

Certified SOC Analyst

Réf. CSA · EC-Council · Cybersécurité ·

Formation certifiante

DURÉE 3 jours	NIVEAU Intermédiaire	MODALITÉS Présentiel · Live · Intra	VOUCHER EXAMEN Inclus
-------------------------	--------------------------------	---	---------------------------------

Présentation

Certified SOC Analyst (CSA) d'EC-Council forme les analystes de niveau 1 et 2 aux opérations quotidiennes d'un centre opérationnel de sécurité. Elle couvre la surveillance, la gestion des logs, l'usage du SIEM et le triage des incidents pour renforcer la détection et la réponse.

Objectifs pédagogiques

- Comprendre l'organisation et les processus d'un SOC
- Analyser les menaces, attaques et méthodologies adverses
- Collecter, corrélérer et analyser les logs de sécurité
- Exploiter un SIEM pour la détection et l>alerting
- Trier, qualifier et escalader les incidents de sécurité
- Intégrer la threat intelligence aux opérations du SOC

Programme détaillé

1. Module 1 — Fondamentaux du SOC

- Composants et rôles d'un SOC
- Processus et workflows opérationnels
- Menaces, attaques et cyber kill chain
- Indicateurs de compromission

2. Module 2 — Journalisation et gestion des logs

- Sources et collecte de logs
- Corrélation d'événements
- Analyse des logs Windows/Linux/réseau
- Cas d'usage de détection

3. Module 3 — SIEM et détection

- Architecture et déploiement d'un SIEM
- Règles de corrélation et alertes
- Détection des incidents et faux positifs
- Threat intelligence et réponse initiale

4. Module 4 — Triage, escalade et reporting

- Triage et qualification des incidents
- Procédures d'escalade
- Intégration avec la réponse à incident
- Reporting et tableaux de bord

Prérequis

Des connaissances de base en réseaux, systèmes et sécurité informatique sont recommandées. Une première expérience en administration ou en support IT est un atout.

Public visé

Analystes SOC de niveau 1 et 2, administrateurs sécurité, techniciens de surveillance et futurs opérateurs de centre opérationnel de sécurité.

Ce qui est inclus

- Courseware officiel EC-Council CSA
- Labs SIEM et analyse de logs
- Voucher d'examen CSA inclus
- Attestation de réussite
- Pauses-café, déjeuner et formateur expert SOC

Certification

Certification CSA (examen 312-39) : QCM de 100 questions à passer en 3 heures. Advancia Training est centre d'examen agréé Pearson VUE / PSI.

1 150 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible