Cybersecurity Professional Automotive

5 jours (35 heures)

Tarif inter : 6600 à 6900 € HT

FORMATION EN PRESENTIEL

Dates, lieux et tarifs sur sia.fr

Personnel concerné

Professionnels en poste ou en reconversion souhaitant acquérir des compétences opérationnelles en cyber sécurité automobile en vue d'une application à venir en projet ou dans un futur poste.
Ingénieurs et techniciens en interaction avec des équipes cyber ou travaillant sur des exigences de cyber sécurité issus de leurs clients ou de leurs partenaires
Etudiants en cyber sécurité, logiciel et électronique embarquée en cycle ingénieur souhaitant se spécialiser en cyber sécurité du produit automobile

Prérequis

Avoir une connaissance du monde automobile et du cycle de développement de produits automobiles.
Avoir une formation générale de niveau technicien ou ingénieur ou posséder une expérience équivalente.

Animateur

Yacine LADJICI, Group Cyber Security Officer Valeo Power - Valeo Master Expert
Président de la communauté des experts en cyber sécurité et accès aux données de la SIA
Président du CSTA 30 de la PFA : comité de standardisation et de normalisation en cyber sécurité automobile

Méthodes et moyens pédagogiques

Apports théoriques avec support Powerpoint
Séquences de questions/réponses afin de favoriser l'interactivité.
Remise d'un support de cours au format électronique.

Moyens techniques

Salle de formation équipée d'un vidéoprojecteur, d'un écran et d'un paper board.

Suivi et évaluation

Feuille d'émargement signée par demi-journée par les stagiaires et cosignée par le formateur.
Évaluation de la formation par les participants.
Évaluation des acquis via un questionnaire en ligne.
Remise d'une attestation de formation.

Délais d'accès

Inter-entreprises : inscription au plus tard 2 jours avant la formation
Intra-entreprise : organisation sous deux semaines minimum.

Accessibilité aux personnes en situation de handicap

OBJECTIFS

Être capable :

- D'identifier et de comprendre les enjeux relatifs à la cyber sécurité du produit automobile et dans le domaine de la mobilité
- D'identifier et d'utiliser les principales réglementations et normes de cyber sécurité applicables au monde automobile
- D'identifier les principales architectures électriques, électroniques et logicielles automobiles et leurs concepts de cyber sécurité
- D'identifier les principales menaces cyber et les mesures d'atténuation préconisées par la réglementation
- D'identifier les enjeux de la norme ISO/SAE 21434 et leur déclinaison dans une organisation automobile
- D'identifier les autres normes ayant des interfaces avec l'ISO/SAE 21434 telles que l'ISO/IEC 27001 , l'ISO 26262 , l'ISO PAS 5112
- De structurer les données d'entrée nécessaires à la réalisation d'une analyse de risque cyber sur un produit automobile
- De citer les étapes d'une analyse de risque cyber selon la méthode TARA (Threat Analysis and Risk Assessment)
- De mettre en œuvre un calcul de la faisabilité d'une attaque cyber selon la méthode TAF (Target Attack Feasibility)
- Déterminer et expliquer les éléments essentiels d'un concept en cybersécurité
- D'identifier les contrôles de cyber sécurité inclus dans les concepts de cyber sécurité
- D'identifier et de déployer les principes d'audit de cyber sécurité organisationnel et technique
- D'identifier les différents types de tests de pénétration
- D'identifier les enjeux relatifs à la gestion des vulnérabilités cyber tout au long du cycle de vie produit
- De lister les enjeux relatifs à l'intelligence artificielle et leur lien avec la cyber sécurité du produit automobile
- De réaliser une étude de cas impliquant la mise en place d'une politique de cyber sécurité et d'évaluer le niveau de cyber sécurité d'un produit automobile

Contact : Larissa RIFFAUD
larissa.riffaud@sia.fr // 07 86 76 12 79

28/04/2025

Cybersecurity Professional Automotive

5 jours (35 heures)

