



SOLUTION DE SÉCURITÉ DES DOMAINES & DNS

- ✓ Gagnez en visibilité et maîtrisez votre environnement domaines et DNS
- ✓ Empêchez l'usurpation de votre identité pour des attaques de spoofing / phishing
- ✓ Augmentez votre niveau de conformité technique et légale, rassurez vos clients
- ✓ Améliorez votre délivrabilité email et la visibilité de votre marque



ÊTES-VOUS PROTÉGÉ CONTRE LE « DOMAIN SPOOFING » ?



Mon domaine est **spoofable** !

N'importe qui peut usurper votre identité en écrivant un email avec @votredomaine.fr

Vous n'avez pas implémenté le protocole DMARC ou votre politique de protection DMARC



Mon domaine est **protégé** !

Assurez-vous de ne pas bloquer d'emails légitimes par l'utilisation d'un outil d'analyse DMARC

Votre politique de protection DMARC est à "Quarantine" ou "Reject"



check.merox.io

TESTEZ
GRATUITEMENT
VOTRE DOMAINE
SUR NOTRE
TESTEUR DNS
PUBLIC

LES RISQUES



Problèmes de délivrabilité



Pertes financières et augmentation de la prime d'assurance



Usurpation d'identité et perte de confiance de ses clients, fournisseurs, partenaires...



Atteinte à l'image



Impact négatif du cyber score



Attaque au président

IDENTIFICATION DES EMAILS

SPF

Garanti que l'email provient bien d'une source connue et validée

Sender Policy Framework



2006

DKIM

Garanti que l'email n'a pas été modifié lors de son transport

Domain Key Identified Mail



2007

DMARC

Va aider le propriétaire d'un nom de domaine à empêcher son usurpation (spoofing)

Domain-based Message Authentication, Reporting & Conformance



2012

BIMI

C'est le "favicon" de l'email (logo de la marque à côté du titre du message)

Brand Indicators for Message Identification



2020

MACRO

ENVIRONNEMENT



L'Agence Nationale de la Sécurité des systèmes d'information :

- Les protocoles de vérification comme DMARC fortement préconisés : Guide de l'ANSSI : paragraphe 5.4 « [Protection contre les courriels illégitimes](#) »



US Homeland Security :

- Imposition à toutes les agences fédérales le déploiement du DMARC en 2017 : Article en ligne EN : « [Implementation of Email Authentication Services Across the Federal Government](#) »



Global Cyberalliance :

- Lutte contre les cyber-risques: Influent dans la démocratisation du DMARC et les protocoles d'authentification du DNS : Guide GCA EN : Chapitre 3 « [Benefits From GCA's DMARC Project](#) »

stoïk

- Critères d'évaluation par les assurances Cyber « [Le scan externe lancé par stoïk](#) »

- DMARC obligatoire dans certains pays : « In the U.S.A., U.K., Norway, Australia, and The Netherlands it's mandatory for governmental organizations to enforce DMARC »

-  « [DMARC Required For UK Government](#) »
-  « [Using DMARC in your organisation](#) »
-  « [DMARC](#) »
-  « [U.S. Government's DMARC Mandate](#) »
-  « [Articles about DMARC on the Government website](#) »

Obligatoire pour certains TLD :
exempldomain.bank « Create DMARC and SPF records for email authentication »

Registrants that have met requirements #1 and #2, and therefore appear in the .BANK or .INSURANCE zone, must publish a valid DMARC record whether or not the domain is used to send emails. If a vendor sends email on your behalf, sending with your *.BANK or *.INSURANCE domain email address, they must comply with [Security Requirement 6](#), Implementing TLS; *DNSSEC is not required*.

MACRO ENVIRONNEMENT



IMMUNITE cyber gendarmerie :
→ Activer des protocoles qui permettent de lutter contre l'usurpation d'adresse mail (comme SPF et DKIM qui renforcent la sécurité du nom de domaine). [Vulnérabilité très importante](#)

