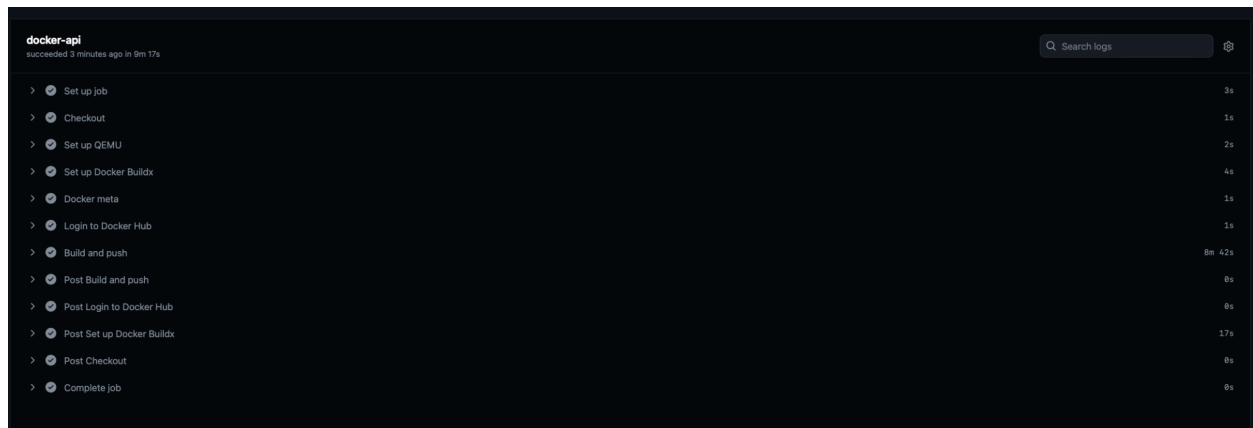
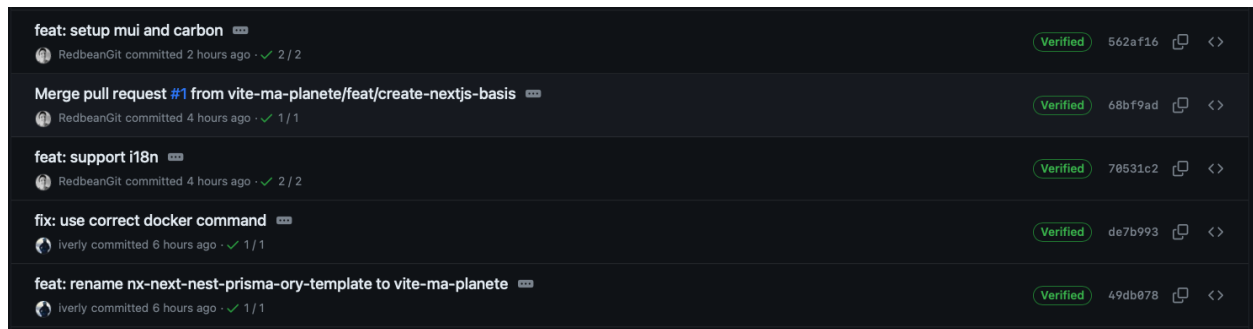


Reporting: Défi CS Group 2023 - La cyber c'est super




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.





iverly force-pushed the `feat/add-ai-module` branch from `a91ecb7` to `9c2c185` 2 hours ago [Compare](#) [Lock](#)


Add more commits by pushing to the `feat/add-ai-module` branch on `vite-ma-planete/vite-ma-planete`.



**Review required**
New changes require approval from someone other than the last pusher. [Learn more about pull request reviews.](#)

**No unresolved conversations**
There aren't yet any conversations on this pull request. [View](#)


**All checks have passed**
2 successful checks [Show all checks](#)

**Merging is blocked**
Merging can be performed automatically with 1 approving review.



☐ **Merge without waiting for requirements to be met (bypass branch protections)**

Merge pull request

You can also [open this in GitHub Desktop](#) or view [command line instructions](#).


 Add a comment


Release v0.1.5 Latest [Compare](#) [Edit](#) [Delete](#)


