escrypt
SECURITY. TRUST. SUCCESS.

DÉTECTION & PRÉVENTION DES INTRUSIONS

Détection des attaques, application d'une politique et analyse en temps réel

Les solutions de sécurité intégrées constituent le seul moyen de protéger efficacement les véhicules connectés contre les cyberattaques. Elles doivent prendre en compte tous les scénarios de risque envisageables et susceptibles de survenir durant l'ensemble du cycle de vie du véhicule. Il est donc essentiel de disposer à tout moment d'une bonne vue d'ensemble des conditions de sécurité réelles des véhicules en circulation.

Détection en temps réel d'une grande fiabilité et application d'une politique de communication

La solution IDPS (Intrusion Detection and Prevention solution) développée par ESCRYPT offre une protection fiable contre les cyberattaques menées sur des véhicules en clientèle.

CycurIDS, le composant central de cette solution clé en main, détecte toute anomalie au sein de la communication à bord du véhicule. Il se base pour ce faire d'une part sur des schémas d'attaque connus, et d'autre part sur des comparaisons entre le comportement actuel en termes de communication et le comportement prévu. CycurIDS permet ainsi une détection performante en temps réel, empêchant qu'une communication malveillante ne puisse atteindre les systèmes critiques pour la sécurité du véhicule sans être détectée.

CycurGATE, le pare-feu pour différentes technologies de réseau embarquées (CAN, Ethernet), s'intègre aisément dans les systèmes existants. Il bloque les tentatives d'envoi de commandes à des calculateurs individuels ou à l'ensemble du réseau, sur la base de l'application d'une politique de communication, c'est-à-dire d'une approche fondée sur une liste blanche (ne permettant que les flux de communication explicitement décrits) modifiée par une liste noire (pour éviter les attaques connues). A titre de prévention des intrusions, l'ensemble de règles pertinentes du pare-feu peut être mis à jour avec de nouvelles règles et des règles révisées.

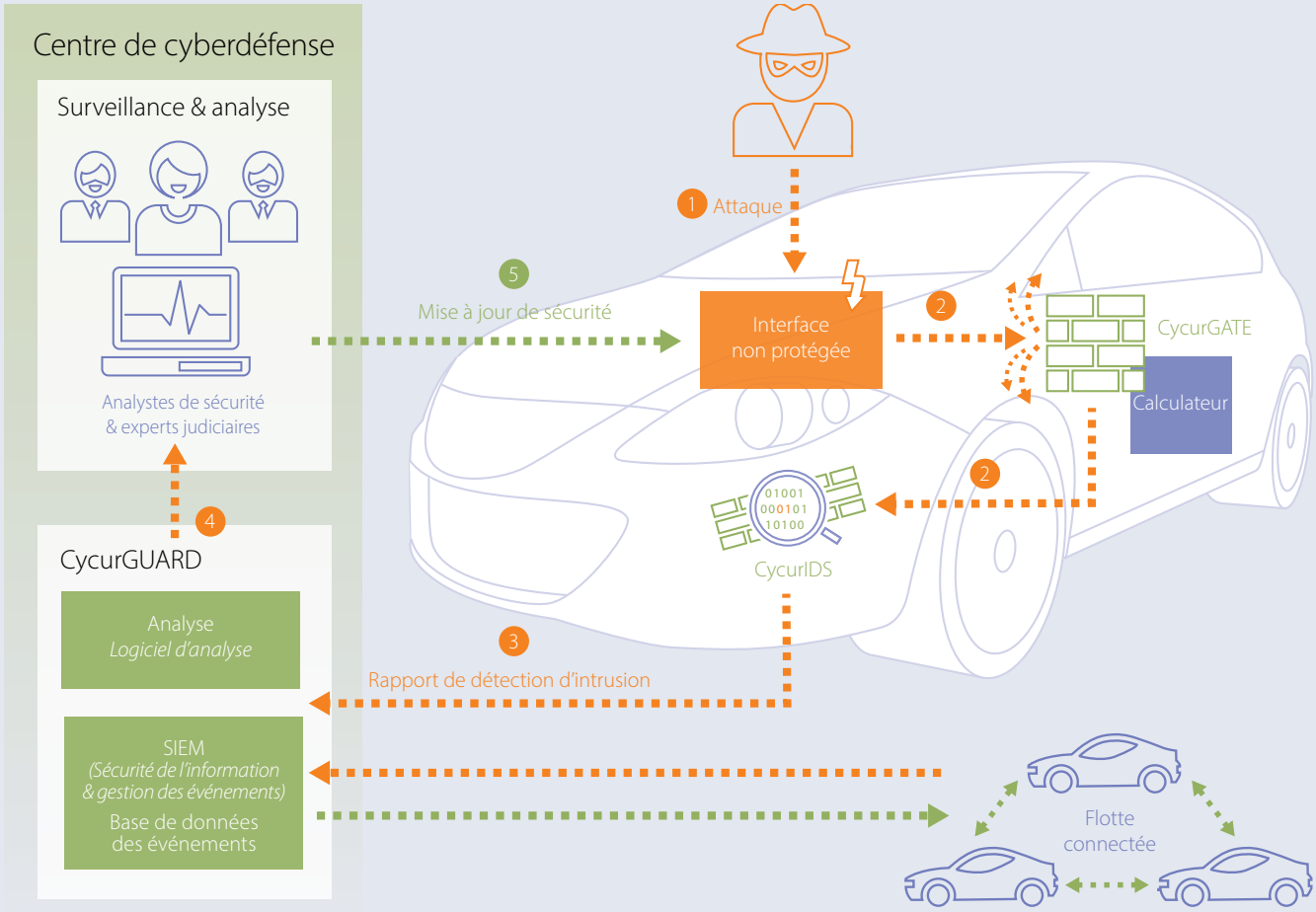
Backend de cyberdéfense – big data pour la sécurité automobile

Tandis que CycurIDS perçoit les événements liés à la sécurité qui affectent une seule voiture, **CycurGUARD** permet d'analyser des données en provenance de l'ensemble de votre flotte connectée, afin d'identifier les nouvelles menaces. Avec ce produit de surveillance backend basé sur des technologies d'analyse du big data, ESCRYPT propose une solution intégrée de collecte et d'analyse des rapports d'anomalies des véhicules en circulation. CycurGUARD identifie de manière fiable les menaces graves en se référant à une vaste base de données de modèles d'attaques connus, qui est enrichie en permanence. L'utilisation de rapports ad hoc ou prédéfinis permet d'évaluer la sécurité et la sûreté de la flotte connectée, d'identifier les changements, de concentrer les ressources sur les points problématiques et d'anticiper l'évolution des menaces.

ESCRYPT 04/2019

escrypt
SECURITY. TRUST. SUCCESS.

Détection & prévention des intrusions



Les avantages dont vous bénéficiez

- Solution logicielle prête à l'emploi pour la détection d'attaques sur les architectures E/E actuelles
- Identification fiable et en temps réel des attaques véritables
- Autorise une défense à point nommé contre les attaques, évitant ainsi de coûteux rappels
- Evite les recours en garantie
- Respecte les obligations légales et réglementaires en matière de sécurité des données à bord du véhicule
- Offre une bonne vue d'ensemble de la sécurité des différents modèles de véhicules en clientèle
- Permet un développement ciblé, et donc plus efficace, des concepts de sécurité

Synthèse de nos services

- Conseil en solutions
- Conception de solutions de sécurité
- Mise en œuvre personnalisée (process, logiciels, matériel)
- Services de sécurité gérés et maintenance
- Formation, support et services de certification