SysDream
Cybersécurité Hub One

FORMATIONS EN **SECURITÉ INFORMATIQUE**

SYSDREAM FORMATION

Édition **2022**

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

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

sysdream.com

ÉDITORIAL

Depuis 2004, SysDream a bâti sa réputation en proposant des programmes de formation orientés selon le point de vue de l'attaquant (Sécurité Offensive ou Ethical Hacking).

Pionniers dans cette approche, nous continuons aujourd'hui de nous entourer des meilleurs profils techniques grâce à notre communauté de hackers éthiques (White Hat). Nous avons par ailleurs élargi notre champ de compétences en couvrant les autres domaines complémentaires de la cybersécurité que sont le management, la sécurité défensive et l'analyse inforensique. Nos consultants formateurs sont des experts passionnés et engagés. Ils partagent leur activité entre le conseil, l'audit (technique et organisationnel), le pentest, la recherche et la formation. Chaque programme dispensé par SysDream est ainsi l'occasion de partager avec vous notre expertise terrain.

Pour répondre aux enjeux de cybersécurité d'aujourd'hui et de demain, SysDream s'appuie sur son laboratoire de recherche et de veille technologique. Indépendante vis-à-vis de toute solution matérielle ou logicielle, elle garantit ainsi une parfaite objectivité dans ses recommandations et choix techniques opérés pour ses clients.

Aujourd'hui, la formation est l'un des piliers d'une sécurité efficace. SysDream conçoit et anime à la fois des formations de haute expertise technique et des programmes de sensibilisation pour les utilisateurs du système d'information, que ce soit en présentiel ou à distance.

Nous formons plus de 1600 professionnels chaque année (techniciens, consultants, analystes sécurité ...), dont les équipes techniques des plus grands groupes.

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.

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

SysDream appartient à la société Hub One.

Grégory MAUGUIN
Directeur-SysDream

SOMMAIRE

POURQUOI SYSDREAM

Attachée à la qualité des formations et 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 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 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 mutualisés 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. Cette certification est valable 3 ans.

4 - SysDream - un gage de confiance

Centre de formation depuis plus de 18 ans, SysDream accompagne chaque année plus de 1600 professionnels d'entreprises de toute taille.

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 à incidents, offrant ainsi une vision et des compétences 360° en cybersécurité.

- 96% de nos formateurs ont été notés à plus de 4,6/5
- 89% de nos stagiaires recommandent nos formations

(Basée sur 587 enquêtes entre septembre et novembre 2021)

NOS ENGAGEMENTS

Expérience de la formation

Depuis 18 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 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 dirigées 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 font activement partie de plusieurs laboratoires de recherche internationalement renommés et sont, de plus, régulièrement consultants pour de grands groupes industriels et 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 tente de donner à tous les mêmes chances d'accéder ou de maintenir l'emploi.

C'est pourquoi nous vous proposons, si vous le souhaitez, de prendre en compte votre handicap, visible ou invisible, pendant toute la durée de votre formation. Pour cela, il sera utile lors de notre entretien d'analyse de votre besoin, avant la formation de nous communiquer la description de votre handicap, afin que nous puissions étudier la faisabilité de la réalisation de l'action de formation. Si nous ne parvenons pas à prendre en compte votre handicap, nous vous orienterons alors vers des organismes compétents (voir liste ci-dessous).
Le choix du dispositif et l'aide financière possible dépendent de votre situation professionnelle, demandeur d'emploi ou salarié.

Nous vous invitons également à consulter le site internet : ici

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.

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.

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

SÉCURITÉ OFFENSIVE - ETHICAL HACKING

Destinées aux consultants et experts en sécurité, ainsi qu'aux administrateurs et techniciens, les formations Ethical Hacking vous permettront d'acquérir les connaissances fondamentales pour la mise en œuvre pratique de tests techniques avancés sur les systèmes et équipements réseaux du SI, lors de vos audits techniques et vos tests de pénétrations.

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
E-SAC	E-Learning : Sensibilisation à la cybersécurité	4 heures												
SACD	Sensibilisation à la cybersécurité pour les dirigeants	1/2 jour												
HSF	Hacking & Sécurité : les Fondamentaux	2 jours		7	7	4	9	13	4		19	10	7	12
HSAv6	Hacking & Sécurité : Avancé v6	5 jours		7	14	11	9	20	4		12	10	14	12
HSEv4	Hacking & Sécurité : Expert v4	5 jours	31			11		20			26		21	
CEHv11	Certified Ethical Hacker v11	5 jours	17	14	14	11	16	13	4	22	19	17	14	12
PNT	Test d'intrusion : Mise en situation d'Audit	5 jours	31			4						17		
AUDWEB	Audit de site web	3 jours			21			13					7	
AUDSI	Mener un audit de sécurité : méthode d'audit d'un SI	3 jours					2				5		28	
REVA	Recherche et exploitation de vulnérabilités sous Android	3 jours			9		30				5		28	
SEC	Social Engineering et contre-mesures	1 jour			28		10				13			
BEVA	Bootcamp Exploitation Vulnérabilités Applicatives	5 jours	31					20					21	
PYTPEN	Python pour le Pentest	4 jours												
CISA	Certified Information Systems Auditor	5 jours			28		30					24		

Formations 100% distanciel

Session hybride

E-LEARNING : SENSIBILISATION À LA CYBERSÉCURITÉ

Comprendre pour appréhender au mieux les menaces informatiques

Code : E-SAC

Cette formation vise à sensibiliser les stagiaires aux menaces informatiques. L'aspect organisationnel lié à la sécurité informatique au sein de l'entreprise sera tout d'abord évoqué.
Une présentation des différentes attaques ainsi que des cas pratiques sera ensuite réalisée, et cela dans l'objectif de démontrer techniquement la faisabilité des attaques.
Enfin un ensemble de bonnes pratiques de sécurité sera présenté pour permettre de pallier aux problèmes abordés.

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.

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
- Catégories
- 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

INFORMATIONS GÉNÉRALES

Code : E-SAC
Durée : 4 heures
Prix :

Tranche utilisateur	€HT/mois et utilisateur	Frais de mise en service
Jusqu'à 10	90 €	200 €
de 11 à 50	85 €	400 €
de 50 à 100	80 €	800 €
de 100 à 500	70 €	1 000 €
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

SENSIBILISATION À LA CYBERSÉCURITÉ POUR LES DIRIGEANTS

Comprendre pour appréhender au mieux les menaces informatiques

Code : SACD

Cette formation vise à sensibiliser les stagiaires aux menaces informatiques. L'aspect organisationnel lié à la sécurité informatique au sein de l'entreprise sera tout d'abord évoqué.
Une présentation des différentes attaques ainsi que des cas pratiques sera ensuite réalisée, et cela dans l'objectif de démontrer techniquement la faisabilité des attaques.
Enfin un ensemble de bonnes pratiques de sécurité sera présenté pour permettre de pallier aux problèmes abordés.

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.

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation.

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
- NIS LPM

Les bonnes pratiques de gouvernance de la cybersécurité

- La stratégie
- L'organisation
- Les instances de pilotage
- Les principes fondamentaux

L'ingénierie sociale

- Messagerie
- Téléphone
- Navigation web
- Pièce jointe

Exemples d'attaques par logiciel malveillant ou rançongiciel

- Zeus
- Stuxnet
- Locky
- WannaCry

Les protections et bons réflexes

- L'usage des mots de passe et les mécanismes d'authentification
- La gestion des droits
- L'utilisation de moyens personnels / professionnels
- Ports de communication des terminaux (USB, Firewire, PCI Express, etc.)
- Chiffrement du disque Verrouillage du poste Mises à jour
- Antivirus et pare-feu
- Connexion sur un réseau inconnu Détection et remontée d'alertes
- Que faire en cas d'incident ?

