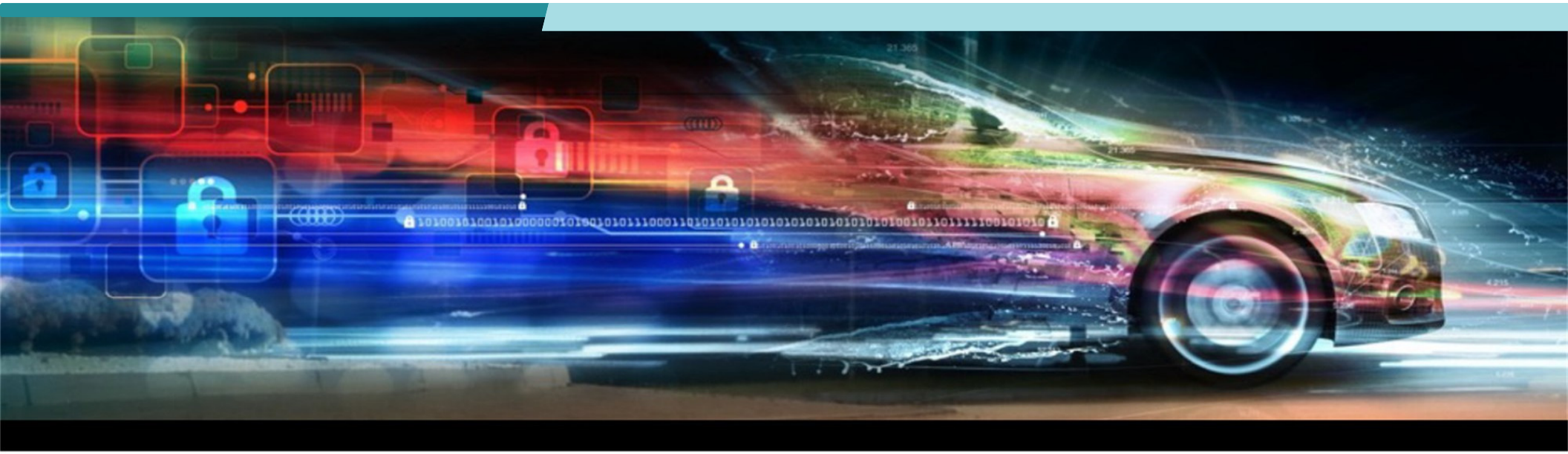


Atelier virtuel sur la sécurité informatique des véhicules de Transports Canada

Centre de partage et d'analyse de l'information sur l'automobile (Auto-ISAC) : L'importance de la collaboration

Faye Francy, directrice générale d'Auto-ISAC

24 mars 2022
De 11 h 25 à 12 h (HE)

AUTO-ISAC
Automotive Information Sharing and Analysis Center

STRATÉGIE DE SÉCURITÉ INFORMATIQUE DES VÉHICULES DE TRANSPORTS CANADA

Objectifs et priorités prospectifs **en matière de sécurité informatique des véhicules** en vue de **renforcer** la **résilience informatique** du transport routier au Canada.

- ***Objectif 1 :*** **Intégrer les considérations relatives à la sécurité informatique des véhicules dans les cadres stratégiques et réglementaires**
- ***Objectif 2 :*** **Promouvoir la sensibilisation et favoriser une approche moderne et novatrice en matière de sécurité informatique des véhicules**
- ***Objectif 3 :*** **Aborder les enjeux émergents et adjacents dans le contexte de la sécurité informatique des véhicules**

La **nature complexe et interconnectée** de la sécurité informatique dans le secteur de l'automobile **exige une collaboration et une coopération** entre un large éventail d'intervenants, et Transports Canada (TC) continuera d'explorer les possibilités d'aborder le **risque de sécurité informatique** dans l'écosystème plus vaste de la technologie du transport routier.

Caractère juridique et réglementaire

En 1998, la DDP 63 a souligné que 90 % des infrastructures essentielles du pays appartiennent au secteur privé et sont exploitées par ce dernier.

On a demandé à chaque industrie de créer une organisation propre au secteur pour **partager de l'information sur les menaces physiques et cybernétiques, les vulnérabilités et les incidents.**

Aujourd'hui, il y a 24 ISAC qui jouent ce rôle.

Les ISAC permettent de partager de l'information fiable par l'entremise de cinq piliers :

Anonymat des présentations ● Partage de l'information authentifiée ● Piloté et exploité par l'industrie ● Limitation de l'utilisation des renseignements ● Conformité avec toutes les exigences juridiques et les lois antitrust des États-Unis.

Voici d'autres politiques habilitant les ISAC :

