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.

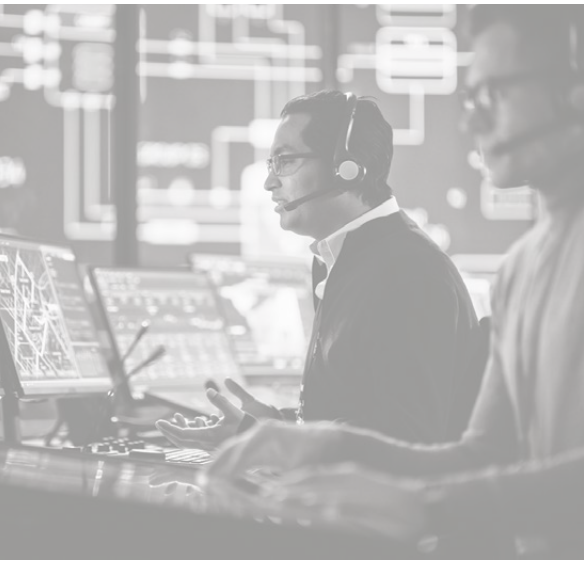
Le programme Certified SOC Analyst (CSA) est la première étape pour rejoindre un SOC - Security Operations Center.
Il est conçu pour les analystes de niveau I et II afin de leur permettre d'acquérir les compétences nécessaires pour effectuer des opérations de premier et deuxième niveau.
Le CSA est un programme de formation et d'accréditation qui aide le candidat à acquérir des compétences techniques recherchées et ce, grâce aux formateurs les plus expérimentés de l'industrie. 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 formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : 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 en fin de module par le formateur, puis par le passage de l'examen.



Plan de cours

- Module 01 : Security Operations and Management
- Module 02 : Understanding Cyber Threats, IoCs, and Attack Methodology
- Module 03 : Incidents, Events, and Logging
- Module 04 : Incident Detection with Security Information and Event Management (SIEM)
- Module 05 : Enhanced Incident Detection with Threat Intelligence
- Module 06 : 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

27 mars 2023,
22 mai 2023,
10 juillet 2023,
18 décembre 2023

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 : 2 600 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
Examen CSA : inclus. Valable 12 mois pour un passage de l'examen à distance.

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 / Internet