Administration et sécurisation – gestion de la messagerie			
Disposez-vous d'un outil dédié d'anti-spam et d'antivirus pour votre messagerie ?	NON / NSP	Vulnérabilité potentielle	Mettre en place une solution anti-spam et antivirus dédiée pour la messagerie, qu'elle soit hébergée en interne ou en externe. Les options intégrées dans les outils de messagerie sont souvent limitées. PEC - guide CT fiche 4 ANSSI - hygiène f. 24 et 31
Les utilisateurs sont-ils sensibilisés aux dangers liés à la réception de mails frauduleux ?	NON / NSP	Vulnérabilité très importante	Sensibiliser les agents en expliquant les risques encourus, les modes opératoires et les bonnes réactions (ne pas faire confiance dans l'adresse mail de l'expéditeur, se méfier des pièces jointes, ne jamais répondre à une demande d'informations confidentielles, vérifier les liens en passant la souris sur ces derniers sans cliquer,...). ACYMA - hameçonnage ANSSI - 5 réflexes ANSSI - protection messagerie
Votre messagerie utilise-t-elle des protocoles permettant de lutter contre les usurpations d'identité ?	NON / NSP	Vulnérabilité très importante	Activer des protocoles qui permettent de lutter contre l'usurpation d'adresse mail (comme SPF et DKIM qui renforcent la sécurité du nom de domaine). ANSSI - sécuriser* messagerie test sécurité messagerie



- [Point de contrôle 9 du CIS Center for Internet Security.](#)
- Implement DMARC : To lower the chance of spoofed or modified emails from valid domain, implement DMARC policy and verification,, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.5	Implement DMARC To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Network	Protect		●	●
9.6	Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		●	●
9.7	Deploy and Maintain Email Server Anti-Malware Protections Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			●



GDPR – UE :
→ Protection du DNS sujet central, DMARC protocole incontournable !

En Pologne : Les fournisseurs d'e-mail d'au moins 500 000 utilisateurs, 500 000 comptes actifs ou les entités publiques seront obligés d'utiliser un mécanisme d'authentification du e-mail. : « [Imposer l'authentification DMARC aux fournisseurs de messagerie e-mail](#) »



→ L'institut de conseil de renommée internationale, cite le DMARC comme projet prioritaire de cybersécurité : Téléchargez le rapport Gartner « [Best practices for implementing DMARC](#) »



→ Prise en considération par les sociétés de scoring de cybersécurité « [Voyez ce que les hackers voient](#) »

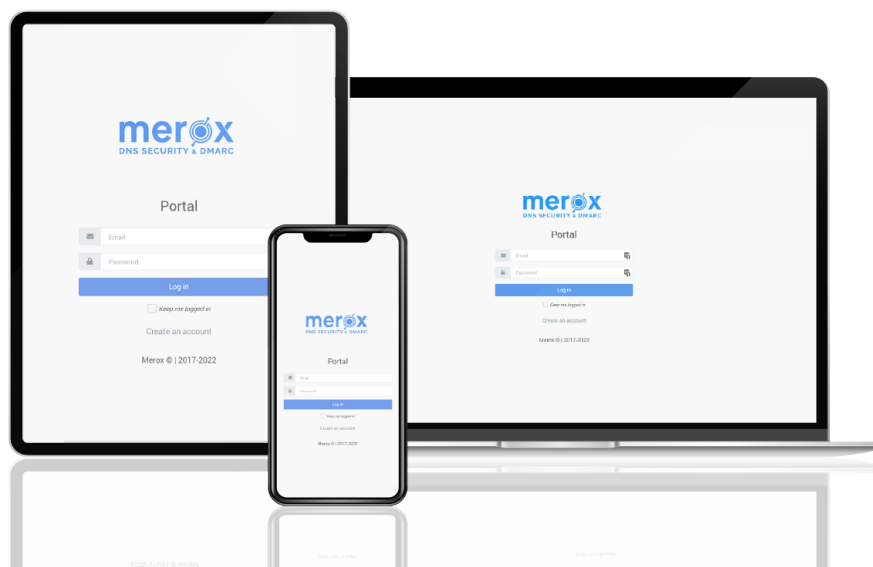
LA PLATEFORME MEROX

Fonctionnalités principales :

Merox est une plateforme SaaS modulaire de surveillance et pilotage de la cybersécurité orienté protection des DNS, de la marque et de la messagerie.

Les différents modules permettent ensuite de gérer et monitorer au quotidien plusieurs aspects techniques spécifiques :

- Cartographie et maîtrise de l'environnement DNS complet
- Analyse des rapports DMARC
- Surveillance et vérification des entrées DNS
- Surveillance des emails et blacklists
- Surveillance des domaines proches
- Conseils sécurité DNS
- Alertes sécurités
- Outils d'aide à l'analyse
- Gestion multi domaine (tags)



Rapidité de mise en place (<30 minutes)

Hébergement et développement 100% Européen (France)

100% "SPOF PROOF" architecture
Aucune délégation de prise en main sur les changements

LES AVANTAGES DE LA PLATEFORME

Plateforme "tout-en-un" de mise conformité des domaines et d'aide à l'implémentation de protocoles technique

2x Brevets déposés :
→ Chiffrement RUF (100% conforme au RGPD)
→ Scoring DNS avec actions automatique

Distribué à travers un réseau de partenaires certifiés

Objectifs :

- Proposer une interface de qualité, des conseils avisés, et des données pertinentes
- Aider à implémenter les protocoles de sécurité DNS
- Améliorer la sécurité de l'identité des entreprises
- Proposer un outil complet, simple et clef en main pour les utilisateurs.

