



ITgate
Training

Your Gateway to Excellence

Formation Sécurité Informatique et Réseaux

Description de la formation Sécurité Informatique et réseaux

Concrète et complète, cette formation Sécurité Informatique et Réseau constitue une introduction à la sécurité des briques techniques fondamentales présentes dans toutes les infrastructures systèmes, réseaux et applicatives des Systèmes d'Information de l'entreprise.

Au cours de cette formation, nous vous expliquerons le fonctionnement des différentes infrastructures des systèmes d'information, ainsi que les failles de sécurité auxquelles toute entreprise est exposée, quelle que soit sa taille.

Vous découvrirez les leviers sur lesquels agir pour se protéger, et comprendrez ainsi pourquoi la transformation digitale des entreprises couplée à la place grandissante du Cloud dans les architectures doit être accompagnée de mesures de sécurité spécifiques à chaque outil ou fonctionnalité : infrastructure, postes de travail, annuaire d'entreprise, téléphonie, messagerie, Office 365, G Suite, applications, toutes les variantes « as a service », etc.

Le but est de vous apporter une vue claire et objective sur la sécurité afin d'échanger avec les acteurs internes et externes du système d'information de votre entreprise.

Objectifs

À l'issue de cette formation Sécurité Informatique et Réseau, vous serez à même de :

- Comprendre le fonctionnement des infrastructures (LAN, postes de travail, systèmes d'information, serveurs)
- Comprendre la place du cloud et ses solutions pour l'entreprise
- Connaître les outils et les méthodes de sécurisation des systèmes
- Connaître les différents types d'attaques informatiques et leur fonctionnement

À qui s'adresse cette formation ?

Public :

Ce cours Sécurité Informatique et Réseau de premier niveau s'adresse à toute personne désirant comprendre en quoi consiste la sécurisation du SI de l'entreprise.

Prérequis :

Pour suivre cette formation Sécurité Informatique et Réseau, il est important d'avoir une expérience préalable et quotidienne sur un poste de travail en réseau (navigateur WEB, explorateur de fichiers, messagerie, etc.). La formation Sécurité Informatique pour Non-Informaticien : Vocabulaire, Concepts et Technologies (Réf. SINI) peut également constituer un bon prérequis.

Contenu du cours Sécurité Informatique et Réseaux

La sécurité dans le contexte de l'infrastructure système (OS)

Comptes utilisateurs, groupes et droits sur les ressources

L'annuaire Active Directory de Microsoft

Intégration de postes informatiques dans l'annuaire

Stratégies de sécurité appliquées aux ordinateurs et utilisateurs de l'annuaire

Authentification LDAP et SSO

Travailler sous Linux au quotidien (Shell, processus, navigation dans l'arborescence)

La virtualisation d'un OS (système d'exploitation) et les impacts au niveau sécurité

Sécurité et Fonctionnement des sites/applications web

Les modes de fonctionnement des applications (connecté / déconnecté, synchrone / asynchrone)

Comment une application « utilise » le réseau ?

Les échanges entre un navigateur et un site / application web (http)

Rôle du firewall dans l'architecture applicative de l'entreprise

Mot de passe de compte utilisateur sur les sites web

Exécution de script, contrôle activeX, applet java nuisibles

L'hameçonnage

L'usurpation d'une session web

Les bons réflexes en cas d'attaque

Travaux pratiques

Visites de sites web malveillants depuis des machines virtuelles

Exemple d'attaque par injection SQL dans un formulaire web

Sécurité du Cloud pour l'entreprise

Liens entre Cloud, Datacenter et Virtualisation

Intégrer tout ou partie de l'infrastructure d'entreprise dans le Cloud (cloud hybride)

Vocabulaire associé : IaaS, PaaS, SaaS

Les offres du marché : Azure, Amazon, G Suite, Apps, Office 365, etc.

Est-on mieux protégé dans le Cloud ?

Travaux Pratiques

Démonstration d'un serveur Microsoft dans le Cloud abritant un annuaire d'entreprise (AD)

Mise en place de la sécurité dans l'annuaire AD sur le Cloud

Architecture et services réseau

Comprendre le réseau et son vocabulaire de base : adresse IP publiques/privées, masque, passerelle, routage, DHCP, DNS

Comment relier de manière fiable et sécurisée le réseau Wifi au réseau local

Gestion de la sécurité des équipements mobiles en entreprise (BYOD, MDM, etc.)

Capital Social: 50000 DT **MF:** 1425253/M/A/M/000 **RC:** B91211472015

Tél. / Fax.: +216 73362 100 **Email:** contact@itgate-training.com **Web:** www.itgate-training.com

Adresse : 12 Rue Abdelkadeur Daghrir - Hammam Sousse 4011 – Tunisie

Sécurisation du réseau

Philosophie d'un firewall (règles)

Philosophie et apport d'une DMZ

Éléments de cryptographie

Principes de fonctionnement d'un VPN (Virtual Private Network)

Architecture et apports des certificats

Architecture et apports d'un serveur d'authentification (RADIUS)

Travaux Pratiques

Connexions à un réseau d'entreprise avec un VPN

Exemple de règles de firewall relatives aux applications

Les attaques informatiques

La faille humaine (ingénierie sociale)

Typologie des différents mails malveillants

Comprendre le fonctionnement des Virus, Antivirus, Malwares, Ransomwares

Protection par défaut de Windows : où en est-on ?

L'espionnage de trames réseaux (sniffing)

Saturer un service volontairement (Déni de Service)

Piratage de session (Hijacking)

Hacking de serveur web

Le ciblage des équipements mobiles

Apports d'un MDM (Mobile Device Management)

Risques avec les objets connectés (IoT)

Travaux Pratiques

Exemples de journaux avec traces d'attaques sur un firewall

Exemple de prise en main d'un serveur web sous Linux sans le mot de passe associé si certaines conditions ne sont pas respectées

Panel de mails malveillants et « dégâts » associés (réalisés sur des machines virtuelles isolées donc sans risque de propagation)

Observation de serveurs en production exposés sur le web (applications disponibles et vulnérabilités)



Capital Social: 50000 DT **MF:** 1425253/M/A/M/000 **RC:** B91211472015
Tél. / Fax.: +216 73362 100 **Email:** contact@itgate-training.com **Web:** www.itgate-training.com
Adresse : 12 Rue Abdelkadeur Daghrir - Hammam Sousse 4011 – Tunisie