

ロールがアーティファクトとイベントを削除できるようにする有効な権限

適用性

Splunk SOAR (急増)

説明

ユーザーがアーチファクトとイベントのみをDELETEできるように特定の権限を設定する方法を調べます。

調査

手順の再現：

ADMINとして：

1. [管理] -> [ユーザー管理] -> [役割とアクセス許可] -> [CSOCオーケストレーションエンジニアロール]を選択します。
2. 「基本アクセス権」タブで、「イベント」「削除」、「編集」および「表示」を選択または使用可能にします。
3. 「ラベル権限」タブで、ユーザーがアーチファクトおよびイベントを削除できる各ラベルについて、「削除」、「編集」および「表示」を選択または使用可能にします。
4. 変更を保存します
5. 指名アカウントユーザとしてログインし、削除権限が付与されているラベルを使用してイベントを作成します。
6. 少数の値を持つアーチファクトを追加します。
7. 作成した同じアーティファクトを削除しようとする、「削除」ボタンがグレー表示されます。
8. 作成した同じイベントを削除しようとする、「削除」ボタンがグレー表示されます。

ロール権限に何か足りない項目があるようです。

ドキュメントはそれほど詳細ではないので、不足しているものを説明することはできません。

トラブルシューティング：

1. ブラウザーを更新しようとしました。
2. 同じ権限を使用して、新しいロールで新しいローカルアカウントを作成しようとしました。

- TEST1という名前の新しいローカルアカウントを作成しました。
- 次に、CSOC ORCHESTRATORロールをTEST1ユーザに追加したところ、ユーザはアーティファクトまたはイベントを削除できませんでした。
- TEST1ROLEという名前の新しいロールを作成しました。
- TEST1ROLEの権限を、CSOC ORCHESTRATORロールとまったく同じになるように設定します。
- ユーザーは成果物とイベントを削除できました。
- TEST1ユーザロールをCSOC ORCHESTRATORに戻したため、ユーザはアーティファクトまたはイベントを削除できませんでした。
- この種のヒントは、何らかの理由で、既存のCSOC ORCHESTRATORロールの解析/適用の問題に関するものです。

3. 両方のロールのrest APIを確認するには、次の手順に従います。

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

ロールIDを取得する最も簡単な方法は、その特定のロール設定に移動することです。URLでは、URLパスの最後に整数の番号が表示されます。これがロールIDです。それ以外の場合は、https://<phantom_ip>/rest/roleを使用してすべてのロールを一覧表示できます。ここでは、各ロールのJSONファイルでIDを確認できます。

JSONファイルの設定に違いがあるかどうかを確認します。

4. CSOC Orchestrator Role JSONの出力が少し大きいように見えます。

5. CSOCオーケストレータロールに、テナントnabCERT CSOCが削除を拒否する設定があります。これは、ユーザが削除できない問題です。

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

解決方法

CSOCオーケストレーションエンジニアロールを変更して、nabCERT CSOCロールの拒否を許可します。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。