



CATALOGUE

DE FORMATION

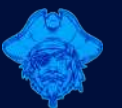
CYBERSÉCURITÉ

FORMATION

Classique



Spécialisée



2026

SOMMAIRE

FORMATION CLASSIQUE

ESSENTIAL SERIES	P.01
CERTIFIED SECURE COMPUTER USER	P.02
CERTIFIED CYBER TECHNICIAN	P.03
CERTIFIED ENCRYPTION SPECIALIST	P.04
CERTIFIED NETWORK DEFENDER	P.13
CERTIFIED ETHICAL HACKER	P.08



FORMATION SPÉCIALISÉE

CERTIFIED SOC ANALYST	P.05
CERTIFIED CLOUD SECURITY ENGINEER	P.06
CERTIFIED THREAT INTELLIGENCE ANALYST	P.07
PENTESTER	P.11
CYBERSECURITY	P.14
EC-COUNCIL CERTIFIED INCIDENT HANDLER	P.15
CASE.JAVA	P.16
CASE.NET	P.17
CERTIFIED ETHICAL HACKER MASTER	P.18
CERTIFIED HACKING FORENSIC INVESTIGATOR	P.19
EC-COUNCIL DISASTER RECOVERY PROFESSIONAL	P.20
EC-COUNCIL CERTIFIED DEVSECOPS ENGINEER	P.21
CERTIFIED CHIEF INFORMATION SECURITY OFFICER	P.22
CERTIFIED PENETRATION TESTING PROFESSIONAL	P.23





ESSENTIAL SERIES

CYBER NOVICE

La série Essentials constitue une porte d'entrée idéale dans l'univers de la cybersécurité. Elle permet d'acquérir les connaissances essentielles à la compréhension des menaces, des technologies et des bonnes pratiques de défense numérique.

Ces modules forment une base solide pour toute personne souhaitant évoluer dans les métiers de la sécurité informatique ou simplement renforcer ses compétences techniques.

OBJECTIFS

- Comprendre les principes fondamentaux de la cybersécurité
- Identifier les menaces et vulnérabilités courantes dans les systèmes informatiques
- Découvrir les principaux domaines techniques : Ethical Hacking, Network Defense, Digital Forensics, Cloud Security, DevSecOps, IoT Security, SOC Essentials, et Threat Intelligence
- Poser les premières bases d'une carrière en sécurité informatique



POURQUOI SUIVRE CETTE FORMATION ?

- Faire ses premiers pas dans le monde de la sécurité informatique
- Explorer plusieurs domaines clés de la cybersécurité avant de se spécialiser
- Acquérir une première expérience structurante ouvrant la voie vers des formations de niveau supérieur

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	●	Français	●



CSCU

CERTIFIED SECURE COMPUTER USER

La formation CSCU (Certified Secure Computer User) vise à sensibiliser les utilisateurs aux enjeux de la sécurité informatique au quotidien. Elle permet de comprendre les menaces présentes sur internet et d'adopter les bons réflexes pour protéger ses données, ses appareils et ses informations personnelles.



OBJECTIFS

- Comprendre les principales menaces informatiques (malwares, phishing, vols de données, etc.)
- Apprendre à sécuriser ses appareils et ses comptes en ligne
- Adopter les bonnes pratiques d'hygiène numérique au quotidien
- Identifier les comportements à risque et savoir réagir en cas d'incident

PUBLIC VISÉ

Cette formation s'adresse à toute personne utilisant un ordinateur, un smartphone ou une tablette, que ce soit à titre professionnel, académique ou personnel. Elle est particulièrement recommandée pour les salariés, étudiants, enseignants et toute personne souhaitant renforcer sa culture numérique.

POURQUOI SUIVRE CETTE FORMATION ?

Dans un monde toujours plus connecté, la sécurité numérique est devenue un enjeu majeur. Le programme CSCU aide chacun à :

- Comprendre les risques liés à l'utilisation d'internet
- Mettre en œuvre des mesures simples mais efficaces pour se protéger
- Réduire les vulnérabilités personnelles et professionnelles



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✓	Français	✓



CCT

CERTIFIED CYBER TECHNICIAN

La certification CCT (Certified Cyber Technician) prépare les apprenants à effectuer les opérations quotidiennes essentielles en cybersécurité.

Elle forme à la fois à la compréhension des fondements techniques de la sécurité informatique et à leur mise en pratique dans des environnements réels.

Grâce à un programme équilibré entre théorie et exercices pratiques, cette formation constitue une excellente première étape vers une carrière dans la cybersécurité opérationnelle.

OBJECTIFS

- Acquérir les compétences de base nécessaires aux métiers techniques de la cybersécurité
- Comprendre les principes de la sécurité des réseaux, de la gestion des incidents et de l'informatique légale
- Maîtriser les notions clé de la sécurité de l'information et des infrastructures
- Développer une approche pratique grâce à des laboratoires concrets représentant 50 % de la formation



PUBLIC VISÉ

- Toute personne souhaitant débiter ou se réorienter vers une carrière en sécurité informatique
- Les étudiants et jeunes diplômés désirant acquérir une première expérience technique
- Les professionnels IT souhaitant renforcer leurs compétences dans la sécurité des systèmes et réseaux

POURQUOI SUIVRE CETTE FORMATION ?

