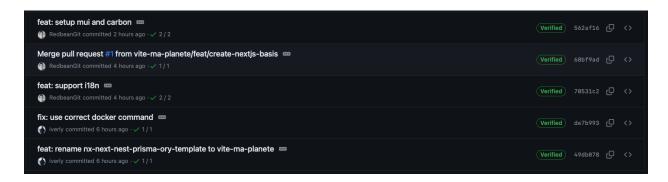
Reporting: Défi CS Group 2023 - La cyber c'est super

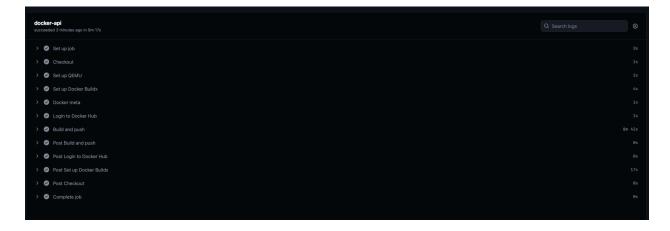


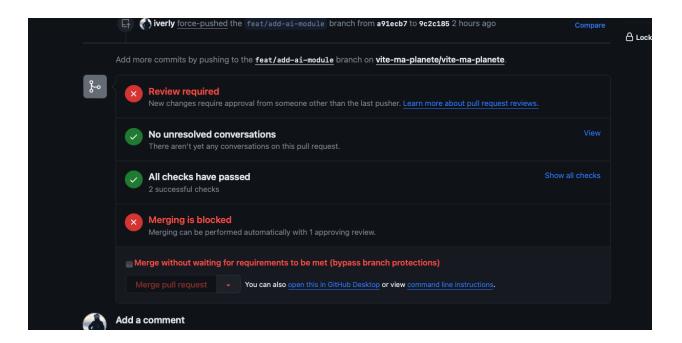


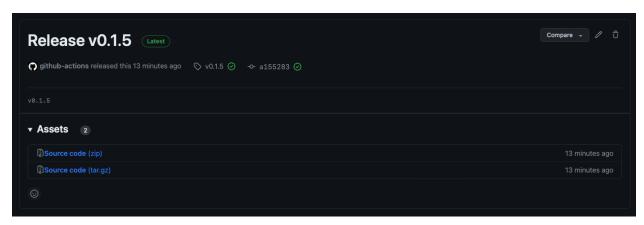
Software Supply Chain

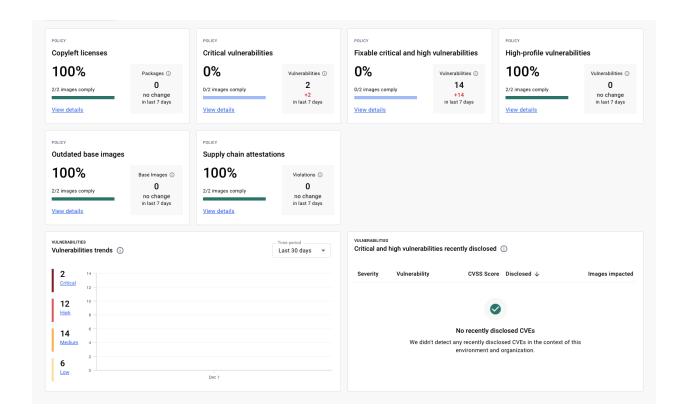
La chaîne d'approvisionnement logicielle est sécurisée de GitHub à Docker Image, incluant la signature des commits pour garantir l'authenticité, la révision des Pull Requests pour maintenir la qualité du code, l'intégration continue pour le linting et la détection de fuites de secrets. Les builds de production sont déclenchées manuellement via GitHub Actions, avec une signature des images Docker par Cosign (afin d'éviter toutes modifications non autorisée) et des analyses hebdomadaires de sécurité avec Docker Scout pour détecter les vulnérabilités sur les images docker et GitHub Dependabot pour garder les paquets à jour et nous avertir en cas de CVE.











