JeromeVosgien | +33 6 75 31 82 81

AdrienDebosschere | +33 6 19 50 17 75

LA Masterclass LogPoint

8 mars 2022

Tensions internationales Cyber menaces - TI: IOC & CSV

LOGPOINT

Pourquoi cette modification d'agenda ?

clubic

Accueil / Cyber sécurité / Cyberguerre Russie - Ukraine

Guerre en Ukraine : l'ANSSI prévient de possibles cyberattaques

Alexandre Boero
03 mars 2022 à 14h25

L'Anssi livre ses recommandations de cyberprotection dans le cadre du conflit ukrainien

Les entreprises et les administrations doivent être particulièrement vigilantes face aux éventuelles cyberattaques dans le contexte de l'invasion de l'Ukraine par la Russie, alerte l'Anssi. Elle vient de publier une série de recommandations à suivre, telles que l'instauration de l'authentification forte, la cartographie des systèmes, la mise en place d'un système de supervision des événements journalisés...

ALICE VITARD | PUBLIÉ LE 02 MARS 2022 À 15H12

CYBERSÉCURITÉ, INFORMATIQUE , DÉFENSE

TWITTER FACEBOOK LINKEDIN FLIPBOARD EMAIL

Face au risque d'attaqu
sécurité des systèmes
de recommandations
durant le conflit entre

Cyber armée ukrainienne : quelles sont les missions de ces hactivistes mercenaires 2.0 ?

Posted On 03 Mar 2022 By : Damien Bancal Comment: 1

Il y a quelques jours, le gouvernement Ukrainien faisait appel aux hackers afin d'intégrer une cyber armée improvisée. ZATAZ a rencontré ces internautes qui veulent aider sans vraiment comprendre le danger de leurs actions.

L'invasion de l'Ukraine par les troupes de l'armée russe a en surpris plus d'un. Cette attaque terre, mer, air a connu son pendant numérique avec des blocages de sites web et la perturbation des communications. Jusqu'ici, nous sommes face à des actions de guerre « classique ». Cependant, c'est la première fois qu'un pays agressé fait appel à la communauté des internautes afin de l'aider à contrer les assaillants.

Le ministre en charge de la transformation digitale, Mykhailo Fedorov, a lancé un appel aux armes numériques « **Nous créons une armée informatique. Nous avons besoin de talents numériques.**

ANSSI | Agence nationale de la sécurité des systèmes d'information

DÉCLARATION VULNÉRABILITÉ | EN CAS D'INCIDENT | ALERTES | PRESSE | RECRUTEMENT

ACTUALITÉS

TENSIONS INTERNATIONALES : RENFORCEMENT DE LA VIGILANCE CYBER

Les tensions internationales actuelles causées par l'invasion de l'Ukraine par la Russie, s'accompagnent d'effets dans le cyberespace. Si les combats en Ukraine sont principalement conventionnels, l'ANSSI constate l'usage de cyberattaques dans le cadre du conflit. Dans un espace numérique sans frontières, ces cyberattaques peuvent affecter des entités françaises et il convient sans céder à la panique de l'anticiper et de s'y préparer. Aussi, afin de réduire au maximum la probabilité de tels événements et d'en limiter les effets, l'ANSSI incite donc les entreprises et les administrations à :

- consulter le bulletin du Centre gouvernemental de veille d'alerte et de réponse aux attaques informatiques (CERT-FR) qui est mis à jour régulièrement ;
- mettre en œuvre les cinq mesures cyber préventives prioritaires détaillées ci-dessous.

