

Mise en place d'une politique de sécurité des emails



WEBERT Léo

IUT RESEAUX ET TELECOMMUNICATIONS

Clermont – Ferrand – 2024/2025

TRIVIUM
PACKAGING

 UNIVERSITÉ
Clermont Auvergne

 iut
réseaux
& télécoms

Remerciements

Je tiens tout d'abord à remercier chaleureusement Monsieur Roel SCHOUTEN, Vice-Président Information Security, mon tuteur professionnel chez Trivium Packaging, pour m'avoir offert une expérience professionnelle des plus enrichissantes. Son accompagnement, ses conseils et sa confiance m'ont permis de développer mes compétences et d'acquérir de solides connaissances dans le domaine de la cybersécurité.

Je souhaite également exprimer ma gratitude à Trivium Packaging pour m'avoir accueilli au sein de ses équipes et m'avoir donné l'opportunité de participer à des projets concrets et variés, afin de couvrir la majorité des aspects de la sécurité informatique.

Un grand merci à l'équipe Infosec de Trivium pour son accueil, sa disponibilité et leur bienveillance. Chacun de ses membres a contribué à rendre mon intégration plus facile et à favoriser les échanges techniques nécessaires à la réussite de mes missions.

Enfin, je remercie le département Réseaux et Télécommunications, ainsi que l'ensemble des enseignants de la spécialité, pour leur soutien académique. Leur encadrement m'a guidé dans la rédaction de ce rapport et dans la réflexion sur mon projet professionnel.

*Veuillez noter que tous les termes suivis du symbole « * » seront définis dans le glossaire*

Table des matières

Remerciements	2
Table des matières	3
Table des figures	4
Introduction.....	5
I. Présentation et contextualisation	6
a. Trivium Packaging.....	6
1. Présentation de l'entreprise et positionnement international	6
2. Secteur d'activité et partenaires.....	7
b. Le service cybersécurité et ma mission.....	8
1. Besoins de l'entreprise	8
2. Existant technique	9
3. Objectif	10
c. Organisation du projet.....	12
1. Cahier des charges	12
2. Outils utilisés	13
3. Planning prévisionnel.....	14
II. Réalisation technique	14
a. Point de départ et choix de la solution.....	14
1. Principe et objectifs de DMARC.....	14
2. Rôle de la quarantaine : chaîne de traitement et impact sur les flux de messagerie	18
3. Comparatif des outils (DMARCian, OnDMARC, EasyDMARC, Valimail)	19
b. Implémentation de Valimail	20
1. Configuration de l'outil	20
2. Passage au plan « enforce » : analyse des rapports et montée vers p=reject.....	22
III. Bilan	23
a. Résultats techniques obtenus	23
b. Difficultés rencontrées.....	24
c. Perspectives d'évolution.....	24
Conclusion.....	25
Bilan Humain	25
English Summary	27
Bibliographie.....	28
Glossaire	29

Table des figures

Figure 1 - Carte des sites Européens de Trivium	6
Figure 2 - Diagramme de la branche Infosec de Trivium	7
Figure 3 - Exemple de rapport ESG	8
Figure 4 - Aperçu de la boîte mail de rapport DMARC	9
Figure 5 - Aperçu du type fichier XML reçu lors d'un rapport DMARC	10
Figure 6 - Exemple d'une tentative d'hameçonnage par usurpation d'identité.....	10
Figure 7 - Existant technique (P=none)	11
Figure 8 - Objectif final (P=reject)	11
Figure 9 - Logo de Valimail (source valimail.com).....	13
Figure 10 - Logo d'Outlook	13
Figure 11- Logo de Teams	13
Figure 12 - Logo de SharePoint	14
Figure 13 - Logo de Microsoft Defender EDR.....	14
Figure 14 - schéma du fonctionnement du protocole SPF.....	16
Figure 15 - schéma du fonctionnement du protocole DKIM.....	17
Figure 16 - schéma du fonctionnement du protocole DMARC.....	17
Figure 17 - Trajet d'un email sans politique active	18
Figure 18 - Règles de redirection des rapports DMARC	21
Figure 19 - Aperçu du tableau de bord de Valimail.....	22

Introduction

Dans le cadre de ma deuxième année de BUT Réseaux et Télécommunications, j'ai eu l'opportunité d'effectuer un stage de deux mois au sein de l'équipe cybersécurité de Trivium Packaging. Cette immersion m'a permis de me familiariser avec les enjeux concrets de la sécurité des systèmes d'information, tout en approfondissant mes connaissances sur les protocoles liés à la protection des flux de messagerie.

Le sujet principal de mon stage portait sur la mise en place d'une politique DMARC* (Domain-based Message Authentication, Reporting and Conformance), visant à protéger les domaines de messagerie de l'entreprise contre les campagnes de phishing*, le spam et l'usurpation d'identité. DMARC repose sur les mécanismes d'authentification SPF* et DKIM*, et permet de définir une politique claire pour le traitement des messages non conformes. L'objectif confié était de faire évoluer progressivement la politique existante de p=none, utilisée à des fins de surveillance, vers une politique stricte de p=reject, bloquant activement les emails frauduleux.

Ce travail soulève une problématique essentielle : comment renforcer efficacement l'authentification des emails entrants tout en maintenant la continuité des communications légitimes et sans perturber les services métiers, ou **comment mettre en place d'une politique de sécurité des emails ?**

Pour y répondre, ce rapport s'ouvre d'abord sur une présentation du contexte de l'entreprise, de son infrastructure de messagerie et des risques identifiés. Il poursuit avec une description détaillée des étapes techniques mises en œuvre pour atteindre une politique DMARC pleinement active, en s'appuyant notamment sur la plateforme Valimail et l'optimisation du processus de quarantaine. Enfin, il se conclut par un bilan des résultats obtenus, une analyse des difficultés rencontrées et une réflexion sur les perspectives d'amélioration, qu'il s'agisse de l'automatisation de certaines tâches ou de la montée en compétence sur des incidents plus complexes.

I. Présentation et contextualisation

a. Trivium Packaging

1. Présentation de l'entreprise et positionnement international

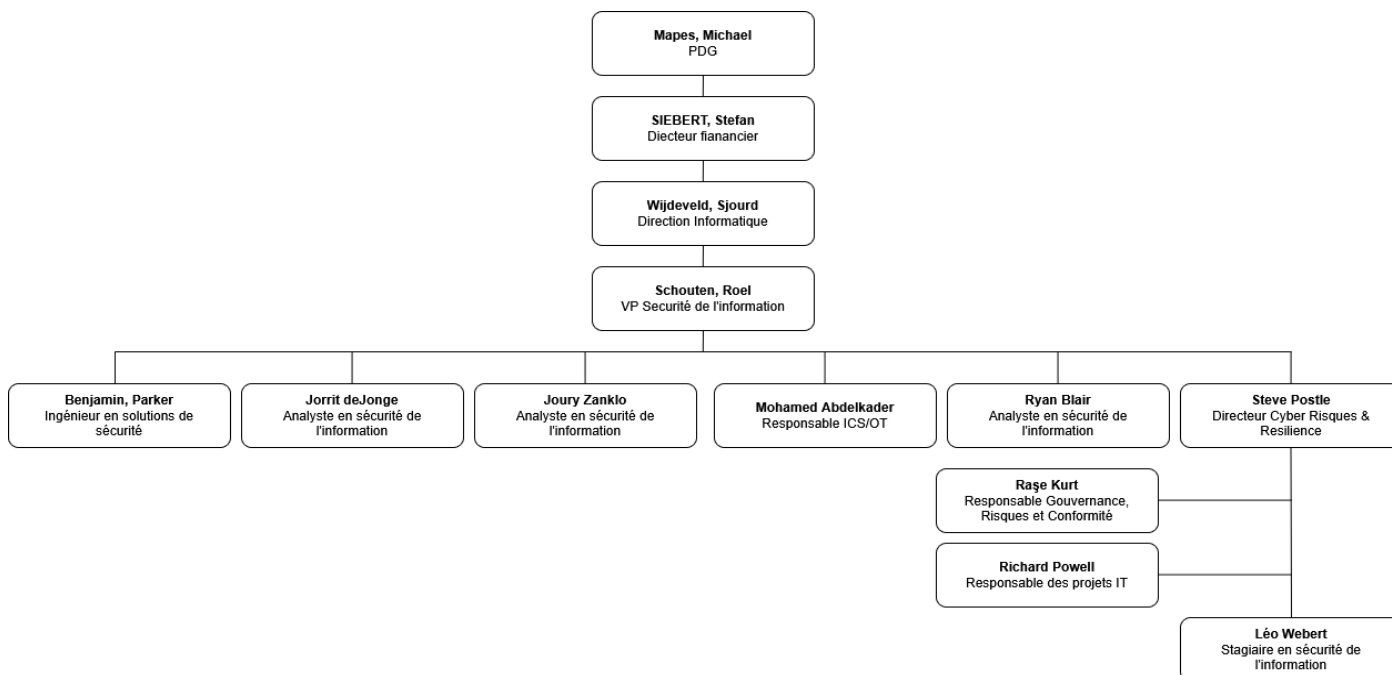
Trivium Packaging est une entreprise internationale spécialisée dans la fabrication d'emballages métalliques recyclables. Présente sur plusieurs continents, elle propose des solutions durables destinées à différents secteurs tels que l'alimentaire, la cosmétique, la santé ou encore l'industrie chimique. Le siège de l'entreprise est situé à Amsterdam, aux Pays-Bas, et elle compte plus de 60 sites répartis à travers le monde principalement en Europe.



