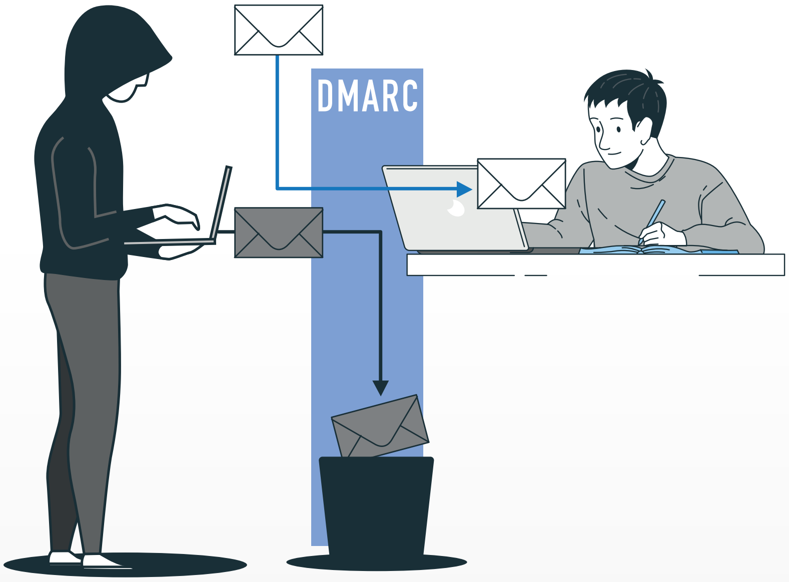
nameshield
Online Assets Security

Secure your e-mail system with DMARC

Email is the main vector of communication in companies. It is also the first vector of cyberattacks with devastating consequences for companies and administrations.

Several protocols, such as SPF, DKIM, DMARC and BIMI can be effectively deployed to secure your email system, particularly against phishing.

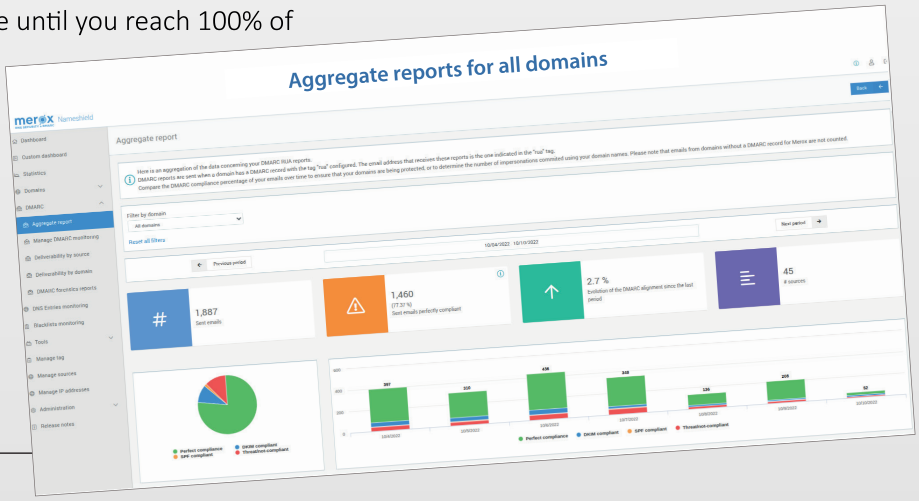


Why implement a DMARC policy?

- To prevent spoofing of the domains used to send emails and protect parked domains, which are too often forgotten.
- To improve emails deliverability: with email flows properly organized and authenticated, your emails will look more reliable to the webmails and anti-spam systems.
- To implement BIMI, which allows the brand logo to be displayed in the recipients' mailboxes.

Nameshield's support adapted to your needs

- Set up of the Merox's platform;
- Assistance in publishing a DMARC policy on all of your domains;
- SPF verification (syntax validity, IP list, deprecated or empty values, ...);
- Recommendation of the best possible emailing strategy in terms of domain use in order to minimize the risk of attack;
- Analysis of your RUA reports and recommendations to help you authenticate all your legitimate email traffic with DKIM and SPF;
- Assistance in the DMARC policy upgrade until you reach 100% of emails in "p=reject";
- Tracking of unusual behavior and phishing attempts.



Aggregate reports for all domains

Aggregate report

Here is an aggregation of the data concerning your DMARC RUA reports.
DMARC reports are sent when a domain has a DMARC record with the tag "rua" configured. The email address that receives these reports is the one indicated in the "rua" tag.
Compare the DMARC compliance percentage of your emails over time to ensure that your domains are being protected, or to determine the number of impersonations commited using your domain names. Please note that emails from domains without a DMARC record for Merox are not counted.

