CYBERNETIES
Academy

Catalogue Cyber 2023

Formation & Sensibilisation

CYBERNETIES
Academy

Les formations en Cybersécurité

La sécurité informatique est devenue un enjeu crucial pour les entreprises, les organisations gouvernementales et les particuliers. Les menaces en ligne sont de plus en plus sophistiquées et fréquentes. Ainsi, il est devenu essentiel de protéger les données sensibles contre les cyberattaques.

Les professionnels de la sécurité informatique sont hautement demandés dans les entreprises et les organisations du monde entier. Les formations en sécurité informatique sont souvent dispensées par des experts du domaine, qui partagent leur expérience et leur savoir-faire avec les apprenants. Les formations peuvent être suivies à distance, en ligne ou en présentiel dans des centres de formation spécialisés.

Nos formations en sécurité informatique sont particulièrement adaptées aux professionnels de l'informatique, aux développeurs, aux administrateurs système, aux analystes et à toute personne intéressée par la sécurité informatique.

Elles sont animées par nos consultants et des formateurs certifiés au vécu opérationnel fort.

CYBERNETIES
Academy

SOMMAIRE

CYBERNETIES
Academy

1 jour

Introduction à la Cybersécurité

Internet un outil essentiel pour les entreprises. Elles l'utilisent au quotidien pour augmenter leur efficacité et explorer de nouveaux marchés, mais cette dépendance croissante en fait une menace pour la sécurité. Les cyberattaques et les violations de la protection des données sont de plus en plus fréquentes et les entreprises doivent prendre au sérieux la question de la cybersécurité. Il est crucial que toutes les mesures de contrôle nécessaires soient mises en place pour prévenir les cyberattaques, et la sensibilisation des employés joue un rôle clé dans cette démarche.

Objectif

- Développer une vision globale de la cybersécurité, de sa définition à son évolution récente et des enjeux de la SSI.
- Découvrir les attaques les plus répandues (social engineering, malware, etc.) ainsi que les bonnes pratiques à adopter pour y faire face.
- Disposer des principaux tests d'audit permettant de contrôler le niveau de maturité de la sécurité IT d'une entreprise.

Public Visé & Prérequis

- Tout publique.
- Connaissances générales des systèmes d'information.

Méthode & Matériel

- Cours magistral interactif avec des exemples.
- Supports intégralement en français.

Programme

- Introduction à la cybersécurité.
- Les risques qui pèsent sur les organisations.
- Cyber menaces, arnaques et dangers sur le réseau.
- Bonnes pratiques en matière de sécurité : gouvernance, organisation, dispositif de contrôle permanent, outils.
- Démonstrations et exemples d'attaques.
- Focus audit et contrôle interne IT : présentation des méthodes, outils et techniques modernes de contrôle de maturité sécurité.

CYBERNETIES
Academy

1 jour

La Gestion du Risque

La gestion du risque en cybersécurité est une approche proactive pour identifier, évaluer et atténuer les menaces potentielles à la sécurité informatique. Elle implique la mise en place de politiques et de procédures de sécurité robustes, ainsi que la formation des employés et l'utilisation d'outils de sécurité pour protéger les systèmes et les données. La gestion du risque en cybersécurité est essentielle pour assurer la confidentialité, l'intégrité et la disponibilité des informations en ligne et pour minimiser les pertes financières et les dommages à la réputation causés par les cyberattaques.

Objectif

- Comprendre ce qu'est un risque et savoir l'évaluer.
- Différencier le risque de sécurité de l'information du risque de sécurité des systèmes d'information.
- Appréhender les enjeux de la gestion des risques.
- Se repérer dans la documentation existante.

Public Visé & Prérequis

- RSSI, gestionnaire des risques, chef de projet, membre d'une équipe de sécurité.
- Connaissances générales des systèmes d'information.

Méthode & Matériel

- Cours magistral interactif avec des exemples.
- Supports intégralement en français.

Certification

- Cette sensibilisation prépare aux formations certifiantes:
  -ISO 27005 Risk Manager
  -EBIOS Risk Manager

Programme

Le risque

- Définir et évaluer le risque de manière générale.
- Panorama des principales menaces actuelles.
- Comprendre le risque de sécurité de l'information.
- Comprendre le risque de sécurité des systèmes d'information.

La gestion des risques

- Définir et comprendre les enjeux de la gestion de risques.
- Le cadre normatif :
  -La norme ISO/IEC 31000
  -La norme ISO/IEC 25000
- Les méthodes de gestions de risques :
  -Panorama des méthodes existantes
  -Comparatif des méthodes existantes
  -Le choix dans la méthodologie

CYBERNETIES Academy

1- 3 jours

Campagne de Phishing

Le phishing est une technique d'attaque courante utilisée par les cybercriminels pour tromper les utilisateurs en leur faisant croire qu'ils communiquent avec une entité fiable. Ces attaques prennent souvent la forme d'e-mails, de messages texte ou de pages web frauduleuses qui imitent des entreprises ou des organisations de confiance. Les cybercriminels utilisent le phishing pour obtenir des informations personnelles, comme des identifiants de connexion ou des informations de carte de crédit, qui peuvent ensuite être utilisées pour commettre des fraudes financières ou voler des identités. En raison de son efficacité et de sa simplicité, le phishing reste une menace importante pour la sécurité en ligne.

Programme

Préparation de la campagne
- Cadrage de la mission
- Validation du périmètre
- Validation des prérequis
- Planification du lancement de la campagne
- Choix et/ou conception des scénarios
- Phase de récolte d'informations

Lancement de la campagne
- Envoi des courriels aux cibles du périmètre
- Collecte des informations de la campagne

Agrégation des résultats
- Consolidation des résultats
- Rédaction du rapport de la campagne
- Restitution avec les différentes parties prenantes

Sensibilisation des employés
- Adaptation de la sensibilisation en fonction des résultats
- Proposition de différents types de sensibilisations au phishing

CYBERNETIES Academy

1- 3 jours

Analyste SOC

Programme d'apprentissage qui vise à fournir les fondamentaux de la sécurité informatique, notamment les techniques d'analyse de log, les méthodologies de détection de menaces, les technologies de sécurité et les protocoles de réponse aux incidents. Ils apprennent également à utiliser des outils de sécurité tels que des SIEM, des IDS et des outils d'analyse de trafic réseau.

