

 JeromeVosgien | +33 6 75 31 82 81

 AdrienDebosschere | +33 6 19 50 17 75

LA Masterclass LogPoint

8 mars 2022

MASTERCLASS

 LOGPOINT

Tensions internationales
Cyber menaces
TI: IOC & CSV



 LOGPOINT



Pourquoi cette modification d'agenda ?



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 VIDARD | PUBLIÉ LE 03 MARS 2022 À 13H12
CYBERSÉCURITÉ, INFORMATIQUE, DÉFENSE

Face au risque d'attaques de 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.

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 cyberspace. 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.



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

Threat Intelligence & CSV

THREAT INTELLIGENCE MANAGEMENT

- General Settings
- Mapping
- Alias
- Emerging Threats
- Critical Stack
- CSIS
- Custom CSV**
- MISP
- Blueliv
- Recorded Future
- STIX/TAXII

Enable Source

CUSTOM CSV

Base URL:

Fetch Interval: Days

Age Limit: Days

Enable Proxy

Proxy Configuration

IP/Port:

Protocol: HTTP HTTPS

Submit Cancel

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

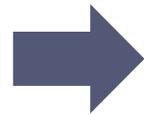
Exemple 1:
Liste d'adresses IP



Transformer une liste d'IPs en fichier CSV

Microsoft Excel

213.183.58.12
194.67.109.14
194.67.109.164



	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

The screenshot shows the 'ENRICHMENT SOURCES' configuration window for a CSV source. The settings are as follows:

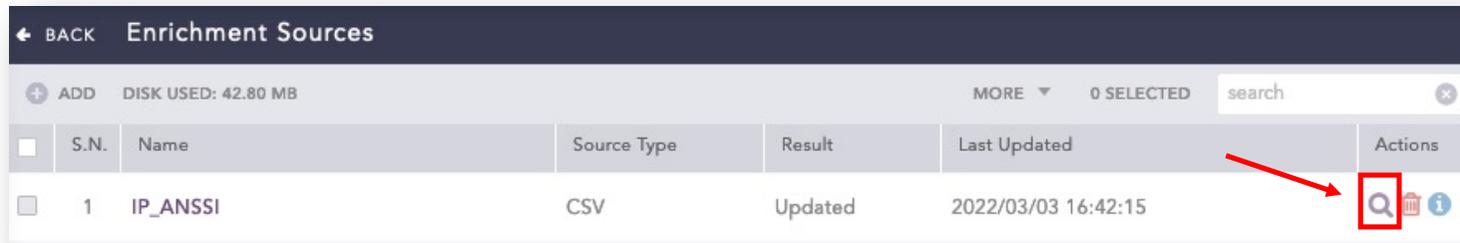
- Name: IP_ANSSI
- Charset: utf_8
- Delimiter: semicolon-separated (marked with a red '1')
- Upload Options: File upload (selected), Fetch from URL
- CSV file: IP_ANSSI.csv (marked with a red '2') with a 'Browse...' button
- CSV file includes header: checked (marked with a red '3') with an 'Upload' button
- SOURCE FIELDS:

Field:	Type:	Sample data in CSV:
destination_address	IP (marked with a red '4')	[213.183.58.12]
source_address	IP	[213.183.58.12]
threat_source	String	[ANSSI]
threat_campaign	String	[malwareXYZ]

At the bottom, there are 'Save' and 'Cancel' buttons, with a red '5' indicating the final step.

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



	S.N.	Name	Source Type	Result	Last Updated	Actions
<input type="checkbox"/>	1	IP_ANSSI	CSV	Updated	2022/03/03 16:42:15	  



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



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

Utilisation dans une recherche

```
source_address=* OR destination_address=*
```

```
| process lookup(IP_ANSSI, source_address)
```

```
| process lookup(IP_ANSSI, destination_address) —> Idem sur le champ "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"

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 apparaît

Mon, Mar 07, 2022 15:45:52

Allow | End | Session | Traffic

