



**INTRINSEC**  
Innovative by design

# Découverte de périmètre

Comment un hacker cartographie la surface web de votre entreprise ?

---

# Qui suis-je ?

- Promo ESIGELEC 2018
- 4 ans d'expérience en sécurité informatique
- CTF
- Bug bounty

 @aikarifb



**Florent BESNARD**

←-----→  
Consultant Red Team



# Avant de débiter

- Ne faites pas de tests « sauvages »
- Il existe des centaines d'outils
- Cette méthodologie en est une parmi tant d'autres

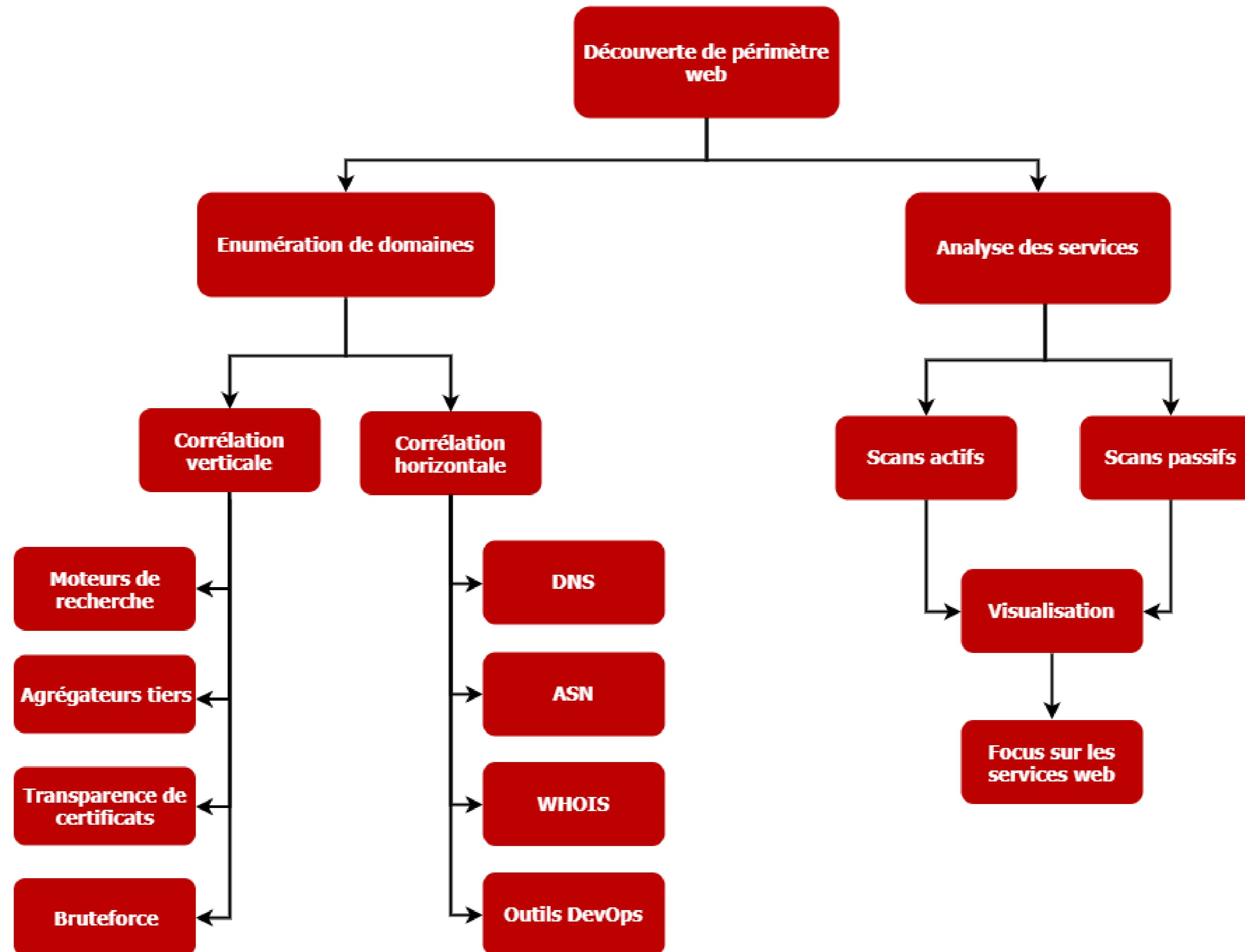


# Pourquoi faire de la « recon » ?

- Augmenter la surface d'attaque
- Obtenir des informations sur les technologies utilisées
- Identifier les vulnérabilités avant que les autres ne le fassent
- Identifier des vecteurs d'exploitation triviaux sans efforts majeurs (identifiants, infos personnelles, etc.)
- Faciliter l'exploitation, la rendre plus rapide et plus furtive (75% de recon pour 25% d'exploitation)



# Approche générale



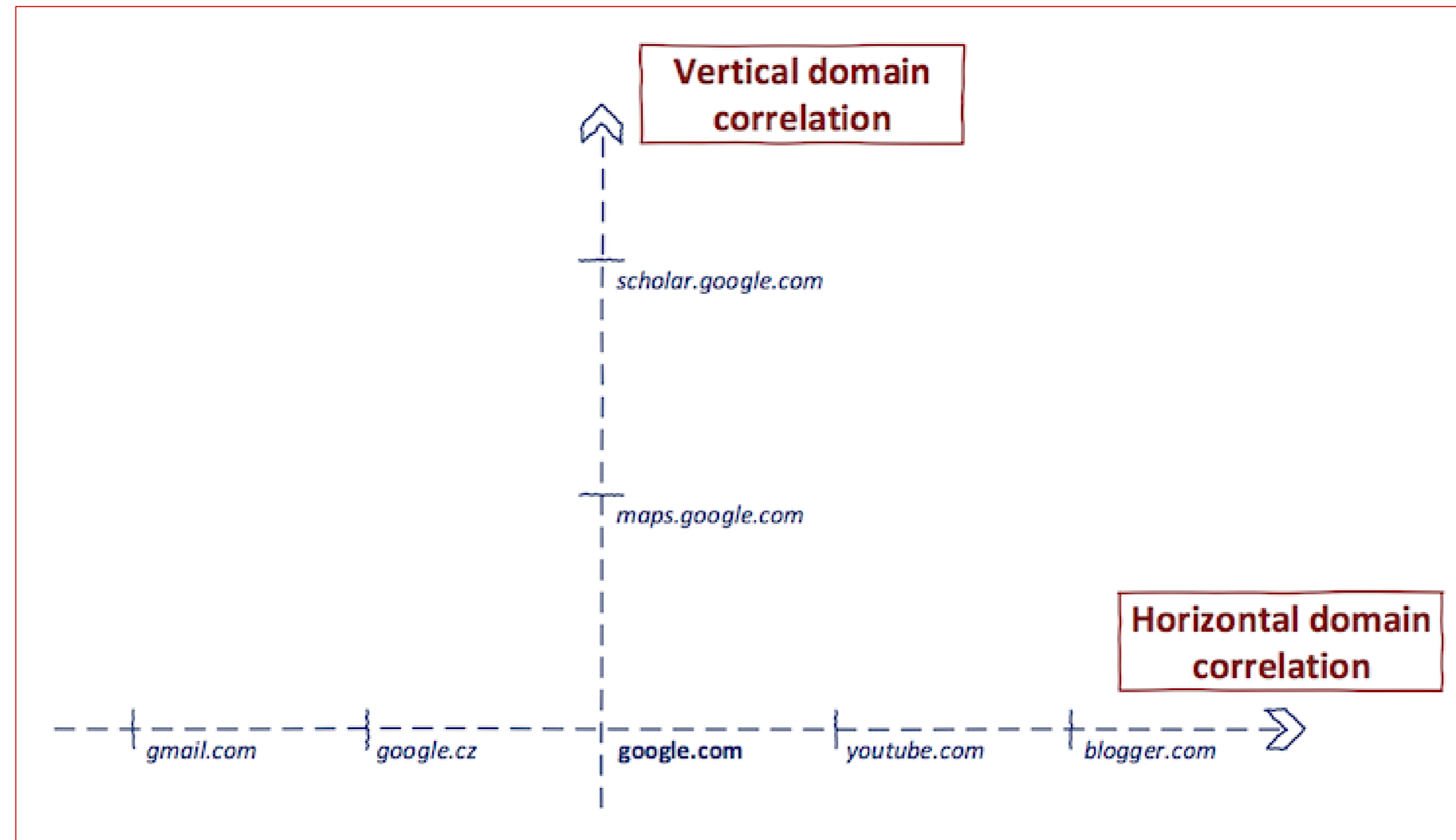
# Enumération de domaines



**INTRINSEC**  
Innovative by design

# Énumération de domaines

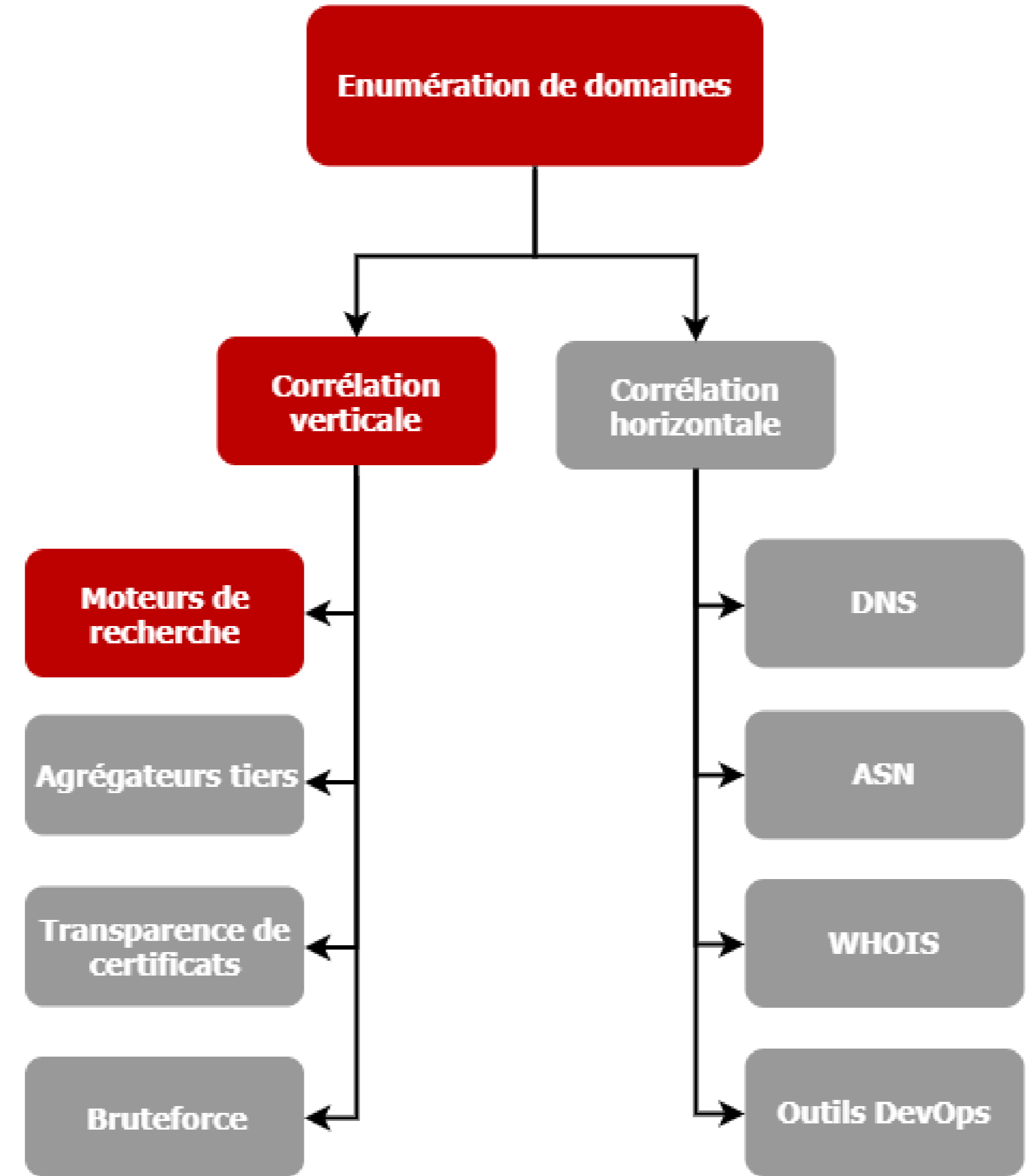
- Corrélation de domaines :
  - Verticale : identifier les domaines qui partagent le même domaine parent (simple)
  - Horizontale : identifier les domaines qui ne partagent pas le même domaine parent (complexe)



<https://0xpatrik.com/content/images/2018/04/hvv.png>



# Moteurs de recherche





# Moteurs de recherche

Google



Bing

Yandex

yahoo!



DuckDuckGo.



# Moteurs de recherche

- Outil qui permet de rechercher des ressources à partir de mots-clés
- Crawling et indexation des données (même les données sensibles !)
- Les résultats sont organisés selon une logique propre à chaque moteur
- Certains moteurs permettent l'utilisation de dorks
  
- Quelques dorks :
  - « site:google.com » : pages du domaine google.com et de ses sous-domaines
  - « site:google.com -www » : idem sans le sous-domaine www
  - « site:news.google.com ext:pdf » : fichiers PDF du domaine news.google.com
  - « site:google.com inurl:robots.txt OR intext:CHANGELOG.txt » : pages du domaine google.com et de ses sous-domaines contenant le terme robots.txt dans l'URL ou le terme CHANGELOG.txt au sein de la page
  
- Chercher les marques déposées, les copyright, les conditions d'utilisation



# Moteurs de recherche

Google

site:google.com -www

Tous Images Actualités Shopping Maps Plus Paramètres

Environ 300 000 000 résultats (0,26 secondes)

[https://store.google.com/magazine/refurbished\\_devices](https://store.google.com/magazine/refurbished_devices)  
**Refurbished Pixelbook & Google Wifi - Google Store**  
 Welcome to the Certified Refurbished program. Each product has the same high standards and rigorous testing of any device with the Google name.

<https://news.google.com/articles> Traduire cette page  
**Nhận định kết quả AFF Cup hôm nay 13/11: Indonesia vs ...**  
 13 nov. 2018 - Nhận định Indonesia vs Đông Timor, 19h00 ngày 13/11 - Dự đoán kết quả vòng bảng AFF Cup 2018 hôm nay.

<https://cloud.google.com/persistent-disk> Traduire cette page  
**Persistent Disk | Google Cloud**  
 Google Persistent Disk is durable and high performance block storage for Google Cloud Platform. Persistent Disk provides SSD and HDD storage which can be ...

ip:176.57.246.58

Tout Images Vidéos Cartes Actualités Shopping | Mes enregistre

89 Résultats Date Langue Pays

**Rouen Givrée 2019 | Rouen.fr**  
<https://www.rouen.fr/rg2019>  
 C'est déjà la 12e édition de Rouen Givrée qui se déroule du 27 novembre 2019 au 5 janvier 2020. Pendant un mois, de nombreuses animations égayeront les fêtes de fin d'année. Marché de Noël, grande roue, animations pour enfants, Grande Parade, Calendrier de "l'avant Noël"... Petits et grands trouveront leur bonheur dans la ...

**L'actualité des quartiers | Rouen ensemble**  
<https://rouenensemble.fr>  
 Un cèdre de l'Atlas a été planté dans le square avenue de la Porte des Champs, en remplacement du hêtre pourpre remarquable qui avait été retiré pour des raisons de sécurité.

**Présentation | Rouen Impressionnée**  
[www.rouenimpressionnee.fr](http://www.rouenimpressionnee.fr)  
 Pour la 3ème édition de sa triennale d'art en espace public, la Ville de Rouen propose une exposition exceptionnelle d'art urbain, aussi appelé "street art".



# Moteurs de recherche

- Lorsque des URL sont très similaires, elles peuvent être considérées comme des doublons
- Même si les contenus sont totalement différents...
- Aller sur la dernière page afin de les afficher

Google site:firebaseio.com

Tous Images Actualités Shopping Maps Plus Paramètres Outils

1 résultat (0,21 secondes)

<https://www.firebaseio.com> Traduire cette page

**Firestore**

Aucune information n'est disponible pour cette page.  
Découvrir pourquoi

*Afin d'afficher les résultats les plus pertinents, nous avons omis quelques entrées qui sont très similaires aux 1 entrées actuelles.*

*Si vous le souhaitez, vous pouvez relancer la recherche pour inclure les résultats omis.*

Google site:firebaseio.com

Tous Images Actualités Shopping Maps Plus Paramètres Outils

Environ 720 résultats (0,15 secondes)

<https://www.firebaseio.com> Traduire cette page

**Firestore**

Aucune information n'est disponible pour cette page.  
Découvrir pourquoi

<https://tutssampleapp.firebaseio.com/>

Aucune information n'est disponible pour cette page.  
Découvrir pourquoi






<https://antonioemartina2018.firebaseio.com/>

Aucune information n'est disponible pour cette page.  
Découvrir pourquoi




# Moteurs de recherche

- <https://hackerone.com/reports/644358> par @alyssa\_herrera\_

13 #644358 PII leakage-Full SSN on [REDACTED] Share:     

State ● Resolved (Closed) Severity ■ Critical (9 ~ 10)


Disclosed October 10, 2019 9:14pm +0200 Participants 

Reported To [U.S. Dept Of Defense](#) Visibility Disclosed (Full)


Weakness Insecure Storage of Sensitive Information

[Collapse](#)

SUMMARY BY ALYSSA\_HERRERA

 This was a simple Google dork search as well as checking other search engines to discover sensitive documents.

