Baromètre de la sécurité DNS 2021 (1ère édition)

Présentation des informations clés

Alexandre MARGUERITE (Cofondateur – Merox)
Olivier LACOMBE (Président associé – Subvitamine)

Digital113
Cluster numérique Sud de France

Les intervenants

Oliver Lacombe

CEO Subvitamine

Membre du Comex Digital 113

Alexandre Marguerite

Co-fondateur de Devensys Cybersecurity & Merox

Formateur CISSP, CEH, CHFI…

Digital113

Sommaire

Digital113
Cluster numérique Sud de France

Digital113
Cluster numérique Sud de France

Innovation & Transformation

Business & Croissance

Stratégie & Financement

Recrutement & Diversité

International

Digital 113 connecte, soutient et fédère les décideurs du numérique d'Occitanie afin de développer l'excellence de leurs entreprises

1 gouvernance de **48 chefs d'entreprise du numérique**

1 équipe de **13 permanents**

1 budget de **1,4 M€**

Près de 300 entreprises, 15000 salariés

Digital113

Les actions de Digital 113

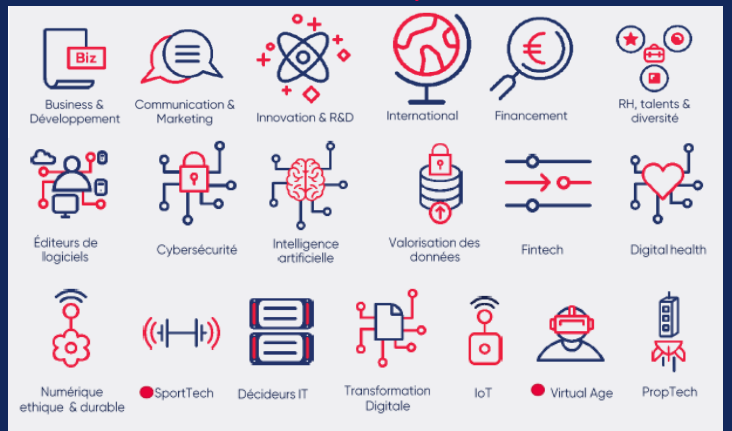
Digital 113 déploie des actions de différentes nature
animations, événements, services, projets
pour répondre aux besoins des entreprises :

- Innover, trouver des partenaires, s'inspirer…
- Recruter, maintenir l'emploi
  et faire monter les collaborateurs en compétences
- Faire du business en France et à l'étranger
- Travailler la stratégie et obtenir des financements
- S'informer, réseauter, échanger
- Se faire connaître
- Se faire représenter, être accompagné
- Obtenir des avantages