Figure 1 - Carte des sites Européens de Trivium

L'activité de Trivium repose sur des engagements forts en matière d'innovation et de développement durable. Grâce à l'utilisation exclusive de matériaux recyclables comme l'aluminium et l'acier, l'entreprise contribue activement à la réduction de l'empreinte carbone de ses clients. Trivium met également l'accent sur la qualité, la sécurité et la conformité de ses produits, ce qui en fait un acteur reconnu dans son domaine.

Au sein de l'entreprise, j'ai intégré l'équipe cybersécurité, un service rattaché à la direction des systèmes d'information. Cette équipe a pour mission de protéger les infrastructures numériques de Trivium, d'anticiper les menaces, et de mettre en œuvre des politiques et des outils visant à garantir la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Organisation de la branche InfoSec :*Figure 2 - Diagramme de la branche Infosec de Trivium*

2. Secteur d'activité et partenaires

Trivium Packaging opère dans le secteur de l'emballage métallique, en fournissant des solutions durables à une grande diversité d'industries. Son activité s'organise autour de quatre domaines principaux : l'agroalimentaire, la santé, le cosmétique et l'industrie chimique. L'entreprise conçoit notamment des boîtes de conserve, des aérosols, des contenants pharmaceutiques, des pots en aluminium pour produits de soin, ou encore des emballages résistants pour peintures, solvants et lubrifiants.

Trivium compte parmi ses clients des marques mondialement connues telles que Nivea, Heinz, L'Oréal, Nestlé, ou encore Unilever. L'entreprise publie régulièrement des rapports ESG (Environnement, Social, Gouvernance) qui témoignent de ses engagements concrets et de ses efforts de transparence.

Press Release



Date: April 29, 2025

Subject: TRIVIUM PACKAGING 2024 SUSTAINABILITY REPORT SHOWCASES PROGRESS TOWARDS DECARBONISATION AND CIRCULAR ECONOMY GOALS

Information:

Trivium Packaging, a global supplier of infinitely recyclable metal packaging solutions, released its 2024 Sustainability Report, highlighting significant strides in environmental performance, circular innovation, and community impact. These efforts come at a critical time when only 7.2% of the world's materials are currently being cycled back into the economy, a gap that Trivium is committed to playing its part in advancing sustainable practices and redefining how materials are used and reused.

"At Trivium Packaging, sustainability is not just an operational goal. It's a foundational mindset that drives our business transformation," says Trivium CEO Michael Mapes. "In 2024, we continued to reduce our carbon footprint while empowering our teams to innovate for a circular economy. We are proud of our progress but remain focused on the work ahead as we strive toward net-zero emissions by 2050. Together with our partners and communities, we are shaping a future where sustainability is at the heart of every decision."

Key Achievements in 2024

- **Reduction in Greenhouse Gas Emissions:** Trivium achieved a 2% reduction in Scope 1 and 2 greenhouse gas (GHG) emissions in 2024, keeping the company on track to meet its Science-Based Targets initiative (SBTI)-validated goal of a 42% reduction by 2030 (from a 2020 baseline).
- **Advancing Circular Solutions:** With metal packaging solutions uniquely positioned to support circularity, Trivium continued to innovate by increasing recycled content and lightweighting products. In 2024, 47% of Trivium's total revenue came from ecodesigned products, moving them closer to their target of 50% by 2030. These efforts align with growing consumer demand for sustainable packaging and stricter regulations such as the European Packaging Waste Regulation (PPWR).
- **Recognition for Innovation:** Trivium's teams received 12 awards from industry associations across business segments in 2024, underscoring the company's technical and sustainable innovation leadership. Among these recognitions are the retention of the Platinum rating by EcoVadis for the fourth year in a row, a spot on CDP's A List for Climate, and multiple product

Figure 3 - Exemple de rapport ESG

b. Le service cybersécurité et ma mission

1. Besoins de l'entreprise

L'infrastructure de messagerie de Trivium Packaging repose principalement sur Microsoft Outlook. Ce service centralisé offre une certaine robustesse en matière de disponibilité, de filtrage et de protection de base, mais il n'élimine pas pour autant les risques liés aux communications par email.

Comme pour de nombreuses grandes entreprises, la surface d'exposition est importante : Trivium gère plusieurs dizaines de domaines de messagerie, répartis selon les pays et les sites de production. En l'absence d'une politique DMARC réellement active, il est difficile pour les serveurs de réception de savoir comment traiter les messages non conformes. Cela laisse la porte ouverte à des attaques par usurpation de domaine, où un attaquant envoie un email frauduleux en se faisant passer pour un collaborateur, un service de facturation ou une entité légitime de Trivium. Ces messages peuvent cibler aussi bien des clients, que des fournisseurs ou des employés de l'entreprise.

Ces constats ont motivé la mise en place d'une stratégie d'assainissement, de contrôle, et d'authentification renforcée de tous les domaines de messagerie utilisés par Trivium Packaging, dans l'objectif de réduire drastiquement les risques de phishing et d'usurpation.

2. Existant technique

L'entreprise présentait plusieurs besoins critiques liés à la sécurisation de ses échanges par email. La politique DMARC existante était configurée en mode « p=none », ce qui permettait seulement une surveillance passive sans intervention active sur les emails non conformes. Ce mode ne protégeait pas efficacement contre les menaces telles que l'usurpation d'identité ou les tentatives de phishing.

Les rapports DMARC, initialement envoyés dans une boîte mail interne dédiée (voir figure 4), arrivaient au format XML* brut (voir figure 5), rendant leur interprétation complexe et leur utilisation opérationnelle difficile. Aucun outil de monitoring ou d'analyse n'était alors en place pour faciliter l'exploitation de ces données.

Ainsi, les besoins prioritaires identifiés par l'entreprise étaient :

- Migrer vers une politique DMARC active (« p=reject »), permettant de rejeter automatiquement les emails malveillants ou non authentifiés.
- Mettre en place une solution efficace pour traiter et analyser rapidement les rapports DMARC.
- Disposer d'un tableau de bord ou d'une plateforme permettant une visualisation claire et accessible des résultats, afin d'améliorer la prise de décision et la réactivité face aux menaces détectées.













From	Subject	Received
<input type="checkbox"/> WEB.DE DMARC Reports	 Report Domain: triviumpackaging.com Submitter: web.de Report-ID: 218ac7...  web.de!triviumpa...	6:33
<input type="checkbox"/> GMX DMARC Report	 Report Domain: triviumpackaging.com Submitter: gmx.net Report-ID: 6bca3...  gmx.net!triviump...	6:33
<input type="checkbox"/> [REDACTED]	 Report domain: triviumpackaging.com Submitter: zoho.com Report-ID: 87ad...  zoho.com!trivium...	5:32
<input type="checkbox"/> [REDACTED]	 Report Domain: triviumpackaging.com Submitter: interia.pl Report-ID: 6005...  interia.pl!triviump...	4:04
<input type="checkbox"/> [REDACTED]	 Report domain: triviumpackaging.com Submitter: mimecast.org Report-ID: f...	4:02
<input type="checkbox"/> Soverin DMARC Reporting	 Report Domain: triviumpackaging.com Submitter: soverin.net Report-ID: triv...  soverin.net!triviu...	1:35
<input type="checkbox"/> Rspamd	 Report Domain: triviumpackaging.com Submitter: artfiles.de Report-ID: trivi...	0:50

