SysDream
Cybersécurité Hub One

FORMATIONS EN **CYBERSÉCURITÉ**

SYSDREAM FORMATION

Édition **2024**

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

En 2024, SysDream fête ses 20 ans. Créée en 2004 SysDream, pure player française de la sécurité informatique vous propose une offre globale et des solutions sur-mesure alignées sur vos enjeux.
20 ans d'expertise en cybersécurité, 20 ans d'audit technique (tests d'intrusion, red team, analyse inforensique, ou encore de détection et de réponse aux incidents de sécurité informatique), 20 ans d'existence de notre centre de formation en cybersécurité, 20 ans que nous accompagnons les organisations à monter en compétence en sécurité des systèmes d'information et nous en sommes très fiers !

Nos formations s'inscrivent pleinement dans notre volonté d'accompagner nos clients dans une démarche vertueuse de lutte contre les cyberattaques. Cet accompagnement s'appuie sur trois piliers complémentaires : Concevoir la Sécurité de votre Système d'Information (SSI), Surveiller votre SI et Renforcer sa sécurité. La réussite de ces missions repose sur les compétences de vos équipes qui doivent s'adapter et se former en permanence.

Nos consultants formateurs en cybersécurité sont reconnus pour vous apporter des formations de qualité en management de la SSI et en sécurité offensive et défensive. Nos experts passionnés et engagés se nourrissent de leurs expériences du terrain en conseil, en audit technique et organisationnel, en test d'intrusion et en réponse aux incidents de sécurité. Nos formateurs consacrent également du temps à de la recherche réalisée dans notre laboratoire de recherche et de veille technologique.

Nous formons chaque année plus de 1600 professionnels des PME jusqu'aux plus grandes organisations. Nous proposons douze parcours de formation adaptés aux différents métiers de l'IT que vous trouverez détaillés pages suivantes. Ils ont été élaborés en respectant la nomenclature du « Panorama des métiers de la Cybersécurité » de l'ANSSI.

Suivre nos formations, toujours plus orientées vers la pratique, vous permettra de bénéficier des années d'expérience de nos consultants et de leurs compétences uniques.

Depuis 20 ans, nous sommes fidèles à notre ADN : vous accompagner tout au long du cycle de vie de la sécurisation de votre système 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 :

APPRENDRE & SE SENSIBILISER
13 FORMATIONS

DÉTECTER & REMÉDIER
10 FORMATIONS

ACCOMPAGNER & SÉCURISER LE SI
6 FORMATIONS

AUDITER & CONTRÔLER
4 FORMATIONS

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

E-learning : sensibilisation à la cybersécurité (E-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)

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 v12 (CEH) ✓
- Hacking et sécurité : les Fondamentaux (HSF)
- Open Source Intelligence : les Fondamentaux (OSINT)
- Hacking et sécurité : Avancé (HSA)
- Audit de site Web (AUDWEB)

AUDITEUR DE SÉCURITÉ TECHNIQUE - PENTESTER (confirmé)

- Hacking et sécurité : Avancé (HSA)
- Sécurité Windows & Active Directory (SWAD)
- Sécurité des applications mobile (SAM)
- Bootcamp Exploitation de Vulnérabilités Applicatives (BEVA)
- Computer Hacking Forensic Investigator v10 (CHFI v10) ✓

✓ Formation certifiante

LES PARCOURS DE FORMATION

RESPONSABLE DE PROJET SÉCURITÉ

- E-learning : sensibilisation à la cybersécurité (E-SAC)
- Hacking et sécurité : les Fondamentaux (HSF)
- Hacking et sécurité : Avancé (HSA)
- Audit de site Web (AUDWEB)
- ISO 31000: Risk Manager (ISO 31000) ✓
- Certified Information Systems Security Professionnal (CISSP) ✓

AUDITEUR DE SÉCURITÉ ORGANISA-TIONNELLE

- Certified Ethical Hacker v12 (CEH) ✓
- Certified Information Systems Auditor (CISA) ✓
- ISO 27001: Certified Lead Auditor (ISO 27001 LA) ✓
- ISO 27005: Certified Risk Manager (ISO 27005 + EBIOS) ✓
- ISO 22361: Certified Lead Crisis Manager (ISO 22361) ✓

DSI

- Hacking et sécurité : les Fondamentaux (HSF)
- Hacking et sécurité : Avancé (HSA)
- ISO 27001 : Certified Lead Implementer (ISO 27001 LI) ✓
- 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) ✓
- ISO 31000: Risk Manager (ISO 31000) ✓
- ISO 22361: Certified Lead Crisis Manager (ISO 22361) ✓

ADMINISTRATEUR SYSTÈME & RÉSEAUX

- Sécurisation des réseaux (SR)
- Sécurisation Linux (SL)
- Hacking et sécurité : Avancé (HSA)
- Sécurité Windows & Active Directory (SWAD)

✓ Formation certifiante

LES PARCOURS DE FORMATION

ARCHITECTE SÉCURITÉ

- Certified Ethical Hacker v12 (CEH)
- Sécurisation des réseaux (SR)
- Sécurité Windows & Active Directory (SWAD)
- ISO 27001: Certified Lead Implementer (ISO 27001 LI)

OPÉRATEUR - ANALYSTE SOC

- Open Source Intelligence : les Fondamentaux (OSINT)
- Sécurisation Linux (SL)
- Sécurisation des réseaux (SR)
- Analyse inforensique avancée et réponse aux incidents (AIARI)
- EC-Council Certified Incident Handler (ECIHv3)
- Certified SOC Analyst (CSA)

ANALYSTE DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ (CERT)

- Certified Ethical Hacker v12 (CEH)
- Analyse inforensique avancée et réponse aux incidents (AIARI)
- EC-Council Certified Incident Handler (ECIHv3)
- Rétro-Ingénierie de logiciels malveillants (RILM)
- Malwares : détection, identification et éradication v2 (MDIE v2)
- Computer Hacking Forensic Investigator v10 (CHFI v10)

Formation certifiante

POURQUOI SYSDREAM ?