Digital113
Cluster numérique Sud de France

Quelques exemples…

Les Factory

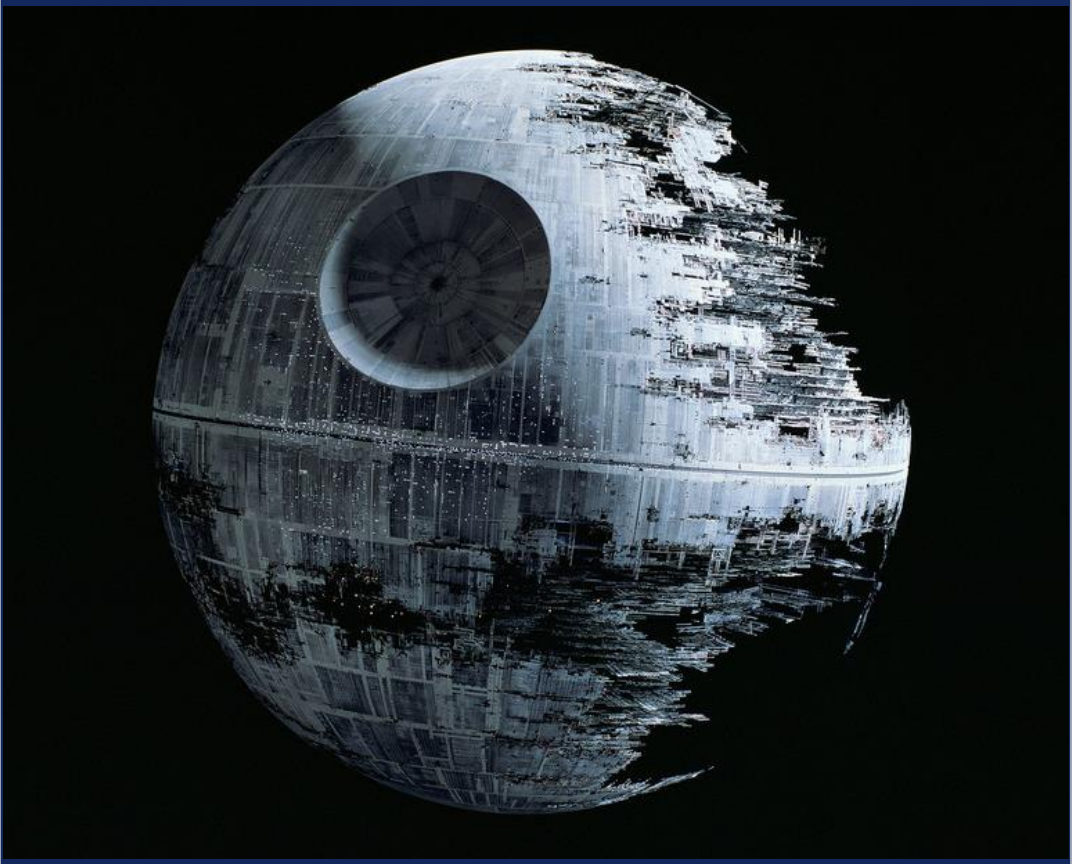


Contexte

- **SPF, DMARC, DKIM…** sont des protocoles primordiaux pour garantir la sécurité de tous
- … mais **peu connus**, **peu utilisés**, **mal implémentés**
- Dans les serveurs DNS se trouvent notamment des configurations capitales pour le **bon fonctionnement** des services emails :
  - assurer la délivrabilité
  - assurer la vérification de l'identité d'un expéditeur, empêchant ainsi le « spoofing » (usurpation)
- Le **DNS agit ici comme « les pages jaunes »** communiquant au monde entier des informations « vérifiées » (un numéro vous appelle se faisant passer pour les impôts, vous vérifiez dans l'annuaire si c'est un de leurs numéros bien listé à la rubrique « impôts »)
- Des protocoles gratuits, « ancestraux » comme SPF ou plus récents comme DMARC doivent être utilisés pour sécuriser et assurer une meilleure délivrabilité des ses emails. Et ce n'est pas tout (DKIM, BIMI…)

Digital113
Cluster numérique Sud de France

Objectifs



- **Analyser l'utilisation des protocoles de sécurité des DNS de certains groupes d'entreprises**
- **Mettre en lumière les progrès à faire en terme de sécurisation des DNS**
- **Permettre une prise de conscience sur l'importance des bons paramétrages des DNS**

Digital113
Cluster numérique Sud de France

Méthodologie

Analyse des configurations DNS auprès d'un échantillon de noms de domaines appartenant à des entités privées et publiques variées.

Ces entités sont toutes classées/issues de différents « groupes » (CAC40, French Tech 120, Digital 113, Hexatrust, Station F, Nubbo Toulouse, Grandes métropoles, Grandes villes, sites gouvernementaux, Alexa Top 50 FR…).

En bref :

- + de 730 noms de domaines analysés
- Données compilées entre le 10 et le 26 juin 2021
- Un seul nom de domaine analysé pour chaque entité
- Utilisation des outils et scanners DNS de « Merox » pour collecter les datas

Digital113
Cluster numérique Sud de France

Baromètre DNS

Présentation des statistiques et informations clés sur les données collectées et analysées des différents domaines scannés.

