Certified SOC Analyst (CSA)

Description

Pourquoi choisir la formation Certified SOC Analyst (CSA) ?

La formation Certified SOC Analyst (CSA) est conçue pour les professionnels souhaitant acquérir des compétences en sécurité des systèmes d'information. Ce cours aborde les processus et les technologies clés utilisés dans les centres des opérations de sécurité (SOC), vous permettant d'identifier, d'analyser et de répondre efficacement aux menaces de sécurité. Grâce à une approche pratique et des exercices en temps réel, vous apprendrez à interpréter les événements de sécurité et à maîtriser les outils modernes tels que Splunk et ELK.

Améliorez votre expertise en sécurité informatique

Rejoindre cette formation vous donnera une compréhension approfondie des stratégies de détection des menaces et de gestion des incidents. En apprenant à utiliser les solutions SIEM et en développant vos compétences en réponse aux incidents, vous deviendrez un acteur clé dans la protection des infrastructures critiques. Avec un contenu structuré, orienté sur la pratique, cette formation est un excellent tremplin pour les analystes SOC ou toute personne cherchant à se spécialiser dans la cybersécurité.

Reference
CSA
Contenu du cours
Module 1 : Le centre des opérations de sécurité

- Introduction aux SOC
- Rôles et responsabilités
- Outils utilisés dans les SOC

Module 2 : La cybermenace CIO et les techniques d'attaque

- Comprendre les menaces CIO
- Techniques d'attaque courantes
- Cas pratiques

Module 3 : Les incidents, les événements et la journalisation

- Types d'incidents de sécurité
- Journalisation des événements
- Analyse des logs

Module 4 : La détection des incidents et la gestion des événements

- Outils de détection des incidents
- Gestion des incidents de sécurité
- Bonnes pratiques en gestion des événements

Module 5 : La détection avancée des incidents avec Threat Intelligence

- Utilisation des solutions Threat Intelligence
- Identification des menaces émergentes
- Automatisation de la réponse aux incidents

Module 6 : La réponse aux incidents de sécurité

- Processus de réponse aux incidents
- Collaboration avec les équipes IRT
- Rédaction de rapports d'incidents

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification Certified SOC Analyst (CCSA) +.
- Pour obtenir la certification Certified SOC Analyst (CCSA) +, les candidats doivent réussir l'examen : 312-39.
- Nombre de questions : 150
- Durée : 4 heures
- Si vous souhaitez passer cet examen, veuillez contacter notre secrétariat qui vous informera du coût des examens et prendra en charge toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Analystes SOC
- Analystes en cybersécurité
- Administrateurs réseau
- Professionnels de la sécurité informatique

Connaissances Préalables

- Notions de base en cybersécurité
- Connaissances en réseaux et télécoms
- Compréhension des concepts de journalisation
- Familiarité avec les solutions SIEM

Objectifs

- Maîtriser les fondamentaux du SOC
- Apprendre à surveiller et analyser des fichiers logs

- Identifier les menaces avec les indicateurs IOC
- Administrer les solutions SIEM
- Détecter et gérer les incidents de sécurité
- Élaborer des rapports d’analyse de menaces

Description
Formation Certified SOC Analyst (CSA)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
3950
Prix de l'inscription en Virtuel (CHF)
3800
Durée (Nombre de Jours)
3