

# Permisos efectivos para permitir que una función elimine artefactos y eventos

## Aplicabilidad

Splunk SOAR

## Descripción

Averiguar cómo establecer permisos específicos para permitir que un usuario ELIMINE sólo artefactos y eventos.

## Investigación

Reproducción de pasos:

COMO ADMINISTRADOR:

1. Vaya a ADMINISTRATION -> USER MANAGEMENT -> ROLES AND PERMISSIONS -> Select "CSOC Orchestration Engineer" role.
2. En la ficha PERMISOS BÁSICOS, seleccione/active los eventos ELIMINAR, EDITAR Y VER
3. En la ficha PERMISOS DE ETIQUETA, seleccione/active SUPRIMIR, EDITAR Y VER para cada etiqueta en la que desee que el usuario pueda suprimir artefactos y eventos.
4. Guarde los cambios
5. INICIE SESIÓN como usuario de mi cuenta con nombre y cree un evento con una etiqueta en la que tenga permisos de eliminación.
6. Añada un artefacto con algunos valores.
7. Ahora intente borrar ese mismo artefacto que acabo de crear y el botón de BORRAR está atenuado.
8. Ahora intente eliminar el mismo evento que acabo de crear y el botón SUPRIMIR aparece atenuado.

Parece que falta algo en los permisos de la función.

La documentación no es tan detallada, por lo que no podemos explicar lo que falta.

Resolución de problemas:

1. Se ha intentado actualizar el explorador.
2. Se ha intentado crear una nueva cuenta local con una nueva función utilizando el mismo

permiso.

- Se creó una nueva cuenta local denominada TEST1
- A continuación, se añadió la función CSOC ORCHESTRATOR al usuario TEST1 y el usuario no pudo eliminar artefactos ni eventos.
- Se ha creado una nueva función denominada TEST1ROLE
- Establezca los permisos de TEST1ROLE para que sean exactamente los mismos que los de CSOC ORCHESTRATOR.
- El usuario ha podido eliminar artefactos y eventos.
- Se ha vuelto a cambiar la función de usuario de TEST1 a CSOC ORCHESTRATOR y el usuario no ha podido eliminar artefactos o eventos.
- Por lo tanto, este tipo de sugerencias apuntan a un problema de análisis/aplicación con la función existente de CSOC ORCHESTRATOR, por alguna razón.

3. Para comprobar el resto de la API para ambos roles:

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

Para obtener el ID de rol, lo más fácil es ir a esa configuración de rol en particular y en la URL encontrará el número entero al final de la ruta de URL. Este es el ID de rol.

De lo contrario, puede enumerar todos los roles con `https://<phantom_ip>/rest/role`, donde encontrará la ID en el archivo JSON para cada rol.

Compruebe si hay alguna diferencia en la configuración del archivo JSON.

4. Parece que el resultado de CSOC Orchestrator Role JSON es un poco más grande.

5. Existe una configuración en CSOC Orchestrator Role en la que el arrendatario nabCERT CSOC deniega la supresión. Este es el problema que no permite al usuario eliminar.

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

# Resolución

Cambie el rol de ingeniero de orquestación CSOC para permitir la denegación del rol 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"
}
```

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).