Responsable management des incidents de sécurité (ISO 27035) (BV-CRMIS), certification Bureau Veritas

Cours Pratique de 4 jours - 28h
Réf : BVJ - Prix 2024 : 3 420€ HT

Pour pouvoir se prémunir des menaces il faut maitriser la connaissance de son système et de ses vulnérabilités et pouvoir réagir au mieux lorsqu'un incident de sécurité survient. Cela est possible en suivant des recommandations internationales, notamment celle de la norme ISO 27035.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre le processus de gestion des incidents de sécurité de l'information

Acquérir le vocabulaire nécessaire

Mettre en place le management de la gestion des incidents selon la norme ISO 27035

CERTIFICATION

Bureau Veritas Certification assure l'examen final de cette formation, délivrée par un organisme indépendant. Cet examen permet d'obtenir une certification de personne.
Examen de 3 heures en 3 parties, sur une plateforme à distance : QCM, mise en situation sur points spécifiques, et sur cas concrets.
Accès au support de cours et aux travaux pratiques pendant 3 semaines à compter du début de session.
Passage de la certification en ce laps de temps. En cas d'échec, possibilité d'un second passage dans les 15 jours suivants le premier.
Cette certification s'inscrit dans un schéma de certification visant à valider les savoirs requis pour les fiches métiers de l'ANSSI suivantes : consultant en cybersécurité, formateur en cybersécurité, évaluateur de la sécurité des technologies de l'information, responsable SOC, responsable CSIRT, auditeur de la sécurité organisationnelle, RSSI.

PARTICIPANTS

Responsables gestion des incidents de sécurité de l'information, chef de projets sécurité, architecte sécurité, intégrateur sécurité, responsable sécurité, auditeur sécurité.

PRÉREQUIS

Avoir suivi le cours "Intégrateur sécurité réseaux niveau 1 (BV-CISR1), certification Bureau Veritas" réf. SRE ou posséder les connaissances équivalentes.

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.

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) Les normes ISO et la gestion des incidents SI

- Famille ISO 27035.
- ISO 27043 et autres normes.
- Approche structurée.
- Vocabulaire.
- Présentation de la norme ISO 27035-1.
- Présentation de la norme ISO 27035-2.
- Présentation de la norme ISO 27035-3.

Travaux pratiques : Etude des normes et des processus associés, quiz, études de cas.

2) Mise en place du management de la gestion des incidents SI

- Compétences, formation, communication.
- Plan de gestion des incidents SI.
- Création d'une IRT.
- Support technique, tests.
- Définition des objectifs.
- Politiques.
- Ressources.

Travaux pratiques : Mise en pratique des points abordés via une étude de cas. Travail en groupe.

3) Suivi et amélioration

- Détection et rapport.
- Evaluation et décisions.
- Réponses.
- Analyses.
- Rapport final et conclusion.
- Amélioration continue.

Travaux pratiques : Mise en pratique des points abordés via une étude de cas. Travail en groupe.

4) Examen

- Révisions.
- Passage de l'examen.

LES DATES

CLASSE À DISTANCE
2024 : 09 avr., 16 juil., 08 oct.

PARIS
2024 : 02 avr., 09 juil., 01 oct.