Mesures cyber préventives prioritaires
652.33 Ko

PDF

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

MESURES CYBER PRÉVENTIVES PRIORITAIRES
TENSIONS INTERNATIONALES ACTUELLES

Cyberattacks on the rise in the wake of the Ukraine crisis: 5 ways to strengthen cybersecurity defenses

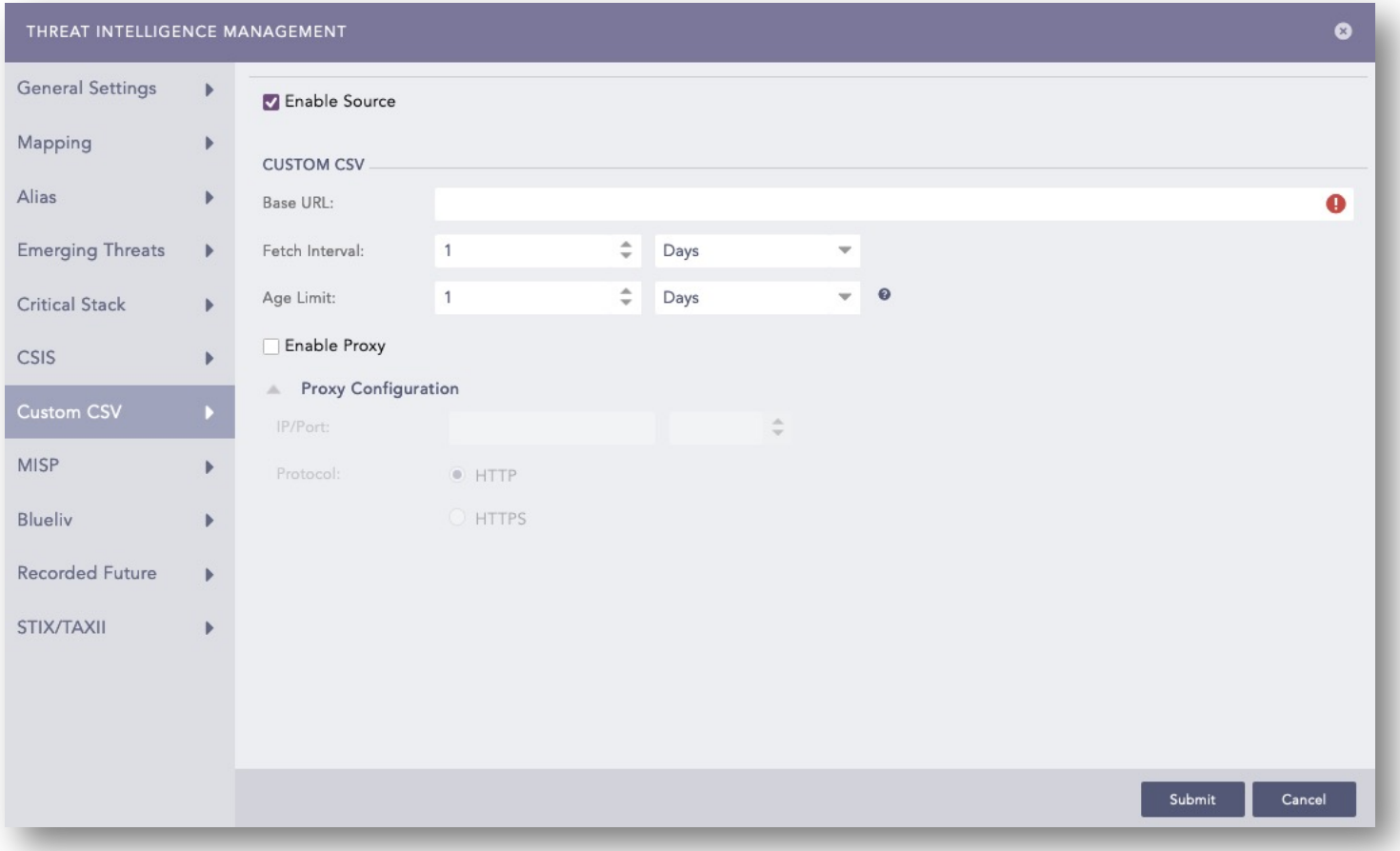
mars 2nd, 2022

By Ivan Vinogradov, Security analyst, Logpoint, and Jan Quach, Global Director of Customer Success

