¿Por qué mi POSTE de prueba no consigue actualizado en los “registros de seguridad de datos”?

Contenido

Pregunta:

¿Por qué mi petición post de la prueba no consigue actualizada en los “registros de seguridad de datos” en el dispositivo de seguridad de la red de Cisco (WSA)?

Síntomas:
Los “registros de seguridad de datos” no se están poniendo al día aunque las peticiones post se están enviando con el WSA.
El “registro del acceso” es de puesta al día y mostrando las peticiones post trabajan correctamente.

Solución:
El tamaño de la petición del POSTE, que esencialmente es la cantidad de datos que son cargados, determinaría si la petición consigue explorada por los filtros de seguridad de datos del en-cuadro o por las directivas de la prevención contra pérdidas de los datos externos (DLP)

Por abandono, WSA tiene un límite mínimo del tamaño de bytes de 4096 bytes (4K) para que el DLP accione. Este tamaño de bytes mínimo es evitar los falsos positivos de la exploración DLP pues evita las cargas como los logines del sitio web, que son pequeñas peticiones post.

Tan ninguna petición post/carga debajo del límite 4K no sería registrada en los “registros de seguridad de datos”. Sin embargo WSA procesará la petición post y registrará la transacción en el “registro del acceso”

Para DLP del en-cuadro (filtros de seguridad de datos)
Podemos cambiar el límite predeterminado de la exploración de WSA CLI usando el comando:
datasecurityconfig

Para DLP del apagado-cuadro (DLP del externo)

Podemos cambiar el límite predeterminado de la exploración de WSA CLI usando el comando:
externaldlpconfig

El valor predeterminado para ambos los comandos antedichos es 4096 bytes.