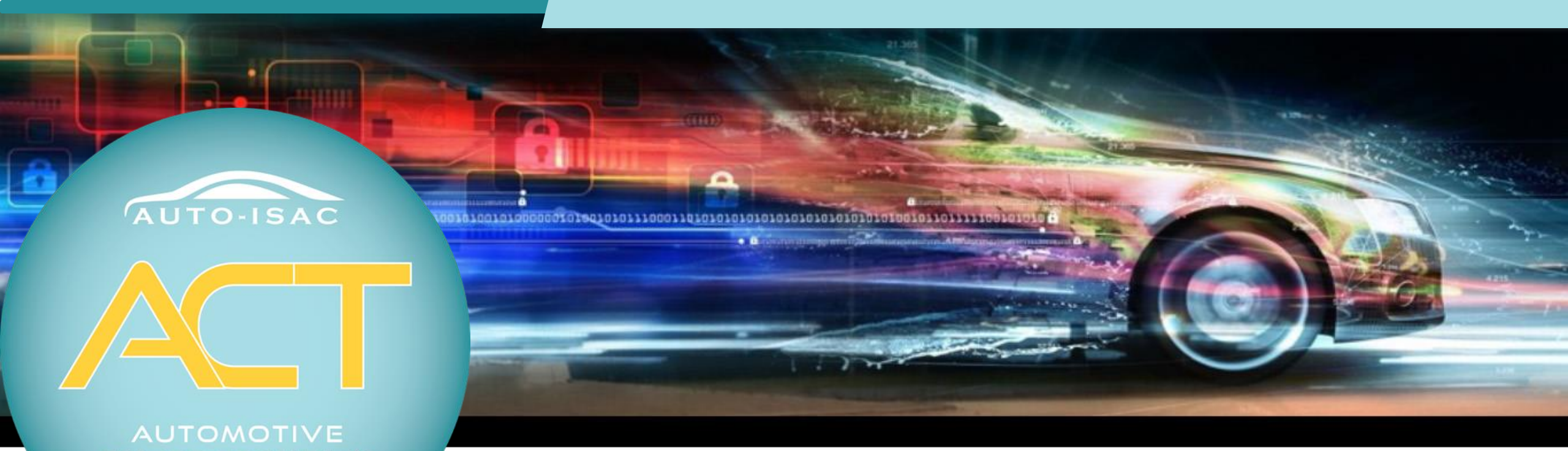


Formation en cybersécurité automobile (Automotive Cybersecurity training [ACT])

Chef du personnel : Tamara Shoemaker, Auto-ISAC

3 février 2023

TLP : CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Présentation de l'orateur

Tamara Shoemaker
Auto-ISAC
Responsable de la formation en cybersécurité

Postes actuels

- Responsable du programme de formation en cybersécurité automobile d'Auto-ISAC —(ACT)
- Cheffe du personnel du comité permanent de l'éducation et de la formation (ETSC)

Postes antérieurs

- Directrice du Center for Cybersecurity & Intelligence Studies de l'université de Detroit Mercy
  - **Désignation d'un centre d'excellence universitaire en cyberdéfense auprès du Department of Homeland Security et du National Security Agency depuis 2004**
- Fondatrice du programme CyberPatriot K-12 du Michigan
- Coordinatrice de programme, Michigan Member Alliance InfraGard
- Cofondatrice de la coalition MCISSE des centres d'excellente académique du Michigan
- Détective privé agréé depuis 12 ans

Véhicules

- Ford Taurus Sho 2019 et Ford T-Bird 2004

Mission de l'Auto-ISAC :

Mission :

