Problemen met Active Directory-gebruikers oplossen die ontbreken in het activiteitenzoekrapport in Umbrella

Inhoud

Inleiding

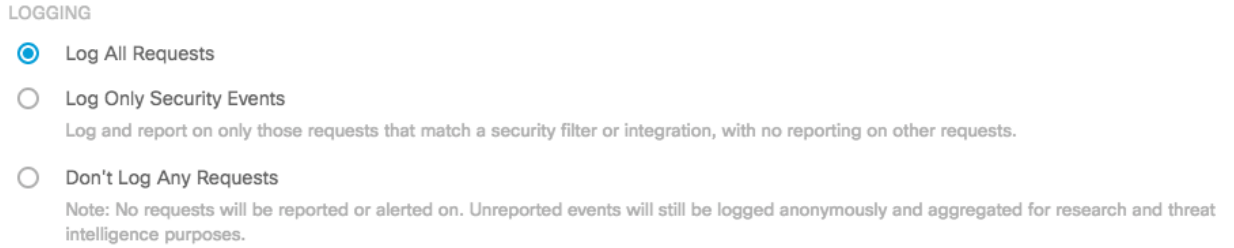
In dit document wordt het activiteitenzoekrapport in Cisco Umbrella beschreven. Het Activity Search Report is een bijna live rapport van alle DNS-zoekopdrachten die uw gebruikers maken. Als u de Cisco Umbrella Active Directory (AD)-integratie hebt ingesteld, kunt u verwachten dat uw AD-gebruikers de kolom Identiteit invullen in uw Activiteit zoeken. Er zijn echter situaties waarin de gebruikers ontbreken in de kolom Identiteit.

resolutie

Als u denkt dat u AD-gebruikers rechtstreeks in de kolom Identiteit in de Activiteit zoeken zou moeten zien, maar ze niet ziet, of er een paar ziet, maar niet zoveel als u had verwacht, zijn hier een paar dingen om te controleren:

1. Sites en Active Directory
    - Controleer al uw AD-componenten om er zeker van te zijn dat er geen fouten of problemen zijn gemeld. Als u grijze, oranje of rode statusindicatoren ziet op een van de onderdelen, verkrijgt u deze gegevens en opent u een supportticket (umbrella-support@cisco.com).
        - Diagnostische test van een getroffen gebruiker (een gebruiker die niet wordt weergegeven in de zoekopdracht Activiteit)
        - Schermafbeelding van de Virtual Appliance (VA)-console, met uitgebreide foutmeldingen
        - Controlelogboeken AD-connector
2. Logboekinstellingen
    - In de Geavanceerde instellingen van elk beleid is er een sectie onderaan die betrekking heeft op hoeveel u moet loggen. U kunt het instellen op:
        - Alle aanvragen registreren
        - Alleen beveiligingsgebeurtenissen registreren
        - Geen aanvragen registreren

- Als uw beleid momenteel is ingesteld op "Alleen beveiligingsgebeurtenissen registreren", kan dat verklaren waarom u niet zoveel zoekopdrachten ziet als u verwacht, of helemaal geen resultaten van sommige gebruikers.



3. Juiste beleidsprioriteit
    - Als u een beleid toepast op een netwerkidentiteit dat hoger is in de lijst met beleidsregels dan uw AD-gebruikersbeleid, is het beleid Netwerkidentiteit waarschijnlijk van toepassing. Dit betekent op zijn beurt dat u bij het zoeken naar activiteiten het netwerk als de gerapporteerde identiteit zult zien. Raadpleeg ook de documentatie van Cisco Umbrella over best practices en beleidsprioriteit.

Oorzaak

Waar haalt de Activity Search de "Identiteit" vandaan?

Wanneer een DNS-query in Umbrella wordt weergegeven, wordt deze informatie doorgegeven in de query, ervan uitgaande dat uw AD-integratie werkt zoals verwacht:

- Intern IP-adres
- AD Identity-hash (gebruiker, host of beide)
- IP-uitgang
- Domein wordt opgevraagd

De AD Identity Hash wordt aan de query toegevoegd door het virtuele toestel, dat deze informatie doorgeeft, en het bijbehorende interne IP-adres voor de aanmeldingsgebeurtenis vanuit de AD Connector.

Cisco Umbrella gebruikt deze informatie vervolgens om de organisatie te vinden en om te bepalen welk beleid van toepassing is. Als u geen beleid hebt dat specifiek is toegepast op uw AD-gebruikers, maar er wel een hebt voor uw netwerken of sites, past Cisco Umbrella het beleid toe met behulp van die identiteit. Dit betekent dat wanneer de query, identiteit en reactie worden gerapporteerd in de Activiteit zoeken, de Identiteit die het beleid dat wordt gerapporteerd geactiveerd. De andere informatie is nog steeds gecodeerd in het verzoek, zodat u nog steeds kunt zoeken naar een AD-gebruiker en de activiteit kunt krijgen die een netwerk rapporteert als de identiteit. Als u bovendien de gegevens voor het zoeken naar activiteiten naar een CSV-bestand exporteert, worden alle identiteitsgegevens weergegeven die aan de zoekopdracht zijn gekoppeld.

Aanvullende informatie

Als u nog steeds geen AD-gebruikers ziet, neemt u contact op met Support (umbrella-support@cisco.com), met een diagnostisch testresultaat en eventuele relevante AD Connector

Audit Logs.

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.