Sécurité informatique : vocabulaire, concepts et technologies pour non-initiés

Comprendre la sécurité informatique

Présentiel ou en classe à distance

2 jours (14 h)

Prix inter : 1.690,00 € HT
Forfait intra : 4.290,00 € HT

Réf.: SR105

La sécurité informatique est devenue un enjeu incontournable face à la multiplication des menaces numériques : malwares, attaques réseau, phishing, ransomwares, vols de données ou failles applicatives. Comprendre les concepts clés comme la **confidentialité, l'intégrité, la disponibilité, la traçabilité et la résilience** est essentiel pour toute organisation qui souhaite protéger ses systèmes d'information.
Ce parcours offre une vision claire et accessible des **technologies de cybersécurité**: antivirus, EDR/XDR, pare-feux nouvelle génération, segmentation réseau (VLAN), VPN, IAM, DLP, SIEM ou encore SOC. Il met également en lumière les **référentiels de sécurité** (ANSSI, NIST, ENISA, RGPD, NIS2) et les tendances majeures, de l'**intelligence artificielle appliquée à la cybersécurité** jusqu'aux apports de la **blockchain et du quantique**.

A qui s'adresse cette formation ?

Pour qui

- Commerciaux, spécialistes du marketing, futurs consultants, chefs de projets ou responsables de formation amenés à évoluer dans l'univers de la sécurité informatique
- Toute personne souhaitant comprendre la sécurité informatique pour optimiser leur collaboration avec les spécialistes du domaine

Prérequis

- Aucun.

Programme

1 - Sécuriser dans les principaux domaines

- Domaines de la sécurité traditionnelle : intégrité, disponibilité, confidentialité, authentification, imputation, traçabilité, résilience...
- Domaine de la Cybersécurité : réseaux, systèmes, applicatifs, cryptographie...
- Notions à connaître : authentification Multi-facteurs, défense en profondeur et périmétrique, PRA/PCA...

2 - Se protéger contre les malwares et les attaques

- Malwares : cheval de Troie, Virus, Rootkit, Spyware...
- Attaques : terminal, réseaux, applications (Sniffing, DCI/DCI, DDoS...)

- Attaques de mots de passe, injection SQL, vol d'identité et de données
- Attaques non-malwares : attaques de phishing (hameçonnage)
- Évaluation des risques

3 - Connaître le fonctionnement des solutions de sécurité pour mieux protéger

- Antivirus et EDR/XDR
- Cryptage AES
- Segmentation des réseaux par la formation des réseaux virtuels (VLAN)
- Cryptage des données en ligne (VPN SSL et VPN IPSec)
- Authentification d'accès : authentification forte, Network Access Control (NAC) et Role Based Access Control (RBAC)
- Filtrage : firewalls protocolaires, de contenus, d'applications, d'identité...
- Filtrage des applications Web : WAF (Web Access Firewall)
- SIEM (Security Information and Event Management)
- AM (Identity et Access Management)
- DLP (Data Lost Prevention) - Data Masking – Cryptage
- Empreintes logicielles et MAC (Mandatory Access Control)
- SOC : Security Operations Center
- Autres domaines spécifiques

4 - Exploiter les plates-formes spécialisées de sécurité

- Plate-forme de Cloud de Sécurité (SecaaS : Security as a Service)
- Plate-forme de gestion et de sécurité des mobiles EMM (Entreprise Mobility Management)
- Plate-forme de sécurité NGFW (Next Generation of Firewall)

5 - Utiliser la combinaison des équipements pour sécuriser

- L'Internet (communication et transaction) : cryptologie PKI (Public Key Infrastructure)
- Les réseaux sans-fil Wifi : 802.11i (802.1X/EAP...) / WPA / WPA2 / WPA3
- Terminaux et applications mobiles et le télétravail (ODE, conteneurisation, App Stores, empreintes logicielles, App Wrapping...) / Banalisation du terminal et publication d'application (TS-WEB, VDI...)
- Le Cloud et le Big Data (IDA, Anonymisation, encryptions, flux de données...)

6 - Mesurer les impacts de la mise en place de la sécurité sur :

- La performance du système global du système informatique
- L'architecture du système d'information

7 - S'appuyer sur les référentiels pour gérer la sécurité informatique

- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
- ENISA (organisme Européen - gestion des risques), NIST (standards suivis par des grands acteurs du secteur de sécurité)
- NIS2 et LPM
- CSA (Cloud Alliance Security)
- CNIL/RGPD (Obligation Légale de sécurité)
- Critères communs
- CVE

8 - Grandes tendances

- Limites des solutions actuelles de sécurité dans le domaine du numérique
- Cybersécurité : recours à l'intelligence artificielle (IA) et à la Machine Learning (UBA)
- Software Defined Security
- Blockchain et Informatique quantique

Les objectifs de la formation

- Comprendre les concepts, les technologies et les solutions de sécurité des réseaux informatiques pour travailler avec les spécialistes et piloter les prestataires
- Acquérir la vision globale de la sécurité
- Connaître les rôles des intervenants du secteur et leurs métiers
- Identifier les nouveaux enjeux associés à la sécurité informatique

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une description des technologies et concepts illustrée d'exemples de solutions concrètes et des usages actuels
- Un effort particulier de vulgarisation des technologies complexes rendant le séminaire accessible aux non spécialistes de l'informatique et de la sécurité
- 90% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence SR105

Dernières places disponibles Session garantie

Bordeaux

du 22 janv. au 23 janv.	du 26 mars au 27 mars	du 24 sept. au 25 sept.

Marseille

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

Nantes

du 22 janv. au 23 janv.	du 26 mars au 27 mars	du 24 sept. au 25 sept.

Lyon

du 22 janv. au 23 janv.	du 26 mars au 27 mars	du 24 sept. au 25 sept.

Paris

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.
du 26 mars au 27 mars	du 24 sept. au 25 sept.	

Lille

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

Rennes

du 22 janv. au 23 janv.	du 26 mars au 27 mars	du 24 sept. au 25 sept.

Rouen

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

Aix-en-Provence

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

Sophia Antipolis

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

Strasbourg

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

Toulouse

du 22 janv. au 23 janv.	du 11 juin au 12 juin	du 26 nov. au 27 nov.

A distance

du 22 janv. au 23 janv. du 26 mars au 27 mars	du 11 juin au 12 juin du 24 sept. au 25 sept.	du 26 nov. au 27 nov.