TP Nushell

Commandes

Pour chercher des informations dans notre fichier, on peut utiliser la commande suivante:

```
open eve.json | find info_qul-oncherche --columns [colone]
```

L'option --columns permet de chercher dans un colonne spécifique de notre ficher.

Pour voir les collones présentent du tableau, on fait :

```
open eve.json | columns
```

La commande suivante nous permet de pouvoir visualiser la signature des paquets:

```
open eve.json | flatten --all | default 'nothing' signature | select signature
| group-by signature
```

Pour filtrer les informations que nous a sortie la commande précédente:

```
open eve.json |flatten --all| default 'nothing' signature |where signature ==
"ET MALWARE DNS Reply Sinkhole - Microsoft - 199.2.137.0/24"| select src_ip
dest_ip timestamp src_port dest_port proto | to csv | save -f eve.csv
```

Voici les 5 premières sorties:

```
╭───┬──────────────┬──────────────┬──────────────────────────────────┬──────────┬─
│ # │    src_ip    │    dest_ip   │            timestamp             │ src_port │ d
├───┼──────────────┼──────────────┼──────────────────────────────────┼──────────┼─
│ 0 │ 200.51.43.5  │ 192.168.1.247 │ 2024-05-07T23:01:01.346692+0200 │       53 │
│ 1 │ 200.51.43.5  │ 192.168.1.247 │ 2024-05-07T23:01:01.348949+0200 │       53 │
│ 2 │ 200.51.43.5  │ 192.168.1.247 │ 2024-05-07T23:01:01.350065+0200 │       53 │
│ 3 │ 200.51.43.5  │ 192.168.1.247 │ 2024-05-07T23:01:01.394828+0200 │       53 │
│ 4 │ 200.51.43.5  │ 192.168.1.247 │ 2024-05-07T23:01:01.396064+0200 │       53 │
│ 5 │ 200.51.43.5  │ 192.168.1.243 │ 2024-05-07T23:01:01.877646+0200 │       53 │
╰───┴──────────────┴──────────────┴──────────────────────────────────┴──────────┴─
```