Figure 4 - Aperçu de la boîte mail de rapport DMARC

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>triviumpackaging.com</org_name>
    <email>[redacted]</email>
    <report_id>triviumpackaging.com</report_id>
    <date_range>
      <begin>1749679200</begin>
      <end>1749765600</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>triviumpackaging.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>[redacted]</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
        <reason>
          <type>local_policy</type>
          <comment>arc=fail as[1].d=microsoft.com as[1].s=arcselector10001</comment>
        </reason>
      </policy_evaluated>
    </row>
  </record>
  <identifiers>
    <header_from>triviumpackaging.com</header_from>
  </identifiers>
  <auth_results>
    <spf>
      <domain>triviumpackaging.com</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</feedback>
```

Figure 5 - Aperçu du type fichier XML reçu lors d'un rapport DMARC

3. Objectif

Face aux risques identifiés sur l'infrastructure de messagerie, la problématique centrale consistait à concilier une authentification rigoureuse des emails et la préservation de la délivrabilité des messages légitimes. Il ne s'agissait pas seulement de mettre en place un contrôle supplémentaire, mais de sécuriser l'ensemble des échanges sans perturber les activités quotidiennes.

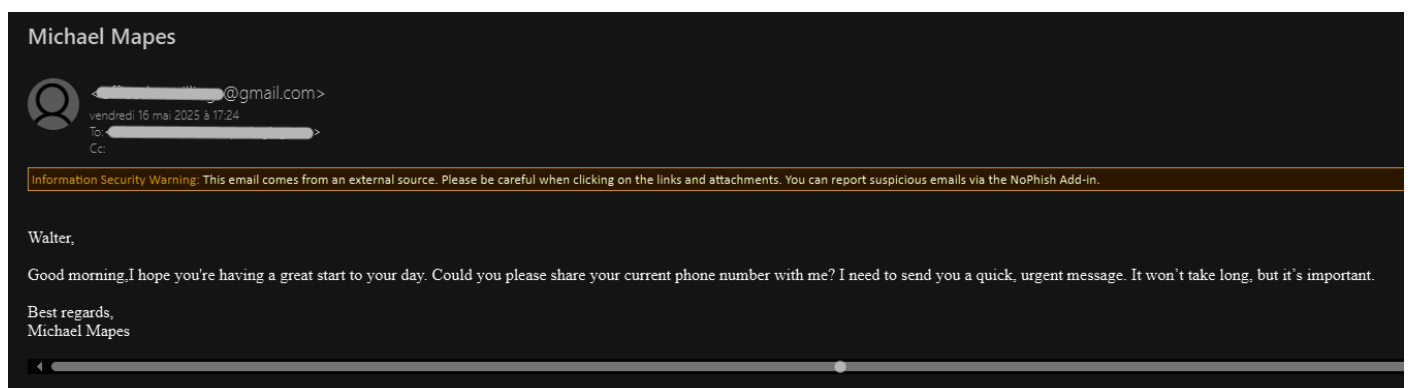


Figure 6 - Exemple d'une tentative d'hameçonnage par usurpation d'identité

L'objectif principal de ma mission a été de définir et de déployer une politique DMARC opérationnelle sur les domaines critiques de Trivium Packaging et de pouvoir un assurer un suivi facilement :

- Une cartographie précise des domaines et de leurs usages (messagerie interne, campagnes marketing, systèmes automatisés), afin d'identifier les sources émettrices et leurs particularités.
- L'exploitation des rapports DMARC pour détecter et valider les flux d'emails légitimes, en mettant en place un processus d'analyse automatisé des données reçues.
- L'élaboration et la mise en œuvre progressive d'un plan de transition, visant à augmenter graduellement la sévérité de la politique (de « p=none » vers « p=reject ») sans interrompre les flux métiers.
- Le suivi et l'analyse continue des rapports DMARC, avec des indicateurs de performance et des bilans réguliers, afin de mesurer l'efficacité de la politique déployée et d'ajuster les paramètres au besoin.

On peut résumer l'existant et l'objectif technique en deux schémas avant / après :

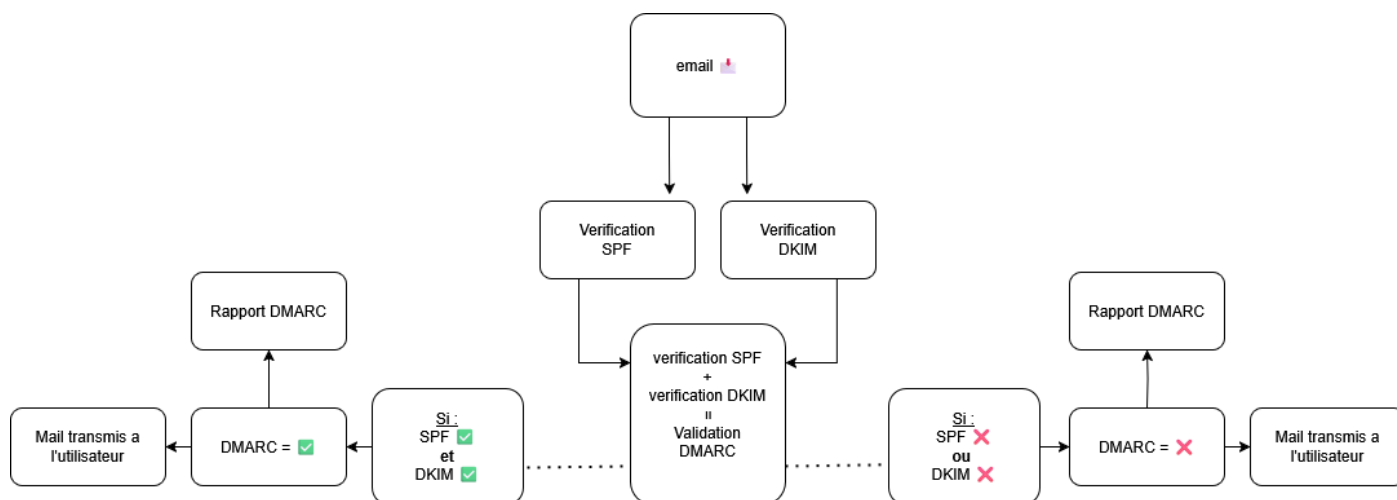


Figure 7 - Existant technique (P=none)

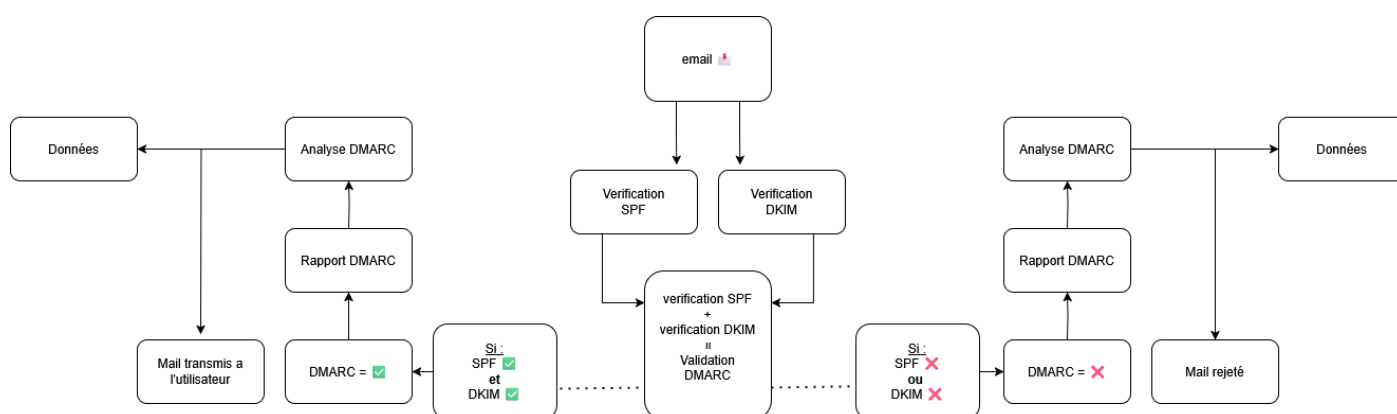


Figure 8 - Objectif final (P=reject)

Les figures ci-dessous illustrent le processus de validation DMARC avant et après la mise en place de la politique active :

Figure 1 – Processus initial (mode p=none)

Tuteur IUT : Joel TOUSSAINT

Tuteur Entreprise : Roel SCHOUTEN

Dans ce schéma, les emails transitent par les vérifications SPF et DKIM, puis la validation DMARC s'effectue sans bloquer les messages non conformes. Les rapports XML sont envoyés vers la boîte interne, sans action sur la livraison des emails.

Figure 2 – Processus cible (mode p=reject)

Après déploiement de la politique active, les messages non conformes sont automatiquement bloqués. Les flux conformes sont transmis normalement, et les rapports DMARC continuent d'être générés pour analyse. Ce fonctionnement garantit une protection renforcée tout en conservant la traçabilité des actions.

c. Organisation du projet

1. Cahier des charges

Trivium Packaging exploite plus de soixante sites et plusieurs dizaines de domaines de messagerie. Au début du stage, tous ces domaines étaient uniquement surveillés par une politique DMARC p = none ; environ un tiers des messages quotidiens n'étaient pas alignés SPF/DKIM et 60 000 rapports XML s'accumulaient dans une boîte partagée sans être. L'entreprise souhaitait donc franchir, sans dégrader la délivrabilité, les étapes menant à p = reject afin d'éliminer définitivement le spoofing.

Objectifs généraux :

- Centraliser 100 % des rapports DMARC dans une plateforme et générer une visibilité exploitable sur 30 jours de trafic.
- Porter le taux d'alignement SPF* ou DKIM* au-delà de 95 % pour tous les flux légitimes.
- Conduire la montée en enforcement : none → quarantaine → reject selon les préconisations de la solution et les seuils internes.
- Garantir zéro interruption des e-mails métiers

Livrables attendus :

- Cartographie des domaines et des expéditeurs
- Tableau de bord Valimail opérationnel avec règles de transfert automatiques.
- Scripts PowerShell* d'archivage et de nettoyage de la boîte DMARC.
- Procédure pas-à-pas pour la mise à jour des enregistrements SPF/DKIM.

Exigences fonctionnelles :

- Synthèse automatique des rapports RUA/RUF*, regroupement par source et par résultat.
- Alertes en cas de nouveau flux non autorisé ou de chute d'alignement.
- Export simple (CSV/PDF) des statistiques pour le reporting interne.

Exigences non fonctionnelles :

- Hébergement des données dans l'Espace économique européen (conformité RGPD*).
- Budget

2. Outils utilisés

Au cours de mon stage j'ai dû utiliser plusieurs outils afin de mener à bien ma mission principale :



Figure 9 - Logo de Valimail (source valimail.com)

Valimail : Cet outil en ligne a servi de tableau de bord : il a rassemblé tous les rapports techniques sur nos e-mails au même endroit. Sans lui, il aurait fallu ouvrir des milliers de fichiers à la main.



Figure 10 - Logo d'Outlook

Outlook : Outlook a été la porte d'entrée de ces rapports. J'y ai créé une règle qui transférerait automatiquement chaque nouveau fichier vers Valimail, puis j'ai utilisé la messagerie pour nettoyer l'ancienne boîte encombrée. C'est aussi l'outil avec lequel toute l'équipe lit et envoie ses e-mails quotidiens.



Figure 11- Logo de Teams

Teams : Avec Teams, nous faisons tous les jours un appel vidéo rapide pour suivre l'avancement. Les membre de l'équipe étant répartis dans plusieurs pays, ce point de contact commun a permis de se mettre d'accord rapidement et de décider quoi faire.



Figure 12 - Logo de SharePoint

SharePoint : Tous les documents : listes de tâches, captures d'écran, rapports hebdomadaires ont été déposés sur SharePoint. Cet outil a permis une collaboration entre les différents membres de l'équipe



Figure 13 - Logo de Microsoft Defender EDR

Microsoft Defender : Pendant la phase de test, les e-mails suspects étaient placés en quarantaine dans Defender. Nous pouvions y jeter un œil, libérer les messages légitimes ou supprimer les indésirables. Ainsi, aucun courriel important ne restait bloqué, et ceux malveillants n'atteignaient jamais la boîte de réception.

3. Planning prévisionnel

Un planning détaillé n'a pas été fixé : le projet a avancé en mode itératif, ajusté chaque semaine selon les résultats obtenus.

II. Réalisation technique

a. Point de départ et choix de la solution

1. Principe et objectifs de DMARC

Afin de mieux comprendre le fonctionnement du protocole DMARC, il faut d'abord comprendre de quoi il est composé, c'est-à-dire de la somme de deux protocoles plus petits (SPF et DKIM). C'est pourquoi, avant toute mise en œuvre, mon tuteur m'a demandé de réaliser une courte étude ; l'objectif était de maîtriser ces briques techniques pour pouvoir ensuite mieux comprendre le

Tuteur IUT : Joel TOUSSAINT

Tuteur Entreprise : Roel SCHOUTEN

fonctionnement global. Cependant, pour savoir comment tout s'agence, il faut d'abord définir une notion fondamentale : le DNS.

Le Domain Name System est « l'annuaire téléphonique » d'Internet : il fait le lien entre un nom de domaine lisible (ex. trivium.com) et des informations techniques associées (généralement l'adresse IP*).

Ces informations sont stockées sous forme d'enregistrements ; dans notre cas, nous utilisons surtout le type TXT, un champ texte simple, universel et interprété de la même façon par tous les serveurs ; il permet de stocker des chaînes de texte libres, dans lesquelles nous publions les règles SPF, DKIM et DMARC. Lorsqu'un serveur de messagerie reçoit un courriel, il consulte automatiquement ces enregistrements pour savoir comment vérifier l'authenticité du message et quelle action appliquer en cas d'échec.

Cette même logique « d'annuaire » est exploitée par le protocole SPF (Sender Policy Framework). Concrètement, l'administrateur publie dans le DNS un enregistrement TXT qui liste les serveurs autorisés à envoyer des e-mails pour le domaine. On déclare dans le DNS un enregistrement TXT du type :

