ManageEngine
Log360 Cloud

MONITOREO DE AD PROACTIVO

con Log360 Cloud

5 CASOS DE USO **CRÍTICOS**

Las empresas confían en Active Directory (AD) por su capacidad para gestionar y organizar recursos como usuarios, computadores y servicios de forma centralizada y segura. Como resultado, siempre existe la posibilidad de que los actores de amenazas ataquen AD y realicen modificaciones y cambios de configuración para obtener acceso no autorizado, lo que conduce a violaciones de datos, interrupciones del servicio y otros incidentes de seguridad. En este documento, analizaremos cinco casos de uso críticos que los administradores de TI y los equipos de seguridad deben tener en cuenta a la hora de proteger su entorno de AD.

1.Auditar las modificaciones en GPO

Un objeto de directiva de grupo (GPO) define varios ajustes para las cuentas de equipos y usuarios dentro de un entorno de AD. Cualquier cambio no autorizado en un GPO relacionado con privilegios, acceso a información o servicios, o ajustes de seguridad puede provocar interrupciones y problemas de seguridad.

1. Auditar los cambios críticos en las políticas, como los cambios en la política de bloqueo de cuenta y la política de cambio de contraseña, ayuda a detectar y responder a actividades maliciosas al instante.
2. Monitorear cualquier cambio o modificación no autorizada en los ajustes de seguridad del GPO es crucial. Algunas modificaciones (como reducir los requisitos de complejidad o longitud de las contraseñas, desactivar los firewalls de Windows o permitir servicios de desktop remoto en redes inseguras) hacen que la organización sea vulnerable a posibles brechas de seguridad.

3. Auditar los GPO también es crucial, ya que se utilizan para gestionar los ajustes de las políticas de actualización de Windows en todas las unidades organizativas. Monitorear estos cambios garantiza que estas políticas estén configuradas correctamente, previniendo cualquier cambio no aprobado que pueda representar una amenaza a su seguridad.

PROBLEMA:

Imagine un escenario en el que un actor malicioso obtiene acceso no autorizado al entorno de AD y modifica los ajustes del GPO. El atacante podría debilitar las políticas de contraseñas, desactivar configuraciones de seguridad críticas o conceder acceso no autorizado a archivos confidenciales.

Tomemos el ejemplo de un atacante que quiere debilitar las políticas de contraseña para poder tener acceso no autorizado a las cuentas de usuario.

En un entorno de AD nativo, las políticas de contraseña se configuran a través de GPO, normalmente en la política de dominio predeterminada.

Una de las configuraciones asociadas con las políticas de contraseña es la longitud mínima de la contraseña.

