THALES

Thales au cœur de la cyber sécurité des véhicules

RETOUR D'EXPÉRIENCE SÉCURITÉ VÉHICULE CONNECTÉ

LAURENT SUDARSKIS
DIRECTEUR DE MISSION- CONSEIL EN CYBER SÉCURITÉ

LE 18 OCTOBRE 2018

Ordre du jour

- Thales, marchés & chiffres
- Conseil Cyber & expérience auprès des OEM
- Cyber sécurité et véhicule connecté
- Quels challenges pour la Cyber sécurité ?

THALES Nos marchés

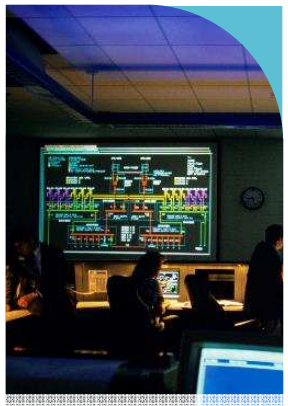
MARCHÉS DUAUX


AÉRONAUTIQUE


ESPACE


TRANSPORT TERRESTRE


DÉFENSE


SÉCURITÉ

UN PARTENAIRE DE CONFIANCE POUR UN MONDE PLUS SÛR

Salariés

64 000

Une présence mondiale

56

14.9 **milliards d'euros**

THALES Conseil en Cybersécurité

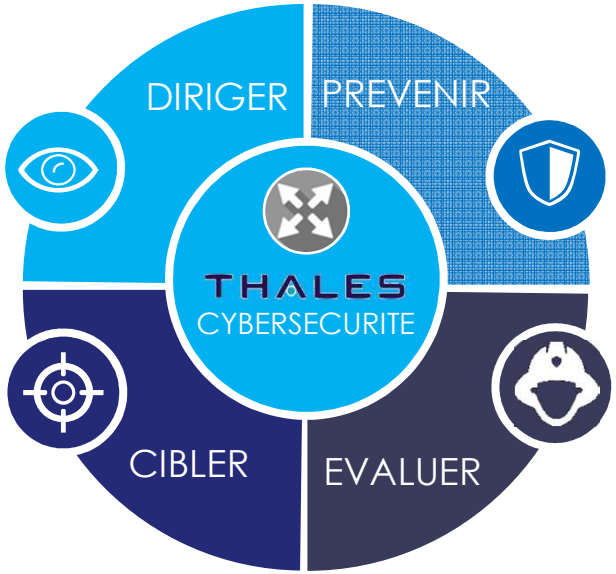
Notre propositions de valeur :

Audit fonctionnel et gouvernance

- Audit/accompagnement RGPD/LPM
- Audits ISO 2700x et RGS
- Accompagnement SMSI
- Gestion de crise
- Analyse de risques
- Cyber Rating

Investigation numérique, rétro-ingénierie et tests d'intrusion

- Réponse sur incidents
- Recherche de compromission
- Rétro-ingénierie
- Tests d'intrusion, Red Team
- Scans de vulnérabilités
- Audits techniques (code, conf.)



Architectures des infrastructures & Applications

- Assistance à la conception d'architectures sécurisées
- Audits d'architecture
- Diagnostic cyber sécurité des systèmes industriels
- Accompagnement à la migration dans le cloud
- Homologations de sécurité

Evaluation Sécurité et Fiabilité

- Laboratoire hardware (CESTI)
- Laboratoire CSPN
- Laboratoire d'analyse de fiabilité (CNES)

Nos implantations : Paris, Toulouse, Lyon, Rennes

Notre expérience auprès des OEM

Assureurs / Gestionnaire de flotte /Entreprises commerciales..

Opérateurs Telecom

Fournisseurs de services

Expertise sécurité architectures Services & Cloud

Expertise sécurité architecture embarquée

Audit cyber sécurité des équipementiers

Validation Cyber & audit-TI ECU embarqués

Gouvernance & Pilotage

Analyse de risque cyber dédiée embarqué

Equipementiers / Tiers 1

Ordre du jour

Cyber sécurité et véhicule connecté : quel contexte ?