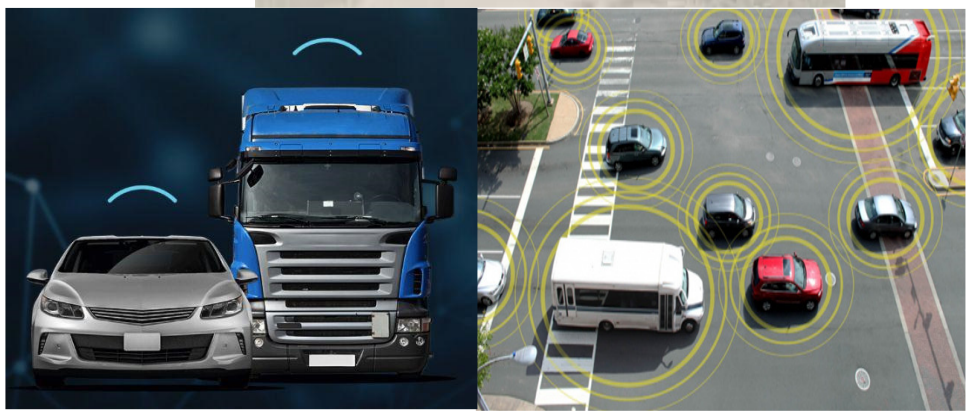
Directive sur les politiques de sécurité nationale (National Security Policy Directive) (2001)	**Initiative globale nationale de cybersécurité (Comprehensive National Cybersecurity Initiative)** (2008)	**Décret exécutif 13636 :** Amélioration de la cybersécurité des infrastructures essentielles (Improving Critical Infrastructure Cybersecurity) (2014)
Directive présidentielle 21 : Sécurité et résilience des infrastructures essentielles (Critical Infrastructure Security and Resilience) (2014)	**Décret exécutif 13691 :** Promouvoir le partage de l'information sur la sécurité informatique dans le secteur privé (Promoting Private Sector Cybersecurity Information Sharing) (2015)	***Cybersecurity Act of 2015*** (2015)

Changements importants dans le monde de l'automobile

Les véhicules connectés numériques offrent des gains d'efficacité opérationnelle, mais cet avantage présente des risques

Serviette de table

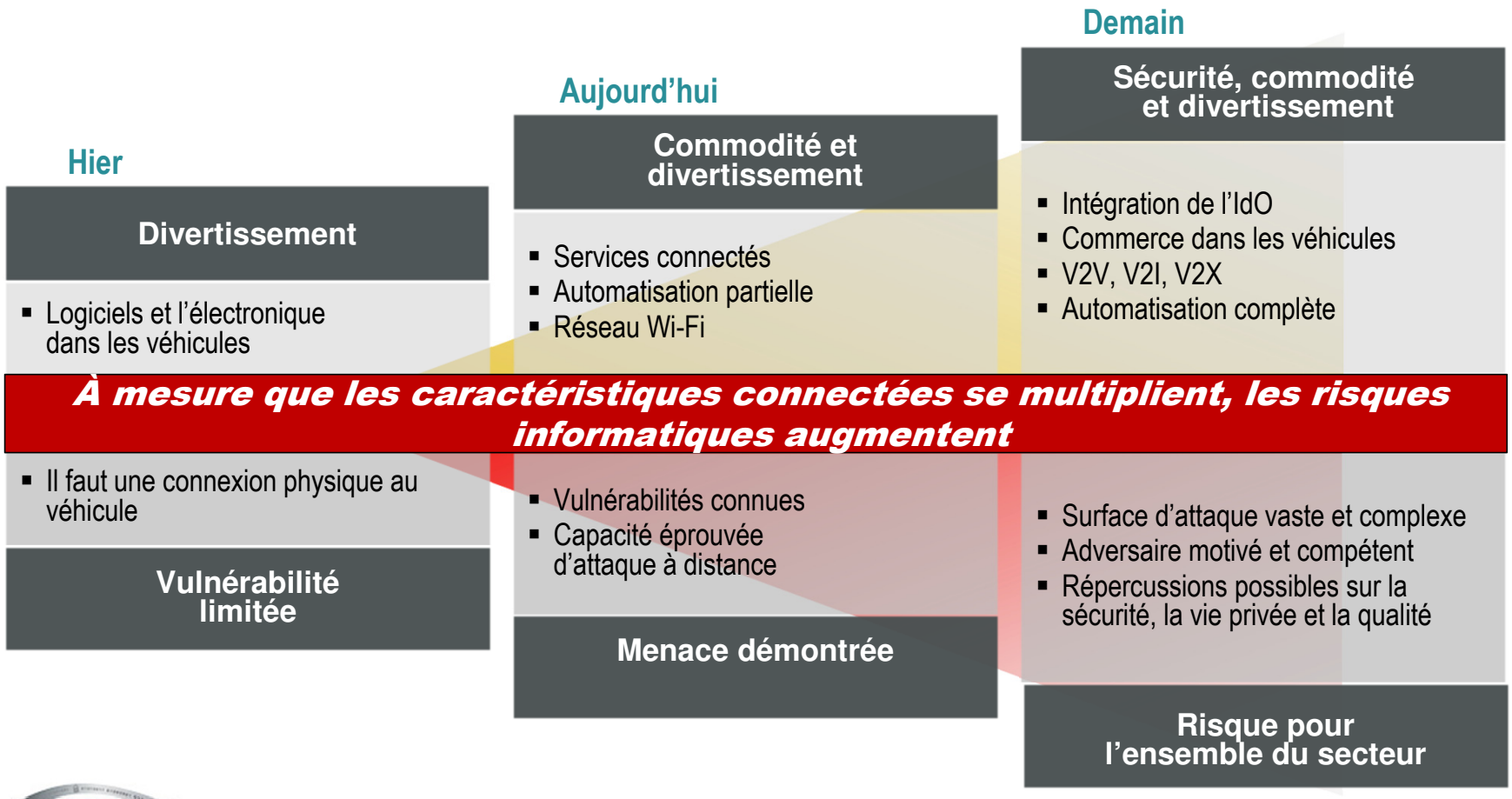
100 millions de lignes de code



- **Ère numérique**
  - ✓ Les clients exigent une connectivité
  - ✓ L'automatisation améliore l'efficacité
  - ✓ Vulnérabilités cybernétiques accrues pour les véhicules connectés
  - ✓ Les médias et les responsables de la surveillance au Congrès exigent des mesures réglementaires

- **Véhicules connectés intégrés aux systèmes des systèmes**
  - ✓ La connectivité accroît l'efficacité, mais aussi les risques
  - ✓ Les menaces informatiques et les vulnérabilités augmentent
  - ✓ Les réglementations et les normes en sont à différentes étapes
  - ✓ L'autonomie augmente : communications entre véhicules (V2V), communications véhicule-infrastructure (V2I), véhicule avec tout (V2X), etc.