FORMATION SUR DEVIS

OBJECTIFS

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

INFORMATIONS GÉNÉRALES

Code : SACD
Durée : 0,5 jour
Prix : Sur devis
Horaires : 13h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Cadres dirigeants, managers, RSSI, DPO

PRÉ-REQUIS

- Accessible à tout manager

RESSOURCES

- Support de cours
- 50% de théorie
- 50% de retours d'expérience et d'exemples

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 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 premières compétences techniques de base, nécessaires à la réalisation d'audits de sécurité (test de pénétration), en jugeant par vous-même de la criticité et 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.

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 (70% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences 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
- Rappels modèles OSI et TCP/IP
- Vocabulaire
- Protocoles ARP, IP, TCP et UDP
- NAT
- Scan de ports
- Sniffing
- ARP Cache Poisoning
- DoS / DDoS

JOUR 2

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
- Outils de contrôle à distance
- Attaques à distance
- Introduction à Metasploit Framework

Scanner de vulnérabilités
- Attaques d'un poste client
- Attaque d'un serveur
- Introduction aux vulnérabilités Web

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

PROCHAINES DATES

7 mars 2022,
4 avr. 2022,
9 mai 2022,
13 juin 2022,
4 juil. 2022,
19 sept. 2022,
10 oct. 2022,
7 nov. 2022,
12 déc. 2022

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
- Connaître les attaques locales
- Se sensibiliser face aux attaques d'ingénierie sociale
- Savoir comment se sécuriser et connaître les notions de cryptographie, stéganographie et d'anonymat
- Mettre en pratique les connaissances acquises

INFORMATIONS GÉNÉRALES

Code : HSF
Durée : 2 jours
Prix : 1 250 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP
- Connaissances sur la sécurité des systèmes Windows et Linux
- Connaissances sur le fonctionnement des applications Web

RESSOURCES

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

SOCIAL ENGINEERING ET CONTRE-MESURES

Comprendre les failles humaines pour mieux s'en prémunir

Cette formation vise à sensibiliser les participants aux attaques par manipulation que peuvent mettre en place les attaquants. Les concepts clés du social engineering et les principales techniques de manipulation y seront abordés. Vous apprendrez à identifier les menaces et à adopter les bonnes pratiques afin d'éviter de vous faire manipuler.

Code : SEC

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) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Introduction au social engineering
- Qu'est-ce que le social engineering ?
- Qui l'utilise et dans quel but ?
- Quels sont les risques liés au social engineering ?

Le modèle de communication
- Présentation
- Développer son modèle de communication

L'incitation
- Le principe
- Le but
- Préparer sa cible
- Comment être efficace
- Exemples courants d'incitations

L'imposture, ou comment devenir n'importe qui
- Le principe
- Les points clés pour réussir
- Exemples d'impostures réussies

L'importance de la psychologie
- Les différents modes de perception
- Les sens
- Le visuel
- L'auditif
- Le kinesthésique
- Les micro-expressions
- La programmation neuro-linguistique

Quelques techniques de SE
- La gestuelle
- L'ancrage
- L'imitation

La persuasion
- Le principe
- Les points clés
- Importance de l'influence
- La réciprocité
- L'obligation
- La concession
- L'attractivité
- L'autorité
- Le cadrage (framing)

Le social engineering appliqué au pentest
- Prise d'information
  - Présentation d'outils
  - Google dorks
  - Shodan
  - DNS
  - Réseaux sociaux et outils collaboratifs
- Choix de/des victimes
- Exploitation humaine
  - SET
  - Création d'une pièce jointe piégée

Prévention et réduction du risque
- Apprendre à identifier les attaques par manipulation
- Sensibilisation du personnel
- Politique d'accès physique
- Politique de mise à jour
- Les bonnes pratiques

PROCHAINES DATES

28 févr. 2022,
10 mai 2022,
13 sept. 2022

OBJECTIFS

- Connaitre les techniques d'ingénierie social et les moyens de s'en prémunir

INFORMATIONS GÉNÉRALES

Code : SEC
Durée : 1 jour
Prix : 850 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

Toute personne désirant comprendre les attaques par manipulation.

PRÉ-REQUIS

Accessible à tous

RESSOURCES

- Support de cours
- 30% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement Windows

HACKING & SÉCURITÉ : AVANCÉ V6

Pratiquez les attaques avancées pour mieux vous défendre

Code : HSA

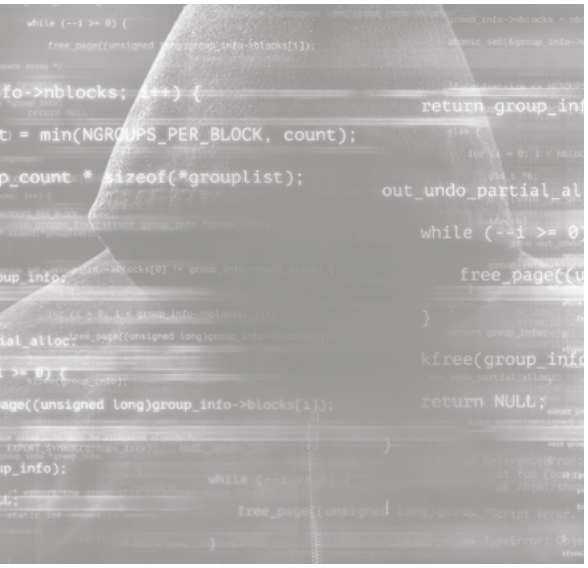
Ce cours est une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises.
Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes.
L'objectif est de vous fournir les compétences techniques nécessaires à la réalisation d'audits de sécurité (tests de pénétration), 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's...) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.



JOUR 1

Introduction
- Rappel TCP/IP / Réseau Matériel
- Protos / OSI - Adressage IP

Introduction à la veille
- Vocabulaire
- BDD de Vulnérabilités et Exploits
- Informations générales

Prise d'information
- Informations publiques
- Moteur de recherche
- Prise d'information active

Scan et prise d'empreinte
- Énumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

JOUR 2

Attaques réseau
- Idle Host Scanning
- Sniffing réseau
- Spoofing réseau
- Hijacking
- Attaques des protocoles sécurisés
- Dénis de service

Attaques système
- Scanner de vulnérabilités
- Exploitation d'un service vulnérable distant
- Élévation de privilèges
- Espionnage du système
- Attaques via un malware
  - Génération d'un malware avec Metasploit
  - Encodage de payloads
- Méthode de détection

JOUR 3

Attaques Web
- Cartographie du site et identification des fuites d'information
- Failles PHP (include, fopen, Upload,etc.)
- Injections SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Bonnes pratiques

JOUR 4

Attaques applicatives
- Escape shell
- 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

PROCHAINES DATES

14 mars 2022,
11 avr. 2022,
9 mai 2022,
20 juin 2022,
4 juil. 2022,
12 sept. 2022,
10 oct. 2022,
14 nov. 2022,
12 déc. 2022

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 : 3 500 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- RSSI, DSI
- Consultants en sécurité
- Ingénieurs / techniciens
- Administrateurs systèmes / réseaux
- Développeurs

PRÉ-REQUIS

- Avoir suivi la formation HSF ou une formation équivalente
- Maîtrise des protocoles réseaux TCP/IP
- Connaissances sur la sécurité des systèmes Windows et Linux
- Connaissances sur le développement Web et le fonctionnement des applications Web
- Connaissances en cryptographie.