I. Des protocoles existants souvent mal maitrisés (SPF…)

II. Des protocoles critiques méconnus et peu déployés (DMARC…)

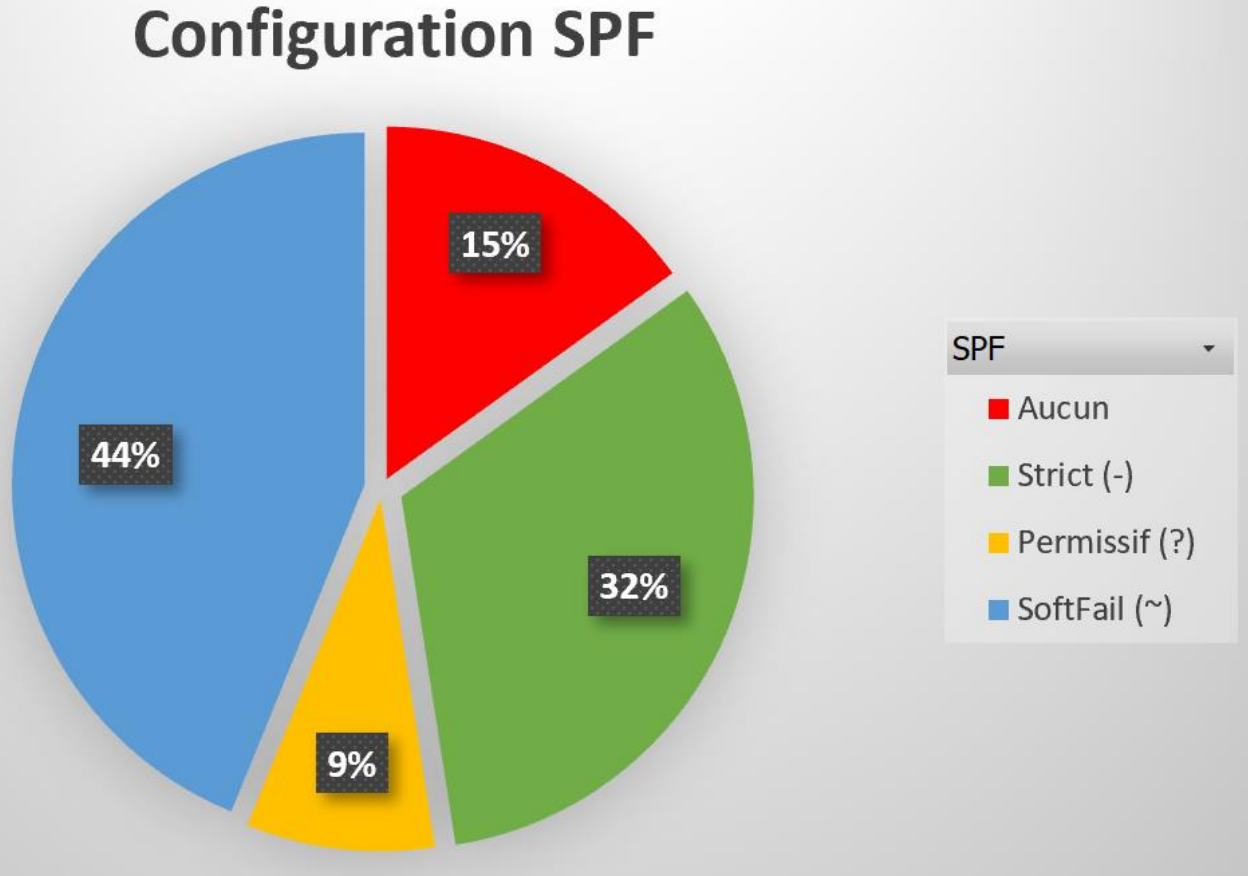
III. Les grandes entreprises en retard, mais moins que les autres

IV. Les services publics et collectivités ont aussi du travail à faire

Digital113
Cluster numérique Sud de France

4. Informations clés

Des protocoles existants souvent mal maitrisés (SPF…)



Sur 730 domaines analysés au niveau du SPF (Sender Policy Framework) :