Filter by domain: All domains
Reset all filters

10/04/2022 - 10/10/2022

1,887
Sent emails

1,460
(77.37 %)
Sent emails perfectly compliant

2.7 %
Evolution of the DMARC alignment since the last period

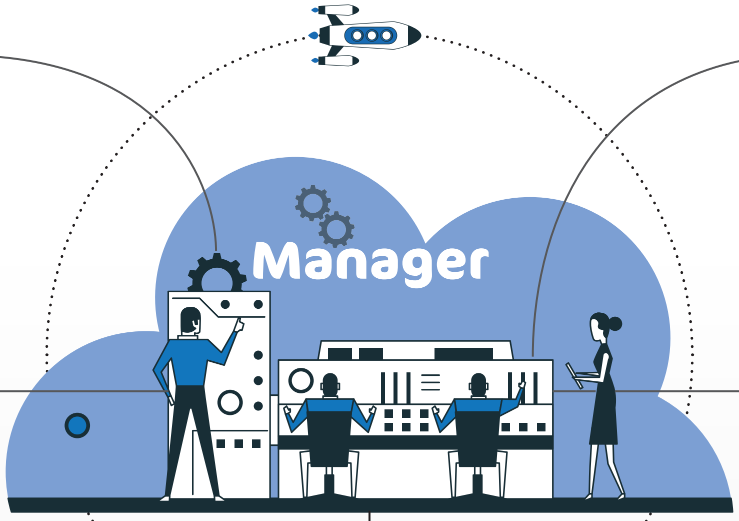
45
# sources

The Merox platform

nameshield
Online Assets Security

DMARC a simple solution

to help administrators to proceed quickly



Block

Block all spoofing attempts and non-legitimate emails.

Collect

Trigger the data collection process by publishing a DMARC policy.

Authenticate

Authenticate your traffic and become DMARC compliant.

Analyze

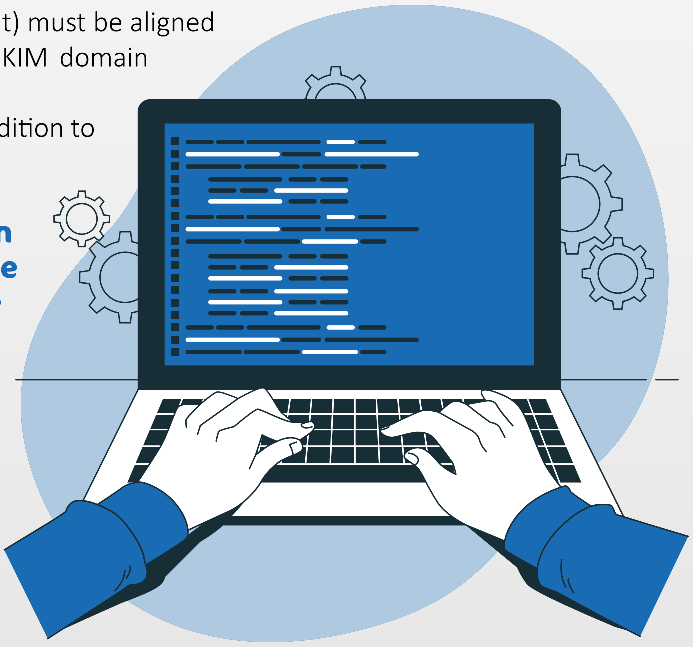
Identify and analyze your legitimate ecosystem.

Implement

Set up your IS following the experts' recommendations.

To be DMARC compliant:

1. the Header From domain (domain visible to the recipient) must be aligned with the SPF domain (envelope domain) and/or the DKIM domain (d=) ;
2. the SPF and/or DKIM authentication must be valid (in addition to the alignment).



DMARC allows the owner of the sending domain to specify what action should be taken on the receiving side (webmail or anti-spam of the recipient) when they see non-compliant incoming emails.

There are 3 possible policies:

- None ➔ the domain's owner leaves the choice to the recipient's webmail/anti-spam in case of DMARC non-compliance: emails can be accepted, put in the spam folder or rejected.
- Quarantine ➔ the domain's owner indicates to the recipient's webmail/anti-spam that emails that don't comply with DMARC should be put in quarantine when possible, or in the spam folder.
- Reject ➔ the domain's owner tells the recipient's webmail/anti-spam that emails that don't comply with DMARC should be rejected (bounced).

Illustration: Nameshield / Storyset.com