- Répondre à la demande croissante de techniciens qualifiés en cybersécurité
- Obtenir une vision globale et opérationnelle des domaines de la sécurité (réseaux, gestion d'incidents, forensic, etc.)
- Développer des compétences techniques concrètes grâce à une formation orientée sur la pratique

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✓	Français	✓



ECES

EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST

La formation ECES (EC-Council Certified Encryption Specialist) offre une introduction complète à la cryptographie et à ses applications dans la sécurité informatique moderne. Elle permet aux participants de comprendre les concepts fondamentaux du chiffrement, les algorithmes clé utilisés dans l'industrie, ainsi que les méthodes de mise en œuvre de la cryptographie pour protéger les données et les communications.

OBJECTIFS

- Comprendre les principes fondamentaux de la cryptographie et leurs cas d'application
- Découvrir les types de chiffrement symétrique et asymétrique
- Étudier les algorithmes modernes tels que Feistel, DES, AES et RSA
- Savoir appliquer la cryptographie à des contextes concrets (VPN, certificats numériques, authentification sécurisée)



PUBLIC VISÉ

- Toute personne souhaitant débiter ou se réorienter vers une carrière en sécurité informatique
- Les étudiants et jeunes diplômés désirant acquérir une première expérience technique
- Les professionnels IT souhaitant renforcer leurs compétences dans la sécurité des systèmes et réseaux

POURQUOI SUIVRE CETTE FORMATION ?

- Découvrir la cryptographie et ses usages concrets dans la cybersécurité moderne
- Comprendre la logique des algorithmes de chiffrement et leur importance dans la protection des données
- Acquérir des compétences techniques recherchées pour les métiers du pentest, du SOC ou de la sécurité des réseaux

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CSA

CERTIFIED SOC ANALYST

SÉCURITÉ DÉFENSIVE – LES BASES POUR REJOINDRE UN SOC

La certification CSA (Certified SOC Analyst) forme les professionnels aux compétences essentielles pour intégrer un Security Operations Center (SOC). Elle permet d'acquérir une compréhension approfondie des opérations de sécurité, de la surveillance des réseaux à la réponse aux incidents, en passant par la gestion des menaces. Cette formation constitue la première étape pour devenir un analyste SOC compétent et autonome.

OBJECTIFS

- Comprendre le fonctionnement d'un SOC et le rôle de l'analyste dans la chaîne de défense
- Apprendre à utiliser les outils de surveillance et d'analyse de logs (SIEM)
- Savoir détecter, analyser et répondre efficacement aux incidents de sécurité
- Maîtriser les techniques de corrélation, de gestion et d'investigation des alertes
- Développer les compétences nécessaires pour intégrer une équipe SOC de niveau 1 ou 2

PUBLIC VISÉ

- Les analystes SOC (Tier I et Tier II) souhaitant consolider leurs bases
- Les administrateurs, ingénieurs et analystes réseau ou sécurité
- Tout professionnel IT impliqué dans les opérations de sécurité réseau
- Les personnes désirant démarrer une carrière dans un SOC



Suivre la formation CSA – Certified SOC Analyst constitue une étape essentielle pour toute personne souhaitant intégrer un Security Operations Center (SOC).

Ce programme offre une compréhension complète des principes fondamentaux des opérations de sécurité, tout en développant une maîtrise pratique des outils et méthodes utilisés dans la surveillance, la détection et la réponse aux incidents.

Grâce à une approche concrète et structurée, cette formation permet d'acquérir une base solide en cybersécurité défensive, préparant ainsi les participants à évoluer vers des rôles plus spécialisés et stratégiques au sein d'équipes de sécurité avancées.



Langue de l'examen Langue de la formation

Anglais ✓

Français ✗

Anglais ✓

Français ✗



CCSE

CERTIFIED CLOUD SECURITY ENGINEER

SÉCURITÉ CLOUD – AZURE, GCP ET AWS COUVERTS

La certification CCSE (Certified Cloud Security Engineer) forme les professionnels à la mise en place, la gestion et la sécurisation des environnements cloud multi-plateformes.

Cette formation aborde les aspects essentiels de la sécurité sur les trois grands fournisseurs de services cloud – AWS, Microsoft Azure et Google Cloud Platform (GCP) – afin de maîtriser les meilleures pratiques, outils et stratégies de protection des infrastructures et données dans le cloud.

OBJECTIFS

- Comprendre les principes fondamentaux de la sécurité dans le cloud
- Apprendre à sécuriser les infrastructures et services déployés sur AWS, Azure et GCP
- Identifier et atténuer les vulnérabilités spécifiques aux environnements cloud
- Maîtriser la conformité, la gestion des accès et la gouvernance multi-cloud
- Développer des compétences pratiques grâce à des études de cas et exercices concrets



PUBLIC VISÉ

- Les administrateurs, ingénieurs et analystes en cybersécurité, réseau ou cloud
- Les professionnels de l'InfoSec et de la CND impliqués dans la gestion ou la sécurisation d'environnements cloud
- Toute personne travaillant dans l'administration, la gestion ou l'exploitation de réseaux et d'infrastructures cloud

POURQUOI SUIVRE CETTE FORMATION ?

