Plan de sécurité

Diffusion : OpenClassrooms – Mentor : Cesare de Padua - Evaluateur : Théo Lemoine

Version	***Date***	***Auteur***	***Motif***
1		Christophe Pierrès	Création du document
2			

Contenu ***Page***

1. Plan de Sécurité.....3
1.1. Risques et solutions identifiés.....3
1.2. Infrastructure principale.....4
1.2.1. Grosse faiblesse de déploiement de la V1.....4
1.2.2. Méthodologie de sécurité appliquée.....4
1.2.3. Architecture de Sécurité Globale pour la V2.....4
1.2.4. Détail des composants.....4
1.2.5. Chiffrage.....5
1.2.5.1. Comparatif coûts par provider.....5
1.2.5.2. Synthèse.....5
1.2.5.3. RGPD facilité.....6
1.2.5.4. Recommandations par Phase.....6

1. Plan de Sécurité

1.1. Risques et solutions identifiés

Risque	**Contexte**	**Gravité (de 1 à 5)**	**Solutions / outils potentiels**
Compromission des données utilisateur par transmission non sécurisée	Certaines API V1 utilisent encore HTTP, exposant les données sensibles en transit	5	- Migration complète vers HTTPS/TLS 1.3 - Implémentation de HSTS (HTTP Strict Transport Security) avec preload list - Headers de sécurité (CSP, HSTS, X-Frame-Options) - Outils : Let's Encrypt
Vol de mots de passe et usurpation d'identité	Système d'authentification V1 utilise MD5 (obsolète et vulnérable) sans politique de mots de passe	5	- Migration vers bcrypt ou Argon2 - Politique de mots de passe robuste (12+ caractères, complexité) - Authentification multi-facteurs (2FA) - Outils : développer son propre système d'authentification (Spring Security) ou Auth0 ou Firebase Auth (Google)
Attaques par déni de service (DDoS)	Architecture V1 sur serveur unique, vulnérable aux attaques volumiques	4	- Load balancer managé avec protection DDoS - CDN avec filtrage de trafic - Auto-scaling des ressources - Outils : HA Proxy (pour OVH), Cloudflare, AWS Shield, Azure DDoS Protection
Injection de code malveillant dans les requêtes	APIs sans validation stricte des entrées utilisateur (catalogue, recherche)	4	- Validation et sanitisation des inputs - Parameterized queries/ORM - Web Application Firewall (WAF) - Outils : OWASP ZAP
Compromission des données de paiement	Nouveau tunnel d'achat V2 manipulant des informations financières sensibles	5	- Compliance PCI DSS - Tokenisation des données de paiement - Utilisation de processeurs de paiement certifiés - Outils : Stripe, PayPal, Square
Attaques sur l'authentification OAuth	Implémentation Google/Apple OAuth sans sécurisation appropriée	3	- Validation des tokens JWT - Implémentation PKCE (Proof Key for Code Exchange) - Rotation régulière des clés API - Outils : OAuth 2.0 libraries, JWT.io
Manipulation des modèles 3D et contenu AR	Simulateur AR pouvant charger du contenu malveillant ou inapproprié	3	- Validation des fichiers 3D uploadés - Sandboxing du moteur de rendu - Signature numérique des modèles

Risque	Contexte	Gravité (de 1 à 5)	Solutions / outils potentiels
			- Outils : 3D file validators, ARCore/ARKit security guidelines
Exposition d'informations sensibles dans les logs	Risque de logging d'informations personnelles ou de paiement	3	- Politique de logging sécurisée - Masquage automatique des données sensibles - Chiffrement des logs - Outils : ELK Stack (**E**lastic search+**L**ogstgash+**K**ibana), solution managée chez OVH (OVH Logs Platform)
Attaques par session hijacking	Sessions utilisateur non sécurisées permettant l'usurpation	3	- Tokens de session sécurisés (HttpOnly, Secure, SameSite) - Rotation automatique des sessions - Détection d'anomalies de connexion - Outils : JWT avec refresh tokens

1.2. Infrastructure principale

1.2.1. Grosse faiblesse de déploiement de la V1

- Mono serveur (pas de tolérance aux pannes, pas de scalabilité)

1.2.2. Méthodologie de sécurité appliquée

Availability Management : Architecture redondante avec load balancing et auto-scaling pour maintenir 99.9% de disponibilité et éviter les pertes financières liées aux indisponibilités.

