




*Cybersécurité de la chaîne d'approvisionnement des véhicules
au Canada*

AJ Khan, directeur général

 ajkhan@cyberstrategiez.com

 +1 (289) 936-9894

<https://vehiqilla.com/>

AJ KHAN



- ▶ Plus de 20 ans d'expérience dans la cybersécurité et les domaines associés
- ▶ Innovation en matière de cybersécurité
- ▶ Implication dans la cybersécurité automobile depuis 2017
- ▶ Coprésident de APMA CSC 2019 – 2021
- ▶ Création de Vehiqilla en juin 2020
- ▶ Président du Global Syndicate for Mobility Cybersecurity
- ▶ Contributeur



<https://vehiqilla.com/>

CYBER SÉCURITÉ UN DÉFI MONDIAL POUR L'INDUSTRIE AUTOMOBILE

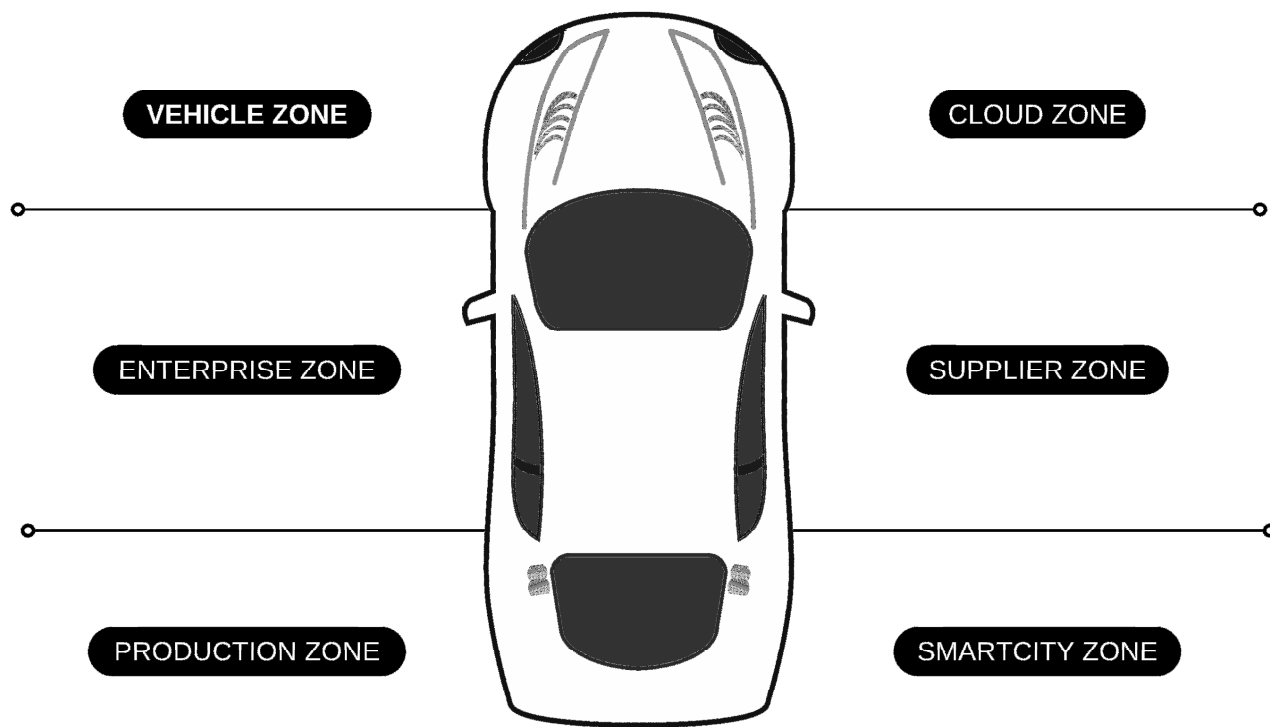


Cybermenaces plus importantes dans l'industrie 4.0

Différence dans la cybersécurité des TI et automobile

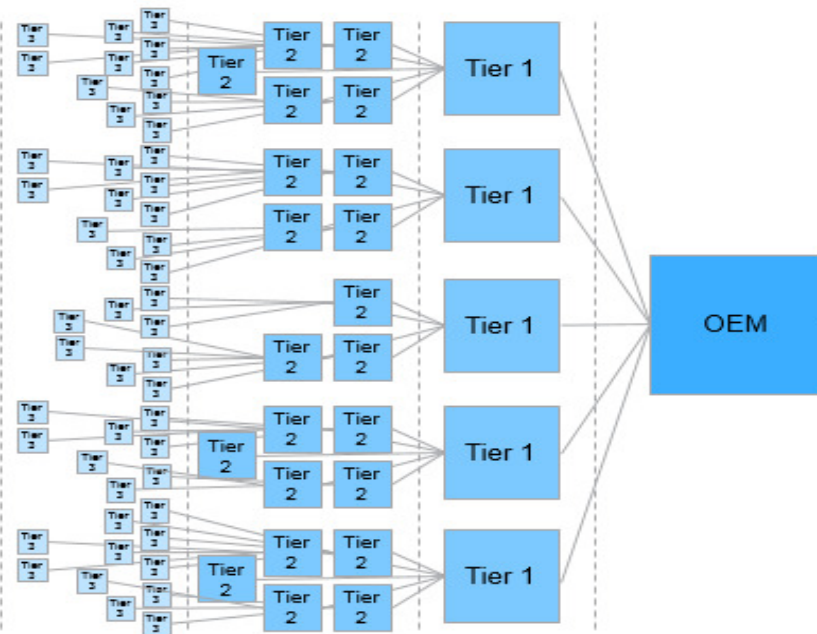
Cybersécurité de la chaîne d'approvisionnement en véhicules