La connectivité suppose un risque cybernétique



Sécurité informatique Auto-ISAC

Le véhicule connecté

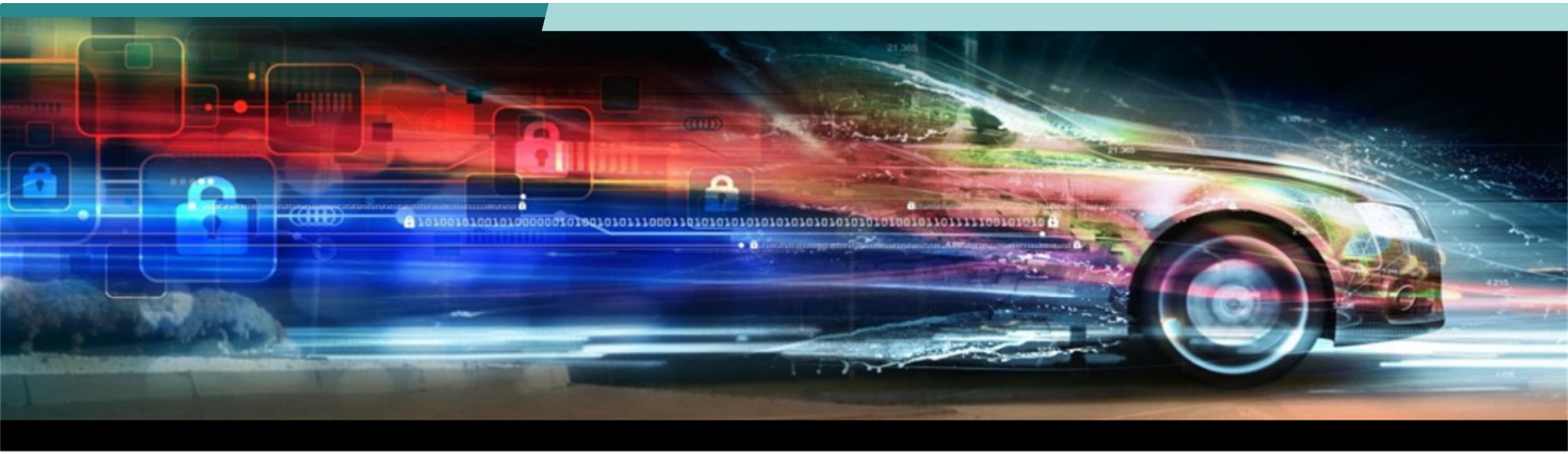
But

- Maintenir la confiance du public
- Réduire les risques et les coûts
- Offrir des renseignements opportuns et exploitables
- Améliorer les connaissances communes de la situation
- Résilience

Avantages

- Accès au renseignement et à l'analyse des menaces
- Surveillance détaillée des menaces
- Vue sectorielle et intersectorielle
- Partage de l'information sur la non-attribution
- Une seule voix

La sécurité informatique est la responsabilité de tous



Auto-ISAC

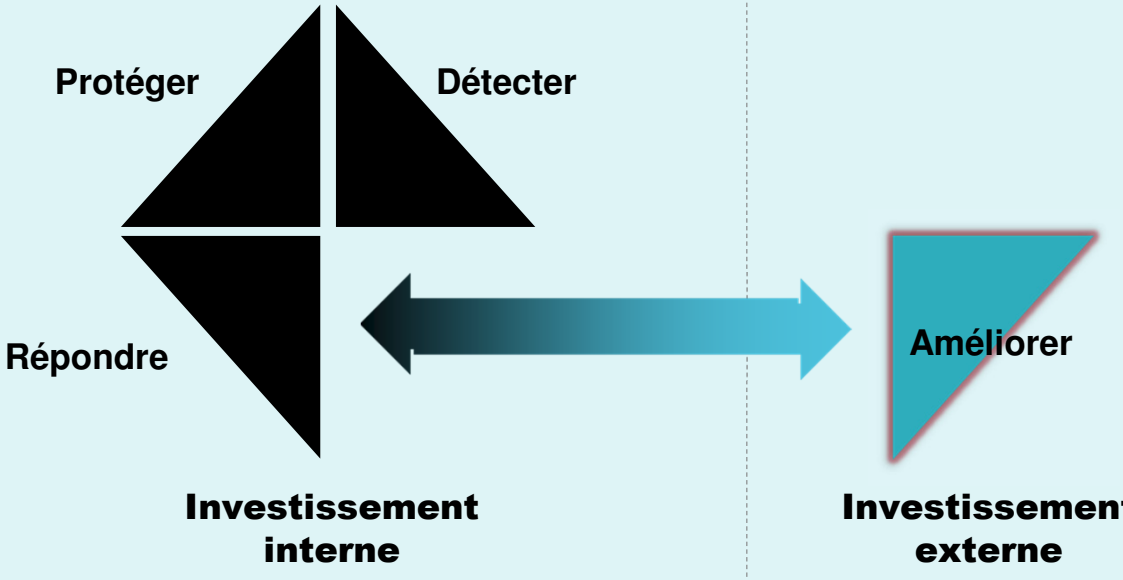
Que font les ISAC?

