EduGroupe
Accompagner pour réussir

Chief Information Security Officer (examen inclus)

Référence : **SECCISO** Durée : **5 jours (35 heures)** Certification : **CISO / EISM**

Connaissances préalables

- Les candidats intéressés par la certification CCISO devront remplir les conditions requises via l'EC-Council's Exam Eligibility avant de s'inscrire à l'examen CCISO. Seuls les stagiaires possédant déjà une expérience d'au moins 5 ans dans trois des cinq domaines pourront passer l'examen CCISO.
- Un stagiaire n'ayant pas cette expérience ou n'ayant pas rempli sa demande pourra passer l'examen Associate CCISO. Une fois les 5 années d'expérience acquises, le candidat pourra s'inscrire à l'examen CCISO.
- Maîtrise de la langue anglaise car le cours est donné en anglais et le support de cours et l'examen sont en langue anglaise

Profil des stagiaires

- RSSI et DSI
- Directeurs sécurité confirmés souhaitant a?rmer leurs compétences par une certification reconnue mondialement
- Aspirants directeurs sécurité souhaitant développer leurs compétences en apprenant à adapter leurs connaissances techniques aux problématiques globales d'entreprise

Objectifs

- Maîtriser les 5 domaines du programme CCISO
- Se préparer à la certification professionnelle CCISO

Certification préparée

Examen CISO pour les stagiaires qui justifient de 5 ans d'expérience dans au moins 3 des 5 domaines.

1. L'expérience est vérifiée via la demande d'admissibilité à l'examen (eligibility form) avant le début de la formation.
2. Format de l'examen : QCM - Nombre de questions : 150 - Durée : 2 heures 30 - Score requis : il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.

Examen EISM (EC-Council Information Security Manager) pour les stagiaires qui n'ont pas encore acquis les 5 années d'expérience pour se présenter à l'examen CCISO.

1. Format de l'examen : QCM - Nombre de questions : 150 - Durée : 2 heures - Score requis : il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Domain 1 – Governance

- Define, implement, manage and maintain Information Security Governance Program
- Information security drivers
- Establishing an information security management structure
- Laws / Regulations / Standards as drivers of Organizational Policy / Standards / Procedures
- Managing an entreprise information security compliance program
- Risk Management
- Risk mitigation, risk treatment and acceptable risk
- Risk management frameworks
- NIST
- Other Frameworks and Guidance (ISO 31000, TARA, OCTAVE, FAIR, COBIT and ITIL)
- Risk management plan implementation
- Ongoing third-party risk management
- Risk management policies and processes Ongoing third-party risk management
- Summary

2. Domain 2 – Security Risk Management, Controls & Audit Management

- Information security controls
- Compliance Management
- Guidelines, good and best practice
- Audit management
- Summary

3. Domain 3 – Security Program Management and Operations

- Program Management
- Operations Management
- Summary

4. Domain 4 – Information Security Core Concepts

- Acces control
- Physical security
- Network security
- Endpoint protection
- Application security
- Encryption Technologies
- Virtualization security
- Cloud computing security
- Transformative technologies
- Summary

5. Domain 5 – Strategic Planning, Finance, Procurement and Vendor Management

- Strategic planning
- Designing, developing and maintaining an Entreprise Information Security Program
- Understanding the Enterprise Architecture (EA)
- Finance
- Procurement
- Vendor management
- Summary

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.