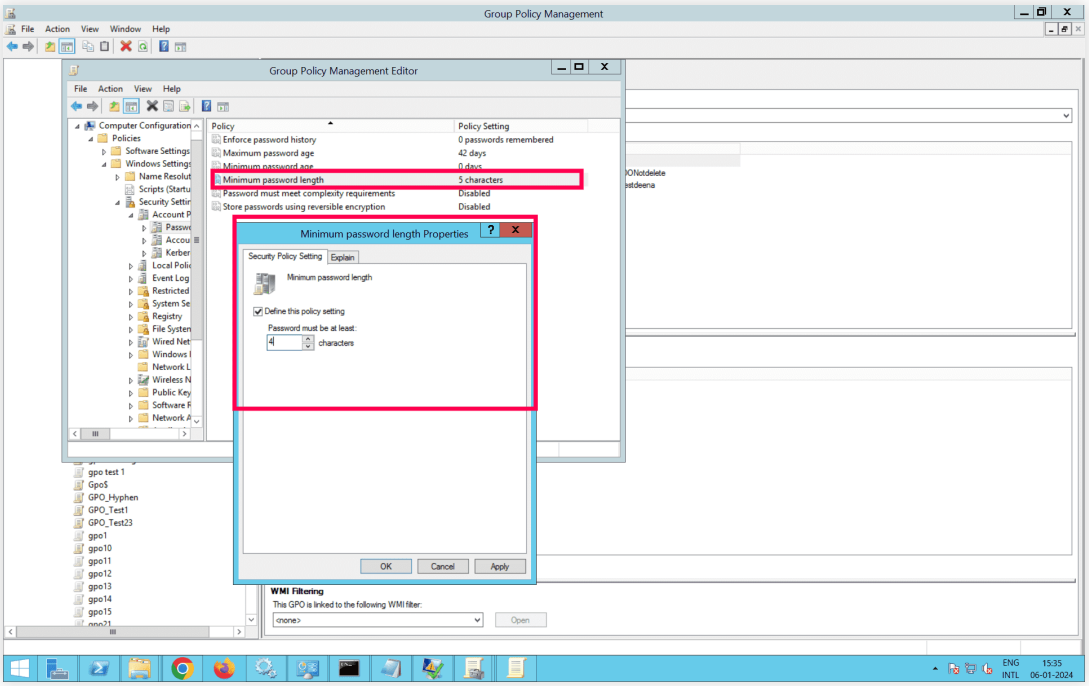

Fig. 1: Modificar la propiedad de longitud mínima de la contraseña

El atacante podría modificar esta configuración para debilitar la política de contraseña reduciendo la longitud mínima de la contraseña, y aumentando así la vulnerabilidad de las cuentas de usuario.

SOLUCIÓN:

Cambios en los ajustes de GPO > Cambios en la política de contraseña

En Log360 Cloud (véase Figura 2):

1. Vaya a la pestaña **Informes**.
2. Vaya a Dispositivos en el menú desplegable y luego al menú **Active Directory**.
3. Vaya a **Cambios en los ajustes de GPO > Cambios en la política de contraseña.**

