SysDream
Cybersécurité Hub One

FORMATIONS EN **CYBERSÉCURITÉ**

SYSDREAM FORMATION

Édition **2025**

Centre de formation agréé n°11 93 05949 93 | Certifié Qualiopi

Qualiopi
processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante :
ACTIONS DE FORMATION

sysdream.com

SOMMAIRE

ÉDITORIAL

2024 : UNE ANNÉE CHARNIÈRE POUR LA CYBERSÉCURITÉ

L'année 2024 a marqué une montée en puissance des cybermenaces, notamment à l'occasion d'événements comme les Jeux Olympiques de Paris, et avec des attaques de plus en plus sophistiquées. L'entrée en vigueur de la directive NIS 2, en octobre 2024, impose également de nouvelles contraintes pour près de 100 000 PME, ETI et organismes publics, exigeant une gestion du risque renforcée.

SYSDREAM À L'AVANT-GARDE DE LA CONFORMITÉ ET DE LA FORMATION

En réponse à ces enjeux, SysDream a lancé son programme « NIS 2 Ready » au Forum INCYBER 2024 pour accompagner les entreprises dans leur conformité à cette nouvelle directive.

NOUVEAUTÉ 2025 : MALICE TRAINING

Nous renforçons notre offre de formation avec « MALICE Training », une plateforme SaaS dédiée aux profils techniques (administrateurs, développeurs, experts réseau). Avec 70 challenges et 4 parcours spécialisés (développement, hacking avancé/expert, SOC analystes), elle s'adapte à différents niveaux et propose des exercices pratiques et modulaires. Des sessions de coaching sont également proposées pour un accompagnement humain personnalisé.

UN ENGAGEMENT FORT POUR LA MONTÉE EN COMPÉTENCES

Cette plateforme s'adresse aux grandes entreprises, écoles, et aux professionnels en reconversion, offrant des outils pour développer des compétences cruciales en cybersécurité. Nos formations, axées sur la pratique, sont animées par des experts reconnus qui partagent leurs expériences en audit, test d'intrusion, et réponse aux incidents. Nous formons chaque année plus de 4 000 professionnels, avec des parcours en ligne avec les référentiels de l'ANSSI.

2024 : LANCEMENT DES ACADÉMIES SYSDREAM

Enfin, nous avons également lancé nos premières académies de cybersécurité pour des clients grands comptes, intégrant des programmes de reconversion et de montée en compétences, financés par les entreprises ou des fonds propres aux salariés.

Rejoindre nos formations, c'est bénéficier de 20 ans d'expérience et d'un accompagnement tout au long du cycle de sécurisation de vos systèmes d'information.

Ylan ELKESLASSY
Directeur BL Formation,
Cyber-Entraînement et Evènements

La certification qualité Qualiopi a été attribuée au titre des actions de formation à la société SysDream.

SysDream est également qualifiée PASSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information) par l'ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information.

UNE EXPERTISE À 360°

Pure player de la cybersécurité depuis 2004, l'audit, le conseil, et la formation sont au cœur de l'ADN de SysDream.

Nous avons enrichi notre offre de formation au fil des années pour accompagner et répondre aux besoins de nos clients tout au long du cycle de vie de la sécurisation de leur système d'information.

Notre expertise à 360° se décline également dans notre proposition de formations.

LES FORMATIONS :

FORMATION HACKING
7 FORMATIONS

SÉCURITÉ DÉFENSIVE
4 FORMATIONS

FORMATION PENTEST
3 FORMATIONS

FORMATION ANALYSTE SOC
2 FORMATIONS

FORMATION CERTIFIANTE
23 FORMATIONS

SENSIBILISATION CYBERSÉCURITÉ
3 FORMATIONS

OSINT
1 FORMATION

LES PARCOURS DE FORMATION

Nous proposons un parcours de formation pour un grand nombre des métiers du référentiel des métiers de la cybersécurité de l'ANSSI. Ainsi, en fonction de votre expérience et de vos souhaits d'évolution, vous trouverez dans les pages suivantes un programme de formations adapté à votre projet professionnel.

CURSUS – SOCLE COMMUN & SENSIBILISATION À LA CYBERSÉCURITÉ

Public visé : toute personne désirant comprendre les menaces liées aux attaques informatiques

Sensibilisation à la cybersécurité (SAC) + Hacking & Sécurité : les Fondamentaux (HSF) + Hacking & Sécurité : Avancé (HSA)

CURSUS DÉVELOPPEUR

- Sensibilisation au développement sécurisé (SDS)
- Sécurité des applications mobile (SAM)
- Audit de site Web (AUDWEB)
- Certified DevSecOps Engineer (EDCDE)

CURSUS DÉVELOPPEUR vers AUDITEUR DE SÉCURITÉ

- Sensibilisation au développement sécurisé (SDS)
- Open Source Intelligence : les Fondamentaux (OSINT)
- Hacking et sécurité : Avancé (HSA)
- Audit de site Web (AUDWEB)
- Hacking et sécurité : Expert (HSE)

AUDITEUR DE SÉCURITÉ TECHNIQUE - PENTESTER (junior)

- Certified Ethical Hacker v13 (CEH) ✓
- Hacking et sécurité : les Fondamentaux (HSF)
- Audit de site Web (AUDWEB)
- Certified Cybersecurity Technician (CCT) ✓
- Hacking et sécurité : Avancé (HSA)

AUDITEUR DE SÉCURITÉ TECHNIQUE - PENTESTER (confirmé)

- Hacking et sécurité : Expert (HSE)
- Sécurité Windows & Active Directory (SWAD)
- Sécurité des applications mobile (SAM)
- Exploitation de Vulnérabilités Applicatives (EVA)
- Computer Hacking Forensic Investigator v11 (CHFI) ✓
- Certified Cloud Security Engineer (CCSE) ✓

✓ Formation certifiante

LES PARCOURS DE FORMATION

RESPONSABLE DE PROJET SÉCURITÉ

- Sensibilisation à la cybersécurité (SAC)
- Hacking et sécurité : les Fondamentaux (HSF)
- Hacking et sécurité : Avancé (HSA)
- Audit de site Web (AUDWEB)
- ISO 27032 : Lead Cybersecurity Manager (ISO 27032 LCM)
- Certified Information Systems Security Professionnal (CISSP)

AUDITEUR DE SÉCURITÉ ORGANISA-TIONNELLE

- Certified Ethical Hacker v13 (CEH)
- Certified Information Systems Auditor (CISA)
- ISO 27001: Certified Lead Auditor (ISO 27001 LA)
- ISO 27002 Foundation (ISO 27002 F)
- ISO 27005: Certified Risk Manager + EBIOS (ISO 27005 RM+ EBIOS)

DSI

- Hacking et sécurité : les Fondamentaux (HSF)
- Hacking et sécurité : Avancé (HSA)
- ISO 27001 : Certified Lead Implementer (ISO 27001 LI)
- ISO 27002 : Lead Manager (ISO 27002 LM)
- ISO 31000 : Risk Manager (ISO 31000)

RSSI (confirmé)

- Certified Information Systems Auditor (CISA)
- ISO 27001: Certified Lead Implementer (ISO 27001 LI)
- Certified Information Security Manager (CISM)
- Certified NIS2 Directive Lead Implémenter (NIS2 LI)
- Certified Chief Information Security Officer (CCISO)

ADMINISTRATEUR SYSTÈME & RÉSEAUX

- Sécurisation des réseaux (SR)
- Sécurisation Linux (SL)
- Certified Cloud Security Engineer (CCSE)
- Certified DevSecOps Engineer (ECDE)
- Certified Network Defender (CND)

Formation certifiante

ARCHITECTE SÉCURITÉ

- Certified Ethical Hacker v13 (CEH)
- Sécurisation des réseaux (SR)
- Sécurité Windows & Active Directory (SWAD)
- Mise en place de sondes de détection d'intrusions (SDI)
- Certified Network Defender (CND)

OPÉRATEUR - ANALYSTE SOC

- Sécurisation Linux (SL)
- Sécurisation des réseaux (SR)
- Analyse inforensique avancée et réponse aux incidents (AIARI)
- EC-Council Certified Incident Handler v3 (ECIH)
- Certified SOC Analyst (CSA)

ANALYSTE DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ (CERT)

- Certified Ethical Hacker v13 (CEH)
- Analyse inforensique avancée et réponse aux incidents (AIARI)
- EC-Council Certified Incident Handler v3 (ECIH)
- Rétro-Ingénierie de logiciels malveillants (RILM)
- Malwares : détection, identification et éradication (MDIE)
- Computer Hacking Forensic Investigator v11 (CHFI)

Formation certifiante

POURQUOI SYSDREAM ?

Forte de plus de 20 ans d'expérience en matière de cybersécurité et attachée à la qualité de ses formations, ainsi qu'à la satisfaction de ses clients, SysDream s'engage sur 4 grands piliers :

1 - Des formations adaptées aux besoins du marché

Plus de 40 formations spécialisées sont actualisées chaque année en fonction des évolutions du marché et de l'actualité de la cybersécurité.

2 - Des formateurs toujours en activité pour partager leurs expériences et bonnes pratiques

Nous nous assurons que nos formateurs soient toujours au cœur des problématiques du marché pour qu'ils puissent partager leurs expériences, élaborer des cas pratiques concrets et proposer des mises en situation réelles.

3 - Une formation axée sur la qualité opérationnelle

Nos formateurs sont spécialistes dans leur domaine et disposent des meilleures certifications en cybersécurité.

SysDream est certifiée Qualiopi : cette certification nationale atteste de la qualité des processus mis en œuvre par les organismes de formation contribuant au développement des compétences. Elle est délivrée par des certificateurs indépendants et permet aux organismes certifiés d'accéder aux financements publics, de mutualiser et d'augmenter leur visibilité et leur crédibilité auprès de leurs publics cibles. SysDream a obtenu la certification Qualiopi au titre de la catégorie « Actions de formation « en 2022. Cette certification est valable 3 ans.

4 - SysDream - un gage de confiance

Centre de formation depuis plus de 20 ans, SysDream accompagne chaque année plus de 4 000 professionnels d'entreprises de toutes tailles.

SysDream, société pionnière en cybersécurité, propose une offre compléte dans les domaines de la formation, du conseil, de l'audit, du test d'intrusion (pentest) et d'un SOC Managé offrant ainsi une vision et des compétences à 360° en cybersécurité.

- Nos formateurs obtiennent une note moyenne de 9,7/10
- 98% de nos stagiaires recommandent nos formations

Données 2024 (recueillies du 1er janvier au 15 septembre 2024).

NOS ENGAGEMENTS

Expérience de la formation

Depuis 20 ans, SysDream forme au quotidien des dizaines de professionnels sur plus d'une trentaine de thématiques. Dans un souci d'amélioration continue, chaque stagiaire remplira au terme de sa formation un questionnaire de satisfaction. Par ailleurs, ce catalogue évolue régulièrement pour satisfaire les besoins et les attentes de nos clients.

Environnement de travail complet

Un support technique de qualité est mis à la disposition de chaque stagiaire durant sa formation. Un réseau virtuel héberge tous les types de systèmes : Microsoft, Linux et Unix, favorisant ainsi le bon déroulement des travaux pratiques.

Travaux pratiques

Toutes nos formations sont construites avec une alternance de cours théoriques et de cas pratiques dirigés par l'intervenant afin d'améliorer l'acquisition des savoirs.

Formations à taille humaine

Afin de favoriser l'interaction et la pratique, nous mettons à disposition un poste informatique par stagiaire lors des formations en présentiel et avons fixé un maximum de 12 apprenants par session pour garantir la disponibilité du formateur.

Formateurs

Tous nos intervenants sont régulièrement consultants pour des grands groupes industriels ou des Ministères.
Nos formateurs disposent de certifications et de qualifications dans plusieurs domaines de la cybersécurité.

POLITIQUE HANDICAP

Vous êtes en situation de handicap et vous souhaitez suivre une de nos formations ?

La loi du 5 septembre 2018 pour la « liberté de choisir son avenir professionnel » a pour objectif de faciliter l'accès à l'emploi des personnes en situation de handicap.
Notre organisme de formation s'efforce, dans la mesure du possible, de donner à tous les mêmes chances d'accéder ou de maintenir l'emploi.

C'est pourquoi nous vous invitons, en amont de votre session, à nous indiquer tout besoin spécifique vous permettant de suivre votre formation dans les meilleures conditions. Lors d'un entretien de recueil de vos attentes et besoins, nous étudierons ensemble la faisabilité de la réalisation de l'action de formation.

Si toutefois nous ne parvenons pas à prendre en compte votre handicap, nous vous orienterons alors vers des organismes compétents.

Nous vous invitons également à consulter le site internet :
https://www.monparcourshandicap.gouv.fr/formation-professionnelle
pour obtenir des informations complémentaires.

Si vous êtes salarié dans le secteur privé :

Vous bénéficiez des mêmes conditions d'accès à la formation que tout autre salarié, avec un droit supplémentaire à un financement, pour cela, merci de contacter : l'AGEFIPH de votre région.

Si vous êtes salarié dans le secteur public :

Vous bénéficiez des mêmes conditions d'accès à la formation que tout autre salarié, avec un droit supplémentaire à un financement, pour cela, merci de contacter : le FIPHFP de votre région.

Si vous êtes demandeur d'emploi :

Pour permettre à un demandeur d'emploi en situation de handicap d'acquérir les compétences nécessaires à un emploi durable, l'AGEFIPH, Pôle Emploi, CAP Emploi ou d'autres financeurs peuvent participer à la prise en charge du coût d'une formation. Celle-ci doit s'inscrire dans un parcours d'insertion et offrir des perspectives réelles et sérieuses d'accès à l'emploi.
Pour bénéficier de ces aides, le candidat doit contacter son conseiller Pôle Emploi ou Mission Locale qui l'orientera vers les dispositifs de financement possibles et les mieux adaptés à son projet professionnel. Toute demande d'aide devra être adressée au moins deux mois avant l'entrée en formation.

Les cyberattaques se multiplient et concernent tout le monde : petites, moyennes et grandes entreprises, administration. SysDream a lancé en 2024 ses premières académies de formation Cyber.

Fort de plus de 20 ans d'expérience en formation, SysDream a fait le choix d'accompagner toute personne désireuse de s'initier ou de renforcer ses compétences en cybersécurité par le biais d'académies diplômantes et certifiantes.

- Fondamentaux, sensibilisation, réglementations
- Détection d'incidents, pentests, forensic, analystes SOC
- Référentiels ISO
- Sécurité Systèmes et Réseaux
- Sécurité applicative

CYBER ACADEMY BY SYSDREAM

- Accompagnement au processus de sélection des apprenants avant entrée dans l'académie
- Remise à niveau des apprenants avant entrée dans le cursus de formation
- Parcours de formation (blocs communs/blocs spécifiques) suivant les exigences client et impératifs projet
- Utilisation des plates-formes de sensibilisation et de formation de SysDream : Malice Learning, Malice Training
- Des modalités pédagogiques adaptables et variées présentiel/distanciel/hybride/classes virtuelles/MOOC en format SCORM/elearning tutoré
- Dans notre centre de formation à Levallois ou dans les locaux client
- Les + des académies SysDream : une «learning expedition» avec visite de notre SOC PDIS et un « Vis ma vie de Pentester »

Les profils concernés sont les demandeurs d'emploi, les salariés en reconversion interne et les personnes souhaitant effectuer une reconversion en cybersécurité.

RECONNAISSANCE DE VOS PARCOURS CYBER

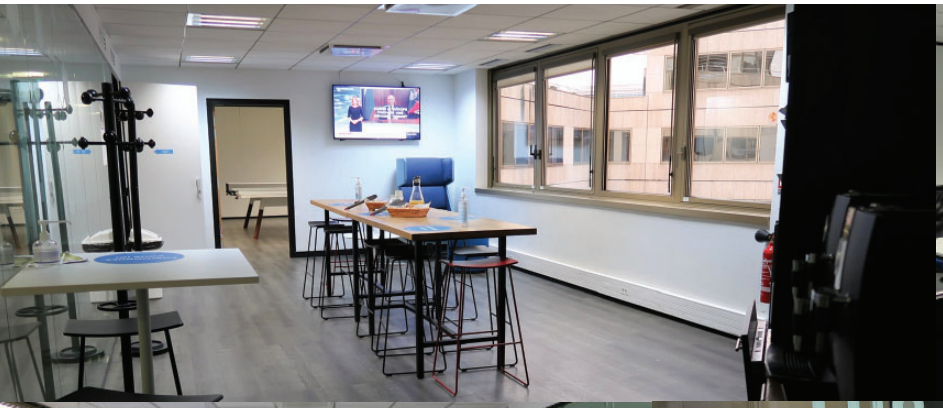
- Parcours certifiants et diplômants avec passage devant jurys et délivrance de titres RNCP suivant les blocs de compétences
- Certifications internationales (CSA, PECB, EC Council...)
- Adapté en nombre de jours et d'heures de formation aux prises en charge par les OPCO (POEI, POEC,..) et par France Travail

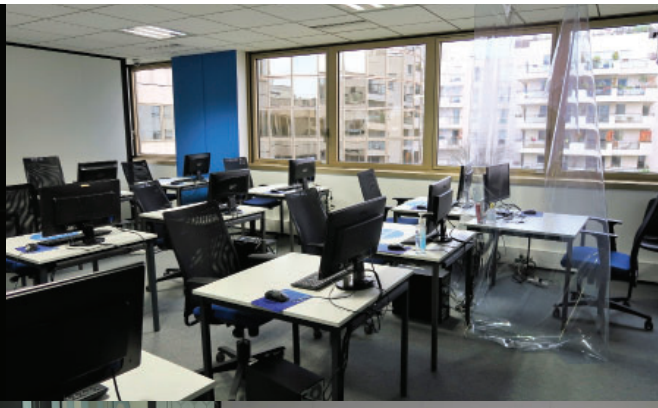
LE CENTRE DE FORMATION

Nous mettons à votre disposition le matériel le plus récent et assurons à chacun des stagiaires un poste individuel équipé des logiciels nécessaires pour toutes nos formations.

Certaines de nos salles sont spécialement équipées pour les sessions en mode hybride offrant ainsi à nos stagiaires les meilleures conditions d'apprentissage possibles qu'ils soient en présentiel ou en distanciel.
Ces équipements permettent des échanges fluides quel que soit le mode de dispense choisi.

Toutes nos salles sont lumineuses et climatisées.
Un espace détente est mis à disposition de nos clients.



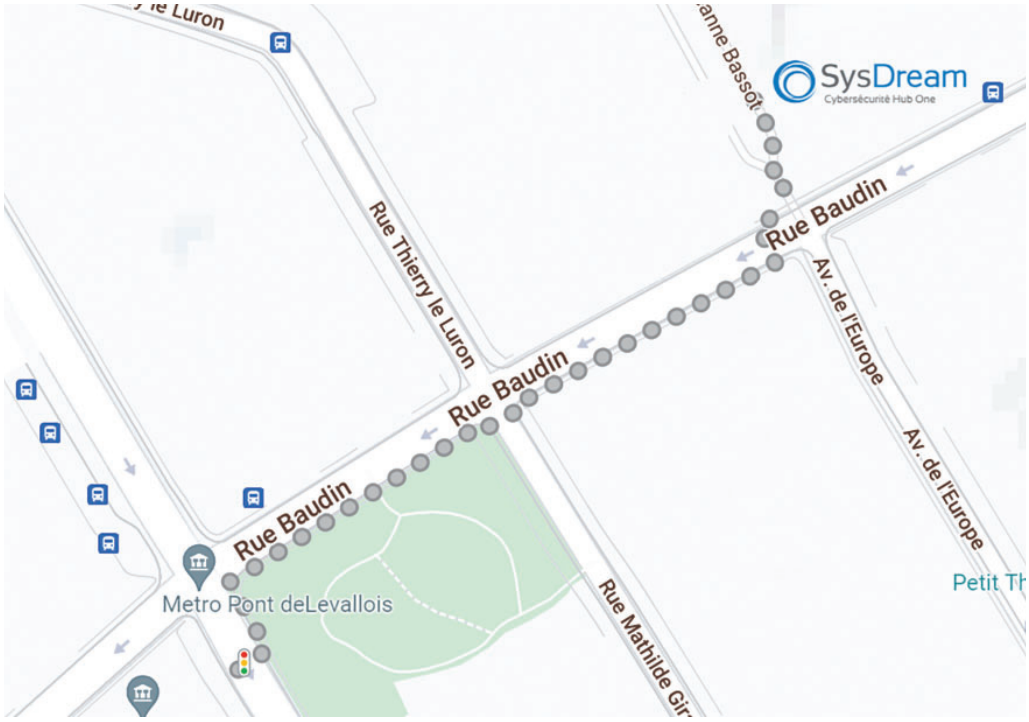


LE CENTRE DE FORMATION

SysDream

14, place Marie-Jeanne Bassot
92300 Levallois
France

Le centre de formation est accessible par la ligne 3 du métro à seulement 15 minutes de la gare de Paris Saint-Lazare et à 300 mètres de la station de métro Pont de Levallois-Bécon.



LES FORMATIONS

FORMATION HACKING

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
EVA	Exploitation de Vulnérabilités Applicatives	5 jours		10			19				15		24	
HSF	Hacking & Sécurité : les Fondamentaux	2 jours		3		7		5			18		3	8
HSA	Hacking & Sécurité : Avancé	5 jours	27		31						29		24	
HSE	Hacking & Sécurité : Expert	5 jours		10				16			8			1
RILM	Rétro-Ingénierie de Logiciels Malveillants	5 jours	27		31					25		27		
SDS	Sensibilisation au Développement Sécurisé	2 jours			6			5			18		20	
SWAD	Sécurité Windows & Active Directory	3 jours		5			12				15			10

AVANCÉ

FORMATION HACKING

EXPLOITATION DE VULNÉRABILITÉS APPLICATIVES

Maîtrisez l'ensemble des techniques d'exploitation applicatives

Ce cours fait le tour des vulnérabilités applicatives et des techniques d'exploitation sur Windows et Linux, de la conception de shellcodes sur mesure pour architectures 32 et 64 bits à l'exploitation de vulnérabilités de type «use after free», combinée à du «Return Oriented Programming» (ROP).

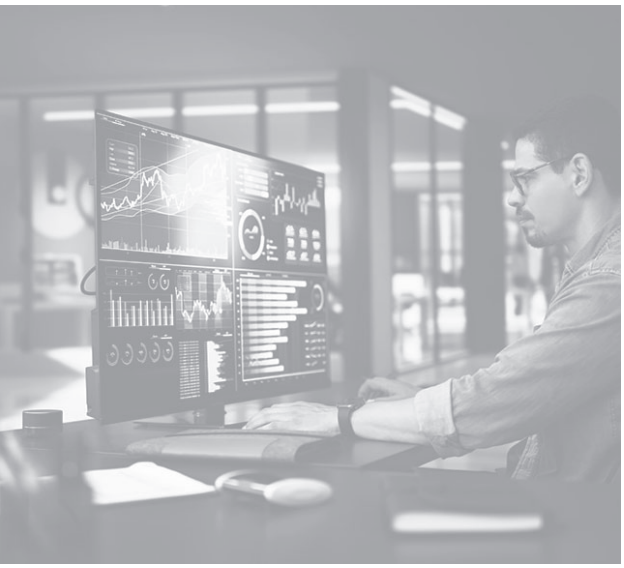
Il s'agit d'une formation pratique avec des exploitations sur des applications d'apprentissage et des programmes réels.

Code : EVA

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.



JOUR 1

Shellcoding Linux, première partie (32 bits)
- Environnement de conception de shellcodes
- Shellcode standard
- Reverse shell TCP
- Bind shell TCP

Buffer overflow sous Linux (IA-32)
- Exploitation sans protection
- Exploitation avec ASLR
- Exploitation avec NX
- Exploitation avec ASLR et NX (ROP)
- Exploitation sur IA-64 (64 bits)

JOUR 2

Shellcoding Linux, deuxième partie
- Shellcoding multi-staged
- Shellcoding 64 bits
- Shellcode standard 64 bits
- Reverse shell 64 bits

Shellcoding sous Windows
- Environnement de conception de shellcodes
- Technique de shellcoding générique

JOUR 3

Shellcoding sous Windows (suite)
- Shellcode MessageBox
- Shellcode Execute

Buffer overflow sous Windows
- Exploitation sans protection
- Contournement du stack canary (/GS)
- Contournement de la protection SafeSEH
- Contournement du DEP

JOUR 4

Format String
- Présentation
- Exploitation sous Windows
- Exploitation sous Linux
- Contre-mesures actuelles

JOUR 5

Vulnérabilités liées à la mémoire dynamique
- Présentation
- Débordement mémoire dans le tas
- Heap Spray
- Use After Free

PROCHAINES DATES

10 février 2025
19 mai 2025
15 septembre 2025
24 novembre 2025

OBJECTIFS

- Apprendre à écrire des shellcodes sur architecture IA 32
- Présenter et exploiter des débordements de tampon (buffer overflow) sous Linux sur architecture IA 32
- Présenter et exploiter des débordements de tampon (buffer overflow) sous Linux sur architecture IA 64
- Apprendre à écrire des shellcodes sous Linux sur architecture IA 64
- Apprendre à écrire des shellcodes sous Windows sur architecture IA 32
- Présenter et exploiter des débordements de tampon (buffer overflow) sous Windows sur architecture IA 32 sans protections
- Présenter et exploiter des débordements de tampon (buffer overflow) sur Windows sous architecture IA 32 avec protection SafeSEH
- Présenter et exploiter des débordements de tampon (buffer overflow) sur Windows sous architecture IA 32 avec protection DEP
- Présenter et exploiter des débordements de tampon (buffer overflow) sur Windows sous architecture IA 32 avec toutes les protections
- Comprendre et exploiter des vulnérabilités de type format string
- Comprendre le fonctionnement de la heap
- Comprendre et exploiter les heap overflows avec la protection NX

INFORMATIONS GÉNÉRALES

Code : EVA
Durée : 5 jours
Prix : 4 150 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Pentesters

PRÉ-REQUIS

- Avoir des notions de sécurité informatique
- Maîtriser des systèmes Windows et Linux
- Avoir des connaissances en architectures IA 32 et IA 64
- Avoir des bonnes connaissances en C, en Python et assembleur

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne

HACKING & SÉCURITÉ : LES FONDAMENTAUX

Apprenez les fondamentaux de la sécurité informatique

Code : HSF

Cette formation est une première approche des pratiques et des méthodologies utilisées dans le cadre de tests d'intrusion. Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes. L'objectif est de vous fournir les premières compétences techniques de base, nécessaires à la réalisation d'audits de sécurité ou de tests d'intrusion. Ainsi, vous jugerez de l'impact réel des vulnérabilités découvertes sur le SI.

