

ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Intégrateur sécurité réseaux - Certification Bureau Veritas

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE: 01 85 77 07 07

E-MAIL: inscription@hubformation.com

CISR1

Objectifs

Démontrer les menaces qui pèsent sur les réseaux maîtriser le rôle des équipements de sécurité mettre en oeuvre un réseau sécurisé

Public

| Comprendre les menaces qui pèsent sur les réseaux

Connaitre le rôle des différents équipements de sécurité

| Savoir mettre en oeuvre un réseau sécurisé

Prérequis

| Connaissance du fonctionnement des réseaux informatique

Programme de la formation

Introduction SSI

Le numérique en entreprise

La convergence des réseaux

Les outils d'attaques

Les typologies d'attaques

Les CVE & CVSS

Les attaques APT

| The Unified Kill Chain

Les piliers de la sécurité

Les principes généraux de la sécurité

La sécurité dans le cyber-espace

Les acteurs de la cybersécurité

| La sécurité offensive

Les bases de la cryptographie

| Vocabulaire et objectifs

| Chiffrement de César & chiffrement de Vigenère

| Principe de Kerckhoffs

Le chiffrement symétrique

| Le chiffrement symétrique

Les recommandations de sécurité

| Fonction de hash

Virtual Private Network & Accès sécurisé

| Définition

| Les implémentations VPN

Les protocoles VPN

I IPSEC

| TLS

| Autres protocoles sécurisés : SSH

| TP : Mise en place du VPN IPSec & mise en place de SSH

SESSIONS PROGRAMMÉES

5 jours (35h)

3 790 €HT

A DISTANCE (FRA)

du 28 juil. au 1er août 2025 du 6 au 10 octobre 2025

PARIS

Référence

Durée

Tarif

du 28 juil. au 1er août 2025 du 6 au 10 octobre 2025

AIX-EN-PROVENCE

du 6 au 10 octobre 2025

BORDEAUX

du 6 au 10 octobre 2025

GRENOBLE

du 6 au 10 octobre 2025

LILLE

du 28 juil. au 1er août 2025

LYON

du 6 au 10 octobre 2025

NANTES

du 28 juil. au 1er août 2025

RENNES

du 28 juil. au 1er août 2025

ROUEN

du 28 juil. au 1er août 2025

SOPHIA-ANTIPOLIS

du 6 au 10 octobre 2025

VOIR TOUTES LES DATES

IAM

l Gestion des identités et des accès

IJAAA

Les méthodes d'authentification

| Cycle de vie des accès

Stratégie de gestion des identités

| LDAP

Les modèles de contrôle des accès

Les implémentations

| Focus sur Kerberos

| TP : Mise en place de Kerberos

Pare-feu

| Définition

| Place du pare-feu dans le modèle OSI

Règles de pare-feu

| Pare-feu Stateless et Statefull

| Politique de filtrage

Les limites des pare-feux traditionnels

Les pare-feux nouvelles génération

| Méthodologie de la mise en place d'une politique de filtrage

| Bonnes pratiques d'ordre général

| TP : Étude d'une cartographie et mise en place d'une politique de filtrage

Proxy

| Définition

| Pourquoi un serveur mandataire ?

Le filtrage URL

Les types de proxy

Les implémentations de proxy

| TP : Mise en place d'un proxy et de règles de filtrage

Les architectures de passerelle d'interconnexion

Le concept

La passerelle d'interconnexion selon les niveaux de sécurité

Sécurité des équipements réseaux

| Administration

| Cloisonnement des réseaux

| Sécurisation des ports

Mécanismes liés à la disponibilité

| Synchronisation horaire et horodatage

| Journalisation

| TP : Durcissement de commutateurs et routeurs

Examen blanc : préparation examen final

Evaluation et validation

| Partie théorique et pratique

Le temps destiné au passage de la certification est de 3H.

L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.

| Il peut se dérouler à distance.

L'accès au support de cours, aux travaux pratiques est assuré pendant trois semaines à compter du début de session.

Le passage de la certification doit être réalisé en ce laps de temps.

| En cas d'échec au premier passage de la certification le candidat a la possibilité de réaliser un second passage dans les 15 j suivants le premier passage.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

2/3 01/07/2025

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.

3/3 01/07/2025