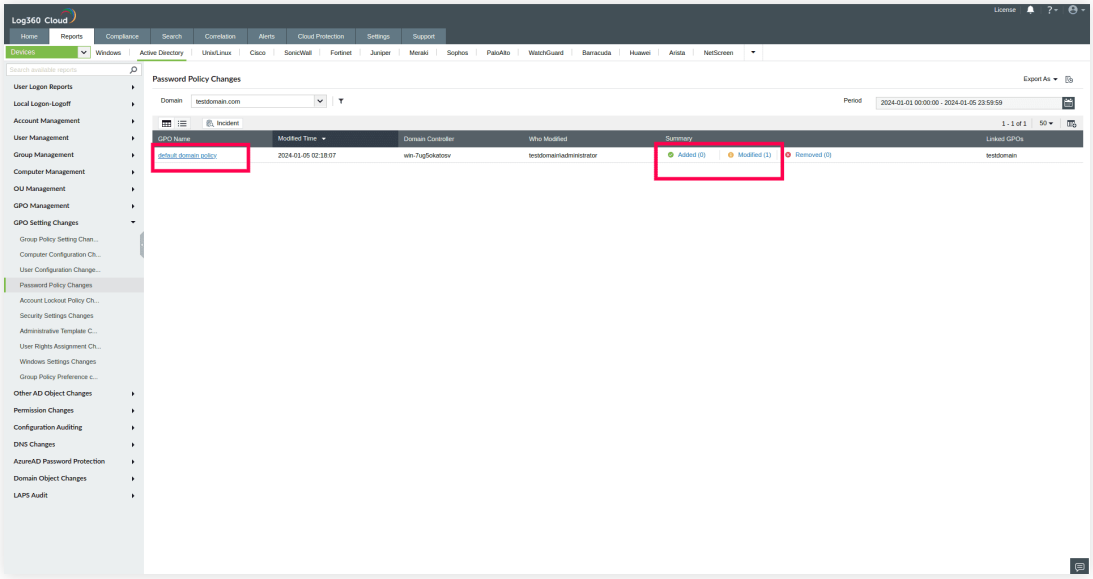

Fig. 2: Cambio en la política de contraseña

4. Haga clic en el cambio reportado.
5. Vea el ajuste del GPO modificado (como se muestra en la Figura 3)

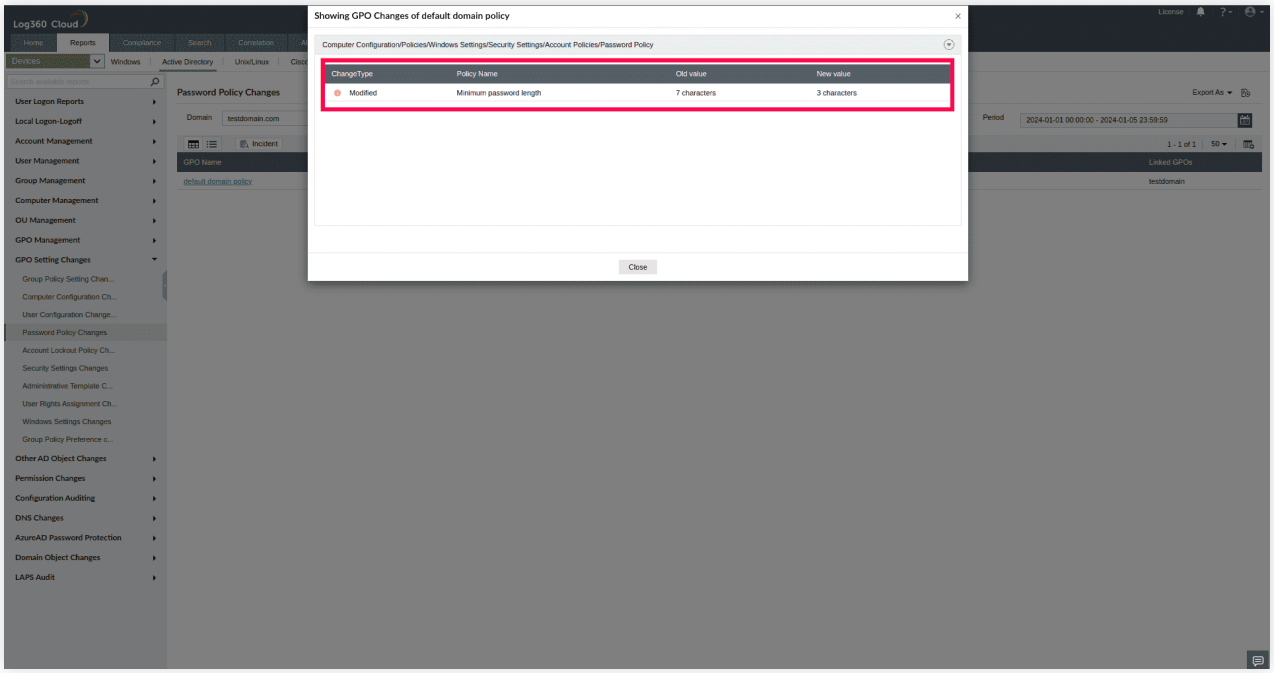

Fig. 3: Cambios en el GPO de la política de dominio predeterminada

2.Auditar los usuarios creados recientemente

Un usuario, con los permisos de cuenta adecuados, puede realizar casi cualquier cambio en el entorno de AD.

PROBLEMA:

Considere un escenario en el que un intruso crea una nueva cuenta de usuario y añade este usuario a un grupo privilegiado. La creación de usuarios puede ser una parte de la secuencia de ataque que el atacante utiliza para navegar dentro de la red. Este usuario podría obtener acceso sin restricciones a datos sensibles, dependiendo del grupo al que haya sido añadido.

SOLUCIÓN:

Gestión de usuarios > Usuarios creados recientemente

En Log360 Cloud (véase Figura 4):

1. Vaya a la pestaña **Informes**.
2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
3. Vaya a **Gestión de usuarios > Usuarios creados recientemente.**
4. Vea los usuarios creados recientemente.