Le programme CCSE constitue une certification de référence en sécurité multi-cloud, offrant une vision complète et approfondie de la protection des environnements AWS, Azure et GCP.

Il permet d'acquérir une expertise technique alignée sur les standards actuels de la cybersécurité cloud, et de maîtriser les outils modernes de détection, de gestion des risques et de conformité.

Conçu pour être cloud neutre, ce cursus garantit une compréhension globale applicable à tout type d'infrastructure hybride ou multi-fournisseurs.

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CTIA

CERTIFIED THREAT INTELLIGENCE ANALYST

ANTICIPATION ET GESTION DES MENACES DE SÉCURITÉ

La certification CTIA (Certified Threat Intelligence Analyst) prépare les professionnels à identifier, analyser et anticiper les menaces de cybersécurité afin de mieux protéger les organisations.

Elle couvre l'ensemble du cycle de la cyberintelligence, depuis la collecte d'informations jusqu'à la transformation des données brutes en renseignements exploitables pour la prise de décision.

Cette formation est conçue pour développer une approche proactive de la sécurité, en permettant de détecter les signaux faibles et d'anticiper les attaques avant qu'elles ne surviennent.

POURQUOI SUIVRE CETTE FORMATION ?

Le programme CTIA permet de se spécialiser dans la cyberintelligence, en apprenant à identifier, comprendre et neutraliser les menaces internes comme externes. Il aide à réduire les risques pour l'entreprise en transformant des données disparates en entités de menace quantifiables, capables d'être suivies, analysées et stoppées avant qu'elles ne causent des dommages. Cette formation apporte une véritable valeur ajoutée en permettant d'adopter une vision proactive, essentielle pour les organisations modernes confrontées à un environnement de menace en constante évolution.

OBJECTIFS

- Comprendre les fondamentaux de la cyberintelligence et ses différentes méthodologies
- Apprendre à collecter, analyser et corréler les informations provenant de sources variées (open source, dark web, réseaux internes...)
- Transformer les données brutes en renseignements exploitables pour les équipes opérationnelles
- Identifier les acteurs de menace, leurs motivations et leurs tactiques
- Développer la capacité à anticiper et atténuer les risques liés aux menaces émergentes

PUBLIC VISÉ

- Les ingénieurs, analystes, spécialistes et architectes sécurité
- Les gestionnaires de la sécurité et responsables techniques
- Les hackers éthiques et membres d'équipes CSIRT/incident response
- Toute personne impliquée dans la détection, la prévention ou l'analyse des menaces

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CEH AI V13

CERTIFIED ETHICAL HACKER

LA RÉFÉRENCE MONDIALE DU HACKING

En tant que certification éthique de hacking la plus reconnue au monde, la formation CEH AI version 13 vous plonge dans l'univers des techniques d'attaque modernes tout en intégrant l'usage de l'IA pour améliorer votre efficacité. Grâce à 20 modules couvrant plus de 550 techniques d'attaque et à 221 laboratoires pratiques, vous apprendrez à penser comme un hacker pour mieux défendre les systèmes.

CE PROGRAMME REPOSE SUR UN CADRE DE 4 ÉTAPES

Learn

Acquisition des connaissances, théorie + pratique sur des machines vulnérables, environnements réseau, outils, systèmes variés

Certify

Examen théorique (QCM, 4h, 125 questions) + examen pratique (6h / 20 défis dans un réseau virtuel)

Engage

Mise en situation d'audit / pentest complet (simulateur)

Complete

Participation à 12 challenges CTF (capture-the-flag) sur une année pour maintenir vos compétences à jour

L'intégration de l'IA vous permet d'automatiser certaines étapes (recherche, génération de commandes, détection assistée), d'améliorer votre productivité (+40 %) et de vous préparer à affronter les menaces de demain.



Avantages clés

- **Certification mondialement reconnue**
- **Composante pratique signifiante**
- **Usage de l'IA pour renforcer l'efficacité**
- **Accès à des challenges continus**



Niveau & prérequis

NIVEAU : INTERMÉDIAIRE À AVANCÉ

PUBLIC VISÉ (PRÉ-REQUIS) :

- Idéalement 2 années d'expérience en sécurité informatique / réseaux
 - Bonne maîtrise des systèmes, réseaux, notions de base en cybersécurité
- Si vous débutez, il est recommandé de commencer par un module "fondamentaux de cybersécurité" avant de postuler à ce programme.

Aucun prérequis formel obligatoire n'est exigé, mais pour réussir pleinement le programme, cette expérience technique est fortement conseillée.

PUBLIC VISÉ (PROFIL IDÉAL) :

- Professionnels de la cybersécurité cherchant à améliorer ou certifier leurs compétences
- Auditeurs, pentesteurs, analystes sécurité, administrateurs réseaux, ingénieurs sécurité
- Équipes IT / sécurité d'entreprises qui veulent monter en compétence en interne
- Organisations gouvernementales, militaires ou publiques cherchant une approche d'audit / défense offensive
- Formateurs ou établissements académiques souhaitant offrir une certification reconnue

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



PENTESTER

OBJECTIF DE LA FORMATION



Cette formation a pour but de maîtriser l'ensemble des phases d'un test d'intrusion (pentest), de la préparation à la restitution des résultats.