Forte 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 30 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 20 ans, SysDream accompagne chaque année plus de 1600 professionnels d'entreprises de toutes tailles.

Afin de renforcer son expertise cyber et comprendre l'ensemble des enjeux du marché, SysDream a élargi ses compétences dans les domaines du conseil, de l'audit, du test d'intrusion (pentest), de l'édition et de l'intégration de solutions sécurisées, de la détection d'incidents, de la réponse aux incidents, 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 2023 (recueillies du 1er janvier au 15 septembre 2023).

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.

SOMMAIRE DES FORMATIONS

HYBRIDE : nos formations HYBRIDE se font en présentiel ou en distanciel.

APPRENDRE & SE SENSIBILISER

PLANNING DES FORMATIONS

				JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
E-SAC	E-Learning : Sensibilisation à la cybersécurité														
HSF	Hacking & Sécurité : les Fondamentaux	HYBRIDE	2 jours		15	14	18	16	20			19	17	21	
HSA	Hacking & Sécurité : Avancé	HYBRIDE	5 jours		12	11	15	13	17			16	14	18	
HSE	Hacking & Sécurité : Expert	HYBRIDE	5 jours		19			27				30		4	
CEHv12	Certified Ethical Hacker v12	HYBRIDE	5 jours	29	26	25	22	27	17	8	26	23	14	18	9
ISO 27005 + EBIOS	ISO 27005 : Certified Risk Manager avec Méthode EBIOS		5 jours				15		10				7		
ISO 31000	ISO 31000 : Risk Manager		3 jours						17			25			16
NIS2	Sensibilisation à la mise en conformité à la Directive NIS2	HYBRIDE	1 jour		5	11	22		3	8		23	21	18	
SDORA	Règlement DORA : Sensibilisation		1 jour	29		25		27		1		9			
ADORA	Règlement DORA : Approfondissement		5 jours						24						2
SAM	Sécurité des Applications Mobiles		3 jours					29					9		
BEVA	Bootcamp Exploitation Vulnérabilités Applicatives		5 jours											25	
SDS	Sensibilisation au développement sécurisé	HYBRIDE	2 jours			7						26			

E-LEARNING : SENSIBILISATION À LA CYBERSÉCURITÉ

Comprendre pour appréhender au mieux les menaces informatiques

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.
Les différentes attaques sont ensuite présentées, ainsi que des illustrations par des exemples réels de démontrer techniquement la faisabilité des attaques.
Enfin, un ensemble de bonnes pratiques de sécurité sera présenté.

Code : E-SAC

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

Exemples d'attaques par logiciel malveillant ou rançongiciel

- Stuxnet
- Locky
- WannaCry

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

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

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 : E-SAC
Durée : 4 heures
Prix :

Tranche utilisateur	€HT/mois et utilisateur	Frais de mise en service
Jusqu'à 10	50 €	500 €
de 11 à 50	45 €	500 €
de 50 à 100	40 €	500 €
de 100 à 500	30 €	500 €
Au-delà de 500	nous consulter	-

Horaires : flexibles
Lieu : en ligne

PUBLIC VISÉ

- Toute personne désirant comprendre les menaces liées aux attaques informatiques

PRÉ-REQUIS

- Accessible à tous

RESSOURCES

- Support e-learning
- Contenus interactifs
- Jeux questions/réponses

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 (trace-route, 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

15 février 2024
14 mars 2024
18 avril 2024
16 mai 2024
20 juin 2024
19 septembre 2024
17 octobre 2024
21 novembre 2024

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

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

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

12 février 2024
11 mars 2024
15 avril 2024
13 mai 2024
17 juin 2024
16 septembre 2024
14 octobre 2024
18 novembre 2024

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

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

FORMATIONS ASSOCIÉES

- HSE : Hacking & Sécurité : Expert
- CEHv12 : Certified Ethical Hacker v12
- TEST-INT : Test d'intrusion : Mise en situation d'audit
- SWAD : Sécurité Windows et Active Directory
- AUDWEB : Audit de site Web

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

19 février 2024
27 mai 2024
30 septembre 2024
4 novembre 2024

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

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

CERTIFIED ETHICAL HACKER V12

Préparez-vous à la certification CEH en apprenant les dernières techniques d'Ethical Hacking - « Accredited Training Center » by EC-Council

Code : CEHv12

La formation Certified Ethical Hacker (CEHv12) est une formation reconnue et respectée, dont chaque professionnel de la sécurité aura besoin. Depuis sa création en 2003, la Certified Ethical Hacker est largement diffusée dans le monde entier, c'est une certification en conformité ANSI 17024, ce qui ajoute de la crédibilité et de la valeur aux membres certifiés. Le cours en est maintenant à sa 12ème version, il a été mis à jour afin de vous apporter les outils et techniques utilisés par les hackers et les professionnels de la sécurité, susceptibles de pénétrer dans n'importe quel système d'information. Ce cours va vous plonger dans « l'état d'esprit du Hacker » dans le but de vous enseigner à penser comme un hacker afin de mieux vous défendre.
Vous apprendrez notamment comment scanner, tester, hacker et sécuriser un système visé. Le cours couvre les cinq phases de l'Ethical Hacking : Reconnaissance, Obtention d'accès, Énumération, Maintien de l'Accès et Disparition des traces. Les outils et techniques de chacune de ces 5 phases seront présentés lors de la formation.

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 dans le lieu de votre choix.

- **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 :**
  - Set de questions «faciles» : 78% minimum de bonnes réponses requises.
  - Set de questions «difficiles» : 70% minimum de 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

29 janvier 2024
26 février 2024
25 mars 2024
22 avril 2024
27 mai 2024
17 juin 2024
8 juillet 2024
26 août 2024
23 septembre 2024
14 octobre 2024
18 novembre 2024
9 décembre 2024

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 : CEHv12
Durée : 5 jours
Prix : 4 700 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Examen CEH : inclus. Valable 12 mois pour un passage de l'examen à distance.