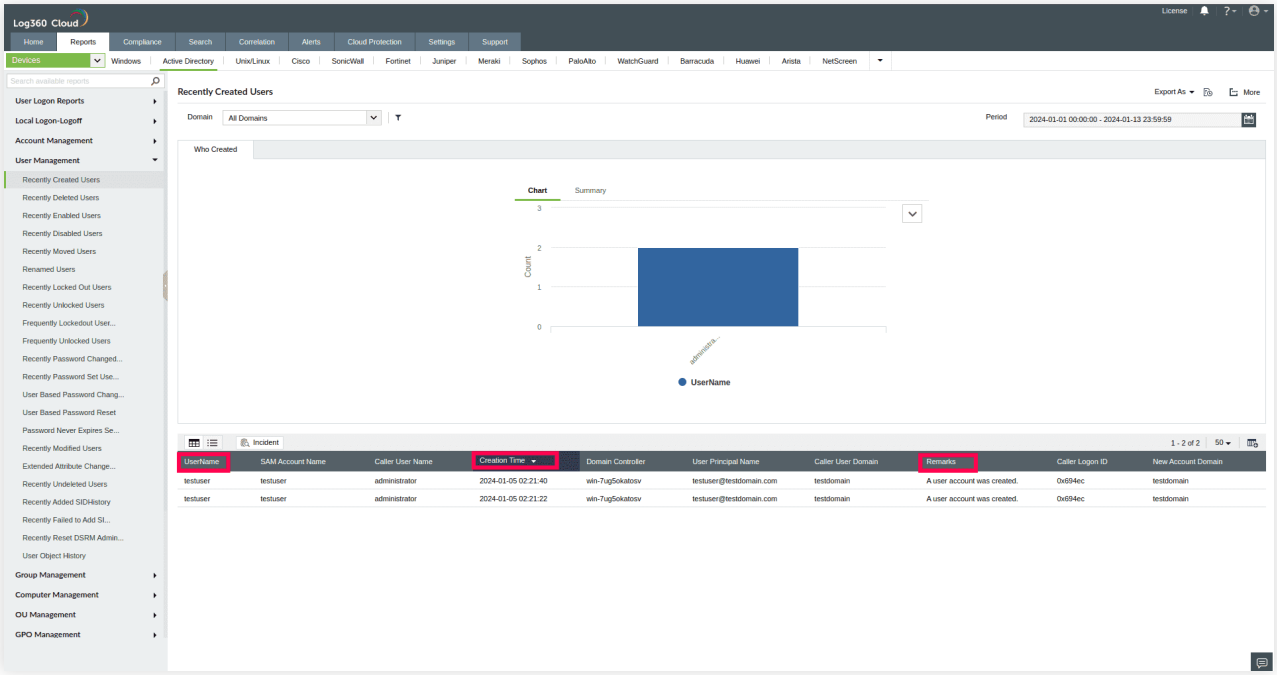

Fig. 4: Usuarios creados recientemente

3. Auditar los usuarios habilitados recientemente

Los actores maliciosos pueden intentar habilitar cuentas de usuario que han permanecido inactivas o deshabilitadas durante largos periodos de tiempo para evitar ser detectados. Los casos en los que la cuenta deshabilitada tiene privilegios administrativos pueden conducir a un escalamiento de privilegios, otorgando a los atacantes permisos elevados.

PROBLEMA:

Considere un caso en el que una cuenta de usuario deshabilitada ha sido habilitada y utilizada indebidamente por agentes maliciosos. Esto puede facilitar el movimiento lateral dentro de la red. Dado que las cuentas deshabilitadas atraen menos atención, volver a habilitar una puede ayudar al atacante a permanecer en la red sigilosamente. Auditar a los usuarios recientemente habilitados es especialmente importante cuando se realizan cambios en los privilegios de los usuarios. Las modificaciones repentinas en las cuentas de usuario, como habilitar el acceso administrativo, podrían indicar un incidente de seguridad o un intento de escalar privilegios.

