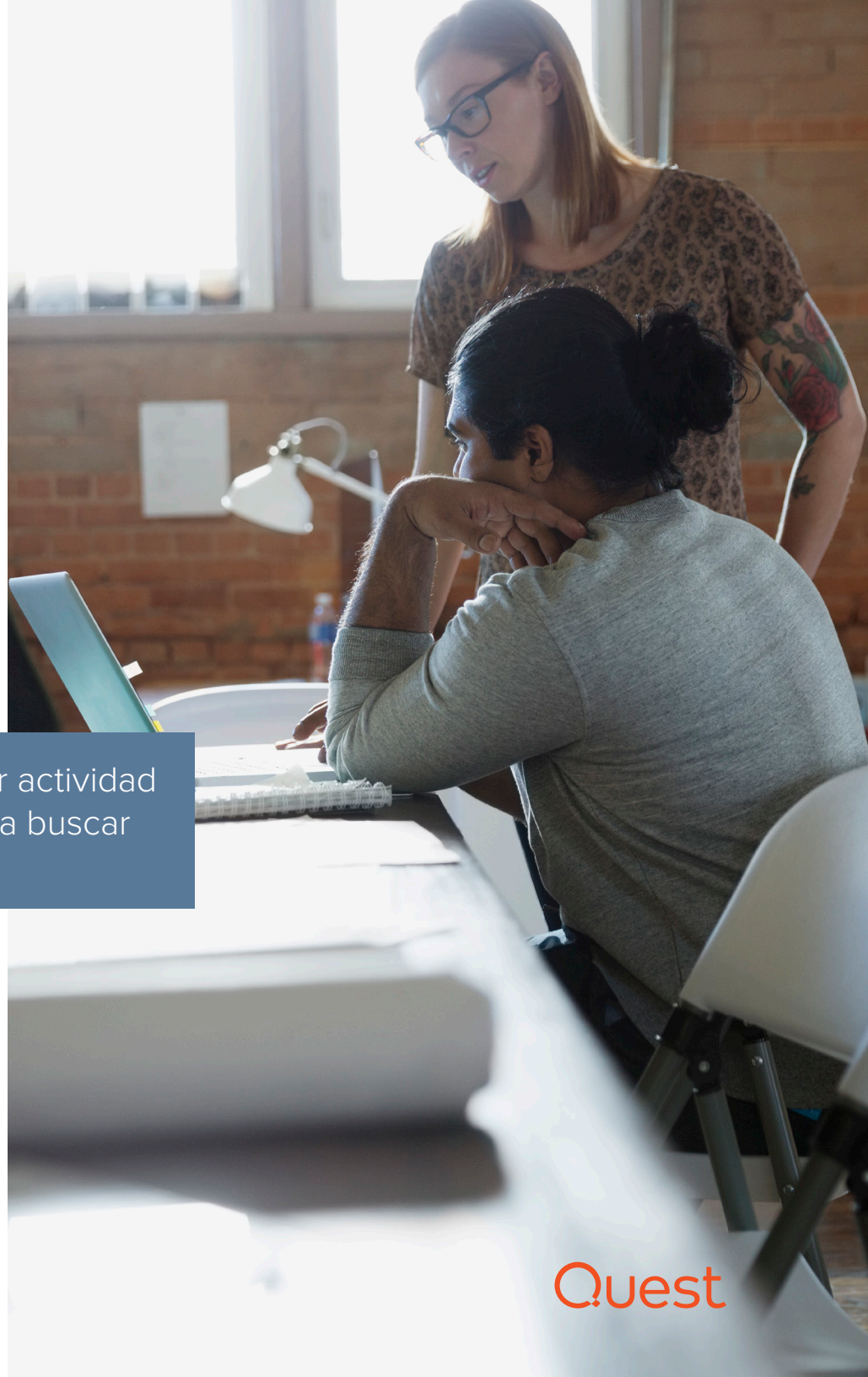
La actividad de correo electrónico no propietaria es habitual en las grandes organizaciones, donde los auxiliares administrativos tienen acceso a las cuentas de correo electrónico de los ejecutivos a los que ayudan, o donde varios empleados comparten buzones de correo. Si la cuenta de un no propietario se ve comprometida, un atacante puede obtener acceso a información confidencial.