```
log_ts=Mon, Mar 07, 2022 15:45:52 | device_ip=10.45.2.50 | device_name=paloalto | col_type=syslog | source_address=172.31.11.81 | source_port=24185 | destination_address=213.183.58.12 | destination_port=10001 | sig_id=4304410 | repo_name=firewalls | action=allow | protocol=tcp | category=any | application=traceroute | event_category=TRAFFIC | source_interface=ethernet1/20 | datasize=3720 | destination_interface=ethernet1/20 | host=RGH_HVH_EDGE_DMZ_FW_01 | received_datasize=0 | reason=aged-out | rule=intrazone-default | sent_datasize=3720 | action_flag=0x8000000000000000 | action_source=from-policy | col_ts=Mon, Mar 07, 2022 15:45:52 | collected_at=LogPoint | destination_location=Denmark | destination_zone=Internet | device_category=Firewall | device_group_hierarchy_1=0 | device_group_hierarchy_2=0 | device_group_hierarchy_3=0 | device_group_hierarchy_4=0 | duration=0 | flag=0x100019 | flag_traffic_non_standard_destination_port=True | log_profile=Log-forwarding | logpoint_name=LogPoint | nat_destination_address=0.0.0.0 | nat_destination_port=0 | nat_source_address=0.0.0.0 | nat_source_port=0 | norm_id=PaloAltoNetworkFirewall | packet=62 | parent_session_id=0 | receive_ts=Mon, Mar 07, 2022 15:45:52 | received_packet=0 | repeat_count=1 | sent_packet=62 | sequence_number=6600790919147017450 | serial_number=013101001869 | session_id=36928985 | source_location=Seychelles | source_zone=Internet | start_ts=Mon, Mar 07, 2022 15:45:52 | sub_category=end | threat_campaign=malwareXYZ | threat_source=ANSSI | tunnel_id_imsi=0 | tunnel_type=N/A | virtual_system=vsys1 | 1242022/03/07 14:45:52 - 1,2022/03/07 14:45:52,013101001869,TRAFFIC,end,0,2022/03/07 14:45:52,172.31.11.81,213.183.58.12,0.0.0.0,0.0.0.0,intrazone-default,,,traceroute,vsys1,Internet,Internet,ethernet1/20,ethernet1/20,Log-forwarding,2022/03/07 14:45:52,36928985,1,24185,10001,0,0,0x100019,tcp,allow,3720,3720,0,62,2022/03/07 14:45:52,0,any,0,6600790919147017450,0x8000000000000000,Seychelles,Denmark,0,62,0,aged-out,0,0,0,0,,RGH_HVH_EDGE_DMZ_FW_01,from-policy,,,0,,0,,N/A
```

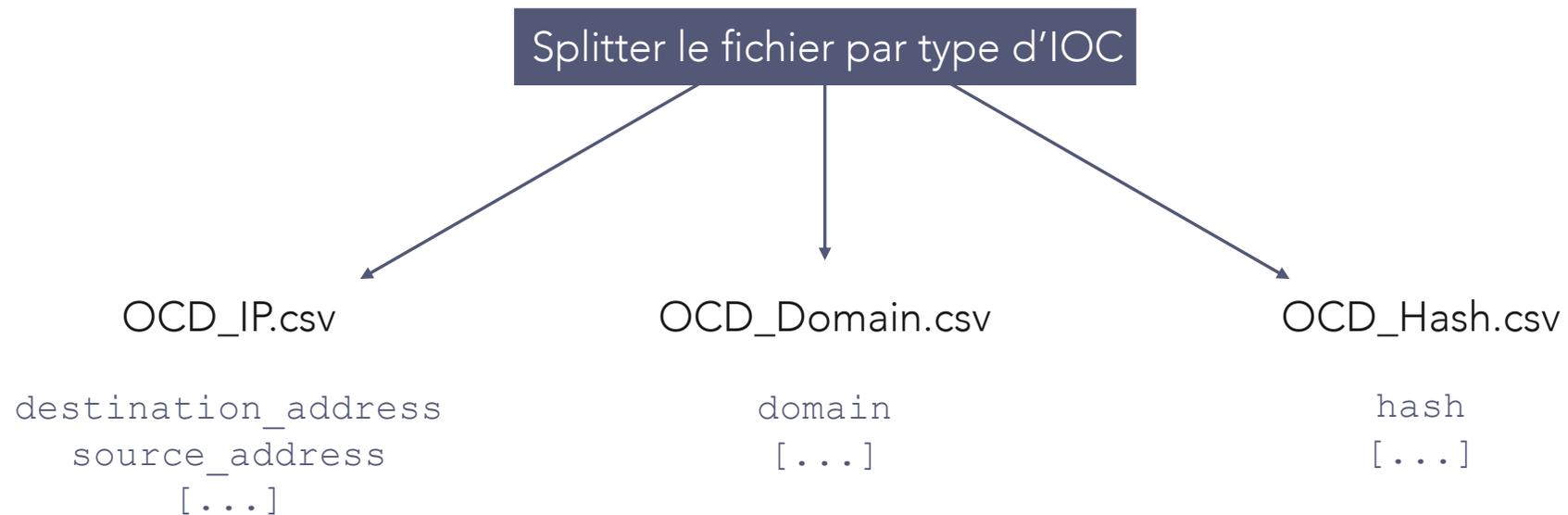
Exemple 2:

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

SPECIFICATION

Enrichment Criteria
Enrichment rule will be applied only if all of the conditions are satisfied by log event

Key Presents	▼	source_address	+	-
Key Presents	▼	destination_address	+	-

Enrichment Rule
Enrichment rule will be applied if all of the conditions below matches

Enrichment Source: IP_ANSSI ▼

Source	Operation	Category	
source_address ▼	Equals ▼	Simple ▼	source_address + -

Add New Specification Remove Specification

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>