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne / Internet
- Metasploit

FORMATIONS ASSOCIÉES

- Hacking & Sécurité : Expert v4
- Certified Ethical Hacker v11
- Test d'intrusion : Mise en situation d'audit

CERTIFIED ETHICAL HACKER V11

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

Code : CEHv11

La formation Certified Ethical Hacker (CEHv11) est une formation reconnue et respectée, dont chaque professionnel de la sécurité aura besoin. Depuis sa création en 2003, le Certified Ethical Hacker est largement diffusé dans le monde entier, c'est une certification respectée et accréditée en conformité ANSI 17024, ce qui ajoute de la crédibilité et de la valeur aux membres certifiés. Le cours en est maintenant à sa 11ème version, il a été mis à jour afin de vous apporter les outils et techniques utilisés par les pirates 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 pirate 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 Hacking
- **Module 19:** Cloud Computing
- **Module 20:** Cryptography

Résultat

directement disponible en fin d'examen.

Passage de l'examen

L'examen CEH (312-50) aura lieu dans les locaux de SysDream. Il est également possible de passer l'examen à distance depuis le lieu de votre choix (en option) mais il faudra alors en faire la demande au moment de votre inscription à la formation.

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

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'information, vous pouvez consulter le site d'EC-Council.

Certification CEH practical (en option)

Présentation : Le CEH Practical est un examen rigoureux de 6 heures, qui demandera aux participants de prouver leurs compétences en ethical hacking. Ils seront interrogés sur des sujets comme l'identification de vecteurs de menace, le scan de réseau, la détection OS, l'analyse de vulnérabilité, hacking de système ou encore d'applications web, le but étant de réussir l'ensemble des challenges en lien avec un audit de sécurité.
Les candidats auront un temps limité, exactement comme pour un exercice réel. Cet examen a été développé par un panel d'experts, il inclut 20 scénarios tirés de véritables expériences avec des questions visant à valider les compétences essentielles requises dans le domaine de l'ethical hacking.

Passage de l'examen : Cet examen est le premier à être complètement en ligne, en direct et automatiquement supervisé par un Proctor à distance.

- **Titre de l'examen :** Certified Ethical Hacker (Practical)
- **Nombre de challenges pratiques :** 20
- **Durée :** 6 heures
- **Langue :** anglais
- **Score requis :** 70%

Destinataire de l'examen : Toute personne officiellement et dûment certifiée CEH (ANSI) pourra se présenter à l'examen CEH Practical.

Processus d'éligibilité : Les candidats intéressés par ce programme devront au préalable remplir un formulaire d'éligibilité. Cette éligibilité, qui est généralement validée entre 5 et 10 jours par EC-Council, est ensuite valable pour 3 mois.
À réception du code Dashboard, à activer sous ASPEN, le candidat aura également 3 mois pour tester et compléter les différents challenges proposés.

PROCHAINES DATES

14 févr. 2022,
14 mars 2022,
11 avr. 2022,
16 mai 2022,
13 juin 2022,
4 juil. 2022,
22 août. 2022,
19 sept. 2022,
17 oct. 2022,
14 nov. 2022,
12 déc. 2022

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 312-50

INFORMATIONS GÉNÉRALES

Code : CEHv11
Durée : 5 jours
Prix : 3 950 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)
Examen CEH : inclus. Valable 10 mois pour un passage de l'examen dans les locaux de SysDream. Passage de l'examen à distance depuis le lieu de votre choix disponible en option. Formation certifiante.
Examens : Contactez-nous pour connaître les prochaines dates.

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 donné en français
- 20% d'exercices pratiques
- 1 PC par personne / Internet

TEST D'INTRUSION : MISE EN SITUATION D'AUDIT

Le PenTest par la pratique

Code : PNT

Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur votre S.I.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise. En effet, le PenTest 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 y étudierez notamment l'organisation et les procédures propres à ce type d'audit ; ainsi qu'à utiliser vos compétences techniques (des compétences équivalentes au cours HSA sont recommandées) et les meilleurs outils d'analyse et d'automatisation des attaques (outils publics ou privés développés par nos équipes) 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 en fin de module par le formateur.

JOUR 1

Méthodologie de l'audit

La première journée sera utilisée pour poser 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 PenTest

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

Aspect réglementaire

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

Exemples de méthodologies et d'outils

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

Éléments de rédaction d'un rapport

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

Une revue des principales techniques d'attaques et 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, un réseau d'entreprise.

Le système d'information audité comportera diverses vulnérabilités (Web, Applicatives, 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 pour qui 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 de terrain
- mettre en pratique la partie théorique de la première journée
- élaborer un planning
- aider les stagiaires à trouver et exploiter les vulnérabilités présentes
- formater les découvertes faites en vue d'en faire un rapport pour le client

Suite...

PROGRAMME

JOUR 5

Le dernier jour sera consacré au rapport. La rédaction de ce dernier et les méthodes de transmission seront abordées.

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
- Description des vulnérabilités trouvées

Transmission du rapport
- Précautions nécessaires
- Méthodologie de transmission de rapport
- Que faire une fois le rapport transmis ?

PROCHAINES DATES

4 avr. 2022,
17 oct. 2022

OBJECTIFS

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

INFORMATIONS GÉNÉRALES

Code : PNT
Durée : 5 jours
Prix : 3 350 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP et HTTP(S)
- Connaissances des systèmes Windows et Linux et des bases de données
- Notions de développement Web

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement virtualisé Windows de démonstration (Windows 2003...) et Linux
- Chaque participant a accès à une infrastructure virtualisée permettant l'émulation de systèmes d'exploitation modernes
- Le test d'intrusion s'effectue sur un SI simulé et mis à disposition des participants

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 y étudierez le déroulement d'un audit, aussi bien d'un côté méthodologique que d'un côté technique. Les différents aspects d'une analyse seront mis en avant à travers plusieurs exercices pratiques.
Cette formation est destinée aux personnes qui souhaitent pouvoir effectuer des tests techniques lors d'un audit ou d'un déploiement de sites Web.

PROGRAMME

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

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

JOUR 1

Introduction
- Rappel méthodologie d'audit
  - Boite noire
  - Boite grise
- Plan d'action
  - Prise d'information
  - Scan
  - Recherche et exploitation de vulnérabilités
  - Rédaction du rapport

Reconnaissance
- Reconnaissance passive
  - Base de données WHOIS
  - Services en ligne
    - Netcraft
    - Robtex
    - Shodan
    - Archives
  - 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
- Contremesures
  - Limiter l'exposition réseau
  - Filtrer les accès aux pages d'administration et aux pages sensibles
  - Remplacer les messages d'erreurs verbeux par des messages génériques

Scan
- Les différents types de scanner
  - Scanner de ports
  - Scanner de vulnérabilité
  - Scanners dédiés
- Limites des scanners