L'apprenant saura identifier, exploiter et corriger les vulnérabilités d'un système d'information, tout en développant une compréhension globale des enjeux stratégiques, techniques et juridiques liés à la cybersécurité.

PUBLIC VISÉ

Cette formation s'adresse aux étudiants et professionnels de l'informatique : administrateurs systèmes et réseaux, techniciens sécurité, RSSI, consultants ou toute personne souhaitant évoluer vers un poste d'expert en sécurité offensive.



MÉTHODOLOGIE

La formation repose sur une alternance de cours théoriques, ateliers pratiques et travaux dirigés.

Chaque participant réalise des exercices concrets en environnement isolé, reproduisant des conditions réelles d'attaque et de défense.

PRÉREQUIS

- Des bases solides en administration système (Windows et Linux), en réseaux et en programmation sont recommandées.
- Une bonne maîtrise des outils courants (terminal, bash, PowerShell) et des concepts de virtualisation (VPN, VLAN, hyperviseurs) facilitera l'apprentissage.

CERTIFICATION ET NIVEAU VISÉ

Cette formation prépare aux certifications internationales en pentesting telles que OSCP.

À l'issue du parcours, le participant atteint un niveau d'autonomie lui permettant de conduire des tests d'intrusion complets, documentés et conformes aux bonnes pratiques du secteur.

10 JOURS

Formation intensive alternant théorie, mise en pratique et exercices guidés.

Langue de l'examen	Langue de la formation
Anglais ✓	Anglais ✓
Français ✗	Français ✗

CONTENU DE LA FORMATION



01. INTRODUCTION À LA CYBERSÉCURITÉ ET AU PENTESTING

- Panorama des menaces, typologie des attaques, cadre juridique et méthodologie d'un test d'intrusion.
- Découverte des principaux frameworks et standards (OWASP, MITRE ATT&CK, NIST...).

02. PRÉPARATION D'UN TEST D'INTRUSION

- Compréhension des aspects réglementaires et juridiques
- Procédure d'engagement
- Préparation d'un questionnaire de pré-engagement
- Définition des étapes clés allant de la signature du contrat à la réalisation
- Désignation des intervenants et des outils
- Rédaction d'un contrat de pré-engagement

03. RECONNAISSANCE ET COLLECTE D'INFORMATIONS

- Techniques d'OSINT, recherche passive, analyse de domaines, exploration de ports et identification de services.
- Introduction aux outils Nmap, Netdiscover, et méthodes de scoring de vulnérabilités (CVSS).

04. EXPLOITATION ET POST-EXPLOITATION

- Découverte des exploits, des attaques par élévation de privilèges, du mouvement latéral et des frameworks offensifs comme Metasploit ou Cobalt Strike.
- Exercices pratiques de pénétration et d'exploitation de failles réelles.

05. SÉCURITÉ WEB ET APPLICATIONS

- Analyse des vulnérabilités courantes (XSS, injections SQL, CSRF, faille d'upload, etc.) avec Burp Suite.
- Mise en pratique via la correction et la sécurisation de scénarios réalistes issus du TOP 10 OWASP.

06. RÉSEAUX SANS FIL ET SÉCURITÉ AVANCÉE

- Étude des protocoles Wi-Fi, des attaques sur les réseaux sans fil et des mécanismes de chiffrement (WPA2, RADIUS).
- Simulation d'attaques contrôlées et contre-mesures associées.

07. RÉDACTION DU RAPPORT DE TEST D'INTRUSION

Méthodologie d'analyse, mise en forme des résultats, restitution au comité de direction et élaboration d'un plan d'actions correctif clair et exploitable.



CND

CERTIFIED NETWORK DEFENDER

La formation CND (Certified Network Defender) a pour objectif de former les professionnels à la mise en œuvre et à la gestion de stratégies de défense réseau efficaces. Elle offre une approche pratique de la cybersécurité défensive en enseignant comment protéger, détecter et répondre aux menaces visant les infrastructures réseau d'une organisation. Cette certification s'inscrit dans une logique de renforcement des capacités opérationnelles face aux cyberattaques modernes.



OBJECTIFS

- Comprendre les principes de la sécurité défensive et les stratégies de protection réseau
- Apprendre à concevoir, déployer et administrer un système de défense réseau robuste
- Maîtriser les techniques de surveillance, détection et réponse aux incidents
- Identifier les vulnérabilités réseau et mettre en place des contre-mesures adaptées
- Développer une expertise pratique à travers des exercices et études de cas

POURQUOI SUIVRE CETTE FORMATION ?

