Cybersécurité des Systèmes Industriels

TD : Étude de Cas

Introduction

Le contexte est celui d'une entreprise française dont l'employeur souhaite équiper les véhicules de fonction de ses commerciaux de dispositifs de géolocalisation[1]. Son but est essentiellement d'optimiser leurs déplacements pour réduire les coûts associés, dans la mesure où il a la charge d'organiser leurs déplacements[2] de manière individuelle.

En effet, l'employeur a constaté les limites des dispositifs de planification standards individuels. Ils ne permettent pas de planifier des itinéraires complexes d'un seul véhicule, et encore moins d'un parc complet. Il n'est donc pas possible d'optimiser les déplacements des commerciaux dans leur ensemble. En outre, ils ne mesurent que la position du véhicule et ne considèrent pas la durée d'utilisation du véhicule, le kilométrage parcouru ou les vitesses de circulation, ce qui limite les possibilités d'optimisation. Le service associé doit donc permettre cette optimisation d'itinéraires.

L'étude des risques a pour objectif de déterminer des modalités de mise en œuvre respectueuses de la vie privée de ses employés. En effet, l'enjeu de l'employeur réside dans l'acceptation du traitement par les commerciaux, qui pourraient contester la proportionnalité du dispositif ou estimer qu'ils doivent avoir une liberté dans leurs déplacements.

L'employeur : Comment faire en sorte que mes commerciaux ne se sentent pas « fliqués » ? Comment prouver à mes employés que seules des données professionnelles sont collectées ?

Un commercial : Puis-je me faire licencier pour avoir utiliser mon véhicule de fonction à des fins personnelles ? Qu'en est-il de ma liberté de déplacement ?

La CNIL : Le dispositif n'est-il pas disproportionné ?

Contexte

L'étude a tout d'abord consisté à décrire le contexte, c'est-à-dire le traitement (sa finalité, son fonctionnement, ses enjeux), les données à caractère personnel , les supports sur lesquels elles reposent, les sources de risques et les références à considérer (lois, règlements, procédures...).

[1] Lorsqu'on parle de géolocalisation il serait plus juste de parler de "chronogéolocalisation". Ce qui est recherché n'est pas seulement où était la personne mais où était la personne tel jour à telle heure. Si elle n'est pas forcément recherchée en temps réel, il s'agit bien d'un suivi dans le temps et dans l'espace des déplacements (traces).

[2] On rappelle qu'il est interdit de géolocaliser un employé disposant de manière certaine d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP...).

Le traitement a pour finalité d'optimiser les itinéraires des commerciaux dans le cadre de leurs tournées, afin de réduire leur longueur et leur coût en carburant. Fonctionnellement, il comprend la planification des visites de clients et prospects par les commerciaux, le suivi du parcours de leurs véhicules et la recherche d'optimisations. Il doit donc permettre d'étudier les parcours de chaque commercial et de fournir des statistiques exploitables concernant l'ensemble des commerciaux pour mesurer l'atteinte des objectifs. Une finalité accessoire est d'assurer le suivi du temps de travail des commerciaux, qui ne peut être réalisé par d'autres moyens. Le principal enjeu réside dans l'augmentation des profits (possibilité de réaliser plus de visites et donc plus de ventes, réalisation d'économies en termes de carburant).

S'agissant des données à caractère personnel, ce sont les données de géolocalisation associées à chaque véhicule, lui-même affecté à un commercial.

Concernant les supports, il est prévu que le traitement repose sur un boîtier GPS embarqué dans les véhicules. Ce boîtier communiquerait par GSM avec un serveur hébergé chez un prestataire, qui stockerait également les données collectées dans une base de données. On note que le boîtier lui-même peut stocker temporairement des données (quelques jours au maximum) pour palier aux soucis de captation du réseau (tunnel, zone peu couverte) ou aux soucis de sur-taxation de la communication (zones frontalières). L'employeur accèderait à une application du prestataire via Internet, afin de gérer le lien entre les véhicules et les commerciaux, de paramétrer le boîtier (horaires, alertes sur zone géographique…) et de visualiser les données. Des tableaux de bord lui seraient envoyés une fois par mois par courrier électronique.

Mesure existantes identifiées

L'accès à l'application web du prestataire (et donc à la base de données) serait contrôlé par un identifiant et un mot de passe. Les processus légaux ne sont pas encore fixés. L'étude devra justement contribuer à les définir.