En el contexto de la administración de Exchange Online, los administradores pueden realizar casi cualquier actividad con sus derechos, incluso concederse acceso para buscar en otros buzones ejecutivos. Aunque toda organización confía en que sus administradores gestionen y realicen un buen mantenimiento de los sistemas, también debe prestar atención a las actividades fraudulentas.

Los administradores pueden realizar casi cualquier actividad con sus derechos, incluso concederse acceso para buscar en otros buzones ejecutivos.

ENCONTRAR ACTIVIDADES DE CORREO ELECTRÓNICO SIN PROPIETARIO EN EL REGISTRO DE AUDITORÍA UNIFICADO

La información sobre la actividad de los no propietarios solo está disponible en el registro de auditoría unificado, como se muestra en la figura 13. Para buscar los tipos de actividad que la mayoría de los no propietarios realizan en los buzones de correo, incluya lo siguiente:



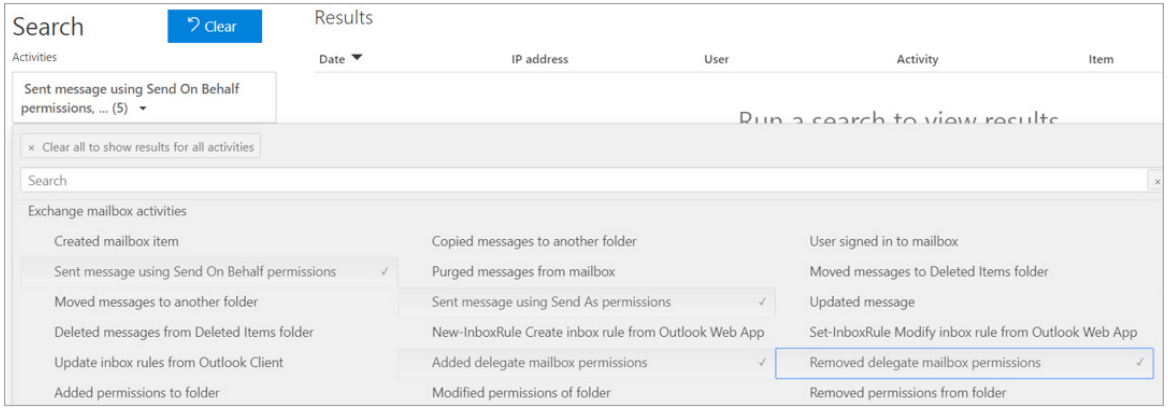


Figura 13: Actividad no propietaria de correo electrónico incluida en el registro de auditoría unificado

Figura 14: Detalle de la columna AuditData

- Se ha enviado un mensaje con permisos de Enviar en nombre de
- Se ha agregado o quitado un usuario con acceso de delegado al calendario/carpeta
- Se ha enviado un mensaje con permisos de Enviar como
- Se han agregado permisos de buzón de correo delegado
- Se han quitado permisos de buzón de correo delegado

Tenga en cuenta, sin embargo, que estas no cubren actividades como añadir, eliminar y mover carpetas y mensajes, ni cambios en algunos permisos, por nombrar algunas. Consultar todas las **actividades del buzón de correo** y exportar los resultados como una hoja de cálculo es la forma de realizar una búsqueda exhaustiva.

Pero el siguiente paso (encontrar eventos de auditoría donde **LogonUserSid** no coincida con **MailboxOwnerMasterSid**) es un trabajo intensivo porque la información está incrustada en la columna **AuditData** con el resto de la información del evento (véase la figura 14).[4]

4 Consulte también "Auditing Privileged Operations and Mailbox Access in Office 365 Exchange Online", https://www.quest.com/docs/auditing-privileged-operations-and-mailbox-access-in-office-365-white-paper-24932.pdf.

Quest

9. Historial de comandos de administración

Microsoft proporciona herramientas administrativas como Microsoft Management Console (MMC) para la gestión local, y portales web para la gestión de la nube. Microsoft hace cada vez más hincapié en PowerShell como el principal método de administración. De hecho, muchas consolas MMC ejecutan comandos PowerShell basados en eventos pasados desde la interfaz de usuario; Exchange es un ejemplo típico.

Sin embargo, por muy importante que sea para asegurar que los comandos se ejecutan correctamente, es casi imposible hacer un seguimiento del historial de comandos. Por ejemplo, es una buena idea hacer un seguimiento de los eventos de consentimiento de la aplicación y cualquier cambio en las políticas de acceso condicional en Azure AD. El acceso de lectura/escritura en objetos concedidos a la aplicación incorrecta puede tener como consecuencia una vulnerabilidad.