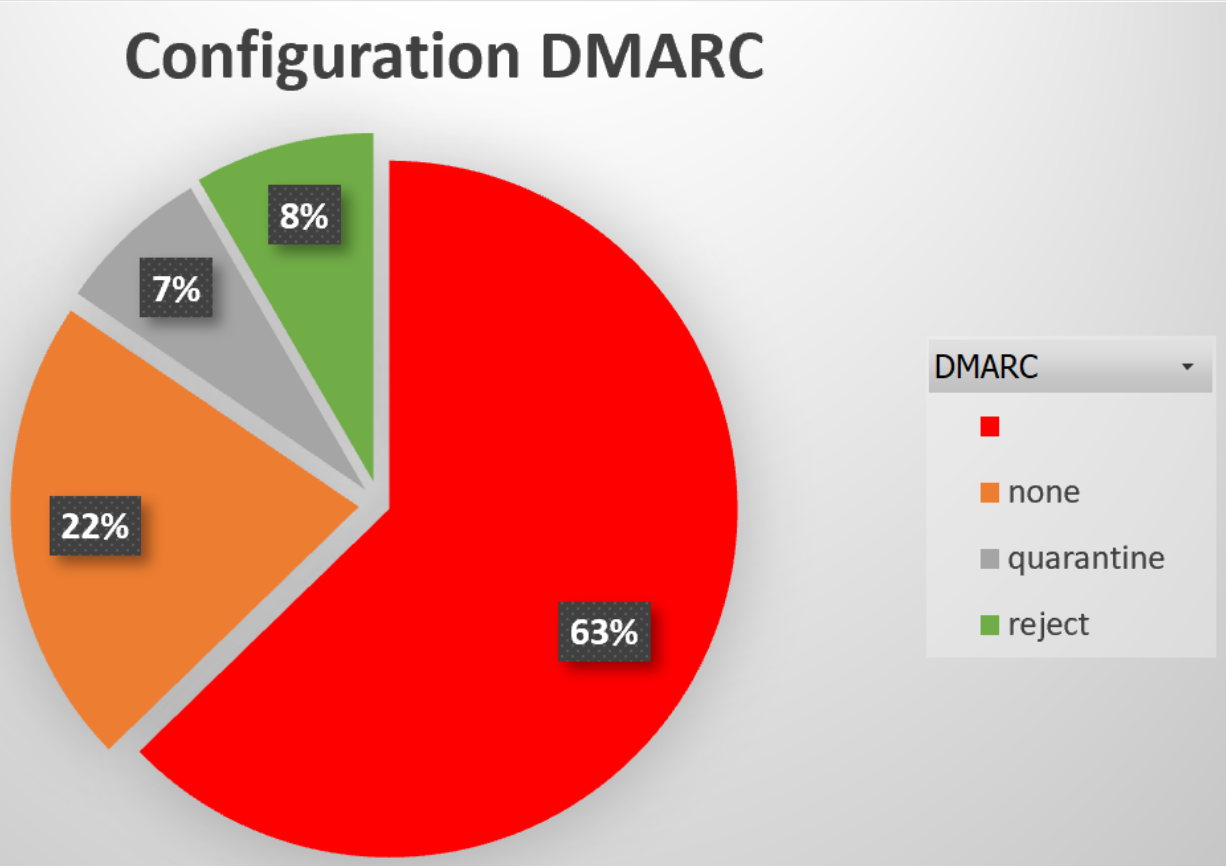
- 15% (110) n'ont aucune configuration SPF !
- 9% (63) en ont une… dangereuse "?all"
- 44% (320) en ont une pas assez stricte "~all"
- 32% (237) en ont une stricte "-all"

15x domaines ont même deux entrées SPF différentes, ce qui n'est pas supporté.
Une grande ville française en a même 3 (non, ce n'est pas Toulouse^^)

Mais le SPF est « imparfait » et ne protège pas de toutes les attaques de « spoofing ».

4. Informations clés

Des protocoles critiques méconnus et peu déployés (DMARC…)



Sur 730 domaines analysés au niveau du DMARC (Domain-based Message Authentication, Reporting, and Conformance) :

