EXPERT

FORMATION CERTIFIANTE

CERTIFIED SOC ANALYST

Un programme certifiant qui atteste d'une solide connaissance des outils, méthodes et processus de gestion d'un SOC pour valoriser vos équipes et rassurer vos clients.

Le programme Certified SOC Analyst (CSA) est la première étape pour rejoindre un SOC - Security Operations Center.
Il est conçu pour les analystes de niveau I et II afin de leur permettre d'acquérir les compétences nécessaires pour effectuer des opérations de premier et deuxième niveau.
Le CSA est un programme de formation et d'accréditation qui aide le candidat à acquérir des compétences techniques recherchées. Le programme met l'accent sur la création de nouvelles possibilités de carrière grâce à des connaissances approfondies et méticuleuses et à des capacités de niveau amélioré pour contribuer de façon dynamique à une équipe SOC.

Ce programme intensif de 3 jours couvre en profondeur les principes fondamentaux des opérations SOC, de la gestion et corrélation des logs, du déploiement SIEM, de la détection avancée des incidents et réponse aux incidents.
De plus, le candidat apprendra à gérer de nombreux processus SOC et à collaborer avec le CSIRT en cas de besoin.

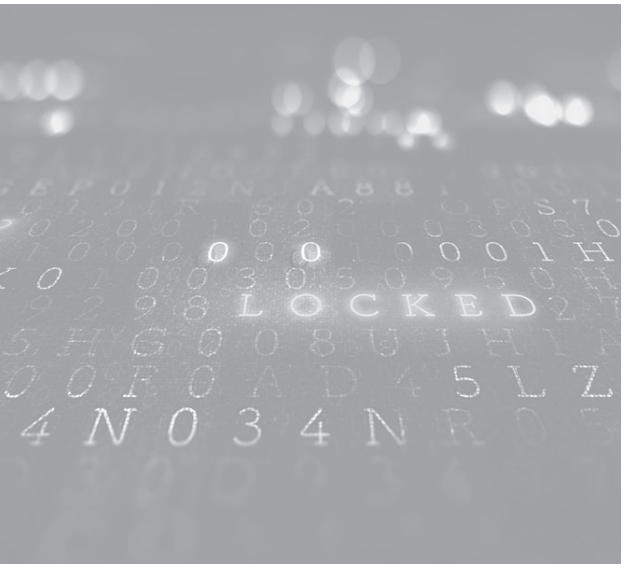
Code : CSA

PROGRAMME

Méthodes mobilisées : cette formati on est construite avec une alternance de cours théoriques et de cas pratiques afi n de favoriser l'acquisiti on des savoirs du programme (cf. Ressources).

Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée.

Puis, les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, puis par le passage de l'examen.



PLAN DE COURS

- **Module 1 :** Security Operations and Management
- **Module 2 :** Understanding Cyber Threats, IoCs, and Attack Methodology
- **Module 3 :** Incidents, Events, and Logging
- **Module 4 :** Incident Detection with Security Information and Event Management (SIEM)
- **Module 5 :** Enhanced Incident Detection with Threat Intelligence
- **Module 6 :** Incidence Response

CERTIFICATION CSA (incluse avec la formation)

Passage de l'examen : l'examen CSA aura lieu à distance, depuis le lieu de votre choix.

- **Titre de l'examen :** Certified SOC Analyst
- **Nombre de questions :** 100
- **Durée :** 3 heures
- **Score requis :** 70%

RÉSULTAT

Directement disponible en fin d'examen.

PROCHAINES DATES

26 février 2025
11 juin 2025
1er octobre 2025
19 novembre 2025

OBJECTIFS

- Comprendre le processus SOC de bout en bout
- Détecter des incidents avec un SIEM
- Détecter des intrusions avec les modèles de menace
- Comprendre le déploiement d'un SIEM

INFORMATIONS GÉNÉRALES

Code : CSA

Durée : 3 jours

Prix : 2 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Analystes SOC (Niveau I et Niveau II)
- Administrateurs de Réseau et Sécurité, Ingénieurs de Réseau et Sécurité, Analyste en Sécurité, Analystes en Défense de Réseau, Techniciens en Défense de Réseau, Spécialistes en Sécurité de Réseau, Opérateur en Sécurité de Réseau, et tout professionnel en sécurité qui s'occupe des opérations de sécurité de réseau
- Analystes en cybersécurité
- Professionnels en cybersécurité débutants
- Quiconque voulant devenir Analyste SOC

PRÉ-REQUIS

- Avoir des connaissances en gestion d'incidents
- Savoir ce qu'est un SOC

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- 20% d'exercices pratiques
- 1 PC par personne