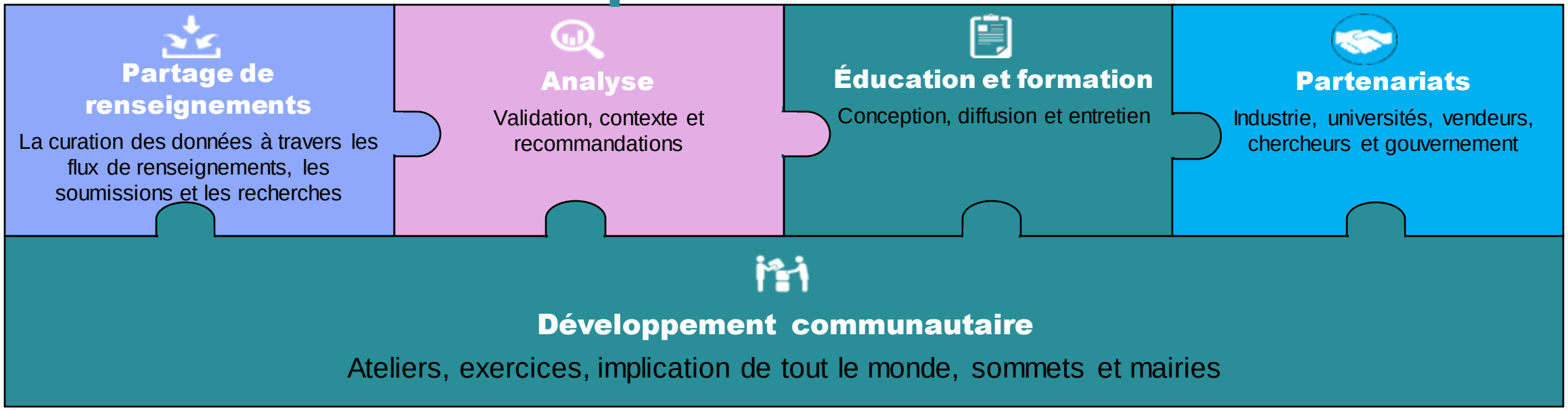
Faire office de courtier d'information impartial afin d'offrir un **point central de coordination et de communication** pour l'industrie automobile mondiale par l'analyse et le partage de renseignements fiables et opportuns sur les cybermenaces.

.

Portée

Véhicules utilitaires légers et lourds, fournisseurs, flottes de véhicules commerciaux et transporteurs. **Nous nous concentrons actuellement sur la cybersécurité des *véhicules*** et nos activités incluent désormais la sécurité des systèmes d'information industriels et la sécurité des systèmes d'information d'entreprise (4T20).

Ce que nous faisons



Protocole TLP (Traffic Light Protocol en anglais) : CLEAR

L'Auto-ISAC et la National Highway Traffic & Safety Administration (administration américaine de la sécurité dans les transports)

En raison de la connectivité accrue des véhicules automobiles, la cybersécurité est désormais une composante essentielle de la sécurité automobile. En effet, l'industrie automobile est confrontée à des défis croissants en matière de gestion des menaces à la cybersécurité et d'amélioration de la résilience de la cybersécurité afin de garantir la sécurité automobile. Pour relever ces défis, des compétences spécialisées et une formation différente des programmes d'enseignement traditionnels de la cybersécurité axés sur les entreprises et les systèmes d'information sont nécessaires.

L'Auto-ISAC a reconnu la nécessité d'un programme éducatif commun sur la cybersécurité des véhicules automobiles. Le programme ACT a été créé parce qu'aucun programme complet ne traitait de la cybersécurité dans le secteur automobile. D'après les pratiques exemplaires de la NHTSA, le développement de la main-d'œuvre et la formation continue constituent des étapes cruciales pour améliorer la cybersécurité des véhicules automobiles.

Programme ACT – Développement du programme et des cours

Conception du programme ACT

- Recherche globale sur les programmes de formation et d'éducation existants en cybersécurité des véhicules
- Examen et validation des adhésions
- Adaptation aux besoins de l'industrie

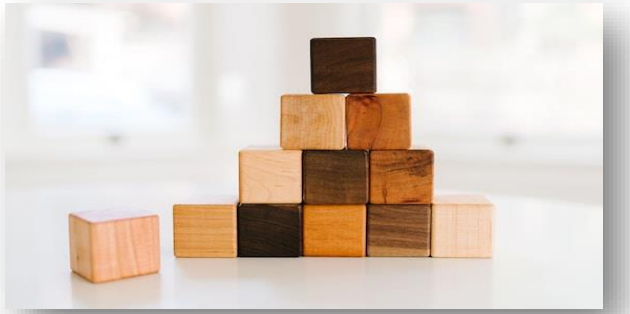
Une **équipe Tiger (tigre)** chargée d'appuyer le développement et la supervision de l'examen :

- Programme d'études
- Supports de cours
- Personnel de formation

- Conduite de **pilotes Alpha et Beta** pour déterminer les éventuelles corrections de trajectoire
- Sélection de stagiaires novices et expérimentés en cybersécurité
- Le programme sera maintenu et mis à jour si nécessaire

