(Télé-)présentiel

Cybersécurité des Systèmes Embarqués et de l'Internet des Objets (IoT)

Objectifs

- Identifier les protocoles de communication utilisés dans l'IoT
- Décrire les enjeux de sécurité liés aux systèmes embarqués et des objets connectés
- Identifier et décrire les vulnérabilités et les différents vecteurs d'attaque des composants d'un architecture IoT

Pré-requis

- Connaissances générales en informatique ;
- Connaissances de base des réseaux informatiques ;
- Aucune connaissance préalable n'est requise sur les systèmes embarqués et l'IoT.

Public

Cette formation s'adresse aux développeurs, intégrateurs systèmes, ingénieurs, responsables sécurité, aux différents responsables de sureté industrielles et ingénieurs / administrateurs souhaitant comprendre les enjeux et vulnérabilités des systèmes embarqués et des objets connectés.

(Télé-)présentiel

Programme de la formation

Introduction sur les objets connectés

- IoT, objets connectés, Smart City, Industrie 4.0, FOG Computing, ...
- Ecosystème et nouveaux protocoles de communication

Domaines d'application

- Les scénarios de l'IoT dans un contexte d'entreprise
- Nouvelles exigences pour l'IT
- Architecture fonctionnelle et solutions IoT dans le monde industriel

Enjeux de cybersécurité

- Vulnérabilités et vecteurs d'attaques
- Modèles et nouvelles dimensions de menaces
- Points de vigilance et approche globale des risques
- Recommandations de sécurité et documents de références

(Télé-)présentiel

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

Patrice ROY Certifié CISSP (Certified Information Systems Security Professional) et GICSP (Global Industrial Cyber Security Professional), il possède une expérience de plus de 10 ans dans la sécurisation des architectures chez différents opérateurs de service Internet.
Depuis 5 ans, il travaille chez Thales Communications & Security dans une cellule d'expertise Sécurité au sein du Pôle Network & Endpoint Security où il contribue à des projets de R&D liés à la sécurisation des protocoles de routage, ainsi qu'à la réalisation de tests d'intrusion et différents types d'audits chez les OIVs (opérateurs d'importance vitale) et au sein de programmes de Défense.
Il est également spécialisé dans la cybersécurité des Systèmes Industriels. Depuis mars 2017, il est Officier de cyber-réserve opérationnelle spécialité cyberdéfense, et à ce titre, il a déjà participé à l'exercice LockShield » organisé par l'OTAN et « DefNet » organisé par l'Etat-major des armées.