

La ricerca delle attività di accesso sicuro visualizza i nomi delle regole SCONOSCIUTI

Sommario

Problema

Durante una migrazione da Umbrella a SSE, gli eventi di ricerca delle attività di accesso sicuro visualizzano il nome della regola come UNKNOWN anziché le regole dei criteri con nome. Questo comportamento è stato osservato per diversi tipi di traffico, incluso il traffico consentito, ad esempio le richieste a chatgpt.com. Il problema era se queste voci dei nomi di regola SCONOSCIUTO indicavano un problema di configurazione dei criteri o di migrazione che richiedeva la risoluzione.

Ambiente

- SSE (Cisco Secure Access)
- Organizzazione in fase di migrazione da Umbrella a SSE
- Creazione di report di Ricerca attività accesso sicuro
- Traffico classificato come domini visualizzati di recente

Risoluzione

Il comportamento Nome regola UNKNOWN è previsto e normale per gli eventi gestiti dalla logica di sistema Secure Access anziché da regole create dal cliente/denominate. Ciò si verifica in genere per il traffico classificato come Nuovi domini visualizzati, in cui il dominio è stato appena visualizzato in fase di query ed è indicato come tale nei report Ricerca attività o Attività di sicurezza.

Interpretazione degli eventi di ricerca attività con nomi di regole SCONOSCIUTI

Quando si incontrano eventi con Nome regola SCONOSCIUTO, esaminare questi campi di evento per determinare il motivo dell'imposizione e confermare la corretta applicazione dei criteri:

- Azione - Mostra se il traffico è stato consentito o bloccato
- Motivo blocco eventi/Motivo blocco: fornisce dettagli di imposizione specifici
- Categorie: visualizza la categorizzazione del contenuto, ad esempio Nuovi domini visualizzati)
- Dominio/IP di destinazione - Destinazione della richiesta
- Identità utente/origine - Origine del traffico
- Timestamp - Quando si è verificato l'evento

Se nel campo Categorie viene visualizzato Nuovi domini visualizzati, SCONOSCIUTO nel campo nome regola è il comportamento previsto e non indica una migrazione non riuscita o il danneggiamento dei criteri.

Passaggi di convalida per comportamento imprevisto

Se si prevede che il traffico corrisponda a una regola denominata specifica ma viene visualizzato UNKNOWN, raccogliere le seguenti informazioni per la convalida del percorso dei criteri:

- 2-3 timestamp evento di esempio
- Dominio/IP di destinazione per ciascun evento
- Identità utente/origine per ogni evento

Queste informazioni possono essere utilizzate per confrontare il percorso dei criteri previsto con il comportamento effettivo dell'evento e determinare se sono necessarie ulteriori verifiche.

Causa

Il nome della regola UNKNOWN viene visualizzato quando la logica di sistema Secure Access elabora il traffico anziché applicare una regola dei criteri denominata/creata dal cliente. Si tratta di un comportamento documentato per alcune categorie di traffico, in particolare per i domini di nuova visualizzazione, in cui i meccanismi integrati di categorizzazione e gestione hanno la precedenza sulle regole denominate durante la valutazione iniziale del dominio.

Contenuto correlato

- [Abilita sicurezza domini appena visualizzati](#)
- [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).