Analyste forensique digital niveau 1 (BV-CAFD1), certification Bureau Veritas

Cours Pratique de 5 jours - 35h
Réf : FRB - Prix 2024 : 3 890€ HT

OBJECTIFS PÉDAGOGIQUES

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

Comprendre le forensique et ses enjeux

Savoir mener une investigation forensique avec méthodologie

Prendre en main les outils de l'analyse forensique

Pratiquer les différents aspects de l'analyse forensique

CERTIFICATION

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.

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) Introduction à la SSI

- Le numérique en entreprise.
- Les risques qui pèsent sur les entreprises.

2) Digital Forensic

- Le forensique et le « Digital Forensics ».
- Comment est apparu le Digital Forensic.
- Les enjeux du forensique pour une entreprise aujourd'hui.
- Mener une investigation forensique : La méthodologie.
- Le contexte d'une investigation : judiciaire, réponse à incident, scientifique, threat intelligence.
- Les standards d'une investigation forensique.
- Les métiers du Digital Forensic.

3) L'analyse forensique réseau

- Les cas d'utilisation de la forensique en réseau.
- Les types de sources de données.
- Les équipements sur lesquels collecter les sources de données.
- Les protocoles réseau à surveiller.
- Les traces laissées par une attaque sur le réseau (exemple d'une attaque).
- Boîte à outils de criminalistique réseau.

Travaux pratiques : Prise en main de WIRESHARK et étude de PCAP.

PARTICIPANTS

Administrateurs système et réseau, ingénieurs système et réseau, développeurs ayant des bases en SSI, responsables sécurité, responsables gestion des incidents, analystes incidents de sécurité.

PRÉREQUIS

Connaissances des bases des réseaux, des bases systèmes Linux et Windows, des bases de la SSI. Quelques connaissances en développement peuvent être un plus.

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.

4) L'analyse forensique des journaux

- L'utilité de l'analyse des journaux.
- Les types de journaux.
- L'importance de l'horodatage.
- L'analyse des journaux traditionnels.
- Les outils d'analyse des journaux traditionnels.
- L'analyse des journaux modernes : les SIEM.
- Les éditeurs de SIEM.
- La méthodologie de l'analyse des journaux.

Travaux pratiques : Prise en main de Kibana et analyse forensique des journaux dans la pratique.

5) L'analyse forensique mémoire

- Qu'est-ce que l'analyse mémoire.
- Pourquoi faire une analyse mémoire.
- Faire un dump mémoire : les outils.
- La méthodologie de l'analyse mémoire.

Travaux pratiques : Prise en main de volatility et analyse de dump de systèmes infectés.

6) L'analyse de disque dur

- Qu'est-ce que l'analyse de disque dur.
- Pourquoi faire une analyse du disque dur.
- Faire une copie du disque dur : les outils.
- Les systèmes de fichiers.
- La méthodologie de l'analyse de disque dur.

Travaux pratiques : Prise en main d'Autopsy et analyse de disque dur Windows et Linux.

7) L'analyse de fichiers

- Qu'est-ce que l'analyse de fichiers.
- Pourquoi faire une analyse de fichiers.
- Les types de fichiers.
- Anatomie d'un des types de fichiers.
- La méthodologie de l'analyse de fichier.
- Les outils.

Travaux pratiques : Analyse de fichiers malveillant.
Exercice final : analyser un environnement compromis.

8) Examen

- Révisions, examen blanc.
- Examen final.

LES DATES

CLASSE À DISTANCE
2024 : 04 mars, 15 avr., 08 juil., 14 oct.

PARIS
2024 : 08 avr., 01 juil., 07 oct.