```
v=spf1 ip4:192.168.1.2 include:spf.protection.outlook.com -all
```

Quand un message arrive, le serveur destinataire compare l'adresse IP de l'expéditeur à celle de l'enregistrement (192.168.1.2), s'elle n'y figure pas, le mail est catalogué comme suspect. SPF agit donc comme un filtre « qui m'envoie un email », il vérifie l'identité technique du serveur expéditeur, mais ne dit rien sur l'intégrité du contenu ni sur la cohérence du nom affiché dans le champ « From ». C'est la première brique indispensable avant d'enchaîner sur DKIM.

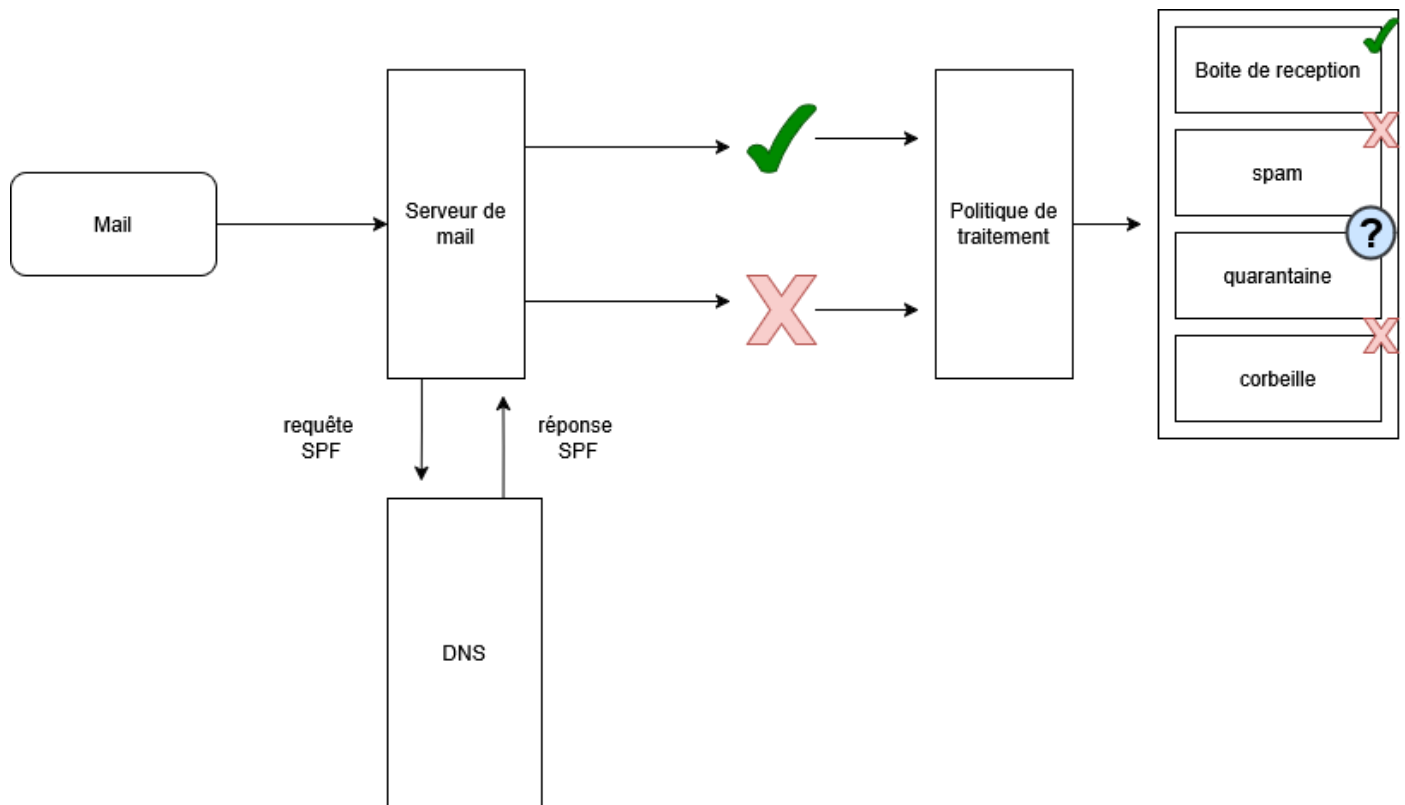


Figure 14 - schéma du fonctionnement du protocole SPF

À cette vérification du serveur émetteur s'ajoute la couche DKIM (Domain Keys Identified Mail), qui se concentre cette fois sur le contenu du message. Avant l'envoi, le serveur d'origine calcule une empreinte du courriel (corps + en-têtes essentiels) et la chiffre à l'aide d'une clé privée. Le résultat, la signature DKIM, est ajouté dans un en-tête dédié du mail.

Lorsqu'un destinataire reçoit ce message, il interroge de nouveau le DNS : un autre enregistrement TXT (commençant par v=DKIM1) contient la clé publique associée. En la combinant avec la signature, le serveur peut confirmer deux points :

1. Le message n'a pas été altéré pendant le transport ;
2. Il provient bien du domaine qui possède la clé privée correspondante.

Autrement dit, DKIM apporte une garantie d'intégrité et d'authenticité du contenu, là où SPF ne valide que la machine émettrice. Toutefois, DKIM ne suffit pas à lui seul : un expéditeur malveillant pourrait signer avec son propre domaine tout en affichant une adresse « From » trompeuse. C'est précisément pour résoudre ce problème et décider quoi faire des échecs SPF/DKIM qu'intervient la couche finale, DMARC.

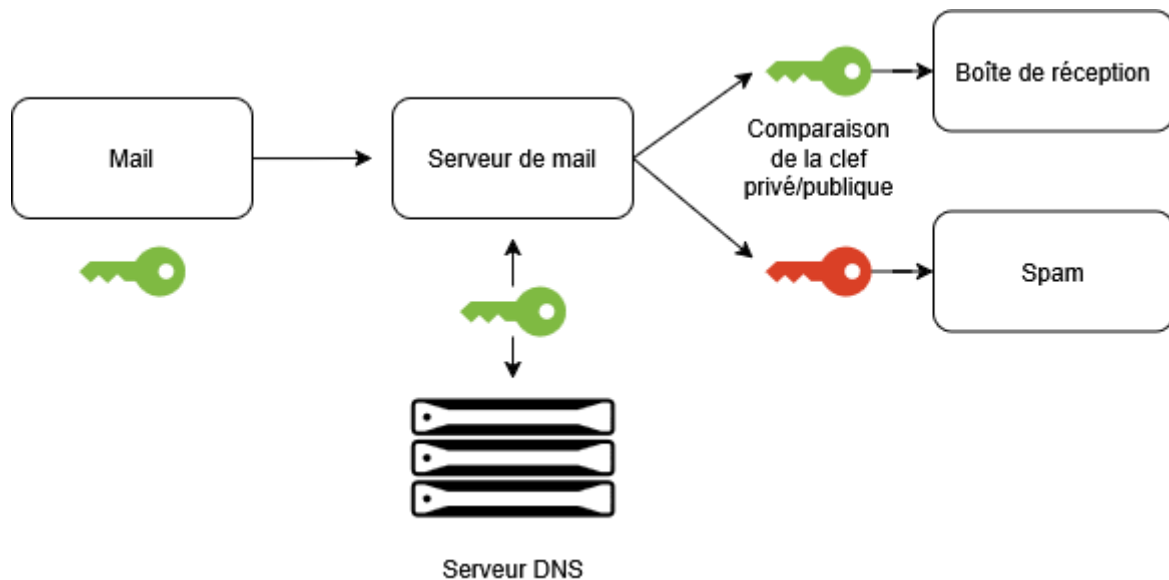


Figure 15 - schéma du fonctionnement du protocole DKIM

À partir des résultats SPF et DKIM, le protocole DMARC (Domain-based Message Authentication, Reporting & Conformance) vient faire la synthèse : il vérifie l'alignement entre le domaine réellement authentifié (par SPF ou par DKIM) et celui affiché dans l'adresse « From : ».

Si l'alignement échoue, DMARC applique la politique publiée dans un nouvel enregistrement TXT :

- P=none : on observe ; rien n'est bloqué, mais les incidents sont consignés.
- P=quarantine : les messages défectueux sont placés en quarantaine.
- P=reject : ils sont purement refusés avant même d'atteindre la boîte du destinataire.

Chaque serveur qui reçoit un e-mail renvoie ensuite un rapport agrégé (fichier XML) vers l'adresse indiquée dans le champ « rua= ». Ce sont précisément ces rapports qu'on souhaite analyser pour en tirer parti

On peut réutiliser le schéma de l'existant technique pour l'illustrer :

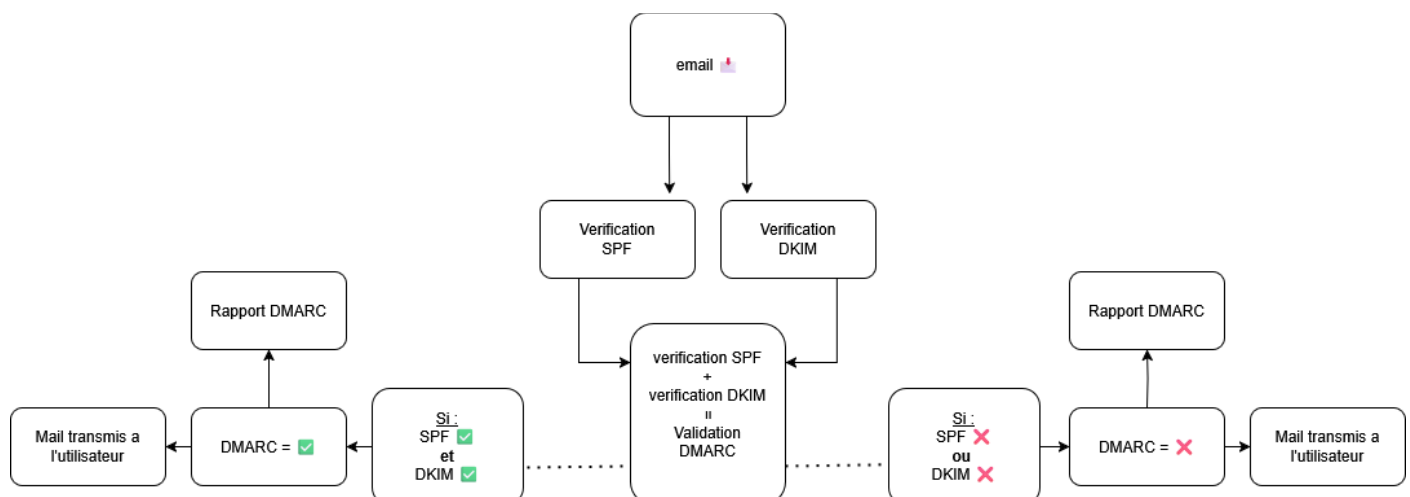


Figure 16 - schéma du fonctionnement du protocole DMARC

2. Rôle de la quarantaine : chaîne de traitement et impact sur les flux de messagerie

Lorsqu'un message échoue aux contrôles DMARC mais que la politique n'est pas encore en « reject », il peut être placé dans une zone tampon : la quarantaine. Chez Trivium, cette quarantaine est gérée par Outlook, la messagerie par défaut de l'entreprise (et non par DMARC) : ce sont donc les filtres internes de Microsoft qui interceptent les emails jugés suspects, souvent à cause d'une signature DKIM manquante, d'un SPF mal configuré ou car le mail reprend des éléments déjà définis comme suspect (liens, demande d'action, de connexion, etc.).

Lorsqu'un message destiné à Trivium arrive sur l'infrastructure Microsoft 365, il franchit d'abord les passerelles de sécurité internes d'Outlook. Là, un moteur d'analyse calcule un score de risque ; si celui-ci dépasse le seuil défini par Microsoft, l'email est immédiatement redirigé vers la file de quarantaine plutôt que livré dans la boîte de son destinataire. Chaque jour, je me connecte donc au portail Microsoft Defender* pour examiner cette file. J'ouvre les en-têtes et le corps du message, je vérifie les domaines, les liens ou les pièces jointes suspects, et, si nécessaire, je contacte l'utilisateur pour confirmer qu'il attendait bien ce mail. Quand toutes les vérifications sont faites, deux issues sont possibles : je relâche le message s'il s'avère légitime (faux positif) ou je le supprime définitivement s'il s'agit d'une tentative de phishing ou de spam malveillant.