JOUR 2

Vulnérabilités
- Vulnérabilités de conception
  - Politique de mise à jour
  - Chiffrement des communications
  - Politique de mot de passe
    - Mots de passe par défaut
    - Mots de passe faibles
    - Stockage des mots de passe
  - Isolation intercomptes
    - Accès aux données d'autres utilisateurs
    - Modification d'informations personnelles
  - Gestion des sessions
    - Sessions prédictibles
    - Session transitant dans l'URL
  - Contremesures
    - Mise à jour des applications et des systèmes
    - Chiffrement des communications
    - Utilisation et stockage des mots de passe
    - Vérification des droits utilisateurs
    - Système de session non prédictible avec une entropie élevée
    - Drapeaux des cookies

Vulnérabilités Web
- Mise en place d'une solution de Proxy (Burp Suite)
- Cross-Site Scripting (XSS)
  - XSS Réfléchie
  - XSS Stockée
  - XSS Dom-Based
  - Contournement des protections
  - Démonstration avec l'outil d'exploitation BeEF
  - Contremesures
- Cross-Site Request Forgery (CSRF)
  - Exploitation d'un CSRF
    - Requête HTTP GET
    - Requête HTTP POST
  - Contremesures
- Injection SQL
  - Injection dans un SELECT
  - Injection dans un INSERT
  - Injection dans un UPDATE
  - Injection dans un DELETE
  - Technique d'exploitation - UNION
  - Technique d'exploitation - Injections booléennes
  - Technique d'exploitation - Injection dans les messages d'erreurs
  - Technique d'exploitation - Injection par délais
  - Technique d'exploitation - Injection dans des fichiers
  - Exemple d'utilisation avec SQLMap
  - Contremesures
- Injection de commandes
  - Chainage de commandes
  - Options des commandes
  - Exploitation
  - Exemple d'exploitation avec commix
  - Contremesures
- Service Side Includes (SSI)
  - Exemples d'attaques
  - Contremesures
- Injection d'objet
  - Exploitation
  - Contremesures

Suite...

PROGRAMME

JOUR 3

Vulnérabilités Web (suite)

- Inclusion de fichier
  - Inclusion de fichiers locaux (LFI)
  - Inclusion de fichiers distants (RFI)
  - Contremesures
- Envoi de fichier (Upload)
  - Exploitation basique
  - Vérification de Content-type
  - Blocage des extensions dangereuses
  - Contremesures
- XML External Entity (XXE)
  - Les entités
    - Entités générales
    - Entités paramètres
    - Entités caractères
    - Entités externes
  - Découverte de la vulnérabilité
  - Exploitation de la vulnérabilité
  - Contremesures
- Service Side Template Injection (SSTI)
  - Exemple d'utilisation de Twig
  - Exemple d'exploitation sur Twig
  - Exemple d'exploitation sur Flask
  - Contremesures

Challenge final

- Mise en situation d'audit d'une application Web

PROCHAINES DATES

21 mars 2022,
13 juin 2022,
7 nov. 2022

OBJECTIFS

- Comprendre les méthodes de prise d'information
- Prendre en main l'outil Burp Suite
- Comprendre les attaques XSS et CSRF
- Mettre en pratique les attaques par injection
- Exploiter les Inclusions et l'envoi de fichiers (LFI/RFI)
- Comprendre et exploiter les XXE et SSTI
- Appliquer l'ensemble des attaques abordées durant les précédents jours sur un nouveau scénario dédié

INFORMATIONS GÉNÉRALES

Code : AUDWEB
Durée : 3 jours
Prix : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Consultants en sécurité
- Développeurs
- Ingénieurs / Techniciens

PRÉ-REQUIS

- Maîtrise des protocoles réseaux TCP/IP et HTTP/HTTPS
- Connaissances sur le développement Web et le fonctionnement des applications Web
- Connaissance des systèmes Linux et Windows.

RESSOURCES

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

MENER UN AUDIT DE SÉCURITÉ : MÉTHODE D'AUDIT D'UN SI

Mettez en place des audits de sécurité de qualité au sein de votre SI

Code : AUDSI

Aujourd'hui, pour affirmer avoir un niveau de protection suffisant sur l'ensemble de son infrastructure, il est nécessaire de réaliser des audits.
Ce cours a pour objectif d'illustrer toutes les méthodes pour éprouver les systèmes avec l'ensemble des attaques connues. Mener un audit impose des règles et des limitations qu'il est nécessaire de connaître. Cette formation décrit les différentes méthodologies d'audit ainsi que leur particularité.

Une présentation des outils indispensables ainsi que des travaux pratiques pour comprendre et connaître leur utilisation sera faite. Pour finir une étude de cas de systèmes vulnérables sera étudiée pour illustrer les principales vulnérabilités rencontrées et comment l'évaluation d'une vulnérabilité est faite en fonction de son impact, de sa potentialité.

PROGRAMME

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

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

JOUR 1

Introduction aux tests d'intrusion
- Définition du test d'intrusion
- L'intérêt du test d'intrusion
- Les phases d'un test d'intrusion
  - Reconnaissance
  - Analyse des vulnérabilités
  - Exploitation
  - Gain et maintien d'accès
  - Comptes rendus et fin des tests

Règles et engagements
- Portée technique de l'audit
  - Responsabilité de l'auditeur
  - Contraintes fréquentes
  - Législation : articles de loi
  - Précautions usuelles

Les types de tests d'intrusion
- Externe
- Interne

Méthodologie
- Utilité de la méthodologie
- Méthodes d'audit
- Méthodologies reconnues

Particularités de l'audit
- d'infrastructure classique
- d'infrastructure SCADA
- web
- de code

JOUR 2

Les outils d'audit de configuration (SCAP, checklists, etc.)

Les outils d'audit de code
- Outils d'analyse de code
- Outils d'analyse statique
- Outils d'analyse dynamique

Les outils de prise d'information
- Prise d'information
  - Sources ouvertes
  - Active
- Scanning
  - Scan de ports
  - Scan de vulnérabilités

Les outils d'attaque
- Outils réseau
- Outils d'analyse système
- Outils d'analyse web
- Frameworks d'exploitation
- Outils de maintien d'accès

JOUR 3

Étude de cas
- Application de la méthodologie et des outils sur un cas concret

Les livrables
- Évaluation des risques
- Impact, potentialité et criticité d'une vulnérabilité
- Organiser le rapport
- Prestations complémentaires à proposer

PROCHAINES DATES

2 mai 2022,
5 sept. 2022,
28 nov. 2022

OBJECTIFS

- Délimiter un audit, connaître les méthodes existantes
- Connaître les règles et les engagements d'un audit, et ses limitations
- Connaître les méthodologies reconnues
- Mettre en place une situation d'audit
- Savoir quels sont les outils nécessaires pour réaliser un audit

INFORMATIONS GÉNÉRALES

Code : AUDSI
Durée : 3 jours
Prix : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Consultants en sécurité
- Ingénieurs / Techniciens
- Développeurs

PRÉ-REQUIS

- Niveau cours HSF/HSA
- Connaissance des systèmes Linux et Windows

RESSOURCES

- Support de cours
- 1 PC par personne / Internet
- 70% de pratique
- Environnement Windows de démonstration (Windows XP, W7, 2008...) et Linux (Kali, Debian)

RECHERCHE ET EXPLOITATION DE VULNÉRABILITÉS : SUR APPLICATIONS ANDROID

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

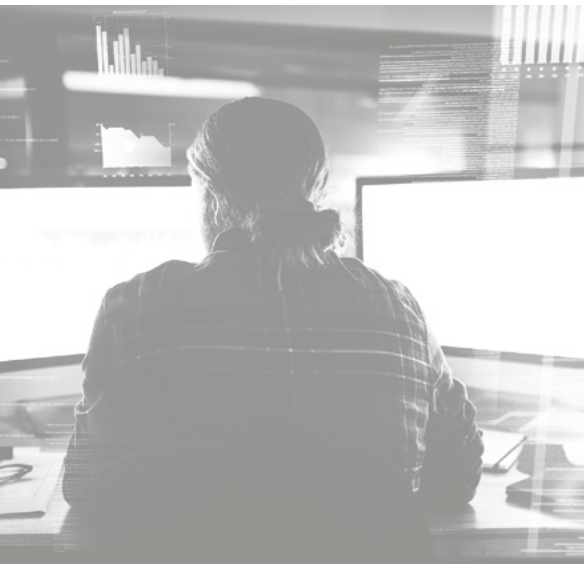
Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur une application mobile Android.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise.
Vous y étudierez l'organisation et les procédures à respecter lors de la mise en place d'un tel audit, ainsi que les différentes approches possibles lors de l'analyse d'une application Android d'un point de vue sécurité.