Tarif inter : 6600 à 6900 € HT

FORMATION EN PRESENTIEL

Dates, lieux et tarifs sur sia.fr

Personnel concerné

Professionnels en poste ou en reconversion souhaitant acquérir des compétences opérationnelles en cyber sécurité automobile en vue d'une application à venir en projet ou dans un futur poste.
Ingénieurs et techniciens en interaction avec des équipes cyber ou travaillant sur des exigences de cyber sécurité issus de leurs clients ou de leurs partenaires
Etudiants en cyber sécurité, logiciel et électronique embarquée en cycle ingénieur souhaitant se spécialiser en cyber sécurité du produit automobile

Prérequis

Avoir une connaissance du monde automobile et du cycle de développement de produits automobiles.
Avoir une formation générale de niveau technicien ou ingénieur ou posséder une expérience équivalente.

Animateur

Yacine LADJICI, Group Cyber Security Officer Valeo Power - Valeo Master Expert
Président de la communauté des experts en cyber sécurité et accès aux données de la SIA
Président du CSTA 30 de la PFA : comité de standardisation et de normalisation en cyber sécurité automobile

Méthodes et moyens pédagogiques

Apports théoriques avec support Powerpoint
Séquences de questions/réponses afin de favoriser l'interactivité.
Remise d'un support de cours au format électronique.

Moyens techniques

Salle de formation équipée d'un vidéoprojecteur, d'un écran et d'un paper board.

Suivi et évaluation

Feuille d'émargement signée par demi-journée par les stagiaires et cosignée par le formateur.
Évaluation de la formation par les participants.
Évaluation des acquis via un questionnaire en ligne.
Remise d'une attestation de formation.

Délais d'accès

Inter-entreprises : inscription au plus tard 2 jours avant la formation
Intra-entreprise : organisation sous deux semaines minimum.

Accessibilité aux personnes en situation de handicap

PROGRAMME

Introduction et contexte
- Historique des attaques dans le monde automobile
- Architectures électroniques et logicielles des systèmes automobiles aujourd'hui et demain
- Protocoles de communication véhiculaires
- Réglementation UN R155
- Annexe 5 de l'UN R155 (Menaces et mesures d'atténuation)
- Exercice d'application sur l'annexe 5

Les normes et les réglementations cyber (IS/IT, produit, industrielles)
- Les principales réglementations cyber européennes NIS2 / CRA / AI Act / UNR 155/156
- Les principales normes cyber internationales
- L'ISO/IEC 27001
- L'ISO/IEC 27002
- L'ISO/IEC 27005
- Critères communs et profils de protection

L'ISO/SAE 21434 (la norme de cyber sécurité automobile)
- Les différents chapitres de la norme
- L'utilisation concrète de la norme en contexte projet
- La méthode TARA (Threat Analysis and Risk Assessment)
- Etude de cas en méthode TARA
- Mise en place d'un CSMS (Cybersecurity Management System)

Introduction au concept de sécurité automobile
- Introduction à la cryptographie utilisée dans le monde automobile
- Lien entre analyse de risque cyber et concept de sécurité
- Les mesures d'atténuation listées dans la réglementation Cyber
- Les contrôles de sécurité au niveau véhicule et composant
- La sécurisation des mises à jour véhicule OTA

Audit de cyber sécurité organisationnel et produit
- Les principes de l'audit de cyber sécurité : ISO 19011 / ISO-PAS 5112
- Les différents types d'audit cyber
- Les standards utilisés en audit de cyber sécurité
- Mise en situation : Préparation d'un audit de cyber sécurité d'une entreprise

Intelligence artificielle et cyber sécurité automobile
- Les concepts de base de l'intelligence artificielle
- Le cadre réglementaire : lien entre UN R155 et AI
- Les menaces cyber issues de l'utilisation de l'IA

Conclusion

Contact : Larissa RIFFAUD
larissa.riffaud@sia.fr // 07 86 76 12 79

MAJ 28/04/2025