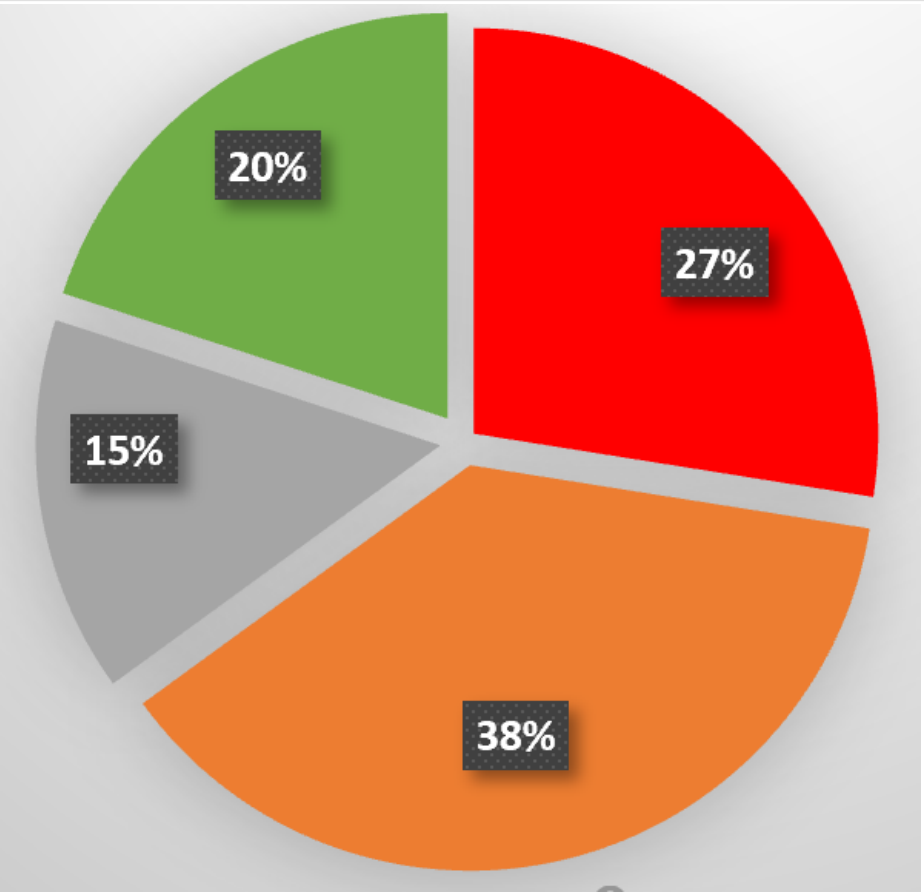
- 63% (458) n’ont aucune entrée DMARC !
- 22% (159) en ont une… inactive “none”
- 7% (52) en ont une intermédiaire "quarantine"
- 8% (61) en ont une stricte "reject"

Mais le DMARC (tout comme le SPF) n’est efficace que lorsqu’il est déployé sur TOUS les domaines et les sous-domaines d’une même organisation (.fr .com …)

Pour rappel, l’ANSSI le recommande depuis longtemps.