TIMELINE

 alyssa\_herrera submitted a report to [U.S. Dept Of Defense](#). Jul 16th (5 months ago)

**Summary:**  
I discovered a pdf file on [REDACTED] that outlines various information corresponding to military members. It reveals information on date of birth, where they were born, marriage status, race, children/dependents, etc

**Description:**  
I discovered what looks to be an internal file that outlines sensitive information on various service member and looks to be publicly accessible

**Impact**  
High

**Step-by-step Reproduction Instructions**  
Visit: [https://\[REDACTED\]/wp-content/uploads/2018/12/\[REDACTED\]](https://[REDACTED]/wp-content/uploads/2018/12/[REDACTED])





# Moteurs de recherche

inurl:/wp-content/uploads/2018/12/

Tous Maps Images Actuel

Environ 5 260 000 résultats (0,43 secondes)

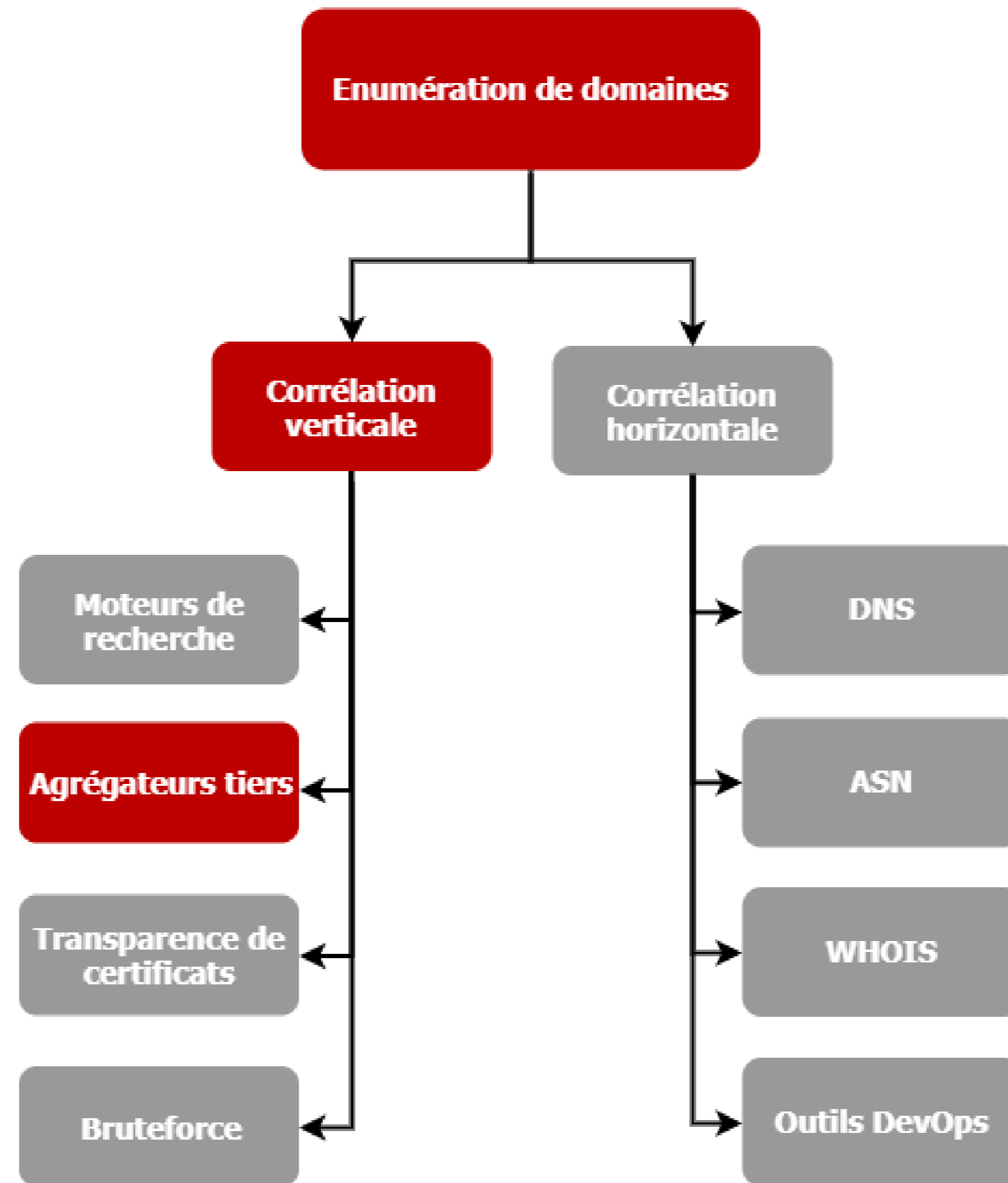
inurl:/wp-content/uploads/

Tous Images Actualités Vid

Environ 274 000 000 résultats (0,30 secondes)



# Agrégateurs tiers



# Agrégateurs tiers

- Différents outils collectent les domaines à notre place
- Données publiquement accessibles
- Résultats potentiellement invalides

## Exemple : DNSDumpster

```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)
```

google.fr ☰ ⓘ ⚡ 🌐 ✦	172.217.164.131 iad30s24-in-f3.1e100.net	GOOGLE - Google LLC United States
store.google.fr ☰ ⓘ ⚡ 🌐 ✦	216.58.193.78 sea15s07-in-f14.1e100.net	GOOGLE - Google LLC United States
cse.google.fr ☰ ⓘ ⚡ 🌐 ✦	172.217.6.46 sfo03s08-in-f46.1e100.net	GOOGLE - Google LLC United States
translate.google.fr ☰ ⓘ ⚡ 🌐 ✦	172.217.164.99 sfo03s18-in-f3.1e100.net	GOOGLE - Google LLC United States
archive.google.fr ☰ ⓘ ⚡ 🌐 ✦	216.58.194.174 sfo07s13-in-f14.1e100.net	GOOGLE - Google LLC United States
adssettings.google.fr ☰ ⓘ ⚡ 🌐 ✦	216.58.195.78 sfo07s16-in-f78.1e100.net	GOOGLE - Google LLC United States

# Agrégateurs tiers

## Exemple : VirusTotal

Enregistrements DNS, domaines (et URLs), commentaires, etc.

DETAILS	RELATIONS	COMMUNITY <span>10</span>
<b>Last DNS Records</b> ⓘ		
Record type	TTL	Value
A	299	172.217.212.101
A	299	172.217.212.113
A	299	172.217.212.138
A	299	172.217.212.102
A	299	172.217.212.100
A	299	172.217.212.139
AAAA	299	2607:f8b0:4001:c03::65
+ CAA	21599	pki.goog
+ MX	599	alt2.aspmx.l.google.com
+ MX	599	alt1.aspmx.l.google.com

DETAILS	RELATIONS	COMMUNITY <span>10</span>	
<b>Passive DNS Replication</b> ⓘ			
Date resolved	IP		
2019-12-09	216.58.204.142		
2019-12-09	216.58.209.238		
2019-12-09	216.58.213.174		
2019-12-09	172.217.22.142		
2019-12-09	172.217.20.206		
2019-12-09	172.217.19.238		
2019-12-09	172.217.1.110		
2019-12-09	108.177.111.102		
2019-12-09	108.177.111.138		
2019-12-09	108.177.111.139		
...			
<b>Subdomains</b> ⓘ			
crowdsourc...google.com	172.217.212.139	172.217.212.101	172.217.212.100
mt1.google.com	108.177.111.138	108.177.111.113	108.177.111.101
enterprise.google.com	74.125.202.102	74.125.202.139	74.125.202.101
images.google.com	172.217.214.100	172.217.214.101	172.217.214.138
domains.google.com	108.177.120.113	108.177.120.138	108.177.120.139
events.google.com	209.85.146.102	209.85.146.113	209.85.146.139
confidential-mail.google.com	108.177.112.139	108.177.112.138	108.177.112.113
apps.google.com	172.217.219.113	172.217.219.139	172.217.219.100
dl-ssl.google.com	74.125.201.190	74.125.201.93	74.125.201.91
ipv4.google.com	74.125.126.113	74.125.126.102	74.125.126.138

**uhhhwhat**

6 months ago

google spies on u bad site

---

**VirusTotalVul**

1 year ago

Official google website.

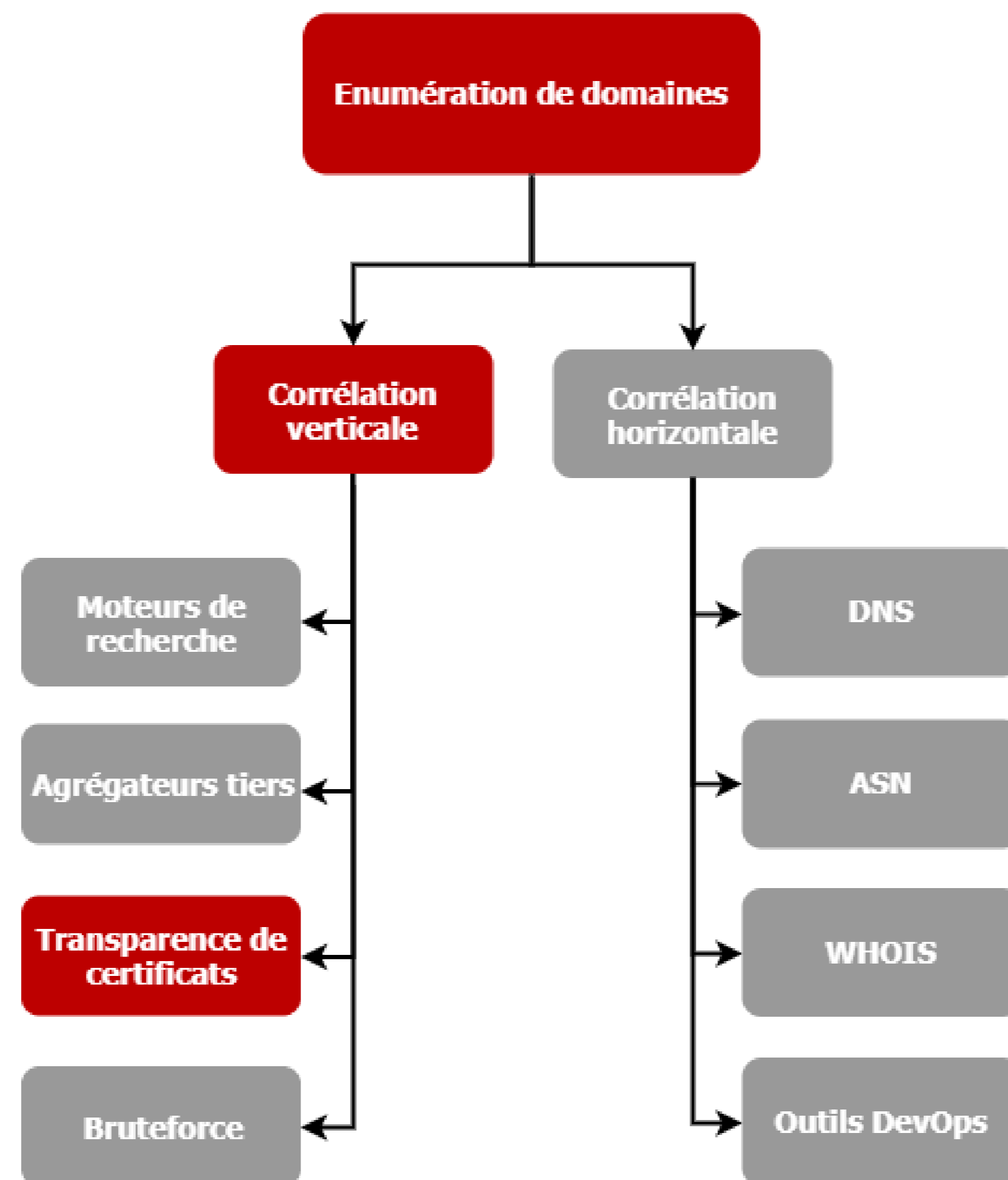
---

**danielva**

1 year ago

test

# Transparence de certificats





# Transparence de certificats

- En 2011, l'autorité de certification DigiNotar est compromise
- Renforcer les contrôles sur les certificats émis par les autorités de certification
- Déceler les certificats frauduleux ou invalides
- Accessible par tous

## Exemple : crt.sh & certspotter.com

Criteria Identity LIKE '%.rouen.fr'					
crt.sh ID	Logged At ↑	Not Before	Not After	Identity	Issuer Name
<a href="#">2102637471</a>	2019-11-12	2019-11-12	2022-02-06	autodiscover.rouen.fr	<a href="#">C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA</a>
<a href="#">2102637471</a>	2019-11-12	2019-11-12	2022-02-06	mail.rouen.fr	<a href="#">C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA</a>
<a href="#">2102637419</a>	2019-11-12	2019-11-12	2022-02-06	autodiscover.rouen.fr	<a href="#">C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA</a>
<a href="#">2102637419</a>	2019-11-12	2019-11-12	2022-02-06	mail.rouen.fr	<a href="#">C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA</a>
<a href="#">2064836816</a>	2019-11-02	2019-11-02	2020-01-31	*.demarches.rouen.fr	<a href="#">C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3</a>
<a href="#">2064836816</a>	2019-11-02	2019-11-02	2020-01-31	demarches.rouen.fr	<a href="#">C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3</a>

```

user@server:~$ curl -s "https://certspotter.com/api/v0/certs?domain=rouen.fr" | jq '.[].dns_names[]' | sed 's/\"//g'
| sed 's/*\"//g' | sort -u
ad-mairie.rouen.fr
autodiscover.ad-mairie.rouen.fr
autodiscover.rouen.fr
demarches.rouen.fr
hdvmsg30.ad-mairie.rouen.fr
mail.rouen.fr
rouen.fr

```

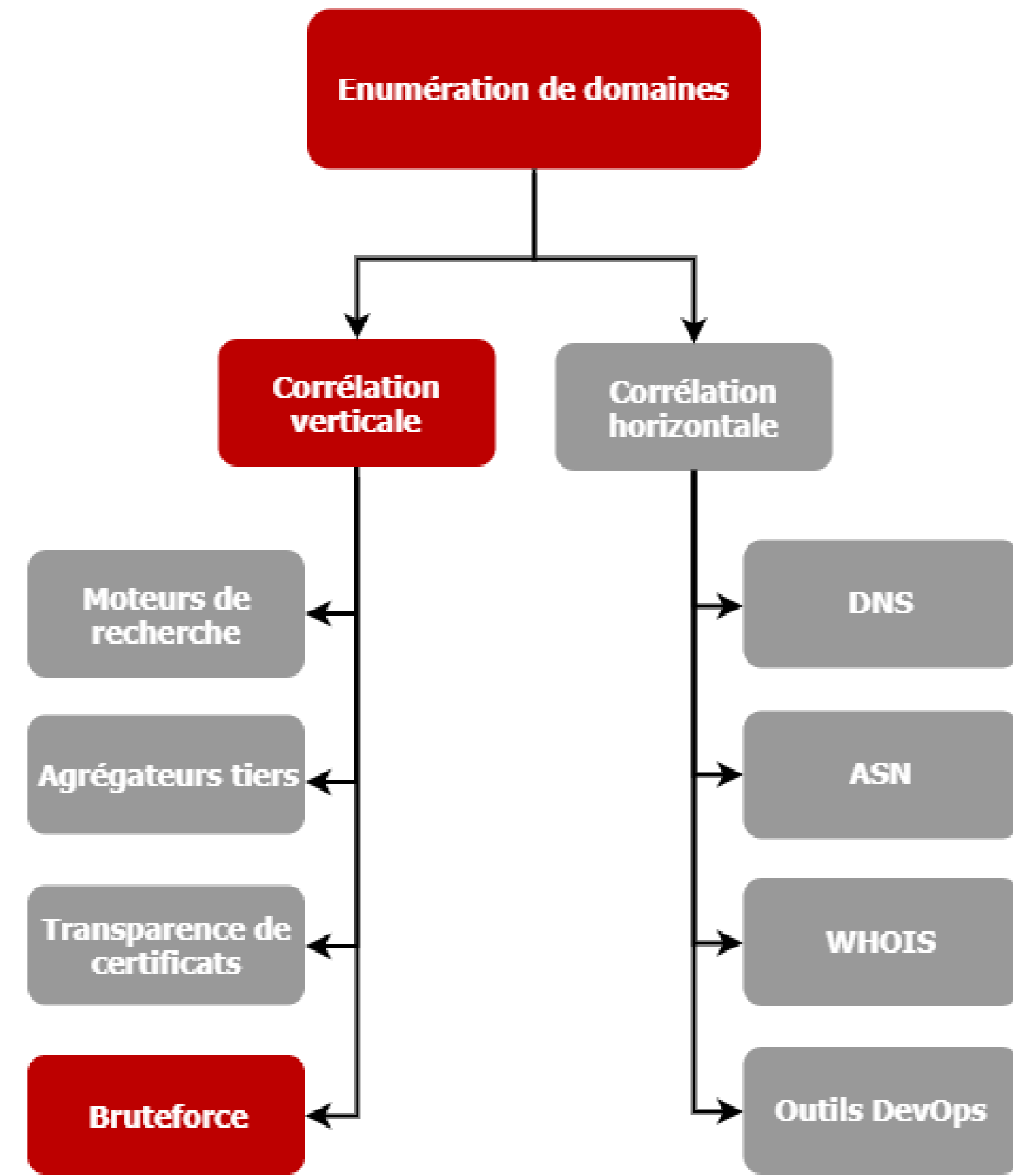
# Transparence de certificats

Exemple : certstream

```
$ certstream
```



# Bruteforce



# Bruteforce

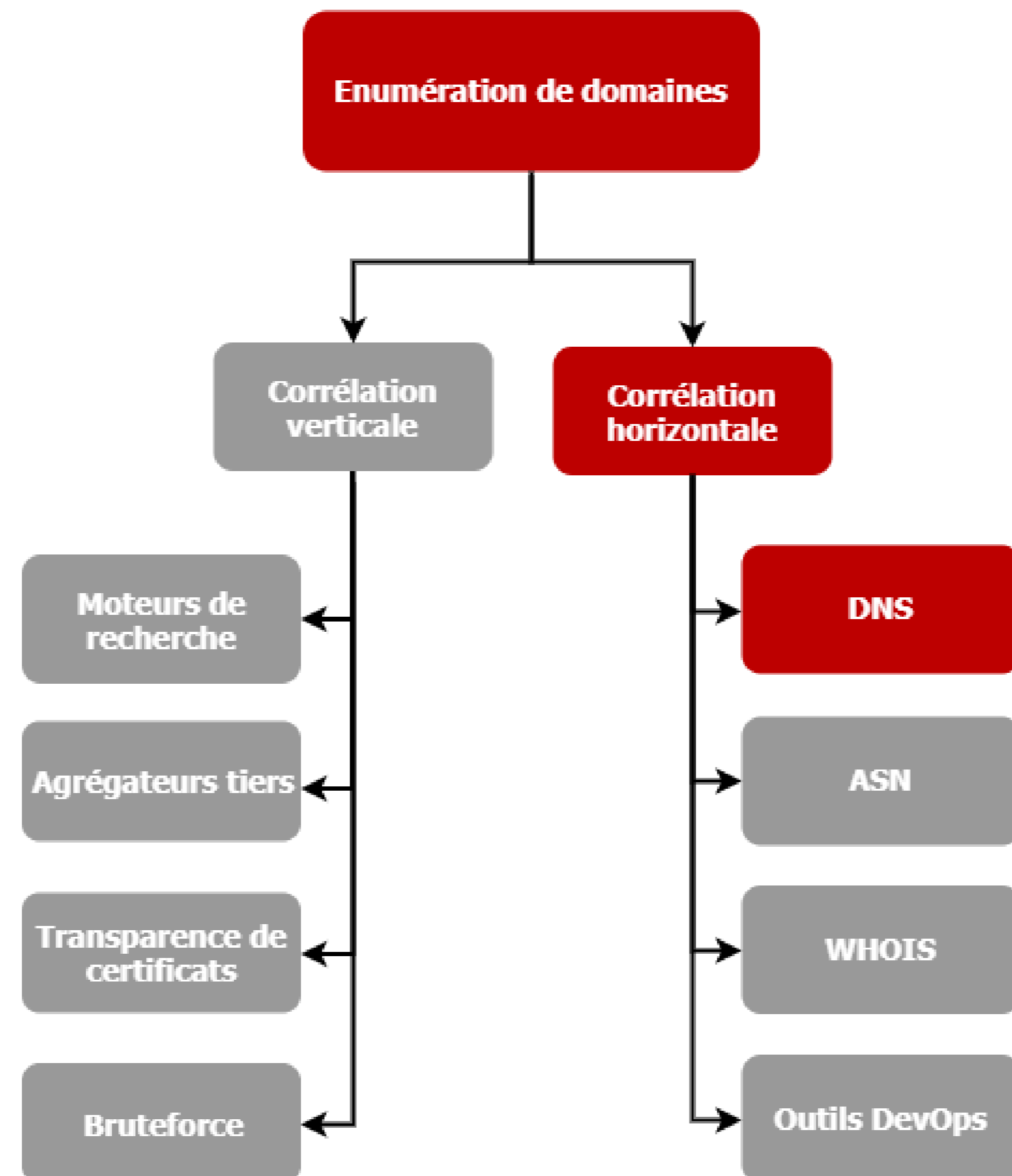
- De nombreux dictionnaires disponibles
- Utiliser des permutations