Code : REVA

PROGRAMME

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

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



JOUR 1

Introduction au système Android
- Modèle de sécurité d'Android
- Permissions
- Anatomie d'une application
- Manifeste d'application
- Activités et Intents
- Utilisation de Content Providers
- Stockage de fichiers sur carte SD

Présentation des outils d'analyse
- Le SDK Android
- ADB (Android Debug Bridge)
- JADX
- Drozer

JOUR 2

Préparation à l'analyse
- Installation du SDK
- Déploiement d'une autorité de certification sur Burp Suite

Prise d'information
- Découverte de l'activité principale
- Récupération d'informations concernant l'API utilisée
- Récupération d'informations depuis les fichiers de logs

Attaque de l'API
- Cross-Site Scripting
- Injection de code SQL

JOUR 3

Attaque de l'API (suite)
- Isolation de comptes utilisateur
- Chiffrement des communications
- Gestion des sessions

Reverse Engineering
- Analyse statique via JADX
- Récupération des points d'entrée de l'API
- Analyse des algorithmes de chiffrement utilisés
- Emplacement de stockage des données (local, carte SD)
- Type de données stockées
- Mots de passe présents dans le code source
- Utilisation d'intents en broadcast

PROCHAINES DATES

9 mars 2022,
30 mai 2022,
5 sept. 2022,
28 nov. 2022

OBJECTIFS

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

INFORMATIONS GÉNÉRALES

Code : REVA
Durée : 3 jours
Prix : 2 600 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Ingénieurs / Techniciens
- Responsables techniques
- Consultants sécurité

PRÉ-REQUIS

- Connaissances en Web
- Connaissances en sécurité

RESSOURCES

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

PYTHON POUR LE PENTEST

Développement et exploitation avec Python pour le Pentest

Code : PYTPEN

Cette formation destinée aux personnes ayant déjà une connaissance basique du langage Python, arbore les di!érents modules et cas d'utilisation de Python lors de tests d'intrusions.
Nous verrons de nombreuses problématiques rencontrées lors d'audits et les solutions pouvant être mises en place rapidement grâce au scripting Python afin d'automatiser les tâches complexes et spécifiques

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 en fin de module par le formateur.

JOUR 1

Python pour le HTTP, requests
- Développement d'un système de recherche exhaustive
- Contournement de captcha

Développement d'un module Python BurpSuite
- Introduction à BurpSuite
- Développement d'un module de détection passif de Web Application Firewalls

Exploitation d'une injection SQL en aveugle
- Extraction bit à bit et analyse comportementale

JOUR 2

Python et l'altération http
- Introduction à MITMProxy
- Développement d'un module «SSL Striping»

Python et le forensics
- Volatility
- Hachoir
- Network Forensics avec Scapy

JOUR 3

Le C et Python, Cython
- ctypes
- Développement d'un module Cython Antivirus et Backdoors

Antivirus et Backdoors
- Shellcodes
- Création d'une porte dérobée avancée

JOUR 4

Chaîne d'exploitation
- Exploitation de multiples vulnérabilités
- Création d'un exploit complet (POC)

TP Final
- Capture the Flag

FORMATION SUR DEVIS

OBJECTIFS

- Faciliter le développement d'exploits en Python
- Automatiser le traitement de tâches et automatiser les exploitations
- Contourner les solutions de sécurité
- Interfacer différents langages avec Python

INFORMATIONS GÉNÉRALES

Code : PYTPEN
Durée : 4 jours
Prix : Sur devis
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

- Connaissances en Python

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne / Internet
- Machine virtuelles Windows/Linux

HACKING & SÉCURITÉ : EXPERT V4

Une analyse poussée de l'attaque pour mieux vous défendre

Code : HSE

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

Cette formation porte également sur une analyse poussée des vulnérabilités.

Cette formation est particulièrement destinée aux consultants, administrateurs et développeurs qui souhaitent pouvoir effectuer des tests techniques évolués lors de leurs audits sur les systèmes internes ou externes, ou pour appliquer des solutions de sécurité adaptées à leur SI.

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's, cas pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Réseau
- Options avancées de Nmap + NSE
- Scapy
- IPv6 - mitm6
- HSRP / VRRP
- Introduction à la sécurité des protocoles de routage (OSPF, BGP, etc.)

JOUR 2

Système
- Exploitation avancée avec Metasploit
- Attaque d'une infrastructure Microsoft (Responder / Pass-The-Hash / CME / ntlmrelayx)
- Elévation de privilèges
- Techniques de contournements d'AV

JOUR 3

Applicatif
- Introduction aux Buffer Overflows 32-bits
- Exploitations basiques de débordement de tampon en 32-bits
- Exploitation via Ret2Libc (32-bits et 64-bits)
- Introduction et exploitation via ROP
- Exploitation de débordement de tampon sous Windows
- Protections contre les Buffer Overflows

JOUR 4

Web
- SQL injection avancées
- XXE
- SSRF
- Injection d'objets / Deserialization
- Exploitation sur NodeJS
- etc.

JOUR 5

CTF final
- CTF sur une journée avec TP MALICE

PROCHAINES DATES

11 avr. 2022,
20 juin 2022,
26 sept. 2022,
21 nov. 2022

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 overflow) et le mettre en pratique
- Appliquer l'ensemble des attaques abordées durant les précédents jours sur un nouveau réseau

INFORMATIONS GÉNÉRALES

Code : HSE
Durée : 5 jours
Prix : 3 900 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

- Avoir suivi la formation HSA ou une formation équivalente
- Maîtrise des protocoles réseaux
- Maîtrise des systèmes Windows et Linux
- Savoir développer des scripts
- Connaissances sur le développement Web et le fonctionnement des applications Web
- Connaissances en cryptographie.

RESSOURCES

- Support de cours
- 1 PC par personne / Internet
- Environnement Windows de démonstration (Windows XP, 2000, 2003 ...), et Linux
- Metasploit

BOOTCAMP EXPLOITATION DE VULNÉRABILITÉS APPLICATIVES

Maîtrisez l'ensemble des techniques d'exploitation applicatives

Code : BEVA

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 en situation concrète.
Ce bootcamp est particulièrement destiné aux consultants souhaitant approfondir leurs connaissances des techniques d'exploitation de vulnérabilités applicatives ainsi que des mécanismes de protection associés. De bonnes connaissances en C, Python et assembleur sont requises.

