

RRA for Fast Car Connect

| | |
|------------------------------------|----------------------------------------------------------------------------------------|
| Service Owner(s) | Département SuperCarX |
| Owner's Director | VP Security de Fast Car |
| Service Data Classification | Confidentiel, Données personnelle et techniques (PII, géoloc, identifiants et secrets) |
| Highest Risk Impact | MAXIMUM |

1. Notes à propos du service

1.1 Description du service

Fast Car est un constructeur automobile qui souhaite sortir une nouvelle voiture connectée qui pourra offrir à ses clients une étendue de nouveaux services de divertissement, d'aide à la conduite ainsi que des capacités d'accès à distance aux données du véhicule.

Ces nouveaux services incluent entre autres la visualisation de la météo et de la qualité de l'air ainsi que la possibilité de retrouver les coordonnées de ses contacts en se connectant à son compte Google. Pour des évolutions à venir (Télédiagnostic et application mobile My FastCar) le véhicule transmettra en temps réel ses indicateurs de fonctionnement.

1.2 Fonctionnement du service

1.2.1 Périmètre

Le schéma ci-après (*Figure 1. Schéma simplifié de l'architecture voiture connecté SuperCarX*) décrit le service faisant l'objet de ce RRA qui est nommé : "Application Microservice" et est situé entre d'une part la voiture connectée et d'autre part les services extérieurs appelées sur le schéma "Service".

Cette architecture est au stade de projet, sa mise en production est prévue pour la sortie de la nouvelle voiture de Fast Car, la SuperCarX fin décembre 2025.

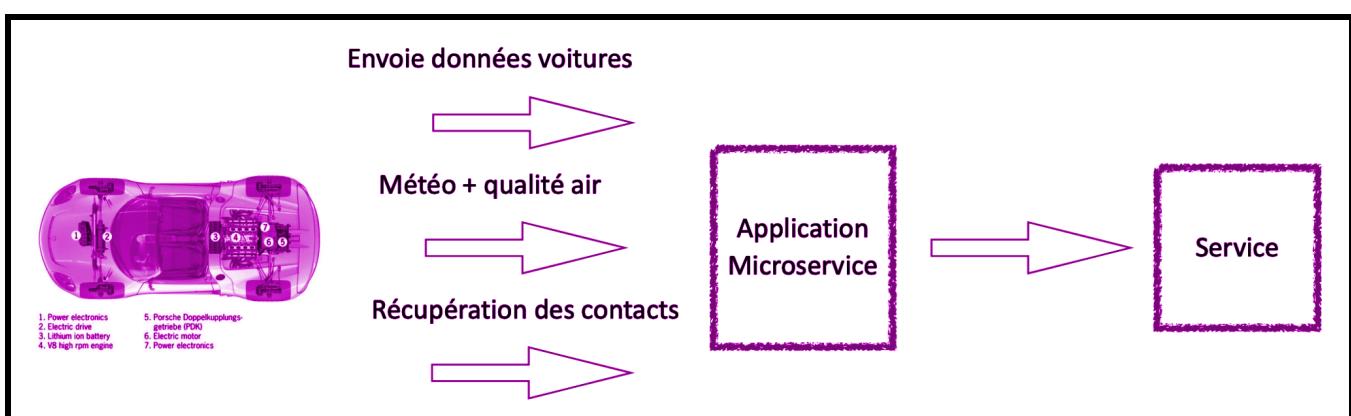


Figure 1. Schéma simplifié de l'architecture de voiture connectée SuperCarX

1.2.2 Décomposition fonctionnelle du service

Le service permet d'opérer les fonctionnalités suivantes :

- Réception des données télémétriques en temps réel depuis le véhicule
- Envoi au véhicule de données météo et de qualité de l'air par géolocalisation en utilisant un service externe
- Récupération des contacts Google de l'utilisateur connecté au véhicule en utilisant Google API (OAuth2).

1.2.3 Décomposition technique du service par composant

1. API Gateway

C'est la plateforme qui communique avec le véhicule, elle possède les services suivants :

1) Authentification du véhicule au serveur en utilisant le mTLS, le véhicule contient en effet une clé privée stockée dans un HSM avec un certificat X.509

2) Réception et traitement des demandes du véhicule :

- Push télémétrie
- Requêtes météo
- Requêtes pour l'import des contacts (flux OAuth de l'utilisateur)

3) Stockage des données de télémétrie rattachées au véhicule

2. Microservice Météo / Air

C'est la plateforme située derrière l'API Gateway qui est chargée de fournir, en utilisant les coordonnées du véhicule, les données de météo et de qualité de l'air depuis une source externe en l'occurrence celle-ci : weatherapi.com

3. Microservice Contacts

C'est la plateforme située derrière l'API Gateway qui est chargée de fournir un service de récupération de contact depuis un fournisseur extérieur en l'occurrence ici google via <https://developers.google.com/people?hl=fr>

4. Services support et transverses

Afin de permettre à la plateforme de répondre à l'état de l'art en terme de sécurité, elle disposera des éléments suivants en terme d'observabilité et de sécurité :

- Journalisation structurée, traces distribuées, SIEM, secrets en coffre (KMS / Vault), SCA/SAST/DAST dans la CI/CD.