SOLUCIÓN:

Gestión de usuarios > Usuarios habilitados recientemente

En Log360 Cloud (véase Figura 5):

1. Vaya a la pestaña **Informes**.
2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
3. Vaya a **Gestión de usuarios > Usuarios habilitados recientemente.**
4. Vea los usuarios habilitados recientemente.

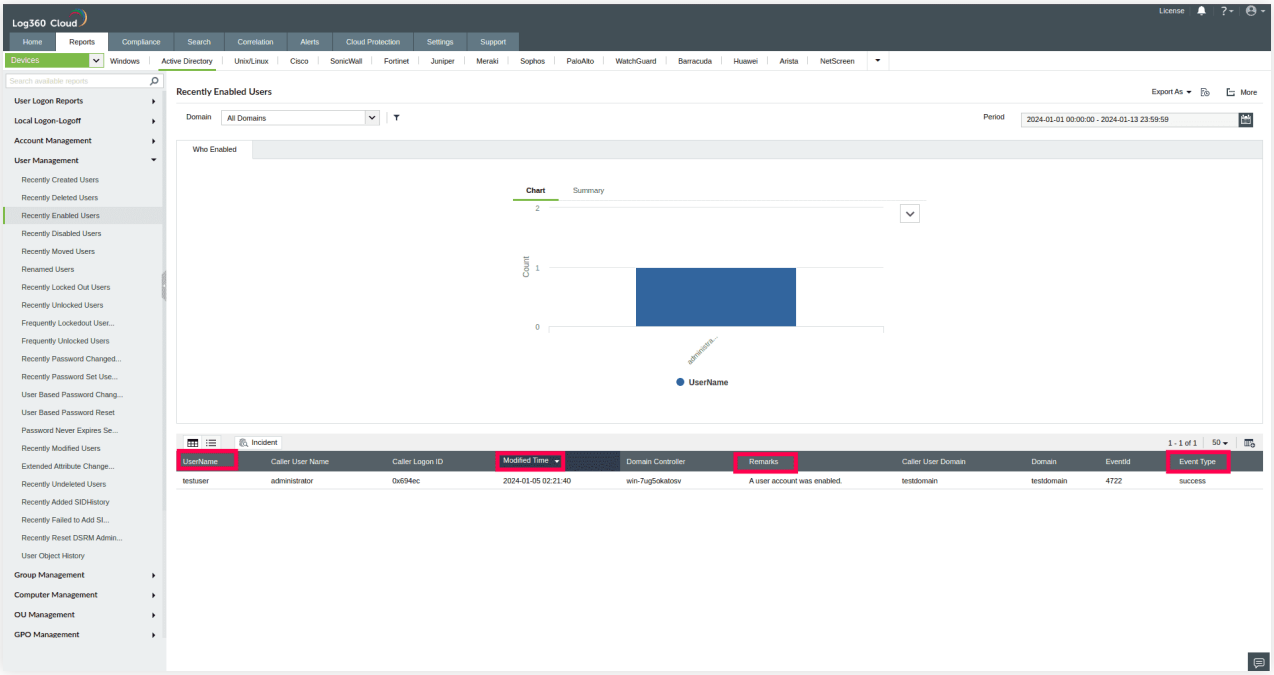

Fig. 5: Usuarios habilitados recientemente

4.Auditar las unidades organizativas modificadas recientemente

Es crítico auditar los cambios en las unidades organizativas (OU) porque son un perímetro administrativo. Pueden contener usuarios, equipos, grupos y otras OU dentro de ellas. Los ajustes de la política se pueden aplicar a nivel de OU, vinculando un GPO a una OU. Cualquier modificación no autorizada, como añadir un usuario a una OU, puede suponer una amenaza para la postura de seguridad de la organización, ya que todos los ajustes que se aplican a la OU también se aplicarán a la OU recién añadida.

PROBLEMA:

Imagine que un atacante bloquea una OU específica para que no herede las políticas de seguridad que el administrador ha implementado, manipulando los ajustes de herencia de políticas de grupo de la OU. Esto significaría que los usuarios y equipos dentro de esa OU son vulnerables a actividades maliciosas.