Dans ce cadre, les principales références à considérer sont les suivantes :

- la [Fiche-Geoloc] et la [NS51] ;
- la fiche n°10 du [Guide-Employeur] et la [Fiche-GSM-GPS] ;
- le Code du travail (proportionnalité, consultation des instances représentatives…) ;
- le Code de la route (limitations de vitesse…).

Dans le contexte étudié, les sources de risques les plus plausibles sont les suivantes :

- l'employeur ;
- le prestataire (en tant qu'exploitant/administrateur) ;
- les commerciaux ;
- des concurrents de l'entreprise ;
- les tiers intervenant sur les véhicules (installateur, garagiste…) ;
- les forces de l'ordre.

Atelier 1 : Cadrage et socle de sécurité

Définition du périmètre métier et technique

Mission	Dénomination de la valeur métier	Description	Entité ou Personne responsable	Dénomination du/des biens supports associés	Description	Entité ou Personne responsable

Identification des événements redoutés

Valeur métier	Événement redouté	Impacts	Gravité

Délimitation du socle de sécurité

Type de référentiel	Nom du référentiel	État d'application	Écarts	Justification des écarts

Atelier 2 : Sources de risques

Identification des couples *sources de risques* (SR) / *objectifs visés* (OV)

Sources de risque	Objecitifs visés

Évaluation des couples SR / OV

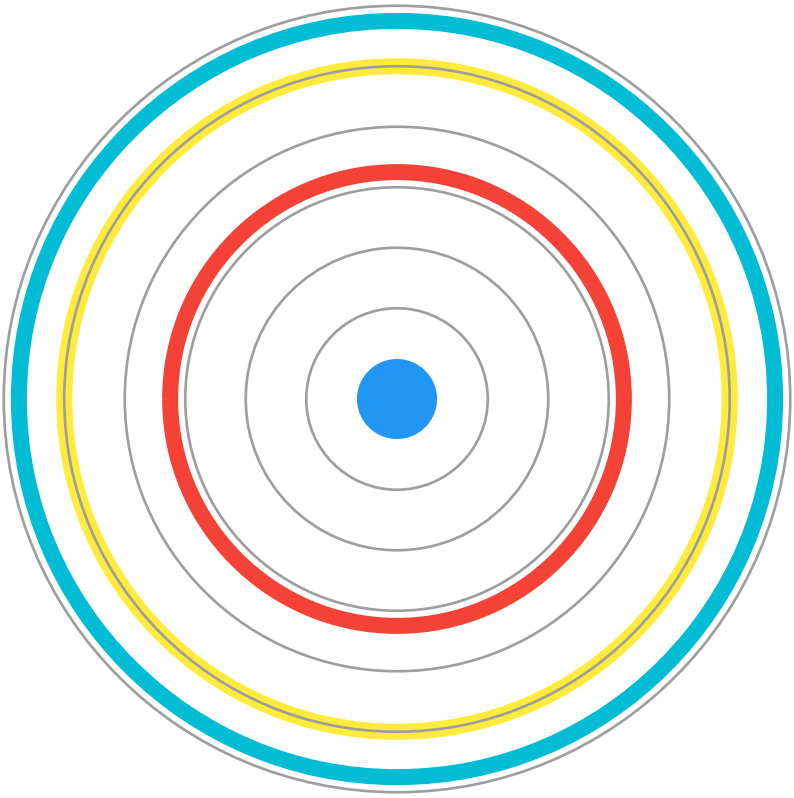
Sources de risque	Objectifs visés	Motivation	Ressources	Activité	Pertinence

Sélection des couples SR / OV jugés prioritaires

Atelier 3 : Scénarios stratégiques

Cartographie de menace numérique de l'écosystème et sélectionner les parties prenantes critiques