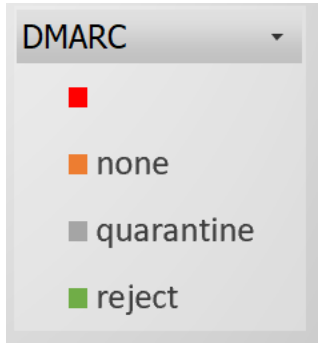
4. Informations clés

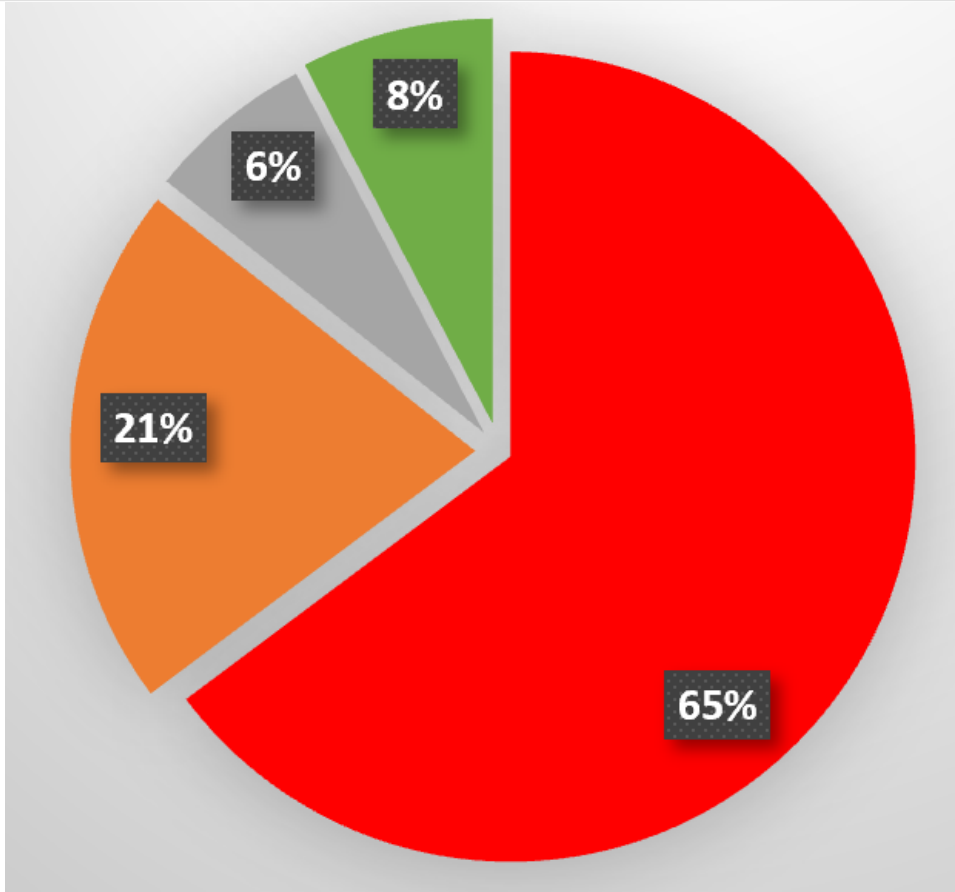
DMARC : Les grandes entreprises en retard - mais moins que les autres



“CAC40”

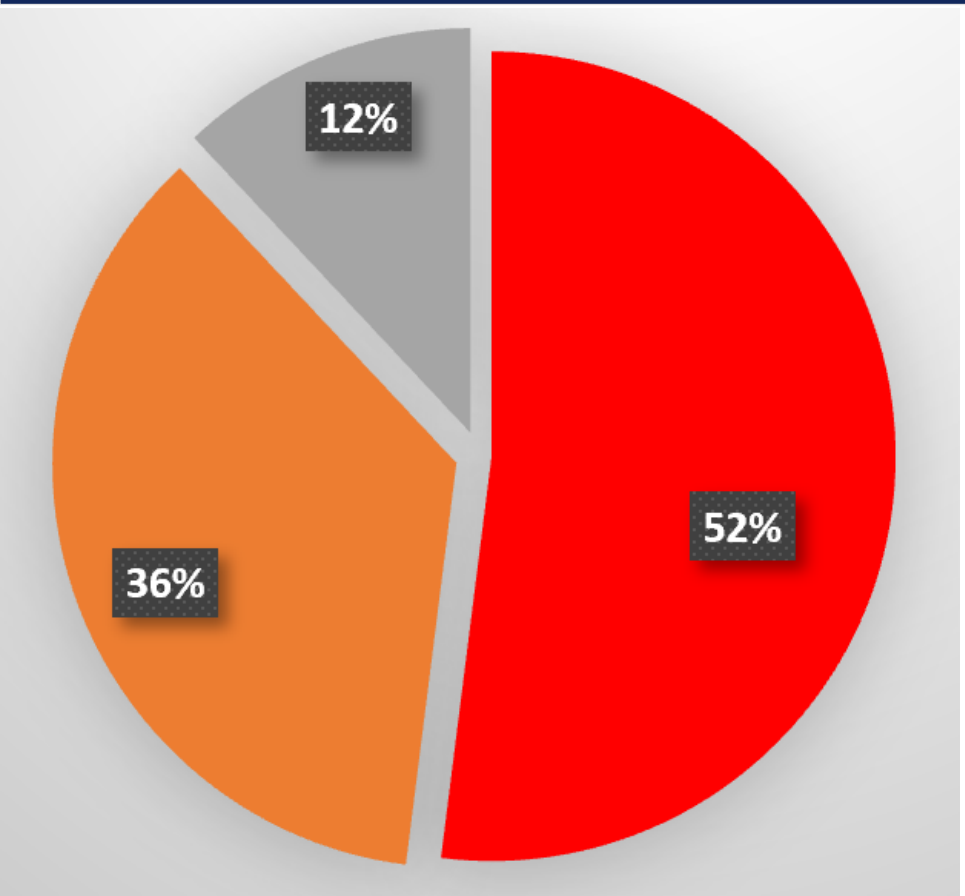
“Le Reste”
(hors CAC)