SOLUCIÓN:

Gestión de OU > OU modificadas recientemente

En Log360 Cloud (véase Figura 6):

1. Vaya a la pestaña Informes.
2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
3. Vaya a **Gestión de OU > OU modificadas recientemente.**
4. Vea las OU modificadas recientemente.

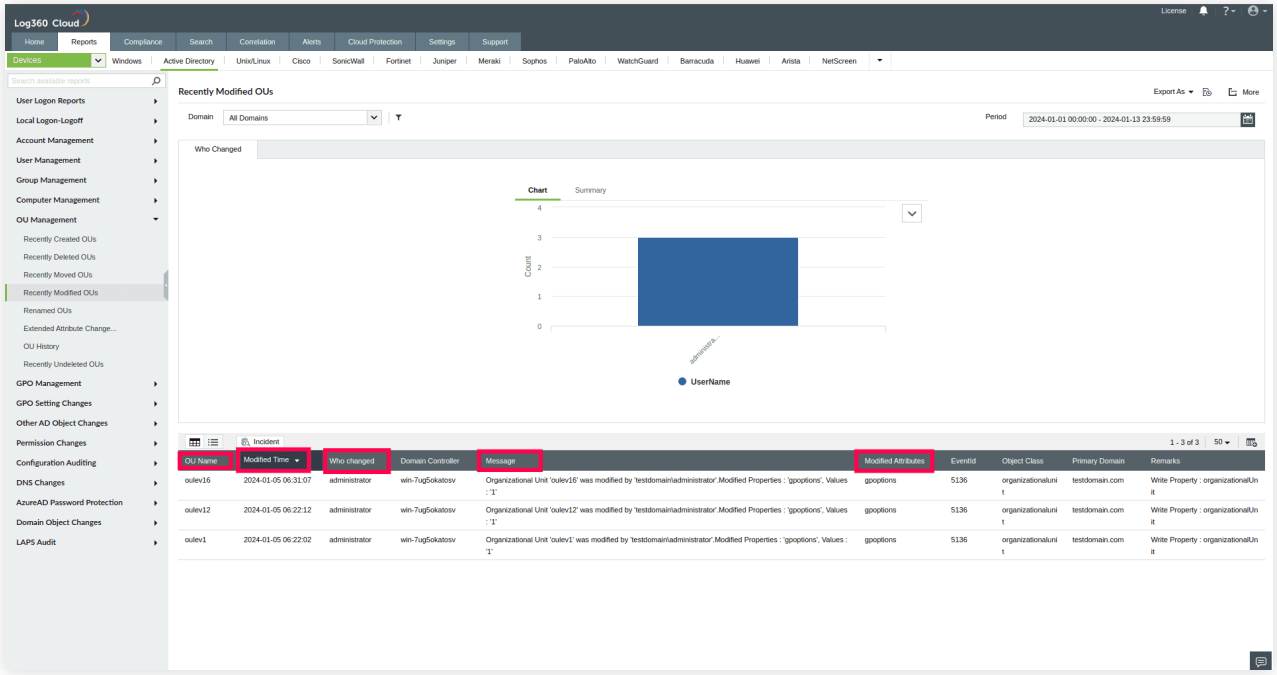

Fig. 6: Unidades organizativas modificadas recientemente

5. Auditar los nuevos miembros añadidos al grupo de seguridad de administradores de dominio

El grupo de administradores de dominio en AD se utiliza para asignar funciones administrativas a los usuarios del dominio. Por defecto, este grupo es miembro del grupo de administradores y, por tanto, lleva asociado un conjunto de privilegios.

Los miembros del grupo de administradores de dominio tienen acceso ilimitado a los recursos compartidos y a los objetos de AD.

PROBLEMA:

Consideremos un escenario en el que un actor malicioso añade un nuevo usuario al grupo de administradores de dominio. Esto proporcionaría al nuevo miembro acceso sin restricciones a los recursos compartidos y objetos de AD.