Programme ACT

Prestation de la formation



Cours fondamentaux

Dispensés en ligne à l'aide du système d'apprentissage de l'université, offerts à la fois de manière synchrone et asynchrone, selon les pistes définies :

1. **Cybersécurité de base (36 heures)**
2. **Ingénierie de sécurité (36 heures)**
3. **Opérations, gouvernement et gestion de la sécurité (36 heures)**

Cours avancés

Dispensés de manière pratique au **American Center for Mobility** à Ypsilanti, Michigan :

1. **Ingénierie avancée (36 heures)**
2. **Technologie sans fil avancée (40 heures)**
3. **Attaques guidées (38 heures)**
4. **VE et infrastructure des VE (36-40 heures)**

Ces cours sont sanctionnés par des certificats de fin d'études.

Mise à jour du programme de formation en cybersécurité automobile (Automotive Cybersecurity Training [ACT])

➢ Mesures du programme ACT :

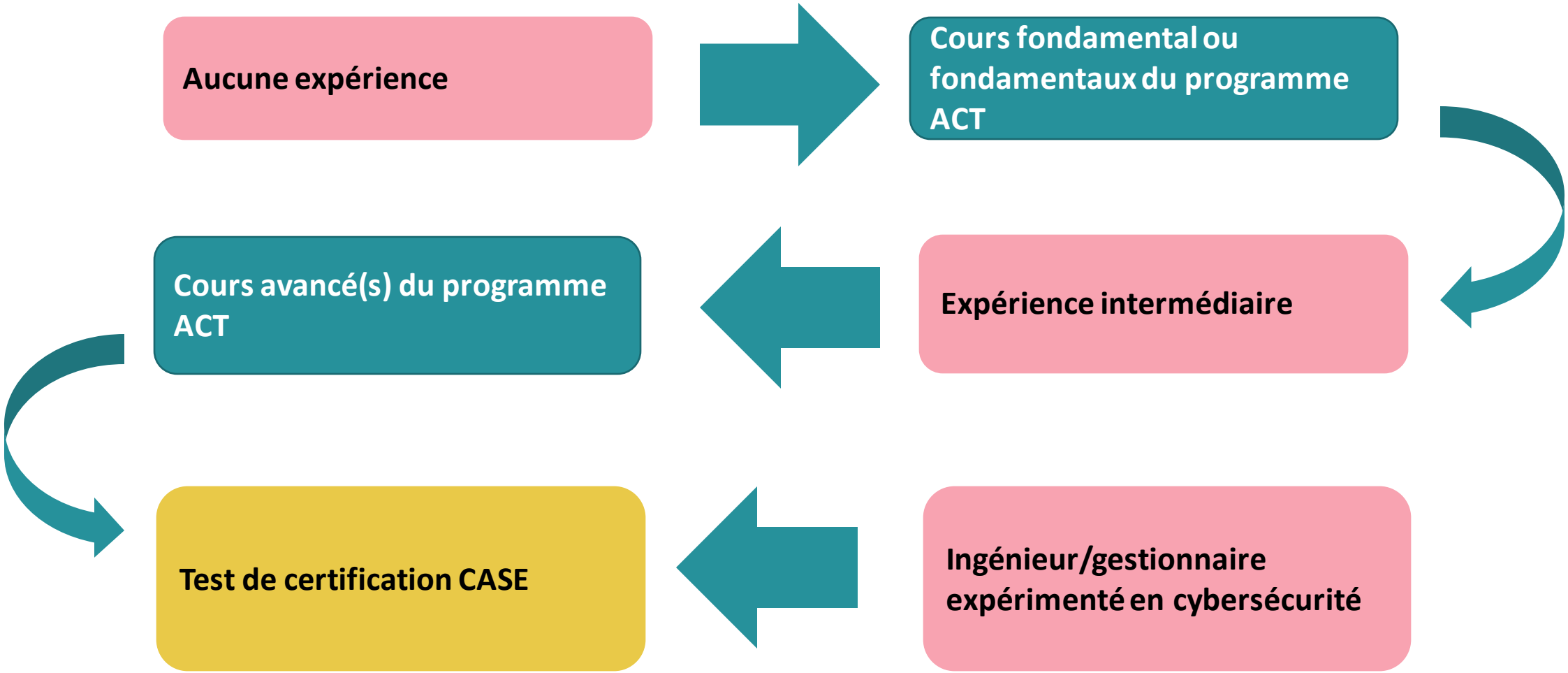
- **224** adhérents (des particuliers) se sont inscrits à des cours de **53** entreprises membres
- **134** stagiaires ont suivi les cours fondamentaux Alpha et Beta
- **105** stagiaires ont suivi les cours avancés Alpha et Beta
- **59** adhérents devront passer le CAPEX (**27** le 24 janvier et **32** en mars)

