

# Sécurité informatique, l'essentiel (BV-ESCYB), certification Bureau Veritas

Cours Pratique de 1 jour - 7h

Réf : SBV - Prix 2024 : 1 140€ HT

Le monde est aujourd'hui digital. Cet écosystème numérique hyper connecté et complexe n'est pas sans danger. Pour l'aborder sereinement, dans sa vie personnelle comme dans sa professionnelle, il est primordial d'avoir une hygiène numérique adaptée et comprise. Cette formation vous apportera les bon réflexes.

## OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les différents acteurs de la cybersécurité en France

Savoir mettre en œuvre les bonnes pratiques de sécurité

Connaître les définitions et les typologies de menace

Connaître les risques pesant sur ma société et savoir les appréhender

Comprendre l'importance de la charte informatique

## CERTIFICATION

Bureau Veritas Certification assure l'examen final de ce programme de formation, délivré par un organisme de formation indépendant. Cet examen permet d'obtenir une certification de personne.

Examen de 30 minutes sur une plateforme à distance, sous forme de QCM.

L'accès au support de cours, aux travaux pratiques est assuré pendant 3 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, le candidat a la possibilité de réaliser un second passage dans les 15 jours suivants le premier.

## PARTENARIAT

La certification est délivrée par Bureau Veritas Certification.

ORSYS et Bureau Veritas Certification se sont associés pour construire une offre de certifications couvrant les principaux domaines de la cybersécurité : architectures sécurisées, sécurité offensive et défensive, sécurité organisationnelle et système de management.

## LE PROGRAMME

dernière mise à jour : 02/2022

### 1) La cybersécurité c'est quoi ?

- Les VIP de la cybersécurité.
- Les acteurs.
- Suis-je un acteur ?
- Gendarme ou voleur ?
- Vocabulaire.

*Travaux pratiques* : Quiz.

## PARTICIPANTS

Tout public.

## PRÉREQUIS

Aucune connaissance particulière.

## COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

## MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

## MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

## MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

## ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

## 2) Les dangers venus d'Internet

- Que trouve-t-on sur moi sur internet ?
- Mot de passe : passoire ou forteresse ?
- Phishing, spear-phishing, ma boîte mail est-elle un espace sûr ?
- La navigation web, un espace de liberté à sécuriser.
- Rouages et mécanique d'une cyberattaque.
- Matériels et protocoles associés.

*Démonstration* : Crack de mot de passe faible, mail piégé, exemple de site vulnérable, OSINT.

## 3) La sécurité en entreprise

- Mon entreprise est-elle vulnérable ?
- La charte informatique : le contrat de sécurité.
- Une hygiène de sécurité.
- Chiffrer ? Vous avez dit chiffrer ?
- Un VPN pour quoi faire ?

*Démonstration* : Protocole en clair vs protocole chiffré, Shodan.

*Quiz guide d'hygiène informatique.*

## 4) La sécurité chez soi

- Télétravail : chez moi je ne risque rien ?
- Mon poste de travail, une mine d'or d'informations.
- Et mon mobile ?
- Où sont mes données ?
- Qui accède à mes données ?
- Comment devenir un maître des bonnes pratiques de sécurité ?

*Travaux pratiques* : Quiz.

# LES DATES

---

CLASSE À DISTANCE

2024 : 22 avr., 19 juil., 18 oct.

PARIS

2024 : 15 avr., 12 juil., 11 oct.