Contact Logpoint

LOGPOINT

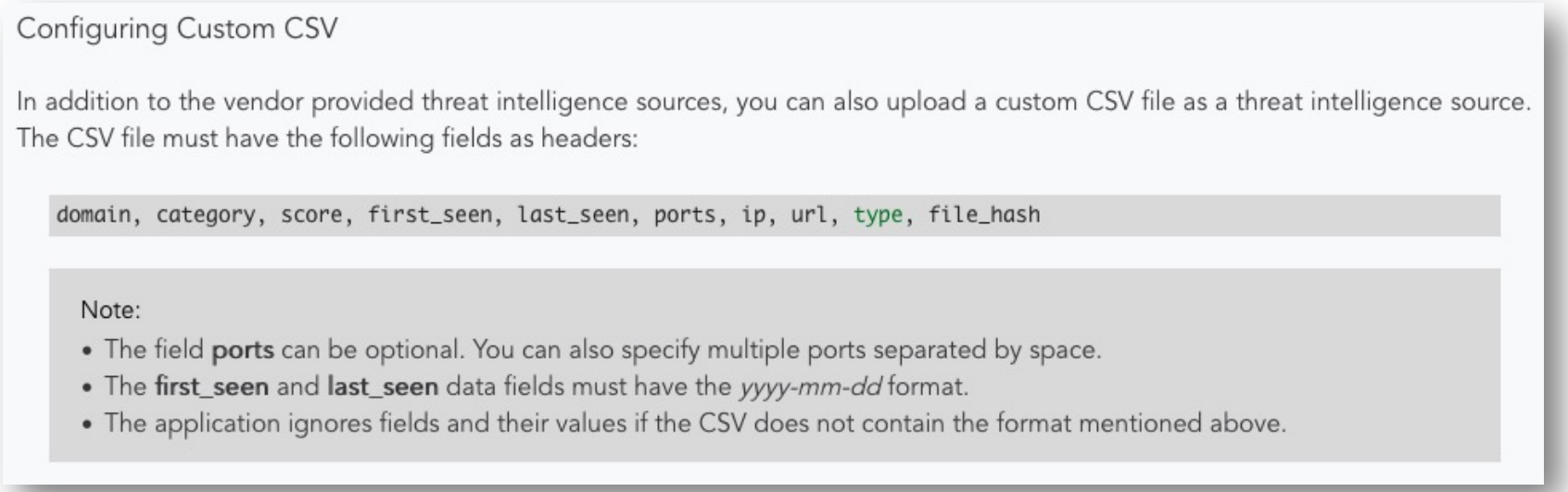
Threat Intelligence & CSV



Threat Intelligence & CSV

Plutôt rigide...

- URL → Le CSV doit être hébergé sur un serveur web, accessible au SIEM
- Format imposé



Configuring Custom CSV

In addition to the vendor provided threat intelligence sources, you can also upload a custom CSV file as a threat intelligence source. The CSV file must have the following fields as headers:

```
domain, category, score, first_seen, last_seen, ports, ip, url, type, file_hash
```

Note:

- The field **ports** can be optional. You can also specify multiple ports separated by space.
- The **first_seen** and **last_seen** data fields must have the *yyyy-mm-dd* format.
- The application ignores fields and their values if the CSV does not contain the format mentioned above.

Enrichissement à base de fichiers CSV

Plus flexible !

- Permet d'uploader un fichier CSV depuis l'interface du SIEM
- Crée un objet de type "Table"
- Cette Table est utilisable:
  - A la demande dans les recherches (→ dashboards, alertes, rapports...)
  - Comme source d'enrichissement lors de la collecte

- Inconvénient: mise à jour manuelle du contenu

Exemple 1:

Liste d’adresses IP

Transformer une liste d'IPs en fichier CSV

```
213.183.58.12
194.67.109.14
194.67.109.164
```

Microsoft Excel

	A	B	C	D
1	destination_address	source_address	threat_source	threat_campaign
2	213.183.58.12	213.183.58.12	ANSSI	malwareXYZ
3	194.67.109.14	194.67.109.14	ANSSI	Pteranodon
4	194.67.109.164	194.67.109.164	ANSSI	Pteranodon

