Afterwork octobre 2022

Sommaire

 # ACTU CNA

 # AFTERWORK en 2 parties

1. *Qu'est-ce qu'un CTF ?*
2. *Qu'est-ce que l'OSINT ?*

Actus CLUSIR NA

« Un campus, vitrine de l'éco-système néo-aquitain »

Le **Campus régional de cybersécurité et de confiance numérique a été officiellement lancé ce lundi 10 octobre** à l'Hôtel de Région à Bordeaux

Créé par le GIP Cybermalveillance, l'Agence de développement et d'innovation de Nouvelle-Aquitaine (ADI-NA), le CLUSIR NA et la Région Nouvelle-Aquitaine, il renforcera les synergies entre les acteurs privés et publics de la cybersécurité.

Le **premier projet est l'ouverture du CSIRT** [Computer Security Incident Response Team] est un centre de réponse aux incidents cyber au profit des entités implantées sur le territoire régional

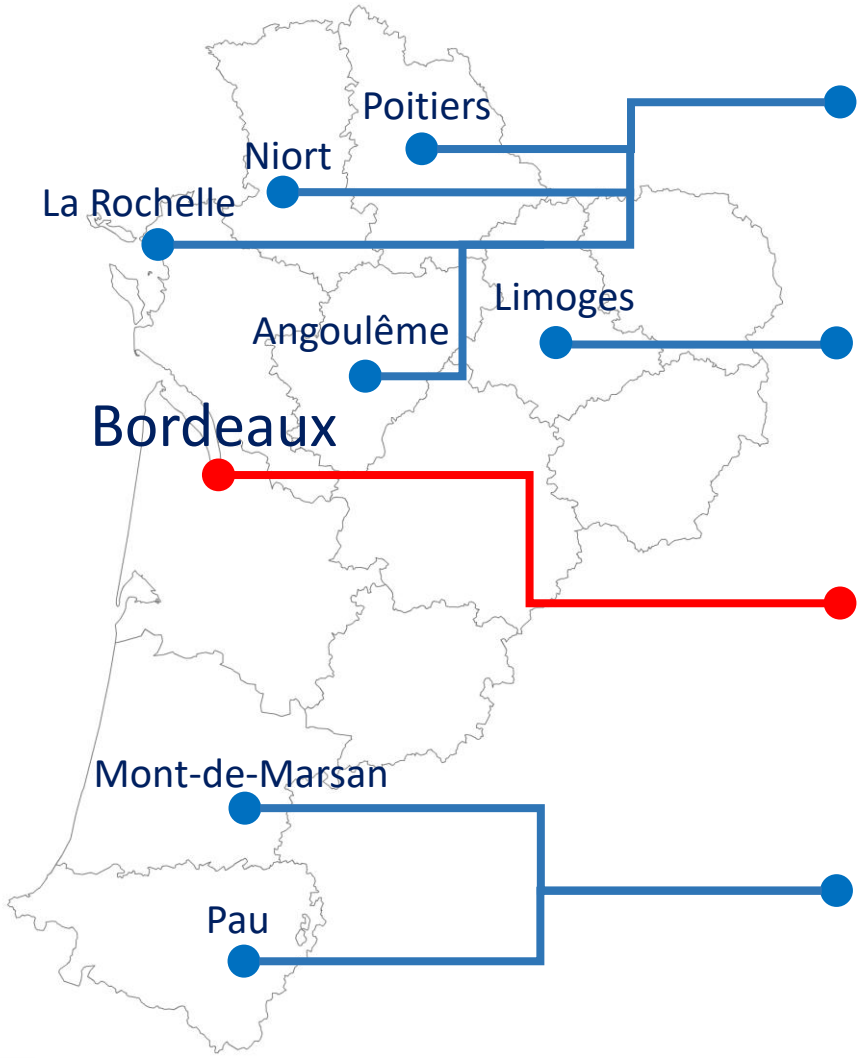
Actus CLUSIR NA

Feedback des Assises 2022

SAVE THE DATE prochaine **#Afterwork** spécial Startup le **mardi 29 novembre**

Visite Datacenter EQUINIX en cours de planification

Antennes CNA en Nouvelle Aquitaine



Antenne Poitou-Charentes Responsable **Didier SPELLA**

Antenne.poitou-charentes@clusir-aquitaine.fr

Antenne Limoges Responsable **Pierre VENOT**

Antenne.limoges@clusir-aquitaine.fr

Bureau CNA Président **Gurvan QUENET**

Bureau@clusir-aquitaine.fr

Antenne 6440 Responsable **Christophe MARNAT & Nicolas TERRADE**

antenne.6440@clusir-aquitaine.fr

Afterwork octobre 2022

Partie 1 *Qu'est-ce qu'un CTF ?*

La Gamification en Cybersécurité

par Les Pires Hat

Qui sommes-nous ?

Anthony

CTO @ Wikodit

Etienne

Security engineer
Offsec @ Yousign

Pierre

OSINT & Security Analyst
@ BreacHunt

Les Pires Hat

Veille technologique

Échange d'informations, d'outils et de sources

Challenges

Participation à de nombreux CTF

R&D

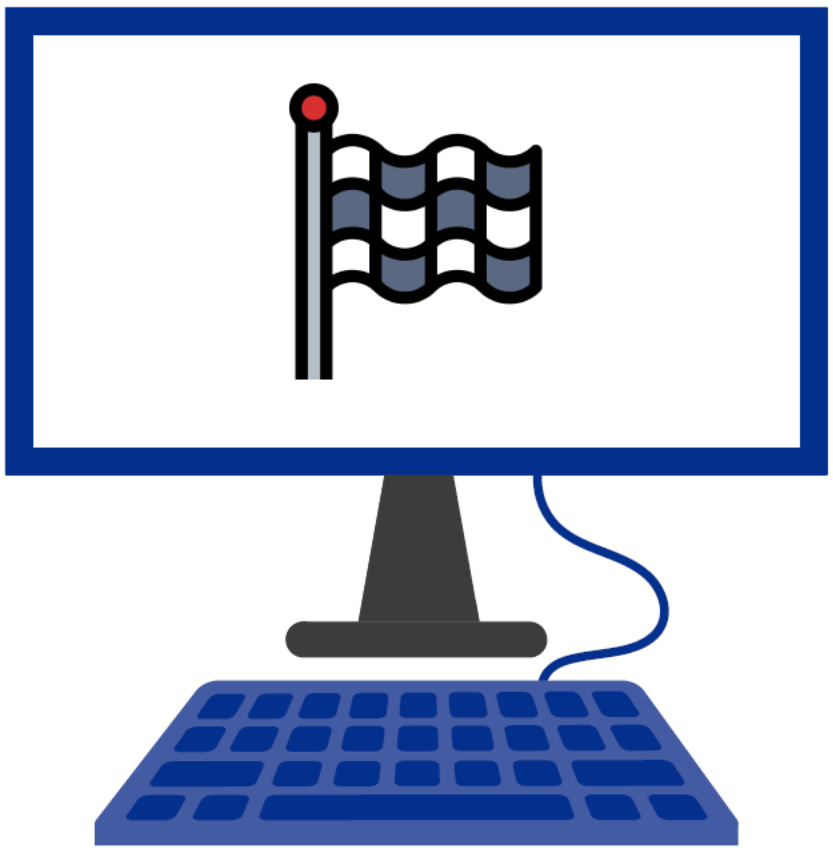
Développement d'outils

Sensibilisation

Événements théoriques et pratiques

Notre équipe

Qu’est-ce qu’un CTF ?



1

Challenges techniques

Des épreuves préparées par des passionnés ou des entreprises du secteur

2

Compétition et stratégie

De jour ou de nuit, objectif de classement

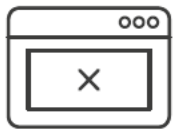
3

Événement

Moment d’échanges et de partages

Différents types de CTF

Jeopardy



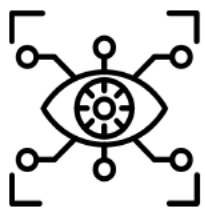
Attaque
Defense

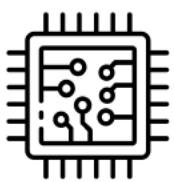
Social

Mise en
situation

OSINT

Hardware





Différents types d'épreuves

Pour toutes les spécialités !