<https://vehiqilla.com/>



CYBERSÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT EN VÉHICULES

\$0.66 Trillion \$1.1 Trillion \$1.82 Trillion \$3.03 Trillion



Normes et réglementations mondiales en matière de cybersécurité automobile

Logiciels automobiles Supply Chain Cybersecurity (Chaîne d'approvisionnement Cybersécurité)

<https://vehiqilla.com/>

C-SCRM (Gestion des risques de la chaîne d'approvisionnement en matière de cybersécurité) appliquée à la chaîne d'approvisionnement des véhicules

État actuel de la cybersécurité dans le réseau canadien de la chaîne d'approvisionnement

C-SCRM (GESTION DES RISQUES DE LA CHAÎNE D'APPROVISIONNEMENT EN MATIÈRE DE CYBERSÉCURITÉ) APPLIQUÉE À LA CHAÎNE D'APPROVISIONNEMENT DES VÉHICULES



Gestion des incidents



Planification de la continuité des activités (PCA) des fournisseurs



Résilience de la fabrication et des essais



Résilience du produit



**LA
CYBERGESTION
DES RISQUES
VISANT LA
CHAÎNE
D'APPROVISION-
NEMENT
AUTOMOBILE
AU CANADA**

Le secteur canadien de l'automobile est conscient des problèmes de sécurité auxquels il est exposé en raison de l'apparition de nouvelles cybermenaces.

La mise en œuvre d'un programme de cybergestion des risques visant la chaîne d'approvisionnement automobile permettra de mettre en place les contrôles nécessaires pour atténuer les risques posés par ces nouvelles menaces

<https://vehiqilla.com/>

ISO 21434, UN R155, R156 ET CYBERSÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT EN VÉHICULES

- La **clause 5 « Gestion de la cybersécurité de l'organisation »** définit la gestion de la cybersécurité de l'organisation et spécifie les politiques, les règles et les processus de cybersécurité de l'organisation.
- La **clause 7 « Activités de cybersécurité réparties »** s'applique si les responsabilités des activités de cybersécurité pour un article ou un composant sont réparties.
- Le règlement **R155** stipule que les auditeurs confirment que les constructeurs automobiles ont fait tous les efforts possibles pour « Recueillir et vérifier les informations requises au titre du présent règlement tout au long de la chaîne d'approvisionnement afin de démontrer que les risques liés aux fournisseurs sont repérés et gérés ».
- Le règlement **R156** demande spécifiquement aux fournisseurs de fournir suffisamment d'informations pour garantir que les contrôles de validation spécifiques décrits dans le règlement puissent être effectués pour toute mise à jour logicielle envoyée au véhicule.

LOGICIELS AUTOMOBILES SUPPLY CHAIN CYBERSECURITY (CHAÎNE D'APPROVISIONNEMENT CYBERSÉCURITÉ)

Cyberrisques

- Des millions de lignes de code dans un véhicule moderne provenant de nombreux fournisseurs différents
- Les mises à jour par voie aérienne (VA) sont devenues une pratique courante dans l'industrie.

Solutions

- Exigences en matière de nomenclature logicielle (SBOM)
- Cybersurveillance en temps réel du véhicule et des données qui circulent dans le nuage

<https://vehiqilla.com/>

PRINCIPAUX DÉFIS

- Compréhension limitée des facilitateurs commerciaux de la cybersécurité
- Absence de mise en œuvre des normes et cadres mondiaux de cybersécurité automobile
- Manque de PME dans le domaine de la cybersécurité automobile
- Manque de gestion du risque de la chaîne de fournisseurs cybernétiques (C-SCRM)
- Collaboration et partage d'informations pour les initiatives de cybersécurité

<https://vehiqilla.com/>

RECOMMANDATIONS POUR L'INDUSTRIE

Élaboration de PME dans le
domaine de la cybersécurité
automobile

Échange de l'information sur la
cybersécurité à l'échelle de
l'industrie

- Centre canadien pour la cybersécurité
- Centre d'échange de l'information et du renseignement automobiles (Auto-ISAC)
- Échange canadien de menaces cybernétiques (ECMC)