Objectif

- Décrire l'état de l'art du SOC (Security Operation Center).
- Méthode d'analyse et d'investigation d'incident.
- Clarification des éléments à apporter post investigation.

Public Visé & Prérequis

- Administrateurs système, équipes informatique ou sécurité, consultants.
- Avoir des connaissances générales en sécurité offensive et défensive, telles que les techniques de hacking et le durcissement des infrastructures.

Méthode & Matériel

- Cours magistral interactif avec des exemples.
- Supports intégralement en français.

Certification

- Cette formation prépare à Certified SOC Analyst (CSA).

Programme

Les missions d'un centre des opérations de sécurité
- Compréhension sur l'essentiel du SOC.
- Débat sur les éléments que compose un SOC.
- Compréhension sur la mise en place du SOC.

Techniques d'attaque
- Définition des locutions cybermenace et attaque.
- Attaques de sécurité réseau.
- Attaques par en-tête d'hôte.
- Attaques applicatives.
- Appréhension sur les indicateurs de compromis (IoC).
- Débat sur les stratégies de piratage des attaquants.

Les incidents, les événements et les logs
- Appréhension sur les opérations de base des incidents, des événements et de la journalisation.
- Décryptage de la journalisation locale.
- Décryptage de la journalisation centralisée.

La détection des incidents et la gestion des événements
- Appréhension sur la gestion des données de sécurité et des événements.
- Débat sur les solutions SIEM.
- Appréhension sur le déploiement d'un SIEM.
- Initiation sur les types d'utilisation pour la détection d'incident applicatif.
- Initiation sur les types d'utilisation pour la détection d'incidents internes.
- Initiation sur les types d'utilisation pour la détection d'incident de sécurité réseau.
- Initiation sur les types d'utilisation pour la détection d'incident par en-tête d'hôte.
- Initiation sur les types d'utilisation pour la mise en conformité.
- Appréhension sur la gestion du tri et de l'analyse des alertes.

La détection avancée des incidents en agrément des menaces
- Appréhension sur l'intelligence des menaces.
- Initiation sur les types de renseignements des menaces.
- Appréhension sur la stratégie de renseignement des menaces.
- Découverte des sources de renseignements sur les menaces.
- Initiation aux plateformes de renseignement sur les menaces.
- Appréhension sur l'importance d'un SOC basé sur l'IA.

La réponse aux incidents de sécurité
- Appréhension sur les bases et les procédures de la réponse aux incidents.
- Apprendre à répondre aux incidents de sécurité réseau.
- Apprendre à répondre aux incidents de sécurité applicatifs.
- Apprendre à répondre aux incidents de messagerie.
- Apprendre à répondre aux incidents d'initiés.
- Apprendre à répondre aux incidents malware.

CYBERNETIES Academy

1- 3 jours

Sécurité des Réseaux

Cette formation couvre les principes fondamentaux de la sécurité des réseaux, y compris les mesures de protection contre les intrusions, les menaces persistantes avancées (APT), la détection d'intrusions et la sécurité des réseaux sans fil.

Objectif

- Les caractéristiques d'une architecture sécurisée.
- Sécuriser les architectures communément mises en œuvre dans les entreprises.
- Evaluer la sécurité d'une architecture donnée.
- Identifier les choix structurant l'architecture de vos prochaines solutions.
- Prendre en compte la sécurité dans les choix d'architecture.

Public Visé & Prérequis

- Toutes les personnes confrontées à la sécurité des architectures des systèmes d'information.
- Avoir une connaissance de base des réseaux et du fonctionnement des TCP/IP.

Méthode & Matériel

- Cours magistral interactif avec des exemples.
- Supports intégralement en français.

Certification

- Cette formation prépare à RNCP32121.

Programme

Introduction
- Principes de sécurisation, objectifs de sécurité.
- Architecture d'administration et d'authentification.
- Protocoles d'administration et usages : RDP, WinRM,SSH, VNC.
- Authentification centralisée : LDAP, NTLM, RADIUS,Kerberos.
- Référentiels centralisés : OpenLDAP, Active Directory.
- Authentification forte : principes, OAuth, U2F, ActivCard.
- Administrateurs et services : Forêts, LAPS, bastions.

Réseaux et segmentation
- IPv4, IPv6.
- Composants : concentrateur, pare-feu, diode, NIDS/NIPS…
- Segmentation physique: ports RJ45 et consoles, 802.1x.
- Segmentation réseau, découpage vertical.
- Routage : statique vs dynamique, OSPF, RIPE, BGP.
- Filtrage : règles fondamentales, matricede flux, local vs central.
- Software-defined network.
- Relais applicatifs et inverses.

Architecture générale
- Systèmes autonomes.
- Segmentation horizontale et administration "out-of-band".
- Positionnement des éléments de sécurité.

Connexion distante
- Connexion à distance et interconnexion multi- sites : MPLS, VPN IPSec, TLS.

Postes de travail
- Virtualisation, VDI, BYOD vs. COPE.

Architecture Windows
- Architecture de domaines, DC et RODC.
- Architectures applicatives.

Accès Internet
- Architectures 2-tiers,3-tiers ; requêtesRPC.
- Stockage : SAN, NAS, partagesréseaux SMB, NFS, EDI, ETL, ERP.

Architecture des fonctions d'infrastructure et de sécurité
- DHCP et usage.
- DNS : interne, public, DNSSEC.
- SMTP : émission interne,réception.
- Journalisation et SIEM / supervision.
- Mise à jour ; configuration et déploiement.
- Cryptographie.

Continuité et haute disponibilité
- Notion de SPOF.
- Réseau : agrégation, clusters, adresses IP virtuelles, boucles.
- Equipements simples : répartition de charge, réplication de données.
- Sauvegarde : Push vs pull.
- Continuité d'activité.

