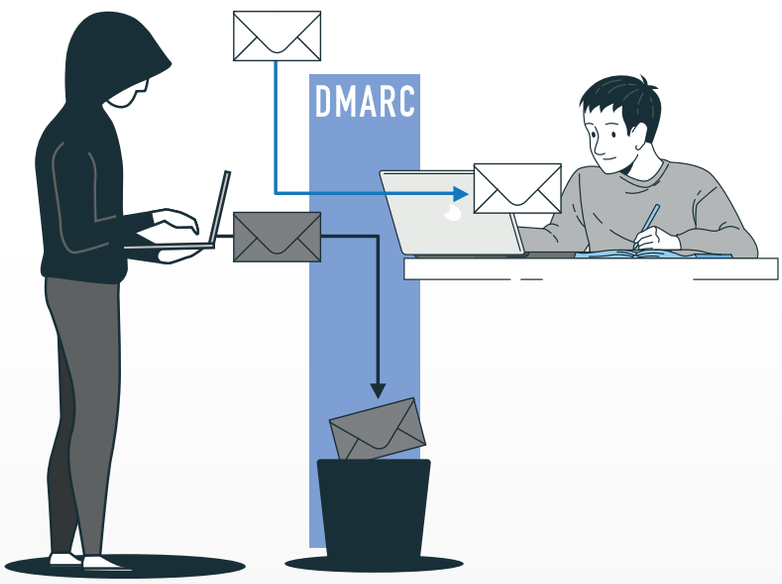
nameshield
Online Assets Security

Sécurisez votre messagerie avec le DMARC

L'email est le premier vecteur de communication en entreprise. C'est aussi le premier vecteur de cyberattaque aux conséquences dévastatrices pour les entreprises et les administrations.

Plusieurs protocoles, comme SPF, DKIM, DMARC et BIMI peuvent être déployés de façon efficace, afin de sécuriser votre messagerie, notamment contre le phishing.

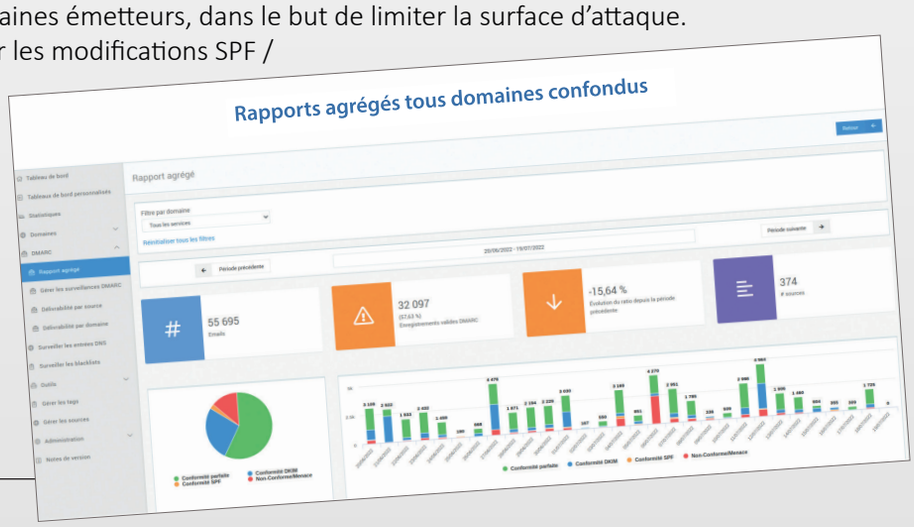


Pourquoi déployer une politique DMARC ?

- pour empêcher l'usurpation des domaines émetteurs de mails et protéger les domaines parkings, trop souvent oubliés.
- pour améliorer la délivrabilité des mails car les flux sont mieux structurés et correctement authentifiés, ce qui les rend plus fiables du point de vue des webmails et anti-spams.
- pour mettre en place le protocole BIMI, qui permet d'afficher le logo de la marque dans la boite mail des destinataires.
- pour optimiser les stratégies d'utilisation des noms de domaine pour les envois de mails et restructurer les différents flux si nécessaire, à l'aide des rapports DMARC.

L'accompagnement Nameshield, des services adaptés à vos besoins

- Paramétrage de la plateforme Merox.
- Accompagnement dans la publication du DMARC à none sur tous les domaines.
- Vérification des SPF (syntaxe, liste IP, valeur dépréciée ou vide, …).
- Proposition d'adaptation des sous-domaines émetteurs, dans le but de limiter la surface d'attaque.
- Analyse des RUA et préconisations pour les modifications SPF / DKIM nécessaires.
- Recommandation des modifications à effectuer : DMARC quarantine, reject et mise en conformité des entrées SPF et DKIM.
- Suivi des comportements anormaux, des tentatives de phishing et sensibilisation.