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Mission d'Auto-ISAC

Centres de partage et d'analyse de l'information (ISAC)

Les organisations doivent agir individuellement pour gérer les risques informatiques



La détection d'une entreprise est

de la prévention pour une autre entreprise

- Identifier plus tôt les menaces émergentes et les vulnérabilités
- Mettre en commun des ressources limitées pour mieux combattre un adversaire adaptatif
- Partager l'information sur l'incident pour agir plus rapidement
- Façonner de façon proactive les pratiques exemplaires à l'échelle de l'industrie
- Protéger la confiance globale à l'égard de l'innovation dans l'ensemble de l'industrie
- Renforcer la résilience à l'échelle du secteur

Auto-ISAC : *Point central de coordination et de communication en matière de sécurité informatique* pour l'industrie mondiale de l'automobile

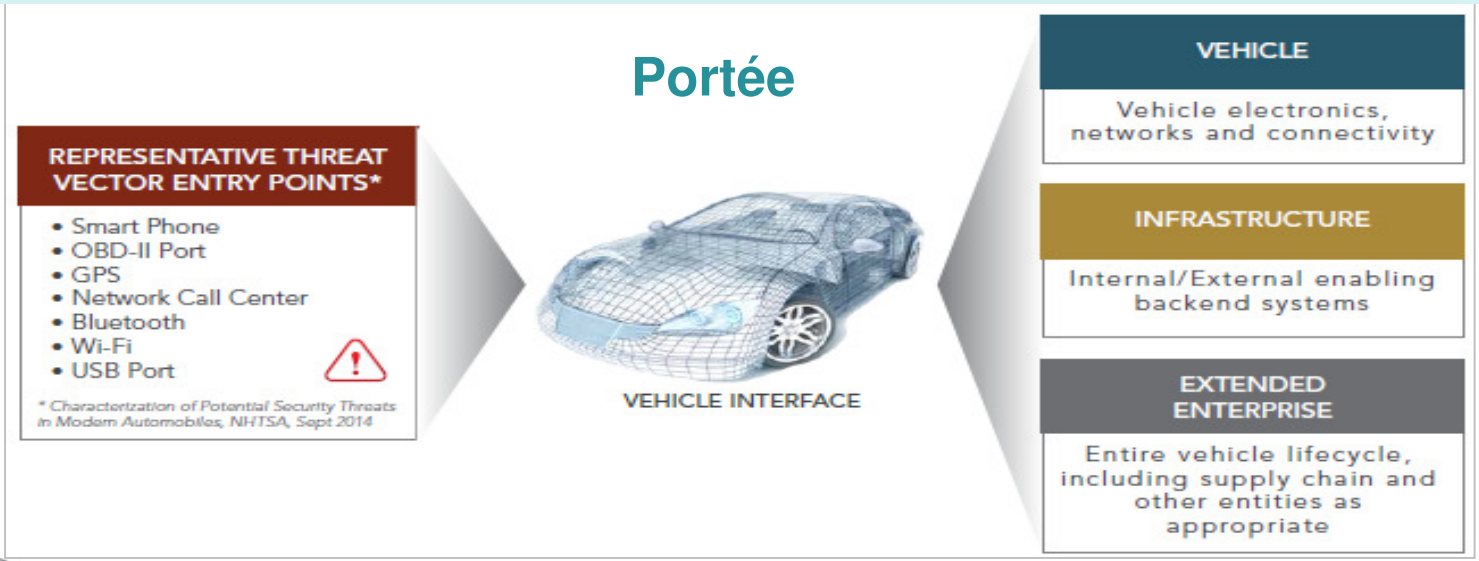
But

- Agir comme courtier d'information **impartial**.
- Accroître la **rapidité, la qualité et la quantité** de l'information échangée.
- Effectuer une **analyse** des menaces.
- Maintenir **l'agilité et la souplesse** nécessaires pour s'adapter aux changements (nouvelles menaces, tactiques, etc.).

Mission

Servir de **point central de coordination et de communication** pour l'industrie automobile mondiale par l'analyse et le partage de l'information fiable et opportune sur les menaces informatiques.

Portée



Auto-ISAC = Environnement d'apprentissage

➢ **Produits et évaluations analytiques**
- ✓ Collaboration et détection précoce | Externalisation ouverte
- ✓ Les meilleurs de l'industrie (membres!)