CYBERNETIES Academy

1- 3 jours

Gestion des Access et des Identités

Cette formation enseigne les meilleures pratiques pour la gestion des identités et des accès, y compris l'authentification, l'autorisation, la gestion des rôles, les politiques de mot de passe, les services d'annuaire et la gestion des certificats.

Objectif

- Comprendre les différentes vulnérabilités exploitées par les attaquants.
- Détecter et corriger les vulnérabilités liées à l'Active Directory.
- Connaitre les outils et architectures permettant une administration sécurisée.
- Acquérir les bonnes pratiques d'administration sécurisée.

Public Visé & Prérequis

- Administrateurs système, équipes informatique ou sécurité, auditeurs techniques, Consultants.

- Avoir une expérience dans l'utilisation des systèmes Windows, connaissances générales en système et réseau.

Méthode & Matériel

- Cours magistral interactif avec des exemples.

- Supports intégralement en français.

Programme

Architecture ActiveDirectory

- Structure d'un AD.
- Les principaux services.
- Relations d'approbation.
- NamingContext LDAP.
- Niveaux fonctionnels.
- Utilisateurs et groupes.
- Authentification.
- Gestion des mots de passe.
- Déploiement d'une politique de sécurité (GPO).

Les points de contrôle et sécurité Active Directory

- Définition.
- Classement de l'ANSSI des points de contrôle les plus importants.
- Les outils existants.
- Cas pratiques: identification, exploitation et correction des principales vulnérabilités d'un Active Directory.
- Backdoors (post-compromission) d'un attaquant.

Modèle d'administration sécurisé

- Les principaux risques :
  - mise en cache des authentifiant Windows
  - faiblesses de NTLM
  - pass-the-hash / pass-the-ticket.
- Atelier de réflexion sur les mesures de protection à mettre en œuvre.
- Le modèle d'administration en Tiers
  - architecture du Tiers 0
  - la PAW, station d'administration sécurisée ;
  - les serveurs du Tiers 0
  - les autres Tiers.
- Mesures de sécurité permettant la mise en place du modèle en Tiers :
  - Kerberos Armoring
  - politiques d'authentification et silos
  - RDP Restricted admin
  - délégations d'administration pour les Tiers 1 et 2.

CYBERNETIES Academy

1- 3 jours

Sécurité des Serveurs et Application

Les applications web sont souvent la cible la plus vulnérable au sein des entreprises, ce qui peut entraîner des failles de sécurité. Les conséquences de ces failles peuvent être importantes. Dans certains cas, des milliers de machines peuvent être compromises si un site web est piraté. Cette formation se concentre sur les vulnérabilités classiques du Web, en utilisant des tests d'intrusion pour les identifier et en enseignant les mesures à prendre pour les remédier.

Objectif

- Les enjeux de la sécurité web.
- Les méthodes d'attaque sur le web et comment s'en protéger.
- Les bases de la cryptographie, quand et comment l'utiliser.
- Les méthodes d'authentification web.
- Les bonnes pratiques de développement sécurisé.
- Les techniques de protection des serveurs.

Public Visé & Prérequis

- Développeur web, Architecte, Administrateur systèmes, Pentester débutant.
- Avoir une expérience dans le développement web ou des connaissances en réseaux et systèmes sont un plus.

Méthode & Matériel

- Cours magistral interactif avec des exemples.
- Supports intégralement en français.

Programme

Introduction
- La sécurité informatique.
- Cadre normatif et législatif.
- Les différents types de menace et leurs évolutions.
- Comprendre l'attaquant pour mieux se protéger.

L'infrastructure web
- Architecture matérielle.
- Architecture applicative.
- Découverte de l'environnement.
- TP : collecte d'information, scan réseau, transfert de zone, protection.

Les protocoles du web
- Le protocole HTTP.
- TP : analyseur de réseau, configuration d'entêtes, attaques sur sessions.

Sécurisation des données et des flux
- Eléments de cryptographie.
- Chiffrement des flux de données.
- Signature électronique, certificats.
- Chiffrement des données.
- Travaux pratiques: récupération de mots de passes.

L'authentification
- Méthodes d'authentification http.
- Méthodes d'authentification forte.
- Modèles de délégation.
- Principes d'infrastructure Single Sign On.

Les applications Web
- Les attaques par injection.
- Les attaques par inclusion.
- Durcissement des serveurs et des OS.
- TP: configuration d'un serveur web, attaques et contre mesures.

CYBERNETIES Academy

1- 3 jours

Essentiel de la Conformité RGPD

Le cadre juridique lié à la protection des données personnelles a été refondu par le règlement européen RGPD. Ce dernier impose diverses obligations aux responsables de traitement et aux sous-traitants, touchant ainsi tous les métiers au sein des organismes. Pour se conformer à ces obligations, il est indispensable de suivre la formation RGPD : essentiel de la conformité, qui permet d'appréhender le texte de manière pratique et opérationnelle. Cette formation convient aussi bien aux profils techniques que juridiques et peut être suivie par toute personne souhaitant se familiariser avec le sujet.

Objectif

- Les principaux points clés du RGPD.
- Les chantiers à mettre en place pour la mise en conformité.
- Les bonnes pratiques quotidiennes de la protection des données.

Public Visé & Prérequis

- Futurs DPO ou DPO débutants, référent RGPD, juristes, RSSI ou techniciens souhaitant renforcer leurs connaissances juridiques.
- Aucun prérequis.

Méthode & Matériel

- Cours magistral interactif avec des exemples.
- Supports intégralement en français.

Certification

- Cette formation prépare a la formation certifiante:
  -PECB « Data Protection Officer.

Programme

Introduction

- Fondamentaux juridiques.
- Historique et avenir du règlement européen.
- Enjeux de la protection des données personnelles.

Quelles sont les enjeux fondamentaux du RGPD ?

