Status van beveiligde toegangsbescherming Inconsistenties in SSE-dashboard weergeven

Inhoud

- uitgifte
- milieu
- resolutie
  - Verificatiestappen
    - Aanvullende diagnostische verzameling
- Oorzaak
- Gerelateerde inhoud

---

uitgifte

Eindpunten die Cisco Secure Client gebruiken, geven met tussenpozen onjuiste DNS- en SWG-beveiligingsstatussen weer in het Cisco Secure Access SSE-dashboard, zelfs terwijl eindpunten actief DNS- en webverkeer genereren. De beschermingsstatusindicatoren variëren inconsistent en tonen combinaties van:

- Zowel de DNS- als SWG-beveiligingsstatus wordt weergegeven als "N/A" (- symbool)
- De ene beschermingsstatus wordt weergegeven als "N/A" terwijl de andere normaal lijkt
- Beide statussen worden weergegeven als "Offline"
- De ene status wordt weergegeven als "Offline" terwijl de andere als "N/A" wordt weergegeven

Deze statusrepresentaties lijken onnauwkeurig en komen niet overeen met de werkelijke

operationele status van de apparaten en Cisco-services die erop worden uitgevoerd. Dit vermindert de zichtbaarheid van de dekking van de endpoint-beveiliging en beïnvloedt de mogelijkheid om de beschermingsstatus op betrouwbare wijze op alle organisatorische apparaten te bewaken.

milieu

- Cisco Secure Access (SSE)-beheerportal
- Cisco Secure Client geïmplementeerd op eindpunten
- Meerdere organisatorische apparaten met agents en services geïnstalleerd en actief
- DNS- en SWG-beveiligingsservices geconfigureerd

resolutie

De aanbevolen methode om de DNS- en WEBBESCHERMINGSSTATUS nauwkeurig te controleren, is om de functionaliteit voor het zoeken naar activiteiten in het SSE-dashboard te gebruiken in plaats van alleen te vertrouwen op de beveiligingsstatusindicatoren die voor afzonderlijke apparaten worden weergegeven.

Verificatiestappen

Aanvullende diagnostische verzameling

Als inconsistente beschermingsstatusindicatoren nog steeds zorgen baren, verzamelt u deze gesynchroniseerde diagnostische uitgangen:

- Screenshot van Cisco Secure Client met WEB/DNS-beschermingsstatus met tijdstempel van systeemklok
- Screenshot van Secure Access Dashboard met beschermingsstatus met tijdstempel van

systeemklok

- DART (Diagnostic and Reporting Tool)-uitvoer verzameld van het betreffende eindpunt

Deze gesynchroniseerde diagnostiek kan helpen bij het correleren van de werkelijke beschermingsstatus met het dashboarddisplay en het identificeren van eventuele timing- of synchronisatieproblemen.

Oorzaak

De hoofdoorzaak van de inconsistente weergave van de beschermingsstatus in het SSE-dashboard werd geïdentificeerd als een verwacht gedrag. Het probleem lijkt verband te houden met de synchronisatie van de dashboardstatusindicator in plaats van de werkelijke functionaliteit van de beveiligingsservice. De aanwezigheid van DNS- en WEBACTIVITEIT in de Activiteit Zoeken bevestigt dat de beveiligingsservices correct werken ondanks de inconsistente statusweergaven.

Dit gedrag is gedocumenteerd als een verzoek om functies voor een mogelijke toekomstige verbetering van de betrouwbaarheid van de statusindicator.

Gerelateerde inhoud

- 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.