PROGRAMME

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

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

JOUR 1

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
- Contremesures actuelles

JOUR 5

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

PROCHAINES DATES

20 juin 2022,
21 nov. 2022

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 : 3 500 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Pentesters

PRÉ-REQUIS

- Notions de sécurité informatique
- Maîtrise des systèmes Windows et Linux
- Connaissance des architectures IA 32 et IA 64
- Savoir développer des scripts.

RESSOURCES

- Notions de sécurité informatique
- Maîtrise des systèmes Windows et Linux
- Connaissance des architectures IA 32 et IA 64
- Savoir développer des scripts.

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's, cas pratiques) et formalisés sous forme de grille d'évaluation des compétences 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 : rotection 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

28 mars 2022,
30 mai 2022,
24 oct. 2022

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 : 3 700 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)
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

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

RESSOURCES

- Support de cours en français
- Cours donné en français

INFORENSIQUE

Les formations du domaine Inforensique offrent un panel de compétences techniques et organisationnelles pour analyser en profondeur un incident de sécurité et y réagir avec les mesures responsables ou intervenant technique en sécurité, système ou de type SOC (Security Operating Center), CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team).

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
AIARI	**Analyse inforensique avancée et réponse aux incidents**	3 jours				4			4				7	
CHFIv10	**Computer Hacking Forensic Investigator v10**	5 jours	24				2			22		24		
RILM	**Rétro-Ingénierie de Logiciels Malfaisants**	5 jours			14		30				26			
MDIE	**Malwares: Détection, Identification et Éradication**	3 jours	24			11				22				

COMPUTER HACKING FORENSIC INVESTIGATOR V10

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

Code : CHFI

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 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 dans les locaux de SysDream.
Il est également possible de passer l'examen depuis le lieu de votre choix grâce à la surveillance de votre examen en ligne (en option) mais il faudra alors en faire la demande au moment de votre inscription à la formation.

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

- **Titre de l'examen :** CHFI 312-49
- **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'information, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

2 mai 2022,
22 août 2022,
24 oct. 2022

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 312-49

INFORMATIONS GÉNÉRALES

Code : CHFI
Durée : 5 jours
Prix : 3 900 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)
Examen CHFI : inclus. Valable 10 mois pour un passage de l'examen dans les locaux de SysDream. Passage de l'examen à distance depuis le lieu de votre choix disponible en option. Formation certifiante.

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

- Connaissances basiques en cyber sécurité 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 donné en français
- 20% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement Windows de démonstration et de mise en pratique

FORMATIONS ASSOCIÉES

- Rétro-Ingénierie de Logiciels Malveillants
- Malwares : détection, identification et éradication v2

MALWARES : DÉTECTION, IDENTIFICATION ET ÉRADICATION V2

Apprenez à connaître les malwares, leurs grandes familles, à les identifier et 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 S.I. Des bonnes pratiques et outils adaptés seront abordés tout au long de la formation, et mis en pratique lors des travaux dirigés.

Code : MDIEv2

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 en fin de module par le formateur.

JOUR 1

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

Éradication réponse à incident
- Processus inforensique et analyste de logiciels malveillants
- Réponse à incident 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

11 avr. 2022,
22 août 2022

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 : MDIEv2
Durée : 3 jours
Prix : 2 250 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

- Notions de sécurité informatique
- Maîtrise des systèmes Windows et Linux
- Connaissance des protocoles réseaux TCP/IP
- Connaissances en développement

RESSOURCES

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

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 à incidents d'un point de vue organisationnel.

Vous étudierez également les méthodologies et outils appropriés utilisés dans la phase technique de la réponse à incident, 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 en fin de module par le formateur.

JOUR 1

Les bases de la réponse à incident et de l'analyse inforensique

- Mise en place de la réponse à incident
  - Préparation à la réponse à incident
  - Détection et analyse
  - Classification et classement par ordre de priorité
  - Notification
  - Confinement
  - Investigation inforensique
  - Éradication et reprise d'activité
- L'analyse inforensique et la législation française
- 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 d'attaques réseaux
  - Les sources de capture
  - Revue d'attaques répandues
- Récupération et analyse d'une capture de mémoire vive (Volatility)

JOUR 3

Analyses ciblées et exercices avancés

- Analyse des fichiers de journaux et corrélation d'événements
  - Approche manuelle
  - Utiliser un indexeur (ELK)
- Analyse inforensique des navigateurs
- Analyse inforensique des e-mails

Mise en pratique sur des cas concrets.

PROCHAINES DATES

4 avr. 2022,
4 juil. 2022,
7 nov. 2022

OBJECTIFS

- Être capable de définir et mettre en place un processus de réponse à incident 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 : 2 500 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (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

- Bonne culture générale en informatique
- Maîtrise de Linux (administration, commandes et programmation shell)
- Connaissance générale des attaques et vulnérabilités (des rappels pourront être effectués)
- Connaissances générales en administration Windows

RESSOURCES

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

RÉTRO-INGÉNIERIE DE LOGICIELS MALVEILLANTS

Créez votre laboratoire d'analyse de malwares et comprenez leur fonctionnement en plongeant dans leur code.

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 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

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

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

Variété des systèmes

Services usuels
- Partage de fichiers
- Services IRC (C&C)

Licensing
- Importance des licences

JOUR 2

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

Installation de Cuckoo/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 Pro
- Utilisation d'IDA Pro
  - 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
  - Zim
- Analyse sous débogueur
  - Step into/Step over
  - Points d'arrêts logiciels et matériels
  - Fonctions systèmes à surveiller
  - Génération pseudo-aléatoire de noms de 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

Suite...

PROGRAMME

JOUR 5

Analyse de documents malveillants

- Fichiers PDFs
  - Introduction au format PDF
  - Spécificités
  - Intégration de JavaScript et possibilités
  - Exemples de PDFs malveillants
  - Outils d'analyse: Origami, Editeur hexadécimal
  - Extraction de charge
  - Analyse de charge
- Fichiers Office (DOC)
  - Introduction au format DOC/ DOCX
  - Spécificités
  - Macros
  - Objets Linking and Embedding (OLE)
  - Outils d'analyse: Oledump, Editeur hexadécimal
  - Extraction de code malveillant
  - Analyse de la charge
- Fichiers HTML malveillants
  - Introduction au format HTML
  - Code JavaScript intégré
  - Identification de code JavaScript malveillant
  - Outils d'analyse: éditeur de texte
  - Désobfuscation de code
  - Analyse de charge

PROCHAINES DATES

14 mars 2022,
30 mai 2022,
26 sept. 2022

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 : 3 500 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Techniciens réponse aux incidents
- Analystes techniques
- Experts sécurité

PRÉ-REQUIS

- Connaissance du système Microsoft Windows
- Maîtrise du langage assembleur 32 et 64 bits
- Maîtrise de l'architecture 32 et 64 bits Intel

RESSOURCES

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

MANAGEMENT

Le management de la Sécurité s'adresse aux responsables d'un système d'information souhaitant mettre en place, ou faire évoluer, une organisation de travail optimisée face aux menaces informatiques contemporaines. Nos formations proposent des démarches organisationnelles et de gestion de risque clés en main, en s'appuyant sur des certifications et des normes internationalement reconnues.