- Apprendre à créer et déployer des systèmes de défense réseau complets et performants
- Approfondir ses compétences grâce à un programme neutre et orienté pratique, couvrant les meilleures approches de mise en réseau sécurisée
- Maîtriser les techniques d'analyse, de détection et de durcissement des systèmes informatiques

PUBLIC VISÉ

- Les administrateurs et techniciens réseau
- Les ingénieurs sécurité réseau
- Toute personne impliquée dans les opérations réseau ou la gestion des infrastructures IT



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



ICS/SCADA

CYBERSECURITY

SÉCURITÉ DES IOT – INDUSTRIAL OPERATION TECHNOLOGY

La formation ICS/SCADA Cybersecurity est dédiée à la sécurisation des systèmes industriels et des infrastructures critiques.

Elle couvre les environnements ICS (Industrial Control Systems) et SCADA (Supervisory Control and Data Acquisition), au cœur des opérations industrielles modernes.

Cette formation permet de comprendre les enjeux de la cybersécurité dans les chaînes de production, les réseaux industriels, l'automatisation et l'IoT industriel, tout en maîtrisant les méthodes avancées d'analyse et de protection.

POURQUOI SUIVRE CETTE FORMATION ?

La formation ICS/SCADA Cybersecurity offre des méthodes puissantes pour analyser et protéger les réseaux informatiques industriels.

Elle aborde le processus complet :

- analyse des risques,
- détection des intrusions,
- identification des logiciels malveillants,
- investigation numérique (forensique),
- et réponse adaptée lors de la découverte d'une brèche.

Elle permet ainsi de renforcer significativement la résilience des systèmes industriels et de réduire les risques liés aux cyberattaques ciblant les infrastructures critiques.

OBJECTIFS

- Comprendre le fonctionnement des systèmes industriels ICS et SCADA
- Identifier les vulnérabilités et menaces propres aux environnements OT (Operational Technology)
- Mettre en place des politiques, pratiques et procédures de sécurité adaptées au secteur industriel
- Savoir analyser les risques et détecter les intrusions dans un contexte industriel
- Maîtriser les processus de forensique numérique et les bonnes pratiques de réponse aux incidents

PUBLIC VISÉ

- Les professionnels chargés de l'établissement et du maintien des politiques de sécurité
- Les spécialistes travaillant sur des infrastructures critiques (énergie, eau, transport, industrie)
- Les responsables et ingénieurs de production, d'automatisation ou d'IoT
- Toute personne impliquée dans la gestion, la surveillance ou la sécurisation d'environnements industriels



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



ECIH

EC-COUNCIL CERTIFIED INCIDENT HANDLER

GESTION ET RÉPONSE AUX DIFFÉRENTS INCIDENTS

La certification ECIH forme les professionnels à la gestion complète des incidents de sécurité, depuis leur détection jusqu'à leur résolution.

Elle permet d'acquérir les compétences nécessaires pour répondre efficacement à une grande variété d'incidents : attaques informatiques, intrusions, compromissions de données, infections malveillantes, violations de politiques internes, etc.

Cette formation met l'accent sur les méthodes, outils et bonnes pratiques indispensables pour structurer un processus de réponse performant et limiter l'impact des incidents sur l'organisation.

POURQUOI SUIVRE CETTE FORMATION ?

La certification ECIH enseigne comment construire un parcours de réponse aux incidents performant, en fournissant une méthodologie claire et des solutions adaptées pour gérer les situations critiques.

Elle aborde également les aspects juridiques liés aux incidents, un élément souvent négligé mais indispensable pour agir dans un cadre réglementaire sécurisé.

Enfin, elle couvre les techniques essentielles de traitement et d'amélioration continue pour renforcer votre capacité à faire face aux incidents futurs.

PUBLIC VISÉ

- Toutes les personnes issues de la sécurité de l'information souhaitant enrichir leurs compétences
- Les analystes SOC, équipes CSIRT et spécialistes de la réponse aux incidents
- Les administrateurs, ingénieurs et responsables techniques voulant structurer un processus de gestion des incidents
- Les professionnels ayant besoin de comprendre l'aspect opérationnel ET juridique de la réponse aux incidents

OBJECTIFS

- Comprendre le cycle de vie d'un incident de sécurité
- Apprendre à identifier, analyser, contenir et éradiquer différents types d'attaques
- Maîtriser les outils et techniques de réponse aux incidents
- Développer des procédures adaptées aux contextes opérationnels et juridiques
- Renforcer la capacité de l'organisation à prévenir et gérer les incidents futurs



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CASE.JAVA

CERTIFIED APPLICATION SECURITY ENGINEER

APPROCHE GLOBALE DE LA SÉCURITÉ DES APPLICATIONS – SDLC

La certification CASE.Java forme les professionnels du développement à intégrer la sécurité au cœur du SDLC (Software Development Life Cycle).

Elle propose une approche complète de la sécurité applicative, depuis la définition des besoins jusqu'au déploiement et à la maintenance, en passant par le design, le développement et les tests.

Cette formation est conçue pour permettre aux développeurs Java de créer des applications plus résilientes et conformes aux meilleures pratiques de sécurité.



POURQUOI SUIVRE CETTE FORMATION ?

La certification CASE.Java offre une vision globale de la sécurité des applications, en couvrant l'ensemble des activités critiques du SDLC : Requirement – Design – Development – Testing – Deployment – Maintenance.