Exemple : aiodnsbrute & all.txt (@jhaddix)

```
user@server:~$ aiodnsbrute -w Wordlists/all.txt -t 1024 intrinsec.com
[*] Brute forcing rouen.fr with a maximum of 1024 concurrent tasks...
[*] Using local resolver to verify intrinsec.com exists.
[*] Using recursive DNS with the following servers: ['127.0.0.53']
[*] No wildcard response was detected for this domain.
[*] Wordlist loaded, proceeding with 1136964 DNS requests
[+] forms.intrinsec.com           ['93.187.41.210']
[+] formulaire.intrinsec.com     ['93.187.40.195']
[+] ftp.intrinsec.com            ['93.187.40.198']
[+] FTP.intrinsec.com            ['93.187.40.198']
[+] fuji.intrinsec.com           ['93.187.43.198']
[+] gapps.intrinsec.com          ['93.187.40.195']
[+] ged.intrinsec.com            ['194.6.240.6']
[+] googleapps.intrinsec.com     ['93.187.40.195']
[+] himalaya.intrinsec.com       ['54.36.216.202']
[+] horizon.intrinsec.com        ['93.187.40.74']
```

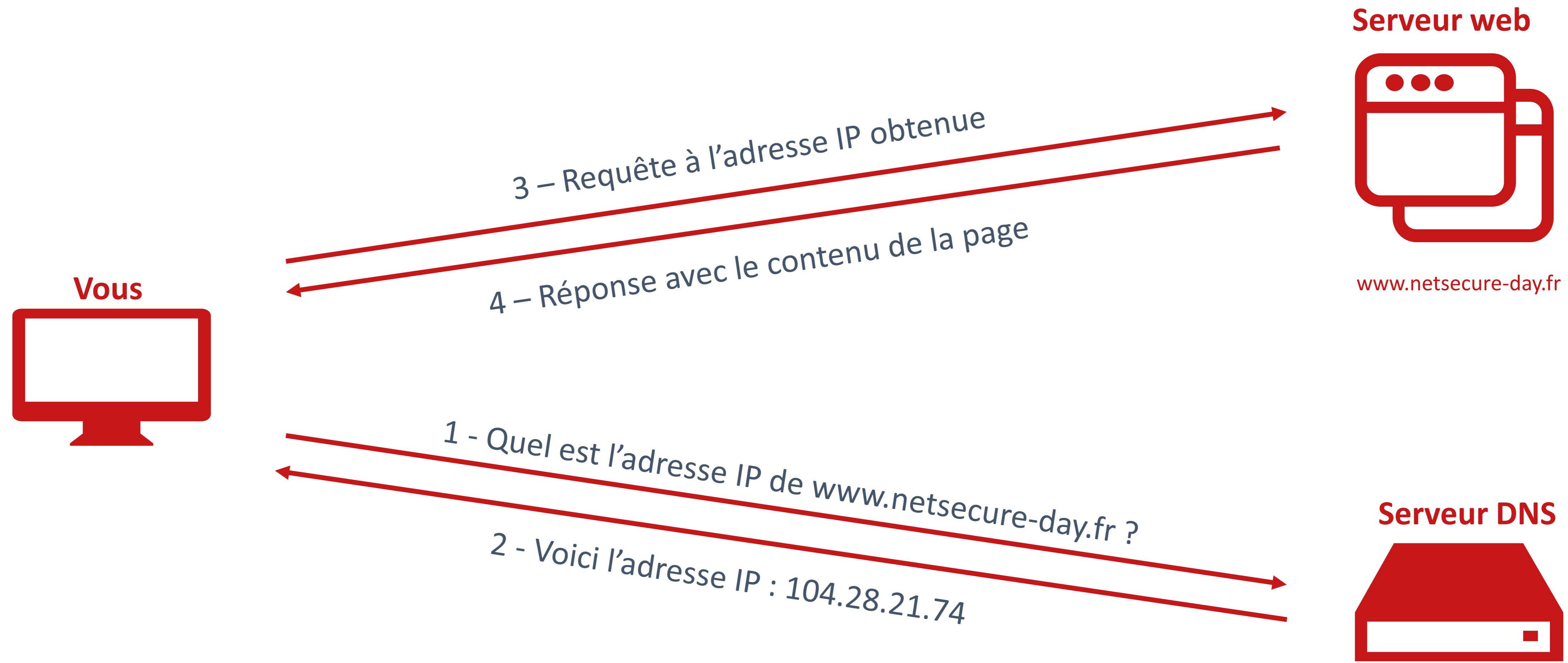


# DNS





# DNS



# DNS

- Transfert de zone
- Réplication des enregistrements entre serveurs DNS
- Permet de récupérer tous les noms de domaines associés

## Exemple : host

```
user@server:~$ host -l zonetransfer.me nsztml.digi.ninja
Using domain server:
Name: nsztml.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztml.digi.ninja.
zonetransfer.me name server nsztml2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
```



# DNS

## Exemple : dig

```
user@server:~$ dig axfr @nsztml.digi.ninja zonetransfer.me

; <<>> DiG 9.10.3-P4-Debian <<>> axfr @nsztml.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.      7200    IN      SOA     nsztml.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600
3600
zonetransfer.me.      301     IN      TXT     "google-site-
verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.      7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.      7200    IN      A       5.196.105.14
zonetransfer.me.      7200    IN      NS      nsztml.digi.ninja.
_sip._tcp.zonetransfer.me. 14000  IN      SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200  IN      PTR     www.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
dc-office.zonetransfer.me. 7200  IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
email.zonetransfer.me. 7200    IN      A       74.125.206.26
home.zonetransfer.me. 7200    IN      A       127.0.0.1
internal.zonetransfer.me. 300     IN      NS      intns1.zonetransfer.me.
```



# DNS

- Enregistrement PTR
- Enregistrement « à l'envers » : associe une adresse IP à un nom d'hôte
- Utile pour les serveurs de messagerie sortants



```
user@server:~$ host -l zonetransfer.me nsztml.digi.ninja
Using domain server:
Name: nsztml.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztml.digi.ninja.
zonetransfer.me name server nsztml2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
```





# DNS

- Sender Policy Framework (SPF)
- Norme de vérification du nom de domaine de l'expéditeur d'un mail
- Combattre l'usurpation de domaines légitimes
- Utile pour déterminer des adresses IP appartenant à une entreprise

Mécanisme	Description
ALL	Correspond à tout
A	Adresse IP dans enregistrement A ou AAAA
IP4	Adresse IP dans plage IPv4
IP6	Adresse IP dans plage IPv6
MX	Adresse IP dans enregistrement MX
PTR	Adresse IP dans enregistrement A du domaine indiqué dans l'enregistrement PTR
EXISTS	Si le domaine est résolu
INCLUDE	Si le domaine correspond



# DNS

- Sender Policy Framework (SPF)
- Norme de vérification du nom de domaine de l'expéditeur d'un mail
- Combattre l'usurpation de domaines légitimes
- Utile pour déterminer des adresses IP appartenant à une entreprise

Qualifieurs	Description
+	Résultat favorable
?	Résultat neutre
~	Léger échec
-	Echec total





# DNS

## Exemple : rouen.fr



```
user@server:~$ dig TXT rouen.fr
rouen.fr.          1800    IN      TXT     "v=spf1 ip4:46.218.136.21
ip4:46.218.136.22 ip4:176.57.246.58 include:spf.protection.outlook.com -all"
```







```
user@server:~$ whois 176.57.246.58

inetnum:          176.57.246.56 - 176.57.246.59
netname:          VILLE_DE_ROUEN
descr:           VILLE_DE_ROUEN
country:         FR
```



# DNS

- Projet SONAR de Rapid7
- Récupération d'une large liste de domaines : dumps TLD zone files, parsing HTTP, certificats SSL, etc.
- Scan actifs de l'ensemble d'Internet (IPv4)
  
- Forward DNS :
  - Pour chaque domaine, récupération des enregistrements DNS : A, AAAA, NS, MX, TXT et CNAME.
- Reverse DNS :
  - Pour chaque domaine, récupération de l'enregistrement DNS PTR

File Name	SHA1-Fingerprint	Size	Updated At
<a href="#">2019-11-29-1574985929-fdns_a.json.gz</a>	0e8cfa1263fef9741af18622ef4773cd03e9d908 	19.7 GB	Nov. 30, 2019
<a href="#">2019-11-29-1574985803-fdns_aaaa.json.gz</a>	c0aa6bc7f22b5203da10ba2250d8b33922f9776c 	1.6 GB	Nov. 30, 2019
<a href="#">2019-11-25-1574640596-fdns_cname.json.gz</a>	500b40dac3b1ae95887c7678665d7b4107981359 	2.2 GB	Nov. 25, 2019
<a href="#">2019-11-23-1574520243-fdns_any.json.gz</a>	e27c1e584ad487dc836a5117ee6945ffc6b775d3 	30.7 GB	Nov. 25, 2019



# Bonus / HS – Subdomain takeover

- <https://hackerone.com/reports/383564> par blurbdust

31

#383564

**Subdomain takeover on svcgatewaydevus.starbucks.com and svcgatewayloadus.starbucks.com**

Share: [f](#) [t](#) [in](#) [v](#) [e](#)

---

State ● [Resolved \(Closed\)](#)

Disclosed **July 23, 2018 7:45pm +0200**

Reported To [Starbucks](#)

Weakness **Privilege Escalation**

Bounty **\$4,000**

Severity Critical (9 ~ 10)

Participants

Visibility [Disclosed \(Full\)](#)

---

TIMELINE

[blurbdust](#) submitted a report to [Starbucks](#).

Hello,

Two starbucks.com subdomains are pointed to Azure with an unclaimed CNAME record. Anyone would be able to serve content on these subdomains.

**svcgatewayloadus.starbucks.com**

```

;; Server: 1.1.1.1:53
;; Size: 191
;; Unix time: 1531965036
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 3697
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

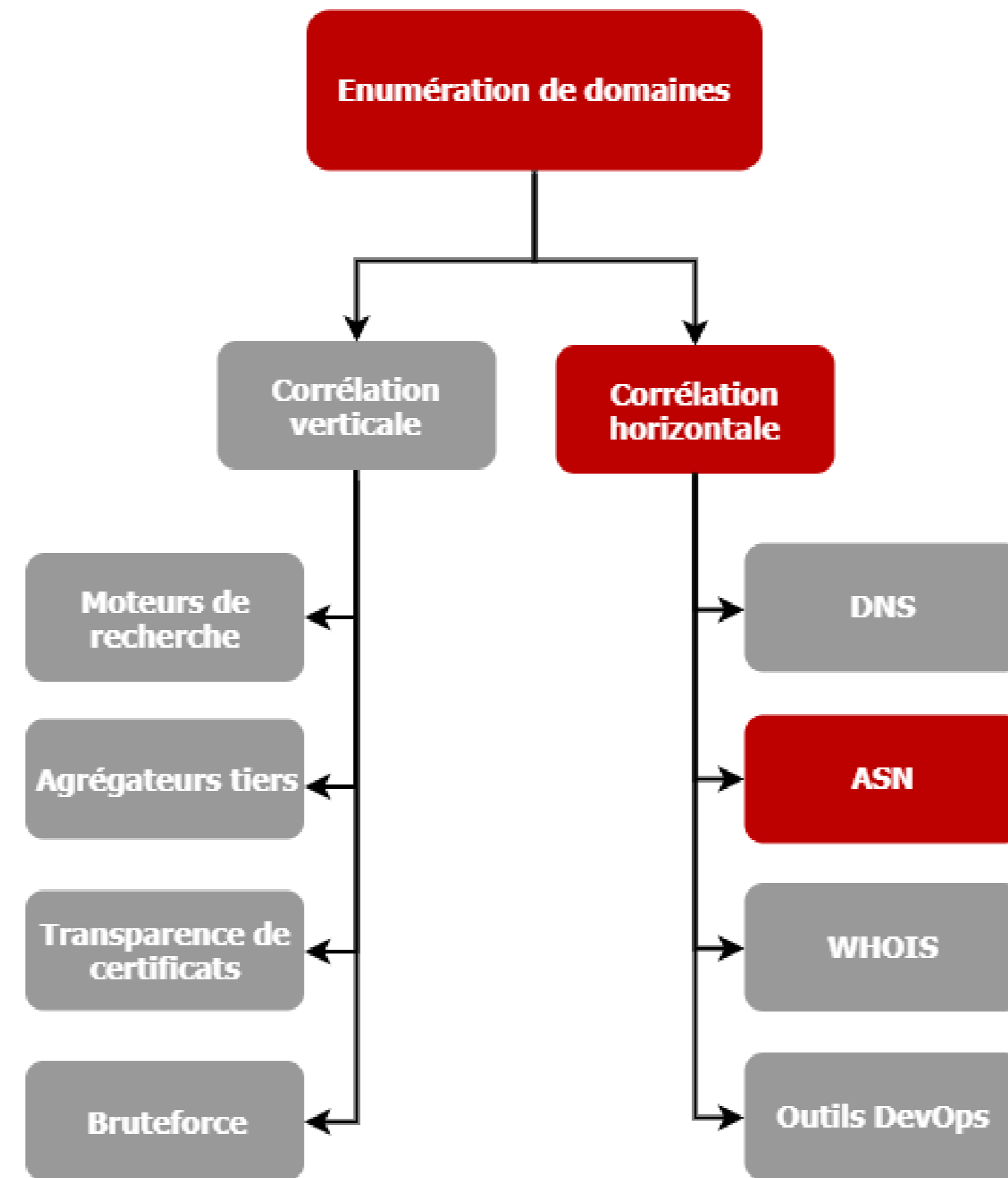
;; QUESTION SECTION:
svcgatewayloadus.starbucks.com. IN A

;; ANSWER SECTION:
svcgatewayloadus.starbucks.com. 600 IN CNAME s00197tmp@crdfulload0.trafficmanager.net.
```

Jul 19th (about 1 year ago)

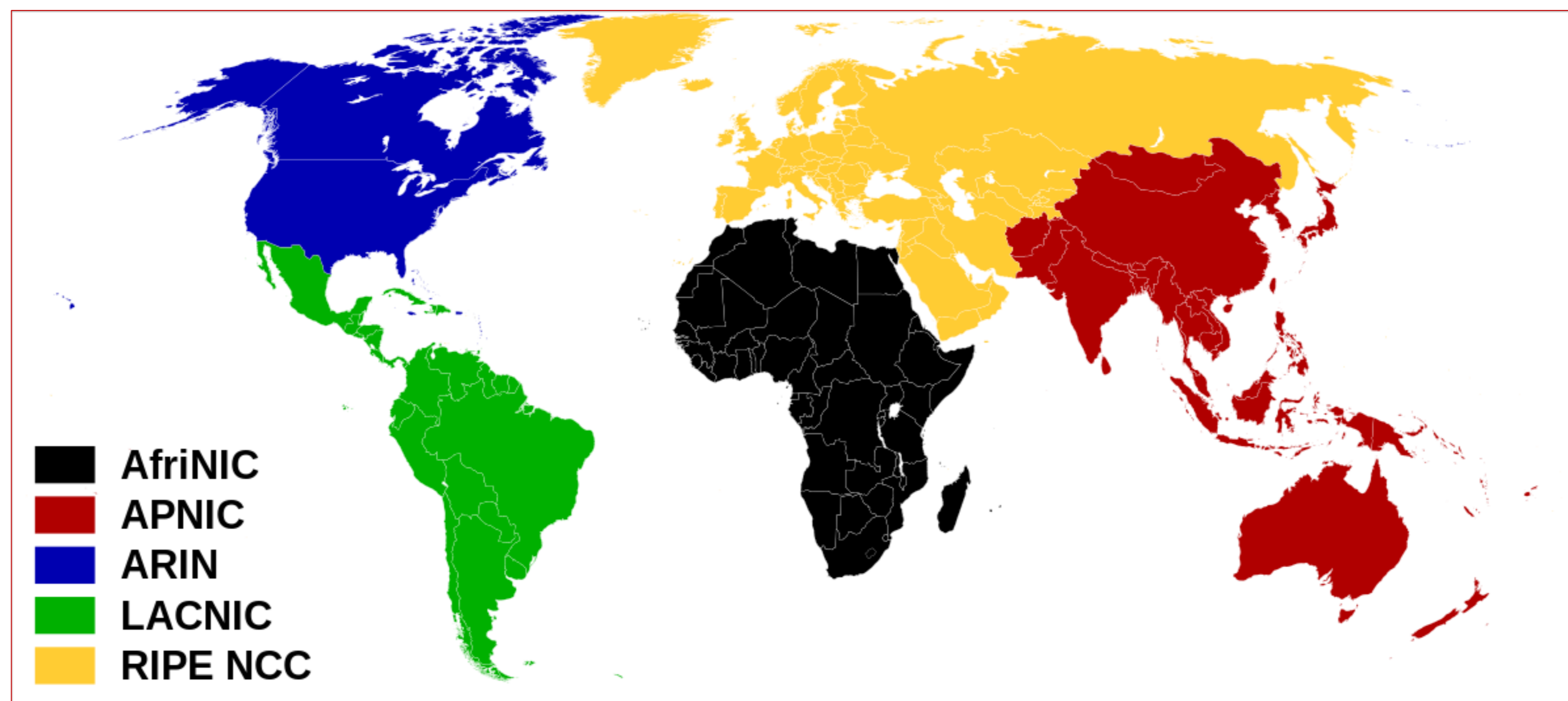
**INTRINSEC**  
Innovative by design

# Autonomous System Number



# Autonomous System Number

- Ensemble de réseaux informatiques gérés par un ou plusieurs opérateurs réseau
- Nécessaire aux opérateurs pour contrôler le routage / échanger des informations avec d'autres FAI
- Internet Assigned Numbers Authority (IANA)
- Presque 100.000 AS loués en 2019
- Permet d'identifier des plages IP appartenant à une entreprise