PUBLIC VISÉ

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

PRÉ-REQUIS

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

ISO 27005 : CERTIFIED RISK MANAGER AVEC EBIOS RISK MANAGER

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.

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 et 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 et 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

15 avril 2024
10 juin 2024
7 octobre 2024

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 : 4 150 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92)

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

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

ISO 31000 : RISK MANAGER

Maîtriser 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

17 juin 2024
25 septembre 2024
16 décembre 2024

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.

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

SENSIBILISATION À LA DIRECTIVE NIS2

Découvrez la Directive NIS2

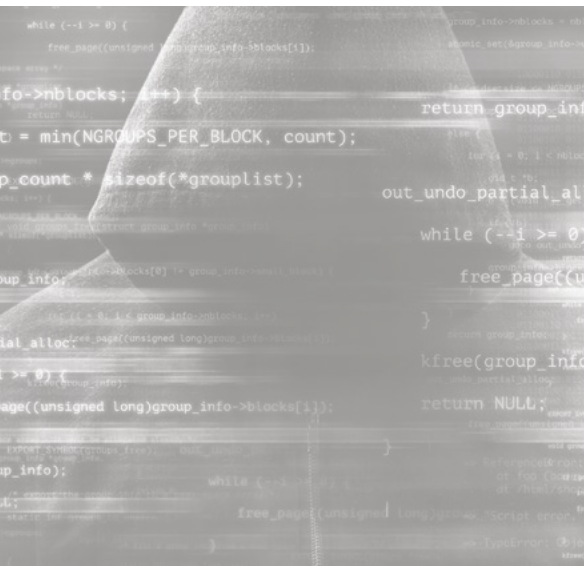
Code : NIS2

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 sur les 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 évalués tout au long de la formation sous forme de questions réponses et formalisés par une étude de cas, ainsi que 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

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

PROCHAINES DATES

29 janvier 2024
25 mars 2024
27 mai 2024
1er juillet 2024
9 septembre 2024

OBJECTIFS

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

INFORMATIONS GÉNÉRALES

Code : NIS2
Durée : 1 jour
Prix : 1 495 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

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 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.

Cette journée de sensibilisation pourra être complétée grâce aux sessions d'approfondissement (5 jours) :
- En INTER : du 24 au 28 juin 2024 **ou** du 2 au 6 décembre 2024
- En INTRA : sur demande, avec possibilité d'ajuster le programme en fonction de vos besoins

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 réglementaire
- Différences et point commun entre DORA et NIS2
- Sanctions prévues par DORA

Chapitre 2
- Les institution et organisation concernés par DORA
- Les exigences fixées par DORA

Chapitre 3
- Cadre de gestion du risque lié au TIC
- Audit régulier du cadre de gestion du risque TIC

Chapitre 4
- Stratégie de résilience opérationnelle numérique
- Les mécanismes de protection et de résilience des actifs
- Les solutions de détection
- Politique de continuité des activités TIC

Chapitre 5
- Procédure de sauvegarde, restauration et de rétablissement
- Les politiques associées

Chapitre 6
- Plan de communication en situation de crise
- Processus de gestion des incidents
- Plan de réponse aux incidents

Chapitre 7
- Veille sur les cybermenaces
- Test de résilience opérationnelle numérique
- Planification des tests d'intrusion fondés sur la menace

Chapitre 8
- Vulgarisation, sensibilisation et formation à la cybersécurité

Chapitre 9
- Évaluation et gestion des prestataires de service TIC

QCM final pour évaluer l'acquisition des savoirs du Règlement DORA

PROCHAINES DATES

29 janvier 2024
25 mars 2024
27 mai 2024
1er juillet 2024
9 septembre 2024

OBJECTIFS

- Découvrir le Règlement DORA au travers de ses 17 exigences.

INFORMATIONS GÉNÉRALES

Code : SDORA
Durée : 1 jour
Prix : 1 495 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

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

Cette journée de sensibilisation pourra être complétée grâce aux sessions d'approfondissement (5 jours) :
- En INTER : du 24 au 28 juin 2024 **ou** du 2 au 6 décembre 2024
- En INTRA : sur demande, avec possibilité d'ajuster le programme en fonction de vos besoins

RÈGLEMENT DORA : APPROFONDISSEMENT

Découvrez les 17 exigences du Règlement DORA et les possibilités de mise en œuvre

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 formation permet d'étudier de façon détaillée et complète les 17 exigences de DORA sur la résilience opérationnelle numérique pour les entités financières.
Chaque stagiaire pourra identifier les possibilités de mise en œuvre du Règlement avec des mesures techniques, organisationnelles et physiques.

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

Code : ADORA

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 (30% d'exercices pratiques + étude d'un cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Chapitre 1

- Cadre réglementaire
- Différences et point commun entre DORA et NIS2
- Sanctions prévues par DORA

JOUR 2

Chapitre 2

- Les institutions et organisations concernées par DORA
- Les exigences fixées par DORA

JOUR 3

Chapitre 3

- Cadre de gestion du risque lié au TIC
- Audit régulier du cadre de gestion du risque TIC

Chapitre 4

- Stratégie de résilience opérationnelle numérique
- Les mécanismes de protection et de résilience des actifs
- Les solutions de détection
- Politique de continuité des activités TIC

JOUR 4

Chapitre 5

- Procédure de sauvegarde, restauration et de rétablissement
- Les politiques associées

Chapitre 6

- Plan de communication en situation de crise
- Processus de gestion des incidents
- Plan de réponse aux incidents

JOUR 5

Chapitre 7

- Veille sur les cybermenaces
- Test de résilience opérationnelle numérique
- Planification des tests d'intrusion fondés sur la menace

Chapitre 8

- Vulgarisation, sensibilisation et formation à la cybersécurité

Chapitre 9

- Évaluation et gestion des prestataires de service TIC

Étude & correction d'un cas pratique

PROCHAINES DATES

24 juin 2024
2 décembre 2024

OBJECTIFS

- Découvrir le Règlement DORA au travers de ses 17 exigences
- Repartir avec des pistes concrètes de mise en œuvre afin de répondre aux exigences du Règlement