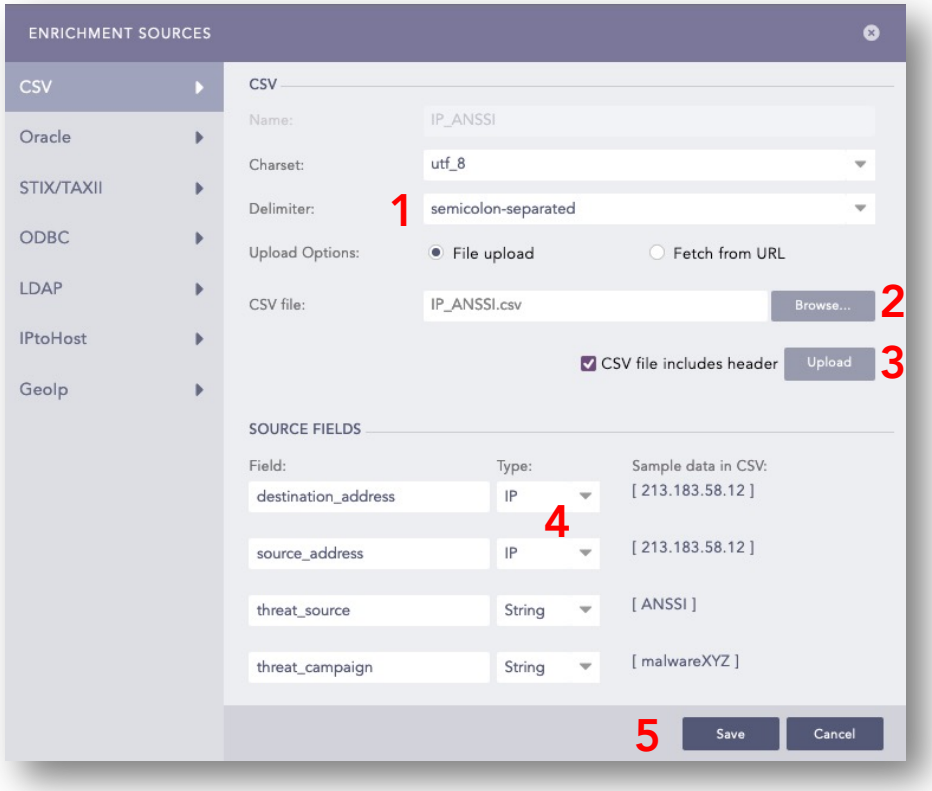
Save as... CSV
(pas UTF8)

```
destination_address;source_address;threat_source;threat_campaign
213.183.58.12;213.183.58.12;ANSSI;malwareXYZ
194.67.109.14;194.67.109.14;ANSSI;Pteranodon
194.67.109.164;194.67.109.164;ANSSI;Pteranodon
```