[https://upload.wikimedia.org/wikipedia/commons/thumb/9/95/Regional\\_Internet\\_Registries\\_world\\_map.svg/1200px-Regional\\_Internet\\_Registries\\_world\\_map.svg.png](https://upload.wikimedia.org/wikipedia/commons/thumb/9/95/Regional_Internet_Registries_world_map.svg/1200px-Regional_Internet_Registries_world_map.svg.png)



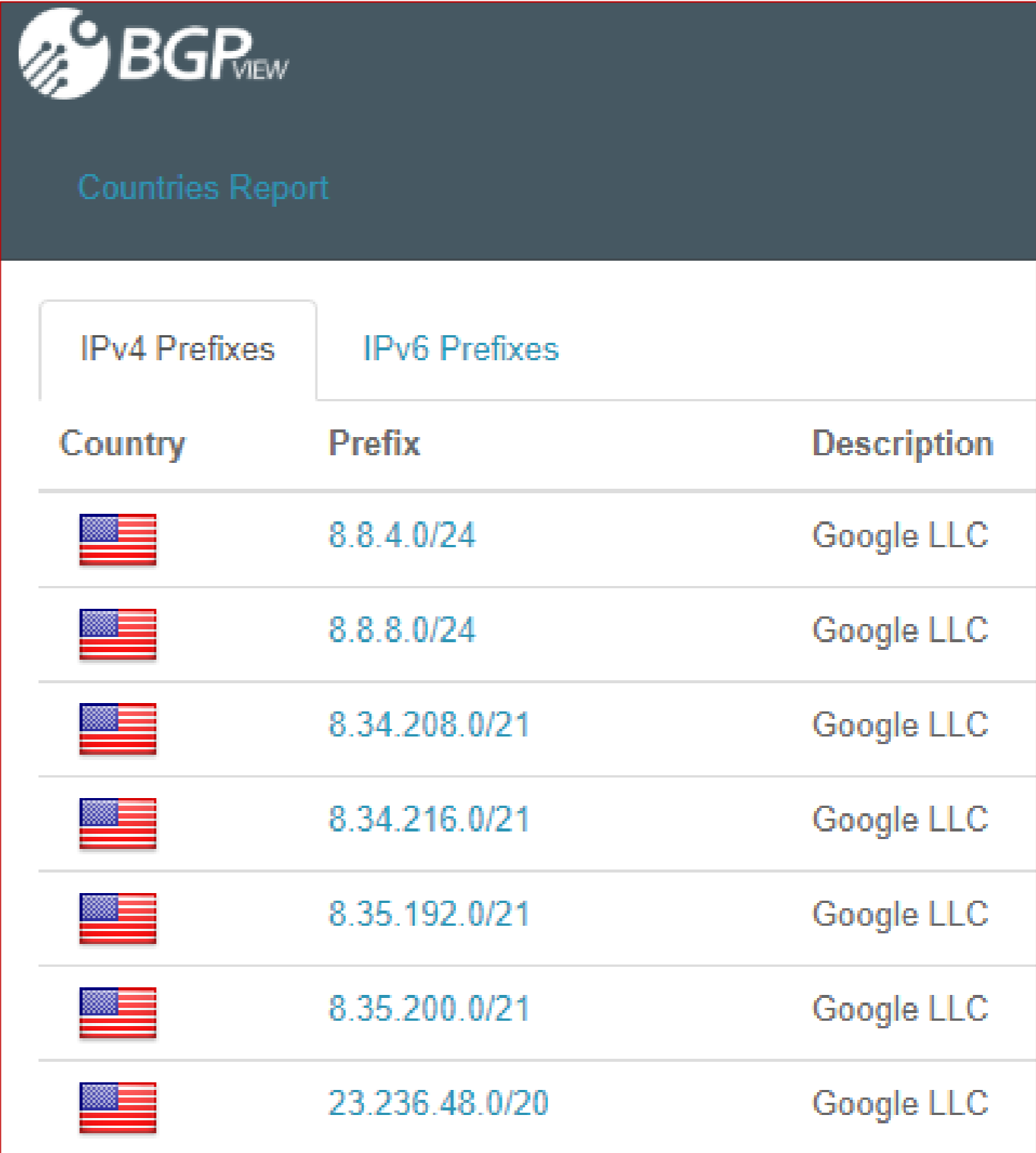
# Autonomous System Number

- Exemple : déterminer des plages IP appartenant à Google LLC








```
user@server:~$ dig google.com +short
216.58.209.238

user@server:~$ whois 216.58.209.238

NetRange:      216.58.192.0 - 216.58.223.255
CIDR:          216.58.192.0/19
NetName:       GOOGLE
NetHandle:     NET-216-58-192-0-1
Parent:        NET216 (NET-216-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS15169
Organization:  Google LLC (GOGL)
RegDate:       2012-01-27
Updated:       2012-01-27
Ref:           https://rdap.arin.net/registry/ip/216.58.192.0
```



The screenshot shows the BGPVIEW interface for Google LLC (AS15169). It displays a 'Countries Report' with a table of IPv4 prefixes. The table has columns for Country, Prefix, and Description. All listed prefixes are for the United States and are owned by Google LLC.

Country	Prefix	Description
	8.8.4.0/24	Google LLC
	8.8.8.0/24	Google LLC
	8.34.208.0/21	Google LLC
	8.34.216.0/21	Google LLC
	8.35.192.0/21	Google LLC
	8.35.200.0/21	Google LLC
	23.236.48.0/20	Google LLC

<https://bgpview.io/asn/15169#prefixes-v4>



# Autonomous System Number

- Outil : ASN Lookup par @yassineaboukir : <https://github.com/yassineaboukir/Asnlookup>
- Intégration avec Nmap et Masscan

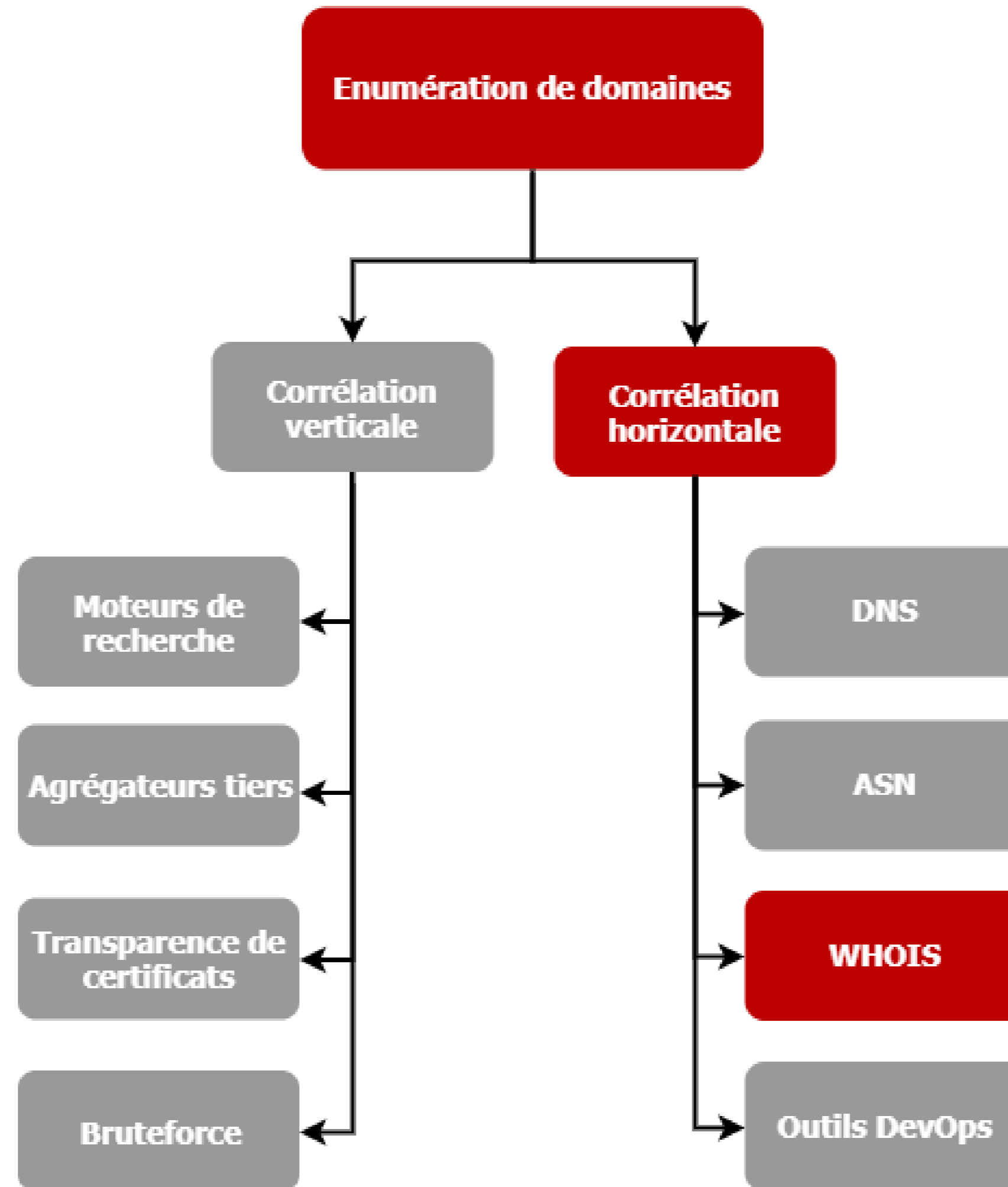
```
ASN Lookup
Home API Contribute Contact

Yay! we've got some good news. Below are IP
addresses we discovered :)

104.132.34.0/24
104.134.92.0/24
104.154.0.0/15
104.154.0.0/19
104.154.128.0/19
104.154.160.0/19
104.154.192.0/19
104.154.224.0/19
104.154.32.0/19
104.154.64.0/19
104.154.96.0/19
104.155.0.0/19
104.155.128.0/19
```



# WHOIS



# WHOIS

- Permet d'effectuer des recherches sur des noms de domaine

## Exemple : google.fr

```

user@server:~$ whois google.fr

nic-hdl:      GIH6-FRNIC
type:        ORGANIZATION
contact:     Google Ireland Holdings
address:     70 Sir John Rogersons Quay
address:     2 Dublin
country:     IE
phone:       +353 14361000
e-mail:      dns-admin@google.com
registrar:   MARKMONITOR Inc.
changed:     2015-03-20T21:13:41Z nic@nic.fr
anonymous:   NO
obsoleted:   NO
eligstatus:  ok
eligsource:  REGISTRAR
eligdate:    2011-12-30T17:15:32Z
reachmedia:  email
reachstatus: ok
reachsource: REGISTRAR
reachdate:   2015-03-20T21:13:41Z
source:      FRNIC

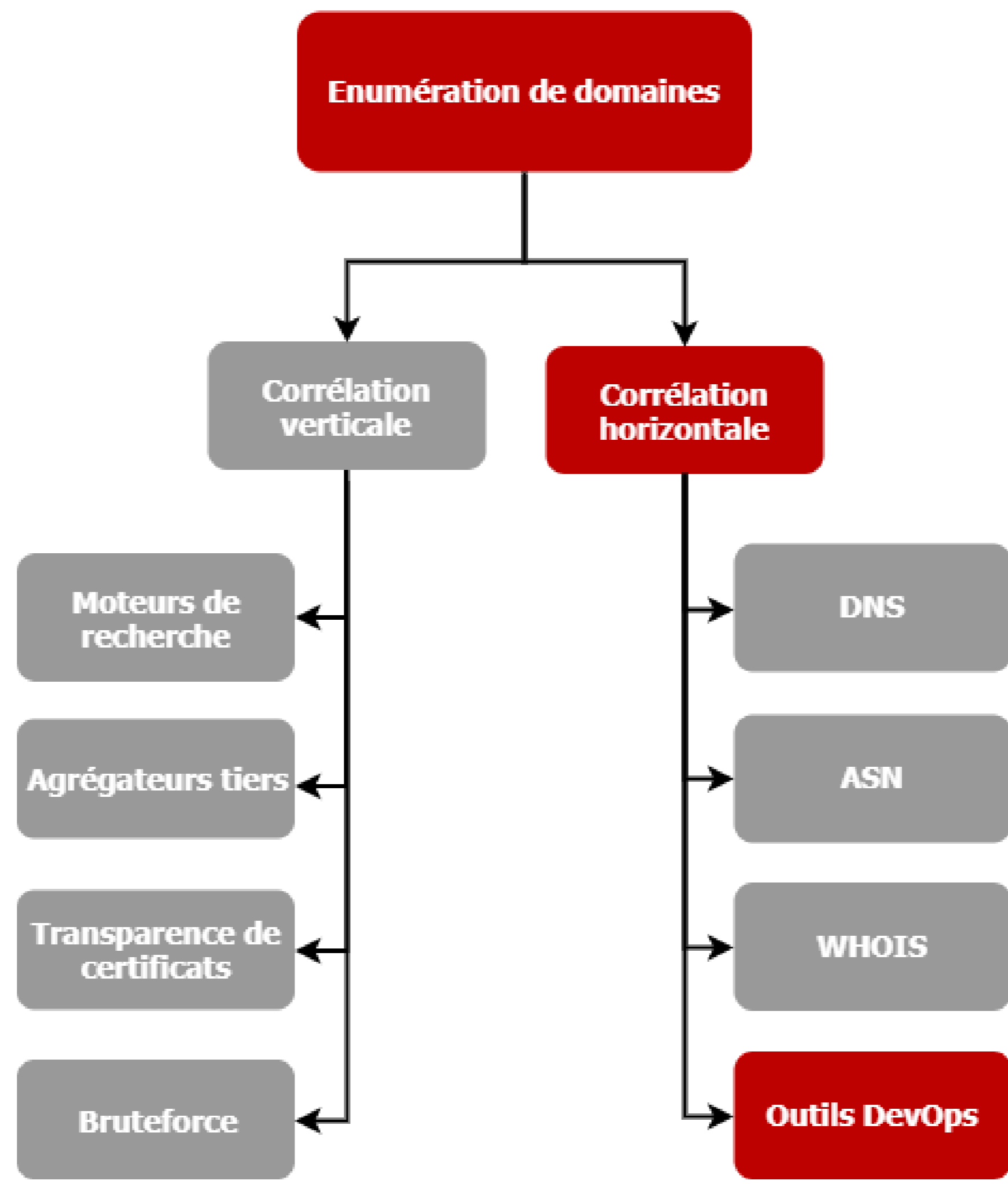
```

dns-admin@google.com

[Reverse Whois](#) » EMAIL [dns-admin@google.com] { 93,854 domain names }

NUM	DOMAIN NAME	REGISTRAR	CREATED	UPDATED	EXPIRY
1	<a href="#">google.fr</a>	-	26 Jul 2000	28 Nov 2019	30 Dec 2020
2	<a href="#">waze.com</a>	MarkMonitor Inc.	1 Apr 2000	28 Feb 2019	1 Apr 2020
3	<a href="#">alooma.com</a>	MarkMonitor Inc.	1 May 2004	9 Apr 2019	1 May 2022
4	<a href="#">deepmind-archive.com</a>	MarkMonitor Inc.	20 Nov 2019	20 Nov 2019	20 Nov 2020
5	<a href="#">doodleforgoogle.com</a>	MarkMonitor Inc.	20 Jul 2009	14 Nov 2019	20 Jul 2020
6	<a href="#">capitalg.com</a>	MarkMonitor Inc.	11 Aug 2002	1 May 2019	1 Jun 2020
7	<a href="#">deepmind.com</a>	MarkMonitor Inc.	14 Mar 2003	5 Nov 2019	14 Mar 2020

# Outils DevOps



# Outils DevOps

- Plateformes d'hébergement de code



**Facebook**  
We are working to build community through open source technology. NB: members must be 18+ years old.  
Menlo Park, California <https://opensource.fb.com> Verified

Repositories 157 Packages People 174 Projects

**jest**  
Delightful JavaScript Testing.  
javascript testing facebook snapshot expectation easy  
painless-javascript-testing  
JavaScript MIT 4,015 28,676 750 (105 issues need help) 104 Updated 23 seconds ago

**litho**  
A declarative framework for building efficient UIs on Android.  
Java Apache-2.0 590 6,446 49 12 Updated 20 minutes ago