Il s'agit d'une bonne introduction au cours HSA pour toute personne souhaitant acquérir les connaissances techniques de base.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction
- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test

Prise d'information
- Objectifs
- Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d'information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d'exploits

Réseau et attaques connues
- Rappels modèles OSI et TCP/IP
- Protocoles ARP, IP, TCP et UDP
- NAT
- Scan de ports
- Sniffing et outils
- ARP Cache Poisoning
- DoS / DDoS

JOUR 2

Attaques à distance
- Introduction à Metasploit Framework
- Scanner de vulnérabilités
- Attaque d'un poste client
- Attaque d'un serveur
- Introduction aux vunérabilités Web

Attaques locales
- Cassage de mots de passe
- Élévation de privilèges
- Attaque du GRUB

Ingénierie sociale
- Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes
- Phishing (hameçonnage)
- Outils de contrôle à distance
- Attaque à distance
- Introduction à Metasploit Framework

Se sécuriser
- Les mises à jour
- Configurations par défaut et bonnes pratiques
- Introduction à la cryptographie
- Présentation de la stéganographie
- Anonymat (TOR)

PROCHAINES DATES

3 février 2025
7 avril 2025
5 juin 2025
18 septembre 2025
3 novembre 2025
8 décembre 2025

OBJECTIFS

- Se familiariser avec les termes techniques et connaître les méthodologies pour mener un test d'intrusion
- Comprendre les méthodes de prise d'information (recherche passive)
- Connaître les notions fondamentales du réseau
- Connaître les attaques distantes et locales
- Se sensibiliser face aux attaques d'ingénierie sociale
- Adopter les bonnes pratiques de sécurité
- Connaître les notions de cryptographie, de stéganographie et d'anonymat
- Mettre en pratique les connaissances acquises

INFORMATIONS GÉNÉRALES

Code : HSF
Durée : 2 jours
Prix : 1 495 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI
- Ingénieurs / Techniciens
- Administrateurs systèmes et réseaux
- Toute personne s'intéressant à la sécurité informatique

PRÉ-REQUIS

- Connaître des notions de sécurité informatique
- Être familier avec les invites de commandes Windows et Linux
- Avoir des connaissances sur le fonctionnement des applications Web

RESSOURCES

- Support de cours
- 50% d'exercices pratiques
- 1 PC par personne

AVANCÉ

FORMATION HACKING

HACKING & SÉCURITÉ : AVANCÉ

Se mettre dans la peau d'un attaquant pour mieux protéger votre SI

Code : HSA

Ce cours est une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises.
Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes.
L'objectif est de vous fournir les techniques offensives des attaques informatiques, en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI.

La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (cas pratiques, TP...) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction
- Vocabulaire
- Vulnérabilités et exploits
- Concepts généraux

Prise d'information
- OSINT
- Google Hacking
- Scan de ports
- Prise d'empreinte du système des services

JOUR 2

Attaques réseau
- Sniffing réseau
- Man-in-The-Middle
- DNS Hijacking
- Attaque des protocoles sécurisés
- Dénis de service

Attaques système
- Attaque depuis un accès physique
- Exploitation d'un service vulnérable distant
- Outil d'exploitation Metasploit
  - Génération d'un malware
  - Encodage de la charge malveillante
  - Exploitation de vulnérabilités

JOUR 3

Attaque Système
- Élévation de privilèges
- Attaque cryptographique sur les mots de passe

Attaques Web
- Cartographie et énumération
- Attaque par énumération (brute-force)
- Inclusion de fichiers (LFI / RFI)
- Injection de commande
- Cross-Site Scripting (XSS)
- Injection SQL
- Upload de fichiers

JOUR 4

Attaques applicatives
- Buffer overflow sous Linux
  - L'architecture Intel x86
  - Les registres
  - La pile et son fonctionnement
  - Présentation des méthodes d'attaques standards
    - Écrasement de variables
    - Contrôler EIP
    - Exécuter un shellcode
    - Prendre le contrôle du système en tant qu'utilisateur root

JOUR 5

Challenge final
- Mise en pratique des connaissances acquises durant la semaine sur un TP final (CTF d'une journée)

PROCHAINES DATES

27 janvier 2025
31 mars 2025
29 septembre 2025
24 novembre 2025

OBJECTIFS

- Comprendre les méthodes de prise d'information
- Savoir mener des attaques réseau
- Mettre en pratique les différents types d'attaques système
- Apprendre le concept des dépassements de tampon (buffer overflow) et le mettre en pratique
- Mettre en pratique les différents types d'attaques Web
- Appliquer l'ensemble des attaques abordées durant les précédents jours sur un nouveau réseau

INFORMATIONS GÉNÉRALES

Code : HSA

Durée : 5 jours

Prix : 4 150 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI, DSI
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Développeurs

PRÉ-REQUIS

- Avoir suivi la formation HSF ou une formation équivalente
- Avoir des connaissances sur les protocoles réseaux TCP/IP
- Avoir des connaissances sur la sécurité des systèmes Windows et Linux
- Avoir des connaissances sur le développement Web et le fonctionnement des applications Web

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne avec un environnement dédié sur notre plateforme MALICE

EXPERT

FORMATION HACKING

HACKING & SÉCURITÉ : EXPERT

Une analyse poussée de l'attaque pour mieux vous défendre

Ce cours vous permettra d'acquérir un niveau d'expertise élevé dans le domaine de la sécurité des systèmes d'information en réalisant différents scénarios complexes d'attaques.

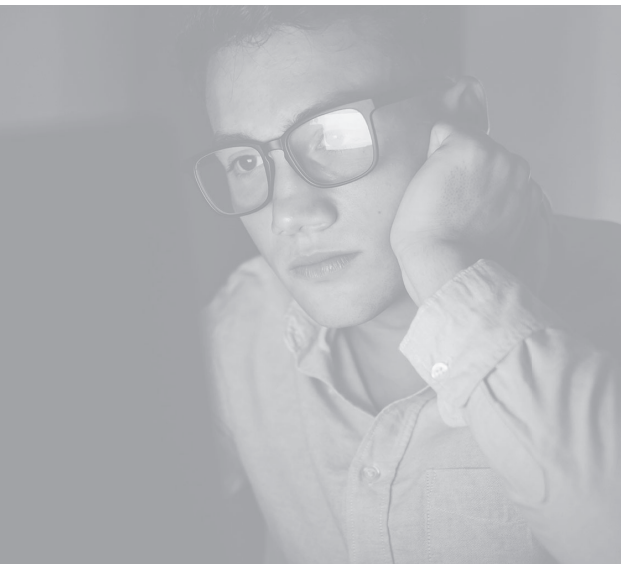
Cette formation porte également sur une analyse poussée des vulnérabilités.

Code : HSE

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (TP, cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.



JOUR 1

Réseau
- Options avancées de Nmap et développement d'un script NSE
- Scapy
- IPv6 - mitm6
- HSRP / VRRP
- Introduction à la sécurité des protocoles de routage (OSPF, BGP, etc.)

JOUR 2

Système
- Exploitation avancée et mise en place d'un pivot avec Metasploit
- Attaque d'une infrastructure Microsoft (Responder / Pass-The-Hash / CME / ntlmrelayx)
- Élévation de privilèges
- Techniques de contournement

JOUR 3

Applicatif
- Introduction aux Buffer Overflows 32-bits
- Exploitations basiques de débordement de tampon en 32-bits
- Exploitation via Ret2PLT (32-bits et 64-bits)
- Contournement de l'ASLR (32 bits)
- Introduction et exploitation via ROP
- Exploitation de débordement de tampon sous Windows
- Protections contre les Buffer Overflows

JOUR 4

Web
- Injections de commandes
- Attaques contre des JWT vulnérables
- Injections SQL avancées
- XXE
- SSRF / CSRF
- Injection d'objets / Dé-sérialisation
- Liens symboliques ZIP
- IDOR

JOUR 5

CTF final
- CTF sur la plateforme MALICE

PROCHAINES DATES

10 février 2025
16 juin 2025
8 septembre 2025
1er décembre 2025

OBJECTIFS

- Comprendre et effectuer des attaques réseau avancées
- Comprendre et effectuer des attaques système avancées
- Apprendre les différentes méthodes d'élévation de privilèges sur un système Windows ou sur un réseau interne
- Comprendre et effectuer des attaques Web avancées
- Apprendre le concept des dépassements de tampon (buffer overflows) et le mettre en pratique
- Appliquer l'ensemble des attaques abordées durant les précédents jours via un CTF

INFORMATIONS GÉNÉRALES

Code : HSE

Durée : 5 jours

Prix : 4 650 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Développeurs

PRÉ-REQUIS

- Avoir suivi la formation HSA ou une formation équivalente
- Maîtriser des protocoles réseaux
- Maîtriser des systèmes Windows et Linux
- Savoir développer des scripts
- Avoir des connaissances sur le développement Web et le fonctionnement des applications Web

RESSOURCES

- Support de cours
- 1 PC par personne
- Environnement Windows de démonstration et Linux
- Metasploit

EXPERT

FORMATION HACKING

RÉTRO-INGÉNIERIE DE LOGICIELS MALVEILLANTS

Créez votre laboratoire d'analyse de malwares et comprenez leurs fonctionnements en plongeant dans leurs codes.

Cette formation prépare à la réalisation d'investigations dans le cadre d'attaques réalisées via des logiciels malveillants, de la mise en place d'un laboratoire d'analyse comportementale à l'extraction et au désassemblage de code malveillant.

Code : RILM

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Rappels sur les bonnes pratiques d'investigation numérique

Présentation des différentes familles de malwares

Vecteurs d'infection

Mécanisme de persistance et de propagation

Laboratoire virtuel vs. physique
- Avantages de la virtualisation
- Solutions de virtualisation

Ségrégation des réseaux
- Réseaux virtuels et réseaux partagés
- Confinement des machines virtuelles
- Précautions et bonnes pratiques

Supervision de l'activité d'une machine
- Réseau
- Système de fichiers
- Registre
- Service

Initiation à l'analyse comportementale

Variété des systèmes

JOUR 2

Mise en place d'un écosystème d'analyse comportementale
- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées
  - VmWare
  - Virtualbox

Installation de CAPEV2/ Virtualbox

Mise en pratique
- Soumission d'un malware
- Déroulement de l'analyse
- Analyse des résultats et mise en forme

Amélioration via API
- Possibilités de développement et améliorations

JOUR 3

Analyse statique de logiciels malveillants
- Prérequis
  - Assembleur
  - Architecture
  - Mécanismes anti-analyse
- Outils d'investigation
  - IDA
- Utilisation d'IDA
  - Méthodologie
  - Analyse statique de code
  - Analyse de flux d'exécution
- Mécanismes d'anti-analyse
  - Packing/protection (chiffrement de code/imports, anti-désassemblage)
  - Machine virtuelle
  - Chiffrement de données
- Travaux pratiques
  - Analyse statique de différents malwares

JOUR 4

Analyse dynamique de logiciels malveillants
- Précautions
  - Intervention en machine virtuelle
  - Configuration réseau
- Outils d'analyse
  - OllyDbg
  - ImmunityDebugger
- Analyse sous débogueur
  - Step into/Step over
  - Points d'arrêts logiciels et matériels
  - Fonctions systèmes à surveiller
  - Génération pseudo-aléatoire de noms de domaines (C&C)
  - Bonnes pratiques d'analyse
- Mécanismes d'anti-analyse
  - Détection de débogueur
  - Détection d'outils de rétro-ingénierie
  - Exploitation de failles système

PROGRAMME

JOUR 5

Analyse de documents malveillants

- Fichiers PDF
  - Introduction au format PDF
  - Spécificités
  - Intégration de JavaScript et possibilités
  - Exemples de PDF malveillants
  - Outils d'analyse : OLE Tools, éditeur hexadécimal
  - Extraction de la charge
  - Analyse de la charge
- Fichiers Office (DOC)
  - Introduction au format DOC/DOCX
  - Spécificités
  - Macros
  - Objets Linking and Embedding (OLE)
  - Outils d'analyse : OLE Tools, éditeur hexadécimal
  - Extraction de code malveillant
  - Analyse de la charge
- Fichiers APK
  - Introduction au format apk
  - Outils d'analyse : jadx, Frida, genymotion, mobsf
  - Contournement de protection d'émulation
  - Compréhension du fonctionnement

PROCHAINES DATES

27 janvier 2025
31 mars 2025
25 août 2025
27 octobre 2025

OBJECTIFS

- Mettre en place un laboratoire d'analyse de logiciels malveillants
- Savoir étudier le comportement de logiciels malveillants
- Analyser et comprendre le fonctionnement de logiciels malveillants
- Détecter et contourner les techniques d'autoprotection
- Analyser des documents malveillants

INFORMATIONS GÉNÉRALES

Code : RILM
Durée : 5 jours
Prix : 4 440 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Techniciens réponse aux incidents
- Analystes SOC/CSIRT N3
- Responsable laboratoire d'investigation
- Experts sécurité

PRÉ-REQUIS

- Avoir des connaissances du système Microsoft Windows
- Maîtriser le langage assembleur 32 et 64 bits
- Avoir des connaissances en architectures 32 et 64 bits Intel

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne

SENSIBILISATION AU DÉVELOPPEMENT SÉCURISÉ

Sensibilisez-vous aux attaques les plus utilisées afin de mieux protéger vos applications

Cette formation vous explique les vulnérabilités Web et applicatives les plus utilisées par les attaquants afin de mieux comprendre comment vous protéger.

Vous apprendrez les bonnes pratiques et les bons réflexes de développement afin de minimiser les risques de compromission.

Cette formation couvre l'essentiel du développement sécurisé dans différents langages, de la conception au déploiement.

Code : SDS

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOURS 1 & 2

Introduction à la sécurité informatique
- Le contexte de la sécurité
- Risques encourus et impacts

Principales attaques sur les applications web
- Vulnérabilités techniques (Injection SQL, Cross-Site Scripting, Inclusion de fichier, etc.)
- Vulnérabilités logiques et spécifiques (Contournement de contrôle d'accès, Timing Attacks, etc.)
- Contre-mesures et recommandations

JOUR 2 (suite)

Principales attaques sur les applications
- Exécution de code à distance
- Problèmes de permissions
- Chiffrement des communications
- Gestion de l'authentification
- Attaques spécifiques (XXE, Pollution de prototype, Désérialisation, etc.)
- Contre-mesures et recommandations

Outils d'analyses
- Gestion des secrets
- Sécurisation des dépendances
- Analyseurs statiques et dynamiques
- Sécurité des conteneurs

PROCHAINES DATES

6 mars 2025
5 juin 2025
18 septembre 2025
20 novembre 2025

OBJECTIFS

- Connaître les attaques sur les APIs
- Connaître les attaques sur les applications Web
- Maîtriser l'authentification et la gestion des habilitations sur les applications Web
- Savoir maîtriser ses dépendances
- Connaître et utiliser les outils de développement et de déploiement
- Savoir intégrer la sécurité dans le processus de développement

INFORMATIONS GÉNÉRALES

Code : SDS

Durée : 2 jours

Prix : 1 980 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Développeurs Web et applicatifs

PRÉ-REQUIS

- Avoir des connaissances en protocoles réseaux TCP/IP et HTTP(S)
- Avoir des connaissances sur le fonctionnement des applications Web
- Maîtriser le développement Web

RESSOURCES

- Support de cours
- 1 PC par personne
- Environnement informatique de démonstration (Windows, Linux)

AVANCÉ

FORMATION HACKING

SÉCURITÉ WINDOWS & ACTIVE DIRECTORY

Comprendre et pratiquer les attaques spécifiques aux infrastructures Windows Active Directory

Ce cours vous confrontera aux enjeux de sécurité de la mise en place d'infrastructures Windows Active Directory.
Il vous permettra d'appréhender l'intérêt de politiques de sécurité efficaces en fonction des actifs du réseau d'entreprise.
Les principales vulnérabilités des systèmes et les problèmes de configuration seront vues et exploitées.
Corrections, bonnes pratiques et protections seront étudiées et analysées.
En effet, la mise en place d'un domaine peut amener à des erreurs de configuration.
Les sujets seront abordés de manière didactique et interactive, sous forme théorique et pratique, en fournissant un environnement de hacking dédié à chaque élève depuis notre plateforme de cyber-entraînement Malice.

Code : SWAD

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction

Enjeux et principes de la sécurité des systèmes d'information
- Défense en profondeur
- Politique de sécurité
  - Politique de mise à jour
  - Politique de sauvegarde
  - Politique de mots de passe
  - Politique de filtrage réseau
  - Politique de gestion des droits
  - Politique de journalisation
  - Politique de gestion des incidents
- Sensibilisation et formation

Durcissement du démarrage
- BIOS
- UEFI
- DMA
- Mesures de protection
  - BIOS / UEFI
  - DMA
  - Chiffrement du disque

Sécurité d'un environnement Windows
- Authentification Windows
- Mise à jour d'un système Windows
- Supervision
- PowerShell
- Protection des postes clients
  - Résolution de nom
  - Pile IPv6
  - SmartScreen
  - AppLocker
  - UAC
  - Device Guard
  - Credential Guard

JOUR 2

Sécurité d'un environnement Windows (suite)
- Active Directory
  - Introduction
  - Kerberos
  - Outils d'audit
  - Stratégies de groupe
  - LAPS

JOUR 3

Sécurité des services
- Principe du moindre privilège
- Autorité de certification
- Domain Name System (DNS)
- Service Message Block (SMB)
- Remote Desktop Protocol (RDP)
- Microsoft SQL (MSSQL)
- Lightweight Directory Access Protocol (LDAP)

PROCHAINES DATES

5 février 2025
12 mai 2025
15 septembre 2025
10 décembre 2025

OBJECTIFS

- Savoir exploiter les faiblesses de configuration du démarrage d'un système
- Comprendre et exploiter les faiblesses des environnements Windows & Active Directory
- Connaître les méthodes d'attaques d'un Active Directory et comment s'en protéger
- Savoir durcir et exploiter les services Windows

INFORMATIONS GÉNÉRALES

Code : SWAD

Durée : 3 jours

Prix : 2 460 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Auditeurs techniques en devenir
- Administrateurs système

PRÉ-REQUIS

- Avoir des notions de sécurité informatique
- Avoir des connaissances en protocoles réseaux TCP/IP
- Avoir des connaissances sur les systèmes Windows (client et serveur) et Active Directory
- Avoir des notions de développement de scripts

Un niveau HSA est recommandé afin de suivre confortablement la formation.

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne
- Environnement Windows de démonstration et Kali Linux

SÉCURITÉ DÉFENSIVE

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
AIARI	**Analyse Inforensique Avancée et Réponse aux Incidents**	3 jours		19			21		2			1		
SDI	**Mise en place de Sondes de Detection d'Intrusion**	3 jours		5			12				22		17	
SL	**Sécurisation Linux**	3 jours				2		2			24		12	
SR	**Sécurisation des Réseaux**	3 jours			3			18			15			8

AVANCÉ

SÉCURITÉ DÉFENSIVE

ANALYSE INFORENSIQUE AVANCÉE ET RÉPONSE AUX INCIDENTS

Préparez-vous à l'analyse post-incident

Code : AIARI

Ce cours vous apprendra à mettre en place une procédure complète d'analyse inforensique sur des environnements hétérogènes.

Vous y aborderez la réponse aux incidents d'un point de vue organisationnel.

Vous étudierez également les méthodologies et outils appropriés utilisés dans la phase technique de la réponse aux incidents, à savoir l'analyse inforensique (ou post-incident).
À l'issue de la formation, vous serez capable de préserver les preuves numériques pour en effectuer l'analyse ultérieure et les présenter dans le cadre d'un recours judiciaire.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Les bases de la réponse aux incidents et de l'analyse inforensique

- Mise en place de la réponse aux incidents
  - Préparation à la réponse aux incidents
  - Détection et analyse
  - Classification et classement par ordre de priorité
  - Notification
  - Confinement
  - Investigation inforensique
  - Éradication et reprise d'activité
- Outils et équipements de surveillance
- Méthodologie et outillage pour l'analyse inforensique
  - S'organiser
  - Choisir ses outils
  - Respecter les méthodes scientifiques
  - Présenter ses conclusions dans un rapport

JOUR 2

Approche de l'analyse inforensique sur les principaux domaines techniques

- Collecte de données et duplication
  - Comprendre les systèmes de fichiers Windows, Linux et BSD
  - Outils et moyens de collecte
- Retrouver des partitions et des fichiers supprimés
- Analyse de journaux d'évènements des différents équipements
- Analyse d'attaques réseaux
  - Les sources de capture
  - Revue d'attaques répandues

JOUR 3

Analyses ciblées et exercices avancés

- Analyse des fichiers de journaux et corrélation d'événements
  - Utiliser un indexeur (ELK)
- Analyse inforensique des navigateurs
- Acquisition et analyse de la mémoire (Volatility)
- Analyse inforensique des e-mails
- Écriture d'un rapport (bonnes pratiques et méthode PRIS)

Mise en pratique sur des cas concrets.

PROCHAINES DATES

19 février 2025
21 mai 2025
2 juillet 2025
1er octobre 2025

OBJECTIFS

- Être capable de définir et mettre en place un processus de réponse aux incidents rigoureux
- Collecter correctement les preuves nécessaires à une analyse de qualité et à d'éventuelles poursuites judiciaires
- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion

INFORMATIONS GÉNÉRALES

Code : AIARI
Durée : 3 jours
Prix : 2 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Professionnels IT en charge de la sécurité des systèmes d'information, de la réponse aux incidents ou de l'investigation légale

PRÉ-REQUIS

- Avoir une bonne culture générale en informatique
- Maîtriser Linux (administration, commandes et programmation shell)
- Avoir des connaissances générales des attaques et vulnérabilités (des rappels pourront être effectués)
- Avoir des connaissances générales en administration Windows

RESSOURCES

- Support de cours
- 60% d'exercices pratiques
- 1 PC par personne
- Environnement Linux et Windows
- Machines virtuelles

AVANCÉ

SÉCURITÉ DÉFENSIVE

MISE EN PLACE DE SONDES DE DÉTECTION D'INTRUSION

Détectez et déjouez les tentatives d'intrusion sur votre système d'information.

Code : SDI

Les attaquants sont de plus en plus motivés et outillés pour s'introduire dans votre système d'information.

Comprendre leurs techniques d'attaque et être en mesure de les détecter est aujourd'hui essentiel !

À travers cette formation vous apprendrez à mettre en place des règles de détection efficaces face aux cyberattaques actuelles et cela avec des sondes de détection open source.

