

# Autorisations effectives pour autoriser un rôle à supprimer des artefacts et des événements

## Applicabilité

Splunk SOAR

## Description

Découvrez comment définir des autorisations spécifiques pour autoriser un utilisateur à SUPPRIMER uniquement les artefacts et les événements.

## Enquête

Étapes à reproduire :

AS ADMIN :

1. Accédez à ADMINISTRATION -> GESTION DES UTILISATEURS -> RÔLES ET AUTORISATIONS -> Sélectionnez le rôle « Ingénieur d'orchestration CSOC ».
2. Dans l'onglet AUTORISATIONS DE BASE, sélectionnez/activez EVÉNEMENTS SUPPRIMER, MODIFIER ET AFFICHER
3. Dans l'onglet AUTORISATIONS D'ÉTIQUETTE, sélectionnez/activez SUPPRIMER, MODIFIER ET AFFICHER pour chaque étiquette dont je souhaite que l'utilisateur puisse supprimer des artefacts et des événements.
4. Sauvegardez les modifications
5. CONNECTEZ-vous en tant qu'utilisateur de mon compte nommé et créez un événement avec une étiquette sur laquelle je dispose de privilèges de suppression.
6. Ajoutez un artefact contenant quelques valeurs.
7. Maintenant, essayez de supprimer ce même artefact que je viens de créer et le bouton DELETE est grisé.
8. Maintenant, essayez de supprimer ce même événement que je viens de créer et le bouton DELETE est grisé.

Il semble qu'il manque quelque chose dans les autorisations de rôle.

La documentation n'étant pas très détaillée, nous ne sommes pas en mesure d'expliquer ce qui manque.

Dépannage :

1. Tentative d'actualisation du navigateur.

2. Tentative de création d'un nouveau compte local avec un nouveau rôle utilisant la même autorisation.

- Création d'un nouveau compte local appelé TEST1
- Ensuite, il a ajouté le rôle CSOC ORCHESTRATOR à l'utilisateur TEST1 et il n'a pas pu supprimer des artefacts ou des événements.
- Création d'un nouveau rôle appelé TEST1ROLE
- Définissez les autorisations du rôle TEST1ROLE de manière à ce qu'elles soient exactement identiques à celles du rôle CSOC ORCHESTRATOR.
- L'utilisateur a pu supprimer des artefacts et des événements.
- Le rôle d'utilisateur TEST1 est redevenu CSOC ORCHESTRATOR et l'utilisateur n'a pas pu supprimer des artefacts ou des événements.
- Ainsi, ce type de conseils à un problème d'analyse/application avec le rôle d'ORCHESTRATEUR CSOC existant, pour une raison quelconque.

3. Pour vérifier l'API restante pour les deux rôles :

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

Pour obtenir l'ID de rôle, le plus simple est d'accéder à cette configuration de rôle particulière et dans l'URL, vous trouverez le nombre entier à la fin du chemin d'accès à l'URL. Il s'agit de l'ID de rôle.

Sinon, vous pouvez lister tous les rôles avec `https://<phantom_ip>/rest/role`, où vous trouverez l'id dans le fichier JSON pour chaque rôle.

Vérifiez s'il existe une différence dans la configuration du fichier JSON.

4. Il semble que la sortie JSON du rôle CSOC Orchestrator soit un peu plus grande.

5. Le rôle CSOC Orchestrator comporte une configuration dans laquelle le CSOC nabCERT du locataire refuse la suppression. Il s'agit du problème qui empêche l'utilisateur de supprimer.

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

```
"view": "allow"
}
```

## Résolution

Modifiez le rôle d'ingénieur d'orchestration CSOC pour autoriser le refus pour le rôle CSOC nabCERT :

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.