INFORMATIONS GÉNÉRALES

Code : ADORA
Durée : 5 jours
Prix : 4 150 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

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
- 30% d'exercices pratiques + étude d'un cas pratique
- 1 PC par personne

SÉCURITÉ DES APPLICATIONS MOBILES

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

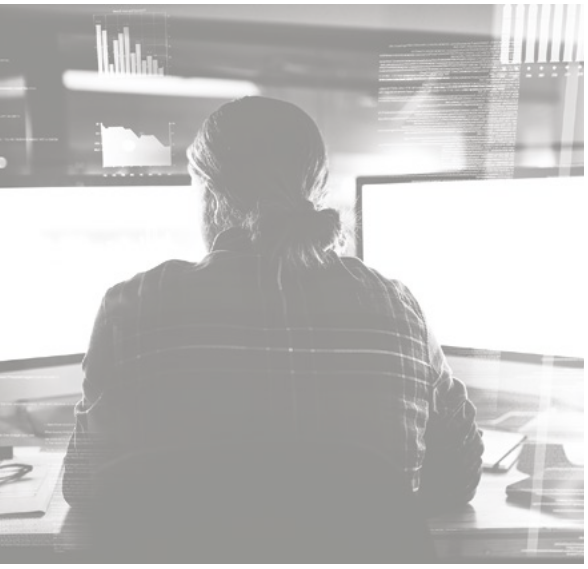
Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type test d'intrusion sur une application mobile Android et IOS.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise.
Lors de cette formation, vous étudierez 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 complétée 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

29 mai 2024
9 octobre 2024

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)

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

BOOTCAMP EXPLOITATION DE VULNÉRABILITÉS APPLICATIVES

Maîtrisez l'ensemble des techniques d'exploitation applicatives

Ce bootcamp 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 : BEVA

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

PROCHAINE DATE

25 novembre 2024

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 : BEVA
Durée : 5 jours
Prix : 4 150 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

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

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
- Contre-mesures et recommandations

Outils d'analyses
- Analyseurs statiques et dynamiques
- Techniques de 'fuzzing'

PROCHAINES DATES

7 mars 2024
26 septembre 2024

OBJECTIFS

- Connaître les attaques sur les APIs
- Maîtriser la gestion de session dans les applications Web
- Connaître les attaques sur les applications Web
- Maîtriser l'authentification et la gestion des habilitations sur les applications Web
- Connaître les patterns de développement usuels
- Connaître et utiliser les outils de développement et de déploiement

INFORMATIONS GÉNÉRALES

Code : SDS
Durée : 2 jours
Prix : 1 850 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

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)

AUDITER & CONTRÔLER

PLANNING DES FORMATIONS

				JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
AUDWEB	Audit de site Web	HYBRIDE	3 jours		21					3				13	
TEST-INT	Test d'intrusion : Mise en situation d'Audit	HYBRIDE	5 jours						24			16			2
CISA	Certified Information Systems Auditor	HYBRIDE	5 jours			18						9			
ISO 27001 LA	ISO27001 : Certified Lead Auditor		5 jours			4			3						2

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

21 février 2024
3 juillet 2024
13 novembre 2024

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

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

TEST D'INTRUSION : MISE EN SITUATION D'AUDIT

Le test d'intrusion (pentest) par la pratique

Code : TEST-INT

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
  - Déni 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

24 juin 2024
16 septembre 2024
2 décembre 2024

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 : 4 025 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

PUBLIC VISÉ

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

PRÉ-REQUIS

- Avoir des notions techniques de sécurité informatique
- Avoir suivi une formation HSA ou d'un niveau équivalent
- 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

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

18 mars 2024
9 septembre 2024

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

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

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 et 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

4 mars 2024
3 juin 2024
2 décembre 2024

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 : 4 150 € 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.

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

DÉTECTER & REMÉDIER

PLANNING DES FORMATIONS

				JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
ISO 22361	Certified Lead Crisis Manager		5 jours				8					30			9
AIARI	Analyse inforensique avancée et réponse aux incidents		3 jours			20								27	
CHFIv10	Computer Hacking Forensic Investigator v10	HYBRIDE	5 jours			25							7		
RILM	Rétro-ingénierie de logiciels malveillants		5 jours				8						21		
MDIE	Malwares : détection, identification et éradication		3 jours						12						4
ECIHv3	EC-Council Certified Incident Handler v3	HYBRIDE	3 jours										2		
CSA	Certified Soc Analyst	HYBRIDE	3 jours							1					
OSINT	Open Source Intelligence : les Fondamentaux		3 jours				24						23	27	
LP-U	Logpoint pour les utilisateurs		2 jours					sur demande							
LP-A	Logpoint pour les administrateurs		2 jours					sur demande							

ISO 22361 : CERTIFIED LEAD CRISIS MANAGER

Maîtriser les connaissances et les compétences de gestion de crise

Code : ISO 22361

La formation Certified Lead Crisis Manager aide les participants à développer leurs compétences pour soutenir une organisation dans la planification, l'établissement, le maintien, l'examen et l'amélioration continue de sa capacité stratégique de gestion de crise sur la base des lignes directrices de la norme ISO 22361 et d'autres bonnes pratiques.
En plus de l'explication des concepts théoriques liés à la gestion de crise, le cours de formation fournit des exemples pratiques et des quiz basés sur des scénarios qui vous aideront à renforcer vos connaissances et à vous préparer à des scénarios de la vie réelle concernant la gestion de crise.
Après avoir réussi l'examen, le certificat démontre que le participant possède les connaissances et les compétences théoriques et pratiques pour soutenir et diriger une organisation dans la conception et le développement de sa capacité de gestion de crise sur la base des lignes directrices de l'ISO 22361.