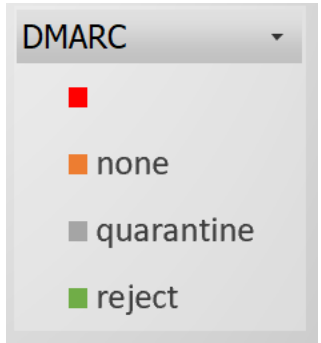


4. Informations clés

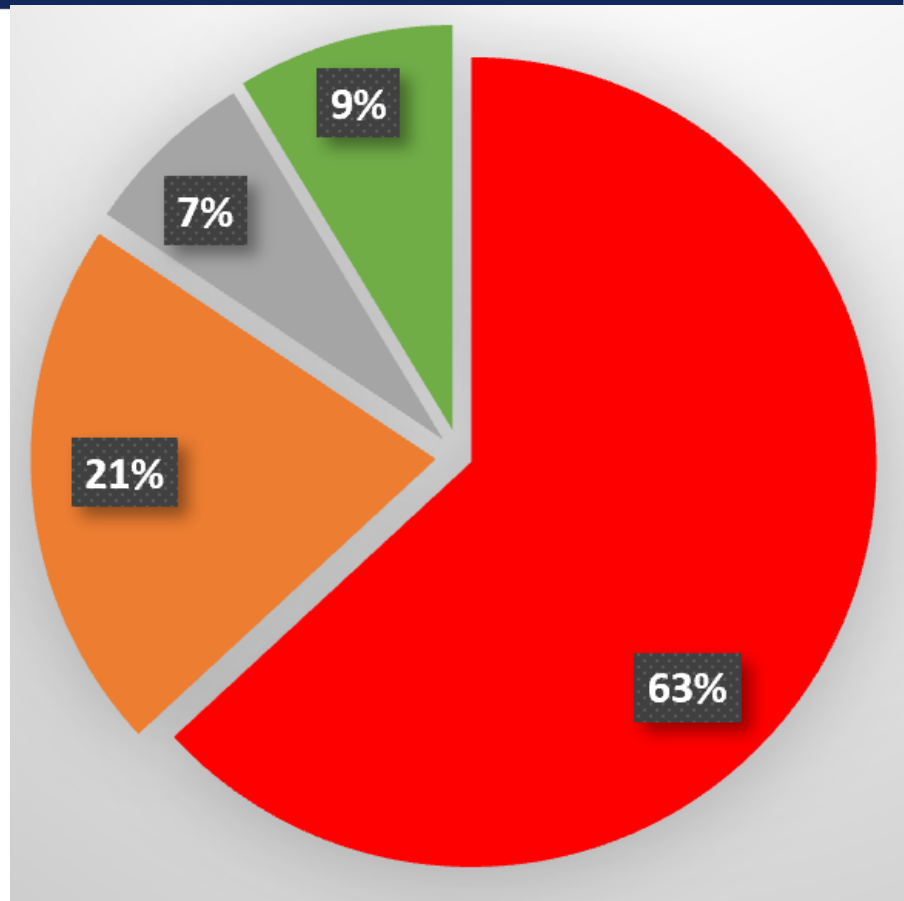
DMARC : Les services publics et collectivités ont aussi du travail à faire



Echantillon de sites publics
+ top metropoles
+ top villes



“Le Reste”



Pour aller plus loin

De nombreuses ressources sont disponibles :

- **Guide de l'ANSSI** « Recommandations relatives à l'interconnexion d'un système d'information à internet v3 » (§ 5.4)
- Guides de la Global Cyber Alliance « **DMARC Bootcamp** » (Weeks 1 to 5)
- Rapport GARTNER « **Best Practices for Implementing DMARC** »
- Différents **guides du CIS** (Center for Internet Security)
- **DMARC.org**

Le baromètre complet sera disponible sur https://barometre.merox.io

Digital113
Cluster numérique Sud de France

Questions ?

Digital113

Cluster numérique Sud de France

RETROUVEZ NOTRE ACTUALITÉ SUR

www.digital113.fr

@digital113_