Analyste SOC

Surveiller le SI et détecter les activités suspectes ou malveillantes - Certification incluse

Présentiel ou en classe à distance

5 jours (35 h) | Prix inter : 3.790,00 € HT | Réf.: CAS01

L'évolution du tout numérique et du tout connecté engendre une augmentation notable des cybermenaces. Être en mesure d'identifier au plus tôt et de traiter les cybermenaces est aujourd'hui un impératif pour toutes les organisations. Parmi les dispositifs sur lesquels elles peuvent s'appuyer, le SOC (Security Operations Center) est certainement le plus efficace. Cette formation certifiante vise à founir les savoirs fondamentaux nécessaires pour bien aborder le métier d'Analyste SOC. Elle permet de valider des savoirs décrits dans les fiches métiers de l'ANSSI (SOC Opérateur, Analyste SOC, Responsable du CSIRT, Analyste réponse aux incidents de sécurité, Gestionnaire de crise de cybersécurité et Analyste de la menace cybersécurité). Cette formation prépare à la certification Bureau Veritas - Analyste SOC Niveau 1 et inclus le voucher pour passer l'examen.

A qui s'adresse cette formation ?

Pour qui

- Techniciens et administrateurs système et réseau
- Intégrateur de la sécurité
- Analyste SOC niveau 1
- Responsable SSI
- Ingénieurs SSI
- Chefs de projets techniques

Prérequis

- Connaissances en sécurité des systèmes et réseau
- Connaissances sur les réseaux et systèmes informatique
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - SOC

- Qu'est-ce qu'un SOC ?
- Objectifs d'un SOC
- Les services et fonctions d'un SOC
- Structures et fonctionnement d'un SOC
- Mise en place d'un SOC

2 - Équipements de détection d'intrusion

- Les NIDS / NDR
- La place du NIDS dans l'architecture
- Mettre en écoute le NIDS
- TP : Étude de PCAP malveillants et récolte des IoC

3 - EDR

- Présentation des règles NIDS / EDR
- TP : Mise en place de règles et détection d'attaque
- Les HIDS / EDR
- TP : Détection d'attaque avec un EDR

4 - SIEM

- Qu’est-ce qu’un SIEM
- Les objectifs d’un SIEM
- Les architectures de SIEM
- Les outils SIEM
- TP : Mise en place d’un SIEM et collecte des événements
- Les règles SIEM
- TP : Mise en place de règles SIEM
- Introduction à l’investigation avec SIEM
- TP : Investigation avec SIEM

5 - Examen blanc : préparation examen final

6 - 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.
- 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.

Les objectifs de la formation

- Savoir mettre en oeuvre les solutions de prévention et de détection d’intrusions
- Être en mesure d’analyser des attaques et en extraire les IoC
- Comprendre le fonctionnement d’un SOC
- Savoir mettre en oeuvre et utiliser un SIEM

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une formation orientée sur la pratique qui intègre de de nombreux TP
- Une formation rythmée durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions. Le passage de l'examen est compris dans le prix de la formation.
- Les retours terrains de consultants expérimentés facilitent la compréhension des sujets abordés

Dates et villes 2026 - Référence CAS01

Dernières places disponibles Session garantie

Rouen

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 7 sept. au 11 sept.

Toulouse

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 16 nov. au 20 nov.

Aix-en-Provence

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 16 nov. au 20 nov.

Paris

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 16 nov. au 20 nov.
du 23 mars au 27 mars	du 7 sept. au 11 sept.	

A distance

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 16 nov. au 20 nov.
du 23 mars au 27 mars	du 7 sept. au 11 sept.	

Marseille

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 16 nov. au 20 nov.

Strasbourg

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 7 sept. au 11 sept.

Lille

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 16 nov. au 20 nov.

Sophia Antipolis

du 19 janv. au 23 janv.	du 15 juin au 19 juin	du 7 sept. au 11 sept.

Lyon

du 23 mars au 27 mars	du 7 sept. au 11 sept.	du 16 nov. au 20 nov.

Rennes

du 23 mars au 27 mars	du 7 sept. au 11 sept.	du 16 nov. au 20 nov.

Nantes

du 23 mars au 27 mars	du 7 sept. au 11 sept.	du 16 nov. au 20 nov.

Bordeaux

du 23 mars au 27 mars	du 7 sept. au 11 sept.	du 16 nov. au 20 nov.