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 to ISO 22361 and crisis management

- Section 1 : Training course objectives and structure
- Section 2 : Standards and crisis management models
- Section 3: Fundamental concepts of crisis management
- Section 4 : Crisis management capability
- Section 5 : Principles for crisis management
- Section 6 : Crisis communications

JOUR 2

Crisis management framework

- Section 7 : Leadership
- Section 8 : Structure
- Section 9 : Culture
- Section 10 : Competence

JOUR 3

Crisis management framework

- Section 11 : Anticipation Leadership
- Section 12 : Assessment
- Section 13 : Prevention and mitigation
- Section 14 : Preparedness

JOUR 4

Crisis response and recovery

- Section 15 : Response
- Section 16 : Recovery
- Section 17 : Continual improvement
- Section 18 : Closing of the training course

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

8 avril 2024
30 septembre 2024
9 décembre 2024

OBJECTIFS

- Maîtriser la norme ISO 22361
- Développer des compétences et des bonnes pratiques pour soutenir une organisation dans sa capacité stratégique de gestion de crise
- Se préparer au passage de l'examen « Certified Lead Crisis Manager »

INFORMATIONS GÉNÉRALES

Code : ISO 22361
Durée : 5 jours (4,5 jours de formation + passage de l'examen l'après-midi du dernier jour)
Prix : 4 150€
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
Examen : inclus. Passage de l'examen l'après-midi de la formation. Formation certifiante.

PUBLIC VISÉ

- Personnes responsables de la mise en place d'une capacité de gestion de crise au sein d'une organisation
- Personnes responsables de la mise en œuvre d'un plan et d'une structure de gestion de crise au sein de l'organisation
- Responsables de crise
- Membres des équipes de gestion de crise
- Personnes cherchant à comprendre en profondeur la gestion de crise
- Personnes souhaitant entamer ou faire progresser leur carrière dans le domaine de la gestion de crise
- Consultants, conseillers et professionnels souhaitant acquérir une connaissance approfondie des lignes directrices de l'ISO 22361 sur la gestion de crise

PRÉ-REQUIS

- Avoir 5 ans d'expérience professionnelle dont 2 ans en gestion de crise et une activité de gestion de crise
- Totaliser 300 heures dans une activité de gestion de risques

RESSOURCES

- Support de cours en anglais
- Cours donnés en français
- Copie de la norme ISO 22361

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

20 mars 2024
27 novembre 2024

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)

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

COMPUTER HACKING FORENSIC INVESTIGATOR V10

La certification de l'investigation numérique - « Accredited Training Center » by EC-Council

Code : CHFIv10

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 CHFIv10 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 CHFIv10 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.

Modules enseignés

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

CERTIFICATION

Passage de l'examen

L'examen CHFIv10 (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.
  En conséquence, si le stagiaire a des « questions faciles », il devra au minimum avoir 78% tandis que celui qui tombe sur les « questions difficiles » sera reçu avec un score de 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

25 mars 2024
7 octobre 2024

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 : CHFIv10
Durée : 5 jours
Prix : 4 650 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Examen CHFI : inclus. Valable 12 mois pour un passage de l'examen à distance.

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

FORMATIONS ASSOCIÉES

- RILM : Rétro-Ingénierie de Logiciels Malveillants
- MDIE : Malwares : Détection, Identification et Éradication

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

8 avril 2024
21 octobre 2024

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 : 4 150 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

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

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

12 juin 2024
4 décembre 2024

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)

PUBLIC VISÉ

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

PRÉ-REQUIS

- 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

EC-COUNCIL CERTIFIED INCIDENT HANDLER V3

Apprenez à gérer les incidents de sécurité - « Accredited Training Center » by EC-Council

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 atouts majeurs 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

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- Forensic Readiness and First Response
- Handling and Responding to Malware Incidents
- Handling and Responding to Email Security Incidents
- Handling and Responding to Network Security Incidents
- Handling and Responding to Web Application Security Incidents
- Handling and Responding to Cloud Security Incidents
- Handling and Responding to Insider Threats
- Handling and Responding to Endpoint Security Incidents

CERTIFICATION ECIH (INCLUSE AVEC LA FORMATION)

Présentation : L'examen ECIH aura lieu à distance dans le lieu de votre choix.

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.

PROCHAINE DATE

2 octobre 2024

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

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

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.

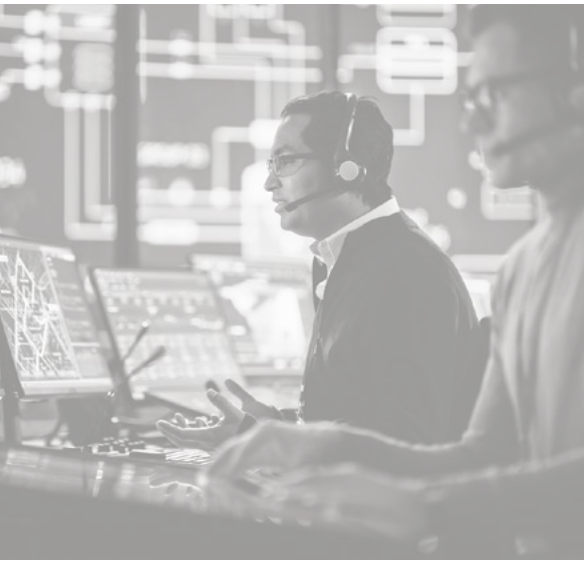
Le programme Certified SOC Analyst (CSA) est la première étape pour rejoindre un SOC - Security Operations Center.
Il est conçu pour les analystes de niveau I et II afin de leur permettre d'acquérir les compétences nécessaires pour effectuer des opérations de premier et deuxième niveau.
Le CSA est un programme de formation et d'accréditation qui aide le candidat à acquérir des compétences techniques recherchées et ce, grâce aux formateurs les plus expérimentés de l'industrie. 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 01 : Security Operations and Management
- Module 02 : Understanding Cyber Threats, IoCs, and Attack Methodology
- Module 03 : Incidents, Events, and Logging
- Module 04 : Incident Detection with Security Information and Event Management (SIEM)
- Module 05 : Enhanced Incident Detection with Threat Intelligence
- Module 06 : 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.

