Sécurité, confidentialité & Infrastructure technique

SECURITE LOGIQUE

1. Infrastructure Technique

Eurécia est une solution SaaS sécurisée et multitenant.

Technologies

Les langages et outils que nous utilisons sont open-source, fiables, performants, éprouvés et maintenus à jour :

- Java/Kotlin (Spring et Hibernate), PHP (Laravel et Eloquent), Typescript (Vuejs)
- Architecture multi-tiers
- Serveurs : Linux Debian, Apache, Tomcat, MySQL, MongoDB, RabbitMQ

SLA

- Accessible 24h/24 et 7j/7
- Taux de disponibilité à l'année 99,7%

Intégrations

Interopérabilité et ouverture vers le système du client

- API / Web services
- Fichiers en FTPS
- Connecteurs

Pour plus de détails sur l'architecture, voir le schéma en annexe

2. Authentification

Authentification intégrée

- Le mot de passe d'un utilisateur doit respecter les exigences suivantes (misent à jour selon les règles de l'ANSSI et de la CNIL) :
- Une longueur minimale de 12 caractères
- Contenant au moins : 1 majuscule, 1 minuscule, 1 chiffre, 1 caractère spécial parmi les suivants : !@#$%^&*()-+
- Le nouveau mot de passe devra être diffèrent des 3 derniers mots de passe

Le nombre de tentatives d'authentification à la plateforme Eurécia est limité à 5. Au-delà, le compte de l'utilisateur est bloqué pendant 15 minutes.

Single Sign-On

Eurécia permet la connexion par SSO au travers du protocole SAML 2.0 (Security Assertion Markup Language). Grace à SAML, l'authentification des utilisateurs est gérée en autonomie par la DSI (ex : LDAP) et Eurécia n'accède qu'aux informations strictement nécessaires.

Pour en savoir plus : https://help.eurecia.com/hc/fr/articles/115000660785Comment-activer-une-connexion-SSO-avec-Eurécia

3. Sécurisation des flux web

La plateforme Eurécia est disponible uniquement en HTTPS (TLS). Les requêtes saisies en http sont automatiquement redirigées de http vers https, de manière totalement transparente pour l'utilisateur.

4. Flux réseau

Seuls les flux indispensables sont ouverts au niveau des pares-feux

5. API

Eurécia propose une API de type REST. Elle permet, par WebServices, la récupération de l'ensemble données saisies dans Eurécia. La sécurisation des accès se fait par token (passé dans le Header de la requête). Le nombre de tentatives d'authentification aux WebServices d'Eurécia est limité à 10.
Au-delà, l'adresse IP utilisée est bloquée pendant 60 minutes.
Pour en savoir plus : http://dev.eurecia.com

6. Sécurité des données

En base de données

Les données sensibles sont chiffrées avec : Un algorithme irréversible pour les mots de passe Un algorithme réversible pour les informations dites sensibles (ex : bancaires) L'algorithme de chiffrement utilisé est du SHA256.Les données au repos (sur disque) sont chiffrés par défaut par GCP avec un algorithme AES-256.

Sur système de fichiers

Les fichiers transférés sur le logiciel Eurécia sont stockés sur Buckets GCP dans des espaces dédiés auxquels seuls les serveurs de Eurécia ont accès. Les fichiers sont ensuite classés selon une arborescence propre à chaque client. Les fichiers au repos (sur disque) sont chiffrés par défaut par GCP avec un algorithme AES-256.

7. Cloisonnement des données

Le cloisonnement des données est assuré par un TENANT_ID associé à chaque client, utilisé dans chaque requête et lié à chaque objet métier stocké en base de données. L'application Eurécia gère la sécurité sur l'ensemble des transactions effectuées au travers de cet ID qui est validé avec l'utilisateur en session.

8. Sauvegarde

Les dumps de base de données sont réalisés 2 fois par jour avec une rétention de 60 jours par sociétés permettant de restaurer l'état d'un client à une date précise. Des dumps de l'ensemble de la base de données sont réalisées quotidiennement. Toutes ces sauvegardes sont répliquées sur plusieurs zones, en France, et sur une seconde région, en Belgique, afin d'assurer un accès à la donnée même en cas de faille d'une zone ou région.

Les fichiers sont synchronisés entre les 3 datacenters de Paris permettant de conserver leur accès même si une des zones venait à être inaccessible.

9. Pare-feu

Nos environnements disposent de deux niveaux de pare-feu :

- Un pare-feu Cloudfare qui gère les flux entrants, limite les accès et détecte les attaques. Complété par une protection Cloud Armor de Google
- Chaque machine dispose en plus de son propre pare-feu logiciel sur lequel des restrictions supplémentaires sont implémentées pour limiter les accès de chaque flux selon une liste blanche prédéfinie.

