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

Mis à jour le 29/11/2023

S'inscrire

Formation Sécurité de l'IoT et 5G

2 jours (14 heures)

PRÉSENTATION

L'émergence du web et des objets connectés ont révolutionné nos modes de vie. La demande en objet connecté a considérablement augmenté ces dernières années.

La sécurité de l'IoT (ou en français, l'Internet des Objets) est un enjeu crucial pour assurer la protection de notre environnement (sécuriser sa maison, sa voiture, etc...).

Une récente étude montre que 90% des consommateurs montrent peu de confiance vis-à-vis des failles de sécurité dans l'IoT. Une enquête réalisée en 2019 dans 6 pays développés dont la France a révélé que 63 % des consommateurs trouvent les appareils connectés "effrayants".

Notre formation sécurité de l'IoT vous enseignera les bonnes pratiques pour protéger votre architecture IoT afin que vos consommateurs ou collaborateurs aient confiance dans l'utilisation des appareils connectés.

OBJECTIFS

- Connaître les bonnes pratiques pour protéger son architecture IoT
- Connaître les différentes failles de sécurité visant l'internet des objets

PUBLIC VISÉ

- Professionnels de la sécurité IT
- Personnes intéressées par les aspects de sécurité liés au hardware ou à l’embarqué
- Amateurs ou professionnels en électronique

Pré-requis

- La maîtrise de Linux en ligne de commande est un plus
- Administration Windows/Linux

PROGRAMME DE NOTRE FORMATION SÉCURITÉ DE l'IOT et 5G

Les fondements d'une architecture IoT sécurisés

- Une brève revue de l'historique et des évolutions des technologies IoT
- Le Data Model dans les systèmes IoT – définition et architecture des sensors, des terminaux, des protocoles de communications
- Risques induits par les services de Supply Chain
- L'écosystème IoT – Les fournisseurs de terminaux, les fournisseurs de gateway, les fournisseurs d'analytics, les fournisseurs de plateformes, les intégrateurs - Les risques associés
- Introduction aux protocoles de communication IoT – Zigbee/NB-IoT/5G/LORA

Revue des menaces informatiques envers les objets connectés

- Firmware Patching
- Revue de Sécurité détaillée des risques connus sur ces protocoles de communication (Zigbee/NB-IoT/5G/LORA) et des layers applicatifs (MQTT)
- Vulnérabilités dans les Gateway
- Vulnérabilités avec les terminaux connectés - Communication avec les Gateway
- Vulnérabilités dans la couche applicative
- Risque inhérent au log management

Le modèle OSASP

- I1 Interface web non sécurisée
- I2 Autentication ou Autorisation insuffisante
- I3 Services réseau non sécurisé
- I4 Manque de cryptage pour le transport
- I5 Problème de confidentialité
- I6 Interface Cloud non sécurisée
- I7 Interface mobile non sécurisée
- I8 Configurabilité insuffisante
- I9 Software/Firmware non sécurisé
- I10 Faible sécurité physique

Études de cas

- Étude de cas concernant l'attaque du 21 octobre 2016
- Les attaques buffer overflow sur les caméras de surveillance
- Le hack du protocole ZigBee
- Les injections SQL
- Cross-Site Scripting (XSS)

Les meilleurs pratiques pour une architecture IoT sécurisée

- Suivre et identifier tous les services connectés à une Gateway
- L'utilisation des adresses MAC
- L'utilisation des hiérarchies d'identification pour les terminaux
- Sécuriser les risques des portails de management d'IoT
- Sécuriser les APIs
- Identifier et intégrer les principes de sécurité dans la chaîne de logistique (Supply Chain)
- Minimiser les vulnérabilités des IoTs par des stratégies de Patch Management

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.