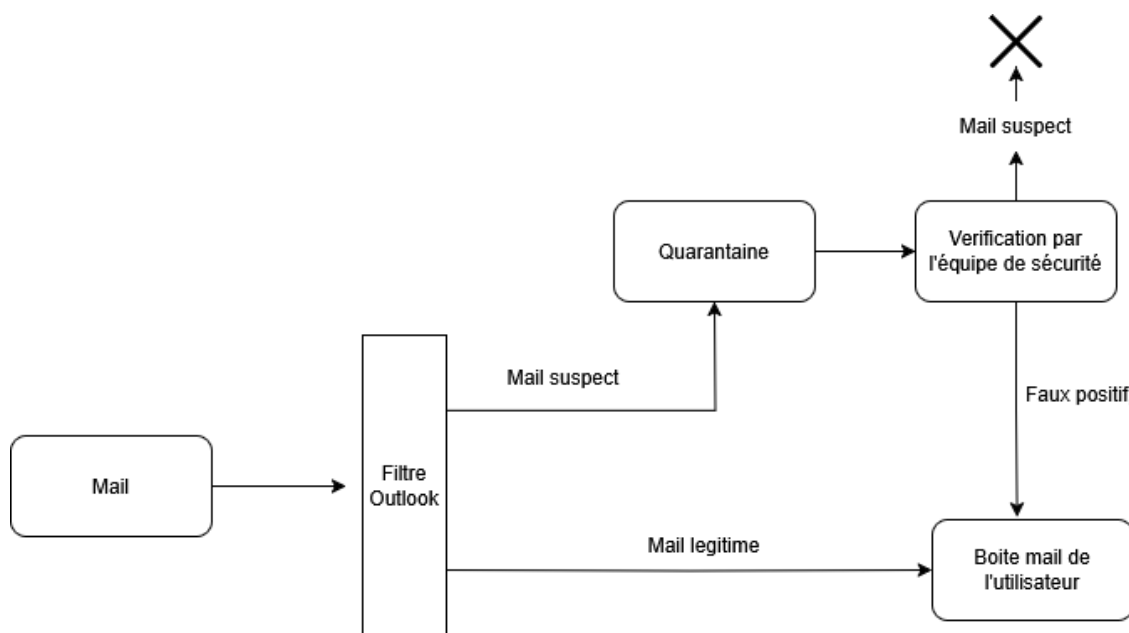


Figure 17 - Trajet d'un email sans politique active

Explication du schéma :

Le schéma illustre le parcours d'un email tant que la politique DMARC est en *p=none* :

1. Arrivée du mail : tout message entrant passe d'abord par le filtre natif d'Outlook.
2. Décision automatique :
 - S'il est jugé légitime, il est remis directement dans la boîte de l'utilisateur
 - S'il semble douteux, Outlook le place en quarantaine.
3. Contrôle humain : l'équipe sécurité examine ensuite chaque élément quarantaine ;
 - Si c'est un faux positif, le message est relâché vers l'utilisateur.

- *S'il s'agit bien d'une tentative de phishing ou de spam, il est supprimé.*

La vérification manuelle présente toutefois de sérieuses limites. D'abord, l'exercice est fastidieux : certains jours, la file peut compter plusieurs dizaines de messages et chaque courriel doit être ouvert individuellement, ses en-têtes analysés, ses liens testés, voire son contenu confirmé auprès de l'utilisateur qui l'attendait. À cette charge s'ajoute le risque d'erreur humaine ; la répétition et la fatigue peuvent conduire à relâcher par inadvertance un e-mail malveillant, ou, à l'inverse, à supprimer un message parfaitement légitime. Enfin, le temps de réaction dépend de la disponibilité de l'équipe de sécurité : tant qu'aucun membre de l'équipe n'a validé le message, celui-ci reste bloqué en quarantaine, retardant parfois des échanges professionnels urgents.

3. Comparatif des outils (DMARCian, OnDMARC, EasyDMARC, Valimail)

Au départ, l'équipe pensait s'appuyer sur DMARCian, solution déjà connue en interne. J'ai donc commencé par tester la plateforme : interface claire, bonnes capacités de visualisation des flux et tarifs modérés. Toutefois, après des tests plus poussés nous avons découvert une contrainte juridique : pour des raisons de conformité, le service est inaccessible depuis les Pays-Bas, où se trouve une partie de l'infrastructure de Trivium. Cette impossibilité d'accès a remis en question le choix initial

J'ai alors cherché des alternatives et dressé un tableau comparatif entre différents candidats en évaluant cinq critères :

4. Accessibilité géographique, l'outil doit être accessible partout dans le monde
5. Résidence des données et conformité RGPD*, les données doivent être stockées en Europe et régies par des lois européennes sur la protection des données
6. Richesse de l'analyse : tableaux de bord, corrélation SPF/DKIM, alertes automatisées
7. Transition vers la politique de rejet
8. Coût et modèle de licence : nombre de domaines, volume de rapports, support...

OnDMARC séduisait d'abord par son interface très épurée : les tableaux de bord mettent immédiatement en évidence les sources d'envoi et les pourcentages de conformité. Son module « Smart Recommendations » propose même, pour chaque sous-domaine, les modifications SPF/DKIM à appliquer. En revanche, le modèle tarifaire repose sur un forfait de base auquel s'ajoute un coût par domaine supplémentaire ; à partir du troisième domaine secondaire, la facture grimpe rapidement, rendant la solution moins viable pour Trivium qui gère un portefeuille d'alias industriels assez large.

EasyDMARC affichait de son côté des prix nettement plus doux et une courbe d'apprentissage minimale. Cependant, les tests ont révélé une absence de filtrage par sous-domaine obligeant à exporter les rapports pour isoler manuellement les flux. En pratique, cela signifiait que l'équipe

aurait dû conserver des scripts* maison pour surveiller les défaillances critiques, ce qui allait à l'encontre de l'objectif « plateforme clé en main et automatique ».

Valimail, enfin, cumulait les points positifs. Les datacenters européens et la conformité RGPD couvraient la contrainte de localisation. Le service propose un « Hosted SPF* » qui aplatit automatiquement les enregistrements SPF trop longs. Ce système permet d'agir comme un condensateur de votre l'enregistrement SPF : il remplace la longue chaîne d' « include » successifs par une seule référence vers un sous-domaine géré par Valimail, lequel contient déjà la version aplatie (toutes les IP, sans autres recherches DNS)

On passe donc d'un enregistrement SPF comme celui-ci :

