Enjeux de la cybersécurité dans les réseaux 5G

Cette formation sur les enjeux de la cybersécurité dans le contexte des réseaux 5G permet d'évaluer les risques de sécurité associés et de comprendre les principes et les mécanismes de sécurité en particulier dans les nouveaux réseaux 5G.

Domaine(s) : **Production des services**
Niveau(x) : **Spécialisation**
Durée : **2 jours**
Public(s) : **Tout public**
Référence : **PS800**

Fiche valable au 22/02/2024

NOS TARIFS

Inter entreprises :
620 € H.T. par jour et par personne
Intra entreprise en présentiel :
2 225 € H.T. par jour de formation, groupe de 8 personnes maximum
Intra entreprise à distance :
2 225 € H.T. par jour de formation, groupe de 6 personnes maximum
Cours particulier :
1200 € H.T. (1 personne) par jour, dans nos locaux en région parisienne ou à distance
Frais de déplacement du formateur en supplément pour toute action de formation réalisée hors Paris et petite couronne.

Objectifs

À l'issue de cette formation, les bénéficiaires seront capables de :

- Comprendre les notions de base et les techniques essentiels de la cybersécurité.
- Identifier les menaces de sécurité en informatique et en télécoms
- Adopter les bonnes pratiques pour protéger les réseaux mobiles
- Conjuguer la technologie 5G avec l'intelligence artificielle et le Big Data
- Connaitre les différentes mesures de sécurité et standards pour avoir une infrastructure et un système d'information sécurisé.

Programme

RAPPELS SUR L'ARCHITECTURE ET LES FONCTIONNALITÉS DE LA 5G

- Topologie et scénarios de déploiements de réseau décentralisé 5G
- Les éléments du cœur de réseau (AUSF, AMF, SMF, UPF, SMF, UDM…)
- Software Defined Network (SDN) et Network Function Virtualization (NFV) : principes de virtualization, le Cloud RAN, etc.
- Place de l'Open Ran, exemples, perspectives et risques
- Gestion de la QoS, concept de network slicing, marchés verticaux et services critiques

CONCEPTS FONDAMENTAUX DE LA SÉCURITÉ INFORMATIQUES

- Concepts de bases : La triade CIA (Confidentiality, Integrity, Availability)
- Gestion du risque : vulnérabilité, menace, risque
- Principes de base : connaître son SI, moindre privilège, défense en profondeur, prévention et détection
- Concepts de la cryptographie : chiffrement, hachage, signature et TLS
- Standard de sécurité de l'information : ISO 27001
- Techniques de test : Tests de pénétration et scan de vulnérabilités

STRATÉGIES ET GESTION DES RISQUES EN CYBERSÉCURITÉ

- Menaces et conséquences des attaques Cyber
- Benchmarking des techniques en Cybersécurité et Cyberdéfense
- Investigations digitales et géopolitique de la Cyber
- Éthique de la société digitale et de l'entreprise 4.0
- Gestion de la sécurité des usages numériques et conduite des audits en cybersécurité
- Méthodologie d'analyse cybersécurité (type EBIOS)

COGICOM - Vos formations télécoms
128 rue Amelot - 75011 PARIS — www.cogicom.com
Contact : info@cogicom.com, +33 1 60 07 62 05 © Cogicom 2024

DIFFÉRENTES TYPES DE MENACES, ATTAQUES ET VULNÉRABILITÉS EN 5G

- Typologie des menaces
- Menaces et risques cyber pour les opérateurs télécoms et les TPE-PME
- Risques liés aux terminaux et attaques de tempêtes de signalisations
- Failles du protocole et attaques basées sur GTP (GPRS Tunneling Protocol)
- Virtualisation des réseaux 5G et augmentation des risques de failles de sécurité
- Vulnérabilités du protocole Internet mobile en 4G/5G
- Tracking des abonnées avec des attaques de Paging, IMSI catcher, etc.

MÉCANISMES DE SÉCURITÉ DANS LES RÉSEAUX 5G

- Vue d'ensemble sur les bonnes pratiques de sécurité dans les réseaux mobiles
- Challenges de sécurité dans les interfaces radio des réseaux télécoms
- Confidentialité des abonnés et la gestion centralisée des identités
- Mécanisme de sécurité en roaming
- Les principales mesures de protection contre les cyberattaques en 5G
- Sécurité du Wi-Fi 5G

SÉCURITÉ EN BIG DATA DANS LE CONTEXTE 5G

- Gouvernance et gestion des données en Big Data
- Technologies analytiques au service de la cybersécurité
- Valorisation de la data avec la 5G et cloud computing
- État de lieu des menaces de sécurité en Big Data
- Gestion et mécanismes de sécurité dans le contexte Big Data en 5G
- Norme de sécurité IoT : 62443, EN 303 645

Méthodes, modalités d'évaluation

Les exposés théoriques sont illustrés d'exemples concrets et de représentations schématiques.

L'atteinte des objectifs est contrôlée tout au long de la formation par des jeux de questions-réponses et des discussions, permettant d'intégrer les notions de cybersécurité en 5G.

Des quizz ludiques à différentes étapes de la formation apportent à chacun la vision de son avancement et sont des occasions d'approfondir certains points.

Le support de formation reproduisant les slides projetées, est remis aux participants.

Personnes concernées, prérequis

Techniciens supérieurs, ingénieurs spécialistes en radio mobile ou en informatique, et consultants experts chez les opérateurs télécoms.

Cette formation requiert une connaissance de base du domaine. Il peut s'agir d'un apprentissage général acquis par la pratique ou d'une connaissance plus théorique qui doit être approfondie.

En particulier, une connaissance des réseaux mobiles et de leur fonctionnement est souhaitable.

Les conditions générales de vente associées à cette formation sont disponibles sur le site www.cogicom.com

COGICOM - Vos formations télécoms
128 rue Amelot - 75011 PARIS — www.cogicom.com
Contact : info@cogicom.com, +33 1 60 07 62 05 © Cogicom 2024