El problema es que actualmente no hay forma de extraer un historial de comandos de administrador ejecutados desde los portales de Azure y Office 365.

Actualmente, no hay forma de extraer un historial de comandos de administrador ejecutados desde los portales de Azure y Office 365.

Quest

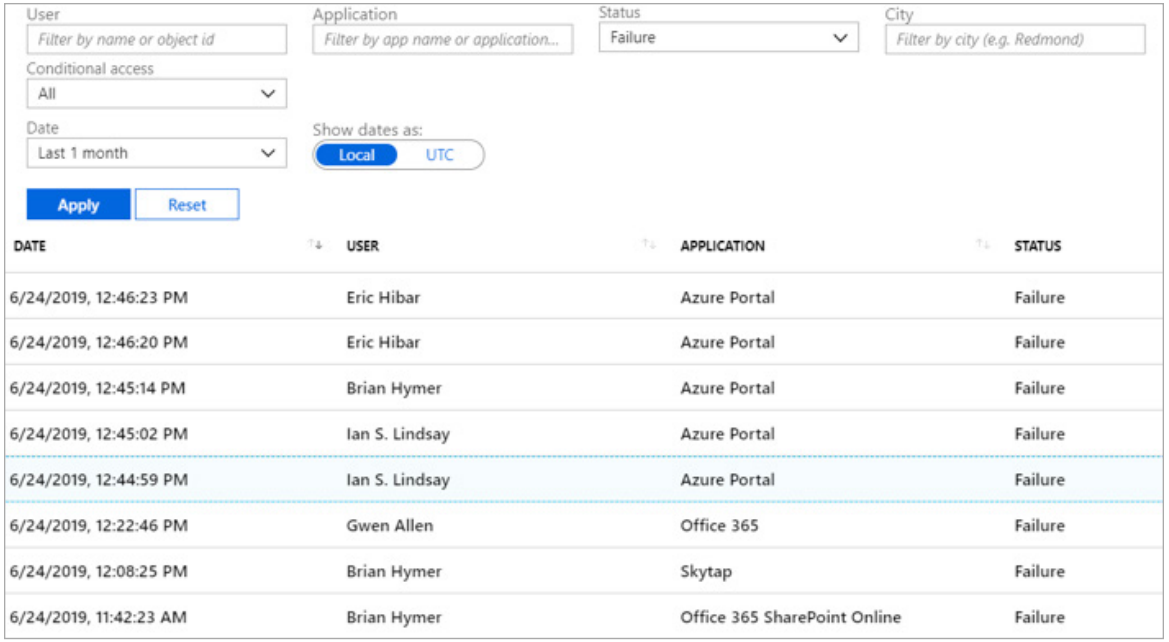


Figura 15: Buscar en inicios de sesión fallidos en Azure AD

Los inicios de sesión repetidos y fallidos pueden indicar actividad maliciosa, ya que los malos actores intentan introducir las contraseñas de los usuarios por la fuerza bruta.

10. Fallos de inicio de sesión

Tanto de forma local como en la nube, el seguimiento de los inicios de sesión fallidos forma parte del trabajo de un administrador. Los bloqueos frustran a los usuarios, que rara vez saben cómo o por qué han sido bloqueados. Los inicios de sesión híbridos a través de Azure AD agravan el problema añadiendo otra fuente potencial de bloqueo. Pero los inicios de sesión repetidos y fallidos pueden indicar actividad maliciosa, ya que los malos actores intentan introducir las contraseñas de los usuarios por la fuerza bruta.

En las instalaciones, la información sobre eventos de inicio de sesión fallidos se almacena en los registros de seguridad de todos los controladores de dominio. En la nube, esa información está en los eventos de auditoría de todos los inquilinos de Azure. Como se muestra en la figura 15, la búsqueda en **Error** en la pantalla **Inicios de sesión** debajo de **Supervisión** en Azure AD de cada inquilino devuelve los eventos de inicio de sesión fallidos.

Pero reunir todos los eventos de inicio de sesión fallidos es solo el comienzo. La siguiente tarea es analizar toda la información de los patrones, tarea que no se ve facilitada por la falta de detalle en los resultados de la búsqueda.

Quest

Conclusión: Auditoría bajo demanda de Quest

Dadas las deficiencias de las herramientas nativas para la elaboración de informes de Office 365 y Azure, ¿qué pasaría si no tuviera que volar a ciegas?