Déroulé


ECW CTF
Rules
Users
Scoreboard
Challenges
Notifications
Profile
Settings
Misc
AR52000
487
jigsaw 1/3
100
jigsaw 2/3
100
jigsaw 3/3
242
welcome
10
Reverse
HotShotGL
500
Six Tunas On A Plane
500
UEFI
499
minifilter
499
Hardware
gates 1/3
100
gates 2/3
217
gates 3/3
396
Network
cry me a river
389
flood
100

1


Challenge
9 Solves
minifilter
499
A user noticed a bug when saving his file from notepad. We found some suspect files his computer. Please find out what it is.
Challenge proposed by : THALES
PS: Please use a virtual machine to run the minifilter :)
minifilter.7z
Flag
Submit

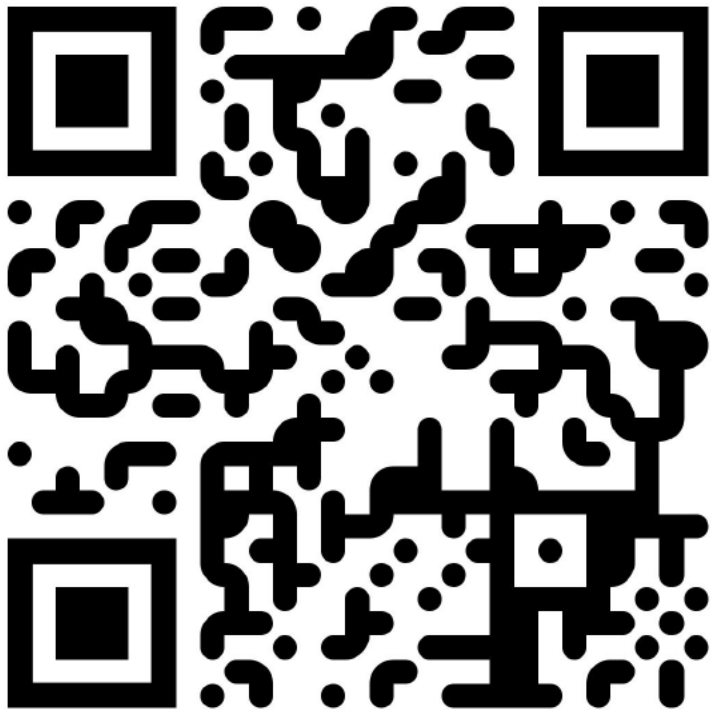
2


ECW CTF
Rules
Users
Scoreboard
Challenges
Notifications
Profile
Settings
Scoreboard
Top 10 Users
10-15 2022
Log_s: 552
Place
User
Category
Score
1
Professional
5588
2
Student
5289
3
Student
5289
4
Student
4898
5
Student
4801

3

Write-up

Retrouvez quelques
exemples sur notre blog :



1. **Prise de notes**
   Organiser son processus d'exploitation

2. **Rédaction**
   Démonstration de la compréhension globale de l' épreuve et travail de rédaction

3. **Partage de connaissance**
   Rendre l'apprentissage de la solution de l'épreuve accessible à tous

À ne pas confondre

Bug Bounty

Recherche de vulnérabilités sur des scopes précis sur un produit/solution existant pour récupérer une récompense

Pentest & Audit

Analyse d'un produit/solution existant sur une période donnée et de manière contractuelle

!==

CTF

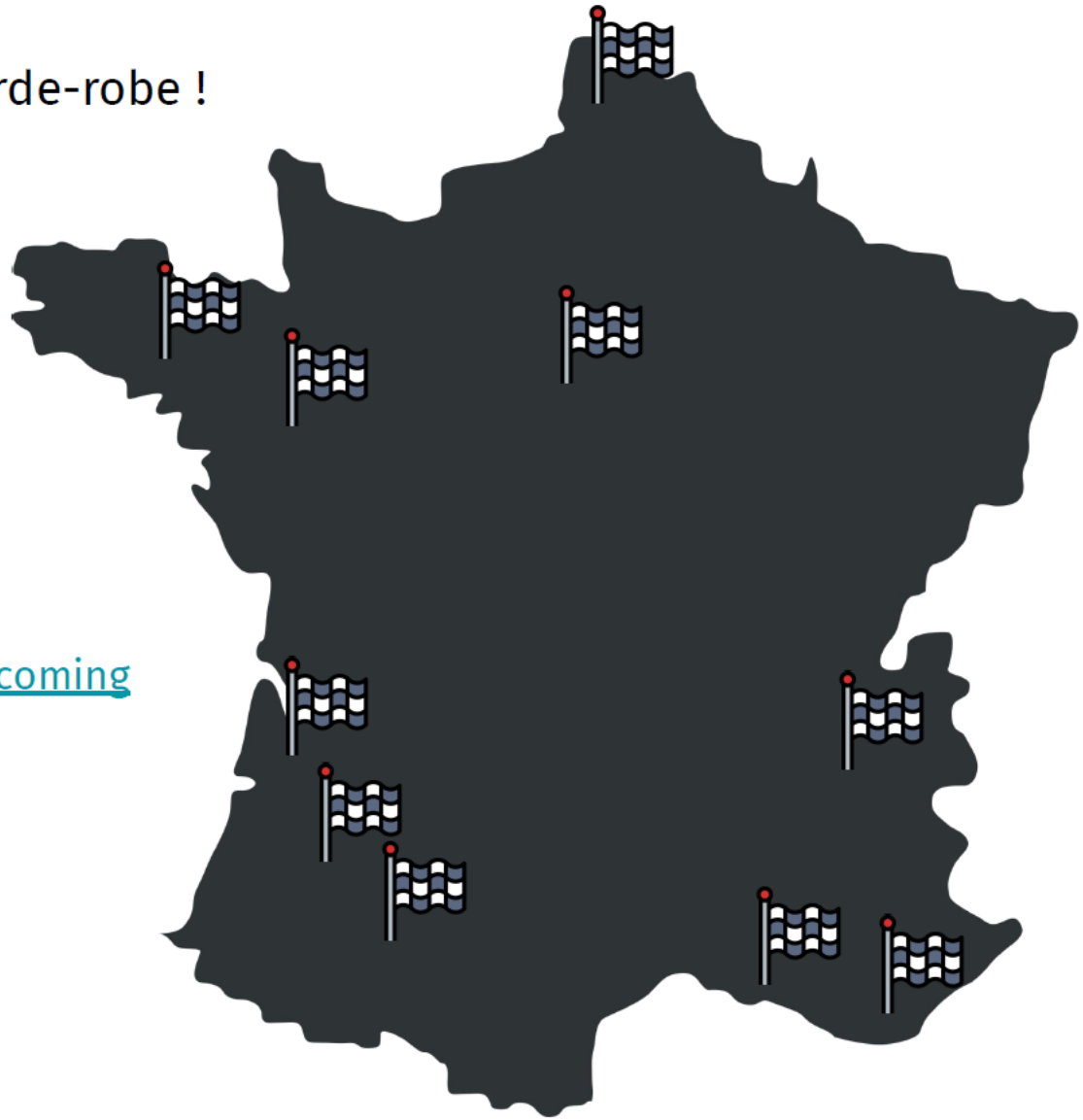
Jeu où il faut résoudre des challenges de sécurité afin de récupérer des points

Hackathon

Challenge autour de la conception d'une solution ou le développement d'un projet dans un temps limité

Le tour de France !

L’occasion de remplir sa garde-robe !



Calendrier sur **CTF Time :**
https://ctftime.org/event/list/upcoming

& Twitter, Linkedin…

Participer à un CTF en entreprise ?

Formation

Partage de compétences

Découverte de **nouvelles techniques/outils**

Gain d'**expérience** sur les vulnérabilités

Réseau

Rencontre des potentiels **futurs collaborateurs** et partenaires

Échange entre les équipes de sécurité et **le reste de l'entreprise**

Communication

Challenger les équipes de sécurité fâce à **la concurrence**

Montrer la dynamique et **l'implication** sur ces sujets

Organiser un CTF en entreprise ?

Sensibilisation

Faire **comprendre par l'exemple** les enjeux de la cybersécurité

Rayonnement

Prenez le **devant de la scène** en organisant le prochain RDV sur ces sujets

Animation

Mettre en place une activité **ludique** avec une **ambiance** informelle

Technique

Challenger vos équipes sur la création d'une **infrastructure robuste** et **performante**

Métriques

Connaître ses points forts et points faibles

En résumé

1. **Pertinent pour vos équipes !**
   Partage d'expériences, découvertes de nouvelles attaques...
   Travail en équipe

2. **En interne comme en externe**
   Impliquer toutes vos équipes
   Rayonner dans le milieu de la sécurité informatique

3. **Du plaisir dans la pratique**
   Échanger dans un cadre ludique et avec une bonne ambiance

CTF best-of

(ne pas reproduire chez soi)

95% Steganographie

Recherche de pixels cachés, énigmes & devinettes

Impossible

Challenges jamais résolus et créateur absent

48h minimum

Les hackers n'ont pas besoin de dormir

Seul au monde

Dans un lieu isolé, sans eau (uniquement du redbull)

Hors ligne

Infrastructure de Schrodinger

Solutions interdites

Retrait des points si épreuves réussies de manière imprévue

Nos précieux soutiens

Et peut-être vous !