Seuls les flux nécessaires au bon fonctionnement de Eurécia sont autorisés.

10. Plan de continuité (PCA) et de reprise d'activité (PRA)

Les bases de données et les fichiers sont configurés chez GCP en HA (High Availability) ce qui assure une redondance entre les 3 zones/datacenters présents dans la région Paris.

Les disques, réseaux et toute l'architecture GCP est ainsi pensée pour assurer une continuité de service maximale.

Ainsi le seul cas d'indisponibilité, lié à l'infrastructure que nous pourrions rencontrer serait une perte de la région Paris.

Ce cas serait extrême mais nous avons tout de même mis en place un PRA afin d'assurer la reprise de service.

Les données et fichiers sont synchronisés en permanence vers une autre région de GCP, la Belgique, comme le conseille les bonnes pratiques de sécurités et de continuité de service.

Nos engagements varient selon les types d'incidents rencontrés et sont dans le pire des cas :

- Objectif de délai de reprise (RTO) de 4h maximum
- Objectif de point de reprise (RPO) de 5h maximum

11. Suivi des failles de sécurité

Eurécia utilise les outils reconnus :

- DependencyTrack
- Sonar (Security Report)

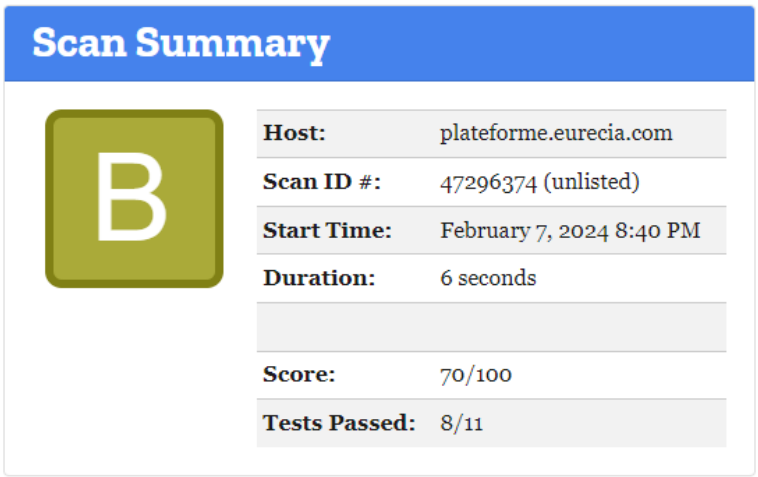
Pour assurer une veille permanente sur les vulnérabilités de son application et ainsi réagir au plus vite pour les corriger.

En complément de cela nous effectuons des tests de pénétration (Pentest) à un rythme annuel avec différentes sociétés (iTrust, Cyblex…) comme le confirme l'attestion en annexe.

12. Mise en place des bonnes pratiques de sécurité Web

Nous suivons les bonnes pratiques en constante évolution pour assurer une sécurité maximum à nos clients. Nos équipes sont formées aux risques en Cybersécurité régulièrement (et de manière avancée sur les techniques de piratage pour les équipes en charge de l'application).

De plus nous suivons les indications des organismes reconnus.



https://observatory.mozilla.org/analyze/plateforme.eurecia.com

13. Administration des environnements

Le personnel d'administration dispose de comptes super utilisateurs nominatifs et unipersonnels sur tous les systèmes de la plateforme. Tous les accès se font en SSH. Les actions nécessitant des privilèges super utilisateur sont consignées dans les journaux systèmes.

SECURITE PHYSIQUE

GCP assure un très haut niveau de sécurité de ses infrastructures physiques.

Les centres de données sont protégés par plusieurs couches de sécurité pour empêcher tout accès non autorisé à vos informations. Ils utilisent des systèmes de défense périmétrique sécurisés, une couverture complète par caméras, une authentification biométrique et une équipe d'agents de sécurité 24h/24, 7j/7. De plus, une politique stricte d'accès et de sécurité aux centres de données et des formations pour l'ensemble du personnel sont mis en place.

Pour en savoir plus, voir la page dédiée à la Data Security.

Afin de démontrer cet engagement, GCP a de très nombreuses certifications tel que ISO 27001, ISO 50001, EU Cloud Code of Conduct, RGPD (GDPR)... Elles sont toutes consultables sur la page des offres de conformités.

Efficacité énergétique

Dans le but de diminuer l'impact de consommation en énergie d'un centre de données, GCP analyse et améliore continuellement son usage et assure une efficacité maximale réduisant ainsi son empreinte carbone.

Pour plus de détail, voir les méthodes d'efficacité misent en place ainsi que leur objectif de développement durable :

https://www.google.com/intl/fr/about/datacenters/efficiency/

https://www.google.com/intl/fr/about/datacenters/cleanenergy/

ANNEXES

Schéma d'architecture