Crowdsec

Installation

- https://docs.crowdsec.net/docs/getting_started/install_crowdsec/

Accès à la console

- https://app.crowdsec.net/

Commandes utiles

Lister les décisions locales

```
cscli decisions
list
       Wed Apr  5 15:28:48 2023


+----+----------+-----------------------------------------+-----------------------------------+--------+---------
+--------------------------------------------------+--------+-------------------+----------+
| ID |  Source  |              Scope:Value                |              Reason               | Action | Country |
AS                     | Events |     expiration     | Alert ID |
+----+----------+-----------------------------------------+-----------------------------------+--------+---------
+--------------------------------------------------+--------+-------------------+----------+
| 18 | crowdsec | Ip:2a01:cb00:8906:7e00:5401:1966:20ac:69ad | crowdsecurity/http-crawl-non_statics | ban    |
FR      | 3215 Orange                              | 89     | 3h59m43.090461234s | 18       |
| 17 | crowdsec | Ip:92.175.107.123                       | crowdsecurity/http-crawl-non_statics | ban    | FR      | 3215
Orange                                | 49     | 3h59m13.25235483s  | 17       |
| 16 | crowdsec | Ip:79.81.205.138                        | crowdsecurity/http-crawl-non_statics | ban    | FR      | 15557
Societe Francaise Du Radiotelephone - SFR SA | 66     | 3h54m44.194349115s | 16       |
| 15 | crowdsec | Ip:212.23.165.14                        | crowdsecurity/http-crawl-non_statics | ban    | FR      | 12566
```

```
Societe Francaise Du Radiotelephone - SFR SA | 46     | 3h52m52.665948387s | 15        |
| 14 | crowdsec | Ip:83.206.19.140                          | crowdsecurity/http-crawl-non_statics | ban    | FR      | 3215
Orange                                          | 43     | 3h52m47.901151072s | 14        |
| 13 | crowdsec | Ip:84.55.185.70                           | crowdsecurity/http-crawl-non_statics | ban    | FR      | 9003
Societe Francaise Du Radiotelephone - SFR SA  | 42     | 3h51m2.636570684s  | 13        |
| 12 | crowdsec | Ip:194.254.79.4                           | crowdsecurity/http-xss-probbing      | ban    | FR      | 2200
Renater                                         | 6      | 3h49m7.676288661s  | 12        |
| 4  | crowdsec | Ip:2a01:cb11:6a0:2d00:bfe7:82c4:c724:9eb7  | crowdsecurity/http-crawl-non_statics | ban    |
FR      | 3215 Orange                                    | 91     | 3h46m13.472584547s | 4         |
| 3  | crowdsec | Ip:176.168.162.101                        | crowdsecurity/http-crawl-non_statics | ban    | FR      | 5410
Bouygues Telecom SA                             | 46     | 3h45m27.591191061s | 3         |
| 2  | crowdsec | Ip:2001:41d0:302:1000::ca9                | crowdsecurity/http-crawl-non_statics | ban    | GB      |
16276 OVH SAS                                   | 47     | 3h43m25.263040245s | 2         |
| 1  | crowdsec | Ip:134.158.79.158                         | crowdsecurity/http-crawl-non_statics | ban    | FR      | 789
Renater                                         | 45     | 3h41m26.974324678s | 1         |
+----+----------+------------------------------------------+------------------------------------+--------+---------
+--------------------------------------------------+--------+--------------------+----------+
7 duplicated entries skipped
```