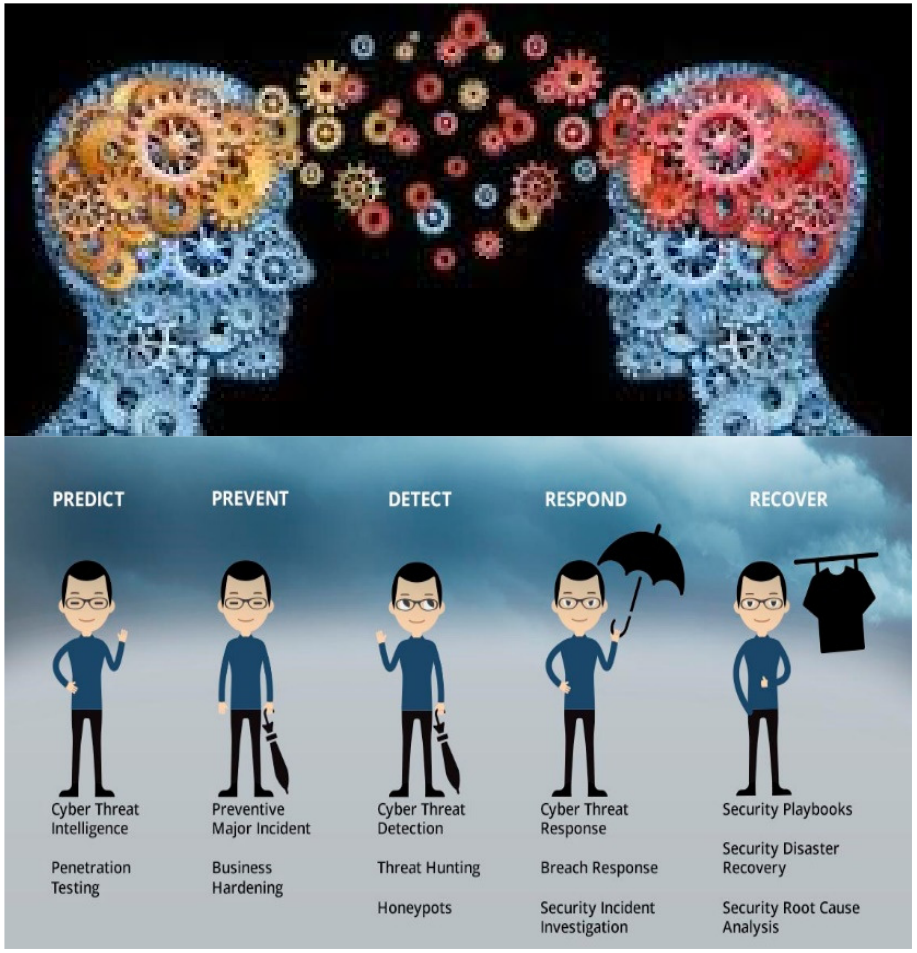
➢ **Exercices sur table (TTX)**
- ✓ Exercices sur table de la haute direction, TTX juridique
- ✓ Exercices sur table des analystes | Pratiques

➢ **Ateliers trimestriels**
- ✓ Engagement des analystes et des cadres en personne
- ✓ Webinaires – Partenariats stratégiques

➢ **Groupes de travail**
- ✓ Défis en temps réel axés sur les membres
- ✓ Élaborer des pratiques exemplaires | Membres – Enseignement – Membres

➢ **Comités permanents**
- ✓ Conseiller le Conseil sur les principaux projets
- ✓ Axé sur les membres | Produits de travail

➢ **Sommet annuel | Conférences téléphoniques communautaires**
- ✓ Membres, partenaires, fournisseurs et collectivité
- ✓ Secteur universitaire et chefs de file en sécurité informatique

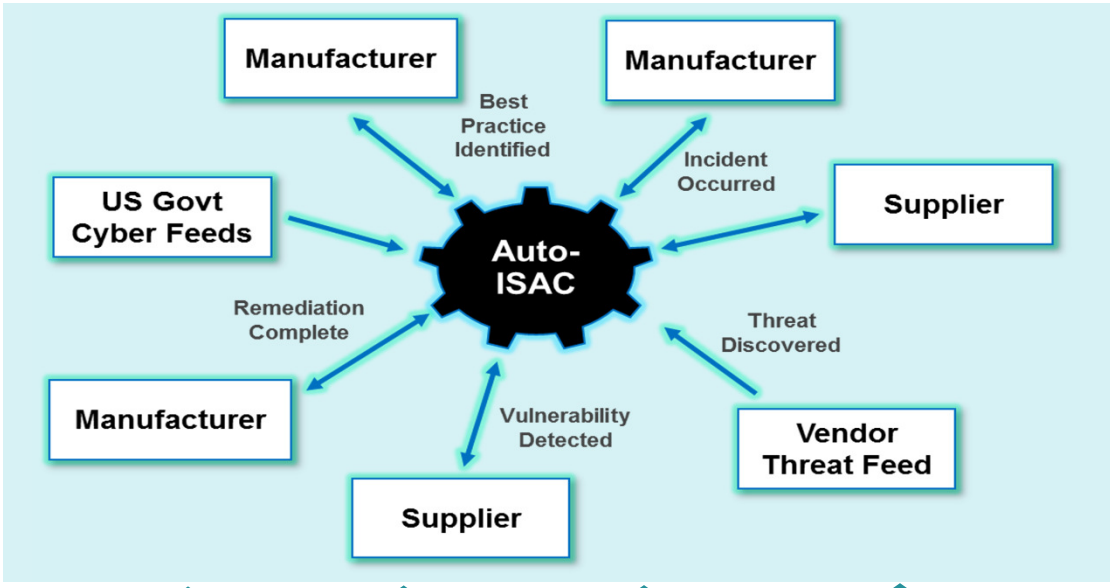


TLP:WHITE

Auto-ISAC permet le partage et l'analyse d'information fiable

sur les menaces informatiques et les vulnérabilités

Centre du renseignement et de l'analyse



Regrouper, analyser et partager de l'information cybernétique sur l'automobile à l'échelle de la surface d'attaque de l'industrie

Avantages

Identification efficace des menaces
en complétant le renseignement interne par des flux externes.

