

Zoeken naar activiteiten voor beveiligde toegang geeft ONBEKENDE regelnamen weer

Inhoud

uitgifte

Tijdens een Umbrella-naar-SSE-migratie worden de gebeurtenissen voor het zoeken naar activiteiten voor beveiligde toegang weergegeven met Regelnaam als ONBEKEND in plaats van benoemde beleidsregels. Dit gedrag werd waargenomen voor verschillende soorten verkeer, waaronder toegestaan verkeer, zoals verzoeken aan chatgpt.com. De vraag was of deze ONBEKENDE regelnaamvermeldingen een probleem met de beleidsconfiguratie of een migratieprobleem aangaven dat moest worden opgelost.

milieu

- Cisco Secure Access (SSE)
- Organisatie die overkoepelende migratie naar SSE ondergaat
- Rapportage over zoekactiviteiten voor beveiligde toegang
- Verkeer gecategoriseerd als Nieuw gezien domeinen

resolutie

De naam van de regel ONBEKEND gedrag wordt verwacht en normaal voor gebeurtenissen behandeld door Secure Access systeemlogica in plaats van door de klant gemaakte / benoemde regels. Dit komt vaak voor bij verkeer dat is gecategoriseerd als Nieuw geziene domeinen, waarbij het domein op het moment van de zoekopdracht nieuw werd gezien en als zodanig wordt gerapporteerd in activiteitenzoekopdrachten of beveiligingsactiviteitenrapporten.

Het interpreteren van zoekactiviteiten met ONBEKENDE regelnamen

Wanneer u gebeurtenissen tegenkomt met Regelnaam ONBEKEND, bekijkt u deze gebeurtenisvelden om de reden van handhaving te bepalen en de juiste beleidstoepassing te bevestigen:

- Actie - Geeft aan of verkeer is toegestaan of geblokkeerd
- Reden voor gebeurtenisblok / reden voor blokkering - Specifieke handhavingsgegevens
- Categorieën - Geeft inhoudscategorisatie weer (zoals Nieuw gezien domeinen)
- Bestemmingsdomein/IP - Doel van het verzoek
- Gebruikers-/bronidentiteit - Bron van het verkeer
- Tijdstempel - Wanneer de gebeurtenis heeft plaatsgevonden

Als het veld Categorieën Nieuw geziene domeinen weergeeft, wordt ONBEKEND in het veld Regelnaam verwacht gedrag en geeft dit geen melding van een mislukte migratie of beleidsbeschadiging.

Validatiestappen voor onverwacht gedrag

Als het verkeer naar verwachting overeenkomt met een specifieke benoemde regel, maar ONBEKEND wordt weergegeven, verzamelt u deze informatie voor de validatie van het beleidspad:

- 2-3 voorbeeldtijdstempels voor gebeurtenissen
- Bestemmingsdomein/IP voor elk evenement
- Gebruikers-/bronidentiteit voor elke gebeurtenis

Deze informatie kan worden gebruikt om het verwachte beleidspad te vergelijken met het werkelijke gebeurtenisgedrag en te bepalen of verder onderzoek nodig is.

Oorzaak

De ONBEKENDE regelnaam wordt weergegeven wanneer de systeemlogica van Secure Access verkeer verwerkt in plaats van een door de klant gemaakte/benoemde beleidsregel toe te passen. Dit is gedocumenteerd gedrag voor bepaalde verkeerscategorieën, met name nieuw geziene domeinen, waarbij de ingebouwde categorisatie- en afhandelingsmechanismen voorrang hebben op benoemde regels tijdens de eerste domeinbeoordeling.

Gerelateerde inhoud

- [Nieuw geziene domeinbeveiliging inschakelen](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.