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
ISO 27001 LI	ISO27001: Certified Lead Implementer	5 jours		28			9				12			5
ISO 27001 LA	ISO27001: Certified Lead Auditor	5 jours			7		30				19			12
ISO 27005 + EBIOS	ISO 27005: Certified Risk Manager avec Méthode EBIOS	5 jours				4		20				3	28	
ECIHv2	EC-Council Certified Incident Handler v2	3 jours				25			6				7	
CISM	Certified Information Security Manager	3 jours			14		2				12			
CISSP	Certified Information Systems Security Professional - Cours format papier	5 jours	24		7	25	30		4	29	26		14	12
CISSP IPAD	Certified Information Systems Security Professional - Cours sur IPAD	5 jours	24		7	25	30		4	29	26		14	12
CCISOv3	Certified Chief Information Security Officer	4 jours					9						21	

Session hybride

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 d'informations 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 matin
  - Format : examen écrit
  - Durée : 3h
  - Langue : disponible en français
- Il remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program). L'examen 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

Suite...

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 relatives au niveau de qualification choisi.
- Pour plus d'information à ce sujet, vous pouvez consulter le site de PECB.

PROCHAINES DATES

28 fevr. 2022,
9 mai 2022,
12 sept 2022,
5 déc. 2022

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
Prix : 3 450 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

Examen ISO : inclus. Passage de l'examen le dernier jour de la formation. Formation certifiante.

PUBLIC VISÉ

- Les gestionnaires de projets ou les consultants voulant préparer et gérer une structure dans la mise en œuvre et la gestion des systèmes de sécurité d'informations
- Les auditeurs ISO 27001 qui souhaitent comprendre pleinement les systèmes de sécurité d'informations 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 qui veulent 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

- 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

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. A 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 matin.
  - Format : examen écrit
  - Durée : 3h
  - Langue : disponible en français
- Il remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program). L'examen 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 au niveau de qualification choisi. Pour plus d'information à ce sujet, vous pouvez consulter le site de PECB.

PROCHAINES DATES

7 mars 2022,
30 mai 2022,
19 sept 2022,
12 déc. 2022

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

Prix : 3 450 € HT

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

Lieu : Levallois-Perret (92)

Examen ISO : inclus. Passage de l'examen le dernier jour de la formation. Formation certifiante.

PUBLIC VISÉ

- Auditeurs internes
- Auditeurs cherchant à réaliser et à mener des audits dans les systèmes de sécurité d'informations
- Gestionnaires de projets ou consultants souhaitant maîtriser les audits des systèmes de sécurité d'informations
- 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

- 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

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 au niveau de qualification choisi.
- Pour plus d'information, vous pouvez consulter le site de PECB.
- 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 au niveau de qualification choisi.
  Pour plus d'information, vous pouvez consulter le site de PECB.

PROCHAINES DATES

4 avr. 2022,
20 juin 2022,
3 oct. 2022,
28 nov. 2022

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
Prix : 3 450 € HT
Horaires : 9h30 - 17h30
Examen ISO : inclus. Passage des examens 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

- Connaissance de base sur la gestion du risque

RESSOURCES

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

EC-COUNCIL CERTIFIED INCIDENT HANDLER V2

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

Code : ECIHv2

Le programme ECIHv2 propose une approche holistique qui couvre de nombreux concepts autour de la réponse et de la gestion d'incident.
Cela va de la préparation et 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 ECIHv2 d'être une des plus complètes sur le marché aujourd'hui, dans le domaine de la réponse et gestion d'incident.
Les compétences acquises dans le programme ECIHv2 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 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

CERTIFICATION ECIH (INCLUSE AVEC LA FORMATION)

Présentation : L'examen ECIH (212-89) aura lieu dans les locaux de SysDream.
Il est également possible de passer l'examen depuis le lieu de votre choix grâce à la surveillance de votre examen en ligne (en option) mais il faudra alors en faire la demande au moment de votre inscription à la formation. 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'information, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

25 avr.. 2022,
6 juil. 2022,
7 nov. 2022

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 : ECIHv2
Durée : 3 jours
Prix : 2 500 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)
Examen ECIH : inclus. Valable 10 mois pour un passage de l'examen dans les locaux de SysDream. Passage de l'examen à distance depuis le lieu de votre choix disponible en option. Formation certifiante.

PUBLIC VISÉ

- gestionnaires d'incidents
- administrateurs d'évaluation des risques
- pentesteurs
- cyber-enquêteurs judiciaires
- consultants en évaluation de vulnérabilité
- 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

- Connaissances générales en réseau et en sécurité

RESSOURCES

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

CERTIFIED INFORMATION SECURITY MANAGER

Préparation à la certification CISM ®

Code : 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 donc la totalité du cursus CBK (Common Body of Knowledge), le tronc commun de connaissances en sécurité défini par l'ISACA.

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 de programme 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

14 mars 2022,
2 mai 2022,
12 sept. 2022

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 : 3 jours
Prix : 3 100 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)
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

- 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'informations. Des dérogations sont néanmoins possible pour un maximum de 2 ans

RESSOURCES

- Cours délivré 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 IT et notamment pour avoir certifié plus de 100 000 personnes 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 sommes dévoués à votre réussite à l'obtention de la certification CISSP. Pour ceci, 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.

Découverte des thèmes, domaines et rubriques de la CBK® (Common Body of Knowledge) et révision en profondeur des fondamentaux de la sécurité des SI. 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 8th 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 est disponible en option et 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. Dans les autres langues, les examens CISSP sont gérés de façon linéaire et fixe.

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

25 avr. 2022,
30 mai 2022,
4 juil. 2022,
29 août 2022
26 sept. 2022,
14 nov. 2022,
12 déc. 2022

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 avec cours au format papier : 3 500 € HT

Prix avec iPad Air 3 (cours au format papier + version électronique du cours sur iPad) : 3 900 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois-Perret (92)

Examen CISSP : disponible 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), le CISSP®
- Non experts, 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 tire Associate of (ISC)2. Il aura alors jusqu'à 6 ans pour acquérir les 5 années d'expérience requises

RESSOURCES

- Cours donné en français
- Support de cours de l'Université de Dallas
- Le CISSP All-in-One Exam Guide 8th Edition
- Le CISSP Practice Exams 5th Edition

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

La certification des RSSI

Code : CCISO

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

PROGRAMME

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

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

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

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

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

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

Domaine 3 – Gestion et Opérations des Projets Technologiques

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

Domaine 4 –Compétences principales en SI

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

Domaine 5 –Planification stratégique et financière

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

Suite...

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

PROGRAMME

CERTIFICATION

Passage de l'examen

L'examen s'effectuera en ligne sur la plate-forme ECC pour un passage dans les locaux de SysDream.
Il est également possible de passer l'examen dans un centre de test Pearson Vue(en option). Dans le cas où vous ne souhaiteriez pas passer l'examen dans les locaux de SysDream, il faudra donc le spécifier lors de votre inscription à la formation.

EXAMEN CISO

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

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

EXAMEN EISM

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

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

Une fois les 5 années d'expérience acquises, le candidat pourra s'inscrire à l'examen CCISO à moindre coût, les certifiés EISM étant éligibles à une remise sur l'examen CCISO.

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'information, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

9 mai 2022,
21 nov. 2022

INFORMATIONS GÉNÉRALES

Code : CCISO
Durée : 4 jours
Prix : 3 700 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

Examen CCISO : inclus.

Valable 10 mois et uniquement dans les locaux de SysDream. Disponible en option pour un passage hors de nos locaux. Formation certifiante.