Elle permet d'adopter une démarche proactive en intégrant la sécurité dès la conception, réduisant ainsi les failles potentielles et garantissant la robustesse des applications tout au long de leur cycle de vie.

OBJECTIFS

- Comprendre les principes fondamentaux de la sécurité applicative
- Savoir intégrer la sécurité à chaque étape du cycle de développement logiciel (SDLC)
- Identifier et corriger les vulnérabilités courantes dans les applications Java
- Mettre en œuvre des techniques de développement sécurisé conformes aux standards internationaux
- Renforcer la qualité, la stabilité et la résilience des applications face aux menaces modernes

PUBLIC VISÉ

- Les développeurs Java possédant un minimum de deux ans d'expérience
- Les professionnels impliqués dans le développement, le test, la gestion ou la protection d'applications
- Les équipes souhaitant adopter une approche DevSecOps ou améliorer la sécurité de leurs projets logiciels



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CASE.NET

CERTIFIED APPLICATION SECURITY ENGINEER

APPROCHE GLOBALE DE LA SÉCURITÉ DES APPLICATIONS – SDLC

La certification CASE.NET forme les développeurs et équipes techniques à intégrer la sécurité au cœur du cycle de développement logiciel (SDLC).

Elle propose une vision complète de la sécurité applicative dans les environnements .NET, en couvrant les pratiques essentielles pour concevoir, développer, tester et maintenir des applications plus robustes et résistantes aux attaques.

Cette formation permet d'adopter une démarche proactive : sécuriser les applications dès la conception plutôt qu'en fin de développement.

POURQUOI SUIVRE CETTE FORMATION ?

La certification CASE.NET offre une approche globale de la sécurité des applications, couvrant l'ensemble des phases du cycle de développement logiciel.

Elle permet de réduire significativement les risques dès les premières étapes du projet en intégrant des pratiques de sécurité robustes.

Cette démarche garantit des applications .NET plus sûres, plus fiables et conformes aux exigences de sécurité modernes.



OBJECTIFS

- Comprendre les fondamentaux de la sécurité applicative dans le contexte .NET
- Savoir intégrer la sécurité à chaque étape du SDLC : Requirement – Design – Development – Testing – Deployment – Maintenance
- Détecter et corriger les vulnérabilités propres aux environnements .NET
- Maîtriser les bonnes pratiques de développement sécurisé et les standards internationaux
- Renforcer la qualité, la stabilité et la sécurité globale des applications .NET

PUBLIC VISÉ

- Les développeurs .NET ayant au minimum deux ans d'expérience
- Les équipes impliquées dans le développement, les tests, la gestion ou la sécurisation d'applications
- Les professionnels souhaitant intégrer une approche DevSecOps dans leurs processus

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CEH MASTER

CERTIFIED ETHICAL HACKER MASTER

SÉCURITÉ OFFENSIVE – LE PENCHANT PRATIQUE DU CEH

La certification CEH Master est la continuité naturelle du Certified Ethical Hacker (CEH), orientée sur la pratique. Elle met les participants face à des scénarios réels de cybersécurité offensive afin d'évaluer et de perfectionner leurs compétences en tests d'intrusion, exploitation de vulnérabilités et défense active. C'est une formation exigeante et concrète, conçue pour transformer la théorie en expérience opérationnelle à travers des défis réalistes.

OBJECTIFS

- Mettre en pratique les connaissances acquises dans la formation CEH
- Réaliser des tests d'intrusion complets sur des environnements simulés
- Identifier, exploiter et corriger des vulnérabilités réseau, système et applicatives
- Développer des réflexes d'analyse, de contournement et de remédiation face à des attaques réelles
- Acquérir une maîtrise technique reconnue dans le domaine du pentest et de la sécurité offensive



Public visé

- Les RSSI, administrateurs réseau et responsables techniques souhaitant comprendre les mécanismes d'attaque et de défense avancés
- Les professionnels de la cybersécurité cherchant à valider leurs compétences par une certification à forte valeur pratique
- Les hackers éthiques désireux de se mesurer à des environnements réalistes



Pour quoi ?

- Prouver concrètement ses compétences en situation réelle grâce à des laboratoires intensifs et chronométrés
- Se confronter à des défis techniques comparables à ceux rencontrés dans le monde professionnel
- Valoriser son profil avec une certification hautement reconnue à l'international dans le domaine du hacking éthique

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CHFI

CERTIFIED HACKING FORENSIC INVESTIGATOR

INVESTIGATION NUMÉRIQUE – OUTILS ET MÉTHODOLOGIES

La certification CHFI forme les professionnels à l'investigation numérique, à l'analyse des incidents de cybersécurité et à la collecte de preuves exploitables.

Elle offre un aperçu complet des techniques, outils et procédures nécessaires pour examiner un acte de cybercriminalité, tout en respectant les exigences légales et judiciaires liées au traitement des preuves numériques.

Cette formation constitue une référence pour tous ceux qui souhaitent se spécialiser dans la forensique numérique et la réponse aux incidents.

POURQUOI SUIVRE CETTE FORMATION ?