PROCHAINE DATE

1er juillet 2024

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

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

OPEN SOURCE INTELLIGENCE (OSINT)

Apprenez les fondamentaux de l'enquête en sources ouvertes

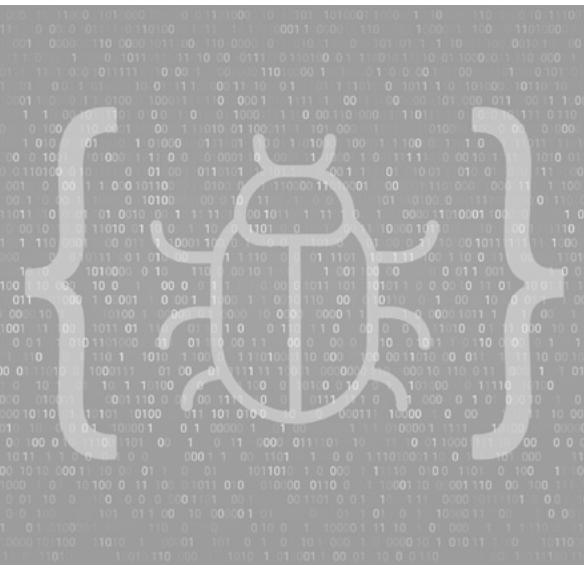
Code : OSINT

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

24 avril 2024
23 octobre 2024
27 novembre 2024

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)

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

LOGPOINT POUR LES UTILISATEURS

Faites face aux défis de sécurité grâce à la solution LogPoint

Code : LP-U

Cette formation User LogPoint vous enseignera les compétences nécessaires pour résoudre des problèmes de cybersécurité complexes et atténuer efficacement les menaces grâce à la solution de SIEM LogPoint.
Il s'agit d'une solution européenne unique sur le marché, certifiée CSPN qui vous permettra de faire face à vos défis de sécurité.
Acquérir la compétence pour transformer des données complexes en informations exploitables est essentiel pour offrir une meilleure visibilité sur la sécurité d'une entreprise.
Maîtriser la détection des menaces en temps réel, identifier les tendances et anticiper les attaques potentielles.
Élaborer des tableaux de bord personnalisés pour visualiser et analyser l'état de la sécurité de votre entreprise.
Cette formation offre une expertise précieuse dans le domaine de la sécurité informatique, fournissant les outils nécessaires pour une défense efficace des systèmes et des données.

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 sur LogPoint

- Présentation de l'environnement de LAB
- Centre d'aide LogPoint
- Tableaux de bord
- Recherches simples :
  - Recherche par mot
  - Recherche par des phrases
- Modèles de recherches
- Utilisation de clé-valeur
- Utilisation de Labels
- Réalisation de l'agrégation
- Macros
- Recherches basiques
- Recherches standards

JOUR 2

- « Search View »
- Templates de recherche
- Reporting
- Configuration des alertes
- LogPoint UEBA

PROCHAINES DATES

Sur demande

OBJECTIFS

À la fin de la formation, vous serez capable de :

- Connaître la différence entre les logs bruts et/ou les logs normalisés
- Faire des recherches sur les Logs bruts
- Faire des recherches sur les Logs normalisés
- Maîtriser l'usage des macros
- Maîtriser l'usage des différentes vues de recherche
- Maîtriser l'usage des templates des recherches
- Maîtriser l'usage des tableaux de bord
- Utiliser le module d'enrichissement
- Mettre en place des alertes et des rapports au sein de la solution

INFORMATIONS GÉNÉRALES

Code : LP-U
Durée : 2 jours
Prix : 1 600 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

- Administrateur système et/ou réseau
- Tous salariés IT souhaitant exploiter la plateforme LogPoint

PRÉ-REQUIS

- Avoir des connaissances en sécurité informatique
- Savoir administrer un poste de travail (Windows et Linux)
- Connaître les équipements réseaux
- Savoir utiliser les outils Office et les fichiers PDF

RESSOURCES

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

LOGPOINT POUR LES ADMINISTRATEURS

Faites face aux défis de sécurité grâce à la solution LogPoint

Code : LP-A

La formation Admin LogPoint vous enseignera les compétences nécessaires pour mettre en place la solution LogPoint et configurer la collecte des journaux de manière optimale.

Il s'agit d'une solution européenne unique sur le marché, certifiée CSPN qui vous permettra de faire face à vos défis de sécurité.

Apprenez à configurer les paramètres de sécurité, analyser les journaux pour identifier les menaces potentielles, mettre en place des stratégies de sauvegarde et de récupération des données.
En résumé, la formation vous donnera des compétences nécessaires pour gérer de manière optimale la solution LogPoint dans divers scénarios et garantir la sécurité et la fiabilité du système.

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 sur LogPoint

- Présentation de l'environnement de LAB
- Configuration du serveur LogPoint :
  - Gestion des licences
  - Mises à jour
  - Paramètres des serveurs
  - Paramètre du profil
- Configuration de LogPoint :
  - Applications
  - Repositories
  - Politiques de routage
  - Politique de normalisation
  - Sources d'enrichissement
  - Processing Policies
  - Politiques de collecte des logs

JOUR 2

- Configuration d'un Device
- L'agent LogPoint :
  - Installation d'un agent LogPoint Windows (LPA)
  - Utilisation de la fonctionnalité Windows File Integrity
- Administration des utilisateurs :
  - Groupes de permissions
  - Groupes d'utilisateurs
  - Groupes d'utilisateurs en cas d'incident
  - Groupe sur la confidentialité des données
- Solution UEBA :
  - Exigences
  - Évaluation et notation
  - Entrées et sorties
  - Licences
- Sauvegarde et restauration
- Snapshots
- Support et dépannage sur LogPoint

PROCHAINES DATES

Sur demande

OBJECTIFS

À la fin de la formation, vous serez capable de :