Lister les alertes

```
cscli alerts list
┌────┬──────────────────────────────────────────┬────────────────────────────────────┬
────────┬──────────────────────────────────────────────────┬────────┬────────────────
──────────────────────┐
│ ID │                  value                   │                reason              │ country │                    as                    │
decisions │               created_at               │
├────┼──────────────────────────────────────────┼────────────────────────────────────┼
────────┼──────────────────────────────────────────────────┼────────┼────────────────
──────────────────────┤
│ 15 │ Ip:212.23.165.14                         │ crowdsecurity/http-crawl-non_statics       │ FR       │ 12566 Societe
Francaise Du Radiotelephone - SFR SA │ ban:1      │ 2023-04-05 13:21:28.67736235 +0000 UTC  │
│ 14 │ Ip:83.206.19.140                         │ crowdsecurity/http-crawl-non_statics       │ FR       │ 3215
Orange                                        │ ban:1      │ 2023-04-05 13:21:35.442813467 +0000 UTC │
│ 13 │ Ip:84.55.185.70                          │ crowdsecurity/http-crawl-non_statics       │ FR       │ 9003 Societe
Francaise Du Radiotelephone - SFR SA  │ ban:1      │ 2023-04-05 13:19:50.40175296 +0000 UTC  │
│ 12 │ Ip:194.254.79.4                          │ crowdsecurity/http-xss-probbing            │ FR       │ 2200
Renater                                       │ ban:1      │ 2023-04-05 13:17:56.216060733 +0000 UTC │
│ 11 │ Ip:194.254.79.4                          │ crowdsecurity/http-cve-2021-41773          │ FR       │ 2200
Renater                                       │ ban:1      │ 2023-04-05 13:17:55.755095951 +0000 UTC │
```

```
│ 10 │ Ip:194.254.79.4                        │ crowdsecurity/http-path-traversal-probing │ FR       │ 2200
Renater                               │ ban:1      │ 2023-04-05 13:17:54.292927884 +0000 UTC │
│ 9  │ Ip:194.254.79.4                        │ crowdsecurity/http-sensitive-files        │ FR       │ 2200
Renater                               │ ban:1      │ 2023-04-05 13:17:52.403785142 +0000 UTC │
│ 8  │ Ip:194.254.79.4                        │ crowdsecurity/http-crawl-non_statics      │ FR       │ 2200
Renater                               │ ban:1      │ 2023-04-05 13:17:52.017817973 +0000 UTC │
│ 7  │ Ip:194.254.79.4                        │ crowdsecurity/http-probing                │ FR       │ 2200
Renater                               │ ban:1      │ 2023-04-05 13:17:52.309312166 +0000 UTC │
│ 6  │ Ip:194.254.79.4                        │ crowdsecurity/http-bad-user-agent         │ FR       │ 2200
Renater                               │ ban:1      │ 2023-04-05 13:17:52.017572598 +0000 UTC │
│ 5  │ Ip:83.206.19.140                       │ crowdsecurity/http-crawl-non_statics      │ FR       │ 3215
Orange                                │ ban:1      │ 2023-04-05 13:17:28.44454104 +0000 UTC  │
│ 4  │ Ip:2a01:cb11:6a0:2d00:bfe7:82c4:c724:9eb7 │ crowdsecurity/http-crawl-non_statics      │ FR       │ 3215
Orange                                │ ban:1      │ 2023-04-05 13:14:35.443575184 +0000 UTC │
│ 3  │ Ip:176.168.162.101                     │ crowdsecurity/http-crawl-non_statics      │ FR       │ 5410 Bouygues
Telecom SA                        │ ban:1      │ 2023-04-05 13:14:13.380354035 +0000 UTC │
│ 2  │ Ip:2001:41d0:302:1000::ca9             │ crowdsecurity/http-crawl-non_statics      │ GB       │ 16276 OVH
SAS                               │ ban:1      │ 2023-04-05 13:12:10.793700983 +0000 UTC │
│ 1  │ Ip:134.158.79.158                      │ crowdsecurity/http-crawl-non_statics      │ FR       │ 789
Renater                               │ ban:1      │ 2023-04-05 13:10:13.259428338 +0000 UTC │
╰────┴───────────────────────────────────────────┴───────────────────────────────────────────┴
──────────┴─────────────────────────────────────────────────┴──────────┴─────────────────────
──────────────────────────────╯
```

Supprimer une décision

```
cscli decisions delete -r 1.2.3.0/24
cscli decisions delete -i 1.2.3.4
cscli decisions delete --id 42
```

Explain

Tester sur les dernieres connexions

```
tail -10 /var/log/httpd/access.miroir.log | cscli explain --verbose --type apache2 -f -
        ├ s02-enrich
        |       ├ 🟢 crowdsecurity/dateparse-enrich (+2 ~1)
        |               ├ create evt.Enriched.MarshaledTime : 2023-04-06T11:17:39+02:00
```

```
|               ├ update evt.MarshaledTime :  -> 2023-04-06T11:17:39+02:00
|               ├ create evt.Meta.timestamp : 2023-04-06T11:17:39+02:00
|       ├ □□ crowdsecurity/geoip-enrich (+13)
|               ├ create evt.Enriched.ASNNumber : 16276
|               ├ create evt.Enriched.ASNOrg : OVH SAS
|               ├ create evt.Enriched.IsInEU : true
|               ├ create evt.Enriched.Latitude : 48.858200
|               ├ create evt.Enriched.Longitude : 2.338700
|               ├ create evt.Enriched.ASNumber : 16276
|               ├ create evt.Enriched.IsoCode : FR
|               ├ create evt.Enriched.SourceRange : 51.75.0.0/16
|               ├ create evt.Meta.SourceRange : 51.75.0.0/16
|               ├ create evt.Meta.IsoCode : FR
|               ├ create evt.Meta.ASNOrg : OVH SAS
|               ├ create evt.Meta.IsInEU : true
|               ├ create evt.Meta.ASNNumber : 16276
|       ├ □□ crowdsecurity/http-logs (+7)
|               ├ create evt.Parsed.file_ext : .gz
|               ├ create evt.Parsed.file_name :
6ae72f04c86cd50a9999cb618d7dd3ec5940bb2f24ecf194c2444baaf87a0334-updateinfo.xml.gz
|               ├ create evt.Parsed.static_ressource : true
|               ├ create evt.Parsed.file_frag :
6ae72f04c86cd50a9999cb618d7dd3ec5940bb2f24ecf194c2444baaf87a0334-updateinfo.xml
|               ├ create evt.Parsed.impact_completion : true
|               ├ create evt.Parsed.file_dir : /rocky/8.7/PowerTools/x86_64/os/repodata/
|               ├ create evt.Meta.http_args_len : 0
|       └ □□ crowdsecurity/whitelists (~2 [whitelisted])
|               └ update evt.Whitelisted : %!s(bool=false) -> true
|               └ update evt.WhitelistReason :  -> private ipv4/ipv6 ip/ranges
└-------- parser failure □□
```