- Champ d'application du règlement.
- Principes fondamentaux.
- Notions essentielles et acteurs.
- Responsabilités (responsabilité du DPO, du sous-traitant, responsabilité conjointe, etc.).
- Les risques de non-conformité.

Comment assurer la conformité de son organisme ?

- Piloter la protection des données personnelles avec un DPO.
- Gérer les risques avec l'analyse d'impact (PIA : Privacy impact assessment).
- Cartographier avec le registre des activités de traitements.
- Veiller aux données particulières (données sensibles, judiciaires, protection des mineurs, etc.).
- Assurer la sécurité des données.
- Gérer les droits des personnes concernées.
- Veiller aux transferts de données en dehors de l'UE.
- Se préparer à un contrôle.
- Coopérer avec les autorités.

Quels sont les outils permettant d'assurer la conformité ?

- Certifications et codes de conduite.
- Méthodologies de conformité.
- Veille.
- Références.

CYBERNETIES
Academy

Les certifications en Cybersécurité

Nous proposons des certifications en cybersécurité en présentiel, à distance et en e-learning, destinées aux professionnels et aux débutants. Nos nombreuses certifications démontrent nos capacités à fournir des prestations réalisées selon les règles de l'art. Dans des domaines en perpétuelle évolution, nos équipes se forment en continu pour proposer un service de haute qualité.

Red Team & Pentest

Logiciel (web, app...), physique, électronique, full Red Team, osint, social engineering...

SOC 24-7 & CSIRT

SOC 24-7 en <30mn, Starter SOC, SIEM, EDR/MDR, réponses aux incidents (CSIRT)...

Sécurité Cloud & Infrastructure

Audit & Conseil, analyse de risques, identité/pki/sso/iam/pam, Azure & M365, email, firewalls...

Formations & Certifications

Formations, certifications, coaching, workshops, sensibilisations, Capture The Flag (CTF)...

CYBERNETIES Academy

Nos formations certifiantes

Nous vous proposons trois certifications que vous avez la possibilité de suivre en session mutualisée ou en session privée.

Certified Cybersecurity Technician (CCT)

- Prestation proposée : Formation + Certification
- Durée totale de la formation : 5 jours (5x7h)
- Voucher officiel d'examen inclus (en anglais)
- Supports de cours officiel inclus (en anglais)
- QCM d'entrainement inclus (en anglais)
- Labs d'entrainement officiels inclus (en anglais)
- Formateur francophone
- Formateur anglophone (option)

- Prix :

2 990€ (/personne) - session mutualisée

3 990€ (/personne) - session privée (groupe de 2)

2 990€ (/personne) - session privée (groupe de 3 à 4)

1 990€ (/personne) - session privée (groupe de 5 à 10)

Certified SOC Analyst (CSA)

- Prestation proposée : Formation + Certification
- Durée totale de la formation : 3 jours (3x7h)
- Voucher officiel d'examen inclus (en anglais)
- Supports de cours officiel inclus (en anglais)
- QCM d'entrainement inclus (en anglais)
- Formateur francophone

- Prix :

3 490€ (/personne) - session privée (groupe de 2)

2 490€ (/personne) - session privée (groupe de 3 à 4)

1 490€ (/personne) - session privée (groupe de 5 à 10)

Certified Ethical Hacker (CEH)

- Prestation proposée : Formation + Certification
- Durée totale de la formation : 5 jours (5x7h)
- Voucher officiel d'examen inclus (en anglais)
- Supports de cours officiel inclus (en anglais)
- QCM d'entrainement inclus (en anglais)
- Labs d'entrainement officiels inclus (en anglais)
- Formateur francophone
- Formateur anglophone (option)

- Prix :

3 790€ (/personne) - session mutualisée

4 790€ (/personne) - session privée (groupe de 2)

3 790€ (/personne) - session privée (groupe de 3 à 4)

2 790€ (/personne) - session privée (groupe de 5 à 10)

Certified Information Systems Security Professional (CISPP)

- Prestation proposée : Formation
- Durée totale de la formation : 6 jours (6x6h)
- Voucher officiel d'examen en anglais (option 749€)
- Supports de cours officiel inclus (en anglais)
- QCM d'entrainement inclus (en anglais)
- Formateur francophone

- Prix :

3 490€ (/personne) - session mutualisée

4 490€ (/personne) - session privée (groupe de 2)

3 490€ (/personne) - session privée (groupe de 3 à 4)

2 490€ (/personne) - session privée (groupe de 5 à 10)

CYBERNETIES
Academy

Nos formations certifiantes en E-Learning

Nous proposons plus d'une dizaine de formations certifiantes en e-learning, vous permettant de gagner du temps et de faciliter l'apprentissage de vos employés et collaborateurs. Cette formation numérique permet également de former et de certifier un nombre illimité d'apprenants et leur permet d'apprendre de manière autonome et flexible.

Nous vous proposons différentes formules pour suivre les cours en E-Learning avec OffSec :

Les cours individuels :

- 90 jours d'accès aux contenus officiels (cours PDF + vidéos + labs + examens..)
- 1 programme avancé au choix (OSCP, OSEP, OSWE, OSWP, OSWA, OSMR, OSDA)
- 1 tentative pour l'examen officiel (inclus en anglais)
- Tentative d'examen supplémentaire (option - 249€)
- Prix : 1 599€ (/personne)

Learn One :

- 365 jours d'accès aux contenus officiels (cours PDF + vidéos + labs + examens..)
- 1 programme avancé au choix (OSCP, OSEP, OSWE, OSWP, OSWA, OSMR, OSDA)
- 2 tentatives pour l'examen officiel (inclus en anglais)
- Tentative d'examen supplémentaire (option - 249€)
- Accès au pack "Learn Fundamentals" (cursus fondamentaux)
- Prix : 2 499€ (/personne)

Apprentissage illimité:

- 365 jours d'accès aux contenus officiels (cours PDF + vidéos + labs + examens..)
- Accès à tous les programmes avancés (OSCP, OSEP, OSWE, OSWP, OSWA, OSMR, OSDA)
- Tentatives illimitées pour l'examen officiel (inclus en anglais)
- Tentative d'examen supplémentaire
- Accès au pack "Learn Fundamentals" (cursus fondamentaux)
- Prix : 5 499€ (/personne)