SOLUCIÓN:

Gestión de grupos > Miembros añadidos recientemente a un grupo de seguridad

En Log360 Cloud (véase Figura 7):

1. Vaya a la pestaña **Informes**.
2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
3. Vaya a **Gestión de grupos > Miembros añadidos recientemente a un grupo de seguridad.**
4. Vea las OU modificadas recientemente.

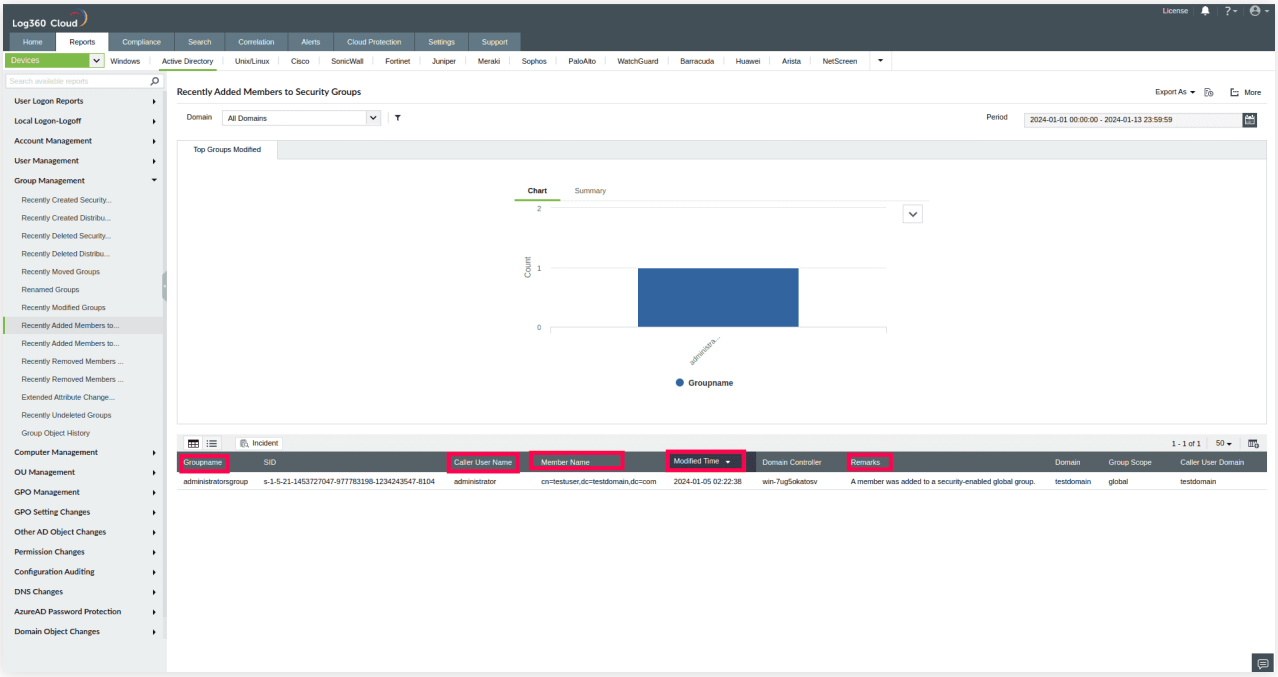

Fig. 7: Miembros añadidos recientemente a un grupo de seguridad

Acerca de log360 Cloud

ManageEngine Log360 Cloud, una solución SIEM unificada en la nube con funciones de CASB integradas, ayuda a las empresas a proteger su red de ataques cibernéticos. Con sus funciones de análisis de seguridad, inteligencia de amenazas y gestión de incidentes, Log360 Cloud ayuda a los analistas de seguridad a detectar, priorizar y resolver amenazas tanto en entornos on-premises como en la nube. La solución es altamente escalable y ayuda a reducir los costos de infraestructura y almacenamiento.

Para obtener más información sobre Log360 Cloud, visite www.manageengine.com/latam/cloud-log-management/

Registrarse gratis

Demostración personalizada