La certification CHFI offre une vision complète du travail d'un enquêteur spécialisé en cybercriminalité.

Elle enseigne non seulement comment traiter et préserver correctement les preuves numériques, mais aussi comment utiliser les outils et méthodes qui permettent de reconstituer les faits, identifier les auteurs et comprendre précisément l'incident.

Cette formation est indispensable pour toute structure souhaitant renforcer sa capacité à réagir efficacement face aux attaques et à soutenir des enquêtes techniques ou judiciaires.



OBJECTIFS

- Comprendre le processus complet d'investigation forensique
- Apprendre à identifier, collecter, analyser et préserver des preuves numériques
- Maîtriser les outils et techniques utilisés pour enquêter sur les cyberattaques
- Savoir documenter les analyses pour garantir l'acceptation des preuves par les tribunaux
- Développer les bons réflexes pour intervenir sur un poste compromis, un réseau infecté ou un incident majeur

PUBLIC VISÉ

- Les professionnels de l'IT impliqués dans la sécurité des systèmes d'information
- Les experts en forensique numérique et en réponse aux incidents
- La police, les forces de l'ordre, les équipes de défense et de sécurité
- Les juristes, professionnels de la banque, de l'assurance et les agences gouvernementales
- Toute personne devant analyser ou traiter des traces numériques après un incident

Langue de l'examen Langue de la formation

Anglais ✓

Français ✗

Anglais ✓

Français ✗



EDRP

EC-COUNCIL DISASTER RECOVERY PROFESSIONAL

CONTINUITÉ ET REPRISE D'ACTIVITÉ APRÈS SINISTRE

La certification EDRP forme les professionnels aux concepts essentiels de Business Continuity (BC) et de Disaster Recovery (DR), deux piliers indispensables pour assurer la résilience d'une organisation face aux incidents majeurs.

Cette formation permet de comprendre comment anticiper, préparer, documenter et exécuter un plan de continuité et de reprise après sinistre, afin de minimiser les interruptions d'activité et de protéger les données critiques.

PUBLIC VISÉ

- Les professionnels et consultants spécialisés en continuité d'activité (BC) et reprise après sinistre (DR)
- Les administrateurs systèmes et réseaux responsables de la résilience des infrastructures
- Les gestionnaires et consultants en risques informatiques
- Les RSSI, directeurs informatiques et responsables techniques souhaitant renforcer leur stratégie de continuité

OBJECTIFS

- Maîtriser les principes de la continuité d'activité et de la reprise après sinistre
- Apprendre à réaliser une analyse d'impact sur les activités (BIA)
- Évaluer les risques susceptibles de perturber l'organisation
- Élaborer des politiques, procédures et plans opérationnels adaptés
- Savoir protéger les données critiques et les restaurer de manière efficace après un sinistre
- Développer une approche structurée pour réduire les interruptions et garantir la résilience organisationnelle

POURQUOI SUIVRE CETTE FORMATION ?

La certification EDRP permet d'acquérir une vision complète de la continuité des opérations et de la reprise après sinistre, en couvrant :

- l'analyse de l'impact sur les activités,
- l'évaluation des risques,
- l'élaboration de politiques et de procédures,
- la mise en œuvre d'un plan complet adapté aux besoins de l'entreprise.

Elle enseigne également comment sécuriser les données, mettre en place les mécanismes de protection adéquats et restaurer les données essentielles d'une organisation à la suite d'un incident majeur.

C'est une certification incontournable pour assurer la résilience et la capacité de redémarrage rapide d'une entreprise.



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



ECDE

EC-COUNCIL CERTIFIED DEVSECOPS ENGINEER

CONCEPTION, DÉVELOPPEMENT ET MAINTIEN D'APPLICATIONS SÉCURISÉES

La certification ECDE est dédiée aux professionnels souhaitant maîtriser la mise en œuvre du DevSecOps, une approche qui intègre la sécurité au cœur du développement, de l'automatisation et des opérations.

Elle couvre l'ensemble du cycle de vie DevOps — planification, développement, construction, tests, déploiement, exploitation et surveillance — en intégrant systématiquement les bonnes pratiques de sécurité. Cette formation constitue aujourd'hui l'un des programmes DevSecOps les plus complets, alliant apprentissage théorique et laboratoires pratiques.

POURQUOI SUIVRE CETTE FORMATION ?

Le cursus ECDE constitue le programme DevSecOps le plus complet du marché, en mettant l'accent sur :

- l'intégration de la sécurité dès la planification,
- la sécurisation des étapes de codage, tests, déploiement et surveillance,
- et la mise en place d'environnements automatisés robustes.

Grâce à ses nombreux laboratoires pratiques, il permet de maîtriser à la fois la sécurisation des applications et celle des infrastructures DevSecOps, que ce soit en environnement on-premise ou cloud-native.

Il s'agit d'une formation idéale pour bâtir une carrière solide dans le domaine du DevSecOps.