1.2.3. Architecture de Sécurité Globale pour la V2

- Mise en place architecture multi-Availability Zones
- Utilisation de bases de données gérées avec réplication automatique
- Stockage des fichiers dans un service de stockage d'objets avec versioning

1.2.4. Détail des composants

- Load Balancer :

HAProxy containerisé en HA (2 instances) avec Keepalived/VIP **OU** Load Balancer managé cloud (OVH/Azure) pour élimination SPOF + health checks automatiques

auto-discovery des services

- Application tier :

2-3 containers Docker de l'application répartis sur plusieurs nœuds

- Base de données :

managée cloud (OVH/Azure) avec backup automatique multi-zones + script de vérification d'intégrité containerisé mensuel

- Monitoring :

Stack Prometheus + Grafana + AlertManager entièrement containerisée sur nœud dédié monitoring

- Reverse Proxy :

NGINX containerisé pour terminaison SSL/TLS et routing, déployé sur nœud edge/DMZ

- Cache :

Redis containerisé sur nœud séparé ou co-localisé avec application selon charge

- Orchestration :

Docker Swarm (simple) ou Kubernetes (avancé) pour scaling automatique multi-nœuds

- CI/CD :

Pipeline Jenkins CI containerisé sur infrastructure dédiée (séparée production)

- Logs :

ELK Stack (Elasticsearch, Logstash, Kibana) en containers sur nœud dédié avec stockage persistant

1.2.5. Chiffrage

1.2.5.1. Comparatif coûts par provider

Composant	OVH Cloud	AWS	Azure	Écart vs OVH
Compute (4 VMs)	160€	335€	210€	AWS: +109% / Azure: +31%
Load Balancer	10€	30€	30€	AWS/Azure: +200%
Base de Données	90€	86€	83€	AWS: -4% / Azure: -8%
Stockage (600GB)	44€	37€	56€	AWS: -16% / Azure: +27%
Réseau (500GB)	29€	90€	52€	AWS: +210% / Azure: +79%
Monitoring/Logs	15€	25€	35€	AWS: +67% / Azure: +133%
Support	Inclus	100€*	50€*	AWS: +100€ / Azure: +50€
TOTAL MENSUEL	348€	603€	466€	AWS: +73% / Azure: +34%
TOTAL ANNUEL	4 176€	7 236€	5 592€	AWS: +3 060€ / Azure: +1416€

*Support technique professionnel en option

1.2.5.2. Synthèse

Critère	🥇 OVH	🥈 Azure	🥉 AWS
Prix	348€/mois	466€/mois (+34%)	603€/mois (+73%)
RGPD	✅ Facilité	✅ Conforme	⚠️ Cloud Act US
Simplicité	✅ Excellente	✅ Bonne	❌ Complexe
Écosystème	⚠️ Limité	✅ Riche	✅ Le plus vaste
Support FR	✅ Inclus	💰 Payant	💰 Très cher
Performance	✅ optimisé EU	✅ Global	✅ Worldwide

1.2.5.3. RGPD facilité

Avantages techniques :

- ✅ Datacenters européens (France/Allemagne)
- ✅ Pas de Cloud Act US
- ✅ Contrat sous-traitance RGPD inclus
- ✅ Certifications ISO 27001, SOC2
- ✅ Chiffrement données au repos/transit
- ✅ Logs d'accès traçables
- ✅ Support juridique français

Avantages RGPD :

- ✅ Droit européen applicable
- ✅ Tribunaux français compétents
- ✅ Pas de transfert hors UE par défaut
- ✅ DPO accessible en français
- ✅ Jurisprudence française connue

Limitations :

- ❌ Ne dispense pas des obligations business
- ❌ Politique confidentialité à rédiger
- ❌ Consentements à gérer

1.2.5.4. Recommandations par Phase

Phase Startup	Coût/mois	Users Max	Justification
🌱 MVP (OVH Light)	130€	1 000	Architecture minimale viable
🚀 Growth (OVH Standard)	348€	10 000	Architecture complète présentée
🏢 Scale-up (OVH Premium)	580€	50 000+	Multi-zones + support premium