

Installation et utilisation de Chainsaw et Hayabusa avec nos logs OpenWEC

Chainsaw

On installe chainsaw avec les commandes :

```
apt update
apt upgrade && apt install sudo git cargo curl -y
git clone https://github.com/countercept/chainsaw.git
cd chainsaw
curl https://sh.rustup.rs -sSf | sh -y
source "$HOME/.cargo/env"
cargo build --release
cd target/release
cp ./chainsaw /usr/local/bin
```

On y copie ensuite les règles Sigma ainsi que les fichiers EVTX témoins :

```
mkdir chainsaw_workdir
cd chainsaw_workdir
git clone https://github.com/countercept/chainsaw.git
git clone https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.git
git clone https://github.com/SigmaHQ/sigma.git
```

Maintenant qu'on tape la commande, on a bien :

```
root@chainsaw:/chainsaw/chainsaw_workdir# chainsaw --version
chainsaw 2.8.1
```

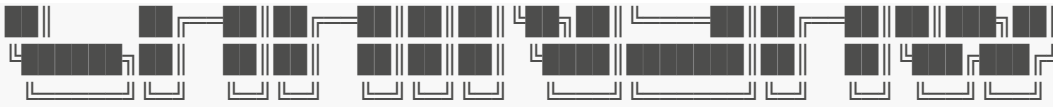
On change nos evenements OpenWEC en xml avec la programme python xml2evtx :

```
root@chainsaw:/home/xml2evtx# python3 xml2evtx.py -x event.xml
2023-12-10 21:16:34 - INFO - start create EVTX.
2023-12-10 21:16:34 - INFO - read event.xml
2023-12-10 21:16:34 - INFO - finised chunk 0.
2023-12-10 21:16:34 - INFO - total event log is 1.
2023-12-10 21:16:34 - INFO - created event.xml.evtx.
```

On utilise maintenant chainsaw sur ce dernier avec la commande :

```
root@chainsaw:/chainsaw/chainsaw_workdir# chainsaw hunt
/home/xml2evtx/event.xml.evtx -s sigma/ --mapping chainsaw/mappings/sigma-
event-logs-all.yml
```





By WithSecure Countercept (@FranticTyping, @AlexKornitzer)

```
[+] Loading detection rules from: sigma/
[!] Loaded 3123 detection rules (375 not loaded)
[+] Loading forensic artefacts from: /home/xml2evtx/event.xml.evtx
(extensions: .evtx, .evt)
[+] Loaded 1 forensic artefacts (69.6 KB)
[+] Hunting: [=====] 1/1
[+] 0 Detections found on 0 documents
root@chainsaw:/chainsaw/chainsaw_workdir#
```

On constate qu'il n'a rien trouvé, ce qui est logique car on a utilisé un seul fichier evtx ce qui restreint l'analyse de logs. J'en ai utilisé qu'un seul car la structure des logs OpenWEC ne rendent pas la manipulation du fichier facile, et j'ai donc essayer d'adapter un fichier de log a l'utilitaire xml2evtx.

Hayabusa


On installe Hayabusa avec :

```
sudo apt install musl-tools libssl-dev -y
rustup install stable-x86_64-unknown-linux-musl
rustup target add x86_64-unknown-linux-musl
git clone https://github.com/Yamato-Security/hayabusa.git --recursive
cd hayabusa
cargo build --release --target=x86_64-unknown-linux-musl
cp ./target/x86_64-unknown-linux-musl/release/hayabusa
/usr/local/bin/hayabusa
chmod +x /usr/local/bin/hayabusa
```

Étant donné qu'on a peu de fichier EVTxs les rapports ne sont pas trop impressionnants, or on sent que c'est un outil qui nous permettrait d'avoir de bons rapports d'incient sur toute une infrastrucutre avec plus de temps. Quelques tests fait :

Métrique des événements les plus courants


```
root@chainsaw:/chainsaw/chainsaw_workdir/hayabusa# hayabusa eid-metrics -d /home/xml2evtx/ -o top.csv
```



```
Generating Event ID Metrics
Start time: 2023/12/10 21:50
Total event log files: 2
Total file size: 139.3 KB
Loading detection rules. Please wait.
[00:00:00] 2 / 2  [=====] 100%
Scanning finished. Please wait while the results are being saved.
Total Event Records: 2
First Timestamp: 2015-11-12 00:24:35.079 +00:00
Last Timestamp: 2023-11-29 14:54:57.887 +00:00
Saved results: top.csv (84 B)
Elapsed time: 00:00:04.444
root@chainsaw:/chainsaw/chainsaw_workdir/hayabusa# cat top.csv
Total,%,Channel,ID,Event
1,50.0%,Sec,4624,Logon success
1,50.0%,TaskSch,129,Unknown
```

Nombre d'évenements recensés

```
root@chainsaw:/chainsaw/chainsaw_workdir/hayabusa# hayabusa computer-metrics -d /home/xml2evtx/
```



```
Start time: 2023/12/10 21:44
Total event log files: 2
Total file size: 139.3 KB
Loading detection rules. Please wait.
[00:00:00] 2 / 2  [=====] 100%
Scanning finished. Please wait while the results are being saved.
```

Computer	Events
WIN-GG82ULGC9GO	1
kingslanding.sevenkingdoms.local	1

```
Total computers: 2
Elapsed time: 00:00:04.741
```

Historique de login sur les machines :

```
root@chainsaw:/chainsaw/chainsaw_workdir/hayabusa# hayabusa logon-summary -d /home/xml2evtx/

HAYABUSA
by Yamato Security

Generating Logon Summary

Start time: 2023/12/10 21:45

Total event log files: 2
Total file size: 139.3 KB

Loading detection rules. Please wait.

[00:00:00] 2 / 2  [=====] 100%

Scanning finished. Please wait while the results are being saved.

Total Event Records: 2

First Timestamp: 2015-11-12 00:24:35.079 +00:00
Last Timestamp: 2023-11-29 14:54:57.887 +00:00

Logon Summary:

Successful Logons:


| Successful | Target Account | Target Computer | Logon Type      | Source Computer | Source IP Address |
|------------|----------------|-----------------|-----------------|-----------------|-------------------|
| 1          | Administrator  | WIN-GG82ULGC9G0 | 2 - Interactive | WIN-GG82ULGC9G0 | 127.0.0.1         |



Failed Logons:
No logon failed events were detected.

Elapsed time: 00:00:04.471
```