Ces détections portent aussi bien sur les parties système et réseau que la partie applicative.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

- Introduction aux menaces cyber actuelles
- Enjeux de la supervision et détection dans les systèmes d'information
- Outils de supervision et de détection
- La gestion d'incident
- Présentation IDS/IPS, EDR, XDR, etc.
- Présentation de la sonde Suricata
- Installation et configuration de Suricata
- Détection d'attaques réseau

JOUR 2

- Présentation de la sonde Wazuh
- Mise en place de Wazuh
- Scans de vulnérabilités avec Wazuh
- Blocage d'une attaque par force brute SSH via Wazuh
- Introduction aux attaques Web
- Détection d'attaques Web via Suricata
- Contournement de règles de détection d'attaques Web

JOUR 3

Détection d'exploitation d'une faille récente avec Suricata

- Intégration de VirusTotal dans Wazuh
- Étude de cas : Détection d'une tentative de compromission par logiciel malveillant :
  - Détection via la réseau et méthodes de contournements
  - Détection via le système hôte

PROCHAINES DATES

5 février 2025
12 mai 2025
22 septembre 2025
17 novembre 2025

OBJECTIFS

- Comprendre les méthodes utilisées pour détecter les attaques
- Savoir créer ses propres règles de détection sur des outils open source
- Comprendre comment les attaquants contournent les systèmes de détection d'intrusion
- Savoir mettre en place les règles adéquats contre des attaques sur le réseau et sur les machines hôtes

INFORMATIONS GÉNÉRALES

Code : SDI

Durée : 3 jours

Prix : 2 460 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Administrateurs réseau / système
- Techniciens réseau / système
- Ingénieurs sécurité

PRÉ-REQUIS

- Avoir des notions de sécurité informatiques
- Maîtriser les modèles OSI et TCP/IP
- Savoir utiliser un environnement Linux

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne avec un environnement dédié sur notre plateforme MALICE

AVANCÉ

SÉCURITÉ DÉFENSIVE

SÉCURISATION LINUX

Protégez efficacement vos systèmes Linux contre les attaques

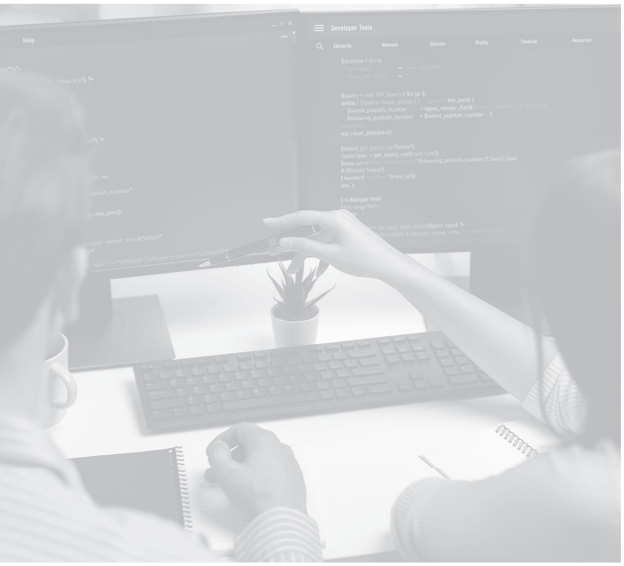
Code : SL

Ce cours a pour objectif d'aborder les problèmes de la sécurisation des serveurs et postes Linux, ce qu'il est nécessaire de savoir et de mettre en place pour protéger son parc. Il comprendra une présentation de GNU Linux et de son fonctionnement, les méthodes de durcissement du noyau ainsi que les principes généraux de l'utilisation de Linux de façon sécurisée (gestion des droits, politique de mot de passe, etc.). Les protections mises en place par le système contre les dépassements de mémoire tampon seront étudiées ainsi que les principes de leur contournement. Des démonstrations des bonnes pratiques à appliquer pour utiliser sûrement les services les plus répandus, ainsi que les techniques d'isolation des services feront également partie de la formation. L'automatisation des processus d'automatisation et de déploiement de configuration sera mise en œuvre.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.



JOUR 1

Présentation des politiques de sécurité

Présentation du système Linux

Mise en place des premières sécurisations
- Secure Boot
- Signatures MOK / EFI
- Grub
- Attaques DMA

Journalisation avancée
- Monitoring avec auditd
- Journalisation centralisée

Gestion des droits et des accès
- Le système d'authentification PAM
  - Double Authentification
  - Authentification centralisée (Kerberos)
- SUDO
- Kernel capabilities
- SELinux / AppArmor

JOUR 2

Sécurité réseau
- Firewalls
  - IPTables
    - ACCEPT/DROP/REJECT
    - Rate Limiting
    - Connection Limiting / Tracking
    - Syn Proxy
  - NFtables
- VPN
  - OpenVPN
  - Strongswan / L2TP / IPSec

System Hardening
- Kernel Hardening
  - Sysctl
- Application Hardening
  - Protection des secrets

Détection d'intrusion
- NIDS - SURICATA
- HIDS - OSSEC

JOUR 3

Sauvegardes
- Gestion des sauvegardes
- Sauvegardes complètes
  - Write-Only Backups
- Sauvegardes bases de données
  - Delayed Syncs

Système de fichier
- Permissions
  - SUID/SGID
- ACL / Quotas
- Chiffrement
  - Dm-crypt
  - LUKS
- ZFS/BTRFS
- Effacement sécurisé
  - Software
  - Hardware

Sécurité des services
- Chroot
- Sandboxing (policycoreutils-sandbox)
- Containers (Namespace, Cgroups, Seccomp) : Docker/LXC/LXD/SystemD
- Virtualization KVM

PROCHAINES DATES

2 avril 2025
2 juin 2025
24 septembre 2025
12 novembre 2025

OBJECTIFS

- Définir une politique de sécurité efficace
  - Définir les besoins des clients
  - Identifier les points de sensibilité
  - Choisir une politique efficace
- Mettre en place une politique de sécurité efficace
  - Connaître les dangers de configuration Linux
  - Comprendre la sécurité mise en place
  - Déployer des configurations robustes
- Ajouter des mécanismes de protection
  - Bien configurer son firewall
  - Compléter son firewall avec d'autres mécanismes
  - Isoler l'exécution des applications

INFORMATIONS GÉNÉRALES

Code : SL
Durée : 3 jours
Prix : 2 460 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Administrateurs
- Ingénieurs / Techniciens
- Consultants

PRÉ-REQUIS

- Avoir de bonnes connaissances en administration Linux
- Avoir des connaissances en réseau
- Avoir des connaissances en système virtualisé

RESSOURCES

- Support de cours
- 1 PC par personne
- 60% d'exercices pratiques
- Environnement Linux (Fedora, Debian, Kali Linux)

AVANCÉ

SÉCURITÉ DÉFENSIVE

SÉCURISATION DES RÉSEAUX

Protégez votre réseau des attaques informatiques

Code : SR

Cette formation a pour but de passer en revue les différentes attaques visant les protocoles et équipements réseau. Une démonstration et mise en pratique des attaques sera faite ainsi que l'explication des contre-mesures à apporter.
Nous étudierons dans un premier temps les attaques visant ou utilisant les protocoles de couche 2 qui profitent de problèmes de configuration des commutateurs (switchs). Suivront les attaques ciblant les routeurs et les systèmes VPN.
Enfin, nous nous intéresserons aux équipements permettant de renforcer la sécurité d'un réseau informatique (Pare-feu, IDS/IPS, Proxy, etc.)

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Présentation des enjeux de la sécurité des réseaux

Démonstration des attaques ciblant les équipements de niveau 2 et leurs contre-mesures
- ARP
- VLAN
- CDP
- Spanning Tree
- Etc.

JOUR 2

Attaque et protection des équipements et protocoles de niveau 3
- Ipv4 et Ipv6
- RIP
- OSPF
- EIGRP
- BGP

JOUR 3

Attaques et contre-mesures sur les passerelles virtuelles
- VRRP
- HSRP
- GLBP

Attaques et contre-mesures sur les VPN

Chiffrement des communications : utilisations et bonnes pratiques

Les outils de protection réseau
- Pare-feu
- IDS/IPS
- Serveur mandataire

PROCHAINES DATES

3 mars 2025
18 juin 2025
15 septembre 2025
8 décembre 2025

OBJECTIFS

- Comprendre et savoir réaliser des attaques et s'en prémunir sur les protocoles réseau de base (CDP, STP, ARP, DHCP et DNS)
- Comprendre et savoir réaliser des attaques et s'en prémunir sur les VLAN (Double Tagging, Virtual Trunking Protocol, Dynamic Trunking Protocol)
- Comprendre et savoir réaliser des attaques et s'en prémunir sur le protocole NDP
- Comprendre et savoir réaliser des attaques et s'en prémunir sur l'auto-configuration IPv6
- Comprendre et savoir réaliser des attaques et s'en prémunir sur les protocoles de routage (RIP, OSPF, HSRP, IPSec IKE)
- Comprendre et savoir réaliser des attaques et s'en prémunir sur les protocoles SSL/TLS
- Comprendre et savoir configurer un pare-feu réseau
- Comprendre et savoir configurer un serveur mandataire
- Comprendre et savoir configurer un IDS

INFORMATIONS GÉNÉRALES

Code : SR
Durée : 3 jours
Prix : 2 460 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Administrateurs réseau / système
- Techniciens réseau / système
- Ingénieurs réseau / système

PRÉ-REQUIS

- Avoir des notions de sécurité informatique
- Maîtriser les protocoles réseaux
- Maîtriser les modèles OSI et TCP/IP
- Avoir des connaissances en architecture des réseaux

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne
- Environnement de démonstration

FORMATION PENTEST

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
AUDWEB	Audit de site Web	3 jours	29			23			2			20		
SAM	Sécurité des Applications Mobiles	3 jours		26			14				10		12	
TEST-INT	Test d'Intrusion : mise en situation	5 jours		17				30		25		27		

AVANCÉ

FORMATION PENTEST

AUDIT DE SITE WEB

L'audit Web par la pratique

Code : AUDWEB

Ce cours vous apprendra à mettre en place une véritable procédure d'audit de site Web. Vous serez confronté aux problématiques de la sécurité des applications Web. Vous étudierez le déroulement d'un audit, aussi bien d'un point de vue méthodologique que technique. Les différents aspects d'une analyse seront mis en avant à travers plusieurs exercices pratiques. Cette formation est destinée aux développeurs, chefs de projets et personnels souhaitant être sensibilisés aux risques de sécurité et vulnérabilités applicatives utilisées par les acteurs malveillants.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction

- Terminologie
- Veille technologique
- Objectifs et limites d'un test d'intrusion
- Méthodologie d'audit
- Cycle d'un audit
- Référentiels utilisés

Reconnaissance

- Reconnaissance passive
  - Base de données WHOIS
  - Services en ligne
  - Moteurs de recherche
  - Réseaux sociaux
  - Outils
- Reconnaissance active
  - Visite du site comme un utilisateur
  - Recherche de page d'administration
  - Recherche de fichiers présents par défaut
  - robots.txt, sitemap
  - Détection des technologies utilisées
- Contre-mesures

Scanners

- Les différents types de scanner
  - Scanners de ports
  - Scanners de vulnérabilités
  - Scanners dédiés
- Limites des scanners

JOUR 2

Vulnérabilités Web

- Rappels, technologies du web et système
- Présentation de l'OWASP
- Présentation de l'outil Burp Suite
- Énumération et recherche exhaustive
  - Contexte d'injection (login, sign-in, forgotten password)
  - Techniques d'identification et d'exploitation
  - Automatisation
  - Contre-mesures
- Inclusion de fichiers
  - Contexte d'attaque (LFI, RFI)
  - Techniques d'identification et d'exploitation
  - Automatisation
  - Contre-mesures
- Cross-Site Scripting (XSS)
  - Contexte d'injection (Réfléchie, Stockée, Dom-Based)
  - Technique d'identification et d'exploitation
  - Automatisation
  - Contre-mesures
- Injection de commandes
  - Technique d'identification et d'exploitation (Commande simple, pipeline, listes)
  - Automatisation
  - Contre-mesures
- Injection SQL
  - Contexte d'injection (SELECT, INSERT, UPDATE, DELETE)
  - Technique d'identification et d'exploitation (Union, Booléenne, erreurs, délais, fichiers)
  - Automatisation
  - Contre-mesures

JOUR 3

Vulnérabilités Web (suite)

- Envoi de fichier (Upload)
  - Technique d'identification et d'exploitation
  - Contre-mesures
- Contrôles d'accès défaillants
  - IDOR, FLAC, FRUA
  - Technique d'identification et d'exploitation
  - Contre-mesures
- Cross-Site Request Forgery (CSRF)
  - Contexte d'attaque (GET, POST, HTML / JSON)
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- Server Side Request Forgery (SSRF)
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- Client / Server Side Template Injection (CSTI / SSTI)
  - Contexte d'injection (Moteurs de template)
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- XML External Entity (XXE)
  - Les entités externes
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- Injection d'objet
  - Contexte d'injection (Langages)
  - Techniques d'identification et d'exploitation
  - Contre-mesures

PROCHAINES DATES

29 janvier 2025
23 avril 2025
2 juillet 2025
20 octobre 2025

OBJECTIFS

- Comprendre les objectifs d'un test d'intrusion Web et les détails de sa terminologie
- Mettre en place une veille en matière de sécurité de l'information
- Comprendre les différentes techniques de reconnaissance avancée
- Présentation des méthodologies de scan et des outils permettant l'identification de vulnérabilités
- Présentation et rappels des notions Web et systèmes
- Présentation du référentiel OWASP
- Présentation et prise en main de l'outil Burp suite
- Comprendre la théorie des différents types de vulnérabilités Web, les identifier et les exploiter
- Mise en situation : réaliser un test d'intrusion en autonomie

INFORMATIONS GÉNÉRALES

Code : AUDWEB

Durée : 3 jours

Prix : 2 760 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Consultants en sécurité (ou toute personne souhaitant identifier et exploiter des vulnérabilités Web)
- Développeurs
- Ingénieurs / Techniciens
- Chefs de projets applicatifs

PRÉ-REQUIS

- Maîtriser les protocoles HTTP/HTTPS
- Connaître les fonctionnement des applications Web
- Avoir des connaissances sur le développement Web
- Avoir des connaissances des systèmes Linux

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne

AVANCÉ

FORMATION PENTEST

SÉCURITÉ DES APPLICATIONS MOBILES

Apprenez les techniques et méthodes utilisées pour découvrir des vulnérabilités sur les applications Android et IOS

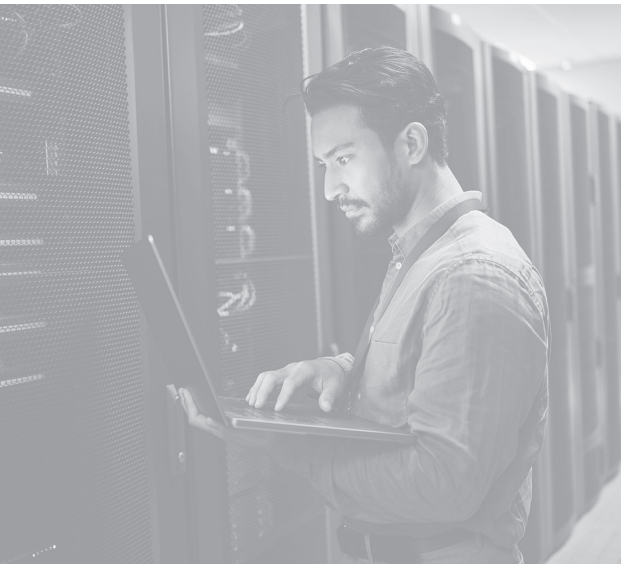
Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type test d'intrusion sur une application mobile Android et IOS.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise.
Lors de cette formation, vous étudierez l'organisation et les procédures à respecter pour la mise en place d'un tel audit, ainsi que les différentes approches possibles pour analyser une application Android et IOS d'un point de vue sécurité.

Code : SAM

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.



JOUR 1

Introduction au système Android
- Modèle de sécurité Android
- Structure et composants d'une application
- Préparation de l'environnement de test
- Mise en place de l'instrumentation
- Analyse statique
- Analyse dynamique

Présentation des outils d'analyse
- Le SDK Android
- ADB (Android Debug Bridge)
- JADX
- RMS (Runtime Mobille Security)
- Frida & Objection
- MobSF

JOUR 2

Vulnérabilités spécifiques aux applications android
- Activity
- Content Providers
- Broadcast Receivers
- Webview

Instrumentation et ingénierie reverse
- Analyse avec Radare

Interceptions des communications
- Proxy HTTP et non HTTP

Attaque sur les API
- Cross-Site Scripting
- Injection de code SQLI
- IDOR
- Authentification

JOUR 3

IOS
- Modèle de sécurité IOS
- Environnement de test
- Méthodologie d'analyse
- Instrumentation

CTF Final
- Mise en situation d'audit
- Recherche et exploitation de vulnérabilités
- Synthèse et contre mesure

PROCHAINES DATES

26 février 2025
14 mai 2025
10 septembre 2025
12 novembre 2025

OBJECTIFS

- Maîtriser les fonctionnalités avancées du système Android et IOS
- Organiser une procédure d'audit de sécurité de type test d'intrusion sur une application mobile Android et IOS
- Se mettre en situation réelle d'audit

INFORMATIONS GÉNÉRALES

Code : SAM

Durée : 3 jours

Prix : 2 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) - en présentiel uniquement

Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Ingénieurs / Techniciens
- Responsables techniques
- Consultants sécurité

PRÉ-REQUIS

- Avoir des connaissances en Web
- Avoir des connaissances en sécurité

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne
- Environnement Linux
- Machine virtuelle avec outils d'analyse Android et IOS

AVANCÉ

FORMATION PENTEST

TEST D'INTRUSION : MISE EN SITUATION D'AUDIT

Le test d'intrusion (pentest) par la pratique

Code : TEST-INT

Vous effectuerez un test d'intrusion : des tests techniques jusqu'à la réalisation du rapport. Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type test d'intrusion (pentest) sur votre SI.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise. En effet, le test d'intrusion est une intervention très technique, qui permet de déterminer le potentiel réel d'intrusion et de destruction d'un pirate sur l'infrastructure à auditer, et de valider l'efficacité réelle de la sécurité appliquée aux systèmes, au réseau et à la confidentialité des informations.
Vous étudierez notamment l'organisation et les procédures propres à ce type d'audit, vous utiliserez vos compétences techniques. Vous découvrirez les meilleurs outils d'analyse et d'automatisation des attaques pour la réalisation de cette intervention.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation grâce à 80% d'exercices pratiques et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Méthodologie de l'audit

La première journée posera les bases méthodologiques d'un audit de type test d'intrusion. L'objectif principal étant de fournir les outils méthodologiques afin de mener à bien un test d'intrusion. Les points abordés seront les suivants :

Objectifs et types de test d'intrusion

- Qu'est-ce qu'un test d'intrusion ?
- Le cycle du test d'intrusion
- Différents types d'attaquants
- Types d'audits
  - Boîte Noire
  - Boîte Blanche
  - Boîte Grise
- Avantages du test d'intrusion
- Limites du test d'intrusion
- Cas particuliers
  - Dénis de service
  - Ingénierie sociale

Aspect réglementaire

- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions
- Points importants du mandat

Exemples de méthodologies et d'outils

- Préparation de l'audit
  - Déroulement
  - Cas particuliers
  - Habilitations
  - Dénis de service
  - Ingénierie sociale
- Déroulement de l'audit
  - Reconnaissance
  - Analyse des vulnérabilités
  - Exploitation
  - Gain et maintien d'accès
  - Comptes rendus et fin des tests

Éléments de rédaction d'un rapport

- Importance du rapport
- Composition
  - Synthèse générale
  - Synthèse technique
- Évaluation du risque
- Exemples d'impacts
- Se mettre à la place du mandataire

Une revue des principales techniques d'attaques et des outils utilisés sera également faite afin de préparer au mieux les stagiaires à la suite de la formation.

JOURS 2, 3 & 4

Une mise en situation d'audit sera faite afin d'appliquer, sur un cas concret, les outils méthodologiques et techniques vus lors de la première journée.

L'objectif étant de mettre les stagiaires face à un scénario se rapprochant le plus possible d'un cas réel.

Le système d'information audité comportera diverses vulnérabilités (applicatives, systèmes, web, Active Directory, etc.) plus ou moins faciles à découvrir et à exploiter.
L'objectif étant d'en trouver un maximum lors de l'audit et de fournir au client les recommandations adaptées afin que ce dernier sécurise efficacement son système d'information.

Pour ce faire, le formateur se mettra à la place d'un client dont les stagiaires auront à auditer le système d'information. Ces derniers seront laissés en autonomie et des points méthodologiques et techniques seront régulièrement faits par le formateur afin de guider les stagiaires tout au long de la mise en situation.

Le formateur aura un rôle de guide afin de :

- faire profiter les stagiaires de son expérience terrain
- mettre en pratique la partie théorique de la première journée
- élaborer un planning
- aider les stagiaires à trouver et exploiter les vulnérabilités présentes
- formaliser les découvertes faites en vue d'en faire un rapport pour le client

PROGRAMME

JOUR 5

Le dernier jour sera consacré au rapport. La rédaction de ce dernier et les méthodes de transmission seront abordées via des exemples et des modèles de rapports.

Préparation du rapport
- Mise en forme des informations collectées lors de l'audit
- Préparation du document et application de la méthodologie vue lors du premier jour

Écriture du rapport
- Analyse globale de la sécurité du système
- Évaluation du risque lié au périmètre client
- Description des vulnérabilités trouvées
- Rédiger des recommandations pertinentes pour corriger les vulnérabilités.

Transmission du rapport
- Précautions nécessaires
- Méthodologie de transmission de rapport

PROCHAINES DATES

17 février 2025
30 juin 2025
25 août 2025
27 octobre 2025

OBJECTIFS

- Maîtriser les différentes vulnérabilités sur les applications Web
- Maîtriser les différentes méthodologies de pivot sur un réseau interne
- Exploiter un Buffer Overflow
- Exploiter des vulnérabilités sur un domaine Active Directory
- Rédiger et relire un rapport de test d'intrusion

INFORMATIONS GÉNÉRALES

Code : TEST-INT
Durée : 5 jours
Prix : 3 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

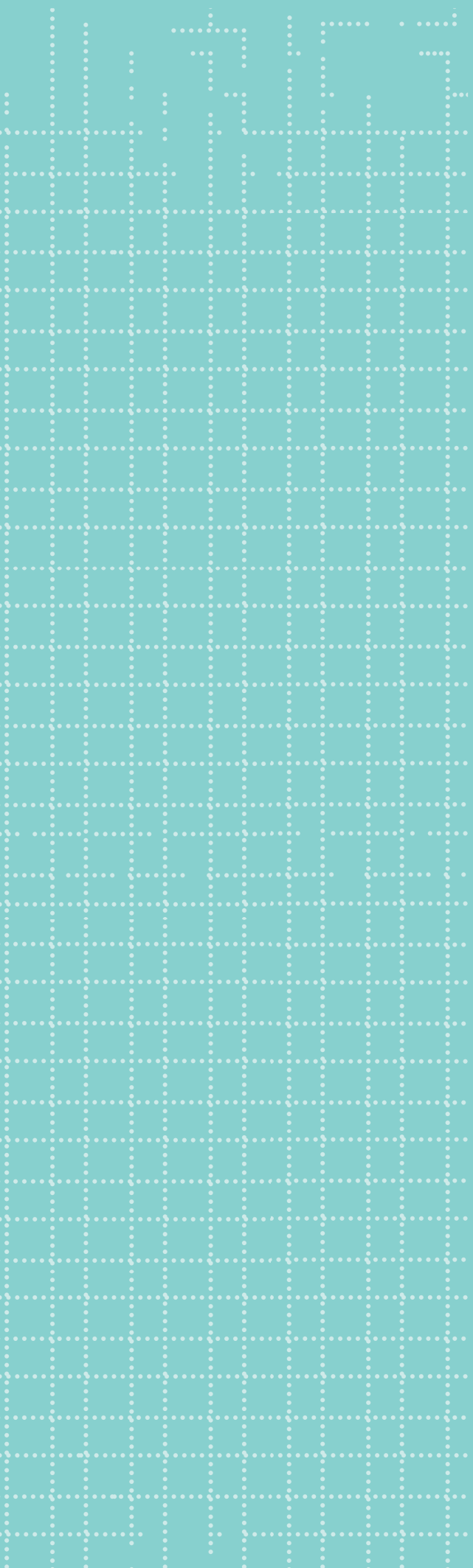
- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Toute personne souhaitant apprendre le pentest (test d'intrusion)

PRÉ-REQUIS

- Avoir des notions techniques de sécurité informatique
- Avoir suivi une formation HSA (ou d'un niveau équivalent) ou avoir participé à des CTF
- Avoir des connaissances en systèmes Windows et Linux et des bases de données
- Avoir des notions de développement Web

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne
- Chaque participant a accès à sa propre instance d'un réseau d'entreprise virtualisée pour mener le test d'instrusion



FORMATION ANALYSTE SOC

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
MDIE	**Malwares : Détection, Identification et Éradication**	3 jours			10			23			29			1
SIEM	**Mise en place d'un SIEM en Open Source**	4 jours			17				7		1		24	

AVANCÉ

FORMATION ANALYSTE SOC

MALWARES : DÉTECTION, IDENTIFICATION ET ÉRADICATION

Apprenez à connaître les malwares, leurs grandes familles, à les identifier et à les éradiquer !

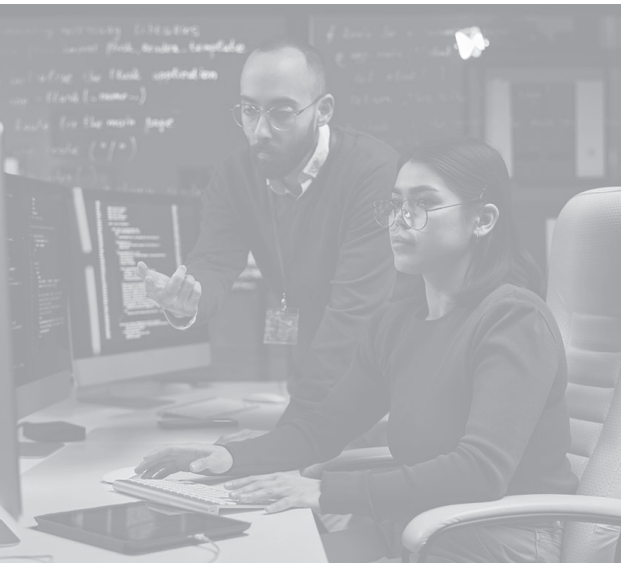
Cette formation permettra de comprendre le fonctionnement des malwares, de les identifier et de les éradiquer proprement, en assurant la pérennité des données présentes sur le SI. Des bonnes pratiques et outils adaptés seront abordés tout au long de la formation, et mis en pratique lors des travaux dirigés.