➢ Certificats de fin de formation et certification

- Application web de certification pour suivre les certificats de fin de formation et la certification CASE.
- Compilation des critères pour les certificats de fin de formation pour les stagiaires actuels.
- **CAPEX** en anglais Capability Exercise, est un exercice de capacité requis pour se qualifier pour la **certification CASE (Certified Automotive cyberSecurity Engineer Certification).**
  - Pour passer le CAPEX : Vous devez être un ingénieur en cybersécurité expérimenté ou un stagiaire ayant suivi les blocs de cours du programme ACT appropriés pour accroître vos connaissances et votre expérience.
  - Pour obtenir le titre d'ingénieur CASE, vous devez réussir cet exercice virtuel d'une journée basé sur des scénarios.

➢ La formation ACT sera programmée pour l'automne 2023 — www.automotiveisac.com.

Public cible du programme ACT



Soutien du programme ACT

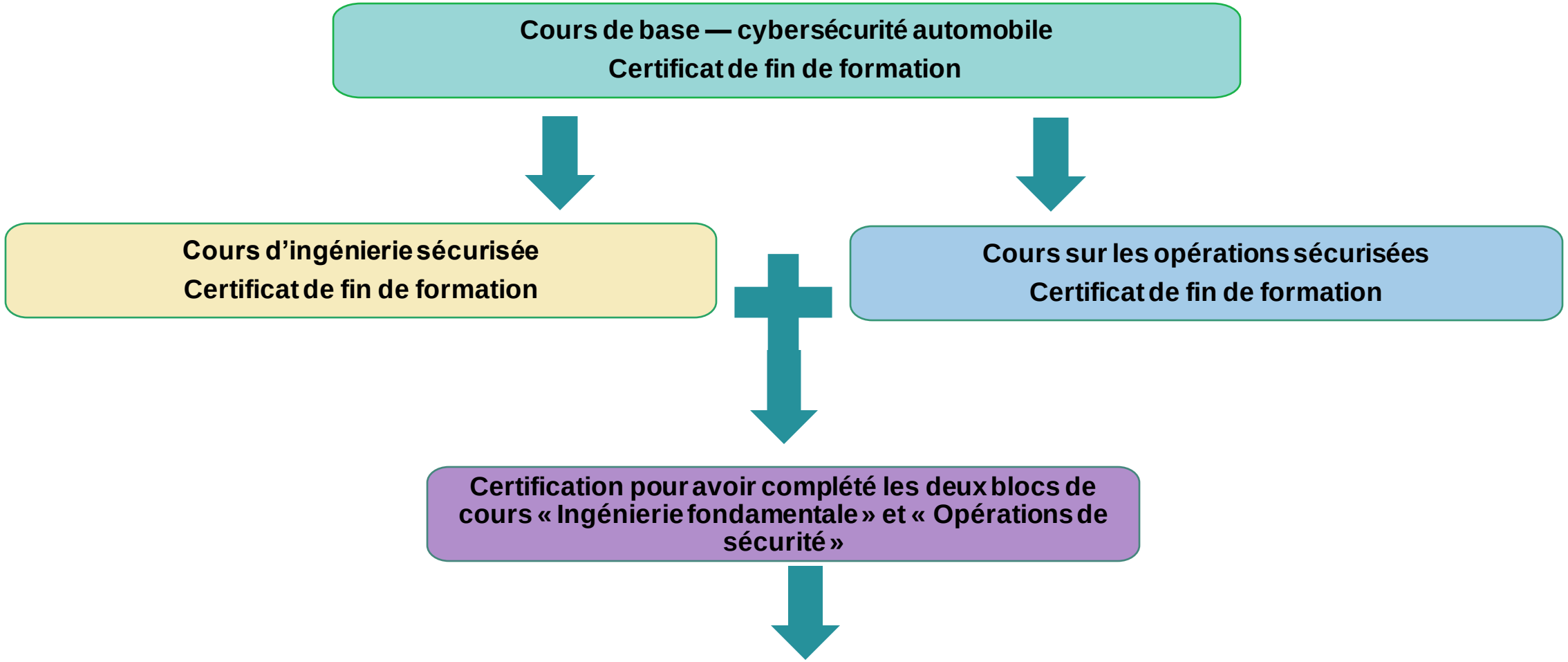
- **Objectif :**
  - Les cours fondamentaux du programme ACT disponibles par l'intermédiaire des partenaires universitaires
  - Cours fondamentaux du programme ACT disponibles par Auto-ISAC grâce à *un système de gestion de l'apprentissage*
  - Cours avancé du programme ACT prévu en personne pour l'automne 2023
  - Certifications délivrées à la fin du cours
  - Certification CASE délivrée après avoir passé le CAPEX