Des questions ?

Partie 2 *Qu'est-ce que l'OSINT ?*

Introduction à l'OSINT

OSINTFR.COM

CLUSIR
#Aquitaine

Qui suis je ?

Hugo Benoist

hugo@breachunt.fr

@realDumbleDork

Co-fondateur OSINT-FR
co-fondateur de BreacHunt

BREACHUNT

OSINTFR.COM

OSINT-FR en quelques mots…

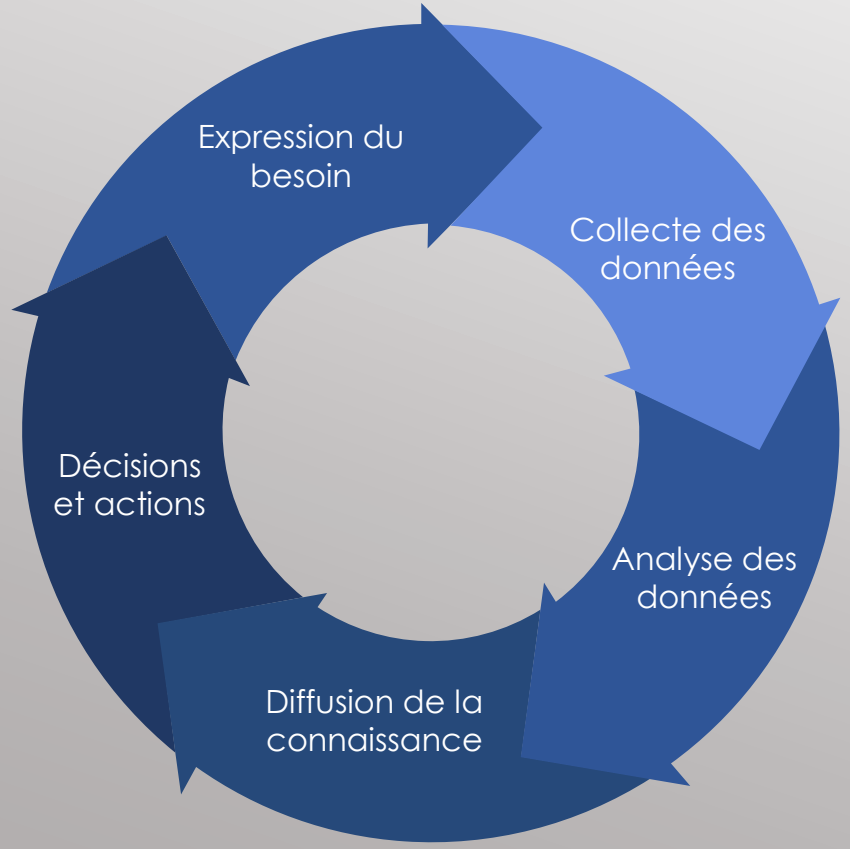
+8000 membres sur le Discord

Bientôt 4 ans d’existence

Qui se veut d’éducation populaire

Des activités variées

OSINTFR.COM



L'OSINT ?

-ROSO en Français : Renseignement d'Origine Source Ouverte

-Issue du domaine du renseignement militaire

-Partie intégrante du cycle du renseignement

OSINTFR.COM

Idée reçues sur l'OSINT

-Date de la création d'Internet => FAUX

-C'est faire du stalking => FAUX

-C'est réservé à une élite technique => FAUX

OSINT = Open Source Intelligence

OSINTFR.COM

Les différents types d’OSINT

SOCMINT (Social Media Intelligence)

IMINT (Imagery Intelligence)

GEOINT (Geospatial Intelligence)

SIGINT (Signals Intelligence)

RECON (Reconnaissance technique numérique)

Avec l’OSINT je peux :

-profiler une personne (ses goûts, habitudes, opinions…)

-cartographier le réseau d’une personne ou entité (professionnelle, amicale…)

-géolocaliser un lieu à partir d’une photo ou d’une vidéo

-désanonymiser une personne malveillante

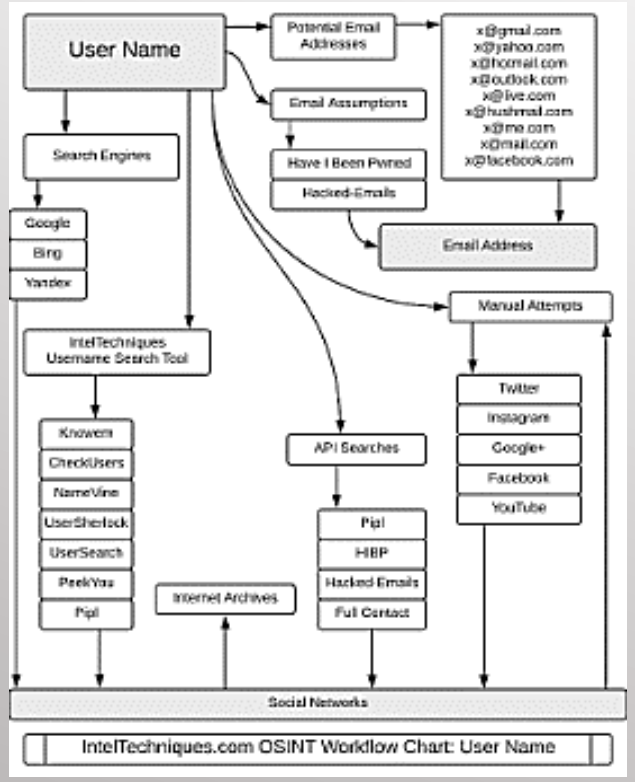
-collecter de l’information sur un concurrent (r&d, technologies internes, profiles...)

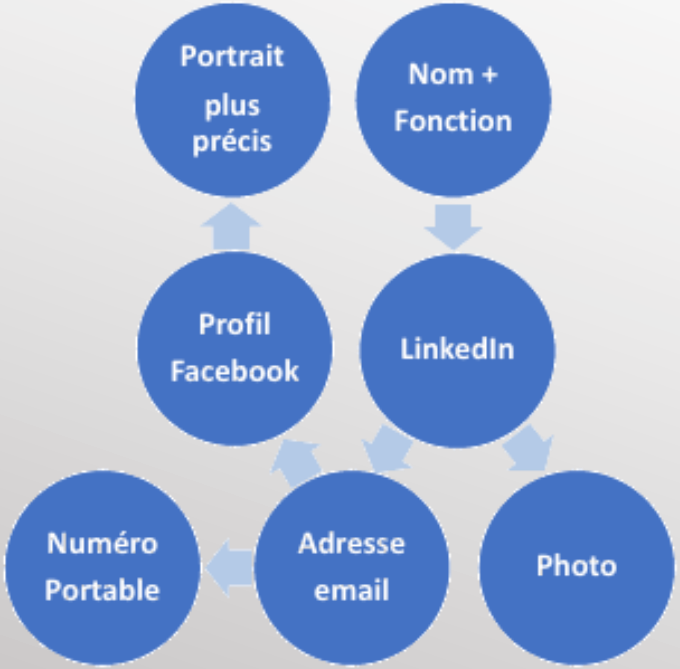
-trouver des assets techniques ou des vulnérabilités