Code : MDIE

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.



JOUR 1

Introduction aux malwares
- Virus
- Vers
- Botnet
- Rançongiciels
- Rootkits (userland – kernel-land)
- Bootkit

Éradication
- Processus inforensique et analyse de logiciels malveillants
- Réponse aux incidents automatisée sur un parc

JOUR 2

Détection
- Les anti-virus et leurs limites
- Chercher des informations sur un malware
- NIDS / HIDS
- EDR
- Concept d'IOC dans le cadre d'un SOC / CERT (hash, motifs, etc.)

JOUR 3

Identification
- Analyse dynamique manuelle
- Analyse dynamique automatisée (sandboxes)
- Analyse statique basique
- Introduction à l'analyse mémoire avec Volatility
- Introduction à la rétro-conception

PROCHAINES DATES

10 mars 2025
23 juin 2025
29 septembre 2025
1er décembre 2025

OBJECTIFS

- Reconnaître les mécanismes de dissimulation de malwares et mettre en place un environnement infecté
- Utiliser différents outils de détection de malware
- Mettre en place un système de collecte d'information
- Réaliser une rétro-ingénierie sur un malware
- Prendre en main les outils d'analyse dynamique
- Comprendre les mécanismes de persistance d'un malware

INFORMATIONS GÉNÉRALES

Code : MDIE
Durée : 3 jours
Prix : 2 760 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Responsables gestions des incidents
- Techniciens réponse aux incidents
- Auditeurs techniques, Analystes de sécurité

PRÉ-REQUIS

- Avoir des notions de sécurité informatique
- Maîtriser les systèmes Windows et Linux
- Avoir des connaissances en protocoles réseaux TCP/IP
- Avoir des connaissances en développement

RESSOURCES

- Support de cours
- 50% d'exercices pratiques
- 1 PC par personne

EXPERT

FORMATION ANALYSTE SOC

MISE EN PLACE D'UN SIEM EN OPEN SOURCE

Maîtrisez votre gestion d'évènements via les solutions de SIEM en open source !

Cette formation permettra de comprendre le fonctionnement des malwares, de les identifier et de les éradiquer proprement, en assurant la pérennité des données présentes sur le SI. Des bonnes pratiques et outils adaptés seront abordés tout au long de la formation et mis en pratique lors des travaux dirigés.

Code : SIEM

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

La technologie SIEM (Security Information and Event Management)
- Présentation du SIEM
- Qu'est-ce qu'un SIEM ?
- Le fonctionnement d'un SIEM
- Les objectifs d'un SIEM et de la corrélation des donnéesRéseaux virtuels et réseaux partagés

JOUR 2

Le Lab
- Le SIEM au sein d'une architecture réseau
- Présentation du Lab de formation
- Préparation du Lab

Mise en place de Windows Server
- Installation de Windows Server R2
- Configuration du serveur
- Activation et configuration du domaine
- Activation et configuration du service Active Directory (AD)

JOUR 3

Présentation de ELK (Elasticsearch, Logstash et Kibana)
- Présentation de la suite ELK
- Découverte de Elasticsearch
- Découverte de Logstash
- Découverte de Kibana

Elasticsearch
- Approche théorique : terminologie
- Application Full REST et utilisation

Travaux pratiques
- Présentation de la solution Cloud
- Installation de Elasticsearch
- Configuration du fichier : yml

Logstash
- Approche théorique : fonctionnement de Logstash

Travaux pratiques
- Installation de Logstash
- Fichier Input

JOUR 4

Kibana
- Utilisation de l'interface Discover
- Visualize et les différentes visualisations
- Comment créer des alertes ?
- Exporter en PDF les données Dashboard
- Comment sécuriser Kibana ?

Travaux pratiques
- Installation et configuration

Détection d'intrusion et remontée d'alertes sur l'Active Directory
- Présentation du scénario et de l'objectif
- Approche théorique sur l'agent WinlogBeat
- Travaux pratiques
- Mise en place de WinlogBeat
- Configurer le Dashboard sur Kibana
- Détecter une intrusion admin dans l'AD
- Détecter une intrusion Pfsens et remonter l'alerte dans le dashboard

PROCHAINES DATES

17 mars 2025
7 juillet 2025
1er septembre 2025
24 novembre 2025

OBJECTIFS

- Traiter des incidents de sécurité et leur management
- Aborder les problématiques liées à la détection d'intrusion, ainsi que leurs limites
- Mettre en place le Prelude SIEM avec implémentation de sondes SNORT et d'agents HIDS dans un réseau existant
- Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation.

INFORMATIONS GÉNÉRALES

Code : SIEM

Durée : 4 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Pentester
- Administrateurs système
- RSSI
- Consultants en sécurité de l'information
- Toute personne ayant des notions d'administration système (si possible ayant pratiqué)

PRÉ-REQUIS

- Avoir des connaissances générales en système, réseau et développement.

RESSOURCES

- Support de cours
- Nombreux travaux pratiques
- 1 PC par personne

FORMATION CERTIFIANTE

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
CCISOv3	Certified Chief Information Security Officer v3	5 jours		24				23			29		24	
CCSEv2	Certified Cloud Security Engineer v2	5 jours		3		7					13			1
CCT	Certified Cybersecurity Technician	5 jours			24			23		25		27		
CEHv13	Certified Ethical Hacker v13	5 jours	27	24	24	14		23			8	6	3	1
CHFIv11	Computer Hacking Forensic Investigator v11	5 jours			10			16			15		17	
CISA	Certified Information Systems Auditor	5 jours			10			16				13		1
CISM	Certified Information Security Manager	4 jours		10			19				22		24	
CISSP	Certified Information Systems Security Professional	5 jours			17			30				20		8
CNDv3	Certified Network Defender v3	5 jours		24		14			7			20		
CSA	Certified SOC Analyst	3 jours		26				11				1	19	
CSCUv3	Certified Secure Computer User v3	2 jours			20			12			11		13	
DORA LM	DORA Certified Lead Manager	5 jours			10			2		25		27		
ECDE	EC-Council Certified Devsecops Engineer v2	3 jours		19		23					24		12	
ECIHv3	EC-Council Certified Incident Handler v3	3 jours		19			21		9			8		
ISO 27001 LA	ISO 27001 : Certified Lead Auditor	5 jours			3			16				6		8
ISO 27001 LI	ISO 27001 : Certified Lead Implementer	5 jours		17				2			22		3	
ISO 27002 F	ISO 27002 : Certified Foundation	2 jours	30			28				28			20	
ISO 27002 LM	ISO 27002 : Certified Lead Manager	5 jours			24			2		25		13		
ISO 27002 + EBIOS	ISO 27002 : Certified Risk Manager avec EBIOS Risk Manager	5 jours		3			12				8		17	
ISO 27032 LSM	ISO 27032 : Certified Lead Cybersecurity Manager	5 jours		10		7					1		3	
ISO 27701 LI	ISO 27001 : Certified Lead Implementer	5 jours			17			23			1	27		
ISO 31000	ISO 31000 : Risk Manager	3 jours				28			9		3		12	
NIS2 LI	NIS2 : Certified NIS 2 Directive Lead Implementer	5 jours		3		14			7			6		

EXPERT

FORMATION CERTIFIANTE

CERTIFIED CHIEF INFORMATION SECURITY OFFICER V3

La certification des RSSI

Code : CCISOv3

Le programme CCISO d'EC-Council certifie des dirigeants de la sécurité de l'information partout dans le monde. C'est la première formation visant à certifier des responsables à de hauts niveaux de compétences dans la sécurité de l'information. Le cours CCISO ne se concentre cependant pas seulement sur les connaissances techniques, il s'oriente plus particulièrement sur l'impact de la gestion de la sécurité de l'information d'un point de vue managérial. Le programme CCISO a été développé par des CISO en poste à destination de leurs pairs et des aspirants CISO.
Chaque module de ce programme a été développé avec la volonté de certifier des aspirants CISO et l'objectif de leur transmettre les compétences nécessaires pour rejoindre la nouvelle génération de dirigeants capables de développer et gérer une réelle politique de sécurité de l'information.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur, puis par le passage de l'examen.

Domaine 1 – Gouvernance (Politique, Légal, et Conformité)

Le premier domaine de la formation CCISO est basé sur :
- Le programme de gestion de la sécurité de l'information
- La définition d'un programme de gouvernance de la sécurité de l'information
- La conformité réglementaire et légale
- La gestion des risques

Domaine 2 – Contrôles de gestion de la SI et Gestion des audits

Le deuxième domaine du programme CCISO, une des pierres angulaires de n'importe quel cours de SI, est basé sur les sujets suivants :
- Le design, le déploiement et la gestion des contrôles de sécurité
- Comprendre les types de contrôles de sécurité et les objectifs
- Mettre en place des cadres d'assurance de contrôle
- Comprendre les processus de gestion d'audit

Domaine 3 – Gestion et Opérations des Projets Technologiques

Le troisième domaine du cours CCISO couvre les responsabilités quotidiennes d'un CISO à travers :
- Le rôle d'un CISO
- Les projets de SI
- L'intégration des contraintes de sécurité au sein des autres
- processus opérationnels (gestion du changement, contrôle de version, reprise d'activité, etc.)

Domaine 4 –Compétences principales en SI

Le quatrième domaine de la formation CCISO regroupe, d'un point de vue exé- cutif, les aspects techniques du poste de CISO, prenant en compte :
- Les contrôles d'accès
- La sécurité physique
- Le plan de reprise d'activité
- La sécurité réseau
- La gestion des menaces et des vulnérabilités
- La sécurité des applications
- La sécurité des systèmes
- L'encodage
- L'évaluation des vulnérabilités et les tests d'intrusion
- Forensique et réponse aux incidents

Domaine 5 –Planification stratégique et financière

Le cinquième et dernier domaine du programme CCISO est basé sur les domaines où les professionnels plus orientés sur la technique auront le moins d'expérience :
- Planification stratégique de la sécurité
- Alignement entre les objectifs d'entreprise et la tolérance des risques
- Tendances émergentes de sécurité
- Les KPI : Key Performance Indicators
- Planification financière
- Développement de cas d'entreprises pour la sécurité
- Analyser, anticiper et développer un budget principal de dépenses
- Analyser, anticiper et développer un budget opérationnel de dépenses
- Retour sur investissement (ROI) et analyse des coûts
- Gestion de la force de vente
- Contraintes d'intégration de la sécurité dans les accords contractuels et dans les processus d'approvisionnement
- Assemblés, ces cinq domaines du programme CCISO donneront les compétences et les connaissances requises en SI à un dirigeant d'entreprise

PROGRAMME

CERTIFICATION

Passage de l'examen

L'examen s'effectuera en ligne sur la plateforme ECC.

Il est également possible de passer l'examen à distance en mode RPS-Remote Proctoring Services.

EXAMEN CISO

Examen CISO pour les stagiaires qui justifient de 5 ans d'expérience dans au moins 3 des 5 domaines. L'expérience est vérifiée via la demande d'admissibilité à l'examen (eligibility form) avant le début de la formation.

- **Format de l'examen :** QCM
- **Nombre de questions :** 150
- **Durée :** 2 heures 30
- **Langue :** anglais
- **Score requis :** il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.

EXAMEN EISM

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.

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

Résultat : Directement disponible en fin d'examen.
Maintien de la certification : Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

24 février 2025
23 juin 2025
29 septembre 2025
24 novembre 2025

INFORMATIONS GÉNÉRALES

Code : CCISOv3
Durée : 5 jours
Prix : 4 890 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
ou en distanciel
Examen : inclus.
Valable 12 mois pour un passage de l'examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

OBJECTIFS

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

PUBLIC VISÉ

- RSSI et DSI
- Directeurs sécurité confirmés souhaitant affirmer 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

PRÉ-REQUIS

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.

RESSOURCES

- Support de cours officiel en anglais
- Cours donnés en anglais
- 1 PC par personne / Internet

AVANCÉ

FORMATION CERTIFIANTE

CERTIFIED CLOUD SECURITY ENGINEER V2

Évoluez dans un environnement multicloud & maîtrisez les compétences en matière de sécurité du cloud

Code : CCSEv2

Le programme Certified Cloud Security Engineer (C|CSE) d'EC-Council répond à la demande croissante des professionnels spécialisés en sécurité cloud.

Cette formation certifiante permet aux professionnels du secteur IT d'acquérir des compétences très demandées et liées au cloud. Le CCSE aidera également les entreprises à mettre en place une solide équipe de sécurité cloud en interne.

Le C|CSE est un mélange de deux concepts liés à la sécurité cloud, à la fois neutres et spécifiques à chaque fournisseur (AWS, Azure, GCP), en faisant un programme unique.

Ce programme met l'accent sur la manière de concevoir et de mettre en œuvre des cadres de gouvernance, de risque et conformité (GRC) dans une architecture de cloud computing.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Introduction to Cloud Security
- **Module 2 :** Platform and Infrastructure in Security Cloud
- **Module 3 :** Application Security in Cloud
- **Module 4 :** Data Security in Cloud
- **Module 5 :** Operation Security in Cloud
- **Module 6 :** Penetration Testing in Cloud
- **Module 7 :** Incident Detection and Response in Cloud
- **Module 8 :** Forensic Investigation in Cloud
- **Module 9 :** Business Continuity and Disaster Recovery in Cloud
- **Module 10 :** Governance, Risk Management and Compliance (GRC) in Cloud
- **Module 11 :** Standards, Policies and Legal Issues in Cloud

RÉSULTAT

Directement disponible en fin d'examen.

PASSAGE DE L'EXAMEN

L'examen CCSE aura lieu à distance.

- **Titre de l'examen :** Certified Cloud Security Engineer
- **Format de l'examen :** QCM
- **Nombre de questions :** 125
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** de 60% à 78%

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

3 février 2025
7 avril 2025
13 octobre 2025
1er décembre 2025

INFORMATIONS GÉNÉRALES

Code : CCSEv2
Durée : 5 jours
Prix : 3 890 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
ou en distanciel
Examen : inclus.
Valable 12 mois pour un passage de l'examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

OBJECTIFS

- Évaluer les techniques de stockage et les menaces pesant sur les données stockées dans le cloud et comprendre comment protéger ces données contre les attaques.
- Concevoir et mettre en œuvre un cadre GRC pour l'infrastructure cloud de l'organisation en évaluant divers cadres de conformité et en comprenant les fonctions de conformité fournies par le fournisseur de services.
- Concevoir et mettre en œuvre un plan de réponse aux incidents dans le cloud pour l'organisation et détecter les incidents de sécurité à l'aide d'outils d'automatisation de la sécurité.
- Concevoir et mettre en œuvre un plan de continuité des activités pour les services en cloud en mettant en œuvre des solutions de sauvegarde et de récupération de bout en bout.
- Mettre en œuvre et gérer la sécurité du cloud sur diverses plateformes telles que AWS, Azure et Google Cloud Platform.
- Utiliser les services et outils de sécurité fournis par Azure, AWS et Google Cloud pour sécuriser l'environnement cloud de l'organisation en comprenant le modèle de responsabilité partagée du fournisseur de services.
- Comprendre les implications juridiques associées à l'informatique en cloud afin d'éviter aux organisations des problèmes juridiques.
- Évaluer les différentes normes de sécurité de l'informatique en cloud et les organisations responsables de la mise en place de ces normes.
- Effectuer des audits de sécurité de l'informatique en cloud et des tests de pénétration pour aider les organisations à respecter les normes, les politiques, les procédures et les réglementations régissant les environnements cloud.
- Comprendre et évaluer les différents programmes de conformité et les fonctionnalités offertes par AWS, Azure et Google Cloud.
- Mettre en œuvre des contrôles opérationnels et des normes pour construire, exploiter, gérer et maintenir l'infrastructure cloud.
- Mettre en œuvre les différents services de détection et de réponse aux menaces proposés par Azure, AWS et Google Cloud afin d'identifier les menaces pesant sur les services cloud de l'organisation.
- Comprendre et mettre en œuvre la sécurité pour les environnements cloud privés, multi-locataires et hybrides.
- Apprendre à sécuriser les environnements informatiques hybrides et multi-cloud.
- Être préparé(e) à l'examen Cloud Security Engineer

PUBLIC VISÉ

- Ingénieurs Cloud
- Administrateurs de la sécurité des réseaux
- Analystes de la cybersécurité
- Tout autre poste impliquant des administrations de réseau/cloud

PRÉ-REQUIS

- Avoir de bonnes connaissances en cybersécurité
- Avoir des connaissances de bases en Cloud
- Avoir de bonnes connaissances en gestion de la sécurité des réseaux.

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d'exercices pratiques
- 1 PC par personne

AVANCÉ

FORMATION CERTIFIANTE

CERTIFIED CYBERSECURITY TECHNICIAN

Apprenez les compétences de base essentielles dans 4 disciplines : la défense des réseaux, le piratage éthique, l'investigation numérique et les opérations de sécurité

Code : CCT

Le C|CT est un programme de cybersécurité pour les nouveaux professionnels de la cybersécurité, conçu par EC-Council, pour répondre aux besoins et à la demande mondiale de techniciens en cybersécurité possédant de solides compétences de base. Le C|CT est axé sur la pratique, avec plus de 50 % du temps de formation consacré aux laboratoires. La certification C|CT d'EC-Council plonge les étudiants dans un transfert de connaissances bien structuré.

Cette formation s'accompagne de tâches de réflexion critique et d'exercices de laboratoire immersifs qui permettent aux candidats d'appliquer leurs connaissances et de passer à la phase de développement des compétences. Le programme propose une approche multidimensionnelle qui intègre la défense des réseaux, le hacking éthique et les opérations de sécurité afin de garantir que les titulaires de la certification disposent d'une formation solide et complète leur permettant de configurer, d'analyser et d'identifier les problèmes au sein d'une organisation.
À l'issue du programme, les professionnels certifiés C|CT disposeront d'une base solide dans les principes et techniques de cybersécurité, ainsi que d'une exposition pratique aux tâches requises dans des postes de travail réels.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% exercices pratiques : labs) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Information Security threats and vulnerabilities
- **Module 2 :** Information Security attacks
- **Module 3 :** Network Security fundamentals
- **Module 4 :** Identification, authentification and authorization
- **Module 5 :** Network Security controls: administrative controls
- **Module 6 :** Network Security controls: physical controls
- **Module 7 :** Network Security controls: technical controls
- **Module 8 :** Network Security assessment techniques and tools
- **Module 9 :** Application Security
- **Module 10 :** Virtualization and cloud computing
- **Module 11 :** Wireless Network Security
- **Module 12 :** Mobile Device Security
- **Module 13 :** Internet of Things (IoT) and Operationnal Technology (OT) Security
- **Module 14 :** Cryptography
- **Module 15 :** Data Security
- **Module 16 :** Network Troubleshooting
- **Module 17 :** Network Traffic Monitoring
- **Module 18 :** Network Log Monitoring and Analysis
- **Module 19 :** Incidence Response
- **Module 20 :** Computer Forensics
- **Module 21 :** Business Continuity and Disaster Recovery
- **Module 22 :** Risk Management

PASSAGE DE L'EXAMEN

L'examen CCT 212-82 aura lieu à distance.

- **Titre de l'examen :** Certified Cybersecurity Technician
- **Format de l'examen :** QCM
- **Nombre de questions :** 60
- **Durée :** 3 heures
- **Langue :** anglais
- **Score requis :** 70% minimum de bonnes réponses.

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

24 mars 2025
23 juin 2025
25 août 2025
27 octobre 2025

INFORMATIONS GÉNÉRALES

Code : CCT
Durée : 5 jours
Prix : 2 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
ou en distanciel
Examen : inclus.
Valable 12 mois pour un passage de l'examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

OBJECTIFS

- Comprendre les concepts clés de la cybersécurité, y compris la sécurité de l'information et la sécurité des réseaux
- Comprendre les menaces, les vulnérabilités et les attaques en matière de sécurité de l'information, ainsi que les différents types de logiciels malveillants.
- Contrôler la sécurité des réseaux :
  - Contrôles administratifs (cadres, lois, actes, programmes de gouvernance et de conformité, politiques de sécurité)
  - Contrôles physiques (politiques de sécurité physique et sur le lieu de travail, contrôles environnementaux)
  - Contrôles techniques (protocoles de sécurité du réseau, segmentation du réseau, pare-feu, systèmes de détection et de prévention des intrusions…), ainsi que serveurs proxy, VPN, analyse du comportement des utilisateurs, contrôle de l'accès au réseau…
- Connaître :
  - les techniques et outils d'évaluation de la sécurité des réseaux (chasse aux menaces, renseignements sur les menaces, évaluation des vulnérabilités, piratage éthique, tests de pénétration, gestion des configurations et des actifs)
  - Les techniques de conception et de test de la sécurité des applications
  - Les principes fondamentaux de la virtualisation, de l'informatique en nuage et de la sécurité en nuage
  - Les principes fondamentaux des réseaux sans fil, cryptage sans fil et mesures de sécurité connexes
  - Les principes fondamentaux des dispositifs mobiles, IoT et OT et mesures de sécurité connexes
  - La cryptographie et infrastructure à clé publique
  - Les contrôles de la sécurité des données, méthodes de sauvegarde et de conservation des données et techniques de prévention des pertes de données
  - Le dépannage du réseau, la surveillance du trafic et des journaux, et l'analyse du trafic suspect.
  - Le processus de traitement et de réponse aux incidents
  - Les principes fondamentaux de la criminalistique informatique et des preuves numériques
  - Les concepts de continuité des activités et de reprise après sinistre
  - Les concepts, phases et cadres de gestion des risques
- Être préparé(e) à l'examen Certified Cybersecurity Technician

PUBLIC VISÉ

- Professionnels de l'informatique en début de carrière
- Responsables informatique
- Toute personne souhaitant démarrer sa carrière dans la cybersécurité ou ajouter une solide compréhension des techniques et concepts fondamentaux.

PRÉ-REQUIS

Les stagiaires doivent avoir des connaissances de base en cybersécurité, en cloud et en gestion de la sécurité des réseaux

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 50% d'exercices pratiques
- 1 PC par personne

AVANCÉ

FORMATION CERTIFIANTE

CERTIFIED ETHICAL HACKER V13

Préparez-vous à la certification CEH en apprenant les dernières techniques d'Ethical Hacking

Code : CEHv13

La formation Certified Ethical Hacker (CEH) est une formation reconnue et respectée, dont chaque professionnel de la sécurité aura besoin.

Le programme CEHv13 se distingue par son intégration poussée de l'IA dans toutes les phases du hacking éthique, offrant aux participants une efficacité accrue de 40% et une productivité doublée.

Contrairement au CEHv12, le CEHv13 inclut des outils et techniques d'IA pour automatiser la détection des menaces, prédire les violations de sécurité et répondre rapidement aux incidents. Il propose également des compétences pour sécuriser les technologies basées sur l'IA.

Le programme comprend 221 laboratoires pratiques, plus de 550 techniques d'attaque, et l'utilisation de plus de 4000 outils de hacking. Il est reconnu mondialement et accrédité par des organismes comme le DoD des États-Unis et l'ANAB, le CEH est la première certification mondiale en piratage éthique depuis plus de 20 ans !

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Introduction to Ethical Hacking
- **Module 2 :** Footprinting and Reconnaissance
- **Module 3 :** Scanning Networks
- **Module 4 :** Enumeration
- **Module 5 :** Vulnerability Analysis
- **Module 6 :** System Hacking
- **Module 7 :** Malware Threats
- **Module 8 :** Sniffing
- **Module 9 :** Social Engineering
- **Module 10 :** Denial-of-Service
- **Module 11 :** Session Hijacking
- **Module 12 :** Evading IDS, Firewalls, and
- Honeypots
- **Module 13 :** Hacking Web Servers
- **Module 14 :** Hacking Web Applications
- **Module 15 :** SQL Injection
- **Module 16 :** Hacking Wireless Networks
- **Module 17 :** Hacking Mobile Platforms
- **Module 18 :** IoT and OT hacking
- **Module 19 :** Cloud Computing
- **Module 20 :** Cryptography

RÉSULTAT

Directement disponible en fin d'examen.

PASSAGE DE L'EXAMEN

L'examen CEH aura lieu à distance.