Application

L'application utilise le stack Ory pour l'authentification et l'autorisation, avec un accent sur le principe du moindre privilège et un accès refusé par défaut. La vérification des JWT est systématiquement effectuée avec Oathkeeper, qui analyse également les droits en amont de l'application. L'implémentation open source Keto de Zanzibar est utilisée, avec des mesures de sécurité supplémentaires comme Helmet, CRSF, et un rate-limit global. Des tokens CRSF sont utilisés sur les routes de l'authentification (par manque de temps, les autres formulaires n'ont pas cette vérification). Chaque route, chaque appel et chaque modification sont alors sécurisés en amont sur différents services. Kratos chiffre les mot de passe des utilisateurs via le protocole bcrypt rendant la possibilité de retrouver le mot de passe original (après une fuite de données) quasiment nulle.

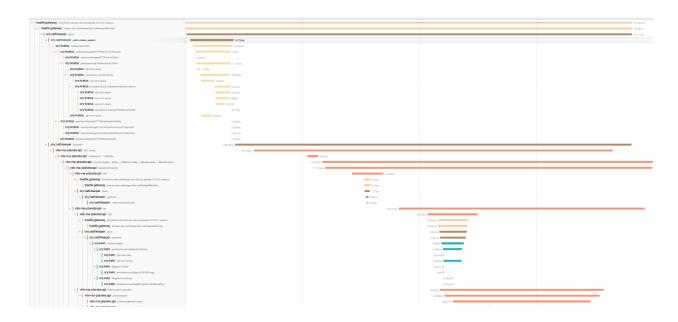
```
1 GET /protected HTTP/1.1
       Host: http-dump.dev.vite-ma-planete.127.0.0.1.sslip.io
       \textbf{Accept:} \ \texttt{text/html,application/xhtml+xml,application/xml;} \\ q = 0.9, */*; \\ q = 0.8
       Accept-Encoding: gzip, deflate
       Accept-Language: en-GB, en; q=0.9
       Authorization: Bearer eyJhbGci0iJSUzINiIsImtpZCI6ImEyYWE5NzM5LWQ3NTMtNGEwZC04N2VlLTYxZjEwMTA1MDI3NyIsInR5cCI6IkpXVCJ9.eyJleHAi0jE3MD
        E50TM1NDcsImlhdC16MTcwMTk5MjY0NywiaXNzTjoiaHR0cDovL29hdGhrZWVwZXIudml0ZS1tYS1wbGFuZXRlLmludGVybmFsIiwianRpIjoiM2UzMDkxNzYtYWU1MS00NWQ
       MjQuMDE00DMxWiIsImFldGhlbnrpY2F0aW9uX2lldGhvZHMiOlt7ImFhbCI6ImFhbDEiLCJjb2lwbGV0ZWRfYXQiOiIyMDIzLTEyLTA3VDIwOjAw0jIzLjk5MjEwMTU2OVoiL
       CJtZXRob2QiOiJwYXNzd29yZCJ9XSwiYXVOaGVudGljYXRvcl9hc3NlcmFuY2VfbGV2ZWwiOiJhYWwxIiwiZGV2aWNlcyI6W3siaWQiOiJjZjJiOGI2OC1lYmYxLTRkNjQtOD
       A2MC0zYTcyZDNjNW15NzUilCJpcF9hzGryzXNzIjoiMTkyLjE2OC4xMDcuMSIsImxvY2F0aW9uIjoiIiwidXNlc19hz2VudCI6Ik1vemlsbGevNS4wIChNYWNpbnrvc2q7IE1
       XR1ZF9hdCI6IjIwMjMtMTItMDdUMjA6MDA6MjMuOTcyNDhaIiwiaWQiOiI3OTVkYzgxMy00OTY4LTQ3ZWEtYTM2Zi04Mzk2ZmQ5MjJhMjciLCJtZXRhZGF0YV9wdWJsaWMi0m
        51bGwsinJlY292%XJ5X2FkZHJlc3Nlcy16W3siY3JlYXRl2F9hdC161jiwMjMtMTItmDdUMjA6MDA6MjMuOTc3Njg3WiIsImlkIjoiMDg4MTFkZDQtnjlkNy000DVmLTkxMjg
        tM2Z1ZGY0OGYyZGVhIiwidXBkYXRlZF9hdCI6IjIwMjMtMTItMDdUMjA6MDA6MjMuOTc3Njg3WiIsInZhbHVlIjoibWF4aWllQHZpdGUtbWEtcGxhbmV0ZS5mciIsInZpYSI6
       XRvcy9zY2hlbWFzL1pHVm1ZWFZzZEEiLCJzdGF0ZSI6ImFjdG12ZSIsInN0YXR1X2NoYW5nZWRfYXQi0iIyMDIzLTEyLTA3VDIwOjAwOjIzLjk3MTE2WiIsInRyYW10cy16ey
       \tt J1bWFpbC16Im1heG1tZUB2aXR1LW1hLXBsYW51dGUuZn1iLCJmaXJzde5hbWUiOiJNYXhpbWUiLCJsYXNOTmFtZS16IkZvdWNoZXIifSwidXBkYXR1ZF9hdC16IjIwMjMtMTI
        Y2U2LT14MmethGU1Zi04MzUyLTk40Wm2YjQzYzewni1sInn0YXR1cy16ImnvbxBszXR1zC1sInvwzGf0ZWrfYxQi0i1yMD1zLTeyLTa3VD1w0jAw0j1zLjk3NTUzOfoiLCJ2Y
        Wx12S161mlheGltzUB2axRllWlhLxBsYW51dGUuZnIilCJ2ZXJpZmllZCI6dHJ1ZSwidmVyaWZpZWRfYXQiOiIyMDIzLTEyLTA3VDIwOjAwOjQ0Ljc5NDA1MloiLCJ2aWEiOi
       {\tt J1bWfpbcJ9XX0sIm1zc3V1zf9hdcI6ijIwMjMtmTitMDdUMjA6MDA6MjMuOTkyMTaxWiJ9LCJzdWIioiI3OTVkYzgxMy00OTY4LTQ3ZWetYTM2Zi04Mzk2ZmQ5MjJhMjcifQ.}
       \verb|cun22fN-fzQJa718rjxuIuq|qt6ulOaNu7g-HgyAH\_PsmXXG3qKT-PXRJZ7uklz3zsUzfqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl\_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl\_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl\_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl\_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnKg-Qd9w9x7VRW3PeripQtvzVeTSkUhAJ5pYh0trWtlZKLsl_aXuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPKmp5YnMp4XuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToMPAXuBUrqCToM
       T6NBIYPTJeHdf74h322Q1H86FiuQNo_b8_F3MuRzzrOnMNZ7_BnnyUs_yPKrhT4M-JM9F0W702VX9gA-yBpC3aZf_kcp0kI4tCSu5aDEJ8GQqKjm39SvqBFN_jmDgDF598xc
