Registri eventi file di accesso sicuro mancanti da SIEM dopo la modifica della licenza

Sommario

Problema

I registri eventi file non sono più stati ricevuti dal SIEM dall'archivio AWS S3 mentre il recapito dei registri DNS ha continuato. I connettori dati Evento file visualizzano un'icona "disconnesso" nell'interfaccia SIEM. I registri non più visualizzati sono stati identificati come record di eventi file relativi a DLP/IPS. I log a livello DNS sono rimasti funzionali per tutto il periodo di emissione.

Durante la migrazione, l'ambiente utilizzava sia Umbrella che Secure Access, con registri inviati allo stesso bucket AWS. Le chiavi sono state ruotate e si è verificato che funzionano correttamente. La versione dello schema è la versione 10, mentre la versione 16 è disponibile.

Ambiente

- Organizzazione Cisco Secure Access con configurazioni Umbrella e Secure Access
- Integrazione dello storage AWS S3 per l'esportazione dei log
- Piattaforma Microsoft Sentinel SIEM
- Schema versione 10 in uso (versione 16 disponibile)
- La licenza Secure Access è cambiata da Advantage a Essentials il 23 giugno 2026
- L'ultimo registro eventi file osservato il 24 giugno 2026

Risoluzione

Dall'indagine è emerso che i registri degli eventi file erano correlati alla funzionalità DLP/IPS, che richiede specifiche funzionalità di licenza. La causa principale è stata identificata nell'analisi successiva.

Passaggio 1: Analisi del traffico

Controllare la Ricerca attività in Accesso sicuro per confermare i modelli di traffico:

1.- Passare a Ricerca attività e filtrare il traffico Web o gli eventi di smaltimento dannosi. Dall'analisi è emerso che il traffico DNS era presente, ma che non sono stati visibili eventi di traffico Web negli ultimi 30 giorni e che non sono state identificate regole con ispezione dei file abilitata.
2.- Flusso traffico > Registri nel report CSA > S3 bucket - SIEM.

Passaggio 2: Revisione della cronologia delle licenze

1.- Esaminare la cronologia delle licenze in Secure Access per identificare eventuali modifiche in linea con i tempi di interruzione del registro eventi file.

2.- Passare a Secure Access > Admin > Subscription (Accesso sicuro > Amministratore > Sottoscrizione) per visualizzare il livello di licenza corrente e il riepilogo delle funzionalità.

L'indagine ha mostrato che la licenza Secure Access è cambiata da Secure Access Advantage a Secure Access Essentials il 23 giugno 2026, in linea con il tempo in cui i registri eventi file non vengono più visualizzati.

Passaggio 3: Verifica funzionalità

Verificare le funzionalità incluse nel livello di licenza corrente. La funzionalità DLP e IPS, che genera registri eventi file, non è inclusa nel livello di licenza Secure Access Essentials.

Passaggio 4: Conferma e root cause

I tempi della modifica della licenza corrispondono perfettamente quando i registri eventi file non vengono più visualizzati. Poiché la registrazione a livello DNS rimane funzionale e costituisce il requisito principale, il caso è stato risolto con la consapevolezza che i registri eventi file non sarebbero stati disponibili con la licenza Essentials corrente.

Causa

I registri eventi file non sono più stati generati a causa di una modifica della licenza da Secure Access Advantage a Secure Access Essentials il 23 giugno 2026. I registri eventi file sono associati alle funzionalità DLP e IPS, che non sono incluse nel livello di licenza Essentials. Il downgrade della licenza ha rimosso l'accesso alle funzionalità di ispezione dei file che generano questi tipi di log specifici.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).