- **Titre de l'examen :** Certified Ethical Hacker (version ANSI)
- **Format de l'examen :** QCM
- **Nombre de questions :** 125
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

27 janvier 2025
24 février 2025
24 mars 2025
14 avril 2025
23 juin 2025
8 septembre 2025
6 octobre 2025
3 novembre 2025
1er décembre 2025

OBJECTIFS

- Maîtriser une méthodologie de piratage éthique qui pourra être utilisée lors d'un test d'intrusion
- Maîtriser les compétences de piratage éthique
- Être préparé(e) à l'examen Certified Ethical Hacker

INFORMATIONS GÉNÉRALES

Code : CEHv13

Durée : 5 jours

Prix : 4 890 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois pour un passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Responsables sécurité
- Auditeurs
- Professionnels de la sécurité
- Administrateurs de site
- Toute personne concernée par la stabilité des systèmes d'information

PRÉ-REQUIS

- Avoir des connaissances de TCP/IP, Linux et Windows Server

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d'exercices pratiques
- 1 PC par personne

EXPERT

FORMATION CERTIFIANTE

COMPUTER HACKING FORENSIC INVESTIGATOR V11

La certification de l'investigation numérique

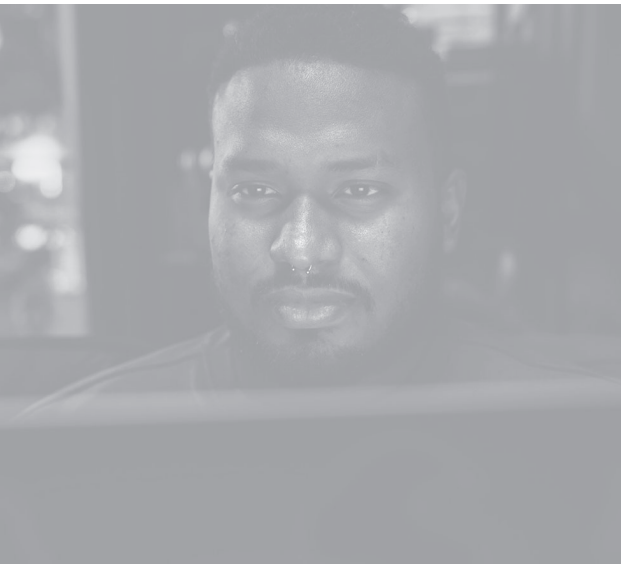
Code : CHFIv11

Les nouvelles technologies sont en train de changer le monde professionnel. Les entreprises s'accommodant rapidement aux technologies numériques comme le cloud, le mobile, le big data ou encore l'IoT, rendent l'étude du forensique numérique dorénavant nécessaire.
Le cours CHFIv11 a été développé pour des professionnels en charge de la collecte de preuves numériques après un cyber crime. Il a été conçu par des experts sur le sujet et des professionnels du secteur, il présente les normes mondiales en matière de bonnes pratiques forensiques. En somme, il vise également à élever le niveau de connaissances, de compréhension et de compétences en cybersécurité des acteurs du forensique.
Le programme CHFIv11 offre une approche méthodologique détaillée du forensique et de l'analyse de preuves numériques. Il apporte les compétences nécessaires à l'identification de traces laissées par un intrus mais également à la collecte de preuves nécessaires à sa poursuite judiciaire. Les outils et savoirs majeurs utilisés par les professionnels du secteur sont couverts dans ce programme. La certification renforcera le niveau de connaissances de toutes les personnes concernées par l'intégrité d'un réseau et par l'investigation numérique.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, ainsi que par le passage de la certification.



PLAN DE COURS

- **Module 1 :** Computer Forensics in Today's World
- **Module 2 :** Computer Forensics Investigation Process
- **Module 3 :** Understanding hard disks and file systems
- **Module 4 :** Data acquisition and duplication
- **Module 5 :** Defending anti-forensics techniques
- **Module 6 :** Operating system forensics
- **Module 7 :** Network forensics
- **Module 8 :** Investigating web attacks
- **Module 9 :** Database forensic
- **Module 10 :** Cloud forensic
- **Module 11 :** Malware forensic
- **Module 12 :** Investigating email crimes
- **Module 13 :** Mobile forensic
- **Module 14 :** Forensic report writing and presentation

PASSAGE DE L'EXAMEN

L'examen CHFIv11 (312-49) aura lieu à distance dans le lieu de votre choix.

Pour passer l'examen à distance, vous devrez alors disposer d'un PC, d'une webcam et d'une bonne connexion à internet.

- **Titre de l'examen :** CHFI
- **Format de l'examen :** QCM
- **Nombre de questions :** 150
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

10 mars 2025
16 juin 2025
15 septembre 2025
17 novembre 2025

OBJECTIFS

- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires
- Se préparer à l'examen CHFI

INFORMATIONS GÉNÉRALES

Code : CHFIv11
Durée : 5 jours
Prix : 4 650 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Examen : inclus. Valable 12 mois pour un passage de l'examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

Toutes les personnes intéressées par le cyber forensique, avocats, consultants juridiques, forces de l'ordre, officiers de police, agents fédéraux et gouvernementaux, personnes en charge de la défense, militaires, détectives et enquêteurs, membres des équipes de réponse après incident, managers IT, défenseurs réseaux, professionnels IT, ingénieurs système/réseau, analystes/consultants/auditeurs sécurité…

PRÉ-REQUIS

- Avoir des connaissances basiques en cybersécurité forensique et gestion d'incident
- L'obtention préalable de la certification CEH est un plus

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d'exercices pratiques
- 1 PC par personne
- Environnement Windows de démonstration et de mise en pratique

EXPERT

FORMATION CERTIFIANTE

CERTIFIED INFORMATION SYSTEMS AUDITOR

Préparation à la certification CISA

Code : CISA

La formation prépare à la certification CISA (Certified Information Systems Auditor), seule certification reconnue mondialement dans le domaine de la gouvernance, de l'audit, du contrôle et de la sécurité des SI.
Son excellente réputation au niveau international vient du fait que cette certification place des exigences élevées et identiques dans le monde entier.

Elle couvre donc la totalité du cursus CBK (Common Body of Knowledge), tronc commun de connaissances en sécurité défini par l'ISACA® (Information Systems Audit and Control Association).

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (TP, cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

Domaine 1 : Processus d'audit des systèmes d'information

- Les standards d'audit
- L'analyse de risque et le contrôle interne
- La pratique d'un audit SI

Domaine 2 : Gouvernance et gestion des systèmes d'information

- La stratégie de la gouvernance du SI
- Les procédures et Risk management
- La pratique de la gouvernance des SI
- L'audit d'une structure de gouvernance

Domaine 3 : Acquisition, conception, implantation des SI

- La gestion de projet : pratique et audit
- Les pratiques de développement
- L'audit de la maintenance applicative et des systèmes
- Les contrôles applicatifs

Domaine 4 : Exploitation, entretien et soutien des systèmes d'information

- L'audit de l'exploitation des SI
- L'audit des aspects matériels du SI
- L'audit des architectures SI et réseaux

Domaine 5 : Protection des actifs informationnels

- La gestion de la sécurité : politique et gouvernance
- L'audit et la sécurité logique et physique
- L'audit de la sécurité des réseaux
- L'audit des dispositifs nomades

PRÉPARATION DE L'EXAMEN

CERTIFICATION CISA

L'inscription à l'examen se fait directement sur le site de l'ISACA.
Le passage de l'examen est disponible dans plusieurs langues, dont l'anglais et le français.

PROCHAINES DATES

10 mars 2025
16 juin 2025
13 octobre 2025
1er décembre 2025

OBJECTIFS

- Analyser les différents domaines du programme sur lesquels porte l'examen
- Assimiler le vocabulaire et les idées directrices de l'examen
- S'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire
- Se préparer au passage de l'examen de certification CISA

INFORMATIONS GÉNÉRALES

Code : CISA

Durée : 5 jours

Prix : 4 400 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : Non inclus. Inscription à l'examen sur le site de l'ISACA.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Auditeurs
- Consultants IT
- Responsables IT
- Responsables de la sécurité
- Directeurs des SI

PRÉ-REQUIS

- Avoir des connaissances générales en informatique, sécurité et audit
- Avoir des connaissances de base dans le fonctionnement des systèmes d'information

RESSOURCES

- Support de cours en français
- Cours donnés en français
- 1 PC par personne

EXPERT

FORMATION CERTIFIANTE

CERTIFIED INFORMATION SECURITY MANAGER

Préparation à la certification CISM®

La formation prépare à l'examen CISM (Certified Information Security Manager), la certification professionnelle mondialement reconnue et délivrée par l'ISACA (Information Systems Audit and Control Association). Elle couvre la totalité du cursus CBK (Common Body of Knowledge), le tronc commun de connaissances en sécurité défini par l'ISACA.

Code : CISM

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification.

La formation couvre les 4 domaines sur lesquels porte l'examen

- Domaine 1 : Gouvernance de la sécurité de l'information
- Domaine 2 : Gestion des risques de l'information
- Domaine 3 : Développement et gestion des programmes de sécurité de l'information
- Domaine 4 : Gestion des incidents de sécurité de l'information
- Examen blanc et procédure de certification

PLAN DE COURS

- Information Security Governance
  - Explain the need for and the desired outcomes of an effective information security strategy
  - Create an information security strategy aligned with organizational goals and objectives
  - Gain stakeholder support using business cases
  - Identify key roles and responsibilities needed to execute an action plan
  - Establish metrics to measure and monitor the performance of security governance
- Information Risk Management
  - Explain the importance of risk management as a tool to meet business needs and develop a security management program to support these needs
  - Identify, rank, and respond to a risk in a way that is appropriate as defined by organizational directives
  - Assess the appropriateness and effectiveness of information security controls
  - Report information security risk effectively
- Information Security Program Development and Management
  - Align information security program requirements with those of other business functions
  - Manage the information security program resources
  - Design and implement information security controls
  - Incorporate information security requirements into contracts, agreements and third-party management processes
- Information Security Incident Management
  - Understand the concepts and practices of Incident Management
  - Identify the components of an Incident Response Plan and evaluate its effectiveness
  - Understand the key concepts of Business Continuity Planning, or BCP and Disaster Recovery Planning, or DRP
- CISM Sample Exam

CERTIFICATION CISM

L'inscription à l'examen se fait directement sur le site de l'ISACA.

Trois langues sont disponibles pour le passage de l'examen dont l'anglais.

La langue française n'est pas disponible.

PROCHAINES DATES

10 février 2025
19 mai 2025
22 septembre 2025
24 novembre 2025

OBJECTIFS

- Découvrir et maîtriser les 4 grands domaines sur lesquels porte l'examen CISM
- Assimiler le vocabulaire de la certification CISM et les idées directrices de l'examen
- S'entrainer au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire
- Se préparer au passage de l'examen de certification CISM

INFORMATIONS GÉNÉRALES

Code : CISM

Durée : 4 jours

Prix : 4 235 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : non inclus. Inscription à l'examen sur le site de l'ISACA. Formation certifiante.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Professionnels en sécurité
- RSSI
- Consultants en sécurité
- Toute personne souhaitant acquérir des connaissances en la matière

PRÉ-REQUIS

- Avoir des connaissances de base dans le fonctionnement des systèmes d'information
- Afin d'obtenir la certification CISM, il faudra justifier de 5 ans d'expérience dans la gestion de la sécurité de l'information. Des dérogations sont néanmoins possibles pour un maximum de 2 ans

RESSOURCES

- Cours délivrés en français
- Support de cours en anglais

EXPERT

FORMATION CERTIFIANTE

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

La certification des professionnels de la sécurité de l'information

Code : CISSP

La certification CISSP est mondialement reconnue pour son niveau avancé de compétences (plus de 100 000 personnes certifiées à travers le monde). C'est la première reconnaissance dans le domaine de la sécurité de l'information à détenir les critères mis en place par la norme ISO/IEC 17024. Obtenir la CISSP prouvera que vous êtes un professionnel qualifié et expert dans le design, la construction et le maintien d'un environnement professionnel sécurisé. Votre CISSP vous permettra de vous afficher comme un futur leader dans le domaine de la sécurité de l'information. Nous avons développé des supports de cours qui vous aideront à préparer le nombre important de domaines présents dans l'examen, ils sont souvent considérés comme "10 miles wide and two inches deep". Nos formateurs sont tous détenteurs de leur certification CISSP et sont des professionnels travaillant sur le secteur IT et de la sécurité de l'information.
Nous vous fournissons les outils pour réussir, notamment des supports de cours, des vidéos des sujets importants et des manuels d'études. Tout ceci a été développé pour acquérir le CBK – Common Body of Knowledge.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification.

Outre la préparation en tant que telle à l'examen de certification CISSP, le but de la formation est d'enrichir les connaissances des participants dans les différents domaines d'expertise. Le contenu a été remanié et mis à jour pour refléter les dernières évolutions des questions de sécurité, des préoccupations et des contre-mesures actuelles.

Nous parcourons les 8 domaines du CBK® - Common Body of Knowledge

1. Gestion des risques et de la sécurité
2. Sécurité des atouts
3. Ingénierie et sécurité
4. Sécurité des télécommunications et des réseaux
5. Gestion de l'identité et des accès
6. Évaluation et tests de sécurité
7. Sécurité des opérations
8. Développement sécurisé de logiciels

Contenu du kit de formation

- Support de cours de l'Université de Dallas
- CISSP All-in-One Exam Guide 9th Edition (mise à jour des 8 domaines du CBK, un contenu digital avec + de 1400 questions pratiques)
- CISSP Practice Exams 5th Edition (+ 250 questions pratiques couvrant les 8 domaines du CBK, des questions concrètes avec des réponses expliquées et détaillées, un contenu digital avec + de 100 questions pratiques additionnelles)

L'examen

Le passage de l'examen a lieu dans un centre de test Pearson Vue.
Pour trouver le centre d'examen le plus proche et consulter les dates d'examen disponibles, vous devez vous créer un compte sur le site de Pearson Vue.

Depuis avril 2018, l'examen CISSP en ligne (CAT : computerized adaptive testing) est disponible pour tous les examens en anglais.

Examen en langue anglaise

- **Durée :** 3 heures
- **Nombre de questions :** entre 100 et 150 questions (le nombre de questions est variable car il dépend des questions et réponses précédentes)
- **Score requis :** 700/1000

Examen en langue française

- **Durée :** 6 heures
- **Nombre de questions :** 250
- **Type de questions :** choix multiples et questions avancées innovantes
- **Score requis :** 700/1000

PROCHAINES DATES

17 mars 2025
30 juin 2025
20 octobre 2025
8 décembre 2025

OBJECTIFS

- Maîtriser les 8 domaines du Common Body of Knowledge (CBK®)
- Se préparer à la certification professionnelle CISSP, la seule formation généraliste et complète traitant de la sécurité des systèmes d'information

INFORMATIONS GÉNÉRALES

Code : CISSP

Durée : 5 jours

Prix : 4 150 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : non inclus. Inscription à l'examen sur le site de l'ISC².

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Experts de la sécurité des systèmes d'information souhaitant se préparer à la certification professionnelle délivrée par l'(ISC²)
- Ingénieurs systèmes / réseaux, consultants, développeurs souhaitant acquérir la terminologie, les fondements et les bases communes de cette discipline large et complexe

PRÉ-REQUIS

- Afin d'obtenir la certification CISSP, il faudra justifier de 5 ans d'expérience professionnelle dans au moins 2 des 8 domaines du CBK®
- Un candidat qui n'a pas l'expérience requise pour obtenir la certification CISSP peut passer l'examen et obtenir le titre Associate of (ISC²). Il aura alors jusqu'à 6 ans pour acquérir les 5 années d'expérience requises

RESSOURCES

- Cours donnés en français
- Support de cours de l'Université de Dallas
- Le CISSP All-in-One Exam Guide 9th Edition
- Le CISSP Practice Exams 5th Edition

AVANCÉ

FORMATION CERTIFIANTE

CERTIFIED NETWORK DEFENDER V3

Formez-vous au seul programme entièrement axé sur la sécurité et la défense des réseaux !

Code : CNDv3

Le Certified Network Defender – CND – est un cours indépendant des fabricants, pratique, donné par un formateur accrédité et qui permettra aux étudiants de se certifier dans le domaine de la sécurité des réseaux. Avec un programme intensif de labs, la formation a été créée sur des compétences précises, directement liées à l'analyse des fiches de poste et au cadre de formation en cybersécurité donné par la National Initiative of Cybersecurity Education (NICE). La formation a également été adaptée aux différentes missions et responsabilités du poste d'administrateur système/réseau publiées par le Department of Defense (DoD).

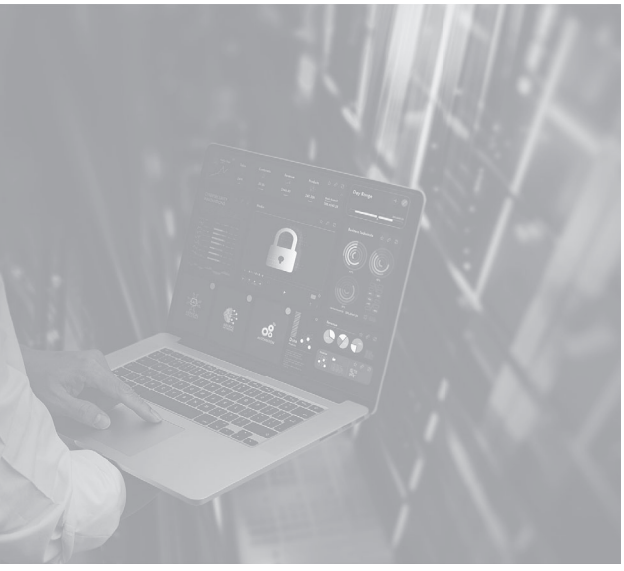
Afin d'obtenir des compétences solides en sécurité défensive des réseaux, la formation prépare les administrateurs réseaux aux dernières technologies et pratiques de sécurité réseau.

Le programme Certified Network Defender v3 a été mis à jour pour vous donner les armes nécessaires afin d'aider les Blue Teams à se défendre. Les particuliers et les entreprises qui cherchent à renforcer leurs compétences en matière de défense de réseau trouveront la CND v3 indispensable.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% exercices pratiques : labs) et formalisés par le passage de la certification.



PLAN DE COURS

- **Module 1 :** Network Attacks and Defense Strategies
- **Module 2 :** Administrative Network Security
- **Module 3 :** Technical Network Security
- **Module 4 :** Network Perimeter Security
- **Module 5 :** Endpoint Security – Windows Systems
- **Module 6 :** Endpoint Security – Linux Systems
- **Module 7 :** Endpoint Security – Mobiles Devices
- **Module 8 :** Endpoint Security – IoT Devices
- **Module 9 :** Administrative Application Security
- **Module 10 :** Data Security
- **Module 11 :** Entreprise Virtual Security
- **Module 12 :** Entreprise Cloud Security
- **Module 13 :** Entreprise Wireless Security
- **Module 14 :** Network Traffic Monitoring and Analysis
- **Module 15 :** Network Logs Monitoring and Analysis
- **Module 16 :** Incident Response and Forensic Investigation
- **Module 17 :** Business Continuity and Disaster Recovery
- **Module 18 :** Risk Anticipation with Risk Management
- **Module 19 :** Threat Assessment with Attack Surface Analysis
- **Module 20 :** Threat Prediction with Cyber Threat Intelligence

PASSAGE DE L'EXAMEN

L'examen CND 312-38 aura lieu à distance.

- **Titre de l'examen :** Certified Network Defender (ANSSI)
- **Format de l'examen :** QCM
- **Nombre de questions :** 100
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** 70% minimum de bonnes réponses

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

24 février 2025
14 avril 2025
7 juillet 2025
20 octobre 2025

OBJECTIFS

- Appréhender les fonctionnalités de protection, de détection, de réponse et de prévision de la sécurité des réseaux
- Être capable de sécuriser les conteneurs et les réseaux définis par logiciel
- Prévenir les menaces
- Être préparé(e) à l'examen Certified Network Defender (ANSI)

INFORMATIONS GÉNÉRALES

Code : CNDv3

Durée : 5 jours

Prix : 3 890 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception.

Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Administrateur réseau / Administrateur sécurité réseau
- Ingénieurs sécurité réseau
- Techniciens défense réseau
- Analystes CND / Sécurité
- Responsable sécurité
- Toute personne impliquée dans des opérations de réseau

PRÉ-REQUIS

- Avoir des connaissances avancées sur les systèmes d'exploitation Windows et Linux (systèmes de fichiers, permissions, sécurité, pare-feu, etc.)
- Maîtriser les fondamentaux des réseaux, tels que les protocoles TCP/IP
- Connaître les rôles et les services qui sont utilisés par les serveurs au niveau du réseau.

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 50% d'exercices pratiques
- 1 PC par personne

EXPERT

FORMATION CERTIFIANTE

CERTIFIED SOC ANALYST

Un programme certifiant qui atteste d'une solide connaissance des outils, méthodes et processus de gestion d'un SOC pour valoriser vos équipes et rassurer vos clients.

Le programme Certified SOC Analyst (CSA) est la première étape pour rejoindre un SOC - Security Operations Center.
Il est conçu pour les analystes de niveau I et II afin de leur permettre d'acquérir les compétences nécessaires pour effectuer des opérations de premier et deuxième niveau.
Le CSA est un programme de formation et d'accréditation qui aide le candidat à acquérir des compétences techniques recherchées. Le programme met l'accent sur la création de nouvelles possibilités de carrière grâce à des connaissances approfondies et méticuleuses et à des capacités de niveau amélioré pour contribuer de façon dynamique à une équipe SOC.

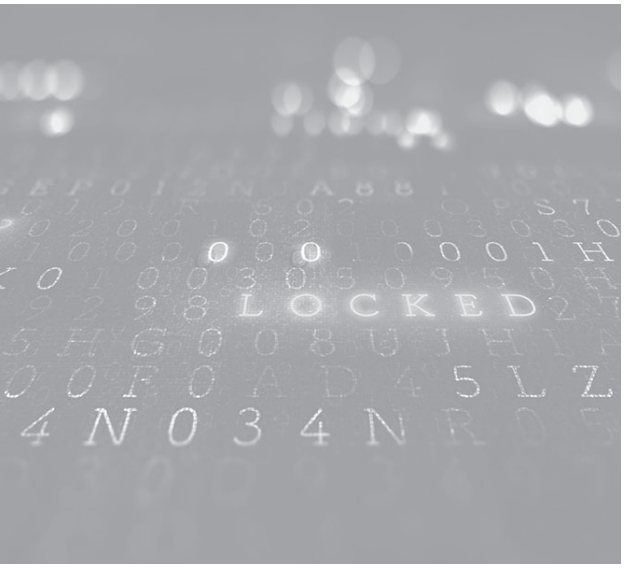
Ce programme intensif de 3 jours couvre en profondeur les principes fondamentaux des opérations SOC, de la gestion et corrélation des logs, du déploiement SIEM, de la détection avancée des incidents et réponse aux incidents.
De plus, le candidat apprendra à gérer de nombreux processus SOC et à collaborer avec le CSIRT en cas de besoin.

Code : CSA

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, puis par le passage de l'examen.



PLAN DE COURS

- **Module 1 :** Security Operations and Management
- **Module 2 :** Understanding Cyber Threats, IoCs, and Attack Methodology
- **Module 3 :** Incidents, Events, and Logging
- **Module 4 :** Incident Detection with Security Information and Event Management (SIEM)
- **Module 5 :** Enhanced Incident Detection with Threat Intelligence
- **Module 6 :** Incidence Response

CERTIFICATION CSA (incluse avec la formation)

Passage de l'examen : l'examen CSA aura lieu à distance, depuis le lieu de votre choix.

- **Titre de l'examen :** Certified SOC Analyst
- **Nombre de questions :** 100
- **Durée :** 3 heures
- **Score requis :** 70%

RÉSULTAT

Directement disponible en fin d'examen.

PROCHAINES DATES

26 février 2025
11 juin 2025
1er octobre 2025
19 novembre 2025

OBJECTIFS

- Comprendre le processus SOC de bout en bout
- Détecter des incidents avec un SIEM
- Détecter des intrusions avec les modèles de menace
- Comprendre le déploiement d'un SIEM

INFORMATIONS GÉNÉRALES

Code : CSA

Durée : 3 jours

Prix : 2 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Analystes SOC (Niveau I et Niveau II)
- Administrateurs de Réseau et Sécurité, Ingénieurs de Réseau et Sécurité, Analyste en Sécurité, Analystes en Défense de Réseau, Techniciens en Défense de Réseau, Spécialistes en Sécurité de Réseau, Opérateur en Sécurité de Réseau, et tout professionnel en sécurité qui s'occupe des opérations de sécurité de réseau
- Analystes en cybersécurité
- Professionnels en cybersécurité débutants
- Quiconque voulant devenir Analyste SOC

PRÉ-REQUIS

- Avoir des connaissances en gestion d'incidents
- Savoir ce qu'est un SOC

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- 20% d'exercices pratiques
- 1 PC par personne

FONDAMENTAUX

FORMATION CERTIFIANTE

CERTIFIED SECURE COMPUTER USER V3

Formation indispensable pour tous les utilisateurs d'outils numériques pour une mise en application immédiate de bonnes pratiques.

Code : CSCUv3

L'objectif de la formation CSCUv3 est d'apporter aux utilisateurs finaux le savoir et les compétences nécessaires à la protection de leurs informations les plus importantes.

Ce cours va immerger les étudiants dans un environnement interactif où ils vont acquérir des connaissances fondamentales sur différents types d'ordinateurs mais aussi sur les menaces de sécurité des réseaux comme l'usurpation d'identité, la fraude à la carte bancaire, les escroqueries des banques en ligne, les virus et backdoors, les emails piégés, les personnes sexuellement malintentionnées, les pertes de données confidentielles, les attaques des pirates ainsi que l'ingénierie sociale.

