

Effektive Berechtigungen zum Zulassen des Löschens von Artefakten und Ereignissen durch eine Rolle

Geltungsbereich

Splunk SOAR

Beschreibung

Erfahren Sie, wie Sie bestimmte Berechtigungen festlegen, damit ein Benutzer nur Artefakte und Ereignisse LÖSCHEN kann.

Untersuchung

Schritte reproduzieren:

AS-ADMIN:

1. Gehen Sie zu ADMINISTRATION -> USER MANAGEMENT -> ROLES AND PERMISSIONS -> wählen Sie die Rolle "CSOC Orchestration Engineer".
2. Wählen/aktivieren Sie auf der Registerkarte GRUNDBERECHTIGUNGEN die Optionen EREIGNISSE LÖSCHEN, BEARBEITEN UND ANZEIGEN.
3. Wählen Sie auf der Registerkarte LABEL PERMISSIONS (LABEL-BERECHTIGUNGEN) für jedes Label die Optionen DELETE (LÖSCHEN), EDIT (BEARBEITEN) UND VIEW (ANZEIGEN) aus, aus denen der Benutzer Artefakte und Ereignisse löschen kann.
4. Speichern Sie die Änderungen
5. MELDEN SIE SICH ALS BENANNTER KONTOBENUTZER AN, und erstellen Sie ein Ereignis mit einer Bezeichnung, auf der ich die Berechtigungen zum Löschen habe.
6. Fügen Sie ein Artefakt mit einigen Werten hinzu.
7. Versuchen Sie nun, das gleiche Artefakt zu löschen, das ich gerade erstellt habe, und die Schaltfläche LÖSCHEN ist ausgegraut.
8. Versuchen Sie nun, genau das Ereignis zu löschen, das ich gerade erstellt habe, und die Schaltfläche Löschen ist abgeblendet.

Es scheint, dass in den Rollenberechtigungen etwas fehlt.

Die Dokumentation ist nicht so detailliert, sodass wir nicht erklären können, was fehlt.

Fehlerbehebung:

1. Versuchte, den Browser zu aktualisieren.

2. Es wurde versucht, mit derselben Berechtigung ein neues lokales Konto mit einer neuen Rolle zu erstellen.

- Neues lokales Konto mit dem Namen TEST1 erstellt
- Anschließend wurde dem Benutzer TEST1 die Rolle CSOC ORCHESTRATOR hinzugefügt, und der Benutzer konnte keine Artefakte oder Ereignisse löschen.
- Neue Rolle mit dem Namen TEST1ROLE erstellt
- Legen Sie fest, dass die Berechtigungen für TEST1ROLE genau mit der Rolle CSOC ORCHESTRATOR übereinstimmen.
- Der Benutzer konnte Artefakte und Ereignisse löschen.
- Benutzerrolle "TEST1" wieder in CSOC ORCHESTRATOR geändert, und der Benutzer konnte keine Artefakte oder Ereignisse löschen.
- Diese Art von Hinweisen deutet auf ein Parsing-/Durchsetzungsproblem mit der vorhandenen CSOC ORCHESTRATOR-Rolle hin.

3. So überprüfen Sie die restlichen APIs für beide Rollen:

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

Um die Rollen-ID abzurufen, gehen Sie am einfachsten zu der jeweiligen Rollenkonfiguration, und in der URL finden Sie die ganze Zahl am Ende des URL-Pfads. Das ist die Rollen-ID.

Andernfalls können Sie alle Rollen mit `https://<phantom_ip>/rest/role` auflisten. Hier finden Sie die ID für jede Rolle in der JSON-Datei.

Überprüfen Sie, ob es einen Unterschied in der JSON-Dateikonfiguration gibt.

4. Die JSON-Ausgabe der CSOC Orchestrator-Rolle ist anscheinend etwas größer.

5. Es gibt eine Konfiguration in der CSOC-Orchestrator-Rolle, bei der der Tenant nabCERT CSOC den Löschvorgang verweigert. Das Problem besteht darin, dass der Benutzer das Löschen nicht zulassen kann.

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

```
"id": 66,  
"view": "allow"  
}
```

Auflösung

Ändern Sie die Rolle des CSOC-Orchestrierungstechnikers, um die Ablehnung der NabCERT-CSOC-Rolle zuzulassen:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.