On Demand Audit Hybrid Suite para Office 365 de Quest proporciona una única vista alojada de la actividad de los usuarios en los entornos híbridos de Microsoft. Expone todos los cambios que tienen lugar, ya sea en las cargas de trabajo de AD local, de Azure AD o de Office 365 como en Exchange Online, SharePoint Online y OneDrive para la Empresa. En lugar de buscar a través de miradas parciales en los registros de auditoría, puede utilizar la búsqueda con capacidad de respuesta en años de datos con el fin de investigar e informar sobre los eventos desde una única ventana. La integración con Power BI de Microsoft le permite generar informes a través de la visualización interactiva de datos, como se muestra en la figura 16.

On Demand Audit Hybrid Suite proporciona un acceso granular y delegado que permite a los usuarios obtener la información que necesitan sin necesidad de realizar ningún cambio de configuración ni de configurar una infraestructura adicional. Con solo unos clics, puede proporcionar a sus equipos de seguridad y cumplimiento de normativas, al personal del servicio de asistencia técnica, a los responsables de TI e incluso a los auditores externos y socios exactamente los informes que necesitan y nada más.

Para obtener más información, visite quest.com/on-demand.

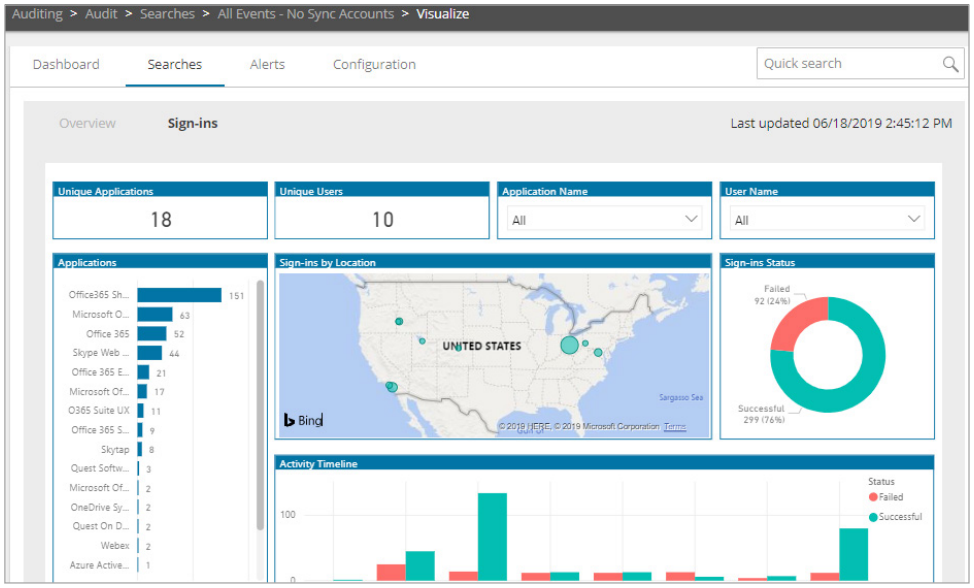


Figura 16: Auditoría bajo demanda

On Demand Audit Hybrid Suite proporciona un acceso granular y delegado que permite a los usuarios obtener la información que necesitan sin necesidad de realizar ningún cambio de configuración ni de configurar una infraestructura adicional.

Quest

ACERCA DE QUEST

Quest ofrece soluciones de software para el mundo de la TI empresarial que cambia rápidamente. Ayudamos a simplificar los retos que plantean la explosión de datos, la expansión de la cloud, los centros de datos híbridos, las amenazas de seguridad y los requisitos normativos. Ofrecemos nuestros servicios de forma global a más de 130 000 empresas de 100 países, incluido el 95 % del Fortune 500 y el 90 % del Global 1000. Desde 1987, hemos creado una cartera de soluciones que ahora incluye la gestión de bases de datos, la protección de datos, la gestión de identidades y accesos, la gestión de la plataforma de Microsoft y la gestión de unificada de puntos finales. Con Quest, las organizaciones dedicarán menos tiempo a la administración de TI y más a la innovación de sus negocios. Para obtener más información, visite www.quest.com.

Si tiene alguna duda sobre el uso que puede hacer de este material, póngase en contacto con nosotros:
www.quest.com

Ebook-SecurityEventsToMonitor-US-GM-ES-WL-40070

Quest