       qI3wzoUYlphdubE2FQuJOjDBhMx9wnvRcZZHGkCeQCy73Jp3oH77Fw47tIR72f8JKzaO3otqn2cQ
      B3: 00000000000000004baa85c832855569-7a04d8dd418f2610-1
       \textbf{Cookie: csrf\_token\_29d645f3c0672a126d42428c4cc5252dc044ce3502f6d96ed7b193c49edf731d=NZigbS/+iqKkavvsWpn3u3iq7o5g5YTj30v/VczsRiE=; orygenerate and the cookies of the co
         \_k ratos\_session=\texttt{MTcwMTk3OTIyNHwwTkkzVEhnSjnPLUR00EQwM1A4cDFNR0pBeHhTMkt2dzFwM2pta1kyd3RUT3dxTzF4OGtfVm552TAzaTVkWXRVT0E1T09yNjZzVG4tM
       {\tt GpiSExTaGJkbwlkMHJRTmFRSV9VQmped3FncwFlVlbKNHloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUHlTmjvhX0N4YzdPSwvlVjbfzHUyOV}{\tt GpiSExTaGJkbwlkMHJRTmFRSV9VQmped3FncwFlVlbKNHloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUHlTmjvhX0N4YzdPSwvlVjbfzHUyOV}{\tt GpiSExTaGJkbwlkMHJRTmFRSV9VQmped3FncwFlVlbKNHloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUHlTmjvhX0N4YzdPSwvlVjbfzHUyOV}{\tt GpiSExTaGJkbwlkMHJRTmFRSV9VQmped3FncwFlVlbKNHloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUHlTmjvhX0N4YzdPSwvlVjbfzHUyOV}{\tt GpiSExTaGJkbwlkMHJRTmFRSV9VQmped3FncwFlVlbKNHloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUHlTmjvhX0N4YzdPSwvlVlybfzHUyOV}{\tt GpiSExTaGJkbwlkMHloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVlybfzHUyOV}{\tt GpiSExTaGJkbwlkMhloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVlybfzHUyOV}{\tt GpiSExTaGJkbwlkMhloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVlybfzHUyOV}{\tt GpiSExTaGJkbwlkMhloOHlDzzJkRFFzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVlybfzHUyOV}{\tt GpiSexTaGJkbwlkMhloOHlDzzJkrFfzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVyBfzHuyOV}{\tt GpiSexTaGJkbwlkMhloOHlDzzJkrFfzzFlPuEE3WUhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVyBfzHuyOV}{\tt GpiSexTaGJkbwlkMhloOHlDzzJkrFfzzFlPuEE3Wuhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVyBfzHuyOV}{\tt GpiSexTaGJkbwlkMhloOhlDzzJkrFfzzFlPuEE3Wuhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVyBfzHuyOV}{\tt GpiSexTaGJkbwlkMhloOhlDzzJkrFfzzFlPuEE3Wuhib3zfumexyllnQwdCcDrpMktoMjNnznhoUhlTmjvhX0N4YzdPSwvlVyBfzHuyOV}{\tt GpiSexTaGJkbwlkMhloOhlDzzJkrffzzFlPuEE3Wuhib3zfumexyllnQwdCcDrpMktoMiDzgJkwhibay}{\tt GpiSexTaGJkwhibay}{\tt GpiSexTaGJkwh
       6Zz09fGSQHnqqkOAM_P9s6vdV0Wp-W-ei8onbmWgcwaKIo2-N
  9 Http-Dump-Remote-Addr: 192.168.107.12:41878
10 Traceparent: 00-00000000000000004baa85c832855569-7a04d8dd418f2610-01
11 Uber-Trace-Id: 00000000000000004baa85c832855569:7a04d8dd418f2610:0:1
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Safari/605.1.15
14 X-B3-Sampled: 1
15 X-B3-Spanid: 7a04d8dd418f2610
16 X-B3-Traceid: 000000000000004baa85c832855569
17 X-Forwarded-Port: 80
18 X-Forwarded-Server: da951316493e
19 X-Real-Ip: 192.168.107.1
```

```
Content-Security-Policy: default-src 'self';base-uri 'self';font-src 'self' https: data:;form-action 'self';fram e-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Date: Fri, 08 Dec 2023 00:15:55 GMT
Keep-Alive: timeout=72
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XXSS-Protection: 0
```

```
- id: "dev:http-dump:protected"
 upstream:
   preserve_host: true
   url: "http://http-dump:3000"
 match:
   url: "http://http-dump.dev.vite-ma-planete.127.0.0.1.sslip.io/protected"
 authenticators:
   - handler: cookie_session
 authorizer:
   handler: allow
 mutators:
   - handler: id_token
 errors:
   - handler: redirect
- id: "dev:api-swagger:anonymous"
 upstream:
   preserve_host: true
   url: "http://api:3100"
   url: "http://api.vite-ma-planete.127.0.0.1.sslip.io/swagger/<.*>"
   methods:
     - GET
     - POST
     - DELETE
     - PATCH
 authenticators:
   - handler: anonymous
 authorizer:
   handler: allow
  mutators:
   - handler: noop
```