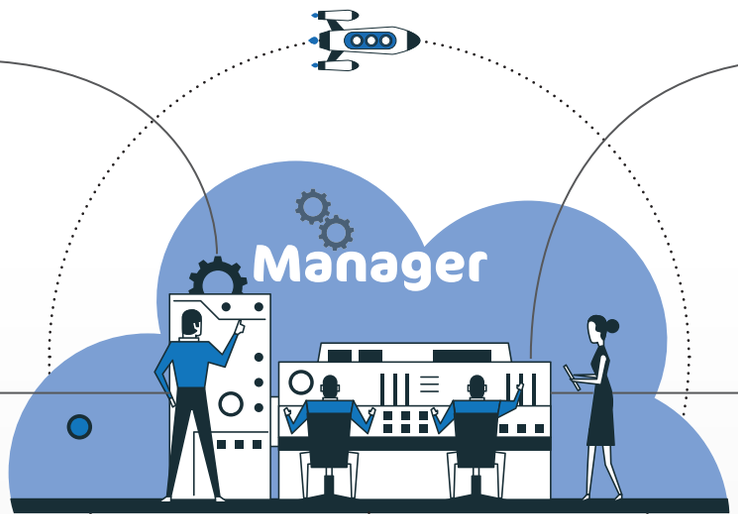


La plateforme Merox

nameshield
Online Assets Security

DMARC une solution simple

pour aider les administrateurs à avancer rapidement



Bloquer

Bloquez toute tentative d'usurpation et d'e-mails non légitimes.

Collecter

Mettez en place le process de collecte des données avec la publication du DMARC.

Authentifier

Authentifiez votre trafic et mettez-vous en conformité.

Analyser

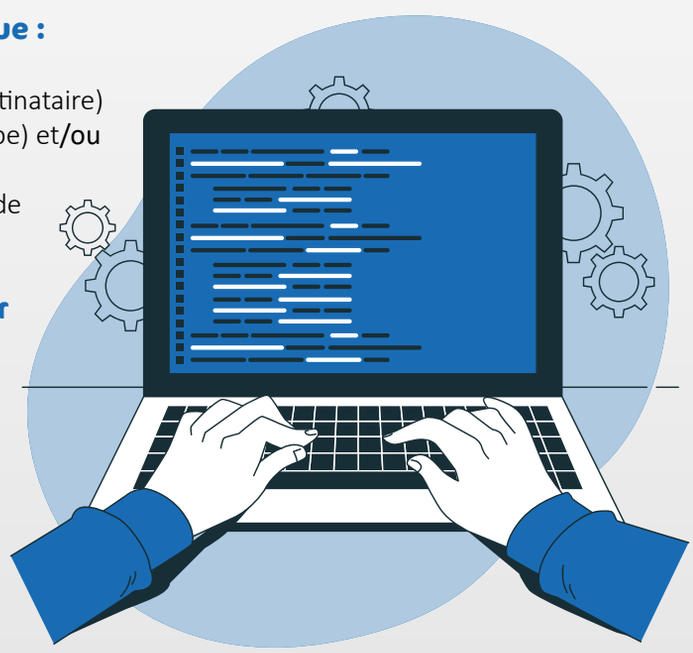
Identifiez et analysez votre écosystème légitime.

Implémenter

Paramétrez votre SI suite aux recommandations des experts.

Pour être conforme à la norme DMARC, il faut que :

1. le domaine du Header From (domaine visible par le destinataire) soit **aligné** avec le domaine du SPF (domaine d'enveloppe) et**/ou** avec le domaine du DKIM (d=) ;
2. l'authentification SPF et**/ou** DKIM soit valide (en plus de l'alignement).



DMARC permet à l'émetteur de spécifier la politique d'acceptation des mails non-conformes aux webmails et anti-spam qui vont les réceptionner. Il y a 3 politiques possibles :

- none ➔ le détenteur du domaine laisse le libre arbitre au webmail/anti-spam du destinataire en cas de non-conformité DMARC : les mails peuvent être acceptés, mis en spam ou rejetés.
- quarantine ➔ le détenteur du domaine indique aux webmails/anti-spam des destinataires que les mails non-conformes au DMARC doivent être mis en quarantaine lorsque cela est possible, ou dans les spams.
- reject ➔ le détenteur du domaine indique aux webmails/anti-spam des destinataires que les mails non-conformes au DMARC doivent être rejetés (bounce).