OSINTFR.COM

Une méthodologie

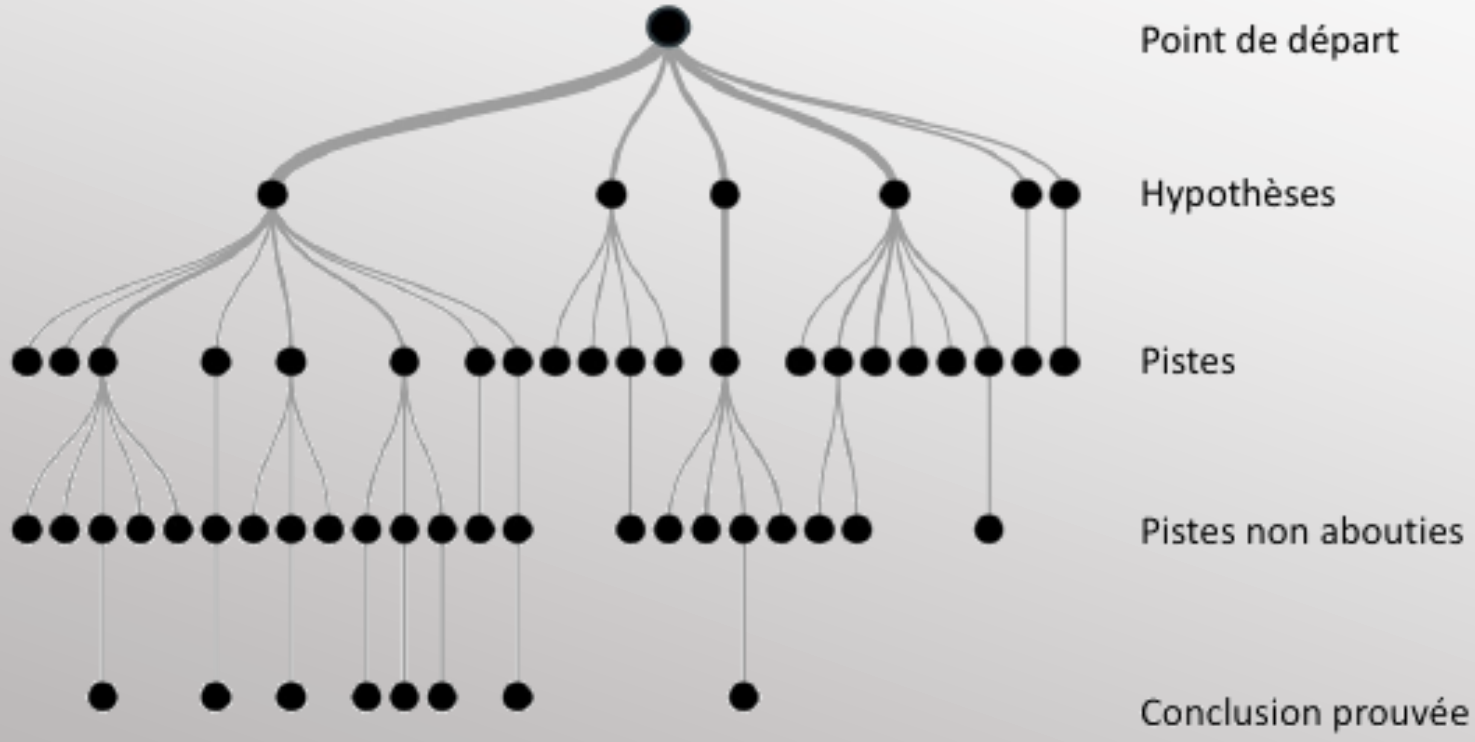
https://osintframework.com/





OSINTFR.COM

Investigation en arbre



OSINTFR.COM

Limites légales de l’OSINT

-Intrusion

-Actif

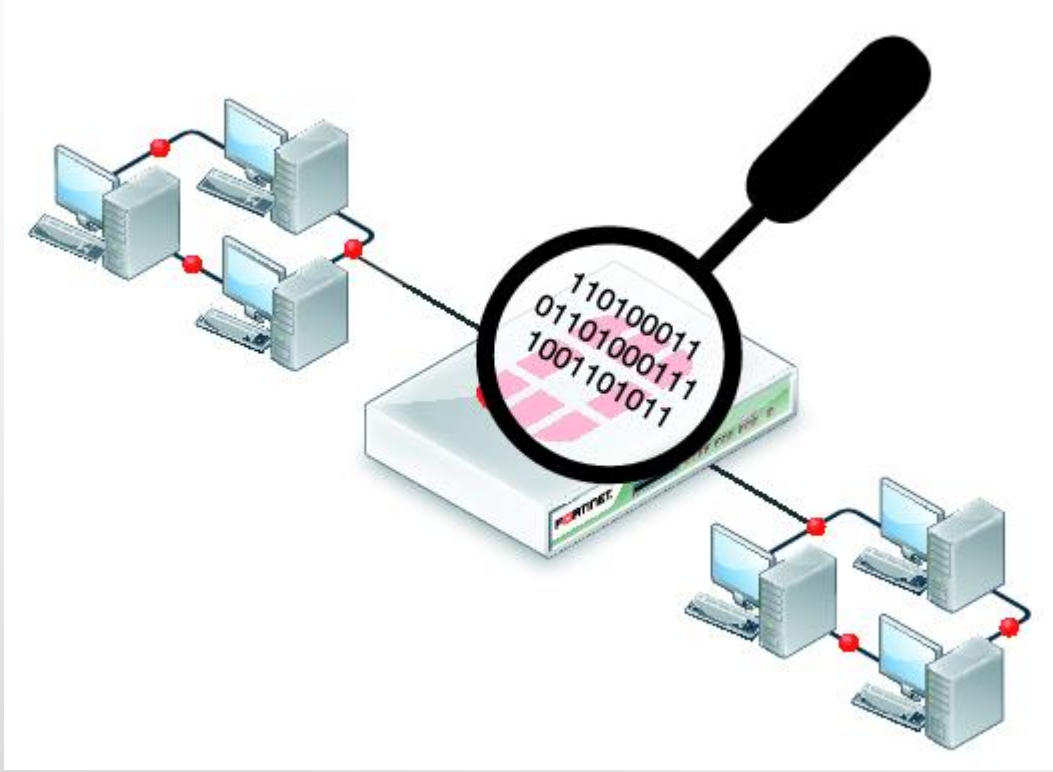
-Stalking/Doxxing

-GDPR

Jurisprudence : Affaire Bluetouff versus ANSES

OSINTFR.COM

Limites techniques de l’OSINT



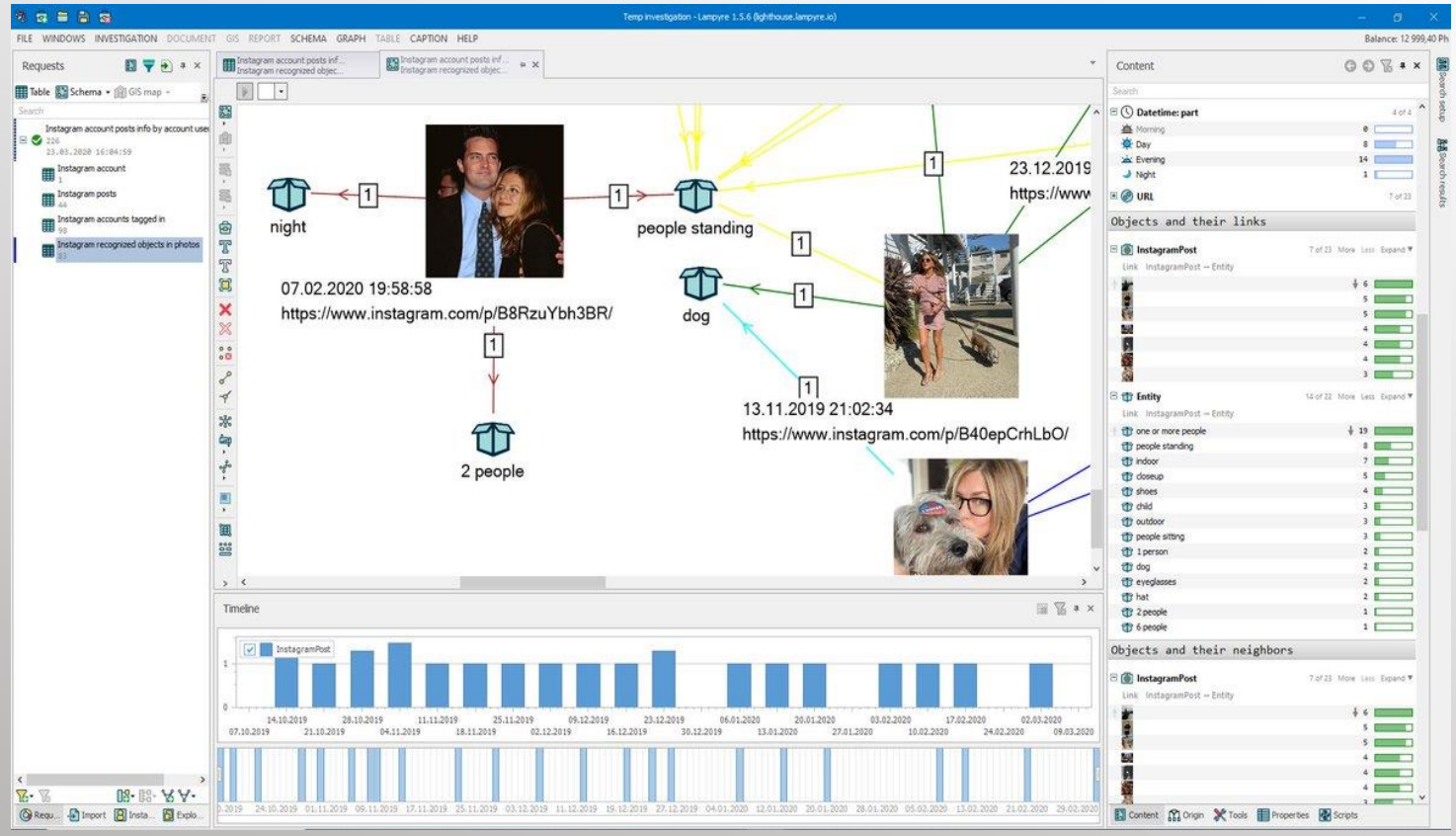
-Il n’y a pas de technique « magique » pour tout