```
v=spf1 include:spf.protection.outlook.com include:_spf.salesforce.com  
include:mail.zendesk.com include:spf.sendgrid.net include:_spf.google.com  
include:mktomail.com include:servers.mcsv.net include:spf.mailjet.com  
include:_spf.mandrillapp.com -all
```

A un simple enregistrement qui pointe vers cette liste :

```
v=spf1 include:trivium._spf.vali.email -all
```

Cela permet plusieurs choses :

9. On masque les serveurs qui vérifient SPF
10. Si l'on ajoute ou retire un prestataire d'e-mailing, on le fait dans le portail Valimail ; le DNS public de l'entreprise reste inchangé et court
11. On ne dépasse pas la limite des 10 résolutions imposée par la RFC 7208* car Valimail a déjà effectué les résolutions DNS pour nous

De plus, le mode "Enforce" guide pas à pas la montée de p=none à p=reject. Côté budget, le prix par domaine est comparable à OnDMARC, mais inclut plusieurs sous-domaines et un support réactif, ce qui rend l'offre globalement plus compétitive. Résultat : Valimail coche toutes les cases fonctionnelles tout en simplifiant le déploiement, raison pour laquelle il a été retenu.

b. Implémentation de Valimail

1. Configuration de l'outil

La première étape a consisté à reprendre le contrôle de la boîte mail dédiée aux rapports DMARC. Après avoir fait réactiver les droits d'accès, j'ai découvert un stock de plus de 62 000 messages accumulés depuis plusieurs années. Cette accumulation rendait toute exploitation impossible, j'ai donc d'abord tenté de créer, dans Outlook, une règle de suppression automatique pour tous les rapports antérieurs à 2024. Cependant le volume de messages était si important que la règle se bloquait systématiquement. J'ai donc sollicité l'équipe IT responsable du compte principale de la boîte mail, afin qu'ils exécutent un script qui, via le protocole IMAP*, va purger en bloc les emails. Une fois ce premier volume éliminé, j'ai archivé les rapports couvrant la période

2024-2025 pour conserver une base de référence, puis vidé les derniers éléments superflus afin de ramener la boîte à un état réellement « neuf »

Une fois la boîte assainie, j'ai créé une règle de transfert : chaque nouveau message contenant un fichier XML de rapport est automatiquement redirigé vers l'adresse de collecte fournie par Valimail. Nous avons volontairement évité d'ajouter le paramètre rua= dans l'enregistrement DMARC car modifier le DNS public de Trivium aurait déclenché un processus de validation long et exposé la zone à un risque d'erreur. La redirection via une règle s'est donc imposée comme la solution la plus simple et la plus rapide.

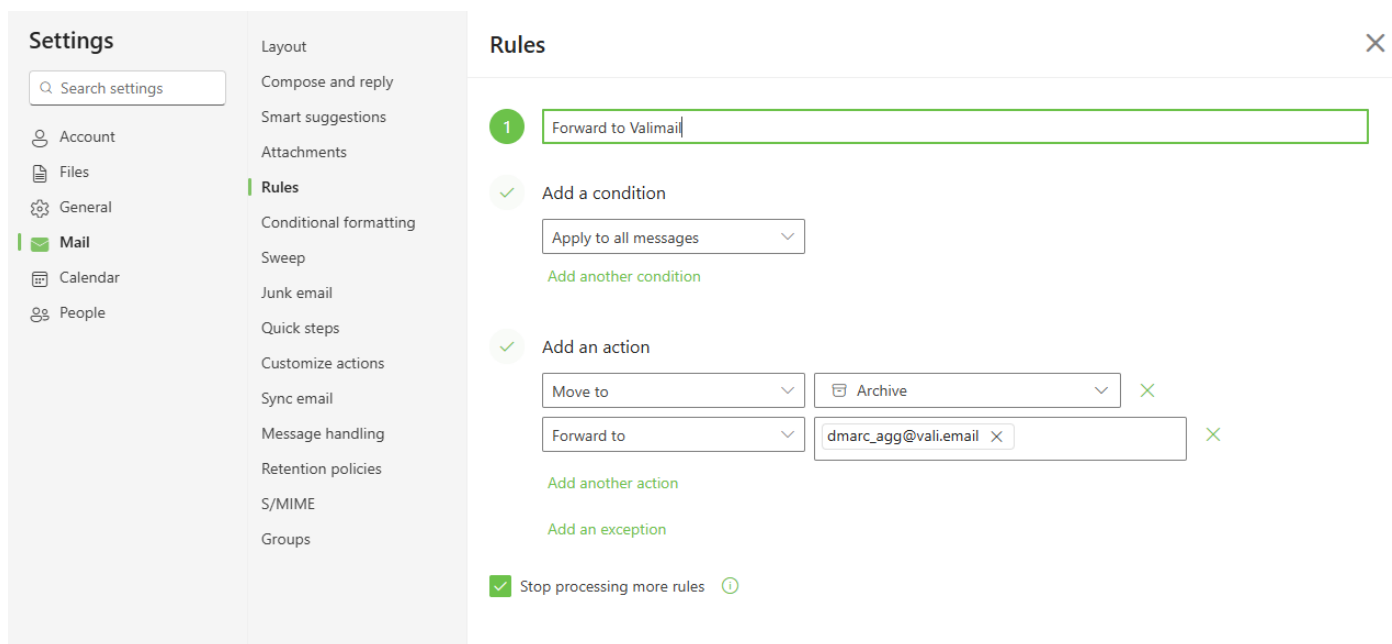


Figure 18 - Règles de redirection des rapports DMARC

Explication de l'image : Cette capture d'écran provient de la boîte mail de rapport DMARC de Trivium packaging, on y remarque clairement où les rapports seront envoyés et qu'ils seront ensuite archivés

Dès la mise en place du transfert, les premiers rapports sont apparus dans le tableau de bord Valimail, confirmant que la redirection fonctionnait et que les données pouvaient désormais être exploitées pour la montée progressive vers p=reject.

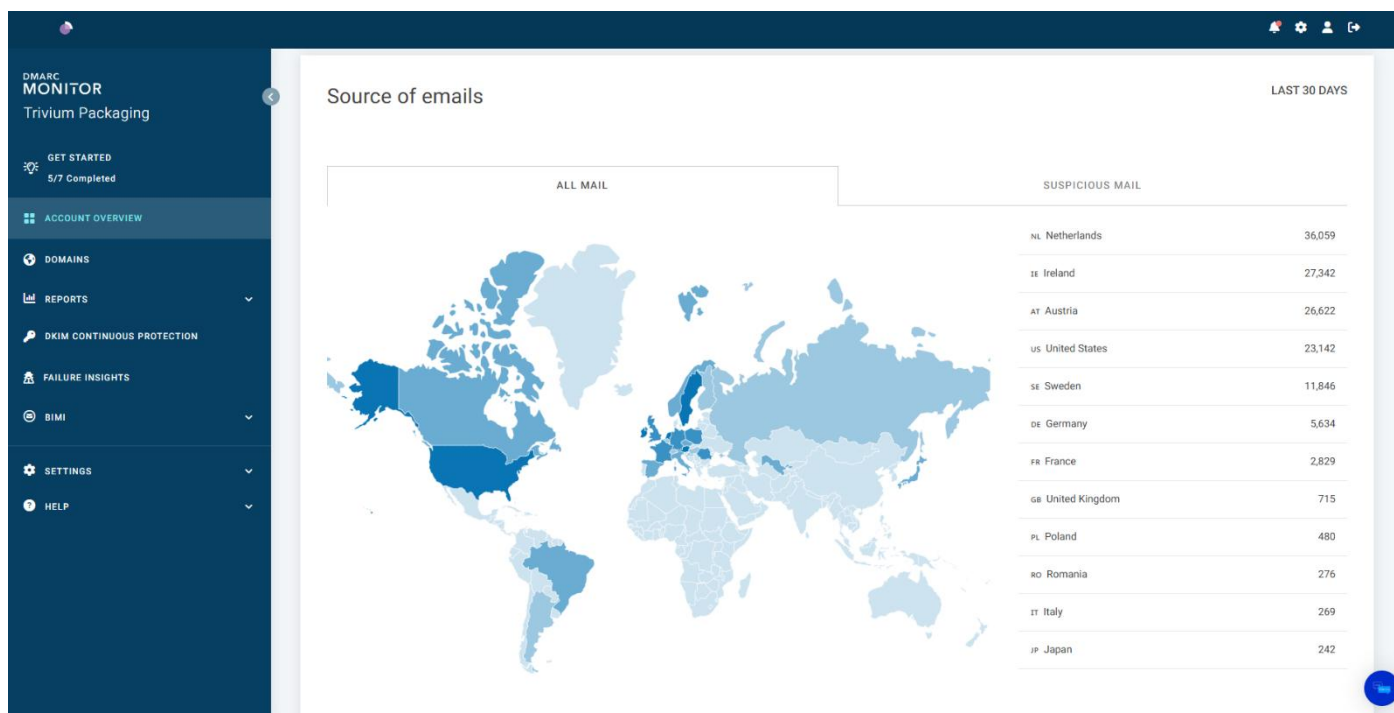


Figure 19 - Aperçu du tableau de bord de Valimail

2. Passage au plan « enforce » : analyse des rapports et montée vers p=reject

L'agrégation des 135 000 rapports DMARC que Valimail a digérés sur les 30 derniers jours dresse un tableau très net de l'état actuel. En moyenne, 33% des emails échouent encore sur le DMARC, et la cause est presque toujours un défaut de signature, le taux d'échec DKIM culmine à 92 %, tandis que l'alignement SPF, bien qu'encore imparfait, réussit déjà dans six cas sur dix. Autrement dit, la plupart des messages sortent bien d'une adresse IP autorisée, mais débarquent chez le destinataire sans signature cryptographique correcte.

En remontant la chaîne, Valimail révèle que le gros du trafic authentifié provient de nos instances Microsoft 365 et SAP SuccessFactors ; à l'inverse, cinq services tiers : Cornerstone OnDemand, Esker, Nmbrs, Campaign Master et Epsilon ratent l'authentification 100 % du temps. Une autre zone d'ombre subsiste : près de 30 % du volume total provient d'expéditeurs que la plateforme ne parvient pas à identifier.

Géographiquement, les points chauds correspondent exactement aux datacenters que nous utilisons : Pays-Bas, Irlande, Autriche et États-Unis totalisent les deux tiers des messages. Ce constat confirme que la plupart des échecs sont dus à une configuration incomplète de la part des partenaires plutôt qu'à des campagnes massives de phishing externes.

Du point de vue « délivrabilité », la plateforme indique qu'99,95 % des emails continuent d'être acheminés « sans enforcement » ; un seul est parti en quarantaine et aucun n'a été rejeté. Cela

confirme que le domaine est encore en politique $p=\text{none}$, ce qui laisse passer le trafic légitime, mais impose aux analystes un tri manuel de tous les mails suspects.

En dix jours de corrections ciblées, le taux d'alignement quotidien est déjà passé d'environ 65 % à plus de 90 % : la trajectoire vers $p=\text{reject}$ est donc réaliste à très court terme, avec à la clé une charge de tri humain quasi nulle et une protection phishing renforcée pour tous les utilisateurs.

III. Bilan

a. Résultats techniques obtenus

Au début du stage, la messagerie de Trivium affichait une politique DMARC $p = \text{none}$ et des rapports XML jamais consultés ; l'objectif était de centraliser ces données, de corriger les configurations SPF/DKIM et de préparer le passage à $p = \text{reject}$.

Aujourd'hui, le premier objectif est pleinement atteint : la boîte DMARC a été remise à zéro, une règle de transfert relaie désormais 100 % des nouveaux rapports vers Valimail et plus de 135 000 messages ont déjà été traités par la plateforme, offrant une visibilité complète sur trente jours de trafic.

