[SOC] Splunk

- [Splunk] SPL

[Splunk] SPL

Introduction

Le SPL est le langage de requête propriétaire à Splunk. Il est extrêmement puissant mais utilise une syntaxe peu triviale.



Cheat-sheet

Index

Pour chercher dans un index :

```
index="main"
```

Opérateurs

Opérateurs
=
!=

>
>=
<
<=

Supprimer un champ de l'affichage

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | fields - User
```

Créer un tableau

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | table _time, host, Image
```

> Ici un tableau sera affiché avec trois colonnes : _time, host et Image.

Renommer un champ

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | rename Image as Process
```

Supprimer les doublons

Vous pouvez supprimer les doublons en vous basant sur un champ :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | dedup Image
```

> Ici, si un même process apparaît plusieurs fois dans les logs, il n'y aura quand même qu'un seul résultat affiché.

Trier

Par exemple pour trier dans le temps :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | sort - _time
```

Statistiques

Pour avoir des statistiques, par exemple le **count** :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=3 | stats count by _time, Image
```

Graphiques

Vous pouvez faire une visualisation avec le mot clé **chart** :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=3 | chart count by _time, Image
```

Eval

Pour effectuer des opérations basiques comme mettre en minuscule un champ :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | eval Process_Path=lower(Image)
```

Regex

Pour effectuer une regex :

```
index="main" EventCode=4662 | rex max_match=0 "[^%](?<guid>{.*})" | table guid
```

Lookup table

Après avoir importé votre CSV dans Splunk, vous pouvez effectuer des vérifications pour ajouter un champ :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | rex field=Image
"(?P<filename>[^\\\]+)$" | eval filename=lower(filename) | lookup malware_lookup.csv filename
OUTPUTNEW is_malware | table filename, is_malware
```

Time range

```
index="main" earliest=-7d latest=-1d EventCode!=1
```

Transaction

Permet de regrouper plusieurs events qui partagent un champ commun :

```
index="main" sourcetype="WinEventLog:Sysmon" (EventCode=1 OR EventCode=3) | transaction Image
startswith=eval(EventCode=1) endswith=eval(EventCode=3) maxspan=1m | table Image |  dedup
Image
```

> Le**maxspan** sert à spécifier une fenêtre de temps maximale entre les deux events.

Subsearches

Permet de faire une sous-recherche comme filtre dans sa requête :

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 NOT [ search index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 | top limit=100 Image | fields Image ] | table _time, Image, CommandLine, User, ComputerName
```

Eventcount

Pour obtenir le nombre d'events de votre query :

```
| eventcount summarize=false index=* | table index
```

Metadata

```
| metadata type=sourcetypes
```

Sourcetype

Filtrer par sourcetype permet d'augmenter les performances de la query :

```
sourcetype="WinEventLog:Security" | table _raw
```

Fieldsummary

Pour avoir un récapitulatif de statistiques :

```
sourcetype="WinEventLog:Security" | fieldsummary
```