ACCOMPAGNEMENT

Service des partenaires certifiés:

- Cartographie et ajout de tous les domaines : les émetteurs et de protection
- Analyse des rapports DMARC afin de rendre les émetteurs légitimes par l'implémentation SPF / DKIM
- Optimisation des SPF en respectant les recommandations (syntaxe, liste IP, valeur dépréciée ou vide, ...)
- Déterminer les cas d'usages (pas de messagerie, messagerie depuis un émetteur maîtrisé, messagerie depuis plusieurs émetteurs prestataires tiers)
- Rédaction de plan d'action par un expert maîtrisant les derniers RFC en vigueur
- Mise en place et suivi des alertes personnalisées
- Surveillance des noms de domaine enregistrés de l'organisation
- Surveillance des IPs chez les blacklisteurs
- Surveillance contre le cybersquatting et le typosquatting
- Service de détection des tentatives de phishing
- Rapports du volume d'emails et domaines détectés, protégés ou non, campagnes de phishing identifiées, amélioration de la délivrabilité ...
- Sensibilisation et aide au suivi de nouveaux protocoles BIMi, DNSSEC, MTA STS...

Chefferie de projet : Assistance des équipes cybersécurité, IT, DevOps, Marketing...



Assistance à la lecture de rapport DMARC



Conseil en politique de sécurité de la messagerie



Protection de la marque par l'analyse externe des noms de domaines (typosquatting, Threat Intelligence, actions de Takedowns)

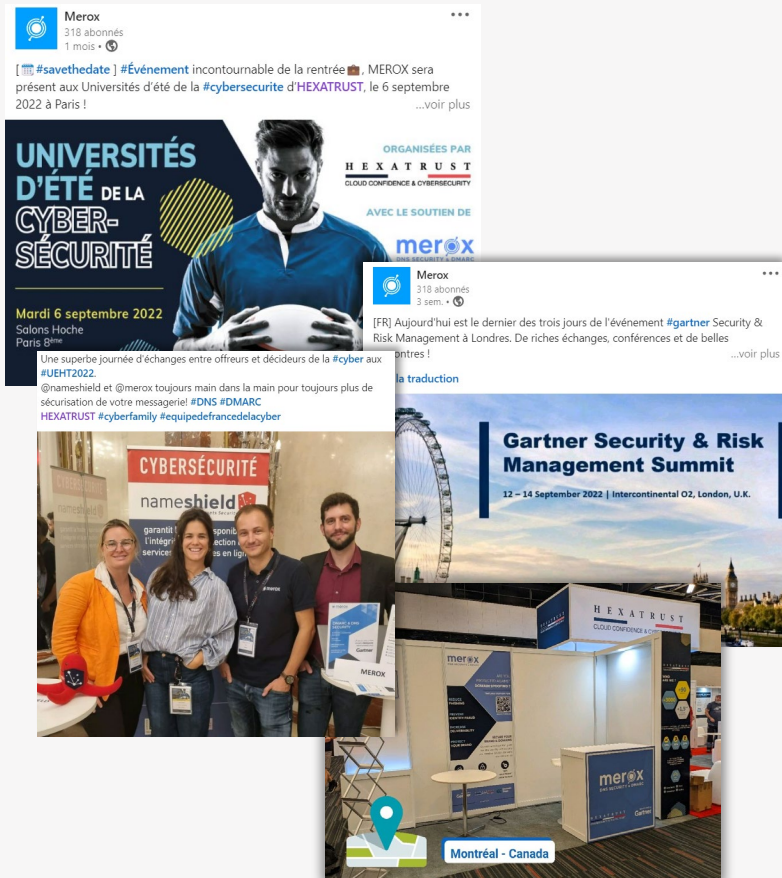


Conseil sur la délivrabilité et sécurité email (messagerie, transactionnelle, marketing...)



Conseils sur les dernières RFC, assistance à la rédaction d'une PSSI messagerie (template grand groupe, etc.)

LA SOCIÉTÉ MEROX



Ils nous font **confiance**



In Extenso



matmut



Nos partenaires



Certification



LinkedIn Merox

Merci !



CONTACT

+33 (0)9 80 80 26 26
contact@merox.io



SIÈGE SOCIAL

836 rue du Mas de Verchant
34000 Montpellier - France



SITE INTERNET

<https://www.merox.io>