- Analyser les composants et la structure de la solution
- Définir les règles de normalisation
- Définir les règles d'enrichissement
- Définir les règles des stratégies de stockage des journaux (Logs)
- Paramétrer la collecter des journaux (Logs)

INFORMATIONS GÉNÉRALES

Code : LP-A
Durée : 2 jours
Prix : 1 600 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

- Administrateur système et/ou réseau
- Tous salariés IT souhaitant exploiter la plateforme LogPoint

PRÉ-REQUIS

- Avoir des connaissances en sécurité informatique
- Savoir administrer un poste de travail (Windows et Linux)
- Connaître les équipements réseaux
- Savoir utiliser les outils Office et les fichiers PDF

RESSOURCES

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

ACCOMPAGNER & SÉCURISER LE SI

PLANNING DES FORMATIONS

				JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
ISO 27001 LI	ISO27001 : Certified Lead Implementer		5 jours			11			24			30		25	
CISM	Certified Information Security Manager	HYBRIDE	4 jours				2								10
CISSP	Certified Information Systems Security Professional	HYBRIDE	5 jours		5		8		10			9	21		9
SWAD	Sécurité Windows et Active Directory	HYBRIDE	3 jours						5					13	
SL	Sécurisation Linux		3 jours					22					14		
SR	Sécurisation des Réseaux		3 jours		7		24					16			16

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

Code : ISO 27001 LI

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).

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 et 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

11 mars 2024
24 juin 2024
30 septembre 2024
25 novembre 2024

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 : 4 150 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
Examen : inclus. Passage de l'examen le vendredi après-midi. Formation certifiante.

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 donné en français
- Copie de la norme ISO 27001

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

2 avril 2024
10 décembre 2024

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 : 3 850 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Examen CISM : non inclus. Inscription à l'examen sur le site de l'ISACA. Formation certifiante.

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

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

5 février 2024
8 avril 2024
10 juin 2024
3 juillet 2023,
9 septembre 2024
21 octobre 2024
9 décembre 2024

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 CISSP : non inclus, examen en option sur demande.
Formation certifiante.

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

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 juin 2024
13 novembre 2024

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 : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

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

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

22 mai 2024
14 octobre 2024

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 : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

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)

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

7 février 2024
24 avril 2024
16 septembre 2024
16 décembre 2024

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 : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

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

RESSOURCES

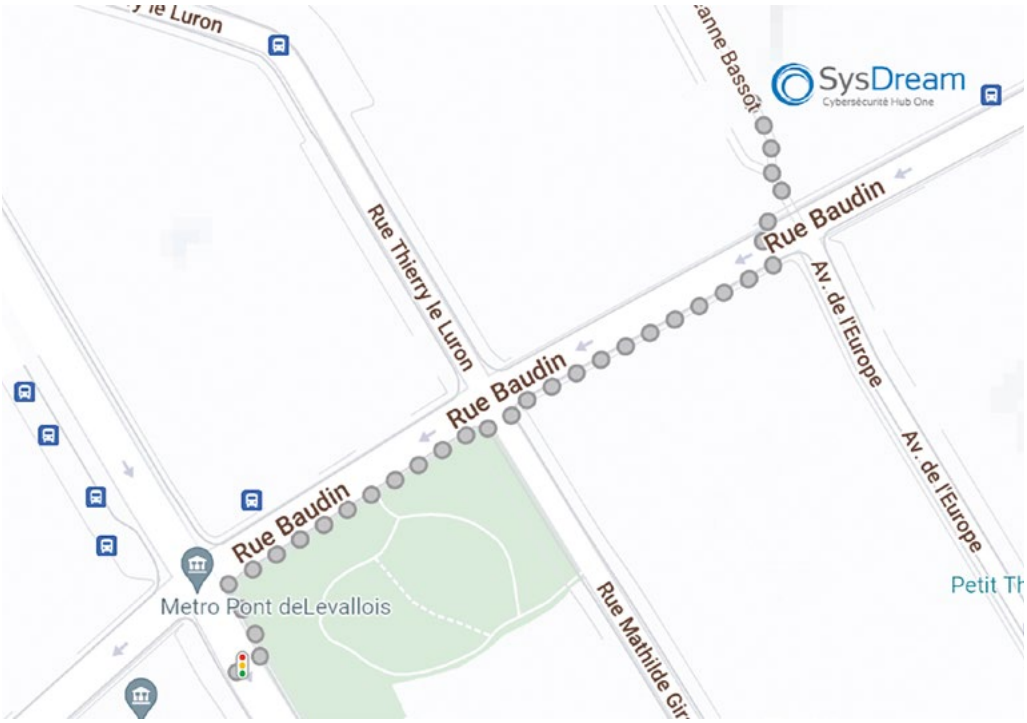
- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne
- Environnement de démonstration

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.