Apprentissage des fondamentaux :

- 365 jours d'accès aux contenus officiels (cours PDF + vidéos + labs + examens..)
- Accès au pack "Learn Fundamentals" (cursus fondamentaux)
- Prix : 799€ (/personne)

Pack "Learn Fundamentals" (cursus fondamentaux)

- - Kali Linux Revealed (PEN-103 KLR) + 1x KLCP tentative
- - OffSec Wireless Attacks (PEN-210 WiFu) + 1x OSWP tentative - PEN-100 (recommandé pour PEN-200 cours avancé)
- - SOC-100 (recommendé pour SOC-200 cours avancé)
- - WEB-100 (recommendé pour WEB-200 cours avancé)
- - EXP-100 (recommendé pour EXP-301 cours avancé)
- - CLD-100 Foundational Cloud Security Training
- - SSD-100 Foundational Secure Software Development

CYBERNETIES Academy

Nos formations certifiantes en E-Learning

OSCP / PEN-200

Cette certification est hautement reconnue sur le marché et démontrera vos compétences en piratage éthique. Vous saurez comment effectuer des tests d'intrusion de manière méthodique et avancée.

OSWP / PEN-210

La certification OSWP™ démontrera votre expertise dans l'audit et la sécurisation des appareils sans fil. Cette formation OSWP™ vous permettra d'identifier les failles de chiffrement et de sécurité existantes sur les réseaux 802.11. Vous pouvez ensuite contourner les restrictions de sécurité du réseau et récupérer les clés de chiffrement.

OSDA / SOC-200

Apprenez les bases de la défense de la cybersécurité avec le nouveau cours sur les opérations de sécurité et l'analyse défensive (SOC-200) de la sécurité offensive, conçu pour des postes tels que les analystes juniors du Centre des opérations de sécurité (SOC) et les chasseurs de menaces.

OSWA / WEB-200

OSWA est la meilleure première étape de votre parcours pour maîtriser la pénétration des applications Web Cette certification permet de prouver ses compétences sur les techniques actuelles de code d'exploitation face aux applications modernes.

OSEP / PEN-300

La certification OffSec destinée aux pentesters expérimentés enseigne les compétences nécessaires pour effectuer des tests de pénétration contre des organisations matures possédant une fonction de sécurité établie, et pour contourner de nombreux types de défenses tout en évitant la détection. Elle ne couvre pas spécifiquement l'acte d'échapper à une équipe bleue, mais plutôt le contournement des mécanismes de sécurité conçus pour bloquer les attaques.

OSWE / WEB-300

OSWE/WEB-300 est un cours de sécurité web qui couvre les principes de base de la sécurité web et comment les exploiter. Il explique les principales méthodes d'attaque et les moyens de les contrer. Il est conçu pour être accessible à tous les niveaux d'utilisateurs et offre des activités pratiques pour aider les étudiants à développer leurs compétences web sécurisées.

CYBERNETIES Academy

Nos formations certifiantes en E-Learning

OSED / EXP-301

OSED/EXP-301 est une norme de sécurité électronique fédérale qui définit les exigences et les procédures pour le développement et la mise en œuvre de systèmes de sécurité électronique dans les environnements fédéraux. Les objectifs de cette norme sont de fournir un cadre de sécurité électronique pour garantir que les informations stockées et transmises par les systèmes informatiques fédéraux sont adéquatement protégées contre l'accès non autorisé et interdire l'altération, la modification et la divulgation des informations.

OSMR / EXP-312

OSMR / EXP-312 est un logiciel de gestion des ressources humaines qui permet aux entreprises de gérer leurs processus de RH de manière efficace. Ces fonctionnalités incluent la gestion des informations des employés, l'analyse des données et des rapports, la gestion des processus de recrutement, la gestion des avantages, la gestion des salaires et des avantages sociaux, ainsi que la création et le suivi des stratégies de RH.

OSEE / EXP-401

OSEE/EXP-401 est un type de logiciel de gestion des ressources humaines créé par Oracle. Il fournit des fonctionnalités pour gérer la paie, les avantages sociaux, les recrutements et bien d'autres.

- cours disponible sur demande

KLCP & OSWP / Learn Fundamentals

Les certifications KLCP et OSWP sont conçues pour aider les professionnels de l'informatique à apprendre et à démontrer leurs compétences en matière de sécurité réseau, de sécurité sans fil et de tests d'intrusion. Les certifications incluent également des connaissances et des compétences liées aux principes fondamentaux de la sécurité de l'information, tels que la cryptographie, la mise en réseau et l'administration système.

- 1 formule disponible pour ce cours : Apprentissage des fondamentaux

CYBERNETIES Academy

Nos formations certifiantes en E-Learning avec EC-Council

iLearn CSCU

iLearn CSCU (Certified Secure Computer User) est une certification qui vise à former les utilisateurs à des pratiques sécuritaires pour les ordinateurs et les réseaux.
Il s'agit d'un cours de formation en ligne qui couvre des sujets tels que la sécurité des informations, les normes de la confidentialité des données, la prévention des virus et des logiciels malveillants, ainsi que la protection des systèmes informatiques et des réseaux

- Prix : 299€ (formation certifiante + passage à l'examen)

iLearn CASE JAVA ou CASE.NET

iLearn CASE JAVA ou CASE.NET (Certified Application Security Engineer) est un certificat d'ingénierie de sécurité des applications qui vise à former et à certifier les professionnels dans le domaine de la sécurité des applications.
La certification est conçue pour les développeurs, les architectes des systèmes, les administrateurs système et les professionnels de la sécurité qui travaillent sur des projets de développement de logiciels.