**Facebook**

Repositories 157 Packages People 174 Projects

**Ariel Mashraki**  
a8m Follow

**António Afonso**  
aadsm Follow

**Aaron Abramov**  
aaronabramov Follow

# Outils DevOps

- <https://hackerone.com/reports/396467> par @th3g3nt3lman

514

#396467
**Github Token Leaked publicly for <https://github.sc-corp.net>**

Share: [f](#) [t](#) [in](#) [y](#)

---

State ● Resolved (Closed)

Disclosed **October 8, 2018 2:57pm +0200**

Reported To [Snapchat](#)

Asset [app.snapchat.com](#)  
(Domain)

Weakness **Cleartext Storage of Sensitive Information**

Bounty **\$15,000**

Severity ■ Critical (9.8)

Participants

Visibility **Disclosed (Full)**

**TIMELINE**

**th3g3nt3lman** submitted a report to [Snapchat](#). Aug 17th (about 1 year ago)

**Description :**

GitHub is a truly awesome service but it is unwise to put any sensitive data in code that is hosted on GitHub and similar services as i was able to find github token indexed *7 hours Ago* by user ██████ - *Software Engineer - Snap Inc*

**Issue & POC :**

You can find the leak in this link :

<https://github.com/%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88/leetcode/blob/0eec6434940a01e490d5eecea9baf4778836c54e/TopicMatch.py>

```
import os
import requests
import sys
pull_number = 76793
pull_url = "https://github.sc-corp.net/api/v3/repos/Snapchat/android/pulls/" + str(pull_number)
payload = {}
payload["Authorization"] = "token " + "9db9ca3440e535d90408a32a9c03d415979da910"
```



# Outils DevOps

- Plateformes de « pasting »
- Partager des données volatiles / morceaux de code

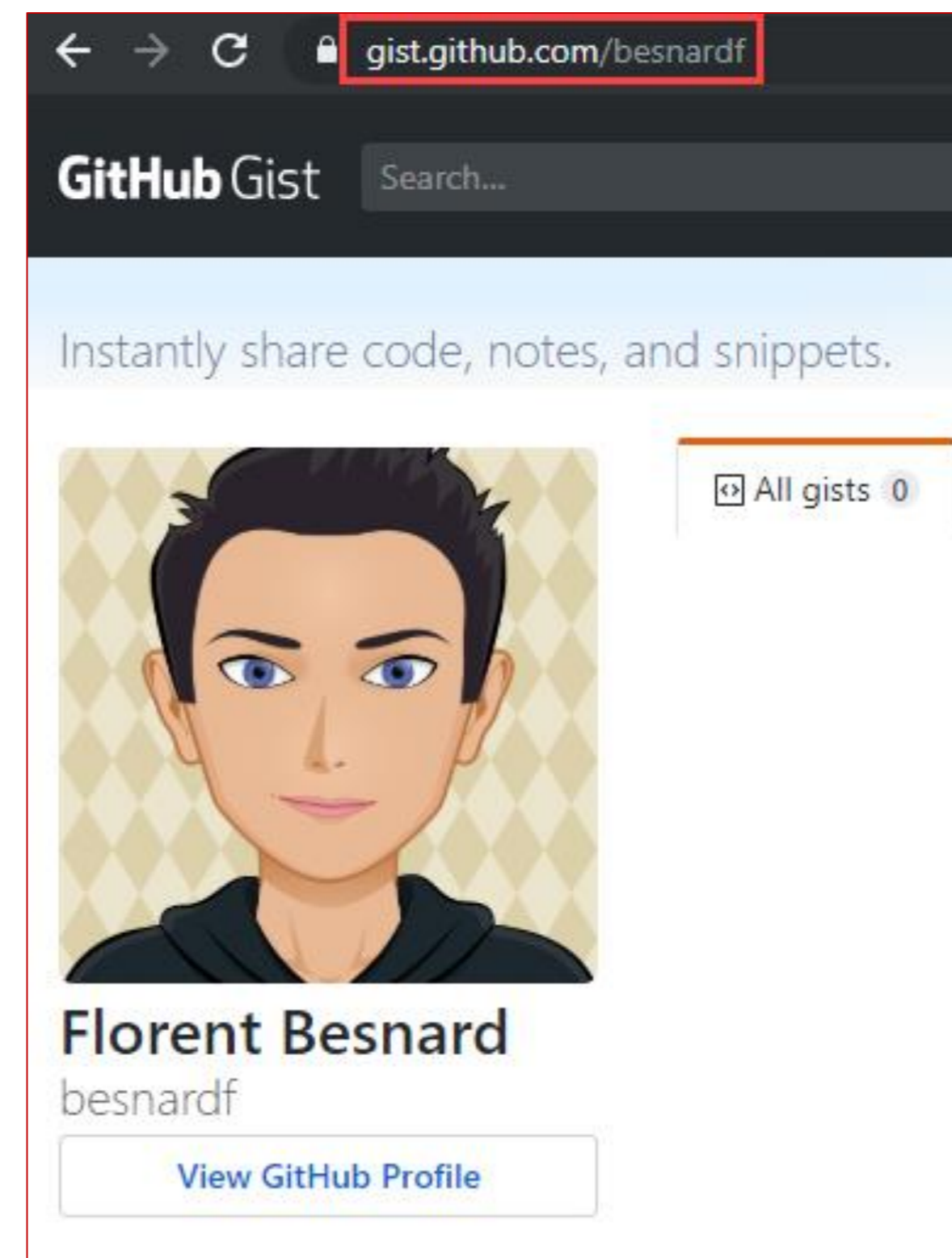
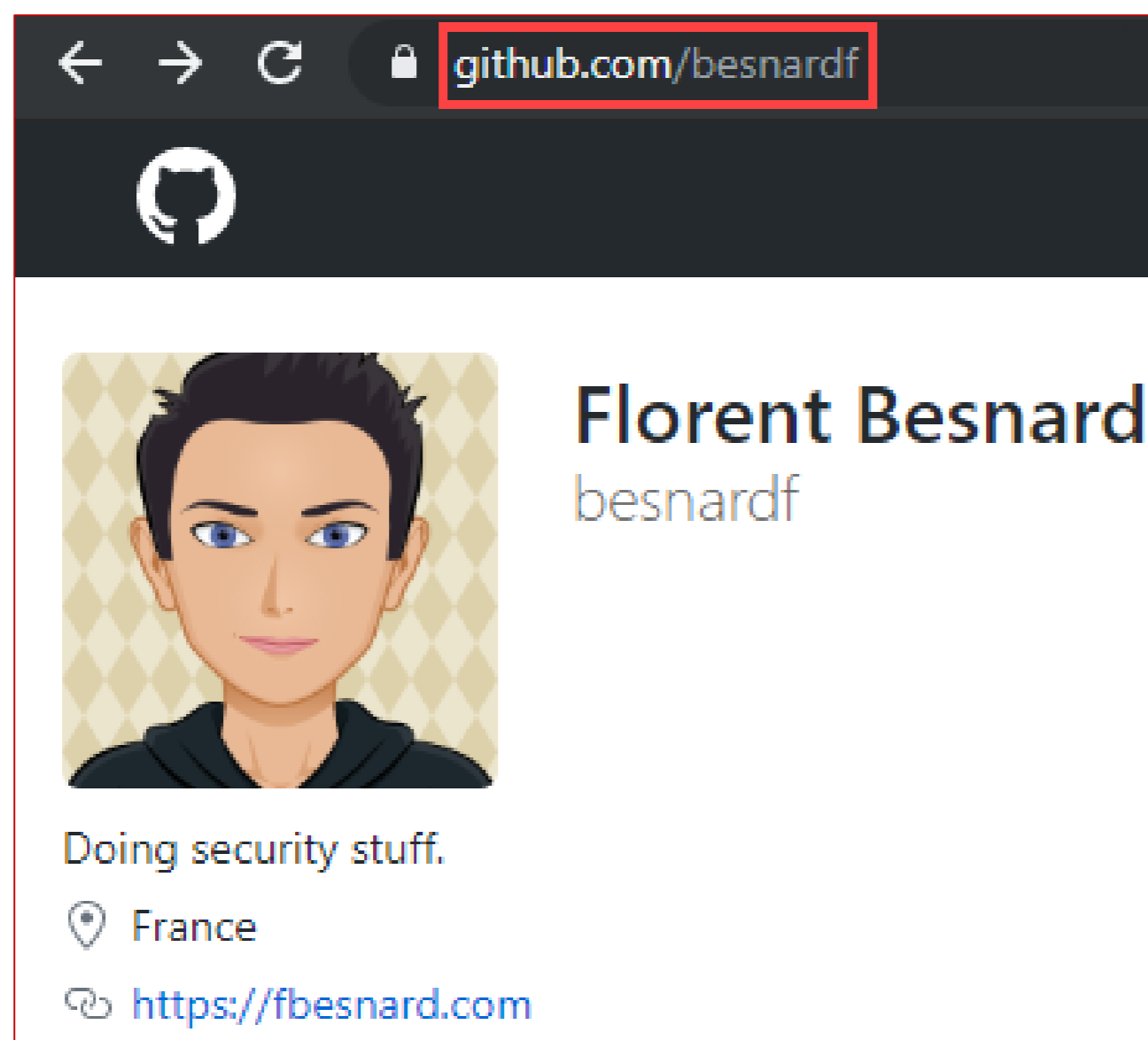


**GitHub** Gist








# Outils DevOps

## Exemple : Gist







# Outils DevOps

- <https://hackerone.com/reports/729040> par @ehsahil

9 #729040 **Shopify's SF and LA offices Dashboard Information disclosed via Public Gist** Share:     

---

State ● Resolved (Closed) Severity  No Rating (---)

Disclosed **November 6, 2019 2:12pm +0100** Participants   


Reported To [Shopify](#) Visibility **Disclosed (Full)**

Asset [\\*.shopify.com](#)  
(Domain)

Weakness **Information Disclosure**

Bounty **\$500**

TIMELINE

 **ehsahil** submitted a report to [Shopify](#). Nov 4th (about 1 month ago)

Hi Team,

During my recon process, I found a public gist containing the Internal Information of the Shopify offices of LA and SF.

The gist belongs to the Shopify employee - <https://gist.github.com/runmad> (He is currently - Engineering Manager at Shopify)

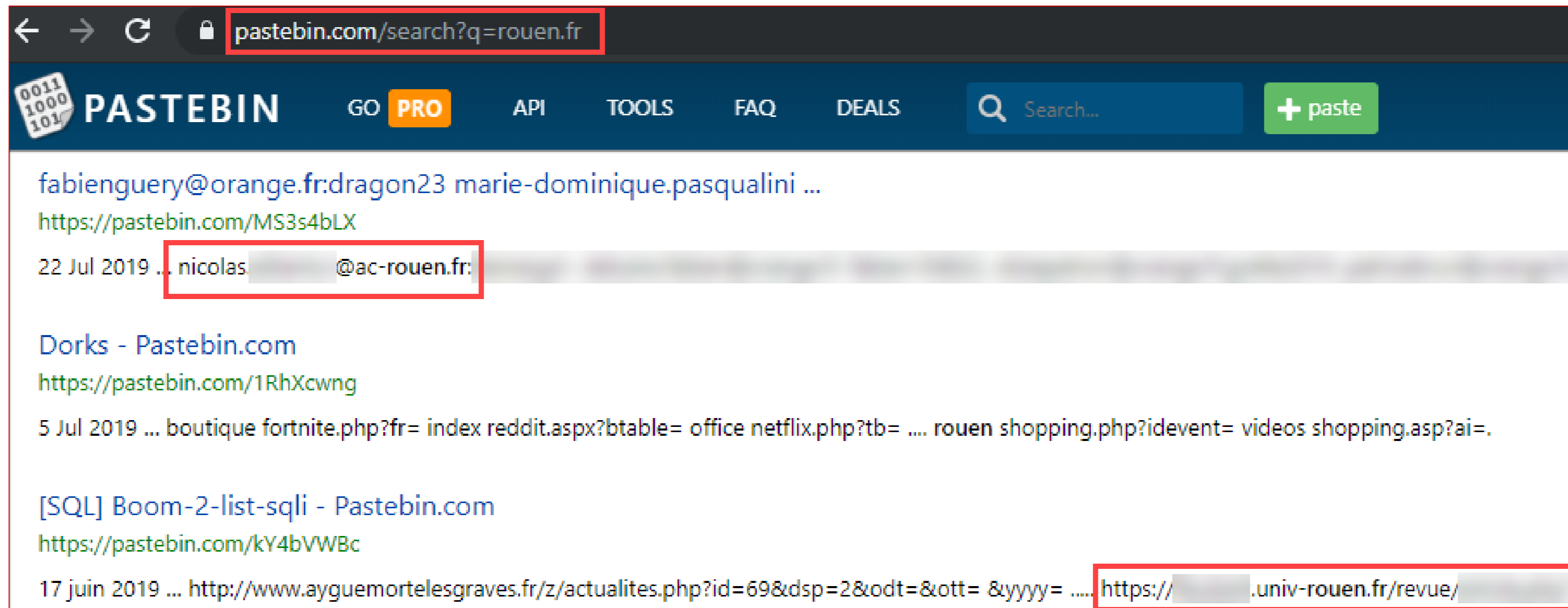
LA Office Dashboard - <https://gist.github.com/runmad/333bc33095f6f40ee8fb606fff94fbd8/revisions>

SF Office Dashboard - <https://gist.github.com/runmad/1e820c6b02d6279914d9bcb8a2a3b9cc/revisions>

The disclosed information contains the Shopify employee email addresses and calendar details.

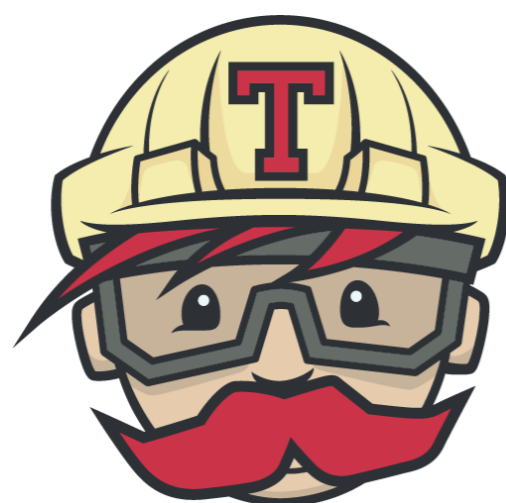
# Outils DevOps

## Exemple : Pastebin



# Outils DevOps

- Plateformes « CI/CD »
- Compiler, tester et déployer du code



# Outils DevOps

Exemple : [github.com/facebook/jest](https://github.com/facebook/jest)

Delightful JavaScript Testing. <https://jestjs.io>

javascript testing painless-javascript-testing facebook immersive painless expect

4,576 commits 5 branches 0 packages 164 releases

Branch: master New pull request

thymikee chore: remove Node 8 references and some dead code (#9284)

- .circleci** chore: run tsc and linting as GH action (#9223)
- .github chore: run tsc and linting as GH action (#9223)
- .azure-pipelines-steps.yml** chore: move "quick-install" to npm script (#9119)
- .azure-pipelines.yml** chore: add caching to azure pipelines (#8866)
- .editorconfig chore: enforce LF line endings (#8809)
- .travis.yml** chore: move "quick-install" to npm script (#9119)
- .watchmanconfig add empty .watchmanconfig (#5683)

circleci.com/gh/facebook/jest

GitHub-Org-66c92f3

**SUCCESS**

pull/9291 #76631

Fix cli init tests

51 min ago 13:18

ab5dd88

build-and-deploy test-node-8

travis-ci.org/facebook

**✓ jest**

LAST BUILD

# 14632

DEFAULT BRANCH

master

COMMIT

b2c8a69

FINISHED

Passed 23 hours ago



# Outils DevOps

Exemple : [github.com/facebook/jest](https://github.com/facebook/jest)

Jobs » facebook » jest » pull/9291 » 76631 (test-node-8) Rerun workflow

**SUCCESS** Finished: 42 min ago (13:18) Previous: 76630 Parallelism: 1x out of 0x Queued: 00:00 waiting + 00:03 in queue Resources: 2CPU/4096MB Workflow: build-and-deploy Context: N/A Triggered by: Anton Alexandrenok (pushed ab5dd88) PR: #929

COMMITTS (1)  
Anton Alexandrenok [ab5dd88](#) Fix cli init tests

Test Summary **Configuration** Timing **Parameters**






```
1 aliases:
2 - keys:
3   - v2-dependencies-{{ .Branch }}-{{ checksum "yarn.lock" }}
4   - v2-dependencies-{{ .Branch }}-
5 - paths:
6   - node_modules
7   - website/node_modules
8   key: v2-dependencies-{{ .Branch }}-{{ checksum "yarn.lock" }}
9 - branches:
10  ignore: gh-pages
```

# Outils DevOps

- <https://hackerone.com/reports/472651> par @rhyorater

**#472651** Private key "tron" leaked via Travis CI Log

---

State	● Resolved (Closed)	Severity	 Critical (9 ~ 10)
Disclosed	May 26, 2019 7:51pm +0200	Participants	   
Reported To	<a href="#">Tron Foundation</a>	Visibility	Disclosed (Full)
Asset	<a href="https://github.com/tronprotocol/java-tron">https://github.com/tronprotocol/java-tron</a> (Domain)		
Weakness	Information Disclosure		
Bounty	\$1,000		

# Outils DevOps

- <https://hackerone.com/reports/472651> par @rhyorater

## Methodology

The following methodology was used to find this vulnerability:

1. List all the repos under `/tronprotocol` on travis-ci.org
2. For each of these repos, grab each of the builds
3. For each of the builds, grab the config and the job log(s)
4. Grep through the job logs and config for sensitive looking strings ( see trufflehog regex and work by ed and karim)

<https://edoverflow.com/2019/ci-knew-there-would-be-bugs-here/>



# Outils DevOps

```
416 Network availability confirmed.
417
418 127.0.0.1 localhost nettuno travis vagrant
419 127.0.1.1 travis-job-ccd9db7e-2aca-42c2-918b-978d26e5a65b travis-job-ccd9db7e-2aca-42c2-918b-978d26e5a65b ip4-loopback trusty64
420
421 W: http://ppa.launchpad.net/couchdb/stable/ubuntu/dists/trusty/Release.gpg: Signature by key
    15866BAFD9BCC4F3C1E0DFC7D69548E1C17EAB57 uses weak digest algorithm (SHA1)
422 $ jdk_switcher use oraclejdk8
423 Switching to Oracle JDK8 (java-8-oracle), JAVA_HOME will be set to /usr/lib/jvm/java-8-oracle
▶ 424 Adding ssh known hosts (BETA) ssh_known_hosts.0
▶ 433 $ git clone --depth=50 https://github.com/tronprotocol/java-tron.git tronprotocol/java-tron git.checkout 0.84s
442
443 Setting environment variables from repository settings
444 $ export encrypted_e5855cb9e09c_key=[secure]
445 $ export encrypted_e5855cb9e09c_iv=[secure]
446
```



# Outils DevOps

```
▼ 7 .travis.yml
@@ -6,21 +6,18 @@ script:
6 6 - ./gradlew test
7 7 - cat tron > ~/.ssh/id_rsa
8 8 - chmod 600 ~/.ssh/id_rsa
9 + - cat tron
9 10 addons:
10 11
18 15 - LICENSE
19 16 deploy:
20 17   provider: script
21 18   script: bash deploy.sh
22 19   on:
23 -   branch: develop
20 +   branch: feature/deploy
24 21 before_install:
25 22 - openssl aes-256-cbc -K $encrypted_e5855cb9e09c_key -iv $encrypted_e5855cb9e09c_iv
26 23 -in tron.enc -out tron -d
```

```
▼ 2 deploy.sh
@@ -1,5 +1,5 @@
...  ...
1 1  #!/bin/bash
2 2  - ./gradlew clean shadowJar
3 + # ./gradlew clean shadowJar
3 3  ssh tron@47.93.9.236 -p 22008 mkdir java-tron
4 4  scp -P 22008 build/libs/java-tron.jar tron@47.93.9.236:/home/tron/java-tron/
5 5  scp -P 22008 start.sh tron@47.93.9.236:/home/tron/java-tron/
```

# Outils DevOps

- Buckets
- Solution cloud utilisée à des fins de stockage : scalabilité, disponibilité et sécurité
- N'importe quel type de données : sauvegarde, données clients, données applicatives, etc.

