

Effectieve machtigingen om een rol toe te staan artefacten en gebeurtenissen te verwijderen

toepasbaarheid

Splunk SOAR

Beschrijving

Uitzoeken hoe u specifieke machtigingen kunt instellen om een gebruiker toe te staan alleen artefacten en gebeurtenissen te VERWIJDEREN.

onderzoek

Stappen reproduceren:

ALS BEHEERDER:

1. Ga naar ADMINISTRATIE -> GEBRUIKERSBEHEER -> ROLLEN EN MACHTIGINGEN -> Selecteer de rol "CSOC Orchestration Engineer".
2. Selecteer/schakel op het tabblad BASISBEVOEGDHEDEN het tabblad GEBEURTENISSEN VERWIJDEREN, BEWERKEN EN WEERGEVEN in
3. Selecteer/schakel op het tabblad LABELBEVOEGDHEDEN de optie VERWIJDEREN, BEWERKEN EN WEERGEVEN in voor elk label waarvan ik wil dat de gebruiker artefacten en gebeurtenissen kan verwijderen.
4. Sla de wijzigingen op
5. Meld u aan als de door mij genoemde accountgebruiker en maak een gebeurtenis met een label waarop ik de rechten moet verwijderen.
6. Voeg een artefact toe met een paar waarden erin.
7. Probeer nu datzelfde artefact te verwijderen dat ik zojuist heb gemaakt en de knop VERWIJDEREN is grijs.
8. Probeer nu dezelfde gebeurtenis te verwijderen die ik zojuist heb gemaakt en de knop VERWIJDEREN is grijs.

Het lijkt erop dat er iets ontbreekt in de rol permissies.

De documentatie is niet zo gedetailleerd, dus we kunnen niet uitleggen wat er ontbreekt.

Problemen oplossen:

1. Probeer de browser te vernieuwen.

2. Probeerde een nieuw lokaal account aan te maken met een nieuwe rol met dezelfde toestemming.

- Een nieuw lokaal account gemaakt met de naam TEST1
- Vervolgens voegde de CSOC ORCHESTRATOR-rol toe aan de TEST1-gebruiker en kon de gebruiker artefacten of gebeurtenissen niet verwijderen.
- Een nieuwe rol gemaakt, TEST1ROLE genaamd
- Stel de rechten van de TEST1ROLE in op exact hetzelfde als de rol van CSOC ORCHESTRATOR.
- De gebruiker kon artefacten en gebeurtenissen verwijderen.
- De gebruikersrol van de TEST1 is teruggezet in CSOC ORCHESTRATOR en de gebruiker kan artefacten of gebeurtenissen niet verwijderen.
- Dus dit soort zinspelen op een parsing / handhaving probleem met de bestaande CSOC ORCHESTRATOR rol, om een of andere reden.

3. Controleer de rest-API voor beide rollen:

```
https://<phantom_ip>/rest/role/<TEST1ROLE_ID>  
https://<phantom_ip>/rest/role/<CSOC_ORCHESTRATOR_ID>
```

Om de rol-ID te krijgen, is het het gemakkelijkst om naar die specifieke rolconfiguratie te gaan en in de URL vindt u het gehele getal aan het einde van het URL-pad. Dat is de rol-ID.

Anders kunt u alle rollen met `https://<phantom_ip>/rest/role` aanbieden, hier vindt u de id in het JSON-bestand voor elke rol.

Controleer of er een verschil is in de configuratie van het JSON-bestand.

4. Lijkt erop dat de CSOC Orchestrator Role JSON output iets groter is.

5. Er is een configuratie in CSOC Orchestrator Role waarbij de huurder nabCERT CSOC de verwijdering weigert. Dit is het probleem dat de gebruiker niet mag verwijderen.

```
{  
  "execute": "deny",  
  "name": "tenant",  
  "extra": "nabCERT CSOC",  
  "edit": "allow",  
  "object_id": 1,  
  "role": 8,  
  "content_type": 20,  
  "delete": "deny",  
  "id": 66,  
  "view": "allow"  
}
```

resolutie

Wijzig de rol van de CSOC Orchestration Engineer om de nabCERT CSOC-rol te kunnen weigeren:

```
{
  "execute": "deny",
  "name": "tenant",
  "extra": "nabCERT CSOC",
  "edit": "allow",
  "object_id": 1,
  "role": 8,
  "content_type": 20,
  "delete": "allow",
  "id": 66,
  "view": "allow"
}
```

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.