- Prix : 999€ (formation certifiante + passage à l'examen)

iLearn CTIA

iLearn CTIA (Certified Threat Intelligence Analyst) est un programme de certification de niveau professionnel conçu pour aider les professionnels à acquérir les compétences nécessaires pour analyser, comprendre et agir sur les menaces informatiques. Ce programme couvre les principes fondamentaux de la menace, les principales sources de renseignements sur les menaces, les outils et méthodes d'analyse des menaces, ainsi que l'utilisation des outils et des techniques pour repérer, analyser et réagir aux menaces.

- Prix : 999€ (formation certifiante + passage à l'examen)

iLearn CSA

iLearn CSA (Certified SOC Analyst) est une certification professionnelle qui permet aux professionnels de la sécurité informatique et à des analystes d'acquérir une expertise pratique dans la gestion des risques de sécurité des systèmes d'information. Elle offre des connaissances approfondies sur la mise en œuvre et la gestion d'un Centre de sécurité opérationnel (SOC), y compris l'analyse des alertes et des événements de sécurité et la mise en œuvre des contrôles de sécurité.

- Prix : 999€ (formation certifiante + passage à l'examen)

iLearn ECIH

iLearn ECIH (Certified Incident Handler) est un cours en ligne qui enseigne aux participants les principes et pratiques fondamentaux nécessaires pour gérer des incidents de sécurité informatique. Le cours aborde des sujets tels que l'analyse de la vulnérabilité, la collecte d'informations sur les incidents, la gestion des menaces, la planification et le rapport des incidents et la réponse aux incidents.

- Prix : 999€ (formation certifiante + passage à l'examen)

CYBERNETIES Academy

Nos formations certifiantes en E-Learning avec EC-Council

iLearn ECES

iLearn ECES (Certified Encryption Specialist) est une certification qui évalue les connaissances et les compétences des spécialistes en chiffrement. La certification couvre les domaines suivants : planification et mise en œuvre de stratégies de chiffrement, sélection et utilisation des technologies de chiffrement, installation et configuration des produits de chiffrement, et définition des politiques de sécurité nécessaires pour assurer la confidentialité des données.

- Prix : 999€ (formation certifiante + passage à l'examen)

iLearn CEH

iLearn CEH (Certified Ethical Hacker) est un cours de certification en ligne qui offre aux professionnels des outils et des techniques nécessaires pour pratiquer l'ingénierie sociale, les attaques par déni de service, les inclusions Web, etc. Il s'agit d'une formation complète et spécialisée sur la sécurité des systèmes informatiques et des réseaux.

- Prix : 1 999€ (formation certifiante + passage à l'examen)

iLearn CHFI

iLearn CHFI (Hacking Forensic Investigator) est un cours de formation à distance qui se concentre sur les technologies et les procédures nécessaires à l'investigation des cybercrimes. En particulier, le cours met l'accent sur l'utilisation des outils et des techniques d'analyse forensique pour identifier, documenter et rapporter l'activité criminelle.

- Prix : 1 999€ (formation certifiante + passage à l'examen)

iLearn CND

iLearn CND (Certified Network Defender) est une certification de niveau professionnel qui vise à fournir aux professionnels des réseaux informatiques et de la sécurité des connaissances et des compétences pour protéger, détecter et répondre aux menaces informatiques. La certification se concentre sur les technologies, les outils et les techniques nécessaires pour défendre les réseaux informatiques contre les cyberattaques.

- Prix : 1 999€ (formation certifiante + passage à l'examen)

iLearn EDRP

iLearn EDRP (Disaster Recovery Professional) offre des connaissances pratiques et des compétences en matière de planification et de mise en œuvre de la récupération après sinistre. Il aborde des sujets tels que le cycle de vie des plans de reprise après sinistre, la gestion des risques, la sauvegarde et la restauration des données, ainsi que le choix des technologies et des processus de récupération.

- Prix : 1 999€ (formation certifiante + passage à l'examen)

CYBERNETIES Academy

Nos formations certifiantes en E-Learning avec EC-Council

iLearn CPENT

iLearn CPENT (Certified Pentester) est une certification professionnelle qui vise à mesurer les compétences en matière de pentest (tests d'intrusion) et de sécurité informatique. Il s'adresse aux professionnels de la sécurité informatique qui souhaitent développer leurs compétences dans ce domaine et qui veulent démontrer leur expertise aux employeurs potentiels. La certification couvre les domaines d'audit de sécurité, de découverte de vulnérabilités, de tests de pénétration et de contre-mesures de sécurité.

- Prix : 2 499€ (formation certifiante + passage à l'examen)

iLearn CCISO

iiLearn CCISO (Chief Information Security Officer) est un programme de formation en ligne conçu pour aider les professionnels à acquérir les compétences et connaissances nécessaires pour devenir un officier de sécurité des informations (CISO). Il couvre des sujets tels que la gestion des risques, la sécurité des systèmes d'information, la gestion des actifs et la conformité.

- Prix : 2 499€ (formation certifiante + passage à l'examen)

CYBERNETIES Academy

Nos formations certifiantes

Les certification ci-dessous se déroulement seulement en présentiel et à partir de 4 personnes.

ISO 27001 (Lead Implementer)

ISO 27001 est une norme internationale qui définit les exigences pour la mise en place, l'amélioration et le maintien d'un système de gestion de la sécurité de l'information. Elle fournit des directives sur la façon de gérer et de protéger les informations sensibles et les données de l'entreprise. Elle donne aux organisations des lignes directrices pour la mise en œuvre d'un système de gestion de la sécurité des informations (SGSI) afin de protéger leurs actifs critiques.

- Prix : 3 200€ (formation certifiante + passage à l'examen)

ISO 27005 (Risk manager)

ISO 27005 est une norme internationalement reconnue qui fournit des directives pour la gestion des risques dans le cadre de la sécurité de l'information. La certification ISO 27005 (Risk Manager 001) est une certification professionnelle spécialisée qui montre que vous avez reçu une formation et une formation spécifiques en matière de gestion des risques de sécurité de l'information. La certification vise à démontrer votre capacité à appliquer et à mettre en œuvre des processus, des pratiques et des méthodologies de gestion des risques conformes à la norme ISO 27005.

