Formation Sécurité systèmes et réseaux - Les fondamentaux

Comprendre les concepts pour se protéger des attaques et garantir la fiabilité de vos données

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Avec Internet, les réseaux sont dorénavant ouverts et par conséquent, beaucoup plus exposés aux attaques virales ou autres actes de piratage. Il est donc devenu primordial de savoir faire face à ces différents risques pour protéger les données de l'entreprise et garantir l'intégrité et le bon fonctionnement de son système d'information. Au cours de cette formation, les participants découvriront les principaux concepts liés à la sécurité des réseaux ainsi les outils permettant de protéger les infrastructures d'entreprise.

Référence	RES220
Durée	4 jours (28h)
Tarif	2 890 €HT

Objectifs

| évaluer les risques internes et externes liés à l'utilisation d'Internet
| Identifier les mécanismes qui permettent de garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
| Expliquer les concepts techniques, la sécurité des systèmes d'information

Public

| Responsables de l'informatique
| Administrateurs réseaux
| Techniciens
| Webmasters
| Responsables de la sécurité informatique

Prérequis

| Il est nécessaire d'avoir une bonne connaissance générale des réseaux et des systèmes d'exploitation courants

Programme de la formation

L'environnement
| Le périmètre (réseaux, systèmes d'exploitation, applications)
| Les acteurs (hackers, responsables sécurité, auditeurs, vendeurs et éditeurs)
| La veille technologique
| Les organismes officiels

Les méthodes des attaquants
| Les scénarios d'attaques intrusion, DDOS, ...
| Les attaques sur les protocoles réseaux
| Les faiblesses des services : Web, VoIP, Messagerie
| Le code vandale : virus, vers et chevaux de Troie

La sécurité des accès, Firewall, WAF, Proxy, NAC
| L'accès des stations aux réseaux d'entreprise,802.1X, NAC
| Les différents types de firewalls
| Les règles de filtrage
| Les règles de la translation d'adresse (NAT)
| La mise en oeuvre d'une zone démilitarisée (DMZ)
| La détection et surveillance avec les iDS
| L'intégration d'un firewall dans le réseau d'entreprise

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 21 au 24 juillet 2025
du 8 au 11 septembre 2025

PARIS
du 21 au 24 juillet 2025
du 8 au 11 septembre 2025

AIX-EN-PROVENCE
du 21 au 24 juillet 2025
du 13 au 16 octobre 2025

BORDEAUX
du 8 au 11 septembre 2025
du 1er au 4 décembre 2025

GRENOBLE
du 8 au 11 septembre 2025
du 1er au 4 décembre 2025

LILLE
du 21 au 24 juillet 2025
du 13 au 16 octobre 2025

LYON
du 8 au 11 septembre 2025
du 1er au 4 décembre 2025

NANTES
du 21 au 24 juillet 2025
du 3 au 6 novembre 2025

VOIR TOUTES LES DATES

| La gestion et l'analyse des fichiers log

La sécurité des systèmes d'exploitation
| Le hardening de Windows
| Le hardening d'Unix/Linux
| Le hardening des nomades : IOS / Android

La sécurité des applications avec exemple d'architectures
| Les serveurs et clients Web
| La messagerie électronique
| La VoIP IPbx et téléphones

La sécurité des échanges, la cryptographie
| L'objectif du cryptage et fonctions de base
| Les algorithmes symétriques
| Les algorithmes asymétriques
| Les algorithmes de hashing
| Les méthodes d'authentification (pap, chap, Kerberos)
| Le HMAC et la signature électronique
| Les certificats et la PKI
| Les protocoles SSL IPSEC S/MIME
| Les VPN réseau privé virtuel site à site et nomade

Méthode pédagogique

L'assimilation d'une méthodologie pour la mise en oeuvre d'une sécurité performante des réseaux.Une formation rythmée par une pédagogie qui repose sur des exemples concrets.Les conseils de consultants experts en sécurité du SI.Les participants intéressés par une mise en pratique opérationnelle de la sécurité préfèreront la formation "Sécurité systèmes et réseaux - Mise en oeuvre" (RES211).

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.