- **Le cours fondamental sera dispensé avec les universités partenaires**
  - Les universités partenaires offrent leur programme d'études en cybersécurité (conditions préalables)
  - Audit du programme d'études, sauf s'il est certifié comme centre d'excellence académique de la NSA/DHS
  - Auto-ISAC dispense les cours fondamentaux du programme ACT
  - Des suivis périodiques seront nécessaires pour assurer l'intégrité du programme

- **Assemblage des cours en fonction du modèle universitaire**
  - Mise en correspondance avec les normes, les règlements et les pratiques exemplaires
  - Adaptation en fonction de l'équipe Tiger, des évaluations des stagiaires et des conseils d'experts
  - Adhésion exigeant une formation en ligne à la demande (SGA)
  - Normalisation des programmes d'études pour les universités partenaires

- **Cours avancés**
  - Négocier des contrats avec plus de 20 instructeurs
  - Choisir les lieux et le SGA
  - Achat d'équipement

Parcours menant à la certification superposable pour les fondamentaux



Programme d'études ACT Beta réajusté

➢ Fondamentaux — Formation en ligne dirigée par un instructeur

▪ Notions de base — de 30 à 36 heures

- ➢ Notions de base sur la cybersécurité (NIST Workforce Framework, CSEC2017, NIST800)
- ➢ Gestion de la menace automobile (clause 15)
- ➢ Gestion des risques (RMF)
- ➢ Conformité réglementaire de la CEE (R155-21434, R156-24089)
- ➢ Opérations de sécurité
- ➢ Confidentialité et protection des données (Règlement général sur la protection des données, PCI. .)

▪ Ingénierie de sécurité — 36 heures

- ➢ Processus d'ingénierie de sécurité des systèmes (24089)
- ➢ CANbus et protocoles
- ➢ Applications crypto
- ➢ Introduction à la sécurité des communications/OSI
- ➢ Processus de mesure et d'évaluation
- ➢ Sécurité des systèmes d'exploitation

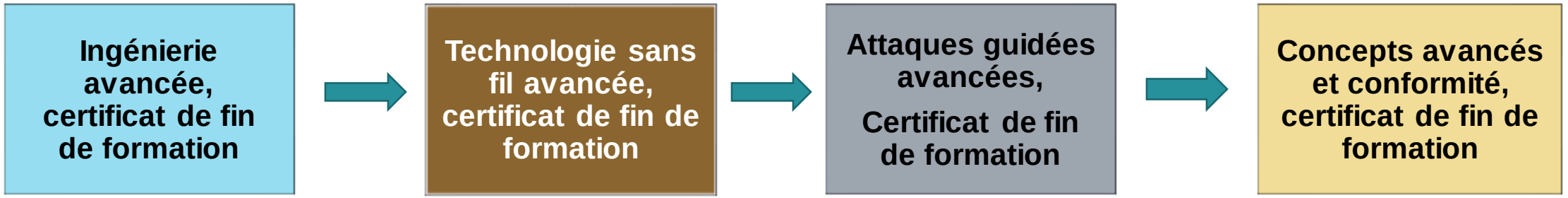
▪ Opérations, gouvernement et gestion de la sécurité — 36 heures

- ➢ Politiques de cybersécurité (clause 5)
- ➢ Mise en œuvre de la politique de cybersécurité (clause 8)
- ➢ Modèles de contrôle de la cybersécurité (clause 8)
- ➢ Gestion de la vulnérabilité des produits/suivi continu (clause 7)
  - Concevoir un guide d'intervention en cas d'incident
  - Processus d'intervention en cas d'incident
  - Problèmes liés à la chaîne d'approvisionnement
- ➢ Autres, flottes, hors route, militaire …

