Organisme de formation professionnelle continue
N° agrément : 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
E-mail : contact@oo2.fr

Devenir analyste SOC certifié (C|SA)

Date et durée

Code formation : CSAFR
Durée : 3 jours
Nombre d'heures : 21 heures

Formation avec certification

C|SA : Certified SOC Analyst

Description

Le titre d'analyste SOC certifié (CSA) est une étape importante dans la carrière d'un **professionnel de la cybersécurité**. Elle valide les compétences et les connaissances en matière de surveillance et de gestion des incidents dans un **centre d'opérations de sécurité (SOC)**. Si vous êtes un administrateur ou un analyste débutant spécialisé en sécurité informatique, cette formation est le moyen idéal pour obtenir la certification CSA du EC-Council.
Pendant 3 jours vous commencerez par suivre un cours axé sur **l'essentiel des opérations SOC et la gestion des connaissances**. Par la suite, vous abordez la corrélation des logs, le déploiement SIEM, la détection avancée des incidents et la réponse aux incidents. Pour finir, vous apprendrez à gérer les processus usuels de **traitement d'un incident de sécurité** et découvrirez la collaboration avec un CSIRT en cas de besoin.
À l'issue de cette formation intensive accompagnée de travaux pratiques, vous pourrez vous présenter pour **passer l'examen officiel** via le portail d'examen EC-Council *(plus d'infos dans l'onglet certification).*

Objectifs

A l'issue de la **formation *CSA***, vous atteindrez les objectifs suivants :

- maitriser les processus, les technologies et les opérations du SOC ;
- comprendre les bases et les aspects techniques liés aux menaces de sécurité, aux attaques, aux vulnérabilités, aux comportements des attaquants, à la Cyber Kill Chain, et bien plus encore ;
- identifier les outils, les stratégies et les pratiques des attaquants afin de définir l'indice de compromission (IOC) ;
- surveiller et analyser les logs et les notifications à partir de différentes technologies et sur plusieurs plateformes ;
- acquérir des connaissances sur le processus de gestion centralisé des logs (CLM) ;
- collecter, surveiller et analyser les événements et les logs de sécurité ;
- maitriser l'utilisation des outils SIEM (Splunk,AlienVault,OSSIM,ELK) ;
- connaitre le processus pratique lié à l'utilisation de solutions SIEM ;
- développer des modèles de menaces et rédiger des rapports ;
- connaitre les différents cas d'utilisation couramment appliqués dans le cadre du déploiement d'un SIEM ;
- planifier, surveiller et analyser des menaces au sein d'une entreprise ;
- suivre les modèles de menaces émergents et analyser les menaces de sécurité ;
- connaitre le processus de triage des alertes ;
- remonter des incidents aux équipes concernées afin d'obtenir une assistance plus approfondie ;
- utiliser un système de gestion de tickets (Service Desk) ;

- préparer des briefings et des rapports sur les méthodes d'analyse et les résultats ;
- connaître les méthodes d'intégration des renseignements sur les menaces dans un système SIEM afin d'améliorer la détection des incidents et la réponse aux incidents ;
- exploiter des informations variées, disparates et en constante évolution sur les menaces ;
- maitriser le processus de réponse aux incidents ;
- comprendre le fonctionnement du SOC et de l'IRT afin d'améliorer la réponse aux incidents ;
- réussir l'examen 312-39 et obtenir la certification C|SA du EC-Council.



Oo2 est accrédité par EC-Council pour dispenser la formation CSA. Ce statut garantit la prestation d'un formateur agréé, des supports de cours officiels et des examens de certifications organisés immédiatement en fin de formation.

Points forts

Une formation certifiante sur les activités d'un analyste SOC, des travaux pratiques et une bonne préparation à la certification Certified SOC Analyst (CSA).

Certification

Informations générales

Cette formation de préparation à la certification CSA vous permet de passer l'examen officiel disponible en ligne sur la plateforme EC-Council ECC Exam. **Les frais d'inscription sont inclus dans le prix de cette formation**. Vous recevrez un bon d'examen (voucher). Une fois l'examen réussi, vous obtiendrez le titre de Certified SOC Analyst.

Détail de l'examen C|SA

Code de l'examen : 312-39
Nombres de questions : 100 QCM
Durée : 3 heures
Score de réussite : entre 60 et 85 %
Validité de la certification : permanente

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Certified SOC Analyst (*CSA*),** nécessitent le prérequis suivant :

- avoir minimum 1 an d’expérience professionnelle dans le secteur de l'administration réseau ou de la sécurité informatique.

Public

Cette formation s'adresse aux publics suivants :

- les analystes SOC de niveau 1 ou 2 ;
- les analystes en sécurité des télécommunications, des réseaux et des systèmes informatiques ;
- les ingénieurs systèmes, réseaux et télécoms ;
- tous professionnels chargés de gérer des opérations de sécurité ou de réseau et qui souhaitent se certifier.

Cette formation s'adresse aux profils suivants

Analyste cybersécurité
Responsable sécurité informatique
Ingénieur système
Ingénieur réseaux - télécoms

Programme

Module 1 :

- Les opérations et la gestion d'un centre d'opérations de sécurité (SOC).

Module 2 :

- Les cybermenaces, les systèmes IoC et les techniques d'attaque.

Module 3 :

- Les incidents, les événements et les logs.

Module 4 :

- La détection des incidents grâce à un système de gestion des informations et des événements de sécurité (SIEM).

Module 5 :

- La détection des incidents avec la threat Intelligence.

Module 6 :

- La réponse aux incidents.

C|SA® est une marque déposée de EC-Council aux États-Unis.