-Attention aux outils : ce qu’ils font et qui les possèdent

OSINTFR.COM

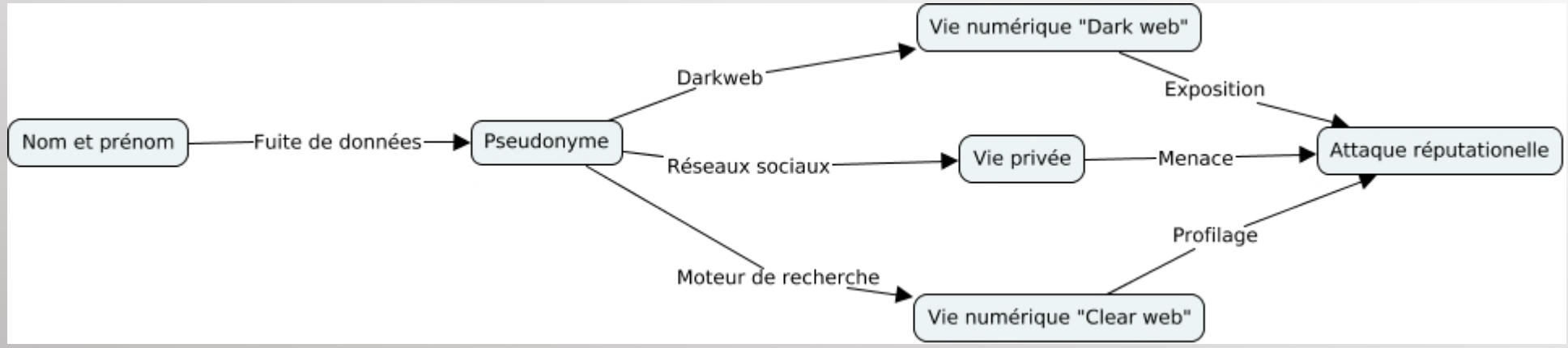
Exemple à éviter

https://lampyre.io/

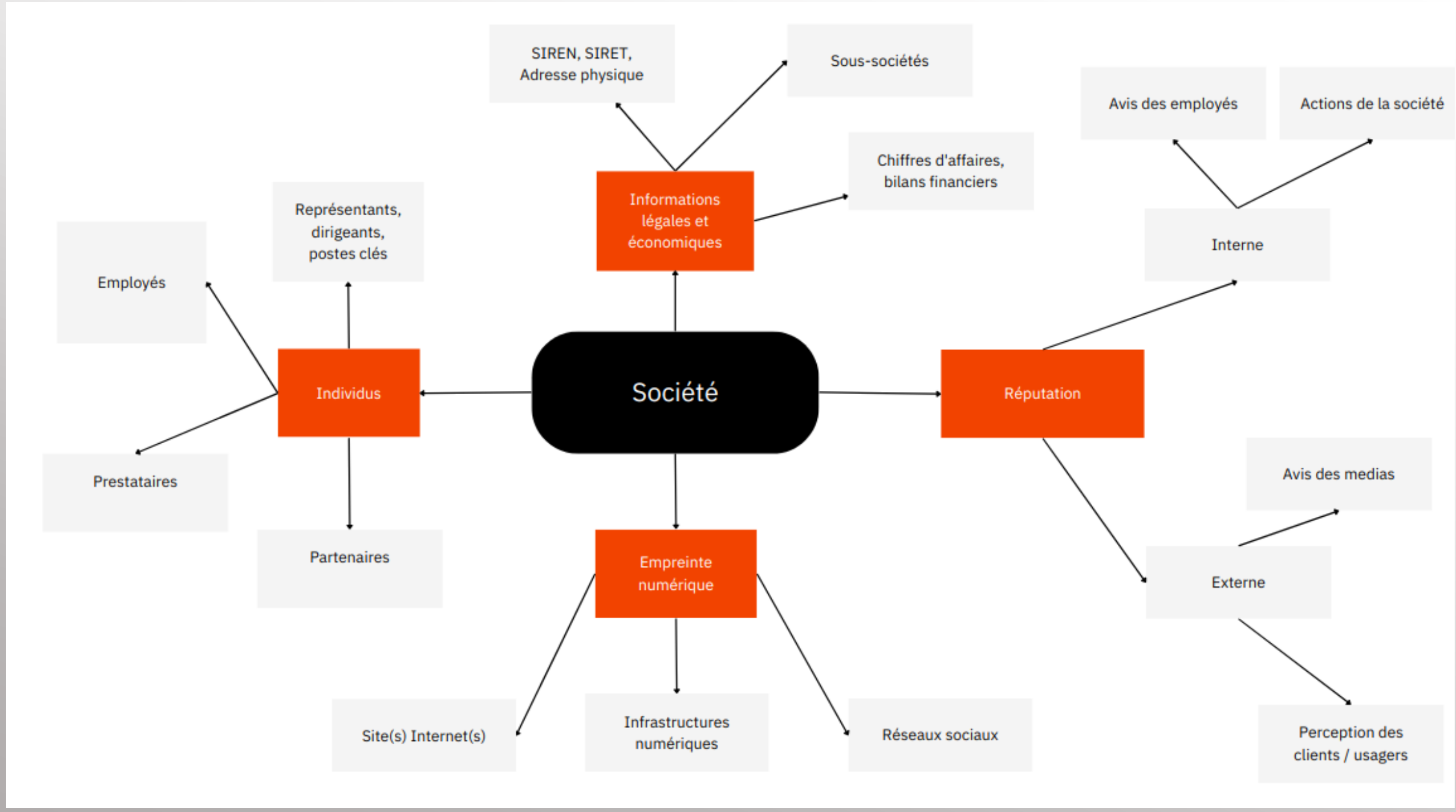


OSINTFR.COM

Investiguer sur des personnes ou des sociétés….



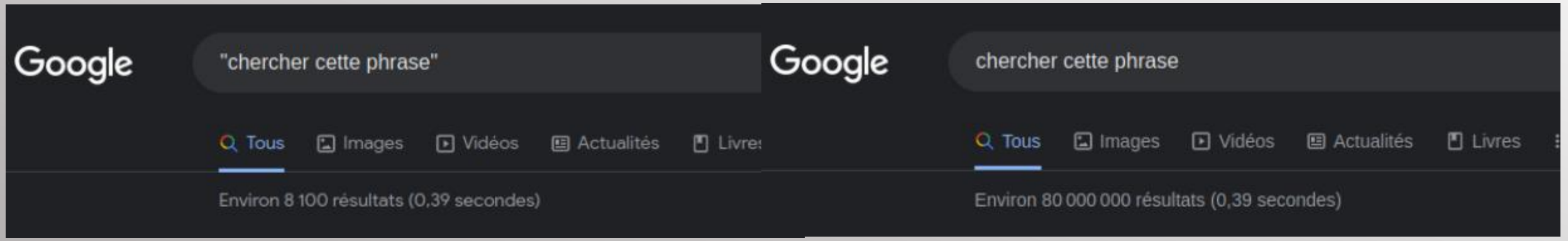
OSINTFR.COM


Société
Informations légales et économiques
SIREN, SIRET, Adresse physique
Sous-sociétés
Chiffres d'affaires, bilans financiers
Individus
Représentants, dirigeants, postes clés
Employés
Prestataires
Partenaires
Réputation
Interne
Avis des employés
Actions de la société
Externe
Avis des medias
Perception des clients / usagers
Empreinte numérique
Site(s) Internet(s)
Infrastructures numériques
Réseaux sociaux

OSINTFR.COM

OSINTFR.COM

chercher cette phrase ≠ "chercher cette phrase"



Ainsi chercher: "hugo benoist" ou "benoist hugo" ou "hugo" "benoist"

ne donnera pas les mêmes retours!