Détection des vulnérabilités plus rapidement
grâce au partage d'information intersectorielle sur la vulnérabilité.

Validation de l'analyse des risques
avec des constatations et des pratiques exemplaires fiables à l'échelle de l'industrie.

Information à communiquer : Types de renseignements

Classification de l'accès et de la distribution

Ce que nous partageons

- **Incidents**
- **Vulnérabilités**
- **Menaces**
- **Connaissance de la situation**

Portée

Partager les renseignements **cybernétiques** liés aux **véhicules** de consommation ou aux véhicules commerciaux qui pourraient avoir une **incidence sur d'autres membres ou être utilisés par d'autres membres.**

La TI et la TE sont inclus.

Vous pouvez partager de façon anonyme ou par attribution; l'accès est contrôlé par le protocole des feux de circulation et nous distribuerons les renseignements en fonction de la criticité.

PROTOCOLE DES FEUX DE CIRCULATION (PFC)

Le PFC indique les restrictions d'accès en fonction de la sensibilité du renseignement

Couleurs du PFC	Description
ROUGE	Limité à un groupe précis et défini (p. ex., seulement ceux qui sont présents à une réunion) en raison du potentiel d'impact élevé.
AMBRE	L'information peut être communiqué uniquement aux membres d'Auto-ISAC. Le traitement de l'information nécessite un soutien, mais il pourrait y avoir un impact si elle est diffusée.
VERT	L'information peut être communiquée aux membres et aux partenaires d'Auto-ISAC, tel que déterminé par Auto-ISAC.
BLANC	L'information peut être communiquée librement et elle est assujettie aux règles du droit d'auteur. L'information comporte un risque minime ou nul.

CRITICITÉ

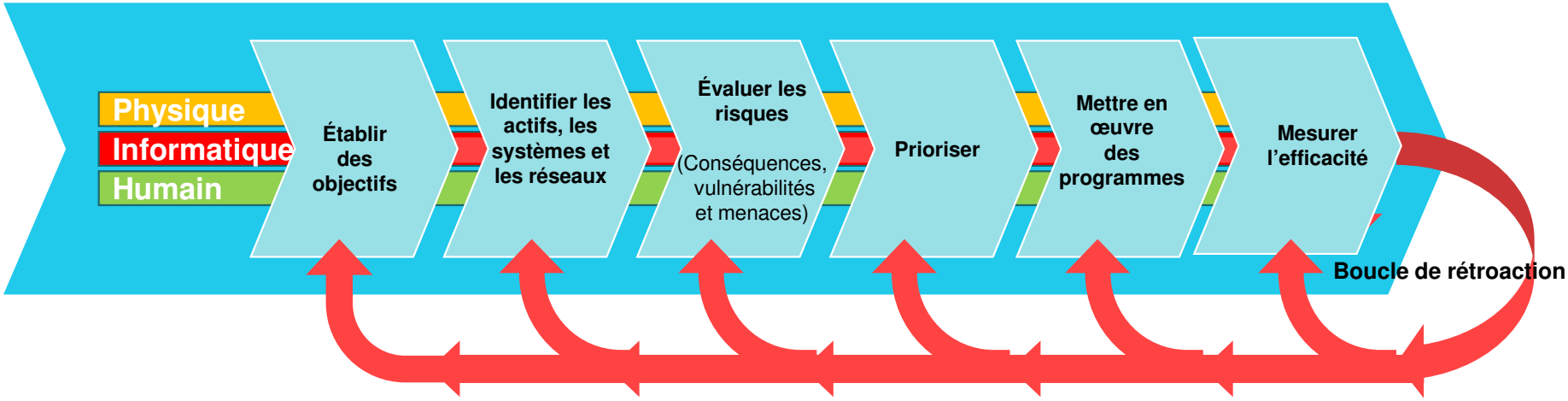
La criticité indique la rapidité avec laquelle les renseignements seront communiqués.

Criticité	Description
URGENT	Critique; on recommande une attention immédiate de la part de l'auteur de la demande ou des membres d'Auto-ISAC.
ÉLEVÉ	Important; on recommande aux membres d'examiner et déterminer si une réponse est nécessaire en temps opportun.
NORMAL	Tous les autres renseignements. Aucune réponse immédiate n'est requise de la part de l'auteur de la demande ou du membre d'Auto-ISAC.