github-actions released this 13 minutes ago v0.1.5  a155283 

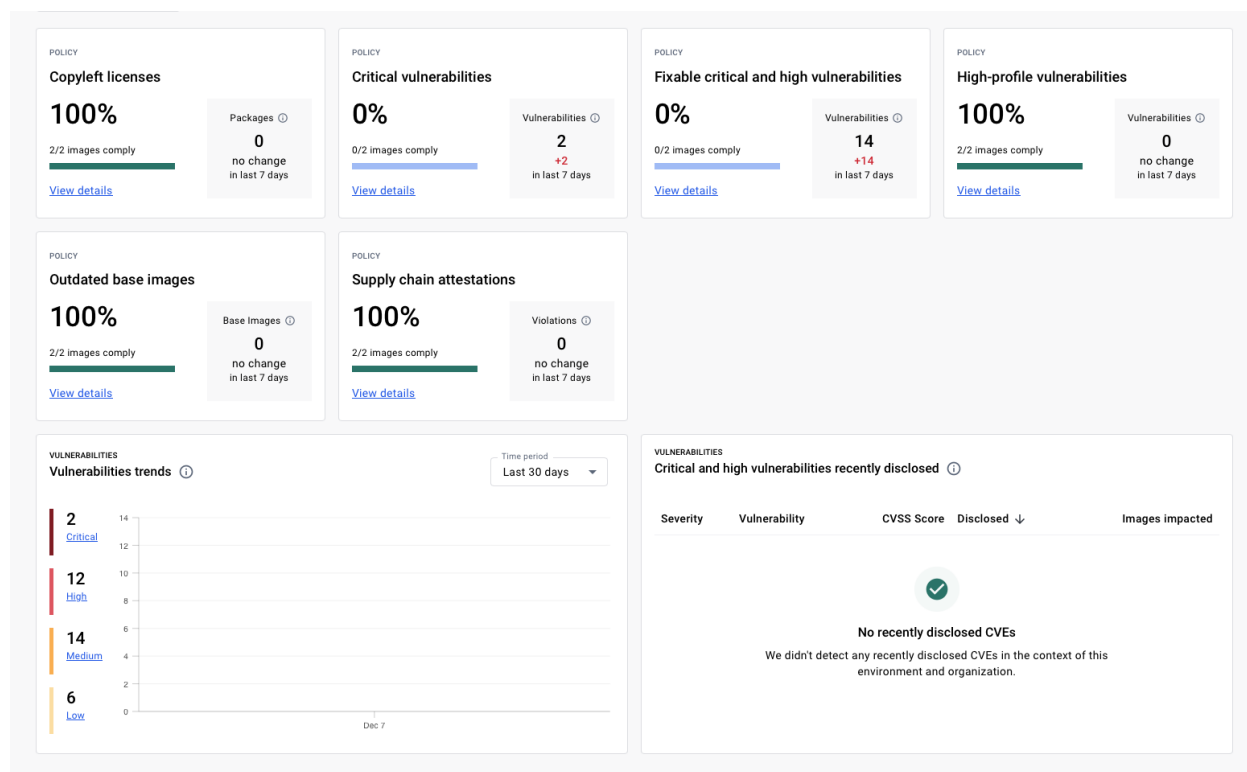
v0.1.5

▼ Assets 2

 Source code (zip) 13 minutes ago

 Source code (tar.gz) 13 minutes ago





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 mots 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.

```

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 'se
lf' 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-XSS-Protection: 0

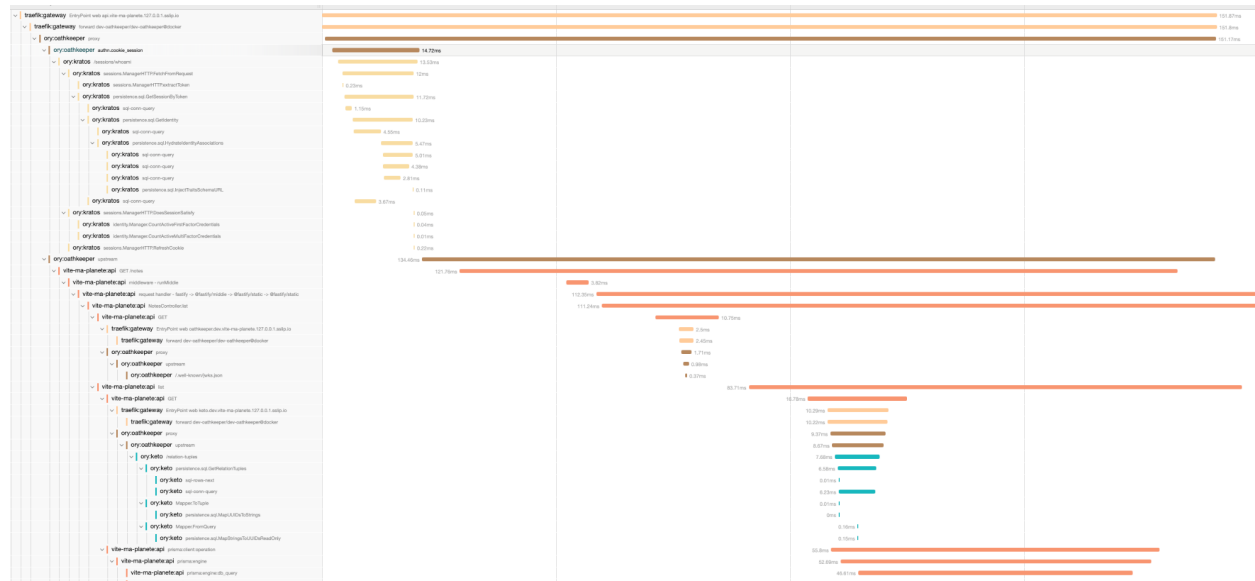
```

```
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"
  methods:
    - GET
  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"
match:
  url: "http://api.vite-ma-planete.127.0.0.1.sslip.io/swagger/<.*>"
  methods:
    - GET
    - POST
    - PUT
    - 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 interactions et les séparations de nos services). Voici un exemple sur l'application :

[illegible]





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 versionner 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.

CNAME	sig1._domainkey	sig1.dkim.vite-ma-planete.fr.at.icloudmai...	 DNS only	Auto	Edit ►
MX	vite-ma-planete.fr	mx02.mail.icloud.com	 DNS only	Auto	Edit ►
MX	vite-ma-planete.fr	mx01.mail.icloud.com	 DNS only	Auto	Edit ►
TXT	_dmarc	"v=DMARC1; p=none; rua=mailto:23f57...	DNS only	Auto	Edit ►
TXT	_github-challenge-vite-ma-pla...	4e74dd68cc	DNS only	Auto	Edit ►
TXT	vite-ma-planete.fr	"v=spf1 include:icloud.com ~all"	DNS only	Auto	Edit ►
TXT	vite-ma-planete.fr	apple-domain=YqU0uXKE55CKlgzm	DNS only	Auto	Edit ►

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.