Les compétences acquises dans cette formation aideront les étudiants à connaitre les étapes nécessaires pour définir leur niveau d'exposition en termes de sécurité. Dans cette dernière version, des Labs sont disponibles dont 6 modules avec des guides & challenges complets !

Nouveauté : version totalement française disponible (labs + certification).

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Introduction à la sécurité des données
- **Module 2 :** Sécurisation des systèmes d'exploitation
- **Module 3 :** Malwares et antivirus
- **Module 4 :** Sécurité d'internet
- **Module 5 :** Sécurité sur les sites de réseaux sociaux
- **Module 6 :** Sécurisation des communications par email
- **Module 7 :** Sécurisation des appareils mobiles
- **Module 8 :** Sécurisation du Cloud
- **Module 9 :** Sécurisation des connexions réseaux
- **Module 10 :** Sauvegarde des données et reprise après sinistre
- **Module 11 :** Sécurisation des appareils IoT et des consoles de jeux
- **Module 12 :** Sécurisation du travail à distance

RÉSULTAT

Directement disponible en fin d'examen.

PASSAGE DE L'EXAMEN

L'examen CSCU 112-12 aura lieu à distance.

- **Titre de l'examen :** Certified Secure Computer User
- **Format de l'examen :** QCM
- **Nombre de questions :** 50
- **Durée :** 2 heures
- **Langue :** français ou anglais
- **Score requis :** 70% minimum de bonnes réponses requises

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

20 mars 2025
12 juin 2025
11 septembre 2025
13 novembre 2025

OBJECTIFS

- Comprendre l'importance de la sécurité des données
- Sécuriser différents systèmes d'exploitation
- Implémenter la sécurité des données
- Installer et configurer des antivirus
- Implémenter des mesures de sécurité lors des navigations en ligne
- Implémenter des mesures de sécurité pour protéger ses échanges mails
- Prévenir les attaques sur les appareils mobiles
- Sécuriser les comptes cloud, les connexions réseaux, les appareils IoT et les consoles de jeux
- Sécuriser les connexions réseaux
- Implémenter les mesures de sécurité appropriées pour protéger vos navigations en ligne
- Être préparé(e) à l'examen Certified Secure Computer User

INFORMATIONS GÉNÉRALES

Code : CSCU

Durée : 2 jours

Prix : 1 490 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

Tous les utilisateurs réguliers d'ordinateurs, qui se servent d'Internet et du web notamment pour travailler, étudier ou jouer et qui souhaitent se former sur les problèmes de sécurité informatique.

PRÉ-REQUIS

- Avoir une compréhension de base des ordinateurs et des appareils informatiques.

RESSOURCES

- Support de cours officiel en français ou en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d'exercices pratiques
- 1 PC par personne

AVANCÉ

FORMATION CERTIFIANTE

DORA CERTIFIED LEAD MANAGER

Maîtrisez les compétences pour conduire la résilience numérique dans les entités financières et assurer la conformité avec DORA

Code : DORA LM

Avec l'entrée en vigueur de DORA le 17 janvier 2025, il est important d'en saisir pleinement les implications et exigences.

Participer à la formation PECB Certified DORA Lead Manager offre une occasion unique pour interagir avec les experts et pairs du secteur, favorisant des discussions enrichissantes et l'échange d'idées précieuses concernant les meilleures pratiques pour la résilience opérationnelle numérique. Par le biais de sessions interactives et d'exercices pratiques, vous obtiendrez des perspectives concrètes concernant la mise en œuvre de stratégies efficaces pour atténuer les risques liés aux TIC(*) et améliorer la résilience opérationnelle des institutions financières.

En outre, la participation à cette formation démontre votre engagement en matière de développement professionnel et vous positionne comme un leader compétent dans le paysage en évolution de la résilience opérationnelle numérique.

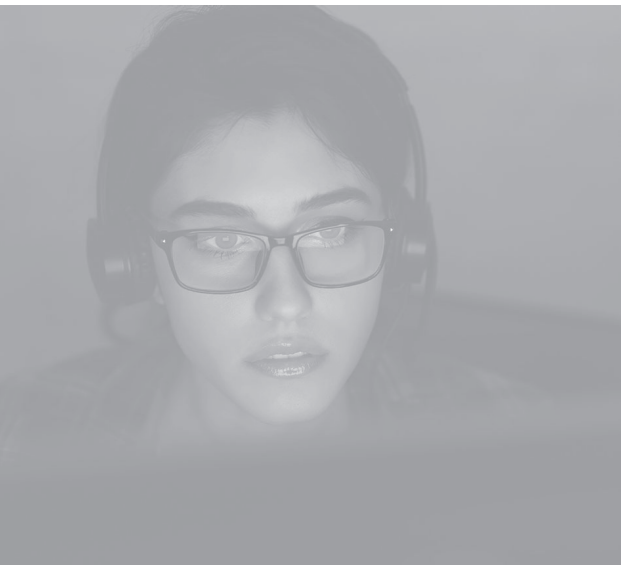
Après la formation et la réussite à l'examen, vous pouvez demander le certificat « PECB Certified DORA Lead Manager ».

(*) : Technologies de l'Information et de la Communication

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, puis par le passage de l'examen.



JOUR 1

Introduction des concepts et des exigences de DORA

JOUR 2

Gestion des risque et incidents liés aux TIC

JOUR 3

Gestion des risques liés aux prestataires tiers et partage des informations

JOUR 4

Réévaluation et amélioration continuelle

JOUR 5

Examen

- Les candidats passeront l'examen le vendredi
- Format : examen écrit
  - Durée : 3 heures
  - Langue : anglais
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

10 mars 2025
2 juin 2025
25 août 2025
27 octobre 2025

OBJECTIFS

- Comprendre le paysage règlementaire et les exigences en matière de conformité du règlement DORA, se basant sur cinq piliers fondamentaux, parmi lesquels la gestion des risques liés aux TIC, la gestion et la notification des incidents liés aux TIC, les tests de résilience opérationnelle numérique et la gestion des risques liés aux prestataires tiers.
- Mettre en œuvre des stratégies et mesures pour améliorer la résilience opérationnelle et atténuer les risques liés aux TIC dans les institutions financières, en se conformant aux exigences de DORA et aux meilleures pratiques du secteur
- Identifier, analyser, évaluer et gérer les risques liés aux TIC qui concernent les entités financières
- Développer et maintenir des cadres robustes de gestion des risques liés aux TIC, des plans de réponse en cas d'incident et des plans de continuité opérationnelle et de reprise après sinistre
- Favoriser la collaboration et la communication avec les principales parties prenantes pour réussir la mise en œuvre et le respect permanent de DORA
- Utiliser des outils et des méthodologies du secteur pour suivre, évaluer et gérer les risques et les vulnérabilités liés aux TIC, améliorant la posture de sécurité globale des institutions financières

INFORMATIONS GÉNÉRALES

Code : DORA LM

Durée : 5 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Cadres supérieurs et décideurs des institutions financières
- Responsables de la conformité et gestionnaires de risques
- Professionnels des TI
- Personnel des affaires juridiques et réglementaires
- Consultants et conseillers spécialisés dans la règlementation financière et la cybersécurité

PRÉ-REQUIS

- Connaître les concepts de base de la sécurité de l'information et de la cybersécurité
- Connaître les principes de la gestion des risques liés aux technologies de l'information et de la communication (TIC)

RESSOURCES

- Support de cours en anglais contenant plus de 450 pages d'informations explicatives, d'exemples, de bonnes pratiques, d'exercices et de quiz
- Cours donné en français

AVANCÉ

FORMATION CERTIFIANTE

EC-COUNCIL CERTIFIED DEVSECOPS ENGINEER V2

Accélérez la transformation numérique grâce à un programme intensif pour concevoir, développer et maintenir des applications et des infrastructures sécurisées.

Avec l'augmentation constante des menaces cyber, le besoin de sécuriser au mieux les applications et infrastructures est de plus en plus présent !

EC-Council Certified DevSecOps Engineer (E|CDE) est un programme de certification DevSecOps complet, pratique et dirigé par un instructeur, qui aide les professionnels à acquérir les compétences essentielles pour concevoir, développer et maintenir les applications et les infrastructures sécurisées.

L'E|CDE est un mélange parfait de connaissances théoriques et pratiques de DevSecOps dans votre environnement on-premises et cloud-native (AWS et Azure). Le programme se concentre sur le DevSecOps des applications et donne un aperçu du DevSecOps des infrastructures. Il aide les ingénieurs DevSecOps à développer et à améliorer leurs connaissances et leurs compétences en matière de sécurisation des applications à toutes les étapes du DevOps.

Code : ECDE

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Understanding DevOps Culture
- **Module 2** : Introduction to DevSecOps
- **Module 3** : DevSecOps Pipeline - Plan Stage
- **Module 4** : DevSecOps Pipeline - Code Stage
- **Module 5 :** DevSecOps Pipeline - Build and Test Stage
- **Module 6 :** DevSecOps Pipeline – Release and Deploy Stage
- **Module 7 :** DevSecOps Pipeline – Operate and Monitoring Stage
- **Module 8 :** Sécurisation des appareils mobiles

RÉSULTAT

Directement disponible en fin d'examen.

PASSAGE DE L'EXAMEN

L'examen ECDE 312-97 aura lieu à distance.

- **Titre de l'examen :** EC-Council Certified DevSecOps Engineer
- **Format de l'examen :** QCM
- **Nombre de questions :** 100
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** 70% minimum de bonnes réponses requises

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

19 février 2025
23 avril 2025
24 septembre 2025
12 novembre 2025

OBJECTIFS

- Comprendre la chaîne d'outils DevSecOps et les contrôles de sécurité dans le pipeline automatisé DevOps.
- Adopter des pratiques de sécurité telles que la collecte des exigences de sécurité, la modélisation des menaces et la sécurisation des revues de code dans le flux de travail de développement.
- Apprendre les outils DevSecOps AWS et Azure pour sécuriser les applications.
- Intégrer des outils et des pratiques pour construire un feedback continu dans le pipeline DevSecOps en utilisant Jenkins et les notifications par email de Microsoft Teams.
- Auditer les poussées de code, les pipelines et les conformités à l'aide de divers outils de journalisation et de surveillance comme Sumo Logic, Datadog, Splunk, ELK et Nagios.
- Être préparé(e) à l'examen EC-Council Certified DevSecOps Engineer

INFORMATIONS GÉNÉRALES

Code : ECDE

Durée : 3 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Toute personne ayant des connaissances préalables de la sécurité des applications
- Professionnel de la sécurité des applications
- Ingénieur DevSecOps
- Ingénieur/testeur en logiciels
- Professionnel de la sécurité informatique
- Analyste en cybersécurité

PRÉ-REQUIS

- Avoir une bonne compréhension des concepts de sécurité des applications.

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 70% d'exercices pratiques
- 1 PC par personne

AVANCÉ

FORMATION CERTIFIANTE

EC-COUNCIL CERTIFIED INCIDENT HANDLER V3

Apprenez à gérer les incidents de sécurité

Code : ECIHv3

Le programme ECIHv3 propose une approche holistique qui couvre de nombreux concepts autour de la réponse et de la gestion d'incidents.
Cela va de la préparation, de la planification du processus de réponse à incident, jusqu'à la récupération des actifs principaux de l'organisation après un incident de sécurité. Dans l'objectif de protéger les organisations, ces concepts sont désormais essentiels pour pouvoir gérer et répondre aux futures menaces et attaques.

Ce programme aborde toutes les étapes du processus de gestion et réponse à incident, cela permettra aux candidats de développer et de réellement valoriser des compétences dans ce domaine. Cette approche permet à la certification ECIHv3 d'être une des plus complètes sur le marché aujourd'hui, dans le domaine de la réponse et gestion d'incidents.
Les compétences acquises dans le programme ECIHv3 sont de plus en plus recherchées à la fois par les professionnels de la cybersécurité mais également par les employeurs, et ce, dans le monde entier.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (lors de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, puis du passage de la certification.

PLAN DE COURS

- **Module 1 :** Introduction to Incident Handling and Response
- **Module 2 :** Incident Handling and Response Process
- **Module 3 :** Forensic Readiness and First Response
- **Module 4 :** Handling and Responding to Malware Incidents
- **Module 5 :** Handling and Responding to Email Security Incidents
- **Module 6 :** Handling and Responding to Network Security Incidents
- **Module 7 :** Handling and Responding to Web Application Security Incidents
- **Module 8 :** Handling and Responding to cloud Security Incidents
- **Module 9 :** Handling and Responding to Insider Threats
- **Module 10 :** Handling and Responding to Endpoint Security Incidents

CERTIFICATION ECIH (incluse avec la formation)

Présentation : L'examen ECIH aura lieu à distance.

Pour passer l'examen à distance, vous devrez alors disposer d'une webcam et d'une bonne connexion à internet.

Passage de l'examen :

- **Titre de l'examen :** EC-Council Certified Incident Handler
- **Format de l'examen :** QCM
- **Nombre de questions :** 100
- **Durée :** 3 heures
- **Langue :** anglais
- **Score requis :** 70%

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

19 février 2025
21 mai 2025
9 juillet 2025
8 octobre 2025

OBJECTIFS

- Apprendre les différentes étapes permettant de gérer et répondre à un incident de sécurité
- Se préparer au passage de l'examen de certification Certified Incident Handler

INFORMATIONS GÉNÉRALES

Code : ECIHv3

Durée : 3 jours

Prix : 3 100 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Gestionnaires d'incidents
- Administrateurs d'évaluation des risques
- Pentesters
- Cyber-enquêteurs judiciaires
- Consultants en évaluation de vulnérabilités
- Administrateurs de systèmes
- Ingénieurs de systèmes
- Administrateurs de pare-feu
- Responsables de réseaux
- Responsables IT
- Professionnels IT
- Toute personne intéressée par la gestion et la réponse aux incidents

PRÉ-REQUIS

- Avoir des connaissances générales en réseau et en sécurité

RESSOURCES

- Support de cours officiel en anglais
- Cours donnés en français
- 1 PC par personne

AVANCÉ

FORMATION CERTIFIANTE

ISO 27001 : CERTIFIED LEAD AUDITOR

Maîtrisez l'audit d'un système de management de sécurité de l'information (SMSI) basé sur la norme ISO/IEC 27001

Code : ISO 27001 LA

Ce cours intensif de 5 jours va permettre aux participants de développer l'expertise nécessaire pour gérer des structures liées à la gestion des systèmes de sécurité d'informations et de gérer une équipe d'auditeurs en leur faisant appliquer des principes, des procédures et des techniques d'audits largement reconnus. Pendant cette formation, le participant va acquérir les connaissances et les compétences nécessaires afin de planifier et de réaliser des audits internes et externes en liaison avec la norme ISO 19011, le processus de certification lié à la norme ISO 1702. À partir d'exercices pratiques, le stagiaire va développer des connaissances (gestion d'audits techniques) et des compétences (gestion d'une équipe et d'un programme d'audits, communication avec les clients, résolution de différends, etc.) nécessaires au bon déroulement d'un audit.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour de la formation.

JOURS 1, 2, 3 & 4

Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par l'ISO 27001

- Cadre normatif, légal et réglementaire lié à la sécurité de l'information
- Principes fondamentaux de la sécurité de l'information
- Processus de certification ISO 27001
- Présentation détaillée des clauses 4 à 10 de l'ISO 27001

Planification et initialisation d'un audit 27001

- Principes et concepts fondamentaux d'audit
- Approche d'audit basée sur les preuves et sur le risque
- Préparation d'un audit de certification ISO 27001
- Audit documentaire d'un SMSI

Conduire un audit ISO 27001

- Communication pendant l'audit
- Procédures d'audit : observation, revue documentaire, entretiens, techniques d'échantillonnage, vérification technique, corroboration et évaluation
- Rédaction des plans de tests d'audit
- Formulation des constats d'audit et rédaction des rapports de non-conformité

Clôturer et assurer le suivi d'un audit ISO 27001

- Documentation d'audit
- Mener une réunion de clôture et fin d'un audit ISO 27001
- Évaluation des plans d'action correctifs
- Audit de surveillance ISO 27001 et programme de gestion d'audit

JOUR 5

L'examen « Certified ISO /IEC 27001 Lead Auditor »

- Les candidats passeront l'examen le vendredi après-midi.
  - Format : examen écrit
  - Durée : 3h
  - Langue : disponible en français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program). Il couvre les domaines de compétence suivants :
  - Domaine 1 : Principes et concepts fondamentaux de sécurité de l'information
  - Domaine 2 : Système de Management de la Sécurité de l'Information
  - Domaine 3 : Concepts et principes fondamentaux d'audit
  - Domaine 4 : Préparation d'un audit ISO 27001
  - Domaine 5 : Conduire un audit ISO 27001
  - Domaine 6 : Clôturer un audit ISO 27001
  - Domaine 7 : Gérer un programme d'audit ISO 27001

RÉSULTATS

Disponibles sous 4 à 8 semaines et directement envoyés par e-mail au candidat.

CERTIFICATION

- Un certificat de participation de 31 crédits CPD (Continuing Professional Development) sera délivré par PECB
- Les personnes ayant réussi l'examen pourront demander la qualification de «Certified ISO/IEC 27001 Provisional Auditor», «Certified ISO/IEC 27001 Auditor» ou «Certified ISO/IEC 27001 Lead Auditor», en fonction de leur niveau d'expérience.
  Un certificat sera alors délivré aux participants remplissant l'ensemble des exigences relatives à la qualification choisie.
  Pour plus d'information à ce sujet, vous pouvez consulter le site de PECB.

PROCHAINES DATES

3 mars 2025
16 juin 2025
6 octobre 2025
8 décembre 2025

OBJECTIFS

- Comprendre la mise en œuvre d'un Système de Management de la Sécurité de l'Information conforme à la norme ISO 27001
- Acquérir une compréhension globale des concepts, démarches, normes, méthodes et techniques nécessaires pour gérer efficacement un Système de Management de la Sécurité de l'Information
- Acquérir l'expertise nécessaire pour assister une organisation dans la mise en œuvre, la gestion et le maintien d'un SMSI, tel que spécifié dans la norme ISO 27001
- Acquérir l'expertise nécessaire pour gérer une équipe de mise en œuvre de la norme ISO 27001
- Demander la qualification de Certified ISO/IEC 27001 Provisional Implementer, Certified ISO/IEC 27001 Implementer ou Certified ISO/IEC 27001 Lead Implementer (après avoir réussi l'examen), en fonction du niveau d'expérience

INFORMATIONS GÉNÉRALES

Code : ISO 27001 LA

Durée : 5 jours (4,5 jours de formation + l'après-midi du dernier jour dédié au passage de l'examen)

Prix : 4 290 € HT

Horaires : 9h30 - 17h30 (jours 1 à 4) & 9h30 - 12h30 (jour 5)

Lieu : Levallois (92)

Examen : inclus. Passage de l'examen l'après-midi du dernier jour de la formation. Formation certifiante.

Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Auditeurs internes
- Auditeurs cherchant à réaliser et à mener des audits des systèmes de sécurité de l'information
- Gestionnaires de projets ou consultants souhaitant maîtriser les audits des systèmes de sécurité de l'information
- CTO/CIO et managers responsables de la gestion IT d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information

PRÉ-REQUIS

- Avoir une connaissance de base de la sécurité des systèmes d'information

RESSOURCES

- Support de cours en français
- Cours donnés en français
- Copie de la norme ISO 27001

AVANCÉ

FORMATION CERTIFIANTE

ISO 27001 : CERTIFIED LEAD IMPLEMENTER

Maîtrisez la mise en œuvre et la gestion d'un système de management de la sécurité de l'information (SMSI), conforme à la norme ISO/IEC 27001

Ce cours intensif de 5 jours va permettre aux participants de développer l'expertise nécessaire pour gérer des structures liées à la gestion des systèmes de sécurité de l'information sur la norme ISO 27001. La formation permettra également aux participants d'appréhender rigoureusement les meilleures pratiques utilisées pour mettre en œuvre des contrôles de sécurité des informations liés à la norme ISO 27002. Cette formation est en accord avec les pratiques de gestion de projet établies dans la norme de ISO 10006 (Quality Management Systems – Guidelines for Quality Management in Projects).

Ce cours est également en adéquation avec les normes ISO 27003 (Guidelines for the Implementation of an ISMS), ISO 27004 (Measurement of Information Security) et ISO 27005 (Risk Management in Information Security).

Code : ISO 27001 LI

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOURS 1, 2, 3 & 4

Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par la norme ISO 27001; Initialisation d'un SMSI

- Introduction aux systèmes de management et à l'approche processus
- Présentation de la suite des normes ISO 27000, ainsi que du cadre normatif, légal et réglementaire
- Principes fondamentaux de la sécurité de l'information
- Analyse préliminaire et détermination du niveau de maturité d'un système de management de sécurité de l'information existant d'après la norme ISO 21827
- Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMSI

Planifier la mise en œuvre d'un SMSI basé sur la norme ISO 27001

- Définition du périmètre (domaine d'application) du SMSI
- Développement de la politique et des objectifs du SMSI
- Sélection de l'approche et de la méthode d'évaluation des risques
- Gestion des risques : identification, analyse et traitement du risque (d'après les dispositions de la norme ISO 27005)
- Rédaction de la Déclaration d'Applicabilité

Mettre en place un SMSI basé sur la norme ISO 27001

- Mise en place d'une structure de gestion de la documentation
- Conception et implémentation des mesures de sécurité
- Développement d'un programme de formation et de sensibilisation ; et communication à propos de la sécurité de l'information
- Gestion des incidents (d'après les dispositions de la norme ISO 27035)
- Gestion des opérations d'un SMSI

Contrôler, surveiller, mesurer et améliorer un SMSI conformément à la norme ISO 27001

- Contrôler les mesures de sécurité du SMSI
- Développement de mesures, d'indicateurs de performance et de tableaux de bord conformes à la norme ISO 27004
- Audit interne ISO 27001
- Revue du SMSI par les gestionnaires
- Mise en œuvre d'un programme d'amélioration continue
- Préparation à l'audit de certification ISO 27001

JOUR 5

L'examen «Certified ISO/IEC 27001 Lead Implementer»

- Les candidats passeront l'examen le vendredi après-midi
  - Format : examen écrit
  - Durée : 3h
  - Langue : disponible en français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program). Il couvre les domaines de compétence suivants :
  - Domaine 1 : Principes et concepts fondamentaux de sécurité de l'information
  - Domaine 2 : Code de bonnes pratiques de la sécurité de l'information basé sur la norme ISO 27002
  - Domaine 3 : Planifier un SMSI conforme à la norme ISO 27001
  - Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO 27001
  - Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI conforme à la norme ISO 27001
  - Domaine 6 : Amélioration continue d'un SMSI conforme à la norme ISO 27001
  - Domaine 7 : Préparation de l'audit de certification d'un SMSI

PROGRAMME

RÉSULTATS

Disponibles sous 4 à 8 semaines et directement envoyés par e-mail au candidat.

CERTIFICATION

- Un certificat de participation de 31 crédits CPD (Continuing Professional Development) sera délivré par PECB.
- Les personnes ayant réussi l'examen pourront demander la qualification de «Certified ISO/IEC 27001 Provisional Implementer», «Certified ISO/IEC 27001 Implementer» ou «Certified ISO/IEC 27001 Lead Implementer», en fonction de leur niveau d'expérience.
- Un certificat sera alors délivré aux participants remplissant l'ensemble des exigences à la qualification choisie.
- Pour plus d'information à ce sujet, vous pouvez consulter le site de PECB.

PROCHAINES DATES

17 février 2025
2 juin 2025
22 septembre 2025
3 novembre 2025

OBJECTIFS

- Comprendre la mise en œuvre d'un Système de Management de la Sécurité de l'Information conforme à la norme ISO 27001
- Acquérir une compréhension globale des concepts, démarches, normes, méthodes et techniques nécessaires pour gérer efficacement un Système de Management de la Sécurité de l'Information
- Acquérir l'expertise nécessaire pour assister une organisation dans la mise en œuvre, la gestion et le maintien d'un SMSI, tel que spécifié dans la norme ISO 27001
- Acquérir l'expertise nécessaire pour gérer une équipe de mise en œuvre de la norme ISO 27001
- Demander la qualification de Certified ISO/IEC 27001 Provisional Implementer, Certified ISO/IEC 27001 Implementer ou Certified ISO/IEC 27001 Lead Implementer (après avoir réussi l'examen), en fonction du niveau d'expérience

INFORMATIONS GÉNÉRALES

Code : ISO 27001 LI
Durée : 5 jours (4,5 jours de formation + passage de l'examen l'après-midi du dernier jour).
Prix : 4 290 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
Examen : inclus. Passage de l'examen le vendredi après-midi. Formation certifiante.
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Les gestionnaires de projets ou les consultants voulant préparer et gérer la mise en œuvre d'une structure, ainsi que la gestion des systèmes de sécurité de l'information
- Les auditeurs ISO 27001 qui souhaitent pleinement comprendre les systèmes de sécurité de l'information et leur fonctionnement
- Les CTO/CIO et les managers responsables de la gestion IT d'une entreprise ainsi que la gestion des risques
- Les membres d'une équipe de sécurité de l'information
- Les conseillers experts en technologie de l'information
- Les experts techniques voulant se préparer pour un poste en sécurité de l'information ou pour la gestion d'un projet lié à la sécurité de l'information

PRÉ-REQUIS

- Avoir une connaissance de base de la sécurité des systèmes d'information

RESSOURCES

- Support de cours en français
- Cours donnés en français
- Copie de la norme ISO 27001

AVANCÉ

FORMATION CERTIFIANTE

ISO 27002 : CERTIFIED FOUNDATION

Appréhendez les bonnes pratiques relatives aux mesures de sécurité de l'information conforme à la norme ISO/CEI 27002

La formation ISO/IEC 27002 Foundation permet aux participants d'apprendre les concepts de base de la mise en œuvre et de la gestion des mesures de sécurité de l'information conformément aux directives de la norme ISO/IEC 27002. Grâce à cette formation, les participants seront capables d'identifier les mesures de sécurité de l'information de la norme ISO/IEC 27002, lesquelles sont regroupées sous quatre thèmes : mesures de sécurité organisationnelles, applicables aux personnes, physiques et technologiques.