## Google Cloud Storage :

- <https://BUCKET.storage.googleapis.com/OBJET>
- <https://storage.googleapis.com/BUCKET/OBJET>



Google Cloud  
Storage



## Amazon S3 :

- <https://BUCKET.s3.amazonaws.com/OBJET>
- <https://s3.amazonaws.com/BUCKET/OBJET>

## Azure Blob Storage :

- <https://BUCKET.blob.core.windows.net/OBJET>





# Outils DevOps

- <https://github.com/RhinoSecurityLabs/GCPBucketBrute> par @rhinosecurity
- Permutations
- Requêtes auprès de l'API [www.googleapis.com](http://www.googleapis.com)



```
user@server:~$ python3 gcpbucketbrute.py -k facebook -u
```

```
Generated 1216 bucket permutations.
```

```
EXISTS: facebook-resources  
EXISTS: facebookvideos  
EXISTS: facebook-events  
EXISTS: facebook0  
EXISTS: facebook_reports  
EXISTS: facebookpublic  
EXISTS: facebook_test  
EXISTS: facebook01  
EXISTS: facebook_export
```



# Outils DevOps

- <https://github.com/hehnope/slurp> par hehnope
- Permutations (presque 30.000)
- Requêtes auprès de s3-1-w.amazonaws.com

```
user@server:~$ slurp domain -t facebook.com -p Wordlists/permutations.json
INFO[0000] Building permutations....
INFO[0000] Processing permutations....
INFO[0025] FORBIDDEN http://facebook-2011.s3.amazonaws.com (http://facebook.com)
INFO[0039] PUBLIC http://facebook-ac.s3.ca-central-1.amazonaws.com/ (http://facebook.com)
INFO[0044] FORBIDDEN http://facebook-ad.s3.amazonaws.com (http://facebook.com)
INFO[0052] PUBLIC http://facebook-ads.s3.amazonaws.com (http://facebook.com)
INFO[0067] FORBIDDEN http://facebook-alpha.s3.amazonaws.com (http://facebook.com)
INFO[0074] PUBLIC http://facebook-analytics.s3.ap-northeast-2.amazonaws.com/ (http://facebook.com)
```

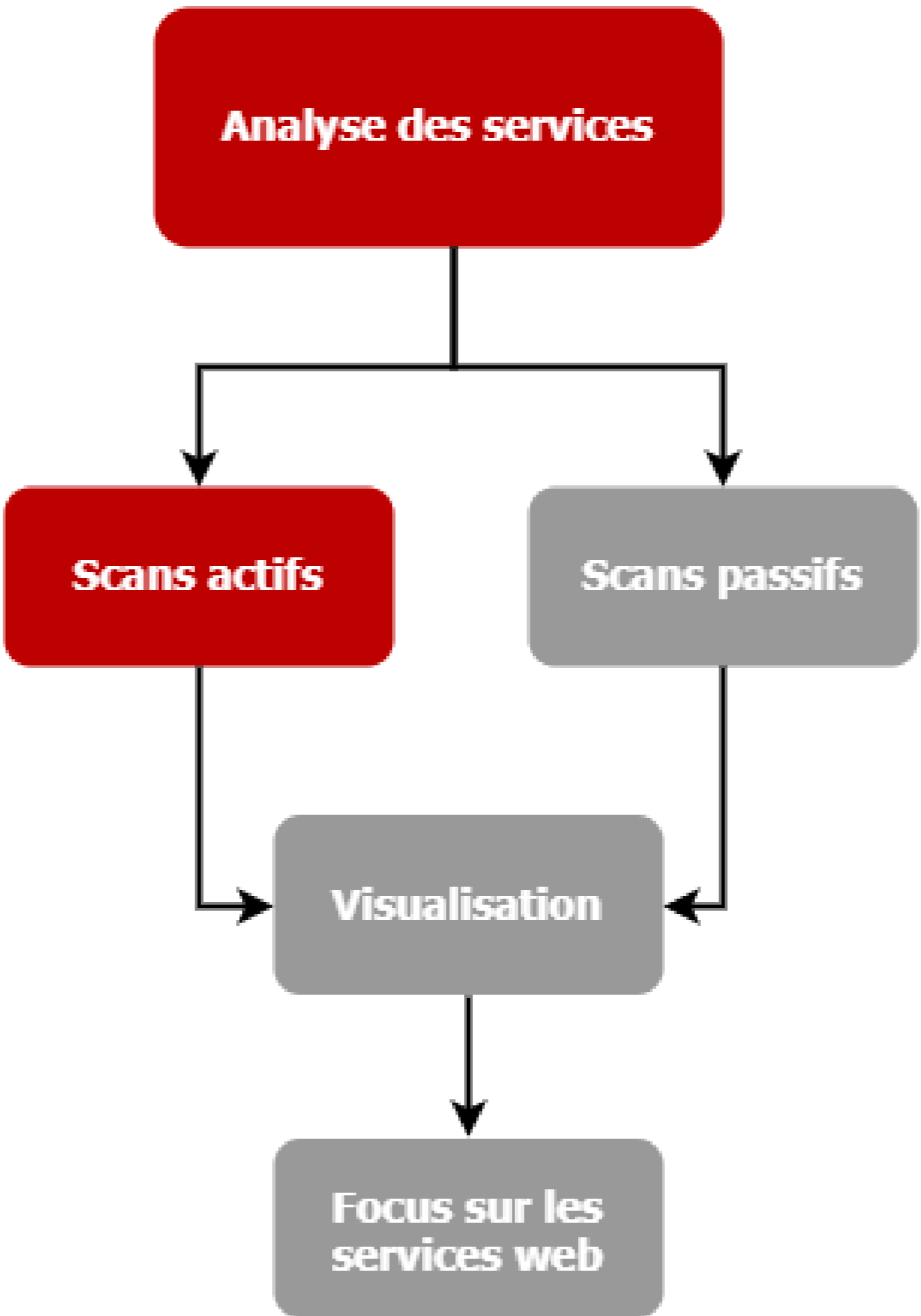


# Analyse des services



**INTRINSEC**  
Innovative by design

# Scans actifs



# Scans actifs

- Prend du temps
- Peuvent déclencher un IDS/IPS
- Meilleure représentation des services accessibles
- 2 outils généralement utilisés : Nmap et Masscan

	Nmap	Masscan
Avantages	<ul style="list-style-type: none"><li>• Synchrones (plus de précision)</li><li>• Moteur de scripts</li><li>• S'adapte à la charge supportée par la cible</li></ul>	<ul style="list-style-type: none"><li>• Asynchrone (plus rapide)</li></ul>
Inconvénients	<ul style="list-style-type: none"><li>• Scans très lents lorsqu'il y a plusieurs centaines de cibles</li></ul>	<ul style="list-style-type: none"><li>• Résultats peu précis lorsque l'on augmente la fréquence</li><li>• Accepte seulement les adresses IP</li></ul>



# Scans actifs

## Exemple : Nmap

```
user@server:~/Tools$ nmap -T4 -A scanme.nmap.org

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256  33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (EdDSA)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
```

```
user@server:~$ nmap -p- -sS -sV -sC scanme.nmap.org
```


```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-11-10 19:04 CET
Stats: 0:05:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.28% done; ETC: 19:21 (0:10:44 remaining)
Stats: 0:40:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 43.77% done; ETC: 20:36 (0:51:23 remaining)
```










# Scans actifs





- <https://hackerone.com/reports/119871> par @zephrfish

 **PhishyZephr (zephrfish)** 2075 Reputation - Rank 4.32 Signal 84th Percentile 16.93 Impact 86th Percentile

---

**#119871** **Unprotected Memcache Installation running** 8 Share:     


---

State	● Resolved (Closed)	Severity	 No Rating (---)
Disclosed	May 26, 2016 5:53am +0200	Participants	  
Reported To	<a href="#">Pornhub</a>	Visibility	Disclosed (Limited)
Weakness	Improper Authentication - Generic		
Bounty	\$2,500		

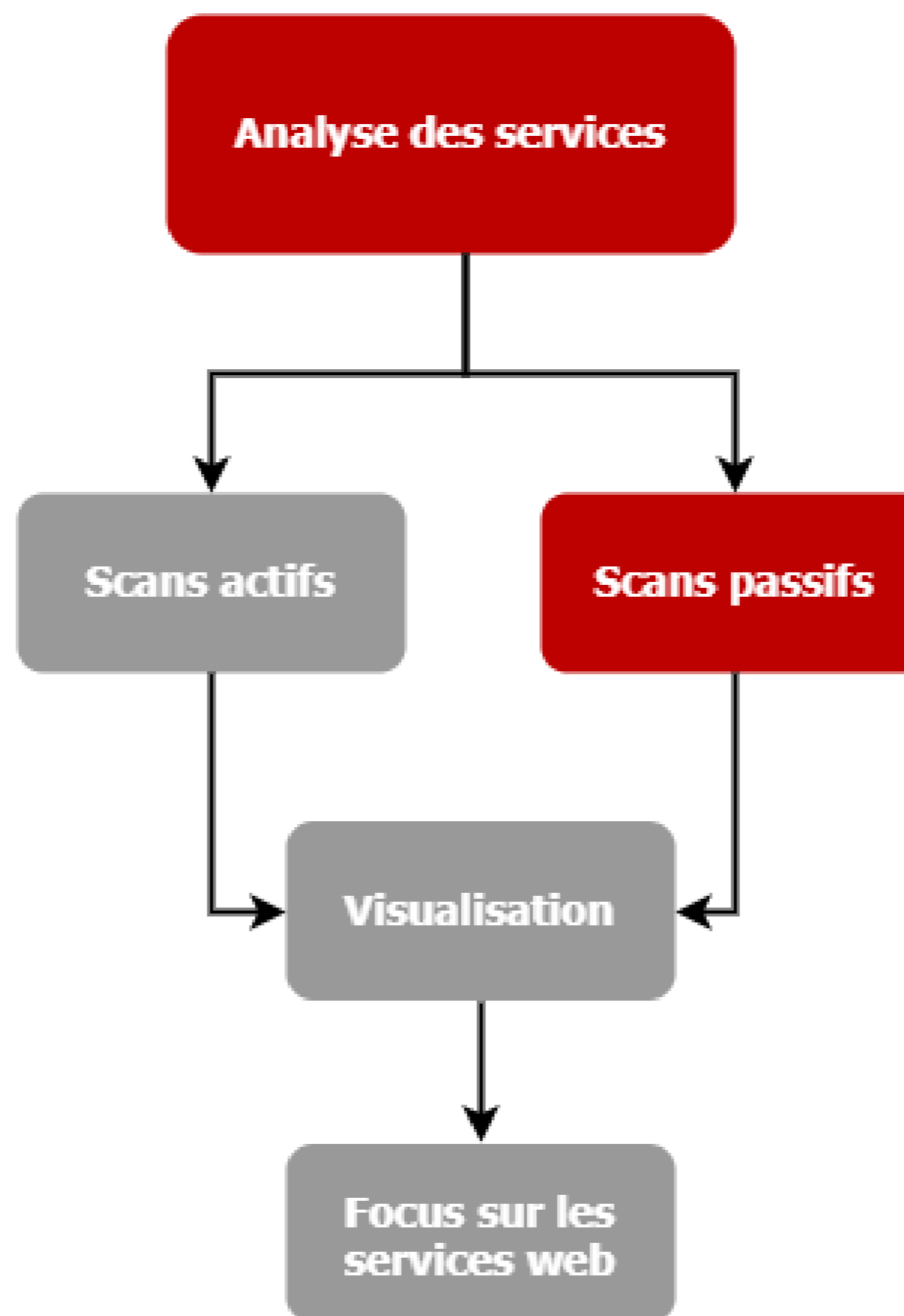
[Collapse](#)

---

SUMMARY BY PORNHUB

 The consultant was able to connect to the stage.pornhub.com subdomain via port 60893, it was determined that the target host was running memcached and required no authentication.

# Scans passifs



# Scans passifs

- Utilisation d'outils / données tierces Shodan, Censys, etc.
- Résultats désormais potentiellement invalides
- Pas de connexion directe avec la cible
  
- Shodan :
  - Net:x.x.x.x/x
  - Org: « entreprise »
  
- Censys :
  - Ip:x.x.x.x/x
  - Autonomous\_system.asn:<ASN>
  - Autonomous\_system.organization:« entreprise »



# Scans passifs

## Exemple : Shodan & Fofa

The screenshot displays the Shodan search engine interface. At the top, the search bar contains 'org.facebook'. Below the search bar, there are navigation tabs for 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'. The main content area is divided into several sections:

- TOTAL RESULTS:** A box highlights the number '7,122'.
- TOP COUNTRIES:** A world map shows search results concentrated in the United States and Ireland. Below the map is a table:
 

United States	4,671
Ireland	2,010
South Africa	353
India	30
Nigeria	28
- TOP SERVICES:** A table lists various services:
 

HTTP S	3,882
HTTP	3,050
HTTP (8080)	77
9443	74
NTP	6
- Search Results:** Two specific results are shown:
  - 31.13.85.1:** edge-atlas-shv-01-gru2.facebook.com, Facebook, Ireland. HTTP/1.1 400 Bad Request.
  - 157.240.15.10:** edge-msgr-latest-shv-02-hkg3.facebook.com, Facebook, United States. Includes an SSL Certificate section:
    - Issued By: Assurance Server CA
    - Common Name: DigiCert SHA2 High Assurance Server CA
    - Organization: DigiCert Inc
    - Issued To: \*
    - Common Name: \*.facebook.com
    - Organization: Facebook, Inc.


# Scans passifs

SHODAN  [Q](#) [Home](#) [Explore](#) [Downloads](#) [Reports](#) [Pricing](#) [Enterprise Access](#)

[Exploits](#) [Maps](#) [Share Search](#) [Download Results](#) [Create Report](#)

**TOTAL RESULTS**  
276

**TOP COUNTRIES**



United States 276

**TOP SERVICES**

HTTPS	152
HTTP	118
9443	3
HTTP (8080)	3

**TOP ORGANIZATIONS**

Facebook	276
----------	-----

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**179.60.193.174** [🔗](#)  
instagram-p42-shv-01-scl1.fbofn.net  
**Facebook**  
Added on 2019-12-10 23:39:45 GMT  
🇺🇸 United States

HTTP/1.1 400 Bad Request  
Content-Type: text/plain  
Server: proxygen-bolt  
Date: Tue, 10 Dec 2019 23:39:45 GMT  
Connection: keep-alive  
Content-Length: 0

**179.60.192.36** [🔗](#)  
edge-star-mini-shv-01-cdg2.facebook.com  
**Facebook**  
Added on 2019-12-10 19:36:23 GMT  
🇺🇸 United States

**SSL Certificate**

Issued By:  
|- Common Name: DigiCert SHA2 High Assurance Server CA  
|- Organization: DigiCert Inc


Issued To:  
|- Common Name: \*.facebook.com  
|- Organization: Facebook, Inc.

HTTP/1.1 301 Moved Permanently  
Vary: Accept-Encoding  
Location: https://www.facebook.com/  
Content-Type: text/html; charset="utf-8"  
**X-FB-Debug: E0ojR/JKn3r+DrIcni+qqT7GZ203**  
Date: Tue, 10 Dec 2019 19:36:20 GMT  
Alt-Svc: h3-24=":443"; m...

**Supported SSL Versions**  
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3








# Scans passifs

header="X-FB-Debug"  [收藏规则](#) [下载数据](#) [使用API](#)


Query: **header="X-FB-Debug"**, Total results: 4,999 (IP results: 4,345 ), took 344 ms, mode: **extended**.  
默认只显示一年内的数据, 点击 [all](#) 链接查看所有.





← Previous **1** 2 3 4 5 6 7 ... 500 Next →

<https://202.88.187.19>  443

📍 202.88.187.19   
🕒 2019-12-11  
🚩  India  
ASN: 17488  
ORG: Hathway IP Over Cable Interne  
t  

HTTP/1.1 301 Moved Permanently  
Connection: close  
Alt-Svc: h3-24=":443"; ma=3600  
Content-Type: text/html; charset="utf-8"  
Date: Wed, 11 Dec 2019 09:36:17 GMT  
Location: https://www.facebook.com/  
X-Fb-Debug: MgGDFU5sijk3jZv/bvZl/NT2n(fkns5kqyggXmif4E3o18J5yV  
vP8c8wZLsTEscZLCv18qKFFXHeHhM1+atAfMw==

<https://103.76.47.148>  443

📍 103.76.47.148   
🕒 2019-12-11  
🚩  Bangladesh / Dhaka  
ASN: 133866  
ORG: Angel Drops Ltd.  
 