Remarques :

- Whitelise car Pays FR

Mises à jour

```
cscli hub update
INFO[05-04-2023 17:02:49] hub index is up to date
```

```
INFO[05-04-2023 17:02:49] Wrote new 651136 bytes index to /etc/crowdsec/hub/.index.json
INFO[05-04-2023 17:02:49] dependency of crowdsecurity/base-http-scenarios : missing scenarios crowdsecurity/http-crawl-non_statics, tainted.
INFO[05-04-2023 17:02:49] update for collection crowdsecurity/http-cve available (currently:1.9, latest:2.0)
INFO[05-04-2023 17:02:49] dependency of crowdsecurity/apache2 : sub collection crowdsecurity/base-http-scenarios is broken : missing scenarios crowdsecurity/http-crawl-non_statics, tainted.
```

Il faut update crowdsecurity/http-cve !

```
cscli collections list

COLLECTIONS
────────────────────────────────────────────────────────────────────────────────
────────────────────────────
 Name                          Status                    Version   Local Path
────────────────────────────────────────────────────────────────────────────────
────────────────────────────
 crowdsecurity/apache2                ✔ enabled                     0.1       /etc/crowdsec/collections/apache2.yaml
 crowdsecurity/base-http-scenarios   ⚠ enabled,tainted            0.6       /etc/crowdsec/collections/base-http-scenarios.yaml
 crowdsecurity/http-cve               ⚠ enabled,update-available   1.9       /etc/crowdsec/collections/http-cve.yaml
 crowdsecurity/linux                  ✔ enabled                     0.2       /etc/crowdsec/collections/linux.yaml
 crowdsecurity/sshd                   ✔ enabled                     0.2       /etc/crowdsec/collections/sshd.yaml
```

Mise à jour :

```
cscli collections upgrade crowdsecurity/http-cve
```

Whitelist

Pour repérer les noms sur lesquels s'appuyer, on peut consulter la taxonomy.

Na pas modifier les fichiers dans le dossier hub. Créer un fichier de conf :

```
/etc/crowdsec/parsers/s02-enrich/whitelist-renater.yaml
```

Contenu :

```
name:
ul/whitelists

description: "Whitelist Renater"
whitelist:

  reason: "Renater"

expression:

    - evt.Meta.ASNNumber == '2200'
```

Lists des parsers :

```
cscli parsers list

PARSERS
────────────────────────────────────────────────────────────────────────────────────────
──────────────────────
 Name                          □□ Status        Version   Local Path
────────────────────────────────────────────────────────────────────────────────────────
──────────────────────
 crowdsecurity/apache2-logs       ✔ enabled          1.3       /etc/crowdsec/parsers/s01-parse/apache2-
logs.yaml
 crowdsecurity/dateparse-enrich   ✔ enabled          0.2       /etc/crowdsec/parsers/s02-enrich/dateparse-
enrich.yaml
 crowdsecurity/geoip-enrich       ✔ enabled          0.2       /etc/crowdsec/parsers/s02-enrich/geoip-enrich.yaml
 crowdsecurity/http-logs          ✔ enabled          1.1       /etc/crowdsec/parsers/s02-enrich/http-logs.yaml
 crowdsecurity/sshd-logs          ✔ enabled          2.0       /etc/crowdsec/parsers/s01-parse/sshd-logs.yaml
 crowdsecurity/syslog-logs        ✔ enabled          0.8       /etc/crowdsec/parsers/s00-raw/syslog-logs.yaml
 crowdsecurity/whitelists         ⚠ enabled,tainted   ?        /etc/crowdsec/parsers/s02-enrich/whitelists.yaml
 whitelist-renater.yaml          □□ enabled,local              /etc/crowdsec/parsers/s01-parse/whitelist-renater.yaml
────────────────────────────────────────────────────────────────────────────────────────
──────────────────────
```

On peut tester la whitelist :

```
tail -10 /tmp/4 | cscli explain --verbose --type apache2 -f -
|       ├ □□ crowdsecurity/whitelists (~2 [whitelisted])
        |               ├ update evt.Whitelisted : %!s(bool=false) -> true
```

```
|           ├ update evt.WhitelistReason :  -> Renater
|     ├ □□ crowdsecurity/whitelists-ipul (~1)
|           ├ update evt.WhitelistReason : Renater -> UL
|     ├ □□ ul/whitelists-fr (~1)
|           ├ update evt.WhitelistReason : UL -> FR
|     └ □□ ul/whitelists-renater (~1)
|           └ update evt.WhitelistReason : FR -> Renater
```

Revision #12
Created 5 April 2023 13:27:49 by Stephane DUGRAVOT
Updated 12 April 2023 12:08:04 by Stephane DUGRAVOT