La formation fournit également des informations sur la façon dont la norme ISO/IEC 27002 est en corrélation avec d'autres normes telles que les normes ISO/IEC 27001 et ISO/IEC 27003.

Code : ISO 27002 F

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOUR 1

Introduction à la norme ISO/IEC et aux mesures de sécurité organisationnelles

- Présentation de la norme ISO/IEC 27002 et des corrélations avec d'autres normes ISO

JOUR 2

Mesure de sécurité applicables aux personnes physiques et technologiques. Examen de certification

- Mise en œuvre des mesures pour la sécurité de l'information conformément à la norme ISO 27002 (approches, méthodes et techniques)

CERTIFICATION

Examen

- Format : examen écrit
  - Durée : 1 heure
  - Langue : français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 14 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

30 janvier 2025
28 avril 2025
28 août 2025
20 novembre 2025

OBJECTIFS

- Expliquer les concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée basés sur la norme ISO/IEC 27002
- Discuter de la corrélation entre les normes ISO/IEC 27001 et ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Interpréter les mesures de sécurité organisationnelles, applicables aux personnes, physiques et technologiques de la norme ISO/IEC 27002 dans le contexte spécifique d'un organisme

INFORMATIONS GÉNÉRALES

Code : ISO 27002 F

Durée : 2 jours

Prix : 1 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Managers et consultants souhaitant en savoir plus sur les mesures de sécurité de l'information de la norme ISO/IEC 27002
- Professionnels impliqués ou responsables dans le domaine de gestion de la sécurité de l'information
- Personnes souhaitant acquérir des connaissances sur les principaux processus d'un système de management de la sécurité de l'information et sur les mesures de sécurité de l'information
- Personnes souhaitant poursuivre une carrière dans le domaine de la sécurité de l'information

PRÉ-REQUIS

Aucun prérequis n'est nécessaire pour participer à cette formation

RESSOURCES

- Support de cours en français contenant plus de 200 pages d'informations et d'exemples pratiques.
- Cours donnés en français

AVANCÉ

FORMATION CERTIFIANTE

ISO 27002 : CERTIFIED LEAD MANAGER

Maîtrisez la mise en œuvre et la gestion des mesures de sécurité de l'information conforme à la norme ISO/CEI 27002

Code : ISO 27002 LM

La formation ISO/CEI 27002 Lead Manager vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/CEI 27002.

Durant cette formation, vous acquerrez des connaissances approfondies sur les meilleures pratiques en matière de mesures de sécurité de l'information et vous serez apte à améliorer la sécurité de l'information dans une organisation.

Après avoir maîtrisé l'ensemble des concepts relatifs aux mesures de sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27002 Lead Manager ». En étant titulaire d'une certification de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour soutenir et diriger une équipe dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/CEI 27002.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOUR 1

Introduction aux mesures de sécurité de l'information conforme à la norme ISO/CEI 27002

- Objectifs et structure de la formation
- Cadres normatifs et réglementaires
- Principes fondamentaux de la sécurité de l'information
- Système de management de la sécurité de l'information
- Politiques de sécurité de l'information
- Management de la sécurité de l'information

JOUR 2

Exigences et objectifs de la sécurité de l'information conforme à la norme ISO/IEC 27002

- Sécurité des ressources humaines
- Gestion des actifs
- Contrôle d'accès

JOUR 3

Surveille, mesurer, analyser et évaluer les mesures de la sécurité de l'information

- Cryptographie
- Sécurité physique et environnementale
- Sécurité liée à l'exploitation
- Sécurité des communications

JOUR 4

Amélioration continue de la performance du Système de management de la sécurité de l'information de l'organisation

- Acquisition, développement et maintenance des systèmes d'information
- Relations avec les fournisseurs
- Gestion des incidents liés à la sécurité de l'information
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Conformité
- Compétences et évaluation des gestionnaires
- Clôture de la formation

CERTIFICATION

Examen

- Les candidats passeront l'examen le vendredi
- Format : examen écrit
  - Durée : 3 heures
  - Langue : français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

24 mars 2025
2 juin 2025
25 août 2025
13 octobre 2025

INFORMATIONS GÉNÉRALES

Code : ISO 27002 LM
Durée : 5 jours
Prix : 3 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Examen : inclus.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

OBJECTIFS

- Maîtriser la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/CEI 27002
- Maîtriser les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion efficace des mesures de la sécurité de l'information
- Comprendre la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain
- Comprendre l'importance de la sécurité de l'information pour la stratégie de l'organisation
- Maîtriser la mise en œuvre des processus de la sécurité de l'information
- Maîtriser l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de la sécurité de l'information
- Maîtriser la formulation et la mise en œuvre des exigences et des objectifs de la sécurité de l'information

PUBLIC VISÉ

- Responsables ou consultants désirant mettre en œuvre un Système de management de la sécurité de l'information (SMSI) conforme aux normes 27001 et ISO/CEI 27002
- Chefs des projets ou consultants souhaitant maîtriser les processus de mise en œuvre du Système de management de la sécurité de l'information
- Toute personne responsable de la sécurité de l'information, de la conformité, du risque et de la gouvernance dans une organisation
- Membres de l'équipe de la sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Agents de la sécurité de l'information
- Gestionnaires de la sécurité de l'information
- Agents de la protection des données personnelles
- Professionnels des TI
- Directeurs de la technologie, directeurs des systèmes d'information (DSI) et aux responsables de la sécurité des systèmes d'information

PRÉ-REQUIS

- Être impliqué(e) dans la sécurité des systèmes d'information
- Connaitre les principes fondamentaux de la norme ISO 27001 et son application

RESSOURCES

- Support de cours en français contenant plus de 500 pages d'informations et d'exemples pratiques.
- Cours donnés en français

AVANCÉ

FORMATION CERTIFIANTE

ISO 27005 : CERTIFIED RISK MANAGER AVEC EBIOS RISK MANAGER

SecNumedu
Formation continue
ANSSI

Acquérir les connaissances sur la gestion des risques en sécurité de l'information (norme ISO 27005 Risk Manager)

... et développer les compétences nécessaires pour réaliser une analyse de risque avec la méthode EBIOS Risk Manager

Ce cours intensif de cinq jours permet aux participants de développer les compétences pour la maîtrise des éléments de base de la gestion des risques pour tous les actifs pertinents de la sécurité de l´information en utilisant la norme ISO/IEC 27005 Risk Manager comme cadre de référence et la méthode EBIOS Risk Manager. La méthode EBIOS Risk Manager (expression des besoins et identification des objectifs de sécurité) a été développée par l'ANSSI en France.
À partir d'exercices pratiques et d'études de cas, les participants pourront acquérir les aptitudes et compétences nécessaires pour réaliser une évaluation optimale du risque de la sécurité de l'information et de gérer le risque dans le temps en étant familier à leur cycle de vie. Cette formation s'inscrit parfaitement dans le cadre d'un processus de mise en œuvre de la norme ISO/IEC 27001.

Ce cours est certifié par l'ANSSI : SecNumedu

Code : ISO 27005 + EBIOS

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOURS 1 & 2

Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005 RISK MANAGER

- Objectifs et structure de la formation
- Concepts et définitions du risque
- Cadres normatifs et réglementaires
- Mise en œuvre d'un programme de gestion des risques
- Compréhension de l'organisation et de son contexte

Mise en œuvre d'un processus de gestion des risques conforme à la norme ISO/CEI 27005 RISK MANAGER

- Identification des risques
- Analyse et évaluation des risques
- Appréciation du risque avec une méthode quantitative
- Traitement des risques
- Acceptation des risques et gestion des risques résiduels
- Communication et concertation relatives aux risques en sécurité de l'information
- Surveillance et revue du risque

JOURS 3 & 4

Introduction à la méthode d'appréciation des risques EBIOS RISK MANAGER

Réalisation de l'appréciation des risques selon la méthode EBIOS RISK MANAGER

JOUR 5

L'examen PECB Certified EBIOS Risk Manager

- Les candidats passeront cet examen le vendredi matin
  - Format : examen écrit
  - Durée : 3h
  - Langue : disponible en français

L'examen PECB Certified ISO/CEI 27005 Risk Manager

- Les candidats passeront cet examen le vendredi après-midi
  - Format : examen écrit
  - Durée : 2h
  - Langue : disponible en français

RÉSULTATS

Disponibles sous 4 à 8 semaines et directement envoyés par e-mail au candidat.

CERTIFICATION

- Deux certificats de participation de 21 crédits CPD (Continuing Professional Development) seront délivrés par PECB (le premier pour la partie ISO 27005 et le second pour la partie EBIOS)
- Les personnes ayant réussi l'examen Certified ISO /IEC 27005 Risk Manager pourront demander la qualification de «ISO/IEC 27005 Provisional Risk Manager», «ISO/IEC 27005 Risk Manager» ou «ISO/IEC 27005 Lead Risk Manager», en fonction de leur niveau d'expérience
- Un certificat sera alors délivré aux participants remplissant l'ensemble des exigences relatives à la qualification choisie
- Les personnes ayant réussi l'examen EBIOS Avancé pourront demander la qualification de «EBIOS Provisional Risk Manager» ou «EBIOS Lead Risk Manager», en fonction de leur niveau d'expérience.
  Un certificat sera alors délivré aux participants remplissant l'ensemble des exigences relatives à la qualification choisie.
  Pour plus d'informations, vous pouvez consulter le site de PECB.

PROCHAINES DATES

3 février 2025
12 mai 2025
8 septembre 2025
17 novembre 2025

OBJECTIFS

- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005 Risk Manager
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques
- Maîtriser les étapes pour conduire une analyse de risque avec la méthode EBIOS Risk Manager
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme

INFORMATIONS GÉNÉRALES

Code : ISO 27005 + EBIOS

Durée : 5 jours (4 jours de formation + le dernier jour dédié au passage des examens)

Prix : 4 290 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92)

Examen : inclus. Passage des examens ISO et EBIOS le dernier jour de la formation. Formation certifiante.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Gestionnaires de risques
- Responsables de la sécurité de l'information ou de la conformité au sein d'une organisation
- Membres d'une équipe de sécurité de l'information
- Consultants en technologie de l´information
- Personnel de la mise en œuvre de la norme ISO 27001 ou cherchant à s'y conformer, ou participant à un programme de gestion du risque basé sur la méthode EBIOS Risk Manager

PRÉ-REQUIS

- Avoir une connaissance de base sur la gestion du risque

RESSOURCES

- Support de cours en français
- Cours donnés en français
- Copie de la norme ISO 27001

AVANCÉ

FORMATION CERTIFIANTE

ISO 27032 : CERTIFIED LEAD CYBERSECURITY MANAGER

Maîtrisez la capacité à mettre en œuvre et à gérer un programme de cybersécurité basé sur les bonnes pratiques du secteur

Code : ISO 27032 LSM

De nos jours, les organismes sont affectés par l'évolution constante du paysage numérique et sont constamment confrontés à de nouvelles menaces et à des cyberattaques de plus en plus complexes et perfectionnées. Le besoin en personnel qualifié capable de gérer et de mettre en œuvre efficacement des programmes de cybersécurité robustes pour contrer ces menaces est pressant.

La formation «Lead Cybersecurity Manager» que nous proposons a été conçue pour répondre à ce besoin.

Les participants à la formation PECB Certified Lead Cybersecurity Manager acquièrent les concepts, stratégies, méthodologies et techniques fondamentaux de la cybersécurité utilisés pour établir et gérer efficacement un programme de cybersécurité basé sur les directives des normes internationales de cybersécurité, tels que la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOUR 1

Introduction à la cybersécurité & lancement de la mise en œuvre de programme de cybersécurité

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Concepts fondamentaux de la cybersécurité
- Programme de cybersécurité
- L'organisme et son contexte
- Gouvernance de la cybersécurité

JOUR 2

Rôles et responsabilités en matière de cybersécurité, gestion des risques et mécanismes d'attaque

- Rôles et responsabilités en matière de cybersécurité
- Gestion de biens
- Gestion des risques
- Les mécanismes d'attaque

JOUR 3

Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité

- Mesures de cybersécurité
- Communication relative à la cybersécurité
- Sensibilisation et formation

JOUR 4

Management des incidents de cybersécurité, surveillance et amélioration continue

- État de préparation des TIC pour la continuité d'activité
- Management des incidents de cybersécurité
- Test de cybersécurité
- Mesurer et rendre compte des performances et des paramètres en matière de cybersécurité
- Amélioration continue
- Clôture de la formation

JOUR 5

Examen

- Les candidats passeront l'examen le vendredi
- Format : examen écrit
  - Durée : 3 heures
  - Langue : français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

10 février 2025
7 avril 2025
1er septembre 2025
3 novembre 2025

OBJECTIFS

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en œuvre et gérer un programme de cybersécurité
- Expliquer la corrélation entre la norme ISO/IEC 27032, le cadre de cybersécurité du NIST ainsi que d'autres normes et cadres pertinents
- Comprendre le fonctionnement d'un programme de cybersécurité et ses composantes
- Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de son programme de cybersécurité

INFORMATIONS GÉNÉRALES

Code : ISO 27032 LCM

Durée : 5 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou distanciel

Examen : inclus.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Responsables et dirigeants impliqués dans la gestion de la cybersécurité
- Personnes chargées de la mise en œuvre pratique des stratégies et des mesures de cybersécurité
- Professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité
- Professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes
- Cadres dirigeants qui ont un rôle crucial dans les processus de prise de décision liés à la cybersécurité

PRÉ-REQUIS

- Avoir une expérience dans le domaine de la sécurité de l'information est fortement recommandée.

Il est conseillé, mais pas obligatoire, d'avoir suivi une formation de base en sécurité informatique ou en cyber sécurité, de type ISO 27001 ou ISO 27002 Fondation (le processus de la gestion de la sécurité, du livre conception de services, s'appuie sur ISO 27001).

RESSOURCES

- Support de cours en français comprenant plus de 400 pages de contenu, y compris des exemples pratiques, des exercices et des quiz.
- Cours donnés en français

AVANCÉ

FORMATION CERTIFIANTE

ISO 27701 : CERTIFIED LEAD IMPLEMENTER

Maîtrisez la mise en œuvre et le management du système de la protection de la vie privée (PIMS) selon la norme ISO/IEC 27701

Code : ISO 27701 LI

Cette formation est conçue pour préparer ses participants à mettre en œuvre un système de management de la protection de la vie privée (PIMS*) en conformité avec les exigences et les lignes directrices de la norme ISO/IEC 27701. Vous acquerrez également une connaissance approfondie des meilleures pratiques en matière de gestion des informations relatives à la protection de la vie privée et apprendrez à gérer et à traiter les données tout en respectant les différents régimes de protection de la vie privée.

Après avoir maîtrisé la mise en œuvre et le management d'un système de management de la protection de la vie privée (PIMS*), vous pouvez vous présenter à l'examen et demander la certification «PECB Certified ISO/IEC 27701 Lead Implementer». Le certificat PECB Lead Implementer, reconnu au niveau international, prouve que vous avez les connaissances pratiques et les capacités professionnelles pour mettre en œuvre les exigences de la norme ISO/IEC 27701 dans un organisme.

(*) PIMS : Privacy Information Management System

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOUR 1

Introduction à l'ISO/IEC 27701 et initiation au PIMS

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Système de management de la protection de la vie privée (PIMS)
- Concepts et principes fondamentaux de la sécurité de l'information et de la protection de la vie privée
- Démarrage de la mise en œuvre du PIMS
- Analyse du domaine d'application du SMSI et de la déclaration d'applicabilité

JOUR 2

Planification de la mise en œuvre d'un PIMS

- Appréciation de l'impact sur la vie privée
- Déclaration d'applicabilité du PIMS
- Gestion de la documentation
- Sélection des mesures
- Mise en œuvre des mesures

JOUR 3

Mise en œuvre d'un PIMS

- Mise en œuvre des mesures (suite)
- Mise en œuvre des mesures spécifiques aux contrôleurs IPI
- Mise en œuvre des mesures spécifiques aux processeurs IPI

JOUR 4

Suivi, amélioration continue et préparation de l'audit de certification du PIMS

- Sensibilisation, formation et communication
- Surveillance, mesure, analyse, évaluation et revue de direction
- Audit interne
- Traitement des non-conformités
- Amélioration continue
- Préparation de l'audit de certification
- Processus de certification et clôture de la formation

CERTIFICATION

Examen

- Les candidats passeront l'examen le vendredi
- Format : examen écrit
  - Durée : 3 heures
  - Langue : français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

17 mars 2025
23 juin 2025
1er septembre 2025
27 octobre 2025

OBJECTIFS

- Expliquer les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS
- Comprendre la corrélation entre les normes ISO/IEC 27701, ISO/IEC 27001 ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le fonctionnement d'un PIMS basé sur la norme ISO/IEC 27701 et ses principaux processus.
- Apprendre à interpréter et à mettre en œuvre les exigences de la norme ISO/IEC 27701 dans le contexte spécifique d'un organisme
- Développer l'expertise nécessaire pour aider un organisme à planifier, mettre en œuvre, gérer, contrôler et maintenir efficacement un PIMS

INFORMATIONS GÉNÉRALES

Code : ISO 27701 LI

Durée : 5 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou distanciel

Examen : inclus.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Responsables et consultants impliqués dans la gestion de la vie privée et des données
- Conseillers experts cherchant à maîtriser la mise en place d'un système de management de la protection de la vie privée
- Personnes responsables des données à caractère personnel (DCP) au sein des organismes
- Personnes chargées de veiller au respect des exigences des régimes de protection de la vie privée
- Membres de l'équipe PIMS

PRÉ-REQUIS

- Avoir une compréhension fondamentale de la sécurité de l'information
- Avoir une connaissance approfondie des principes de mise en œuvre du SMSI

RESSOURCES

- Support de cours en français comprenant des exemples pratiques
- Cours donné en français

AVANCÉ

FORMATION CERTIFIANTE

ISO 31000 : RISK MANAGER

Maîtrisez les meilleurs pratiques en matière de management du risque

Code : ISO 31000

La formation ISO 31000 : Risk Manager fournit une connaissance approfondie des principes fondamentaux, du cadre et des processus de la gestion des risques conforme à l'ISO 31000.

Ce cours est basé à la fois sur la théorie et sur les meilleures pratiques en matière de gestion des risques. Les exercices pratiques sont basés sur une étude de cas qui comprend des jeux de rôle et des présentations orales. Les tests pratiques sont similaires à l'examen de certification.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 3ème jour.

JOUR 1

Introduction aux principes et au cadre organisationnel de la norme ISO 31000

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Introduction aux principes et aux concepts de la norme ISO 31000
- Principe, cadre et processus de la norme ISO 31000
- Établissement du cadre et définition de la gouvernance

JOUR 2

Mise en place du processus de management du risque et appréciation du risque selon la norme ISO 31000

- Périmètre, contexte et critères du risque
- Identification du risque
- Analyse du risque
- Évaluation du risque

JOUR 3

Enregistrement et rapports, suivi et revue, communication et consultation selon la norme ISO 31000

- Traitement du risque
- Enregistrement et élaboration de rapports
- Suivi et revue
- Communication et consultant
- Clôture de la formation

Examen de certification « PECB certified 31000 Risk Manager »

Les candidats passeront cet examen l'après-midi du dernier jour de la formation

- Format : examen écrit
  - Durée : 2h
  - Langue : disponible en français
- Une Attestation d'achèvement de formation de 21 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation.
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

28 avril 2025
9 juillet 2025
3 septembre 2025
12 novembre 2025

OBJECTIFS

- Maîtriser les meilleures pratiques en matière de management du risque
- Savoir mettre en œuvre un processus de management du risque
- Établir, maintenir et améliorer en continu un cadre de management du risque
- Appliquer le processus de gestion des risques conformément aux lignes directrices de la norme ISO 31000
- Se préparer au passage de l'examen «Certified 31000 Risk Manager»

INFORMATIONS GÉNÉRALES

Code : ISO 31000

Durée : 3 jours (2,5 jours de formation & la dernière après-midi dédiée au passage de l'examen)

Prix : 3 100 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92)

Examen : inclus. Passage de l'examen la dernière après-midi de la formation. Formation certifiante.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Responsables ou consultants chargés de la gestion des risques au sein d'une organisation
- Toute personne souhaitant acquérir une connaissance approfondie des concepts, processus et principes de la gestion de risques
- Consultants impliqués dans la gestion des risques

PRÉ-REQUIS

- Avoir 2 ans d'expérience professionnelle dont 1 année en gestion des risques
- Totaliser 200 heures dans une activité de gestion de risques

RESSOURCES

- Support de cours en français
- Cours donnés en français
- Copie de la norme ISO 31000

AVANCÉ

FORMATION CERTIFIANTE

NIS2 : CERTIFIED NIS 2 DIRECTIVE LEAD IMPLEMENTER

Maîtrisez la mise en œuvre et la gestion d'un programme de cybersécurité basé sur la Directive NIS 2

Code : NIS2 LI

L'importance des mesures de cybersécurité robustes ne peut être surestimée, car les organismes sont de plus en plus confrontés à tous les types de cyberattaques. La directive NIS 2 est une législation conçue pour renforcer la posture de cybersécurité des secteurs d'infrastructures critiques.

En participant à la formation NIS 2 Directive Lead Implementer, vous acquérez une connaissance approfondie des exigences de la directive, des stratégies de mise en œuvre et des bonnes pratiques qui protègent les infrastructures critiques contre les cybermenaces. Grâce à des sessions interactives et des exercices pratiques, vous apprendrez à évaluer les risques de cybersécurité de l'organisme, à élaborer des plans robustes de réponse aux incidents et à mettre en œuvre des mesures de sécurité efficaces pour répondre aux exigences de la directive NIS 2. De plus, vous obtiendrez des informations sur les normes et les bonnes pratiques de l'industrie qui vous permettront de rester au courant de l'évolution du paysage des menaces et de mettre en œuvre des solutions de cybersécurité de pointe.

Après avoir terminé avec succès cette formation, vous posséderez l'expertise nécessaire pour naviguer dans le paysage complexe des infrastructures critiques de cybersécurité et contribuerez à la résilience de votre organisme et de la société dans son ensemble.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5ème jour.

JOUR 1

Introduction à la Directive NIS 2 et initiation à sa mise en œuvre

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Directive NIS 2
- Exigences de la directive NIS 2
- Initiation de la mise ne œuvre de la Directive NIS 2
- L'organisme et son contexte

JOUR 2

Analyse du programme de conformité à la Directive NIS 2, de la gestion des actifs et de la gestion des risques

- Gouvernance de la cybersécurité
- Rôles et responsabilités de cybersécurité
- Gestion des actifs
- Gestion des risques
- Mise en œuvre des mesures spécifiques aux processeurs IPI

JOUR 3

Contrôles de cybersécurité, gestion des incidents et gestion des crises

- Contrôles de cybersécurité
- Sécurité de la chaîne d'approvisionnement
- Gestion des incidents
- Gestion des crises

JOUR 4

Communication, tests, surveillance et amélioration continue de la cybersécurité

- Continuité d'activité
- Sensibilisation et formation
- Communication
- Tests en cybersécurité
- Audit interne
- Mesurer, surveiller et rendre compte des performances et des indicateurs
- Amélioration continue
- Clôture de la formation

CERTIFICATION

Examen

- Les candidats passeront l'examen le vendredi
- Format : examen écrit
  - Durée : 3 heures
  - Langue : français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

PROCHAINES DATES

3 février 2025
14 avril 2025
7 juillet 2025
6 octobre 2025

OBJECTIFS

- Expliquer les concepts fondamentaux de la directive NIS 2 et ses exigences
- Apprendre à interpréter et à mettre en œuvre les exigences de la directive NIS 2 dans le contexte spécifique d'un organisme.
- Initier et planifier la mise en œuvre des exigences de la directive NIS 2, en utilisant la méthodologie de PECB et d'autres bonnes pratiques.
- Acquérir les connaissances nécessaires pour soutenir un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de cybersécurité conformément à la directive NIS 2.
- Acquérir une compréhension approfondie des principes, stratégies, méthodologies et outils nécessaires à la mise en œuvre et à la gestion efficace d'un programme de cybersécurité conformément à la directive NIS 2.