La deuxième cible, la cartographie des émetteurs, est réalisée à près de 90 %. L'analyse Valimail montre que le taux d'alignement quotidien est passé d'environ 65 % à plus de 90 % grâce à l'activation de signatures DKIM et à l'ajout d'incluses SPF pour dix services internes. Les flux légitimes majeurs (Microsoft 365, SAP SuccessFactors, Salesforce, SendGrid, etc.) passent désormais DMARC à plus de 90 %, tandis que cinq prestataires, pour le moment non conforme, ont été identifiés et sont en cours de mise en conformité.

Le troisième objectif le changement de politique n'est pas encore finalisé mais est prévue sur le plan technique : Valimail recommande le basculement en « $p = \text{quarantine}$ », condition franchie grâce à un alignement ≥ 95 % sur plusieurs jours consécutifs. En résumé : la collecte et l'analyse sont entièrement opérationnelles, la conformité a fait un bond de 25 points et toutes les conditions sont réunies pour appliquer, à très court terme, une politique « $p = \text{reject}$ » sans risque pour la délivrabilité des e-mails légitimes.

b. Difficultés rencontrées

La première difficulté et la plus chronophage a été le nettoyage de la boîte DMARC. Entre l'inventaire, la tentative infructueuse de règle Outlook, la coordination avec l'équipe IT et l'exécution du script IMAP, l'opération a mobilisé près d'une journée complète avant d'obtenir une boîte enfin exploitable.

Deuxième obstacle a été mon absence totale d'expérience sur DMARC en début de stage. J'ai donc dû assimiler, en quelques jours, le fonctionnement de SPF, DKIM et DMARC, puis comprendre la logique des rapports XML et de l'alignement des domaines avant même de pouvoir manipuler Valimail ou DMARCian.

c. Perspectives d'évolution

Pour l'instant, le domaine principal reste en « p = none » : nous observons, mais nous ne bloquons rien. Le but est de passer à un rejet total sans compromettre la délivrabilité légitime des emails.

Dans un premier temps, il s'agit de porter l'alignement quotidien au-delà de 95 %, seuil à partir duquel Valimail recommande le passage au plan « enforcement ». Concrètement : activer DKIM pour chaque partenaire, corriger les enregistrements SPF/DKIM des cinq services encore « Globalement en échec » et qualifier les expéditeurs inconnus (liste blanche pour les flux internes et blocage pour les autres). Une fois ces configurations terminées, les faux positifs devraient devenir moins courant et le tableau de bord rester vert plus longtemps.

La deuxième étape consistera à basculer la politique en « p = quarantaine ». Pendant cette phase pilote, l'équipe sécurité surveillera la file de quarantaine : si moins de 1 % des messages retenus sont légitimes, nous pourrions considérer la cartographie comme fiable. Valimail déclenchera automatiquement une notification dès qu'un nouvel expéditeur échoue DMARC, afin d'éviter que la quarantaine ne soit saturée.

Lorsque la quarantaine sera stable, la fenêtre de changement suivante permettra de passer en « p = reject ». Tout mail suspect d'un expéditeur non conforme aux recommandations DMARC/SPF/DKIM devra être bloqué sur toute la chaîne, prouvant que la politique est effective.

Enfin, la montée en mode « reject » ne s'arrêtera pas à la bascule du paramètre « p = reject ». Des améliorations continues resteront nécessaires c'est pour cela que l'équipe InfoSec continuera :

- À suivre quotidiennement les tableaux de bord Valimail pour repérer tout nouvel émetteur non aligné ;
- À travailler avec les prestataires encore « Mostly Failing (globalement en echec) » afin de finaliser leurs enregistrements SPF/DKIM ;

- À vérifier régulièrement les statistiques d'alignement et les volumes de quarantaine afin de s'assurer que la politique « reject » n'écarte pas de courriels légitimes.

Ces actions, déjà planifiées et suivies chaque semaine, garantiront la pérennité de la conformité DMARC et la protection continue contre l'usurpation d'identité.

Bilan Humain

Sur le plan humain, ce stage m'a fait progresser de façon très concrète. Le premier bénéfice est linguistique : les réunions Teams quotidiennes se déroulaient entièrement en anglais avec des interlocuteurs de plusieurs nationalités. Cette pratique intensive m'a permis de gagner en aisance à l'oral, d'enrichir mon vocabulaire professionnel et de prendre confiance dans un environnement en anglais.

La mission m'a également appris à collaborer avec des équipes : j'ai dû planifier les tâches, rendre des rapports et faire circuler l'information de manière claire et concise. Cette collaboration m'a sensibilisé à la gestion des priorités et à l'importance d'une communication pour maintenir la participation dans une équipe.

Enfin, la variété des activités analyse de rapports, automatisation par script, présentation de résultats, suivi de prestataires a renforcé ma polyvalence. J'ai découvert comment la sécurité des e-mails s'intègre aux processus métiers d'une entreprise internationale et j'ai acquis une expérience précieuse en gestion de projet technique, confirmant mon ambition de me spécialiser dans la sécurité informatique.

Conclusion

Au terme de ces deux mois au sein de l'équipe InfoSec de Trivium Packaging, l'étude et la mise en place d'une politique DMARC se sont inscrites dans une démarche globale de réduction des risques liés au phishing et à l'usurpation d'identité. Après avoir analysé le contexte international de l'entreprise, cartographié son infrastructure de messagerie et précisé les besoins (faire évoluer la politique « p = none » vers « p = reject » tout en préservant la délivrabilité) nous avons défini un cahier des charges clair :

- Centraliser les rapports DMARC
- Identifier les flux légitimes
- Planifier une montée en politique de reject progressive.

La réalisation technique a reposé sur trois leviers:

- Le nettoyage complet de la boîte de rapports XML
- L'implémentation de la plateforme Valimail

- L'harmonisation des enregistrements SPF/DKIM pour chaque émetteur.

Les premiers résultats témoignent d'une progression rapide : plus de 135 000 rapports traités, un taux d'alignement quotidien passé de 65 % à plus de 90 % et une visibilité fine sur les services encore non conformes. Ces chiffres confirment la pertinence des choix techniques et valident la faisabilité du passage en « p = quarantaine » à très court terme.