- Prix : 3 000€ (formation certifiante + passage à l'examen)

Lead Cloud Security Manager

La formation Lead Cloud Security Manager est une formation de spécialisation en sécurité cloud qui vise à aider les professionnels à développer des compétences techniques et comportementales pour gérer les menaces et les vulnérabilités liées à la sécurité cloud. La formation se focalise sur la gestion des risques, la conformité aux standards et la planification et la mise en œuvre de stratégies de sécurité cloud. Elle aborde également des sujets tels que la gestion des identités, la plate-forme de sécurité cloud, la gestion des droits d'accès et la gestion des incidents.

- Prix : 3 500€ (formation certifiante + passage à l'examen)

ISO/IEC 27002 Lead Manager

ISO/IEC 27002 (Lead Manager) est une norme internationale qui fournit des lignes directrices pour la gestion des risques et la sécurité des systèmes d'information. Elle fournit des recommandations sur la sélection, l'implémentation et la surveillance des contrôles de sécurité pour les systèmes d'information. Elle vise à aider les organisations à établir et à maintenir un niveau approprié de sécurité des systèmes d'information. La norme peut aider les gestionnaires à prendre des décisions informées sur les mesures à prendre pour protéger les informations et communiquer ces mesures aux parties prenantes.

- Prix : 3 500€ (formation certifiante + passage à l'examen)

PECB Lead Pentest

PECB Lead Pentest Certification 001 est une certification professionnelle qui est conçue pour reconnaître les compétences des auditeurs de sécurité informatique et leur permettre de mettre en œuvre et de gérer des tests de pénétration. La certification couvre des domaines tels que la planification des tests, l'exécution des tests, l'analyse des résultats, la présentation des rapports et l'intégration des meilleures pratiques.

- Prix : 3 200€ (formation certifiante + passage à l'examen)

CYBERNETIES Academy

Nos formations certifiantes

ISO 27001 (Lead Auditor)

La certification ISO 27001 Lead Auditor est une certification professionnelle spécialisée qui démontre que l'auditeur a une connaissance et une compréhension approfondies des exigences de l'ISO 27001 et de son processus d'audit, et qu'il est capable de mener des audits de conformité ISO 27001.

- Prix : 3 200€ (formation certifiante + passage à l'examen)

Risk manager

Le Risk Manager (méthode d'analyse de risque EBIOS) est une méthode de gestion des risques qui vise à évaluer et à gérer les risques liés à un projet, à une activité ou à un processus. Cette méthode est basée sur une approche systémique et itérative qui prend en compte les contraintes, les acteurs, les risques et leur interconnexion. Elle permet aux entreprises d'identifier, d'analyser et de gérer les risques de manière plus efficace et plus cohérente.

- Prix : 2 100€ (formation certifiante + passage à l'examen)

AWS Technical Essentials

AWS Technical Essentials est une formation destinée aux développeurs et aux professionnels IT. Il fournit une introduction de base aux services cloud et aux produits AWS, ainsi qu'une compréhension approfondie du Cloud Computing et de la façon dont AWS peut aider les organisations à optimiser leur utilisation des technologies cloud.

- Prix : 1 000€

Architecture sur AWS

Architecture sur AWS est une méthode pour construire et gérer des applications et des services sur le cloud computing d'Amazon Web Services (AWS). Il s'agit d'un ensemble de services d'infrastructure et de plateformes que les entreprises peuvent utiliser pour développer, héberger et gérer leurs applications de manière sécurisée et évolutive. AWS offre des services pour le stockage, le calcul, le réseau, la base de données, le développement et l'analyse, qui peuvent être combinés pour créer des architectures de cloud personnalisées.

- Prix : 2 500€ (formation certifiante + passage à l'examen)

Developing on AWS

AWS fournit un ensemble complet de services et d'outils basés sur le cloud qui permettent aux développeurs de créer et de déployer des applications dans le cloud. Ces services incluent la puissance de calcul, le stockage de bases de données, la diffusion de contenu et d'autres éléments essentiels pour les applications cloud.

- Prix : 2 500€ (formation certifiante + passage à l'examen)

DeVops Engineering on AWS

DevOps Engineering on AWS est un ensemble d'outils, de services et de pratiques permettant de mieux exploiter et gérer les infrastructures cloud d'Amazon Web Services (AWS). Cela comprend des outils pour le déploiement, la gestion et le monitoring des services AWS, ainsi que des pratiques DevOps pour le développement, le test et le déploiement des applications sur AWS.

- Prix : 2 800€ (formation certifiante + passage à l'examen)

CYBERNETIES Academy

Nos formations certifiantes

Bases de données sur AWS

Planifier et concevoir des bases de données sur AWS consiste à créer et configurer des bases de données sur le cloud AWS pour stocker et gérer des données. Cela inclut le choix et la configuration d'un type de base de données approprié, la conception et l'optimisation des tables et des index, la définition des règles de sécurité et la gestion des performances. AWS offre une gamme complète de services de base de données pour différents scénarios, dont Amazon RDS, Amazon Aurora, Amazon DynamoDB et Amazon Redshift.

- Prix : 2 800€ (formation certifiante + passage à l'examen)

AWS Security essentials

AWS Security Essentials est un ensemble de services et de technologies qui vous permettent de protéger vos applications et données sur Amazon Web Services (AWS). Il comprend des solutions de surveillance et d'audit des ressources, la gestion des identités et des accès, le chiffrement des données, la protection contre les attaques et les menaces, et la gestion des outils de contrôle. Ces solutions aident à minimiser les risques, à détecter les anomalies et à réagir rapidement aux incidents

- Prix : 1 000€ (formation certifiante + passage à l'examen)

Ingénierie de sécurité sur AWS

L'ingénierie de sécurité sur AWS est une pratique qui permet de protéger votre système informatique contre les menaces externes et internes. Elle s'applique à la configuration et à la gestion des systèmes informatiques, des applications et des données sur Amazon Web Services (AWS). Elle implique la mise en œuvre de mesures de sécurité pour assurer que les informations sont sécurisées et protégées, que le système est fiable et opérationnel, et que les applications et les données sont accessibles aux utilisateurs légitimes.