TLP : CLEAR

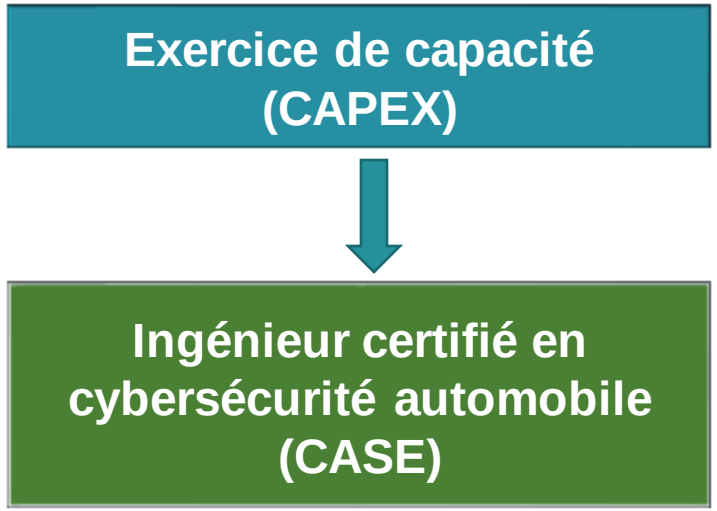
Cours avancés et certification pour CASE

Les personnes sans expérience devraient suivre les cours dans cet ordre.



Les personnes ayant une expérience intermédiaire peuvent suivre des cours qui répondent à leurs besoins.

Les experts peuvent aller directement au CAPEX.



VE avancé à la place de C et C bientôt disponible!

TLP : CLEAR

Programme ACT Beta

Avancé — Formation pratique collaborative en personne

- **Ingénierie avancée (Advanced Engineering) — 36 heures**
  - Approches au Design Thinking sécurisé
  - Outils CAN et interactions de bas niveau
  - Aperçu des principes de conception du matériel de sécurité
  - Information sur l'ISO-TP
  - UDS interactif
  - Mises à jour des logiciels
  - Défauts de l'information-divertissement et correctifs
  - Médecine légale
  - Évaluation des risques automobiles
  - Introduction à l'ingénierie inverse de matériel
  - Introduction à l'ingénierie inverse de logiciel
- **Analyste du renseignement avancé — 36 heures**
  - Bluetooth
  - WiFi
  - Proximité
  - Cellulaire et télématique
  - Protocoles et diagnostics
  - Radio logicielle et GPS
  - V2X
  - Bande ultra large
- **Attaques guidées — 40 heures**
  - Télédéverrouillage
  - Analyse par canal auxiliaire et injection d'erreurs
  - Attaques matérielles par relais
  - Attaques par radiofréquence
  - Attaques des applications téléphoniques
  - ARM/Intel/etc. Exploitation
  - ISO 21434 – Attaques avancées
  - Fusion de capteurs, IA contradictoire
  - Système de surveillance sans fil de la pression des pneus
- **Future session VE — 36 heures**
  - Sécurité des VE et interactions avec le réseau
  - Cours pour cette section à déterminer

Système de certification

- **Certificats de fin de formation**
  - **Une certification par bloc de cours complété**
  - **Une certification pour avoir complété tous les cours fondamentaux et avancés**

- **Ingénieur certifié en sécurité automobile (CASE)**
  - **Cours complétés plus CAPEX pour les débutants**
  - **Cours avancés achevés plus CAPEX pour un niveau d'expérience intermédiaire**
  - **CAPEX pour les professionnels de la cybersécurité**

TLP : CLEAR

Maintien du programme ACT

➢ Automne 2023 – *consultez notre site Web pour les mises à jour*

- **Fondamentaux, ingénierie de sécurité et opérations de sécurité, gouvernement et gestion offerts en ligne à travers le système de gestion de l'apprentissage et par le biais d'universités partenaires**

- **Cours avancés : ingénierie, technologie sans fil, attaque guidée et VE dispensés dans la région métropolitaine de Détroit (Michigan)**

- **L'exercice de capacité (CAPEX) pour le titre de Certified Automotive Cybersecurity Engineer (CASE) (Ingénieur certifié en cybersécurité automobile) est offert selon les besoins**

www.automotiveisac.com

Merci!


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

Nos coordonnées

Tamara Shoemaker
Responsable de la formation en cybersécurité

20 F, rue NW, bureau 700
Washington, DC 20001
313-804-0544
tamarashoemaker@automotiveisac.com

www.automotiveisac.com@auto-ISAC