5. Architecture

Plateforme de microservices conteneurisées consommées par une voiture connectée. Le code est hébergé sur Gitlab avec des exigences DevSecOps.

1. Dictionnaire de données

Liste des données stockées ou en transit dans le service.

| Data name / type | Classification | Comments |
|-------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| UUID du véhicule | Interne | Id technique |
| Télémétrie (vitesse, carburant, temp. Moteur, états freins, etc.) | Confidentiel | Peut révéler des habitudes de conduite et l'état du véhicule. |
| Position GPS | Confidentiel (PII) | Données personnelles sensibles (trajectoire, etc.) Permettrait de géolocaliser la voiture -> utiliser géohash pour minimiser la précision |
| Contacts Google | Confidentiel (PII) | Importés via service google read-only |
| Tokens auth Google | Restreint | Secret sensible (stockage KMS/vault uniquement) |
| Logs (requêtes, métriques, traces) | Restreint | Interdire PII en clair : infos à masquer et filtrer |
| Métadonnées réseau (IP, user-agent) | Interne | À pseudonymiser si exportation pour analyse |

2. Scénarios de menace

| Réputation | Productivité | Financier | C-I-A | Threat Scenario | Justifications impacts |
|------------|--------------|-----------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAXIMUM | MEDIUM | € | C | <p>Fuites de diverses données :</p> <ul style="list-style-type: none"> • Tokens OAuth Google : logs CI, variables gitlab exposées, extraction des contacts • Coordonnées GPS • Via dépendance : WeatherAPI • Via logs trop bavards : PII, tokens, etc. • Via GitLab : projet public par erreur -> fork, .env avec secrets, etc. • Périmètre OAuth trop large : collecte excessive, non conformité RGPD | <p><u>Réputation</u> : Perception de faible qualité. Perte de confiance.</p> <p><u>Productivité</u> : Temps d'analyse, de correction de déploiement.</p> <p><u>Financier</u> : Correspond à une perte de chiffre d'affaires, conséquence de la baisse des ventes..</p> |
| MAXIMUM | MAXIMUM | €€€ | I | <p>Un attaquant accède et altère les données utilisées par le système de conduite ou le système lui-même causant accident, inconfort ou dommage au véhicule ou à des tiers:</p> <ul style="list-style-type: none"> • Commande du véhicule: <ul style="list-style-type: none"> ◦ Climatisation : contrôler la température de chaud à froid pour provoquer un inconfort ou une impossibilité d'utilisation ◦ Batterie : provoque une consommation excessive pour décharger, rendre inutilisable ou dangereux le véhicule ◦ Modification malveillante des données, du système d'assistance à la conduite provoquant des accidents au véhicule et ou à des tiers ◦ Vol de véhicule • Stockage des données <ul style="list-style-type: none"> ◦ Corruption des données lors du stockage local (e.g. base de données contacts) | <p><u>Réputation</u> : les clients ne font plus confiance au constructeur et veulent se séparer de leur véhicule. Dommages humains, effondrement des ventes avec faillite du constructeur.</p> <p><u>Productivité</u> : Temps d'analyse, de correction de déploiement très importante pour des véhicules qui peuvent ne pas être connectés régulièrement au réseau. Frais de SAV.</p> <p><u>Financier</u> : Correspond à une perte de chiffre d'affaires dû à un effondrement des ventes et changement de priorité pour prioriser l'analyse et la recherche de solutions.</p> |
| HIGH | HIGH | €€ | I | <p>Spoofing véhicule</p> <ul style="list-style-type: none"> • Absence de mTLS ou validation faible -> injection télémétrie falsifiée, alertes erronées, investigations coûteuses. | <p><u>Réputation</u> : Impact sur l'image de l'entreprise</p> <p><u>Productivité</u> : Temps d'analyse long, déploiement de nouveaux certificats</p> |