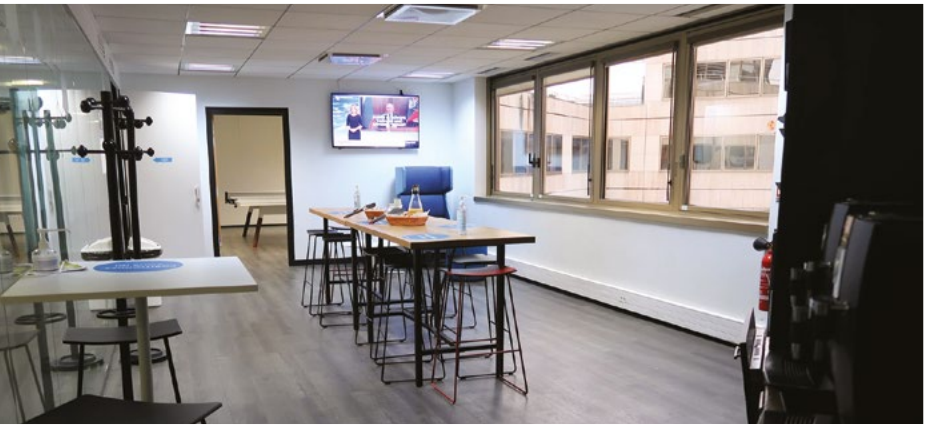


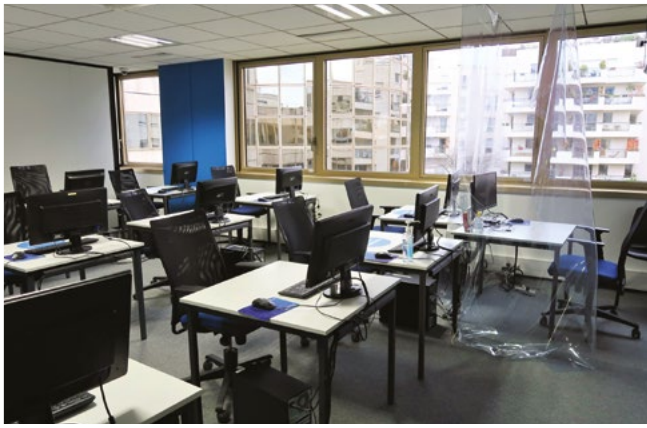
LE CENTRE DE FORMATION

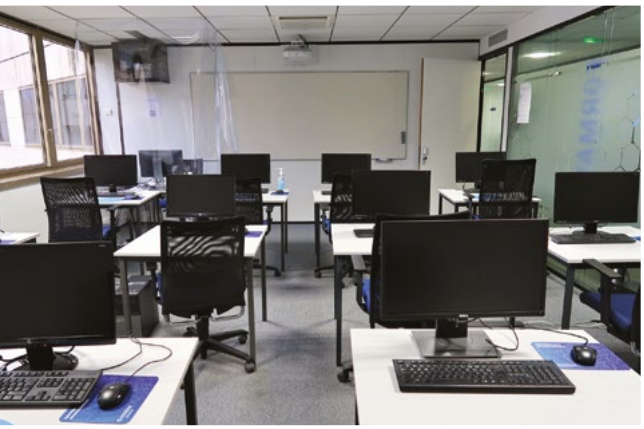
Nous mettons à votre disposition le matériel le plus récent et assurons à chacun des stagiaires un poste individuel équipé des logiciels nécessaires pour toutes nos formations.

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.

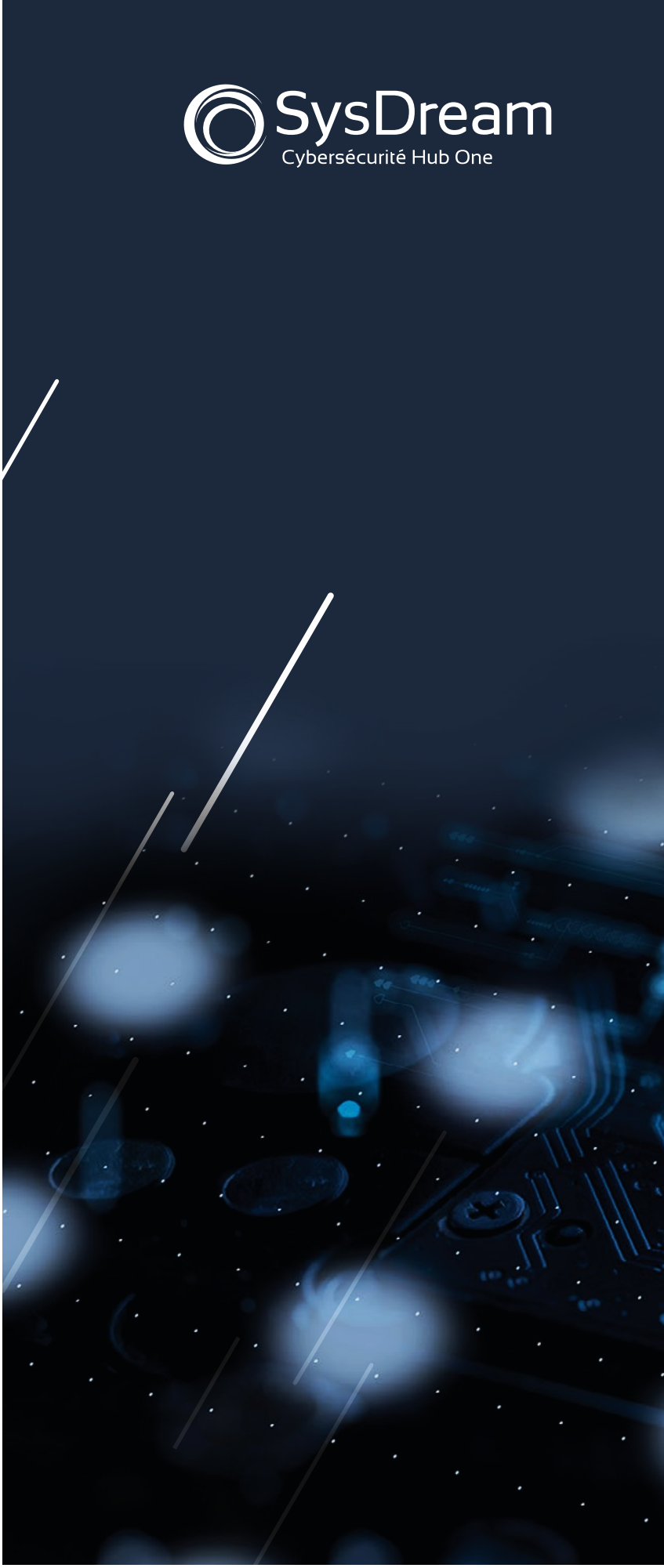
Toutes nos salles sont lumineuses et climatisées.
Un espace détente est mis à disposition de nos clients.







SysDream
Cybersécurité Hub One



SysDream

14, place Marie-Jeanne Bassot
92300 Levallois, France

Tel : +33 1 78 76 58 00
Mail : formation@sysdream.com

@sysdream

sysdream.com