Les opérateurs via Google

site:gouvernement.fr : ne cherche que sur le site gouvernement.fr

site:gouv.fr : ne cherche que les sites ayant comme TLD gouv.fr

site:gouvernement.* cherche tous les sites nommés gouvernement avec tout type de TLD

inurl:gouvernement : cherche toutes les URL qui contiennent le terme « gouvernement »

intitle:gouvernement: cherche toutes les URL qui ont pour titre « gouvernement «

Allinurl & allintitle fonctionnent aussi !

Ext : ou Filetype : permettent de filtrer par type de fichier

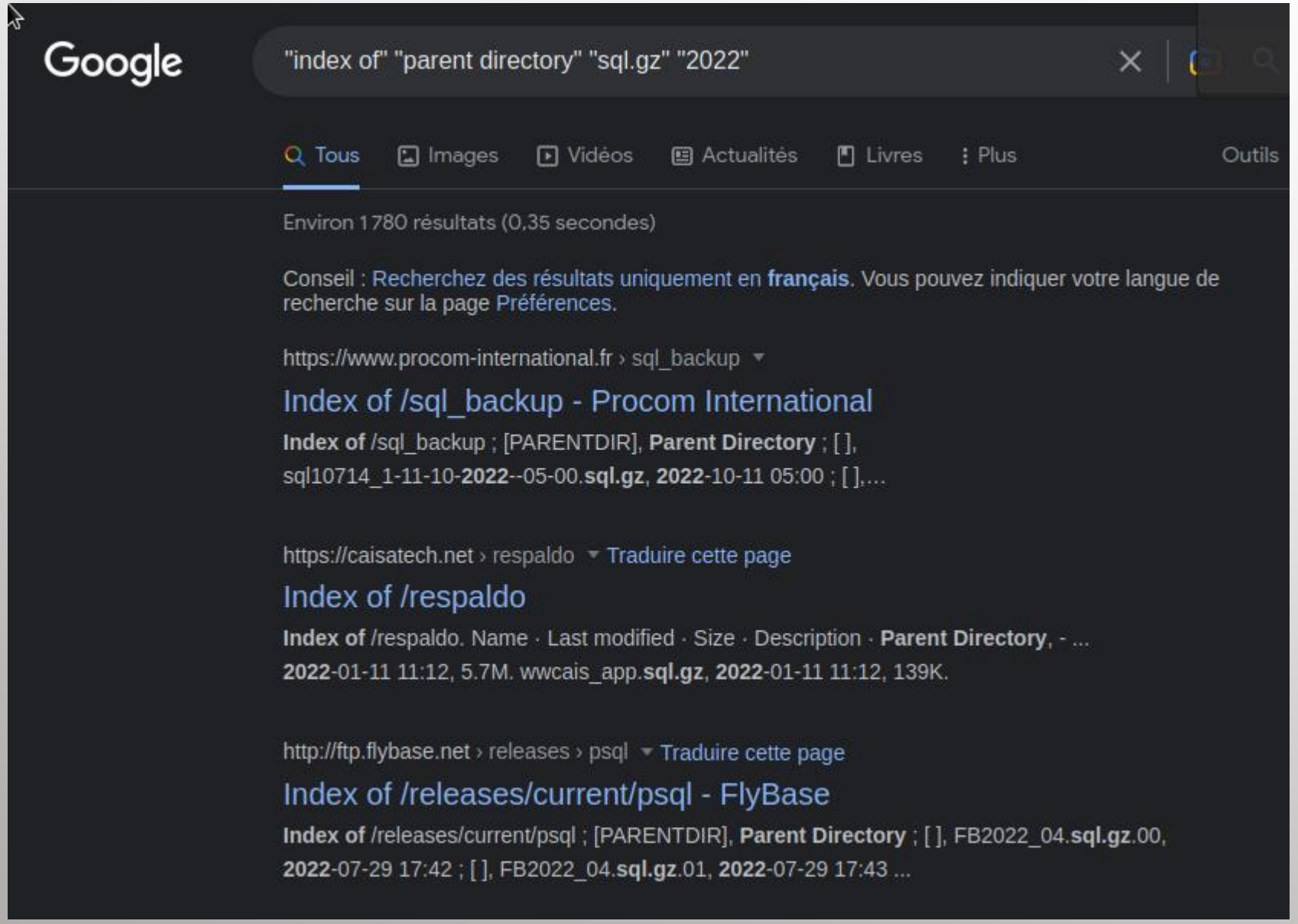
- sans oublier l’opérateur moins pour retirer certains resultats

OSINTFR.COM

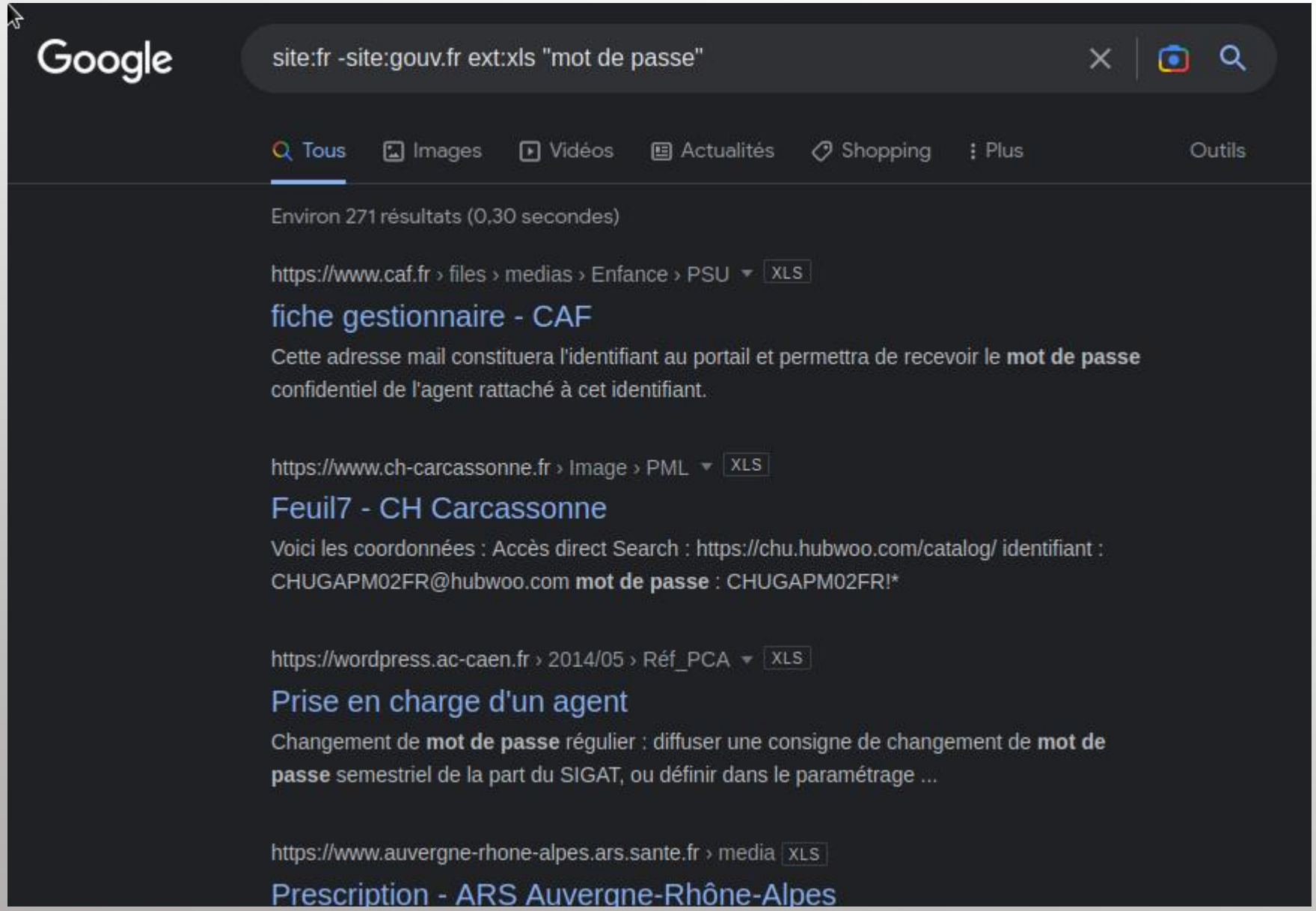
En pratique le Google « hacking » en OSINT c'est quoi ?