Un autre axe de développement de l'application s'est basé sur l'implémentation d'OpenTelemetry (un outil pour améliorer l'observabilité à travers des logs, des métriques et des traces) qui est un point très important afin d'extraire des logs (pour détecter des potentiels accès corrompus), des metrics et des traces des différents échanges entre les services (permettant de valider pendant la phase de développement les bonnes intéractions et les séparations de nos services). Voici un exemple sur l'application :

```
['level':info', 'time', '2023-12-88102.09:19.5192', 'reg', 'reg', 'method':'GE', 'url':'/notes, 'query':1]. 'headers':['not':-apl.vite-ma-planete.127.0.0.1.sslip.io', 'user-agent': 'Mozilla/5.0 (Manc S X 10:15) Applemekt/665.1.15 (KiffMl, like Geck) Version/17.0 Safari/665.1.15 (Apl.vite-ma-planete.127.0.0.1.sslip.io',wagger', 'traceparent': '00-0000000000000031866ea44c0733.1 Safari/665.1.15 (Apl.vite-ma-planete.127.0.0.1.sslip.io',wagger', 'traceparent': '00-00000000000000031866ea44c0733.1 Safari/665.1 Safari/665.1 Safari/665.1 Safari/665.1 Safari/665.1 Safari/665.1 Safari/665.1 Safar
```



