

Bei der Suche nach Aktivitäten für sicheren Zugriff werden unbekannte Regelnamen angezeigt.

Inhalt

Problem

Während einer Umbrella to SSE-Migration zeigen Ereignisse zur Suche nach Aktivitäten für sicheren Zugriff den Regelnamen als UNBEKANNT an, anstatt benannte Richtlinienregeln anzuzeigen. Dieses Verhalten wurde bei verschiedenen Datenverkehrstypen beobachtet, einschließlich des zulässigen Datenverkehrs, z. B. Anfragen an chatgpt.com. Die Bedenken bezogen sich darauf, ob diese UNBEKANNTEN Regelnameneinträge auf ein Richtlinienkonfigurationsproblem oder ein Migrationsproblem hindeuteten, das behoben werden musste.

Umwelt

- Cisco Secure Access (SSE)
- Organisation, die eine Umbrella-to-SSE-Migration durchläuft
- Berichte zu Secure Access Activity Search
- Datenverkehr als neu erkannte Domänen kategorisiert

Auflösung

Das Verhalten von Regelname UNBEKANNT wird für Ereignisse, die von der Systemlogik für sicheren Zugriff behandelt werden, erwartet und ist normal, nicht für vom Kunden erstellte/benannte Regeln. Dies tritt in der Regel bei Datenverkehr auf, der als neu erkannte

Domänen kategorisiert ist, bei denen die Domäne zum Abfragezeitpunkt neu erkannt wurde und als solche in Aktivitätssuche- oder Sicherheitsaktivitätsberichten gemeldet wird.

Interpretieren von Ereignissen zur Aktivitätssuche mit unbekannten Regelnamen

Wenn Ereignisse mit Regelname UNBEKANNT auftreten, überprüfen Sie diese Ereignisfelder, um den Grund für die Durchsetzung zu ermitteln und die ordnungsgemäße Anwendung der Richtlinie zu bestätigen:

- Aktion - Zeigt an, ob Datenverkehr zugelassen oder blockiert wurde
- Grund der Ereignisblockierung/Blockierung: Details zur Durchsetzung
- Kategorien - Zeigt die Kategorisierung von Inhalten an (z. B. neu erkannte Domänen)
- Zieldomäne/IP - Ziel der Anforderung
- Benutzer-/Quellidentität - Quelle des Datenverkehrs
- Zeitstempel - Wann das Ereignis eingetreten ist

Wenn im Feld Kategorien Neu erkannte Domänen angezeigt wird, wird UNBEKANNT im Feld Regelname als Verhalten erwartet, das nicht auf eine fehlgeschlagene Migration oder eine beschädigte Richtlinie hinweist.

Validierungsschritte für unerwartetes Verhalten

Wenn erwartet wurde, dass der Datenverkehr mit einer bestimmten benannten Regel übereinstimmt, aber UNBEKANNT anzeigt, erfassen Sie diese Informationen für die Richtlinienpfadvalidierung:

- 2 bis 3 Zeitstempel für Beispielergebnisse
- Zieldomäne/IP für jedes Ereignis
- Benutzer-/Quellenidentität für jedes Ereignis

Anhand dieser Informationen kann der erwartete Richtlinienpfad mit dem tatsächlichen Ereignisverhalten verglichen werden, um festzustellen, ob weitere Untersuchungen erforderlich

sind.

Ursache

Der UNBEKANNTE Regelname wird angezeigt, wenn die Systemlogik von Secure Access den Datenverkehr verarbeitet, anstatt eine vom Kunden erstellte/benannte Richtlinienregel anzuwenden. Dies ist ein dokumentiertes Verhalten für bestimmte Datenverkehrskategorien, insbesondere für neu erkannte Domänen, bei denen die integrierten Kategorisierungs- und Verarbeitungsmechanismen bei der anfänglichen Domänenbewertung Vorrang vor benannten Regeln haben.

Verwandte Inhalte

- [Sicherheit für neu erkannte Domänen aktivieren](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.