Enfin, le bilan met en évidence un double apport. Sur le plan opérationnel, Trivium dispose désormais d'une base solide pour atteindre l'objectif final : bloquer systématiquement les emails non authentifiés sans impacter les échanges légitimes. Sur le plan personnel, ce projet m'a permis de consolider mes compétences en sécurité des emails, en gestion de projet et en travail d'équipe. Les prochaines étapes, finaliser la conformité des derniers prestataires, basculer successivement en « quarantaine » puis en « reject », et maintenir une veille continue via Valimail – garantiront la protection durable des utilisateurs face aux menaces d'usurpation.

English Summary

During the eight weeks I spent as a security intern with Trivium Packaging's global Cyber-Security team, my mission was to transform an under-used e-mail standard into a frontline defence. Trivium's metal-container business relies on professional, round-the-clock exchanges between more than sixty production sites, but its principal domain still ran Domain-based Message Authentication, Reporting and Conformance (DMARC) in passive "p = none" mode. A dormant mailbox contained tens of thousands of unread XML aggregates, and only about two-thirds of daily traffic satisfied SPF or DKIM alignment. In practical terms, any threat actor could send a spoofed message that looked convincingly like a purchase order or shipping update, with little chance of being blocked or even noticed.

My first objective was therefore to reduce the risk. I archived the 60 000 historical reports, created an automatic forwarder, and funneled every new DMARC message into Valimail Enforce, the SaaS platform we selected after a short benchmark for its EU data residency and its ability to flatten SPF records. With the dashboard finally populated, it became clear that roughly 135 000 messages touched the domain in a single month, giving us a reliable baseline. By mapping those flows to business units and vendors, I drew up a remediation plan that targeted misconfigured senders first, then unknown ones.

Alignment leapt from about 65 percent to more than 90 percent, and the dashboard pinpointed five external services that still failed every check. Because the policy remained in monitoring mode, legitimate messages kept flowing, yet managers could at last see hard numbers: which suppliers continued to break authentication, how many forged messages were attempting to slip through, and how close the company was to a defensible threshold. With that visibility, the team drafted a phased transition, first "p = quarantine" for a short observation window, then "p = reject" once any lingering false positives had been ironed out, to shut the door on spoofing without causing trouble to day-to-day commerce.

Beyond the technical metrics, the project reshaped my own skills. I was able to analyze unfamiliar XML schemas and present risk-reduction figures to my tutor. The work forced me to juggle scripts, dashboards and conference calls in equal measure, and taught me that security control only succeeds when it respects operational reality.

Bibliographie

Recherches internet :

<https://www.triviumpackaging.com/>

<https://www.valimail.com/>

<https://easydmarc.com/>

<https://redsift.com/pulse-platform/ondmarc>

<https://dmarcian.com/fr/>

Documents :

RFC 7208 – “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email”, IETF, 2014.

RFC 6376 – “DomainKeys Identified Mail (DKIM) Signatures”, IETF, 2011.

RFC 7489 – “Domain-based Message Authentication, Reporting, and Conformance (DMARC)”, IETF, 2015.

DMARCIAN alternatives.xlsx : [google drive](#)

Strengthening Trivium’s Email Security with DMARC.docx : [google drive](#)

Weekly report #1 : [google drive](#)

Weekly report #2 : [google drive](#)

Weekly report #3 : [google drive](#)

Weekly report #4 : [google drive](#)

Glossaire

Adresse IP : Identifiant numérique unique attribué à chaque appareil connecté à un réseau, utilisé pour l'acheminement des paquets Internet

DKIM (Domain Keys Identified Mail) : Signature cryptographique ajoutée au courriel. Le serveur destinataire vérifie ainsi que le message n'a pas été altéré et qu'il provient bien du domaine annoncé.

DMARC (Domain-based Message Authentication, Reporting & Conformance) : Cadre qui combine SPF et DKIM, il définit la politique à appliquer aux messages défaillants (observer, mettre en quarantaine ou rejeter) et envoie des rapports XML de synthèse

DNS (Domain Name System) : il relie un nom de domaine lisible à des données techniques (adresses IP, enregistrements TXT, etc.)

Hosted SPF : Service géré chez Valimail qui aplatit un enregistrement SPF trop long en le remplaçant par une simple référence vers un sous-domaine, évitant la limite des 10 recherches DNS

IMAP (Internet Message Access Protocol) : Protocole qui permet à un client de lire et gérer des e-mails directement sur le serveur, utilisé ici pour purger la boîte de rapports

Phishing : Technique frauduleuse qui trompe l'utilisateur (e-mail ou site factice) pour voler des données sensibles

PowerShell : Shell et langage d'automatisation Windows, utilisé ici pour nettoyer la boîte DMARC

RFC 7208 : Spécification officielle du protocole SPF publiée par l'IETF, elle fixe notamment la limite des 10 requêtes DNS

RGPD : Règlement européen encadrant la collecte et le traitement des données personnelles (General Data Protection Regulation)

RUA / RUF : Rapports DMARC : RUA pour les agrégats anonymisés, RUF pour les échecs détaillés (forensic) Rapport de stage.

Scripts : Petits programmes (ici PowerShell) destinés à automatiser des tâches répétitives, comme l'archivage d'e-mails

SharePoint : Plateforme de partage de documents de Microsoft 365, héberge les exports, listes de tâches et comptes-rendus

SPF (Sender Policy Framework) : Enregistrement TXT indiquant quels serveurs sont autorisés à envoyer des e-mails pour le domaine, il bloque l'usurpation d'adresse IP

XML (rapport DMARC) : Format de fichier structuré dans lequel les serveurs envoient leurs rapports DMARC agrégés