OSINTFR.COM

Même une surface maitrisée peut être mal gérée ou configurée



OSINTFR.COM


Google
site:fr -site:gouv.fr ext:xls "mot de passe"
Tous
Images
Vidéos
Actualités
Shopping
Plus
Outils
Environ 271 résultats (0,30 secondes)
https://www.caf.fr › files › medias › Enfance › PSU XLS
fiche gestionnaire - CAF
Cette adresse mail constituera l'identifiant au portail et permettra de recevoir le mot de passe confidentiel de l'agent rattaché à cet identifiant.
https://www.ch-carcassonne.fr › Image › PML XLS
Feuil7 - CH Carcassonne
Voici les coordonnées : Accès direct Search : https://chu.hubwoo.com/catalog/ identifiant : CHUGAPM02FR@hubwoo.com mot de passe : CHUGAPM02FR!*
https://wordpress.ac-caen.fr › 2014/05 › Réf_PCA XLS
Prise en charge d'un agent
Changement de mot de passe régulier : diffuser une consigne de changement de mot de passe semestriel de la part du SIGAT, ou définir dans le paramétrage ...
https://www.auvergne-rhone-alpes.ars.sante.fr › media XLS
Prescription - ARS Auvergne-Rhône-Alpes

Ne jamais se limiter à une seule source...

SHODAN | Explore | Downloads | Pricing | http.title:"index of" html:"backups" | Account

TOTAL RESULTS

295

TOP COUNTRIES

United States	137
Germany	37
United Kingdom	10
Netherlands	10
Singapore	9

More...

TOP PORTS

80	149
443	118
8080	10
9800	8
81	3

More...

TOP ORGANIZATIONS

Unified Layer	35
Amazon Technologies Inc	16

View Report | Download Results | Historical Trend | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Index of /

Politechnika Warszawska
Poland, Warsaw

self-signed

SSL Certificate

Vulnerabilities
FREAK
Logjam

2022-06-05T13:15:50.148131
HTTP/1.1 200 OK
Date: Sun, 05 Jun 2022 13:15:49 GMT
Server: Apache/2.2.13 (FreeBSD) PHP/5.2.11 with Suhosin-Patch DAV/2 SVN/1.6.6 mod_ssl/2.2.13 OpenS
Content-Length: 2004
Content-Type: text/html;charset=UTF-8

Index of /

NetActuate, Inc
United States, Durham

2022-06-05T12:38:42.837380
HTTP/1.1 200 OK
Date: Sun, 05 Jun 2022 12:02:23 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html

Index of /

InMotion Hosting, Inc.
United States, Washington

SSL Certificate
Issued By:
|- Common Name:

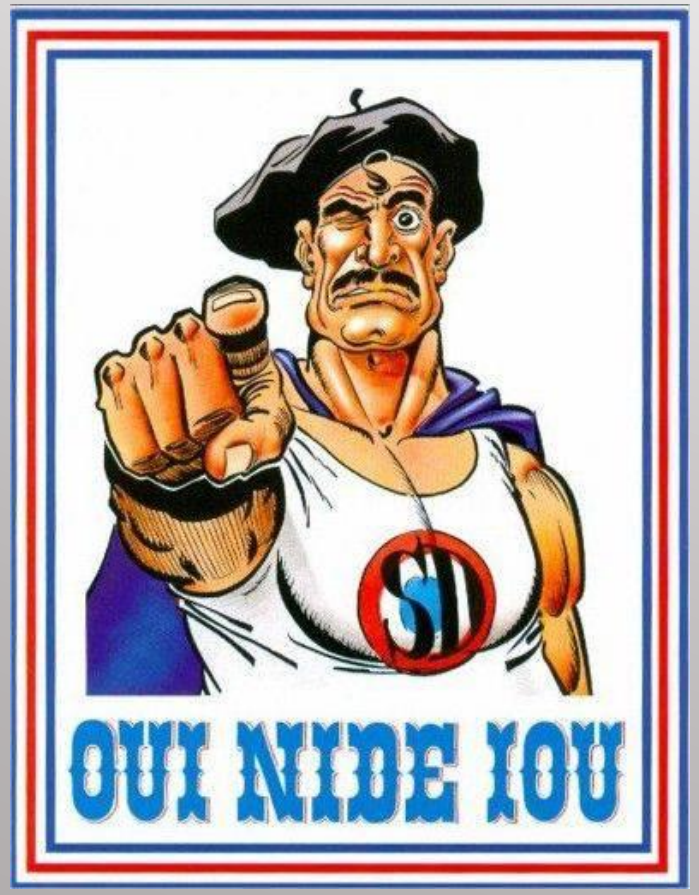
2022-06-05T12:20:20.367961
HTTP/1.1 200 OK
Date: Sun, 05 Jun 2022 12:20:20 GMT
Server: Apache
Content-Length: 1320
Content-Type: text/html;charset=ISO-8859-1

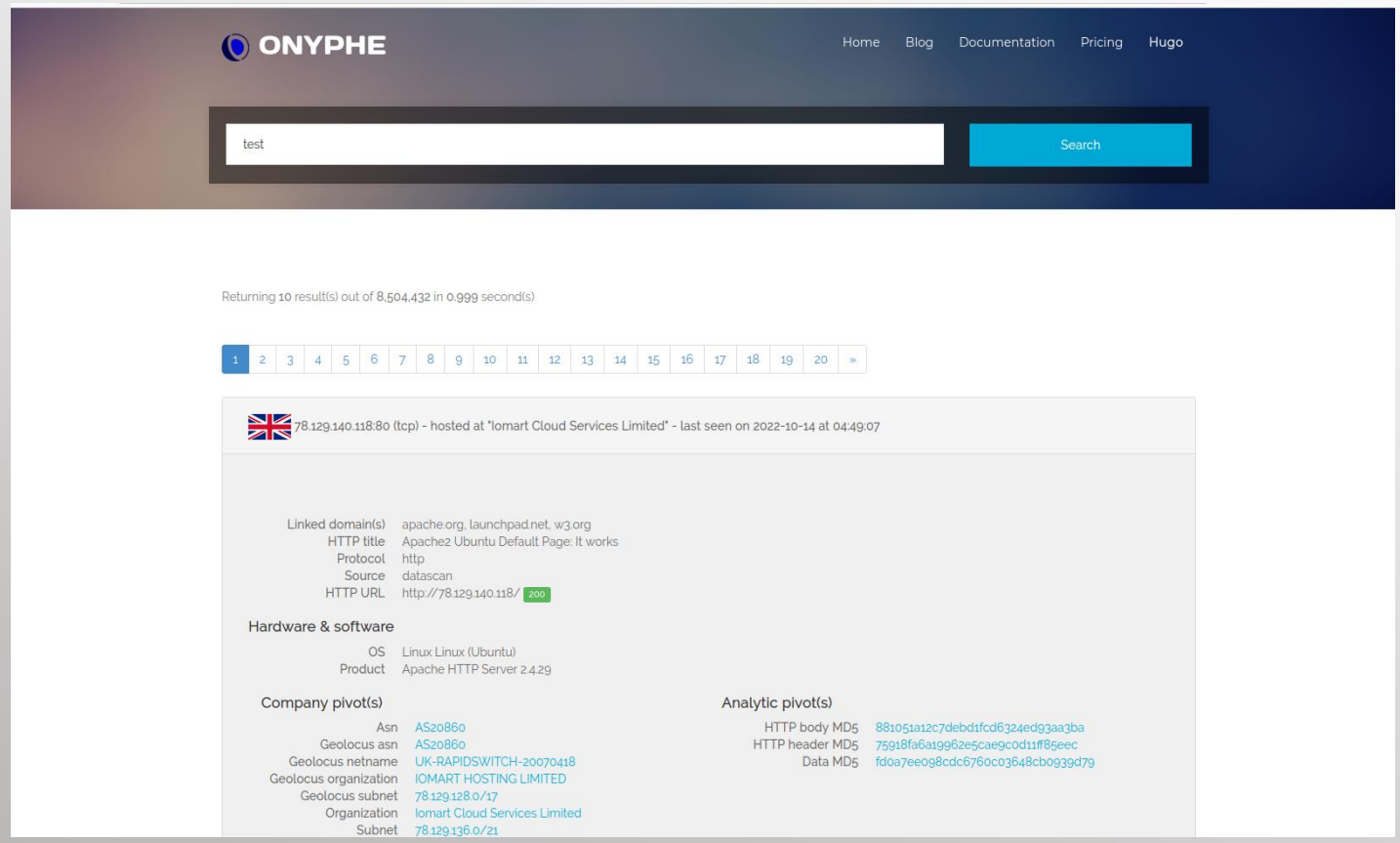

OSINTFR.COM


SIMPLY WALKS INTO MORDOR
CONVERTS ORCS
TO COMMUNISM
quickmeme.com


API
会员
登录
FOFA
试运行
Search...
查询语法
FOFA网络空间测绘 ©华顺信安 Version 4.9.144 京ICP备18024709号-2
京公网安备11010102005893号
数据更新
帮助中心
关于我们
联系我们