Cadre de sécurité informatique pour les véhicules connectés

Stratégie : Gestion du risque

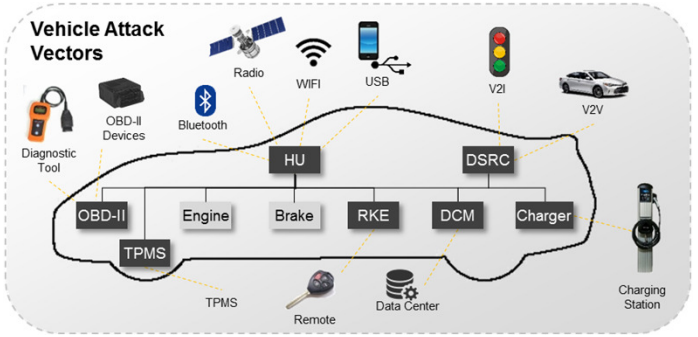
- ✓ **Risque** = menace + vulnérabilités et conséquences qui en découlent
- ✓ Le **cadre** met l'accent sur la prise de décisions tenant compte des risques
- ✓ **Objectif opérationnel** = atténuer la menace en utilisant des techniques de prévention, de détection et d'intervention



Amélioration continue pour améliorer la protection

Cadre pour la sécurité informatique automobile

1. Établir des pratiques exemplaires communes de sécurité informatique pour le secteur automobile
2. Établir une culture de sécurité informatique
3. Comprendre la menace
4. Comprendre le risque
5. Communiquer les menaces et assurer la connaissance de la situation
6. Intervenir en cas d'incident
7. Renforcer le système défensif
8. Définir les principes de conception
9. Définir les principes opérationnels
10. Effectuer la recherche et le développement nécessaires
11. Veiller à ce que le secteur privé, le gouvernement et les partenaires travaillent ensemble



Renforcer la résilience dans l'industrie automobile

Statistiques intéressantes

- **Les véhicules connectés à l'échelle mondiale** augmenteront de **134 %,** passant de 330 millions en 2018 à **774 millions en 2023**[1].
- D'ici 2025, une **voiture connectée** produira **26 Go** de données par heure et **50 Go si elle est autonome**[2].
- En **2021**, nous avons constaté une **augmentation des attaques sophistiquées** qui posent des défis à l'ensemble de l'écosystème automobile.
- En **2021**, la **majorité des piratages** a été effectuée par des **pirates informatiques** (chapeau noir) (57 %), 39 % par des chapeaux blancs et 4 % par des pirates autrement définis[3].
- Les **segments de l'industrie automobile** qui ont été touchés ont été largement répartis dans **tous les segments** : fabricants d'équipement d'origine, fournisseurs de premiers niveaux, VE, gestion de parc automobile, covoiturage, location de voitures, concessionnaires automobiles, covoiturage, etc.
- En **2021**, nous avons constaté une augmentation **de l'utilisation et de la sophistication des cyberattaques** à travers différents vecteurs d'attaque. Les **pratiques d'attaque avancées** sensibilisent davantage l'industrie à la **vulnérabilité** de tout point de connectivité aux **nouvelles menaces**.

1. https://www.juniperresearch.com/whitepapers/connected-cars-how-5g-connected-commerce-blockchain-will-disrupt-the-ecosystem
2. https://www.wevolver.com/article/high-speed-data-and-connected-cars
3. Upstream2022Report

