Solución de problemas de usuarios de Active Directory que faltan en el informe de búsqueda de actividad en Umbrella

Contenido

Introducción

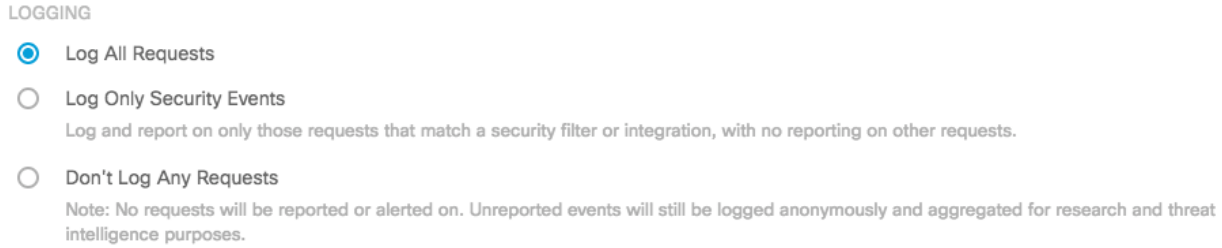
Este documento describe el Informe de búsqueda de actividad en Cisco Umbrella. El Informe de búsqueda de actividad es un informe casi activo de todas las consultas de DNS que realizan los usuarios. Si ha configurado la integración de Cisco Umbrella Active Directory (AD), es probable que los usuarios de AD rellenen la columna Identidad en la búsqueda de actividad. Sin embargo, hay situaciones en las que los usuarios no aparecen en la columna Identidad.

Resolución

Si cree que debería ver a los usuarios de AD directamente en la columna Identidad de la búsqueda de actividad, pero no los ve, o ve algunos, pero no tantos como esperaba, a continuación se indican algunas cosas que debe comprobar:

1. Sitios y Active Directory
    - Compruebe todos los componentes de AD para asegurarse de que no haya errores o problemas notificados. Si ve indicadores de estado grises, naranjas o rojos en alguno de los componentes, obtenga estos detalles y abra un ticket de soporte (umbrella-support@cisco.com).
        - Prueba de diagnóstico de un usuario afectado (un usuario que no aparece en la búsqueda de actividad)
        - Captura de pantalla de la consola del dispositivo virtual (VA), con los mensajes de error expandidos.
        - Registros de auditoría del conector AD
2. Configuración de registro
    - En la Configuración avanzada de cada política, hay una sección en la parte inferior que se refiere a la cantidad de registro. Se puede establecer en:
        - Registrar todas las solicitudes
        - Registrar solo eventos de seguridad
        - No registrar ninguna solicitud

- Si su política está configurada actualmente en "Registrar solo eventos de seguridad", eso puede explicar por qué no está viendo tantas consultas como espera o ningún resultado de algunos usuarios.



3. Precedencia de políticas correcta
    - Si tiene una política que se aplica a una identidad de red que es más alta en la lista de políticas que su política de usuario de AD, es probable que se aplique la política de identidad de red. Esto, a su vez, significa que en la búsqueda de actividad, verá la red como la identidad notificada. Consulte también la documentación de Cisco Umbrella sobre Prácticas recomendadas y Prioridad de las políticas.

Causa

¿De dónde obtiene la "Identidad" la búsqueda de actividades?

Cuando una consulta DNS entra en Umbrella, suponiendo que la integración de AD funciona como se esperaba, esta información se pasa en la consulta:

- Dirección IP interna
- Hash de identidad de AD (usuario, host o ambos)
- IP de salida
- Dominio consultado

El Hash de identidad de AD es agregado a la consulta por el Dispositivo virtual, a quien se le pasa esa información, y la dirección IP interna correspondiente para el evento de inicio de sesión desde el Conector de AD.

A continuación, Cisco Umbrella utiliza esta información para buscar la organización y determinar qué política debe aplicarse. Si no tiene ninguna política aplicada específicamente a los usuarios de AD, pero sí tiene una para las redes o los sitios, Cisco Umbrella aplica la política mediante esa identidad. Esto significa que cuando se informa de la consulta, la identidad y la respuesta en la búsqueda de actividad, la identidad que desencadenó la política de la que se informa. La otra información se sigue etiquetando en la solicitud, por lo que aún puede buscar un usuario de AD y obtener la actividad que informa de una red como la identidad. Además, si exporta los datos de búsqueda de actividad a un archivo CSV, mostrará toda la información de identidad asociada a la consulta.

Additional Information

Si todavía no ve a ningún usuario de AD, comuníquese con el Soporte técnico (umbrella-support@cisco.com), con un resultado de la prueba de diagnóstico, y cualquier registro de

auditoría del conector de AD que sea relevante.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).