OSINTFR.COM


OUI NIDE IOU


ONYPHE
Home
Blog
Documentation
Pricing
Hugo
test
Search
Returning 10 result(s) out of 8,504,432 in 0.999 second(s)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 »
78.129.140.118:80 (tcp) - hosted at "Iomart Cloud Services Limited" - last seen on 2022-10-14 at 04:49:07
Linked domain(s) apache.org, launchpad.net, w3.org
HTTP title Apache2 Ubuntu Default Page: It works
Protocol http
Source datascan
HTTP URL http://78.129.140.118/ 200
Hardware & software
OS Linux Linux (Ubuntu)
Product Apache HTTP Server 2.4.29
Company pivot(s)
Asn AS20860
Geolocus asn AS20860
Geolocus netname UK-RAPIDSWITCH-20070418
Geolocus organization IOMART HOSTING LIMITED
Geolocus subnet 78.129.128.0/17
Organization Iomart Cloud Services Limited
Subnet 78.129.136.0/21
Analytic pivot(s)
HTTP body MD5 881051a12c7debd1fcd6324ed93aa3ba
HTTP header MD5 75918fa6a19962e5cae9c0d11ff85eec
Data MD5 fd0a7ee098cdc6760c03648cb0939d79

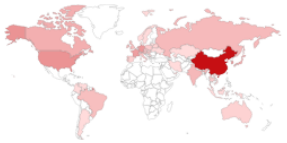
Fournisseurs, partenaires, clients… sont aussi des chemins pour vous atteindre

SHODAN | Explore | Downloads | Pricing | http.favicon.hash:573035254 | Account

TOTAL RESULTS

2,063

TOP COUNTRIES



China	1,701
United States	53
Germany	41
Korea, Republic of	37
France	32

More...

TOP PORTS

8443	851
8080	194
443	117
8888	103
80	92

More...

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	770
Tencent cloud computing (Beijing) Co., Ltd	263

View Report | Download Results | Historical Trend | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Gitblit

China, Hangzhou

2022-06-05T13:19:28.465040

SSL Certificate

Issued By:
|- Common Name:
Gitblit Certificate Authority
|- Organization:
Gitblit

Issued To:
|- Common Name:
localhost
|- Organization:
Gitblit

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2

```
HTTP/1.1 200 OK
Date: Sun, 05 Jun 2022 13:19:27 GMT
Set-Cookie: JSESSIONID=mc1kjjehv31ll4dhqcvhphim;Path=/;HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Language: zh-CN
Link: <[redacted]>; rel="canonical"
Pragma: no-cache
Cache-...
```

Gitblit

Tencent cloud computing (Beijing) Co., Ltd.
China, Shanghai

2022-06-05T13:17:08.503287

SSL Certificate

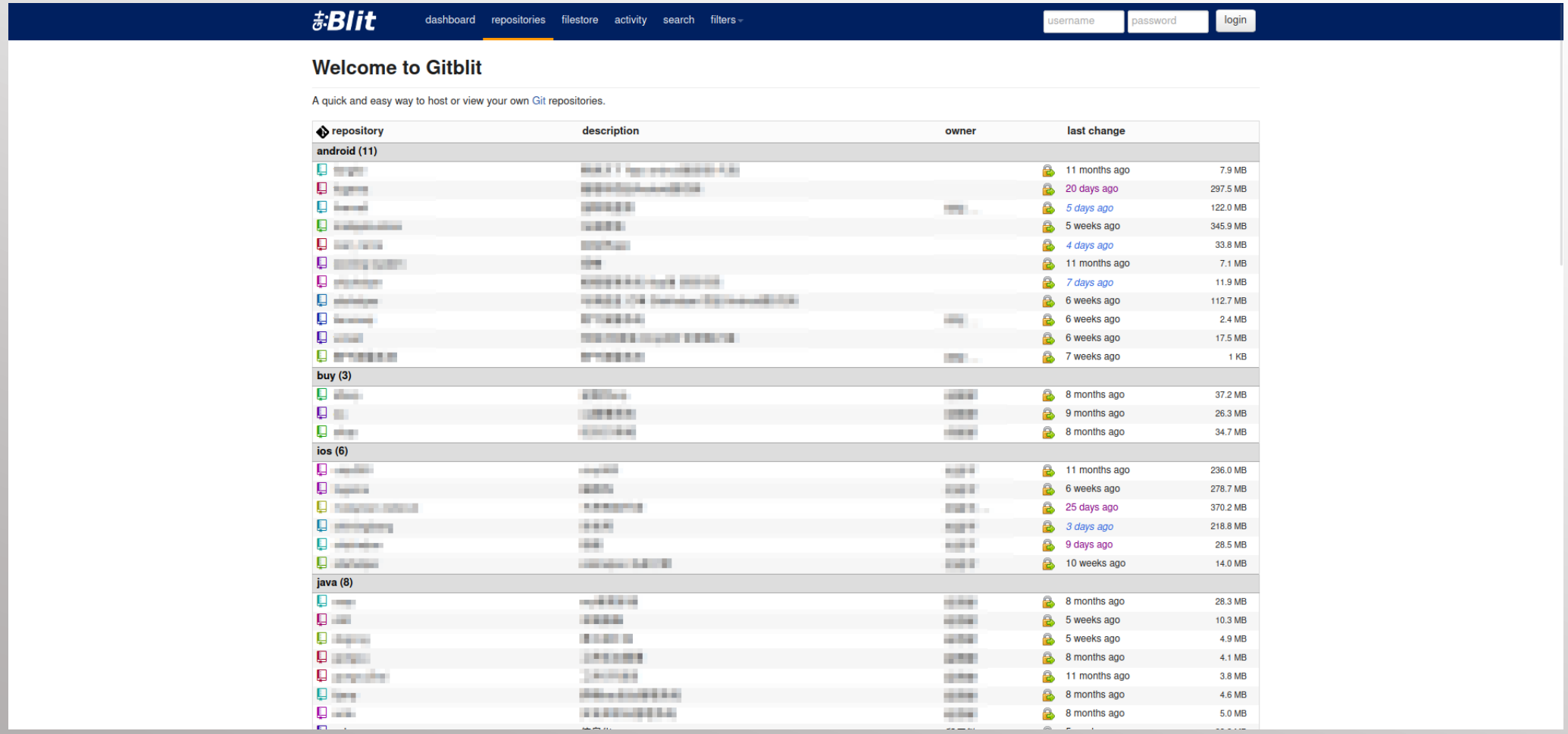
Issued By:
|- Common Name:
Gitblit Certificate Authority
|- Organization:
Gitblit

Issued To:
|- Common Name:
localhost
|- Organization:
Gitblit

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Sun, 05 Jun 2022 13:17:08 GMT
Set-Cookie: JSESSIONID=1p300txgs0umlu4dxct2f3sgc;Path=/;HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Language: zh-CN
Link: <[redacted]>; rel="canonical"
Pragma: no-cache
Cach...
```

La diversité des canaux et méthodes de compromissions sont aussi au coeur des attaques hybrides



En résumé l’OSINT est une technique puissante :

Où il est encore difficile de remplacer totalement l’humain

Qui permet de produire de l’intelligence par le pivotage et l’analyse

Avec lequel on peut protéger ses actifs, sa réputation et ses informations

Qui dans un cadre offensif, est la base des tests d’intrusions

Où il faut être vigilant sur son OPSEC , sur les outils et la méthode

Accessible à tous, mais où les experts professionnels sont peu nombreux

Hugo Benoist

hugo@breachunt.fr

@realDumbleDork

BREACHUNT

Questions ?

OSINTFR.COM

Merci de votre attention !

CLUSIR Nouvelle Aquitaine