HTTP/1.1 301 Moved Permanently  
Connection: close  
Alt-Svc: h3-24=":443"; ma=3600  
Content-Type: text/html; charset="utf-8"  
Date: Wed, 11 Dec 2019 09:30:41 GMT


**TYPE**






Website	4,999
---------	-------

**Years**

2019	4,997
2018	2

**TOP COUNTRIES**



 Brazil	860	▼
 United States of America	848	▼
 India	196	▼
 Korea, Republic of	162	▼
 Ireland	150	▼

**TOP PORTS**

443	4,337
80	467
33338	136
9443	5





# Scans passifs

## Exemple : Censys

**Censys** IPv4 Hosts

**Quick Filters**  
For all fields, see [Data Definitions](#)

**Autonomous System:**  
3,584 FACEBOOK - Facebook, Inc.

**Protocol:**  
3,482 443/https  
2,435 80/http  
80 8080/http  
8 53/dns  
3 25/smtp

**Tag:**  
3,441 https  
2,648 http  
8 dns  
3 smtp

**IPv4 Hosts**  
Page: 1/144 Results: 3,584 Time: 789ms

- [157.240.193.63 \(instagram-p3-shv-01-fco1.fbcdn.net\)](#)  
FACEBOOK - Facebook, Inc. (32934) United States  
443/https, 80/http  
\*.instagram.com, \*.cdninstagram.com, instagram.com
- [31.13.79.18 \(edge-star-shv-02-bom1.facebook.com\)](#)  
FACEBOOK - Facebook, Inc. (32934) Ireland  
443/https, 80/http  
\*.facebook.com, \*.facebook.net, \*.m.facebook.com
- [157.240.201.15 \(xx-fbcdn-shv-01-ams4.fbcdn.net\)](#)  
FACEBOOK - Facebook, Inc. (32934) United States  
443/https, 80/http  
\*.facebook.com, \*.facebook.net, \*.m.facebook.com
- [157.240.21.19 \(secure-edge-latest-shv-01-cdt1.facebook.com\)](#)  
FACEBOOK - Facebook, Inc. (32934) United States  
80/http

# Scans passifs

## Exemple : ZoomEye

知道创宇 | ZoomEye 首页 探索 开发 专题 商务 贡献 私有版

**185.60.218.16**

edge-secure-shv-01-otp1.facebook...

443/https

Romania, Otopeni

2019-12-11 15:07

```

HTTP/1.1 301 Moved Permanently
Vary: Accept-Encoding
Location: https://www.facebook.com/
Content-Type: text/html; charset="utf-8"
X-FB-Debug: DXEM75e3pNqCNWcdCfzpj3uW8mVrVLRCE9Zc7Ty0BEQTXsZhnyuWdJszwNj
Date: Wed, 11 Dec 2019 07:07:32 GMT
Alt-Svc: h3-24=":443"; ma=3600
Connection: close
Content-Length: 0

Http response from 302 moved url https://www.facebook.com/:
X-Fb-Debug: onfVyWM1y9t4JLLe5Gt3G/84wOwANRtiRHJ8Sizoez2UuI3KmJTOL9Q010e

```

mysql 41

**设备**

Unknown	6245
starttls	21
security-misc	8
load balancer	7
switch	1

**端口**

80	2808
443	2334
8883	363
25	121
8080	93
9443	74
22	54
110	53
3478	50
3306	41

**179.60.194.169**

edge-z-p4-shv-02-kut2.facebook.c...

443/https

Malaysia

2019-12-11 14:28

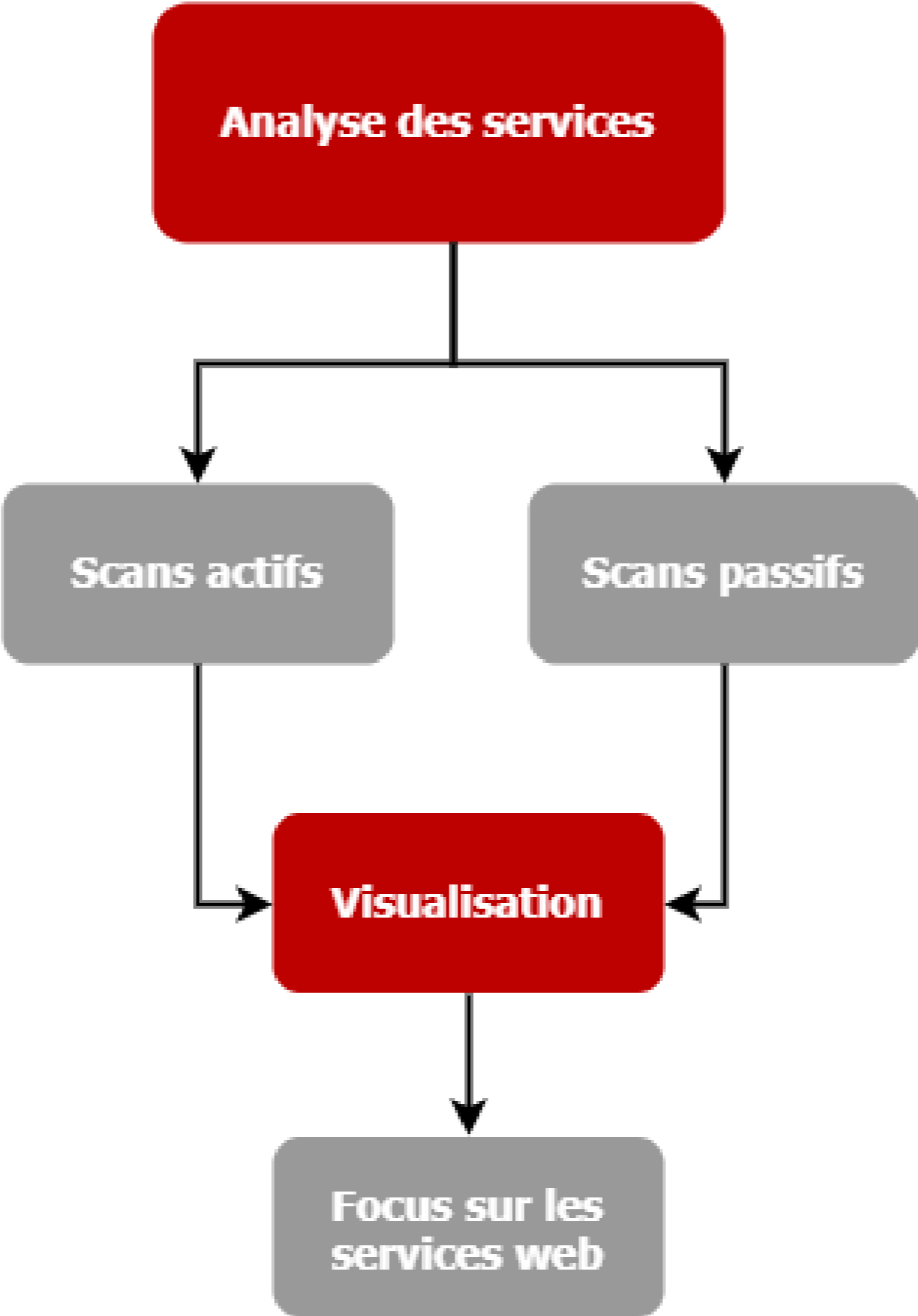
```

HTTP/1.1 301 Moved Permanently
Vary: Accept-Encoding
Location: https://www.facebook.com/
Content-Type: text/html; charset="utf-8"
X-FB-Debug: DoE28rLPvXLqRrurhFyBTNcxXwfIbZZARTpB1BJyYYhCIgeZdrJN5ydwG+H
Date: Wed, 11 Dec 2019 06:28:44 GMT
Alt-Svc: h3-24=":443"; ma=3600
Connection: close
Content-Length: 0

Http response from 302 moved url https://www.facebook.com/:
Set-Cookie: fr=13Mk7aaamtlsUEDKA..Bd8Iyc.jC.AAA.0.0.Bd8Iyc.AwXowKau; e

```

# Visualisation



# Visualisation

- Impossible d'analyser tous les services identifiés
- Automatisation nécessaire

## Exemple : Aquatone

```

└─$ cat hosts.txt | gshuf | head -n 500 | aquatone
aquatone v1.3.2 started at 2018-11-04T12:29:33+01:00

Targets      : 500
Threads     : 4
Ports       : 80, 443, 8000, 8080, 8443
Output dir  : .

lo0.tor74-63-gra.ne1.yahoo.com port 80: open
lo0.tor18-82-gra.ne1.yahoo.com port 80: open
et19-1.fab7-2-gdc.ne1.yahoo.com port 80: open
et24-1.fab5-2-gdc.ne1.yahoo.com port 80: open
lo0.tor344-476-pdb.ne1.yahoo.com port 80: open
lo0.tor211-282-gra.ne1.yahoo.com port 80: open
dp-propane-broker-bcp1.data.ne1.yahoo.com port 80: open
et-9-3-2.clr2-a-gdc.ne1.yahoo.com port 80: open
vn.yahoo.com port 80: open
et-0-0-0.clr2-a-gdc.ne1.yahoo.com port 80: open
lo0.tor111-169-pdb.ne1.yahoo.com port 80: open
lo0.tor225-381-pdb.ne1.yahoo.com port 80: open
lo0.tor287-429-pdb.ne1.yahoo.com port 80: open
ds25.ab.ne1.yahoo.com port 80: open
usw2-1-lbc.ne1.yahoo.com port 80: open
lo0.tor336-380-gra.ne1.yahoo.com port 80: open
lo0.tor288-354-pda.ne1.yahoo.com port 80: open
lo0.tor16-80-gra.ne1.yahoo.com port 80: open
sandycm-pda-01.netops.sg3.yahoo.com port 80: open
ge-0-1-4.msri.ne1.yahoo.com port 80: open

```

[https://michenriksen.com/images/aquatone\\_1\\_3\\_2/start.png](https://michenriksen.com/images/aquatone_1_3_2/start.png)

```

└─$ cat masscan.xml | aquatone -nmap
aquatone v1.3.2 started at 2018-11-04T12:39:57+01:00

Targets      : 796
Threads     : 4
Ports       : 80, 443, 8000, 8080, 8443
Output dir  : .

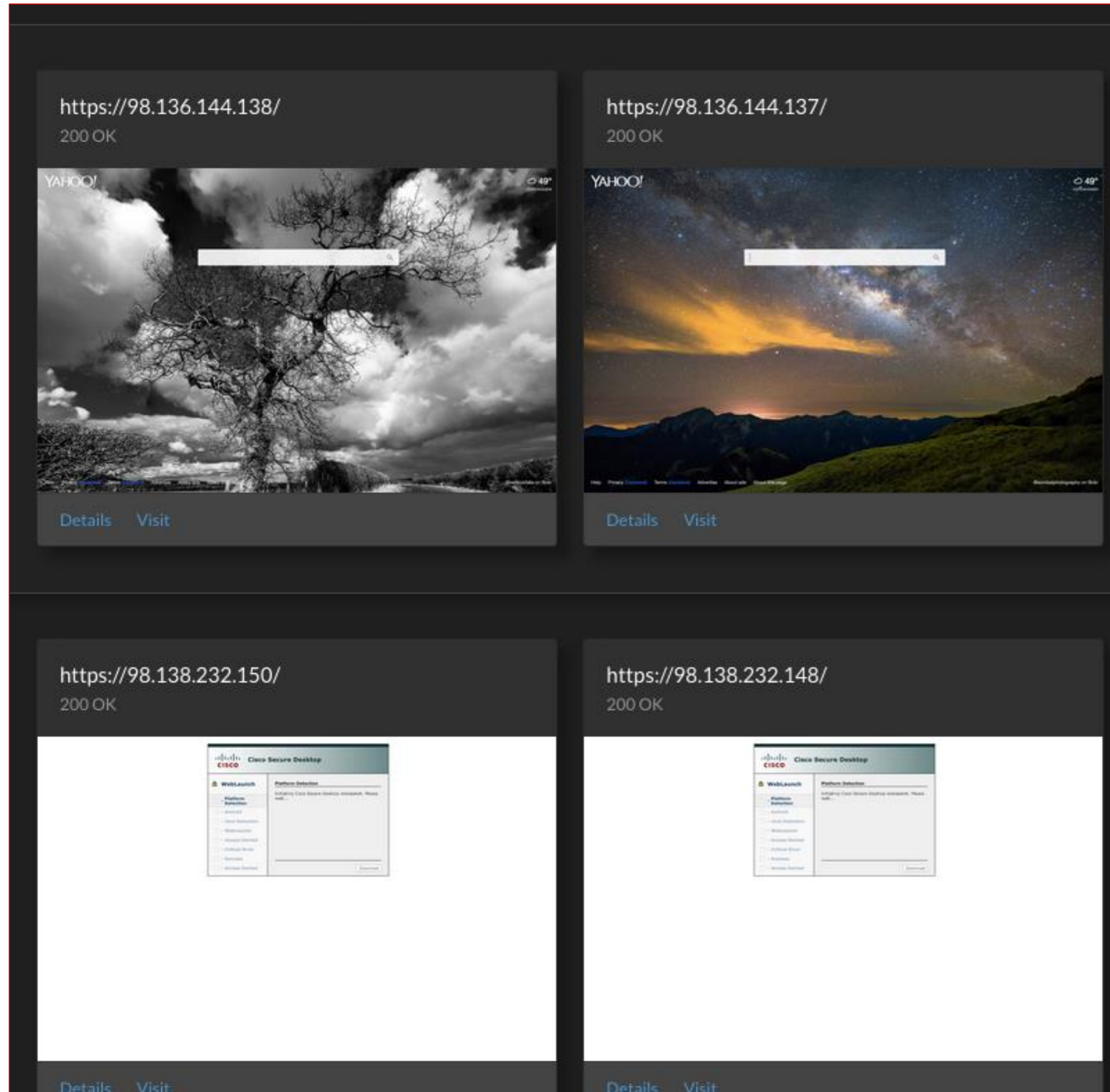
http://69.147.80.205/: 401 Unauthorized
https://188.125.95.254/: 404 Not Found on Accelerator
http://98.139.159.40/: 200 OK
https://98.136.100.146/: 404 Not Found on Accelerator
http://98.138.219.61/: 404 Not Found on Accelerator
http://188.125.90.201/: 404 Not Found on Accelerator
http://69.147.83.62/: 404 Not Found on Accelerator
http://69.147.82.75/: 401 Unauthorized
http://98.136.96.140/: 200 OK
http://209.73.186.53/: 502 Server Hangup
https://69.147.86.138/: 401 Unauthorized
https://203.84.220.182/: 404 Not Found on Accelerator
http://98.139.225.43/: 502 connect failed
http://69.147.86.12/: 404 Not Found on Accelerator
https://98.138.219.75/: 404 Not Found on Accelerator
http://98.138.219.77/: 404 Not Found on Accelerator
http://87.248.106.202/: 404 Not Found on Accelerator
http://203.84.194.189/: 403 Forbidden
https://69.147.118.77/: 200 OK
https://188.125.95.253/: 404 Not Found on Accelerator

```

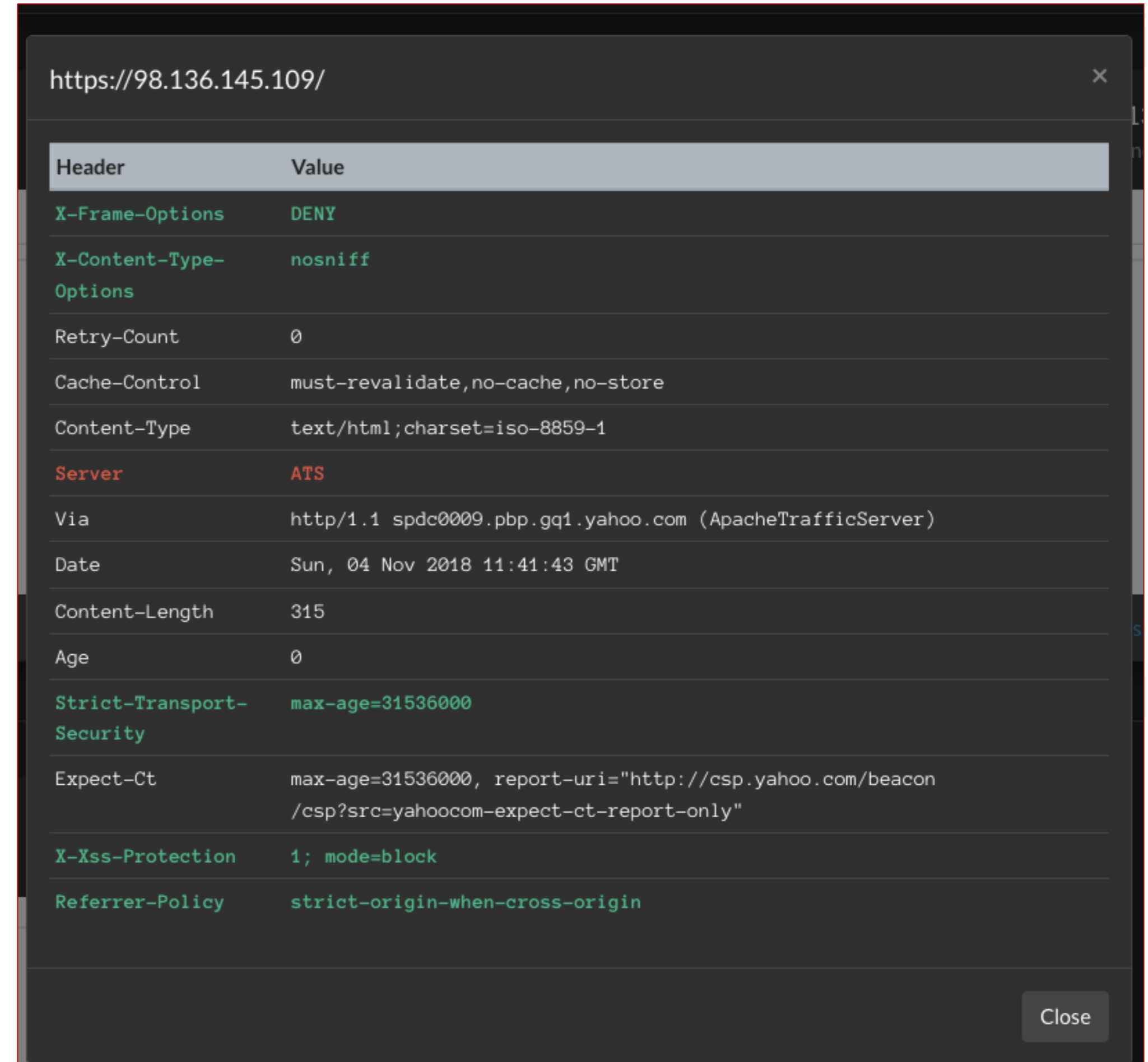
[https://michenriksen.com/images/aquatone\\_1\\_3\\_2/masscan.png](https://michenriksen.com/images/aquatone_1_3_2/masscan.png)