Catégorie	Partie prenante



Élaboration des scénarios stratégiques

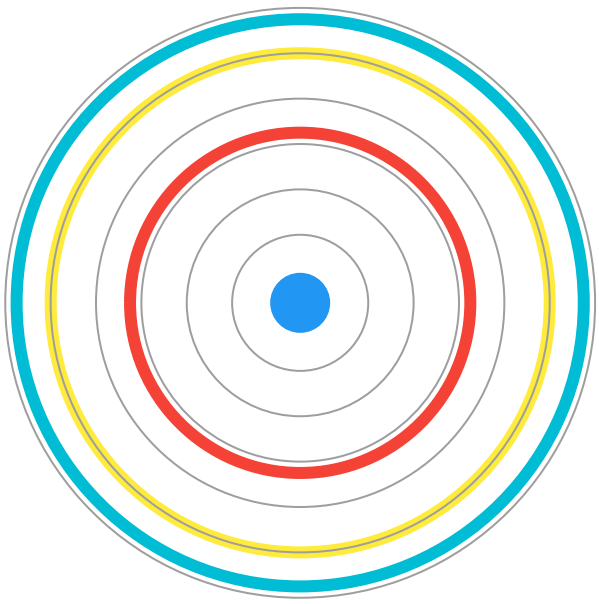
Synthèse

Sources de risque	Objectifs visés	Chemins d'attaque stratégique	Gravité

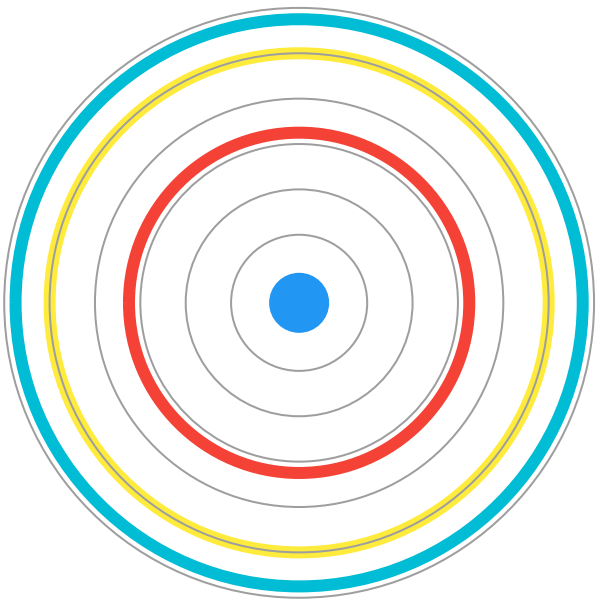
Définition des mesures de sécurité sur l'écosystème

Partie prenante	Chemins d'attaque stratégique	Mesures de sécurité	Menace Initiale	Menace Résiduelle

Initial



Résiduel



Atelier 4 : Scénarios opérationnels

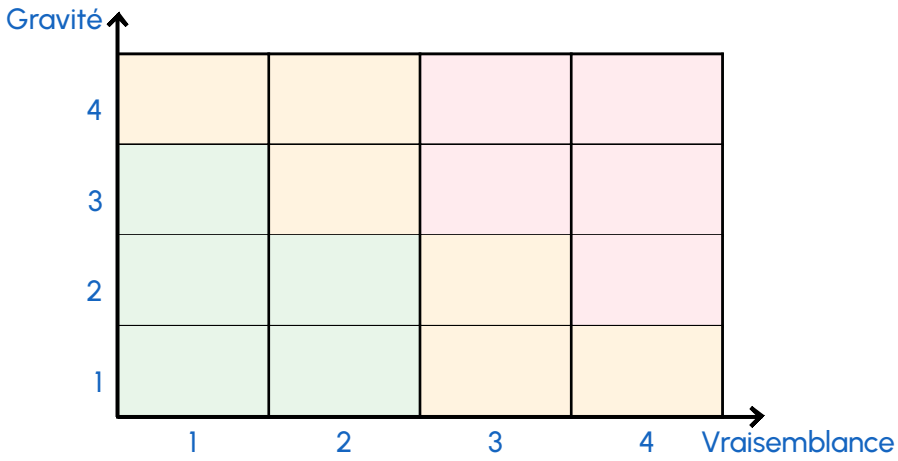
Élaboration des scénarios opérationnels

Évaluation de leur vraisamblance

Chemins d'attaque stratégiques (associés aux scénarios opérationnels)	Vraisemblance globale

Atelier 5 : Traitement du risque

Synthèse des scénarios de risque



Scénarios de risques

Définition de la stratégie de traitement du risque et des mesures de sécurité

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Gouvernance						
Protection						
Défense						
Résilience						