<https://vehiqilla.com/>

RECOMMANDATIONS SUR LA C-SCRM POUR L'INDUSTRIE AUTOMOBILE

Pratiques exemplaires en matière de gouvernance de la cybersécurité automobile

- Veiller à ce que la cybersécurité fasse partie de l'énoncé de mission de l'organisation.
- Veiller à ce qu'un officier principal de la sécurité de l'information (OPSI) soit chargé de la gestion des cyberrisques dans l'organisation.
- S'assurer qu'un système de gestion de la cybersécurité (SGC) a été mis en place dans l'organisation.
- Veiller à ce que l'organisation soit conforme aux normes et réglementations pertinentes en matière de cybercriminalité, notamment la norme ISO 21434 et les règlements R155 et R156 du WP.29 de la CEE-ONU.
- Veiller à ce que la « sécurité par la conception » soit mise en œuvre dans l'organisation.

RECOMMANDATIONS SUR LA C-SCRM POUR L'INDUSTRIE AUTOMOBILE

Culture et état d'esprit en matière de cybersécurité

- Instaurer une culture de la cybersécurité dans l'organisation en encourageant une approche proactive de la cybersécurité au sein du personnel.
- Veiller à ce que la « sécurité par la conception » soit mise en œuvre dans l'organisation.
- Veiller à ce que les pratiques exemplaires de « création de logiciels sécurisés » soient suivies dans l'organisation.

RECOMMANDATIONS SUR LA C-SCRM POUR L'INDUSTRIE AUTOMOBILE

Programme de gestion des risques de la chaîne d'approvisionnement cybernétique (C-SCRM)

- S'assurer que la C-SCRM fait partie intégrante de la stratégie de gestion des risques de l'organisation.
- Propriété de la C-SCRM.
- Politique de la C-SCRM de haut niveau qui met clairement en évidence les exigences de l'organisation en matière de cybersécurité de la chaîne d'approvisionnement en véhicules.
- Les intervenants (p. ex., les services juridiques, les entreprises, les RH, les finances, les TI de l'entreprise, la technologie des opérations, la gestion des programmes, le développement des produits, la gestion des risques, les acquisitions/les achats, la logistique de la chaîne d'approvisionnement, etc.).

RECOMMANDATIONS SUR LA C-SCRM POUR L'INDUSTRIE AUTOMOBILE

C-SCRM et intégration des fournisseurs

- La cybersécurité est intégrée dans les obligations contractuelles.
- Tout fournisseur finalisé est intégré au cadre de la C-SCRM de l'organisation.
- Des accords d'interface avec les fournisseurs en matière de cybersécurité sont conclus avec tous les fournisseurs.

RECOMMANDATIONS SUR LA C-SCRM POUR L'INDUSTRIE AUTOMOBILE

Évaluations des risques de cybersécurité des fournisseurs

- Évaluation des risques de cybersécurité des fournisseurs.
 - au moment de l'intégration
 - sur une base périodique
- Définir un ensemble minimal de contrôles de base de la sécurité des informations que tout fournisseur de l'organisation doit respecter une fois qu'il est intégré au cadre de la C-SCRM de l'organisation.

RECOMMANDATIONS SUR LA C-SCRM POUR L'INDUSTRIE AUTOMOBILE

Gestion des incidents de cybersécurité

- Incidents de piratage, de pandémies, de catastrophes naturelles, etc.
- Programme de gestion des cyberincidents.

OUTILS D'ÉVALUATION DE LA CYBERGESTION DES RISQUES VISANT LA CHAÎNE D'APPROVISIONNEMENT AUTOMOBILE

Axé sur 6 catégories

Cybersécurité de l'organisation

Normes et cadres

Gestion des risques de la chaîne d'approvisionnement cybernétique (C-SCRM)

Cybersécurité des produits

Gestion des incidents

Culture de la cybersécurité

<https://vehiqilla.com/>

AVANTAGES DE LA CYBERGESTION DES RISQUES VISANT LA CHAÎNE D'APPROVISION NEMENT AUTOMOBILE



Aide les fabricants à connaître le profil de cybersécurité de leur fournisseur.



Permet aux fabricants de prendre de meilleures décisions en matière de produits.



Les fournisseurs peuvent renforcer leur cybercrédibilité auprès des fabricants.



Une meilleure visibilité de la force et de la faiblesse du profil cybernétique de l'organisation du fournisseur



Augmente la motivation des fournisseurs.



Contribue à la détermination et à l'analyse des exigences de sécurité.

<https://vehiqilla.com/>

MERCI!



ajkhan@cyberstrategiez.com



+1 (289) 936-9894



**4510, Rhodes Drive,
bureau 510, Windsor (Ontario)
N8W 5K5**

<https://vehiqilla.com/>

