Cyberattaque automobile : détection et approche méthodologique de gestion des dossiers d'expertise.

CYBERSECURITE - SOFTWARE

Délais d'accès à la formation : entre 1 et 3 mois (délais de planification).

Modalités d'inscription : renvoyer le bulletin d'inscription complété, nous contacter pour toute demande d'inscription.

Pour les formations INTRA, au moins un entretien téléphonique préliminaire sera réalisé.

OBJECTIFS

A l'issue de cette formation, les stagiaires seront capables de déceler une cyber attaque automobile (dans la limite des preuves techniques) et d'apporter un point de vue cybersécurité dans le traitement des dossiers d'expertise.

PUBLIC VISÉ

Expert référents techniques

PRÉ REQUIS

Connaisance des notions de bases du véhicule.

OBJECTIFS PÉDAGOGIQUES

-Identifier les fondamentaux règlementaires et technique en terme de cybersécurité automobile
-Distinguer les principales techniques d'attaques et les principaux moyens de détection d'attaque
-Consolider une approche méthodologique commune

MÉTHODES ET MOYENS PÉDAGOGIQUES

Présentation théorique illustrée avec des exemples.
Cas pratiques, échanges et questions/réponses avec le formateur.
Remise d'une documentation pédagogique numérique pendant le stage.

QUALIFICATION INTERVENANT(E)(S)

Expert cybersécurité

PARCOURS PÉDAGOGIQUE

Les fondamenteux de la cybersécurité : notions et enjeux
Contexte règlementaire en cybersécurité automobile, de l'environnement et des besoins actuels
Principales exigences en cybersécurité automobile : comprendre la cybersécurité et les risques associés
Tendances en matière de cyber attaques :
Les grands types de menaces/attaques cyber automobile
Le profil des attaquants
Tendants en matière de cyber attaques sur les dernières années
Profils des véhicules les plus attaqués/les plus fiables
Détection des attaques
Attaques les plus courantes et traces de détection (phare avant/Kit)
Surfaces d'attaques des véhicules
Différences entre attaque embarquée et attaque débarquée
Revue du process interne à partir d'un dossier d'expertise (anonymisé)
Mise en pratique : Ateliers d'essais cyber attaque automobile (avec mise à disposition d'un véhicule) Présentation de 2 scénarios de cyber attaques et des outils mis à disposition (embaquée/débarquée)
Réalisation des scénarios par groupe de 4 stagiaires
Débrief du cas pratique
Debriefing/tour de table
Propositions d'améliorations du process interne

MÉTHODES ET MODALITÉS D'ÉVALUATION

QCM individuel d'évaluation des connaissances de fin de formation.

MODALITÉS D'ACCESSIBILITÉ

Personne en situation de handicap, nous contacter pour échanger sur vos éventuels besoins d'aménagement à prevoir. Référente handicap : Christelle AUGER : christelle.auger@utac.com

Cyberattaque automobile : détection et approche méthodologique de gestion des dossiers d'expertise.

7.00 Heures
1 Jour

De 4 à 8 Personnes

Contactez-nous !

Audrey RISSOT
Chargée de formation

Tél. : 0169801708
Mail : audrey.rissot@utacceram.com

Février 2026

Version : 410-20260806