Contexte

➢ Market trends

2014	2030
Autonomous Drive	
0-1%	15%
Connected Cars	
30%	100%
Electric Vehicle	
1%	25%

Les constructeurs vivent une véritable (r)évolution de leur business model

- Le passage du thermique à l'électrique
- L'explosion de la connectivité & de l'offre de services (Car sharing …)
- L'émergence du véhicule autonome & des nouveaux usages associés (Car As a Service, Robot Vehicule...)
- Le véhicule se positionne au cœur d'un écosystème d'IOT (Smart city, V2X..)

- **Les constructeurs se définissent de + en + comme des acteurs et des fournisseurs de services de mobilité**

- **La maitrise et la protection des données & des services deviennent des enjeux stratégiques**

Contexte

- **By 2020 connected vehicles making the automotive industry a contributor of 33% of all cellular devices**
- **OEMs now learning security lessons software companies learned 2 decades ago !! (Charlie Miller & Chris Valasek)**

La cyber sécurité au cœur des véhicules

- Les surfaces d'attaques se multiplient : IVC, IVI, OBD, connexions Off/On-board, AppStore, V2X ..
  - 125 ECU & +/- 100 M de lignes de code par véhicule connecté
  - 10-15 erreurs/1 000 lignes de code → autant de portes ouvertes à exploiter !!
- L'externalisation des services multiplie les acteurs et les interfaces
- Les motivations pour des attaquants sont réelles
- Les véhicules sont déjà des cibles (Jeep, Nissan, BMW, Tesla..)
- Les attaquants vont se professionnaliser (Cf IT/IS)
- L'avantage technologique d'un temps n'est pas durable

- **Nécessité d'assurer la cohabitation Safety / Cyber sécurité / Privacy**

Ordre du jour

Quels challenges pour la Cyber sécurité ?

Les challenges (1/3)

La sécurité un enjeu transverse au-delà des organisations qui implique tous les acteurs (On/Off Board, Safety, Tiers1…)

- Favoriser **une approche** de la sécurité **E2E + by Design** (*cf innovation*) ;
- **Sensibiliser/former** à la Cyber/privacy les acteurs impliqués dans le cycle de vie du véhicule ;
- Prendre en compte le périmètre de l'embarqué au sein de la PSSI ;

- **Synchroniser Safety & Sécurité** (*ex : étendre les critères des analyses de risques et intégrer un critère Safety*) ;
- Participer aux **travaux de normalisation / règlementation** (*ISO/SAE standard on cybersecurity…*) ;
- **Aligner les roadmaps** Cyber avec les Tiers1 et les fondeurs ;

Les challenges (2/3)

Faire cohabiter au sein du véhicule différents niveaux de sensibilité & d'exposition à la menace

- Assurer la **sécurité des fonctions critiques** via une approche de **défense en profondeur** ;
- **Limiter** au maximum **la surface d'attaque des fonctions Safety** (*allocation des fonctions par niveau de confiance, gestion des moindres privilèges*) ;
- Privilégier **une approche système** / limiter les ECU / exposer des API ;

- Définir les **mesures de sécurité** des architectures embarquées (à venir *nouveau réseau, gestion différentes des ressources ECU, nouvelle architecture logicielle…*) :
  - Diminution des ECU, plate-forme logicielle multi-OS, Ethernet, CAN-IP, virtualisation & hyperviseur ;
  - Secure boot, authentification et chiffrement des logiciels, contrôle des flux d'information, Secure storage, IPS/IDS embarquées…

Les challenges (3/3)

Gérer le cycle de vie de la sécurité de la conception à la vie série (y compris le retrait)

- **Maitriser** dans le temps **la gestion de configuration** + gestion inventaire ;
- **Mettre à jour le niveau de sécurité** à distance (ex : *FOTA*) ;
- **Maintenir la vigilance** vis-à-vis du risque Cyber :
  - Poursuivre le déploiement des capacités de validation cyber des ECU ;
  - Se doter de capacités de veille, de détection, d'investigation et de réaction face aux attaques (*notion de SOC véhicule*) ;
  - Ouvrir les architectures à la communauté sécurité (*Bug Bounty..*)

Merci de votre attention