IP_ANSSI.csv

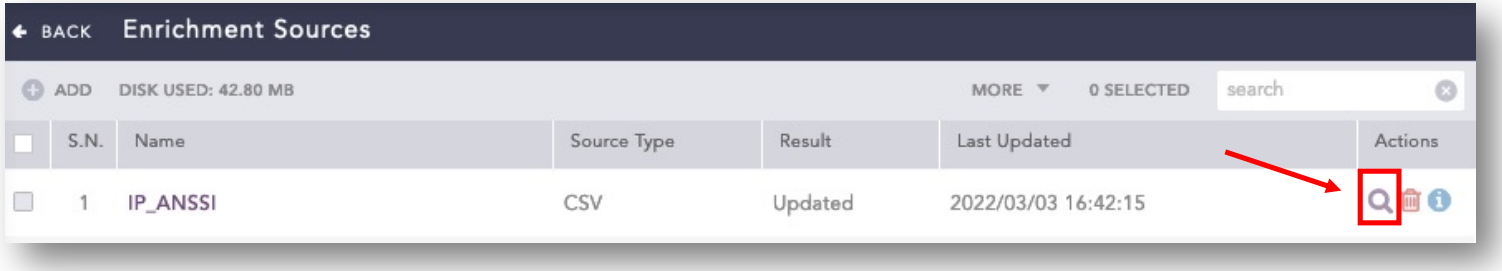
Importer ce CSV dans LogPoint

Settings > Configuration > Enrichment Sources > + ADD > CSV

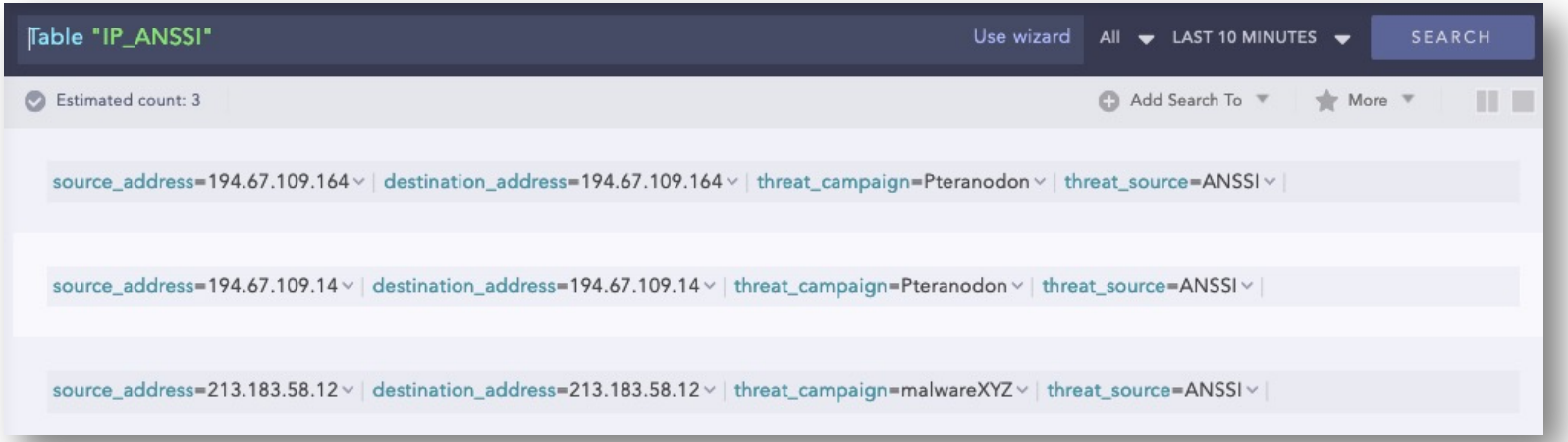


1. Choisir le delimiter “semicolon-separated” (format CSV d’Excel)
2. Cliquer sur Browse et aller chercher le fichier CSV
3. Cliquer sur Upload
4. Sélectionner le type “IP” pour les champs contenant des IPs
5. Sauvegarder

Vérifier la table d'enrichissement créée



La Table peut prendre plusieurs minutes à se remplir...



Utilisation dans une recherche

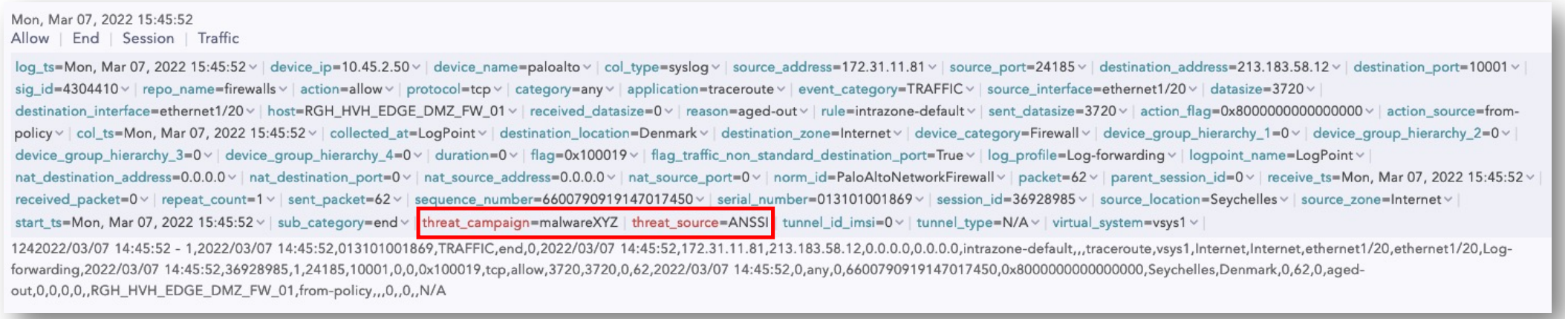
```
source_address=* OR destination_address=*
| process lookup(IP_ANSSI, source_address)
| process lookup(IP_ANSSI, destination_address)
| filter threat_campaign=*
```