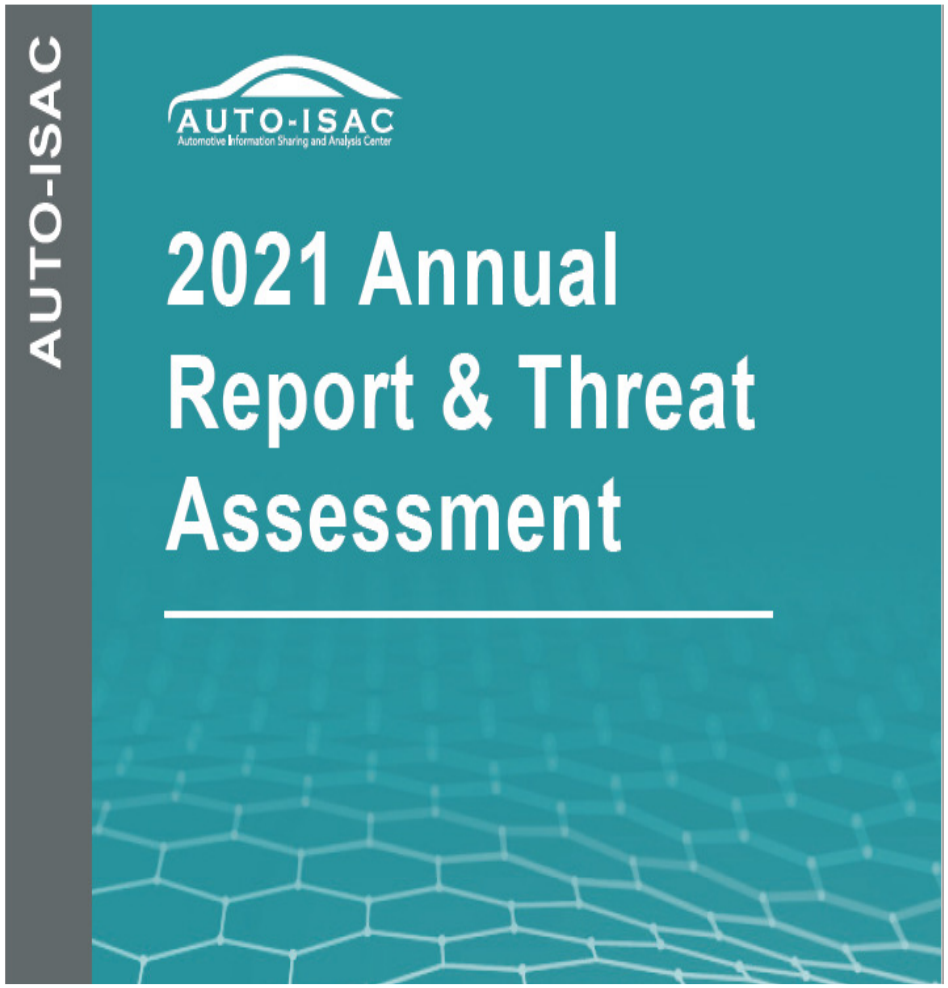
Autres statistiques

- Il y a plus de lignes de code dans un véhicule connecté que dans un avion de chasse ou un Boeing 787!
- La technologie d'entrée sans clé représente près de 50 % de tous les vols de véhicules.
- Rançongiciel + chaîne d'approvisionnement = *d'importants nouveaux défis*.
- *« Le rançongiciel est la plus grande menace à la sécurité de la plupart des organisations aujourd'hui », affirme Ryan Kovar, stratège distingué en matière de sécurité de Splunk. « Honnêtement, la question n'est pas de savoir si vous allez être victime d'un rançongiciel, mais plutôt quand. »*

Vecteurs d'attaque les plus courants pour les véhicules connectés[1]

Serveurs, dans et entre les véhicules
Saisie sans clé/porte-clés
Bloc de commande électronique
Applications mobiles
Infodivertissement
Port OBD
Capteurs
Wi-Fi
Réseaux embarqués

[1] *Rapport en amont 2022 sur la sécurité informatique*



CONTENTS

Contents

ÉVALUATION DE LA MENACE AUTO-ISAC 2021

7 PRINCIPES CLÉS

Menaces prévues pour l'industrie automobile en 2022
❑ Groupes de rançongiciels
❑ Autres organisations cybercriminelles
❑ Groupes de menaces avancés persistantes parrainés par l'État
❑ Vol de véhicules grâce à la technologique

- En 2021, de nombreux rançongiciels et d'autres attaques cybercriminelles ont été perpétrés contre des entreprises, des fournisseurs de matériel et des fournisseurs de services du secteur automobile, ce qui a entraîné des interruptions des activités commerciales et industrielles et la perte de renseignements de nature délicate.
- Les vols de véhicules aux États-Unis ont diminué considérablement (-4 %) en 2019, puis ont grimpé de près de 11 % en 2020 (au début de la pandémie de COVID-19), ce qui est bien supérieur à la tendance annuelle quinquennale précédente (+/ – 1 à 2 %). Le nombre de vols de véhicules devrait demeurer élevé au cours de la prochaine année.
- La portée d'entrée réelle de l'activité mondiale de vol de véhicules technologiques n'est pas claire en raison du manque de mesures sur les différentes tactiques de vol.

ÉVALUATION DE LA MENACE AUTO-ISAC 2021

7 PRINCIPES CLÉS

Menaces potentielles prévues pour les véhicules connectés en 2022

- ❑ **Sites Web, applications et fichiers infectés par des logiciels malveillants accessibles au moyen d'appareils connectés à Internet synchronisés avec les systèmes embarqués**
- ❑ **Exploitation malveillante de vulnérabilités dans l'information, les communications et la technologie d'exploitation**
- ❑ **Utilisation par les auteurs de menaces d'armes cybernétiques de qualité nationale**

- ➢ **À moins que la technologie ne permette le vol de véhicules, il n'y a pas de cyberattaques malveillantes sur les véhicules connectés.**
- ➢ **Les chercheurs découvrent et signalent les vulnérabilités des véhicules connectés aux fabricants de véhicules.**
- ➢ **L'imagination proactive quant à la façon dont les vulnérabilités, les maliciels et les outils nouveaux et existants pourraient mener à des cyberattaques qui menacent la sécurité des véhicules permettra à l'industrie de garder une longueur d'avance sur les menaces potentielles et l'environnement de menace en constante évolution.**

Protection de la sécurité informatique des véhicules connectés

La trajectoire

- **Le partenariat public-privé est essentiel**
  - ✓ Cadre de sécurité informatique pour le partage d'information
  - ✓ Collaboration et partage du secteur privé | Gouvernement
- **Résilience – risque, menace, atténuation**
  - ✓ Connaissance commune de la situation
  - ✓ *La détection d'un est la prévention de l'autre*
- **Cadre de travail concerté**
  - ✓ Un cadre et une feuille de route des véhicules connectés sont nécessaires
  - ✓ Il est essentiel de mettre en place une stratégie internationale de sécurité informatique
  - ✓ Politique coordonnée pour le domaine informatique de l'automobile

trajectory

Aucun cyberincident lié à la sécurité


THANK
YOU
GRAZIE
ASANTE
MERCI
MULTUMESC
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
GRAZIE
MERCI
MOCHCHAKKERAM
CHOKRANE
MATUR NUWUN
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
MAAKE
OBRIGADO
SPASIBO
WELALIN
JUSPAXAR
OBRIGADO
MATONDO
KIITOS
SALAMAT
MOCHCHAKKERAM
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
KIITOS
OBRIGADO
DANK JE
VINAKA
NIRRINGRAZZJAK
MAMANA
MULTUMESC
ARIGATO
KIITOS
DANKON
NIRRINGRAZZJAK
MOCHCHAKKERAM
MOCHCHAKKERAM
OBRIGADO
SPASIBO

Nos coordonnées

Faye Francy
Directrice générale

20 rue F, Nord-Ouest
Bureau 700
Washington (DC) 20001
1-703-861-5417
fayefrancy@automotiveisac.com

http://www.automotiveisac.com