+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 10/10/2024

S'inscrire

Formation norme de Cybersécurité automobile (ISO 21434)

2 jours (14 heures)

Présentation

Notre formation sur la norme ISO 21434 de cybersécurité automobile vous permettra de comprendre et d'appliquer les exigences de cette norme essentielle dans l'industrie automobile. Cette formation est conçue pour vous aider à intégrer des pratiques de cybersécurité robustes dès les premières phases de conception de vos véhicules et systèmes.

Durant cette formation, vous découvrirez les enjeux critiques de la cybersécurité dans l'industrie automobile, les réglementations internationales pertinentes et les méthodes d'analyse des risques spécifiques au domaine automobile.

À l'issue de cette formation, vous serez capable de gérer efficacement la cybersécurité tout au long du cycle de vie de vos produits, de la conception à la mise hors service, tout en répondant aux exigences des réglementations en vigueur.

Objectifs

- Comprendre les enjeux de la cybersécurité dans l'industrie automobile et les principales menaces et vulnérabilités
- Acquérir une connaissance approfondie de la norme ISO 21434
- Maîtriser les phases de gestion de la cybersécurité, de la conception à la décommission
- Appliquer les méthodologies d'analyse des risques et de gestion des menaces (TARA)
- Gérer les incidents de cybersécurité et mettre en œuvre des stratégies de mise à jour et d'amélioration continue
- Rester informé des évolutions technologiques et normatives pour assurer une cybersécurité proactive

Public visé

- Ingénieurs en cybersécurité
- Responsables de la gestion des risques
- Développeurs de logiciels embarqués
- Chefs de projet automobile
- Responsables qualité et conformité
- Toute personne impliquée dans la conception, le développement et la maintenance des systèmes automobiles

Pré-requis

- Aucune expérience en sécurité embarquée nécessaire
- Notions sur les infrastructures automobiles est un plus

PROGRAMME DE NOTRE FORMATION NORME DE CYBERSÉCURITÉ AUTOMOBILE

INTRODUCTION À LA CYBERSÉCURITÉ AUTOMOBILE ET À LA NORME ISO 21434

- Présentation des enjeux de la cybersécurité dans l'industrie automobile
- Introduction générale à la norme ISO 21434
- Distinction entre sûreté et cybersécurité
- Impact des nouvelles technologies sur la cybersécurité automobile
- Aperçu des principales menaces et vulnérabilités

FONDAMENTAUX DE LA GESTION DE LA CYBERSÉCURITÉ SELON L'ISO 21434

- Comprendre la structure et les objectifs de la norme
- Gestion organisationnelle de la cybersécurité
- Importance de l'intégration de la cybersécurité dès la conception
- Phases de gestion de la cybersécurité : de la conception à la décommission
- Rôles et responsabilités dans la mise en œuvre de la norme

RÉGLEMENTATIONS INTERNATIONALES ET HOMOLOGATION

- Vue d'ensemble des Règlementations n°155 et n°156 de l’ONU
- Processus d'homologation et exigences pour les systèmes de gestion de la cybersécurité (CSMS)
- Gestion de la cybersécurité dans la chaîne d'approvisionnement
- Implications de ces réglementations sur les pratiques actuelles

ANALYSE DE RISQUE ET MÉTHODES D'ÉVALUATION (TARA)

- Introduction à la méthodologie d'analyse des risques et de gestion des menaces (TARA)
- Approches pour identifier et évaluer les risques de cybersécurité
- Exemples pratiques et étude de cas
- Application de TARA dans le cycle de développement automobile

GESTION DES INCIDENTS ET MISE À JOUR DE LA CYBERSÉCURITÉ

- Principes de la gestion des incidents de cybersécurité
- Stratégies pour la mise à jour des systèmes en réponse aux vulnérabilités découvertes
- Exigences de la norme pour la surveillance continue et l'amélioration
- Cas pratiques sur la gestion des mises à jour et des patches de sécurité

VEILLE TECHNOLOGIQUE ET NORMATIVE

- Évolutions récentes de la norme ISO 21434
- Impact de l'Internet des objets (IoT), de l'IA et du jumeau numérique sur la cybersécurité automobile
- Discussion sur les futures mises à jour et évolutions de la norme
- Importance de la veille technologique et normative pour rester à jour

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.