On travaille sur les logs avec au moins un de ces champs

On croise la table “IP_ANSSI” avec chaque log sur le champ “source_address”

Idem sur le champ “destination_address”

Le champ “threat_campaign” provient de la table, il est présent s’il y a une correspondance, donc on garde uniquement les logs où il apparait

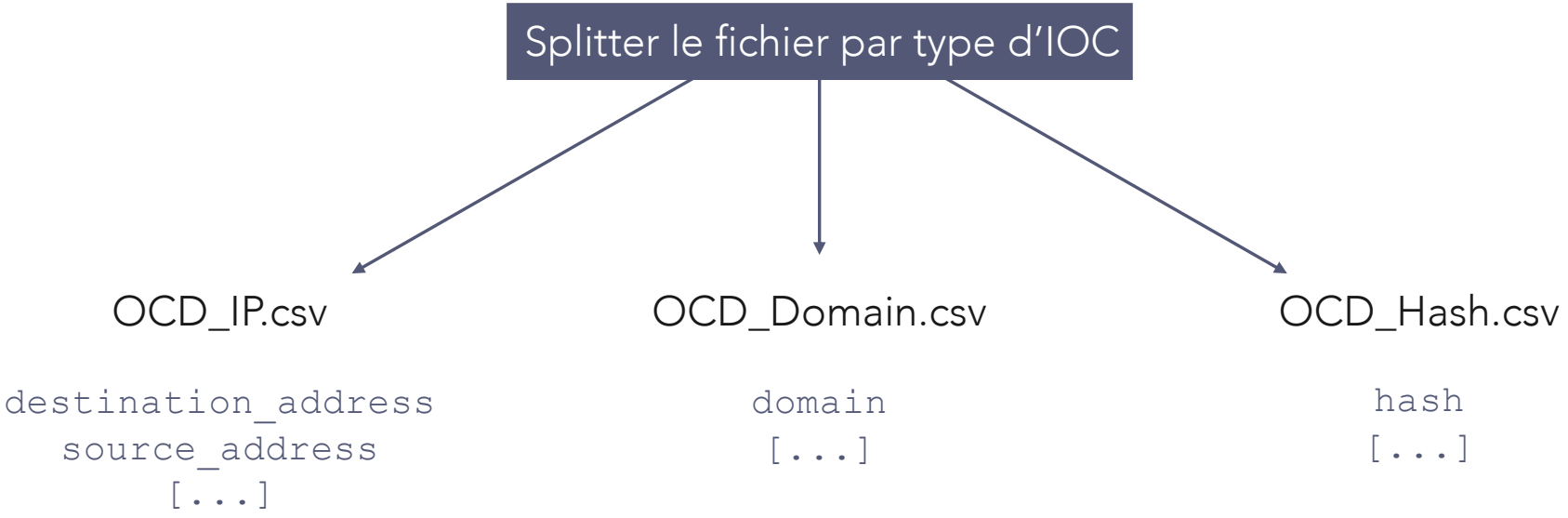


Exemple 2:

Liste avec plusieurs types d'IOC

Plusieurs types d'IOC

- Liste publique d'Orange Cyber Défense
  - https://github.com/Orange-Cyberdefense/russia-ukraine_IOCs/blob/main/OCD-Datalake-russia-ukraine_IOCs-ALL.csv



Enrichissement lors de la collecte

Enrichment Policy

Configuration > Enrichment Policy

Champs qui doivent être présents dans le log

Source d'enrichissement à utiliser

Champ dans la source d'enrichissement

Champ dans le log

https://docs.logpoint.com/docs/data-integration-guide/en/latest/Configuration/Enrichment%20Policies.html