# Visualisation



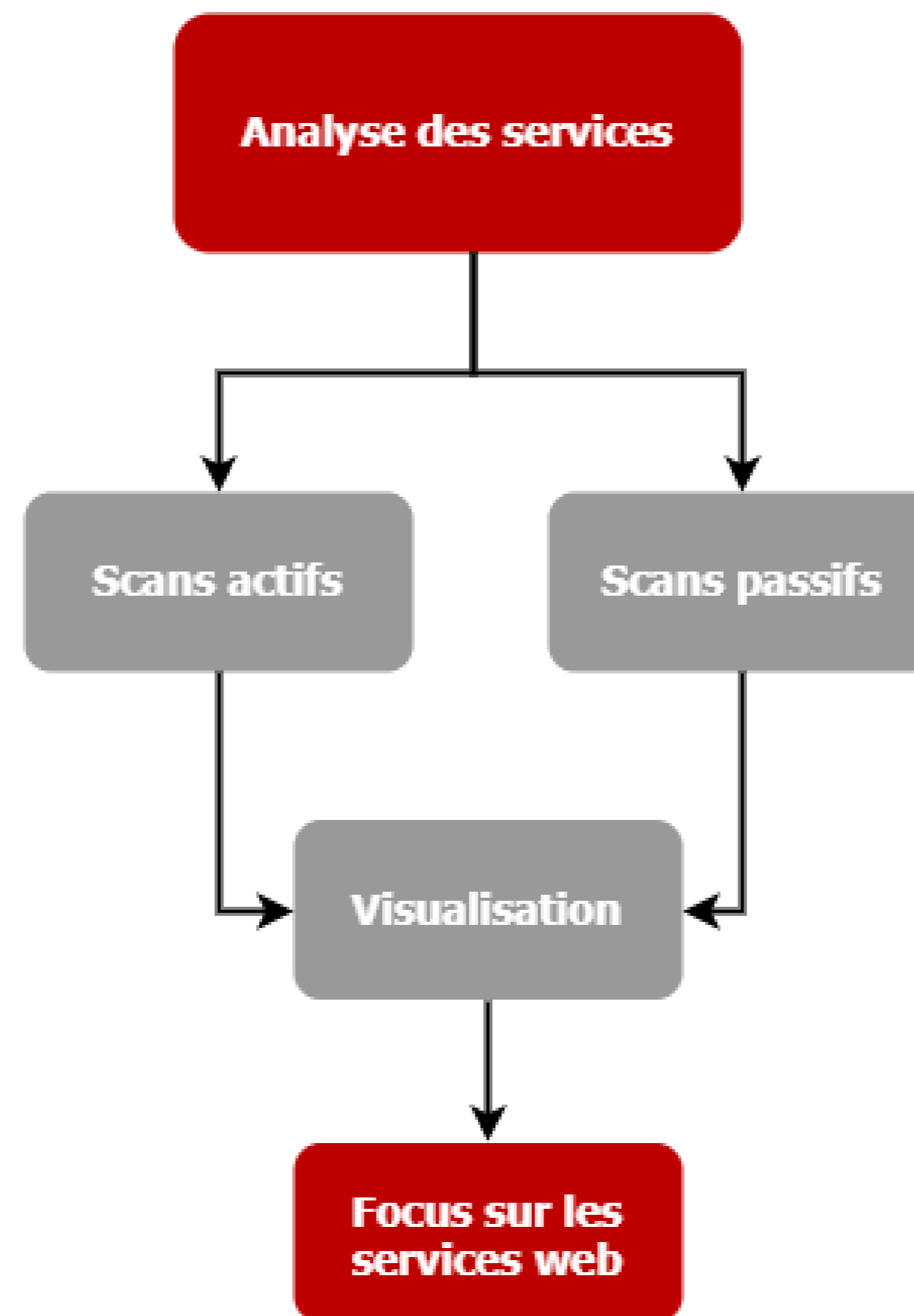
[https://michenriksen.com/images/aquatone\\_1\\_3\\_2/masscan\\_report.png](https://michenriksen.com/images/aquatone_1_3_2/masscan_report.png)



[https://michenriksen.com/images/aquatone\\_1\\_3\\_2/report\\_details.png](https://michenriksen.com/images/aquatone_1_3_2/report_details.png)



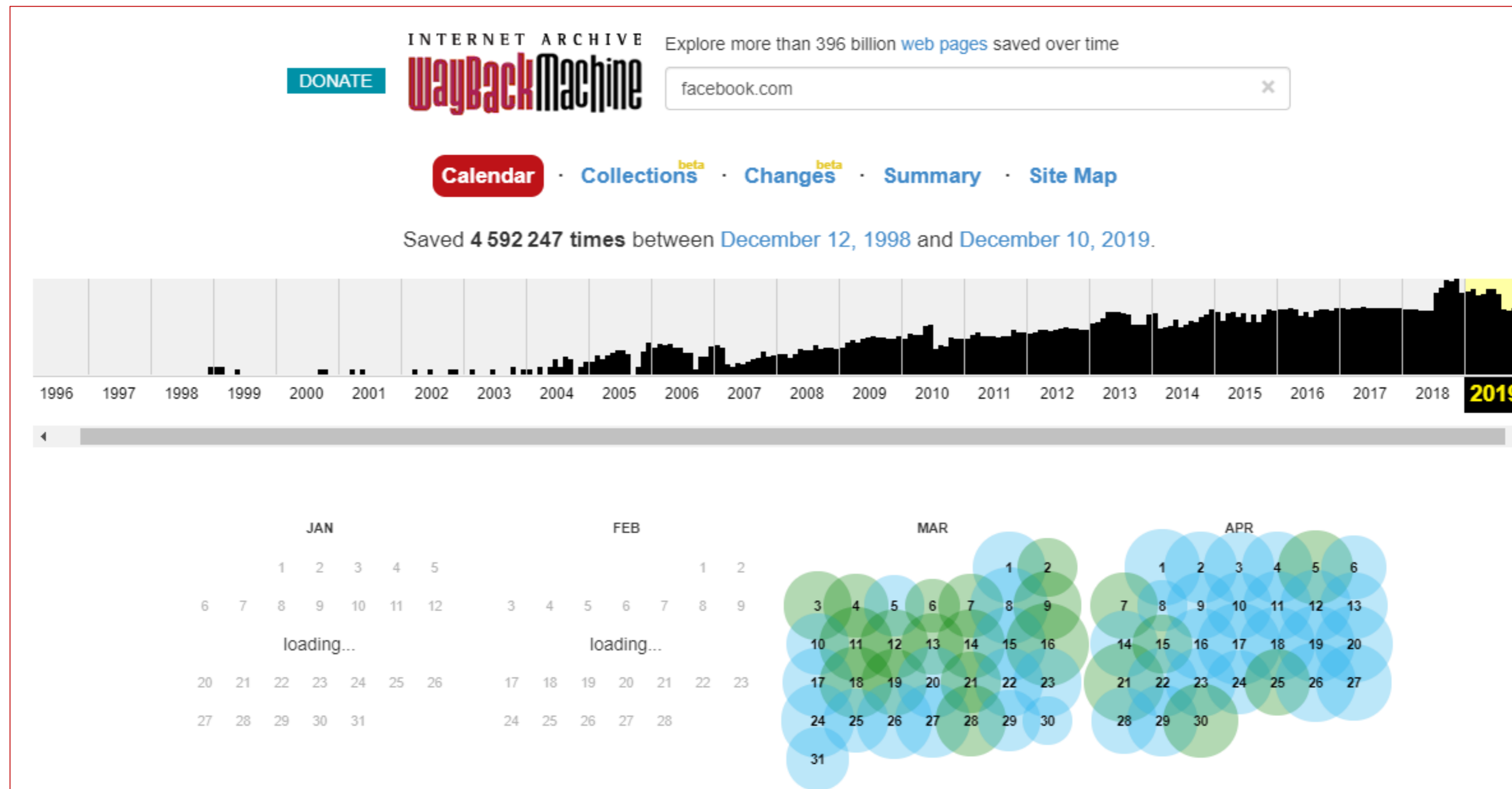
# Focus sur les services web





# Archives web

- The Internet Archive (Wayback Machine)
- Capture et enregistre des pages web depuis 1996
- Identifier des pages désormais inaccessibles



# Archives web

Go JAN FEB MAR  
2005 2006 2007

facebook login register help

Welcome to Facebook!

Facebook is an online directory that connects people through social networks at schools.  
The site is open to a lot of schools, but not everywhere yet. We're working on it.

You can use Facebook to:

- Look up people at your school.
- See how people know each other.
- Find people in your classes and groups.

Login Register

about contact jobs advertise  
a Mark Zuckerberg product  
Facebook © 2006

```

220
221 </div>
222 <!-- content -->
223
224 <div id="pagefooter">
225 <ul id="fnav">
226 <li><a href="https://web.archive.org/web/20060228155307/http://www.facebook.com/about.php">about</a></li>
227 <li><a href="https://web.archive.org/web/20060228155307/http://www.facebook.com/contact.php">contact</a></li>
228 <li><a href="https://web.archive.org/web/20060228155307/http://www.facebook.com/jobs.php">jobs</a></li>
229 <li><a href="https://web.archive.org/web/20060228155307/http://www.facebook.com/media.php">advertise</a></li>
230 <li><a href="https://web.archive.org/web/20060228155307/http://www.facebook.com/terms.php">terms</a></li>
231 <li><a href="https://web.archive.org/web/20060228155307/http://www.facebook.com/policy.php">privacy</a></li>
232 </ul>
233 <p>a Mark Zuckerberg production</p>
234 <p>Facebook <span title="9">&copy;</span> <span title="10.1.0.77">20</span><span title="760136">06</span></p>
235 </div>

```



# Archives web

- Outil Waybackurls par @tomnomnom : <https://github.com/tomnomnom/waybackurls>

```
user@server:~/Tools$ echo 'www.netsecure-day.fr' | ./waybackurls
http://netsecure-day.fr
http://www.netsecure-day.fr:80/?p=14
http://www.netsecure-day.fr:80/?p=2173
http://www.netsecure-day.fr:80/?p=617
http://www.netsecure-day.fr:80/?p=643
http://www.netsecure-day.fr/_images/favicon.ico
http://netsecure-day.fr/_images/logo.png
http://www.netsecure-day.fr:80/_mail/Hack'in_Day.html
http://www.netsecure-day.fr:80/association
http://www.netsecure-day.fr:80/cdn-cgi/l/email-protection
http://www.netsecure-day.fr:80/comments/feed/
http://www.netsecure-day.fr:80/conference-nsd14/
http://www.netsecure-day.fr:80/contact/
```



# Code côté client

- Fonctionnalités / design des pages web
- Chercher certains mots-clés : « api », « url », « // », « http:// », « https:// », « location.search », etc.
- Chercher les paramètres / variables, références à des fonctionnalités « cachées »
- Chercher les commentaires



# Code côté client

## Exemple : LinkFinder

```
user@server:/tmp/LinkFinder$ python3 linkfinder.py -i https://fr.yahoo.com -d -o cli
```

```
Running against: https://s.yimg.com/oa/build/js/site-a4d72cd5.js
```

```
/beacon
application/json
/api/cms/entry/athena/
https://s.yimg.com/oa/build/css/site-ltr-ffbc30a0.css
image/png
https://s.yimg.com/oa/build/images/favicons/yahoo.png
6nqIfv7x/MZnl2Sp8W7ddSZ0jR7ZAxyj
/redirect?to=https%3A%2F%2Fmydata.oath.com%2F%23sharingdata
/collectConsent/partners?sessionId=3_cc-session_0a2b864e-b274
FR&step=EU_SINGLEPAGE
/consent
https://guce.yahoo.com/copyConsent?sessionId&#x3D;3_cc-se
212677be758a&inline&#x3D;false&lang&#
https://fr.yahoo.com/?guccounter&#x3D;1
```

### File: <https://s.yimg.com/oa/build/js/site-a4d72cd5.js>

[/beacon](#)

```
var url = '/beacon';
```

[/api/cms/entry/athena/](#)

```
var mapiUrl = 'https://' + domain + '/api/cms/entry/athena/ + editionCode + '-' + entryId;
```

### File: [/api/cms/entry/athena/](#)

[/redirect?to=https%3A%2F%2Fmydata.oath.com%2F%23sharingdata](#)

Découvrez - en plus sur la manière dont < a href = "[/redirect?to=https%3A%2F%2Fmydata.oath.com%2F%23sharingdata](#)"





# Bruteforce

- Virtual host : <https://github.com/codingo/VHostScan> par @codingo\_
- Paramètres GET / POST
  - <https://github.com/maK-/parameth> par maK-
  - <https://github.com/s0md3v/Arjun> par @s0md3v
- Répertoires / fichiers
- Mire d'authentification
- Dictionnaires : <https://github.com/danielmiessler/SecLists> par @danielmiessler



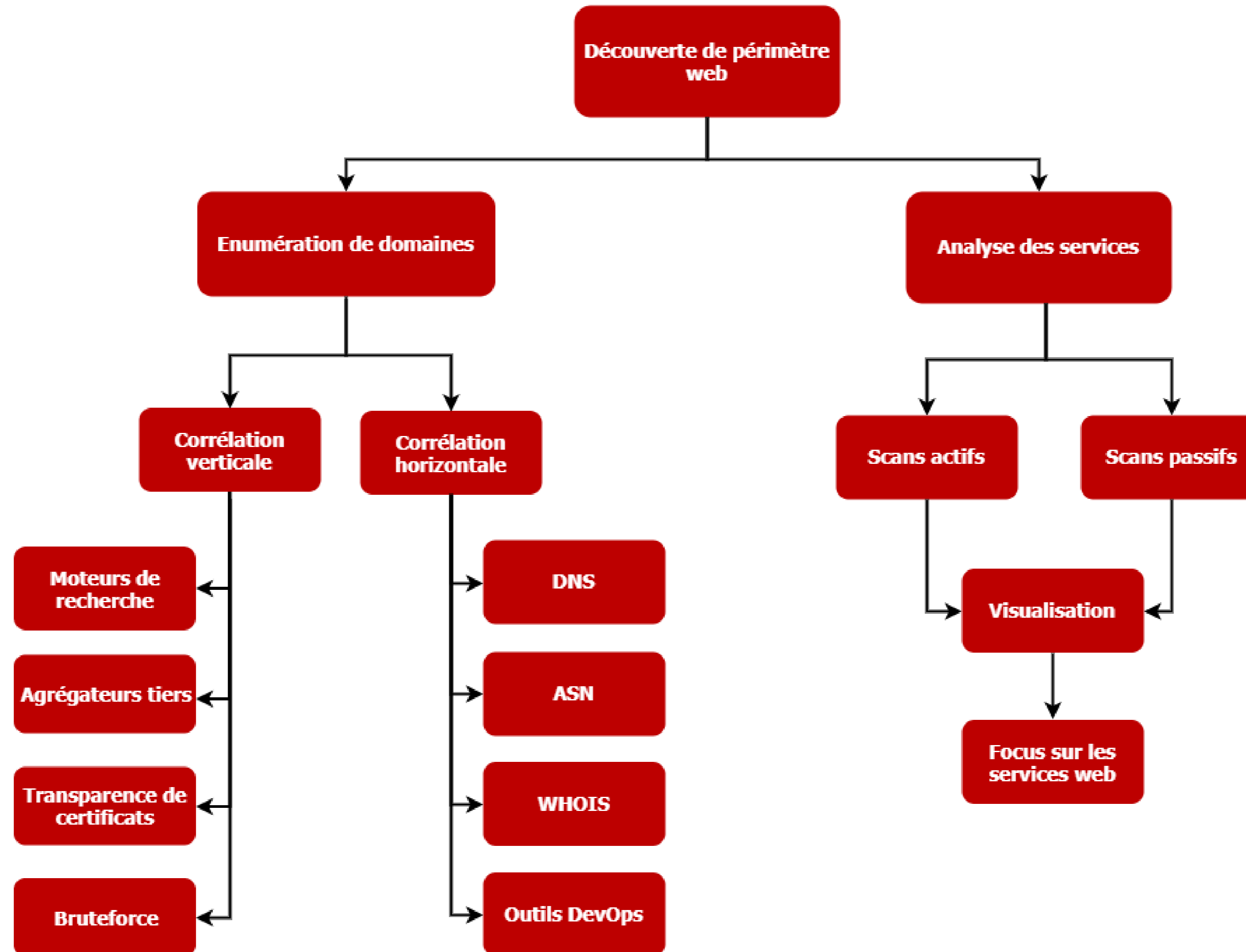
# Application mobile

- Version mobile d'une application web
- Différentes versions, différents endpoints
- Téléchargement d'APK :
  - <https://apkpure.com/>
  - <https://apps.evozi.com/apk-downloader/>
  - <https://www.apkmirror.com/>
- <https://github.com/s0md3v/Diggy/blob/master/diggy.sh>





# Conclusion



# Conclusion

- Nombreux outils, nombreuses sources de données
- Peu coûteux et très utile
- Automatisation nécessaire :
  - Périmètres larges
  - Agrégation des données
- Mise en place de monitoring :
  - Fuites de données (identifiants de collaborateurs)
  - Usurpation d'identité (certificats frauduleux)
  - Services publiés
  - Legacy



Merci !







**INTRINSEC**  
Innovative by design

# Contact



[contact@intrinsec.com](mailto:contact@intrinsec.com)



01 41 91 77 77



[www.intrinsec.com](http://www.intrinsec.com)

