Formation Analyste forensique réseaux (BV-CAFRX), certification Bureau Veritas

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

Les cyber attaques font parties du lot quotidien du monde de l'entreprise et du numérique. Il devient alors vital de pouvoir investiguer sur le cyber crime et retrouver tous les éléments utiles pour réagir et être recevable devant la loi. Le réseau est une des pistes d'investigation.

Référence	BVW
Durée	5 jours (35h)
Tarif	3 750 €HT
Repas	repas inclus

Objectifs

| Identifier 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

Public

| Administrateur système et réseau, ingénieur système et réseau, responsable sécurité, responsable gestion des incidents, analyste Incident de sécurité.

Prérequis

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

Programme de la formation

Introduction à la forensique réseau
| Relation avec les autres domaines de la forensique.
| Les différents types de preuves.
| Relation avec les NIDS/IPS.
| Collecte de preuves.
| Outils.
| Travaux pratiques : Analyse d'attaques avec wirershark, règles NIDS/IPS, collecte de preuves.

Journalisation et surveillance
| Principes.
| Conditions préalables pour l'analyse.
| Analyse de la chronologie.
| Agrégation et corrélation des sources.
| Collecte et stockage du trafic.
| Principes juridiques.
| Collecte et analyse de logs, réalisation de timelines.

Détection
| Distinguer le trafic malveillant.
| Détecter les intrusions.
| Threat intelligence.
| Mise en situation d'intrusions, détection et mise en place de modèles.

Analyse et interprétation des données

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 1er au 5 juillet 2024
du 9 au 13 septembre 2024
du 9 au 13 décembre 2024

PARIS

du 24 au 28 juin 2024
du 2 au 6 septembre 2024
du 2 au 6 décembre 2024

VOIR TOUTES LES DATES

| Méthodologie.
| Vue d'ensemble.
| Chaine de contrôle.
| Rapports.
| Leçons apprises.
| Amélioration continue.
| Travaux pratiques : Analyser un environnement compromis. Rapport d'analyse.

Examen
| Révisions.
| Passage de l'examen.

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.

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.