Fast Car Confidential - Specific Workgroups and Individuals Only

| Réputation | Productivité | Financier | C-I-A | Threat Scenario | Justifications impacts |
|----------------|----------------|-----------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | | <ul style="list-style-type: none"> L'Autorité de Certification qui signe le certificat (X.509) du véhicule est corrompue -> des certificats peuvent être générés et être acceptés par l'API Gateway La clé privée du véhicule est corrompue -> elle est utilisée pour usurper le véhicule | <p>potentiellement coûteux à faire en retour SAV ou avec une MAJ OTA si disponible.</p> <p><u>Financier</u> : Élevé dû aux coûts de SAV, aux impacts sur les ventes et à la mobilisation des équipes pour analyser et corriger.</p> |
| MEDIUM | LOW | € | I | Replay attacks (absence nonce/horodatage) -> duplication d'événements, pollution des séries temporelles. | <p><u>Réputation</u> : Impacts sur l'image de l'entreprise, manque de fiabilité</p> <p><u>Productivité</u> : faible complexité pour l'analyse et le correction</p> <p><u>Financier</u> : faible diminution des ventes</p> |
| MAXIMUM | MAXIMUM | \$\$\$ | I | Supply-chain (image compromise, dépendance NPM/PyPI malveillante) -> code altéré, portes dérobées. Exploitation malveillante des véhicules à distance pouvant provoquer des accidents. | <p><u>Réputation</u> : les clients ne font plus confiance au constructeur et veulent se séparer de leur véhicule. Dommages humains, effondrement des ventes avec faillite du constructeur.</p> <p><u>Productivité</u> : Complexité à corriger et à redéployer</p> <p><u>Financier</u> : Élevé dû aux coûts de SAV, aux impacts sur les ventes et à la mobilisation des équipes pour analyser et corriger.</p> |
| LOW | LOW | € | I | Corruption partielle des contacts (écriture non voulue, mapping défectueux) -> mauvaise expérience utilisateur, erreurs côté voiture. | <p><u>Réputation</u> : Impacts sur l'image de l'entreprise, manque de fiabilité</p> <p><u>Productivité</u> : Analyse, correction et rattrapage de données</p> <p><u>Financier</u> : faible diminution des ventes</p> |

Fast Car Confidential - Specific Workgroups and Individuals Only

| Réputation | Productivité | Financier | C-I-A | Threat Scenario | Justifications impacts |
|----------------|---------------|-----------|-------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HIGH | HIGH | € | A | DDoS/API flood (gateway non protégé, manque de rate-limit) -> indisponibilité des services en conduite. | <u>Réputation</u> : Impacts sur l'image de l'entreprise, image de manque de fiabilité, associé à des dysfonctionnements. Difficultés d'utiliser son véhicule <u>Productivité</u> : Compliqué à corriger si une infra spécifique n'a pas été prévue pour limiter les attaques DDOS. <u>Financier</u> : Baisse des ventes |
| MEDIUM | MEDIUM | € | A | Quota/Outage vendors (Weather/Google) -> dégradation fonctionnalités ; erreurs en chaîne si absence de circuit-breaker. | <u>Réputation</u> : Impacts sur l'image de l'entreprise, manque de fiabilité, associé à des dysfonctionnements <u>Productivité</u> : Diagnostic trivial mais difficulté de trouver rapidement un nouveau fournisseur <u>Financier</u> : Baisse du volume des ventes |
| LOW | MEDIUM | € | A | Pics télémétrie (tempêtes d'événements flottes) -> saturation files, backpressure, latence accrue. | <u>Réputation</u> : Impact sur l'image de l'entreprise <u>Productivité</u> : Complexité à diagnostiquer et corriger <u>Financier</u> : Baisse du volume des ventes |
| MAXIMUM | MEDIUM | €€€ | A | Incidents CI/CD (déploiement défectueux) -> indisponibilité ; absence de rollback automatique. Véhicule potentiellement rendu inutilisable | <u>Réputation</u> : Fort impact sur l'image de l'entreprise <u>Productivité</u> : Complexité à diagnostiquer et à corriger |

Fast Car Confidential - Specific Workgroups and Individuals Only

| Réputation | Productivité | Financier | C-I-A | Threat Scenario | Justifications impacts |
|------------|--------------|-----------|-------|-----------------|----------------------------------------------------------------------------------------------------------|
| | | | | | <u>Financier</u> : Frais de SAV en plus des impacts sur le chiffre d'affaires dû à la perte de confiance |

3. Recommandations

Liste des recommandations.

| Impact | Recommandations |
|----------------|---------------------------------------------------------------------------------------------------------------------|
| MAXIMUM | Utiliser le protocol mTLS pour l'identification et la communication entre le véhicule et le service |
| MAXIMUM | Utiliser le protocole OAuth avec une politique de moindres priviléges |
| MAXIMUM | Gérer les secrets avec l'utilisation de KMS / Vault |
| HIGH | Minimisation des données : Géohash de la localisation pour appels météo, pas de persistance des contacts par défaut |
| HIGH | Sécurisation de l'API : utilisation de JWT et d'une politique de rate limiting |
| HIGH | Logs et détection : Logs sans PII, traçage et métriques, SIEM, alertes |
| HIGH | Supply chain et CI/CD : SBOM, SCA, signature d'images, scans SAST/DAST/IaC, attestation SLSA >= L3 |