

Autorizzazioni valide per consentire a un ruolo di eliminare elementi ed eventi

Applicabilità

Splunk SOAR

Descrizione

Informazioni su come impostare autorizzazioni specifiche per consentire a un utente di eliminare solo elementi ed eventi.

Indagine

Passi Riproduzione:

AS ADMIN:

1. Accedere ad AMMINISTRAZIONE -> GESTIONE UTENTI -> RUOLI E AUTORIZZAZIONI -> Selezionare il ruolo "CSOC Orchestration Engineer".
2. Nella scheda AUTORIZZAZIONI DI BASE, selezionare/abilitare gli EVENTI DELETE, EDIT E VIEW
3. Nella scheda AUTORIZZAZIONI ETICHETTA, selezionare/abilitare DELETE, EDIT AND VIEW per ogni etichetta da cui si desidera che l'utente possa eliminare artifact ed eventi.
4. Salvare le modifiche
5. ACCEDI come utente con account denominato e crea un evento con un'etichetta su cui eliminare i perm.
6. Aggiungere un artifact contenente alcuni valori.
7. Tentare ora di eliminare lo stesso artifact appena creato e il pulsante ELIMINA è disattivato.
8. Tentare ora di eliminare lo stesso evento che ho appena creato e il pulsante ELIMINA è disattivato.

Sembra che manchi qualcosa nelle autorizzazioni del ruolo.

La documentazione non è molto dettagliata, quindi non siamo in grado di spiegare cosa manca.

Risoluzione dei problemi:

1. Tentativo di aggiornare il browser.
2. Tentativo di creare un nuovo account locale con un nuovo ruolo utilizzando la stessa

autorizzazione.

- È stato creato un nuovo account locale denominato TEST1
- Il ruolo CSOC ORCHESTRATOR è stato quindi aggiunto all'utente TEST1 e non è stato possibile eliminare elementi o eventi.
- È stato creato un nuovo ruolo denominato TEST1ROLE
- Impostare le autorizzazioni di TEST1ROLE in modo che siano esattamente uguali a quelle del ruolo ORCHESTRATOR CSOC.
- L'utente è riuscito a eliminare elementi ed eventi.
- Il ruolo utente TEST1 è stato nuovamente modificato in CSOC ORCHESTRATOR e l'utente non ha potuto eliminare gli elementi o gli eventi.
- Questo tipo di indizi suggerisce un problema di analisi/imposizione con l'esistente ruolo di ORCHESTRATOR CSOC, per qualche ragione.

3. Per controllare l'API rest per entrambi i ruoli:

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

Per ottenere l'ID ruolo, la soluzione più semplice consiste nel passare alla configurazione del ruolo specifica e nell'URL è possibile trovare il numero intero alla fine del percorso URL. Questo è l'ID ruolo.

In caso contrario, è possibile elencare tutti i ruoli con `https://<phantom_ip>/rest/role`, dove è possibile trovare l'ID nel file JSON per ogni ruolo.

Verificare se ci sono differenze nella configurazione del file JSON.

4. Sembra che l'output JSON del ruolo Orchestrator CSOC sia un po' più grande.

5. In CSOC Orchestrator Role è presente una configurazione in cui il tenant nabCERT CSOC nega l'eliminazione. Questo è il problema che non consente all'utente di eliminare.

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

Risoluzione

Modificare il ruolo di ingegnere dell'orchestrazione CSOC per consentire la negazione del ruolo 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"
}
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).