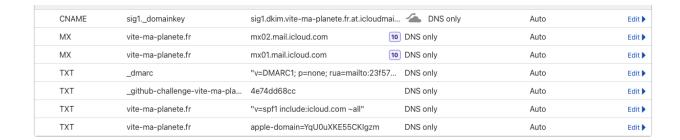
Nous suivons les principes du GitOps, donc la seule source de vérité de notre application est notre repository github, nous devons donc obligatoirement y mettre nos secrets de production. Pour cela, nous avons utilisé les Sealed Secrets de bitnami, qui permet de chiffrer les secrets avec une clé publique sur notre git et qui, une fois ajoutés sur le cluster Kubernetes, va automatiquement les déchiffrer avec la clé privée. Cela nous permet de versioner les modifications apportées depuis Git tout en ne les compromettant pas en cas d'accès non autorisé.

Infrastructure

L'infrastructure repose sur Kubernetes, appliquant le principe du moindre privilège. Un service mesh est utilisé pour chiffrer les communications entre les services et pour autoriser ces communications (avec un accès refusé par défaut), renforçant ainsi la sécurité et la gestion du trafic au sein de l'infrastructure. Les différentes applications sont conteneurisées afin d'être dans un environnement sandboxé (grâce au kernel) pour plus de sécurité, il aurait été préférable d'utiliser des VMs mais ici, la criticité des données était suffisamment faible pour imposer une isolation aussi forte et des ressources que nous n'avions pas.

Mailing

Les protocoles SPF, DKIM, et DMARC sont mis en place pour renforcer la sécurité des e-mails. Ces mesures aident à prévenir le spoofing, garantissent l'authenticité des e-mails envoyés et améliorent la réputation et la fiabilité des serveurs de messagerie.



Proxy

Cloudflare est utilisé comme proxy pour offrir une protection en amont contre les attaques et les DDoS, tout en masquant les IP des load balancers. Cette stratégie améliore significativement la sécurité en agissant comme un bouclier contre diverses menaces en ligne. Cloudflare offre un chiffrement TLS (HTTPS) aux utilisateurs finaux et délivre un certificat entre leurs serveurs et nos serveurs afin de chiffrer les communications entre les deux.