OBJECTIFS

- Comprendre les fondamentaux du DevSecOps et son rôle stratégique dans la sécurisation des applications
- Intégrer la sécurité dans chaque étape du cycle DevOps (SDLC & CI/CD)
- Maîtriser les pratiques modernes d'automatisation de la sécurité (tests, scans, pipelines...)
- Déployer des infrastructures et applications sécurisées en environnements on-premise et cloud-natifs
- Développer une expertise pratique grâce à un programme fortement orienté laboratoires (70 %)

PUBLIC VISÉ

- Les professionnels certifiés CASE ou impliqués dans la sécurité applicative
- Les ingénieurs DevOps, ingénieurs cloud ou administrateurs systèmes souhaitant intégrer la sécurité dans leurs pipelines
- Les analystes en cybersécurité ou spécialistes de l'automatisation
- Toute personne disposant de connaissances préalables en sécurité applicative et désirant évoluer vers le DevSecOps

Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CCISO

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

STRATÉGIE DE GESTION DES SI EN ACCORD AVEC LES OBJECTIFS DE L'ORGANISATION

La certification CCISO est dédiée aux leaders et décideurs qui pilotent la stratégie de sécurité de l'information au sein d'une organisation.

Elle combine une vision stratégique, managériale, opérationnelle et financière de la cybersécurité, permettant aux futurs ou actuels dirigeants de maîtriser l'ensemble des compétences nécessaires pour conduire un programme de sécurité performant, aligné sur les objectifs de l'entreprise.

Cette formation constitue une référence internationale pour celles et ceux qui aspirent à exercer des fonctions de haut niveau dans la gouvernance de la sécurité.

POURQUOI SUIVRE CETTE FORMATION ?

La certification CCISO offre un cadre complet pour diriger un programme de sécurité de l'information.

Elle couvre :

- la gouvernance,
- les audits,
- les contrôles des systèmes d'information,
- la gestion du capital humain,
- le développement de programmes stratégiques,
- l'expertise financière indispensable pour garantir le succès des initiatives de sécurité.

Ce programme unique permet d'acquérir toutes les compétences nécessaires pour prendre des décisions éclairées et orchestrer efficacement la sécurité à l'échelle d'une organisation.



OBJECTIFS

- Développer une vision stratégique de la sécurité de l'information
- Maîtriser la gouvernance, les audits et les systèmes de contrôle internes
- Comprendre les enjeux liés à la gestion du risque, à la conformité et à la continuité d'activité
- Gérer efficacement le capital humain, les ressources et les budgets associés à la cybersécurité
- Piloter la conception et l'exécution de programmes de sécurité à grande échelle

PUBLIC VISÉ

- Les CEO, directeurs généraux et hauts responsables décisionnaires
- Les CISO, CIO, CTO, directeurs IT et directeurs sécurité
- Les cadres et managers souhaitant évoluer vers un rôle stratégique dans la cybersécurité
- Toute personne impliquée dans la prise de décision et nécessitant une vision globale de la gestion des SI

Langue de l'examen	Langue de la formation
Anglais ✓	Anglais ✓
Français ✗	Français ✗



CPENT

CERTIFIED PENETRATION TESTING PROFESSIONAL

Domaine : Vulnerability Assessment & Pentesting

Thématique : sécurité offensive – le niveau ultime en pentest

PUBLIC VISÉ

Cette formation s'adresse aux :

- Hackers éthiques
- Pentesters
- Administrateurs réseau et systèmes
- Analystes sécurité
- Professionnels de l'évaluation des risques
- Analystes forensiques
- Analystes SOC
- Spécialistes de la sécurité applicative

Le CPENT vous plonge dans les environnements les plus avancés du pentest.



POUR QUOI ?

Vous apprendrez à :

- Tester des systèmes IoT et OT
- Écrire et personnaliser vos propres exploits et outils
- Réaliser des exploits binaires avancés
- Effectuer un double pivot pour atteindre des réseaux cachés
- Créer et adapter des scripts/exploits pour pénétrer les segments les plus profonds du réseau

Aucun autre cours de pentest au monde n'offre un niveau de réalisme et de complexité comparable au CPENT.

OBJECTIF DE LA CERTIFICATION

Valider des compétences avancées en cybersécurité offensive, capables de simuler des attaques complexes sur des infrastructures hybrides et de maîtriser l'ensemble du cycle d'intrusion, du test initial jusqu'à l'exploitation post-intrusion.



INFORMATIONS PRATIQUES

- Durée : à définir selon le format choisi (intensif ou étendu)
- Pré-requis : certification CEH ou expérience équivalente en pentest
- Langues : français / anglais
- Certification délivrée par : EC-Council

DEVENEZ UN EXPERT EN CYBERSÉCURITÉ OFFENSIVE !

Avec la certification CPENT – Certified Penetration Testing Professional, plongez au cœur du hacking éthique et apprenez à exploiter, infiltrer et sécuriser les réseaux les plus complexes. Repoussez vos limites, maîtrisez les environnements IoT et OT, et atteignez le niveau ultime du Pentest.



Langue de l'examen		Langue de la formation	
Anglais	✓	Anglais	✓
Français	✗	Français	✗



CONTACTEZ-NOUS



TÉLÉPHONE: 0590 500 436



E-MAIL : CONTACT@CYBER-CORSAIRE.COM



SITE WEB: WWW.CYBER-CORSAIRE.COM