- Prix : 2 800€ (formation certifiante + passage à l'examen)

Running Containers on AWS EKS

L'exécution de conteneurs sur AWS EKS (Amazon Elastic Kubernetes Service) est un service géré qui permet aux organisations de déployer et de gérer plus facilement des applications conteneurisées sur Amazon Web Services (AWS). Il fournit un environnement hautement fiable et sécurisé pour l'exécution de charges de travail conteneurisées sur le cloud AWS. Il simplifie également le processus de mise à l'échelle et de gestion des applications et des services conteneurisés, permettant aux organisations de déployer, gérer et mettre à l'échelle rapidement et facilement leurs applications sur le cloud AWS.

- Prix : 2 800€ (formation certifiante + passage à l'examen)

CYBERNETIES Academy

Nos formations certifiantes

Certification ISO/IEC 27001 foundation

La certification ISO/IEC 27001 Foundation et Compléments ISO/IEC 27002 est une certification internationale prouvant que votre système de gestion de la sécurité de l'information (SGSI) répond aux normes internationales. La certification vous aidera à améliorer votre sécurité de l'information et à vous conformer aux réglementations et aux normes internationales. Il vous aidera également à améliorer la confiance des clients et à établir votre crédibilité sur le marché.

- Prix : 810€ (certification + passage à l'examen compris)
- Durée : 3 jours

ISO/CEI 27001 lead auditor

ISO/CEI 27001 Lead Auditor est une certification qui reconnaît les compétences des auditeurs en matière de conformité aux normes de sécurité de l'information. La certification est conçue pour aider les professionnels à évaluer, implémenter et maintenir des systèmes de gestion de la sécurité de l'information conformes à la norme ISO/CEI 27001. Les auditeurs certifiés ISO/CEI 27001 Lead Auditor sont en mesure d'auditer et de certifier la conformité aux exigences de la norme

- Prix : 2 000€ (certification + passage à l'examen compris)
- Durée : 5 jours

ISO/CEI 27001 lead implementer

ISO/CEI 27001 Lead Implementer est une certification professionnelle qui reconnaît la compétence d'une personne à mettre en œuvre des systèmes de gestion de la sécurité de l'information conformément aux exigences de la norme ISO/CEI 27001. Cette certification indique que le titulaire a une bonne compréhension des normes, des processus et des méthodologies requis pour mettre en œuvre un système de gestion de la sécurité de l'information et en assurer le maintien.

- Prix : 2 000€ (certification + passage à l'examen compris)
- Durée : 5 jours

ISO/CEI 27005 security risk manager

ISO/CEI 27005 Security Risk Manager est un standard international pour la gestion des risques de sécurité qui fournit des lignes directrices pour l'identification, l'évaluation, la gestion et la surveillance des risques de sécurité. Le standard s'applique à tous les types d'organisation et couvre l'ensemble des technologies, infrastructures et services informatiques. Il définit des principes et des pratiques communes pour identifier et gérer les risques de sécurité et fournit des lignes directrices pour le développement et la mise en œuvre d'une stratégie de gestion des risques de sécurité.

- Prix : 2 000€ (certification + passage à l'examen compris)
- Durée : 5 jours

ISO/CEI 22301 lead implementer

ISO/CEI 22301 Lead Implementer est une certification qui permet aux professionnels de démontrer leur expertise dans la mise en œuvre et l'audit d'un Système de Management de la Continuité des Activités (SMCa). Elle couvre les domaines de la planification stratégique, de la gestion des risques, de l'analyse des vulnérabilités, de la mise en œuvre des activités et de l'évaluation des résultats. La certification ISO/CEI 22301 Lead Implementer permet aux professionnels d'aider les organisations à s'assurer que leurs activités se dérouleront sans interruption en cas de risques ou de perturbations.

- Prix : 2 000€ (certification + passage à l'examen compris)
- Durée : 5 jours

CYBERNETIES Academy

Nos formations certifiantes

Bootcamp : IT security leader - certification ITIL

Un Bootcamp IT Security Leader - Certification ITIL est une formation intensive destinée aux professionnels de l'informatique et de la sécurité des systèmes d'information. Il s'agit d'une formation de 5 jours qui couvre les domaines de l'architecture de sécurité, de l'analyse des risques, de la gestion des incidents, de l'audit et de la conformité, de la gestion des configurations et des services, ainsi que de la gestion des incidents et des problèmes. La formation vise à aider les professionnels à obtenir la certification ITIL, qui est une certification reconnue dans le domaine des technologies de l'information.

- Prix : 1 824€ (certification + passage à l'examen compris)
- Durée : 6 jours

Délégué à la protection des données personnelles (DPO)

Le délégué à la protection des données personnelles (DPO) est une personne chargée de veiller à la mise en œuvre et à l'application des règles de protection des données personnelles dans les organisations. Il est responsable de surveiller et de surveiller le traitement des données à caractère personnel, et de s'assurer que les principes de protection des données personnelles sont respectés. Il est également responsable de fournir des conseils et des avis sur les questions liées à la protection des données, de surveiller et de gérer les plaintes relatives à la protection des données, et de sensibiliser le personnel à la protection des données.

- Prix : 1 699€ (certification + passage à l'examen compris)
- Durée : 5 jours

Certification ITIL 4 foundation

La certification ITIL 4 Foundation est une certification professionnelle internationale qui vise à fournir aux professionnels des connaissances et des compétences nécessaires pour gérer efficacement un système de service informatique. La certification ITIL 4 Foundation est conçue pour aider les entreprises à améliorer leurs processus et leurs activités de service informatique en mettant l'accent sur les principes et les pratiques de l'approche ITIL 4. Elle couvre les principaux domaines de base de l'ITIL 4, tels que les principes, les processus, les fonctions et les rôles, les pratiques et les techniques de service informatique

- Prix : 815€ (certification + passage à l'examen compris)
- Durée : 3 jours