

Permissões efetivas para permitir que uma função exclua artefatos e eventos

Aplicabilidade

Splunk SOAR

Descrição

Descobrimos como definir permissões específicas para permitir que um usuário EXCLUA somente artefatos e eventos.

Investigação

Etapas Reproduzir:

COMO ADMIN:

1. Vá para ADMINISTRATION -> USER MANAGEMENT -> ROLES AND PERMISSIONS -> Selecione a função "CSOC Orchestration Engineer".
2. Na guia PERMISSÕES BÁSICAS, selecione/ative os eventos DELETAR, EDITAR E EXIBIR
3. Na guia PERMISSÕES DE LABEL, selecione/ative DELETE, EDIT AND VIEW para cada label do qual eu quiser que o usuário possa deletar artefatos e eventos.
4. Salve as alterações
5. EFETUE LOGIN como meu usuário de conta nomeado e crie um evento com um rótulo no qual eu tenha permissões de deleção.
6. Adicione um artefato com alguns valores.
7. Agora, tente excluir o mesmo artefato que acabei de criar e o botão EXCLUIR ficará esmaecido.
8. Agora, tente deletar o mesmo evento que acabei de criar e o botão DELETAR ficará esmaecido.

Parece que há algo faltando nas permissões da função.

A documentação não é tão detalhada, então não podemos explicar o que está faltando.

Troubleshooting:

1. Tentativa de atualizar o navegador.
2. Tentativa de criar uma nova conta local com uma nova função usando a mesma permissão.

- Criada uma nova conta local chamada TEST1
- Em seguida, adicionou a função ORQUESTRADOR CSOC ao usuário TEST1, e o usuário não pôde excluir artefatos ou eventos.
- Uma nova função foi criada chamada TEST1ROLE
- Defina as permissões de TEST1ROLE para serem exatamente as mesmas que a função ORQUESTRADOR CSOC.
- O usuário conseguiu excluir artefatos e eventos.
- A função de usuário TEST1 foi alterada de volta para CSOC ORCHESTRATOR e o usuário não pôde excluir artefatos ou eventos.
- Por algum motivo, esse tipo de sugestão aponta para um problema de análise/aplicação com a função ORQUESTRADOR CSOC existente.

3. Para verificar a API restante para ambas as funções:

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

Para obter o ID da função, o mais fácil é ir para essa configuração de função específica e, no URL, você encontrará o número inteiro no final do caminho do URL. Essa é a ID da função. Caso contrário, você pode listar todas as Funções com `https://<phantom_ip>/rest/role`, onde você encontrará a ID no arquivo JSON para cada função.

Veja se há alguma diferença na configuração do arquivo JSON.

4. Parece que a saída JSON da Função do Orquestrador CSOC é um pouco maior.

5. Há uma configuração na Função do CSOC Orchestrator em que o locatário nabCERT CSOC nega a exclusão. Esse é o problema que impede o usuário de excluir.

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

Resolução

Altere a Função de Engenheiro de Orquestração do CSOC para permitir deny para a função de 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"
}
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.