INFORMATIONS GÉNÉRALES

Code : NIS2 LI

Durée : 5 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Formation certifiante.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

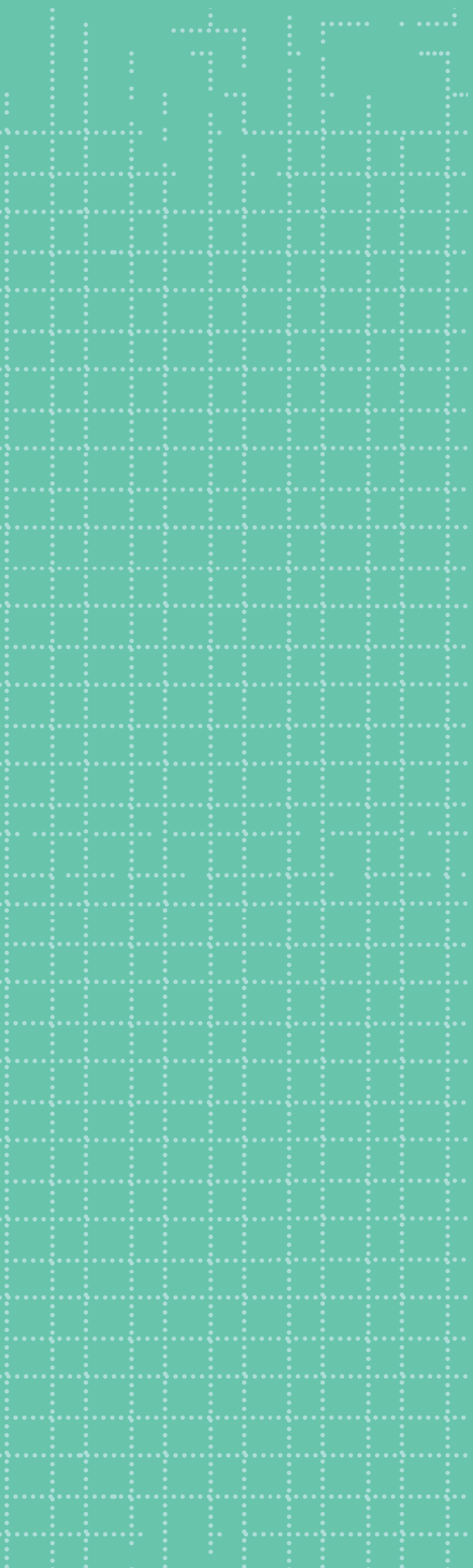
- Professionnel de la cybersécurité cherchant à acquérir une compréhension approfondie des exigences de la directive NIS 2 et à apprendre des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes.
- Responsables informatiques et professionnels souhaitant acquérir des connaissances sur la mise en œuvre de systèmes sécurisés et améliorer la résilience des systèmes critiques.
- Responsables gouvernementaux et réglementaires chargés de faire appliquer la directive NIS 2

PRÉ-REQUIS

- Avoir une compréhension fondamentale de la cybersécurité
- Bénéficier d'une bonne vue d'ensemble des normes législatives et de leur application dans un contexte IT

RESSOURCES

- Support de cours en français contenant plus de 400 pages d'informations explicatives, d'exemples, de bonnes pratiques, d'exercices et de quiz
- Cours donné en français



SENSIBILISATION CYBERSÉCURITÉ

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
CASSI	**Conseils relatifs à l'Administration Sécurisée des Systèmes d'Information**	1 jour			21				11			17		12
NIS2	**Sensibilisation à la Directive NIS2**	1 jour			3			13				10		5
SAC	**Sensibilisation à la Cybersécurité**	1 jour		17				13			5		14	
SDORA	**Sensibilisation au Règlement DORA**	1 jour		14			23				26		28	

CONSEILS RELATIFS À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION

Découvrez les 71 recommandations de l'ANSSI

Pendant cette formation, nous aborderons les principes essentiels de l'administration sécurisée des systèmes, en mettant l'accent sur les méthodes et les outils nécessaires pour identifier, évaluer et atténuer les risques de sécurité.

Code : CASSI

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (20% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

CHAPITRE 1 : Introduction
- Objectif d'apprentissage de la journée
- Aperçu du contenu du cours

CHAPITRE 2 : Les administrateurs, acteurs clés de la sécurité du système d'information
- Rôle et responsabilités des administrateurs
- Intégration des administrateurs dans l'écosystème du SI de l'entité

CHAPITRE 3 : Généralités sur le système d'information d'administration
- Analyse de risque et objectifs de sécurité
- Zones de confiance et zones d'administration
- Produits qualifiés par l'ANSSI
- Confiance dans le cloisonnement des environnements virtualisés

CHAPITRE 4 : Poste d'administration
- Maîtrise du poste d'administration
- Mesures de sécurisation du poste d'administration

CHAPITRE 5 : Identification, authentification et droits d'administration
- Processus d'identification
- Méthodes d'authentification
- Attribution et gestion des droits d'administration

CHAPITRE 6 : Connectivité sécurisée et travail à distance
- Maintien en condition de sécurité
- Sauvegarde, journalisation et supervision de la sécurité
- Administration à distance et nomadisme
- Systèmes d'échanges sécurisés
- Administration par des tiers et assistance à distance
- Cas particuliers d'architectures de SI d'administration

PROCHAINES DATES

21 mars 2025
11 juillet 2025
17 octobre 2025
12 décembre 2025

OBJECTIFS

- Énoncer les principes de base de l'administration sécurisée d'un système d'information.
- Maintenir un système d'information en condition opérationnelle tout en garantissant sa sécurité.
- Acquérir des connaissances sur la gestion des changements mineurs et des évolutions majeures dans un environnement informatique.
- Examiner les objectifs de sécurité et les principes fondamentaux pour élaborer une architecture technique sécurisée d'administration.
- Explorer des cas d'usage concrets pour illustrer les concepts discutés.
- Adapter les recommandations de sécurité présentées à son propre contexte et à ses propres besoins.
- Intégrer les recommandations de sécurité dans la politique de sécurité du système d'information de son organisation.
- Mettre en pratique les connaissances acquises pour améliorer la sécurité de son propre environnement informatique.

INFORMATIONS GÉNÉRALES

Code : CASSI

Durée : 1 jour

Prix : 1 090 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI / DSI
- CTO
- Le public visé par cette formation inclut les professionnels de l'informatique et de la cybersécurité, tels que les administrateurs système et réseau, les responsables de la sécurité des systèmes d'information, ainsi que toute personne impliquée dans la gestion et la sécurisation des systèmes d'information au sein d'une organisation.

PRÉ-REQUIS

- Avoir des connaissances de base en informatique, en administration de systèmes, et une compréhension des principes fondamentaux de la sécurité des systèmes d'information.

RESSOURCES

- Support de cours
- 1 PC par personne

SENSIBILISATION À LA DIRECTIVE NIS2

Découvrez la Directive NIS2

Code : NIS2S

Pour renforcer la cybersécurité dans toute l'Europe, le Parlement européen a voté pour adopter la directive révisée sur les réseaux et les systèmes d'information 2022/0383, plus connue sous le nom de «NIS2».
NIS2 vise à étendre, renforcer et harmoniser la mise en œuvre du cadre de cybersécurité existant de l'UE. Elle constitue un élément important de la stratégie de cybersécurité de l'UE et s'inscrit dans la priorité de la Commission européenne de préparer l'Europe à l'ère numérique.

Cette formation a pour objectif de sensibiliser les stagiaires aux mesures spécifiques de cybersécurité à mettre en œuvre dans le cadre de la Directive NIS2.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques), ainsi que par la grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction à la Directive NIS2

- Présentation de la Directive NIS2, son importance et son contexte
- Les objectifs de la journée de sensibilisation et l'ordre du jour

Compréhension des Principes Fondamentaux de la Directive NIS2

- Les domaines clés de la Directive NIS2 : identification des actifs, gestion des risques, sécurité des systèmes d'information
- Responsabilités et rôles dans la conformité à la Directive NIS2

Mise en Pratique de la Directive NIS2

- Étude de cas : Identification des actifs et évaluation des risques
- Exercices interactifs sur la sécurité des systèmes d'information

Bonnes Pratiques et Conformité à la Directive NIS2

- Bonnes pratiques pour la conformité à la Directive NIS2
- Questions et réponses, discussion ouverte

Clôture de la Journée de Sensibilisation à la Directive NIS2

- Récapitulatif des points clés de la journée
- Remise de documents de sensibilisation et certificats de participation

PROCHAINES DATES

3 mars 2025
13 juin 2025
10 octobre 2025
5 décembre 2025

OBJECTIFS

- Découvrir La Directive NIS2, son importance et son contexte
- Comprendre les principes fondamentaux de la Directive NIS2

INFORMATIONS GÉNÉRALES

Code : NIS2S
Durée : 1 jour
Prix : 1 090 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI / DSI
- CTO
- DPO / Juriste
- Toute personne souhaitant découvrir la Directive NIS2

PRÉ-REQUIS

- Aucun prérequis n'est nécessaire

RESSOURCES

- Support de cours
- Étude de cas
- Documents de sensibilisation
- 1 PC par personne

SENSIBILISATION À LA CYBERSÉCURITÉ

Comprendre pour appréhender au mieux les menaces informatiques

Code : SAC

Cette formation vise à sensibiliser les stagiaires aux menaces informatiques. L'aspect organisationnel lié à la sécurité informatique au sein de l'entreprise sera tout d'abord évoqué.

Une présentation des différentes attaques, ainsi que des cas pratiques seront réalisés, et cela dans l'objectif de démontrer techniquement la faisabilité des attaques.

Enfin, un ensemble de bonnes pratiques de sécurité sera présenté.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques afin de favoriser l'acquisition des savoirs du programme.

Modalités d'évaluation : les objectifs sont évalués durant chaque module sous forme de questions/réponses.

Introduction à la sécurité informatique

- Acteurs au sein de l'entreprise
- Système d'information (SI)
- Sécurité des systèmes d'information (SSI)
- Objectifs de la sécurité informatique
- Vulnérabilités et attaques informatiques
- Risques et enjeux pour l'entreprise
- Motivations d'une attaque

Le cadre législatif

- Politique de sécurité
- Charte informatique
- Protection des données personnelles
- RGPD
- LPM

Les attaques locales

- Ports USB
- Ports d'extension haute vitesse (DMA)
- Câble Ethernet
- Disque dur interne

Les attaques distantes

- Interception sur le réseau
- Téléchargement
- Réseau sans-fil
- Système non à jour

L'ingénierie sociale

- Le phishing
- Les cibles
- Les catégories
- Les méthodologies

Les mots de passe

- Rôle et usage
- Importance de la complexité
- Attaque par recherche exhaustive
- Intérêt de la double authentification
- Utilité du stockage sécurisé
- Problème lié à la réutilisation de mots de passe

Les protections et bons réflexes

- Chiffrement du disque
- Verrouillage du poste
- Mises à jour
- Antivirus et pare-feu
- Connexion sur un réseau inconnu
- Détection et remontée d'alertes

PROCHAINES DATES

17 février 2025
13 juin 2025
5 septembre 2025
14 novembre 2025

OBJECTIFS

- Découvrir et assimiler la sécurité informatique
- Appréhender et comprendre les attaques informatiques
- Identifier les menaces informatiques
- Adopter les bonnes pratiques pour se prémunir des menaces informatiques

INFORMATIONS GÉNÉRALES

Code : SAC
Durée : 1 jour
Prix : 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Toute personne désirant comprendre les menaces liées aux attaques informatiques

PRÉ-REQUIS

- Accessible à tous

RESSOURCES

- Support de cours
- Cas pratiques

SENSIBILISATION AU RÈGLEMENT DORA

Découvrez les 17 exigences du Règlement DORA

Code : SDORA

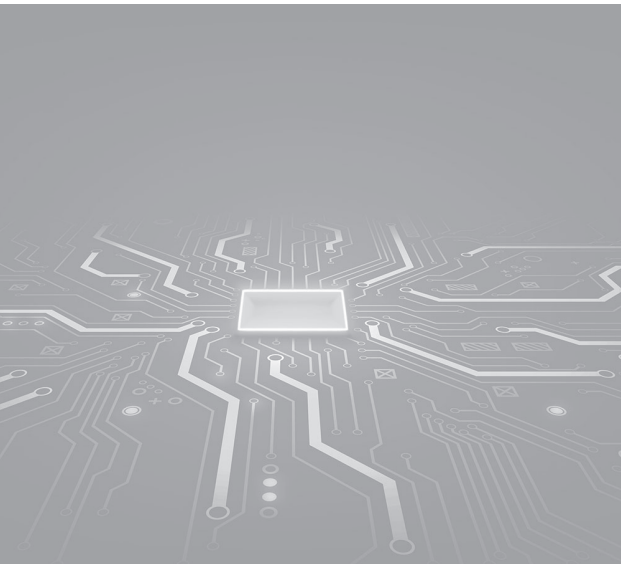
Le Règlement DORA (n°2022/2554), ou Digital Operational Resilience Act(*), est un texte législatif majeur de l'Union Européenne sur la cybersécurité des entités financières, comme les banques ou les établissements de crédit.
Cette journée de sensibilisation permet une mise en lumière du Règlement via la checklist des 17 exigences de DORA.
Il sera évoqué aussi la possibilité de mise en œuvre du Règlement avec des mesures techniques, organisationnelles et physiques.

(*) En français : DORA = Règlement sur la résilience opérationnelle du numérique.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont évalués lors d'un QCM final et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.



JOUR 1

Chapitre 1 - Cadre légal français de la résilience

- Cadre réglementaire
- Différences et points communs entre DORA et NIS2
- Quizz express
- Autorités de contrôle
- Sanctions prévues par DORA
- Vrai/faux DORA

Chapitre 2 - Gouvernance de conformité

- Cadre de gouvernance
- Rôle et missions de l'instance dirigeante dans DORA
- Atelier de brainstorming
- Cadre de gestion du risque lié aux TIC
- Travaux de groupe – Fonctions/processus

Chapitre 3 – Gestion du risque lié aux TIC

- Cartographier les risques liés aux TIC
- Travaux de groupe – Analyse de risques
- Évaluation des prestataires tiers liés aux TIC
- Exercices pratiques – Clauses contractuelles
- Cadre de supervision des prestataires tiers critiques de services TIC

Chapitre 4 – Gestion des incidents

- Procédure de gestion des incidents
- Cas pratiques – Simulation d'une situation de crise
- Tests de résilience
- Synthèse de l'ensemble des travaux individuels et en groupe
- Conclusion : Q&A

QCM final pour évaluer l'acquisition des savoirs du Règlement DORA

PROCHAINES DATES

14 février 2025
23 mai 2025
26 septembre 2025
28 novembre 2025

OBJECTIFS

- Découvrir le Règlement DORA au travers de ses 17 exigences.

INFORMATIONS GÉNÉRALES

Code : SDORA
Durée : 1 jour
Prix : 1 090 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI/DSI
- CTO
- DPO/Juriste
- Toute personne au sein d'institutions financières souhaitant découvrir le Règlement DORA

PRÉ-REQUIS

- Avoir des connaissances de l'environnement ou du contexte des entités financières, et/ou être un professionnel des Technologies de l'Information et de la Communication (TIC)

RESSOURCES

- Support de cours
- QCM final
- 1 PC par personne

OSINT

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
OSINT	Open Source Intelligence (OSINT)	3 jours			26			25				22		3

OPEN SOURCE INTELLIGENCE (OSINT)

Apprenez les fondamentaux de l'enquête en sources ouvertes

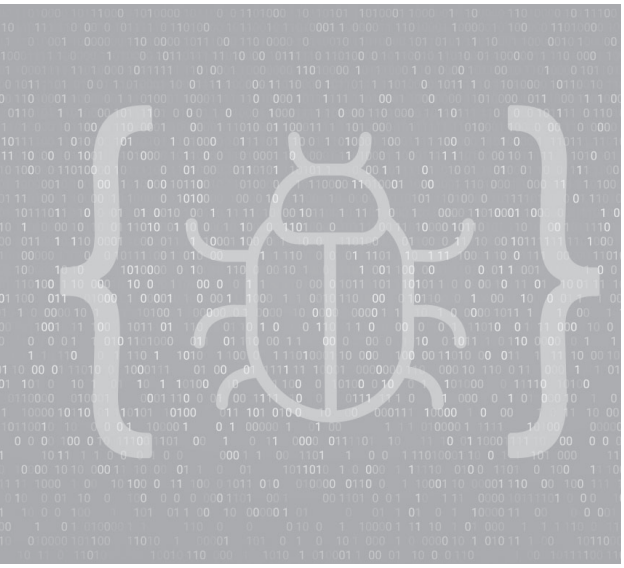
Code : OSINT

La formation Open Source Intelligence (OSINT) vous initie aux pratiques et aux méthodologies de collecte et d'analyse de données en ligne. Elle vous fournira les compétences techniques de base pour mener des enquêtes et évaluer les menaces en utilisant des sources d'information ouvertes. Que vous soyez novice ou professionnel de la sécurité, cette formation vous offre une introduction essentielle à l'OSINT pour comprendre son rôle en sécurité numérique. Explorez ce domaine en pleine croissance et devenez compétent dans le domaine du renseignement ouvert. Cette formation constitue une excellente introduction pour toute personne souhaitant acquérir les connaissances de base de l'OSINT.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont évalués tout au long de la formation sous forme de questions réponses et d'études de cas, ainsi que par la grille d'évaluation des compétences complétée en fin de module par le formateur.



JOUR 1

Introduction

- Qu'est-ce que l'OSINT et son importance
- Principes éthiques et légaux de l'OSINT
- La psychologie de la recherche d'informations en ligne
- Couvrir ses opérations d'investigation
- Utilisation efficace des moteurs de recherche
- Recherche sur les médias sociaux

ÉTUDES DE CAS PRATIQUES

JOUR 2

- Suivi des adresses IP et de la géolocalisation
- Recherche d'informations sur les personnes et organisations
- Exploration des bases de données publiques
- Outils de collecte de données
- Techniques avancées de recherche (exif data, e-mails, pseudonymes...)

ÉTUDES DE CAS PRATIQUES

JOUR 3

- Cas concret - Enquête sur une Personne disparue
- Présentation d'un cas fictif de personne disparue
- Utiliser des techniques et outils d'OSINT pour collecter des informations pertinentes
- Rédaction du rapport et présentation des résultats

ÉTUDES DE CAS PRATIQUES

PROCHAINES DATES

26 mars 2025
25 juin 2025
22 octobre 2025
3 décembre 2025

OBJECTIFS

- Comprendre les fondements de l'OSINT et son importance dans le contexte de la sécurité numérique.
- Maîtriser les techniques de recherche sur le web et les médias sociaux.
- Savoir trier, valider et corréler des données en source ouverte.
- Utiliser des outils et des logiciels spécialisés pour la collecte d'informations.
- Respecter les normes éthiques et juridiques liées à l'OSINT.

INFORMATIONS GÉNÉRALES

Code : OSINT
Durée : 3 jours
Prix : 2 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- RSSI / DSI
- Ingénieurs / Techniciens
- Analyste en conformité
- Recruteurs
- Avocats
- Journalistes d'investigation
- Toute personne s'intéressant à l'OSINT

PRÉ-REQUIS

- Connaissance de base en informatique
- Compréhension des médias sociaux
- Esprit analytique
- Éthique
- Aucune expérience préalable en OSINT n'est nécessaire.

RESSOURCES

- Support de cours
- 50% d'exercices pratiques
- 1 PC par personne

CONDITIONS D'ANNULATION

« **La mention ci-après est donnée à titre informatif et ne saurait engager la responsabilité de SysDream ni constituer un engagement contractuel étant rappelé que, toute commande Sysdream est soumise à la signature du devis accompagné des Conditions Générales de Vente.**

En cas d'annulation d'une prestation :

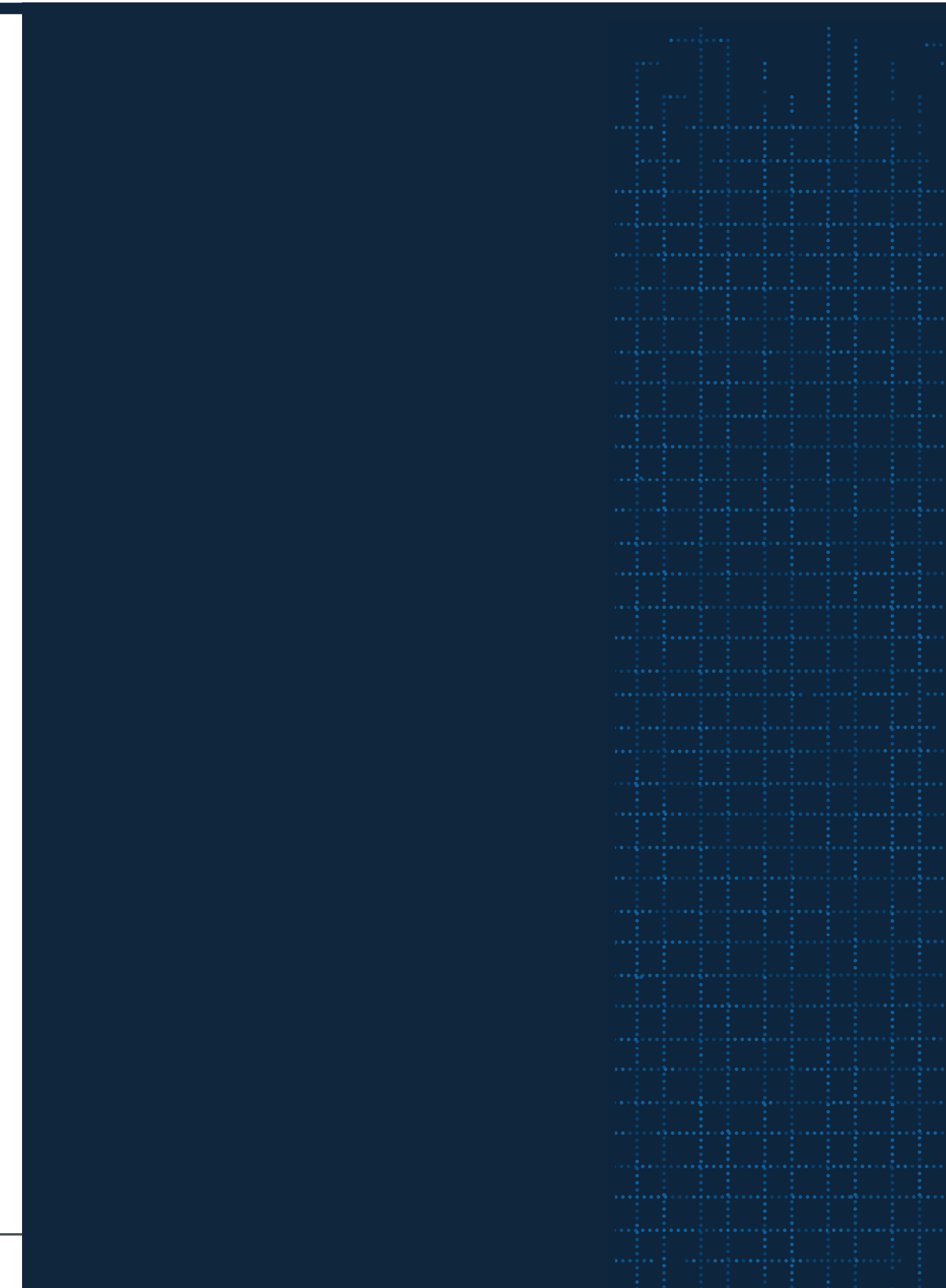
- de formation « interentreprises » (dispensée à plusieurs sociétés clientes de SysDream) dans les quinze (15) jours précédant ladite formation, SysDream sera en droit de facturer 100% du montant de la prestation correspondante et le Client pourra reporter cette formation dans un délai de six (6) mois maximum, à compter de la date d'annulation ;
- de formation « intra-entreprise » (dédiée aux équipes du Client) dans les trente (30) jours précédant ladite formation, SysDream sera en droit de facturer 100% du montant de la prestation correspondante et aucun report ne sera ne sera possible.

Pour toute annulation acceptée par Sysdream, de toute ou partie de la Commande par le Client, les sommes versées par le Client à titre d'acompte resteront acquises à SysDream à titre d'indemnité d'annulation. En absence d'acompte mais d'acceptation de l'annulation de la commande, SysDream se réserve le droit de facturer une indemnité de dédit forfaitaire conformément aux conditions suivantes :

A - Toute annulation de la Commande survenue dans les 48h de l'acceptation de la Commande pourra entrainer la facturation de 10 % de la Commande.

B - Toute annulation de la commande survenue au-delà du délai de 48h, pourra entrainer la facturation de 30 % de la Commande.

En outre, SysDream se réserve la possibilité de réclamer au Client le remboursement de l'intégralité des frais engagés. »



SysDream
Cybersécurité Hub One

MARKCOM-CATALOGUE-SD-FORMATION -VF - 20241107 / SysDream – 14 place Marie-Jeanne Bassot – 92300 Levallois - Capital Social 267 720 euros - RCS NANTERRE B 451676126 - Ne pas jeter sur la voie publique - Crédits photos : ©Shutterstock

SysDream

14, place Marie-Jeanne Bassot
92300 Levallois, France

Tel : +33 1 78 76 58 00
Mail : formation@sysdream.com

@sysdream