CERTIFIED SOC ANALYST V2

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.

Code : CSA v2

Le programme Certified SOC Analyst (C|SA) est un tremplin essentiel pour les personnes qui aspirent à rejoindre ou à progresser au sein d'un centre d'opérations de sécurité (SOC), en se concentrant sur ses fonctions, son développement et sa gestion.
Le cours C|SA fournit une formation et une certification dans les principes et pratiques fondamentaux des opérations de sécurité, du renseignement sur les menaces et de la réponse aux incidents. Il permet de comprendre en profondeur les processus, les technologies et les techniques utilisés pour détecter, enquêter et répondre aux menaces de sécurité.
Le programme de formation Certified SOC Analyst couvre un large éventail de sujets, notamment les vecteurs d'attaque courants, l'utilisation d'outils et de technologies de sécurité, la gestion des informations et des événements de sécurité (SIEM), les processus de réponse aux incidents, la coordination et le développement d'un SOC.
Ce cours vous permet d'acquérir des compétences en matière de gestion centralisée des journaux (CLM), de triage des incidents, de reconnaissance et d'investigation des indicateurs de compromission (IOC) et de la chaîne de la mort cybernétique, ce qui leur permet de réagir de manière proactive aux menaces potentielles.
Ainsi que la capacité à reconnaître les modèles de menaces émergents, de développer des règles de corrélation et de créer des rapports efficaces qui aident les organisations à maintenir une posture de sécurité robuste.
Apprenez également à exploiter les outils et les plateformes basés sur l'IA pour améliorer les capacités SIEM, l'analyse des comportements et la hiérarchisation des alertes, et automatiser la détection et la chasse aux menaces à l'aide de solutions telles que Splunk AI, Elastic AI, Copilot, ChatGPT et PowerShell AI.

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

PLAN DE COURS

- **Module 1 :** Security Operations and Management
- **Module 2 :** Understanding Cyber Threats, IoCs, and Attack Methodology
- **Module 3 :** Log Management
- **Module 4 :** Incident Detection and Triage
- **Module 5 :** Proactive Threat Detection
- **Module 6 :** Incidence Response
- **Module 7 :** Forensic Investigation and Malware Analysis
- **Module 8 :** SOC for Cloud Environments

CERTIFICATION CSA
(incluse avec la formation)

L'examen CSA 312-39 aura lieu à distance.

- **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 9 FEV - 11 MAI - 31 AOÛT - 14 DEC

OBJECTIFS

- Maîtrisez les workflows SOC, l'analyse des menaces, la gestion des journaux et la sécurité
- Acquérir une expérience pratique du SIEM avec Splunk, AlienVault, Elasticsearch, Logstash et Kibana (ELK) tout en maîtrisant le développement de cas d'utilisation, les tableaux de bord et la détection des menaces
- Maîtrisez la réponse aux incidents, l'analyse forensic, le renseignement sur les menaces et la recherche proactive des menaces dans les opérations SOC
- Acquérir une expertise dans le triage des alertes, l'escalade des incidents, l'analyse des logiciels malveillants, la détection des menaces par l'IA/ML et la préparation des rapports de sécurité
- Apprendre à exploiter les outils et les plateformes d'IA

INFORMATIONS GÉNÉRALES

Code : CSA v2

Durée : 3 jours

Prix : 2 790 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) - en présentiel uniquement

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