OBJECTIFS

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

PUBLIC VISÉ

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

PRÉ-REQUIS

- Pour passer la certification, il faudra justifier de 5 ans d'expérience professionnelle dans au moins 3 des 5 domaines. Le candidat devra remplir les conditions requises via l'EC-Council's Exam Eligibility
- Un stagiaire n'ayant pas cette expérience ou n'ayant pas rempli sa demande pourra passer l'examen EC-Council Information Security Manager (EISM). Une fois les 5 années d'expérience acquises, le candidat pourra s'inscrire à l'examen CCISO.

RESSOURCES

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

SÉCURITÉ DÉFENSIVE

Les formations de Sécurité Défensive fournissent des éléments de sécurisation concrets et techniques sur les briques essentielles d'un système d'information. Elles sont ouvertes à tout personnel technique et couvrent les principaux domaines : Réseau, Système, Développement Logiciel et Supervision de la Sécurité.

PLANNING DES FORMATIONS

			JANV	FEV	MARS	AVR	MAI	JUIN	JUIL	AOUT	SEPT	OCT	NOV	DEC
SL	**Sécurisation Linux**	3 jours	18			20				30		25		
SW	**Sécurisation Windows**	3 jours		7				8				3		
SR	**Sécurisation des Réseaux**	3 jours		7						29		24		
CSA	**Certified Soc Analyst**	3 jours			2			8						6
SDS	**Sensibilisation au Développement Sécurisé**	2 jours		16					7					5

Formations 100% distanciel

SÉCURISATION LINUX

Protégez efficacement vos systèmes linux contre toute attaque

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. Cette formation se destine à des administrateurs, consultants souhaitant sécuriser leur SI.

PROGRAMME

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

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

JOUR 1

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
- Monotoring avec auditd
- Journaliation centralisée

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

JOUR 1

Sécurité réseau
- Firewalls
  - IPTables
    - ACCEPT/DROP/REJECT
    - Rate Limiting
    - Connection Limiting / Tracking
    - Syn Proxy
  - NFtables
- VPNs
  - 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

20 avr. 2022,
30 août 2022,
25 oct. 2022

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 : 1 950 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Administrateurs
- Ingénieurs / Techniciens
- Consultants

PRÉ-REQUIS

- Connaissances en administration Linux
- Connaissances en réseau
- Connaissances en système virtualisé

RESSOURCES

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

SÉCURISATION WINDOWS

Protégez efficacement votre infrastructure Windows

Code : SW

Ce cours vous confrontera à la mise en place de la sécurité des systèmes Windows. Il vous permettra de définir une politique de sécurité efficace en fonction des composantes du réseau d'entreprise. Les principales vulnérabilités du système et les problèmes de configuration seront étudiés et les corrections et bonnes pratiques à appliquer seront vues. Des protections mises en place par le système d'exploitation seront étudiées et analysées. La mise en place d'un domaine peut amener à des erreurs de configuration et des bonnes pratiques doivent être appliquées afin d'optimiser la protection des postes. L'utilisation des GPO permet de les appliquer de manière automatique sur l'ensemble du parc et de forcer les clients à appliquer des principes de sécurité.

PROGRAMME

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

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

JOUR 1

Introduction

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

Durcissement 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

Durcissement d'un environnement Windows
- Active Directory
  - Introduction
  - Kerberos
  - Outils d'audit
  - Stratégies de groupe
  - **LAPS**

JOUR 3

Durcissement de 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

8 juin 2022,
3 oct. 2022

OBJECTIFS

- Savoir durcir et exploiter le démarrage d'un système
- Savoir durcir et exploiter un environnement Windows
- Connaître les méthodes d'attaques d'un Active Directory et comment s'en protéger
- Savoir durcir et exploiter les services Windows

INFORMATIONS GÉNÉRALES

Code : SW
Durée : 3 jours
Prix : 1 950 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Auditeurs techniques
- Administrateurs système

PRÉ-REQUIS

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP
- Maîtrise des systèmes Windows (client et serveur) et Active Directory
- Savoir développer des scripts.

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement Windows de démonstration (Windows 7, 10, server 2016) et 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 (switch). 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 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

29 août 2022,
24 oct. 2022

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 : 1 950 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

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

PRÉ-REQUIS

- Notions de sécurité informatique
- Maîtrise des protocoles réseaux
- Maîtrise des modèles OSI et TCP/IP
- Connaissances en architecture des réseaux.

RESSOURCES

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

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 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 (Conditions de course, Timing Attacks, etc.)
- Contre-mesures et recommandations

JOUR 2 (suite)

Principales attaques sur les applications
- Débordement de tampon
- Problèmes de permissions
- Chiffrement des communications
- Contre-mesures et recommandations

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

PROCHAINES DATES

7 juil. 2022,
5 déc. 2022

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 : 1 550 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Développeurs Web et Applicatifs

PRÉ-REQUIS

- Connaissance des protocoles réseaux TCP/IP et HTTP(S)
- Connaissances sur le fonctionnement des applications Web
- Maîtrise du développement Web

RESSOURCES

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

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.

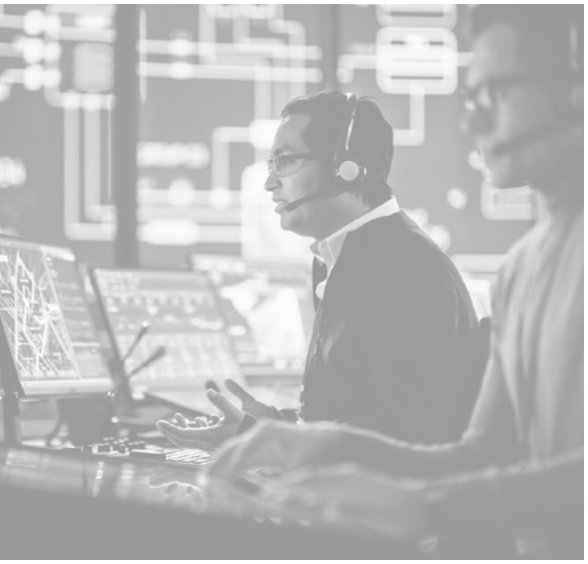
Le programme Certified SOC Analyst (CSA) est la première étape pour rejoindre un SOC - Security Operations Center.
Il est conçu pour les analystes de niveau I et II afin de leur permettre d'acquérir les compétences nécessaires pour effectuer des opérations de premier et deuxième niveau.
Le CSA est un programme de formation et d'accréditation qui aide le candidat à acquérir des compétences techniques recherchées 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.
Étant un programme intensif de 3 jours, il 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 en fin de module par le formateur, puis par la 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 (312-39) aura lieu dans les locaux de SysDream. Il est également possible de passer l'examen à distance depuis le lieu de votre choix (en option) mais il faudra alors en faire la demande au moment de votre inscription à la formation.

- **Titre de l'examen :** Certified SOC Analyst
- **Code de l'examen :** 312-39
- **Nombre de questions :** 100
- **Durée :** 3 heures
- **Score requis :** 70%

Résultat : Directement disponible en fin d'examen.

PROCHAINES DATES

2 mars 2022,
8 juin 2022,
6 déc. 2022

OBJECTIFS

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

INFORMATIONS GÉNÉRALES

Code : CSA
Durée : 3 jours
Prix : 2 450 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)
Examen CSA : inclus. Valable 10 mois pour un passage de l'examen dans les locaux de SysDream. Passage de l'examen à distance depuis le lieu de votre choix disponible en option. Formation certifiante.

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 Cybersecurité
- Professionnels cybersecurité débutants
- Quiconque voulant devenir Analyste SOC

PRÉ-REQUIS

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

RESSOURCES

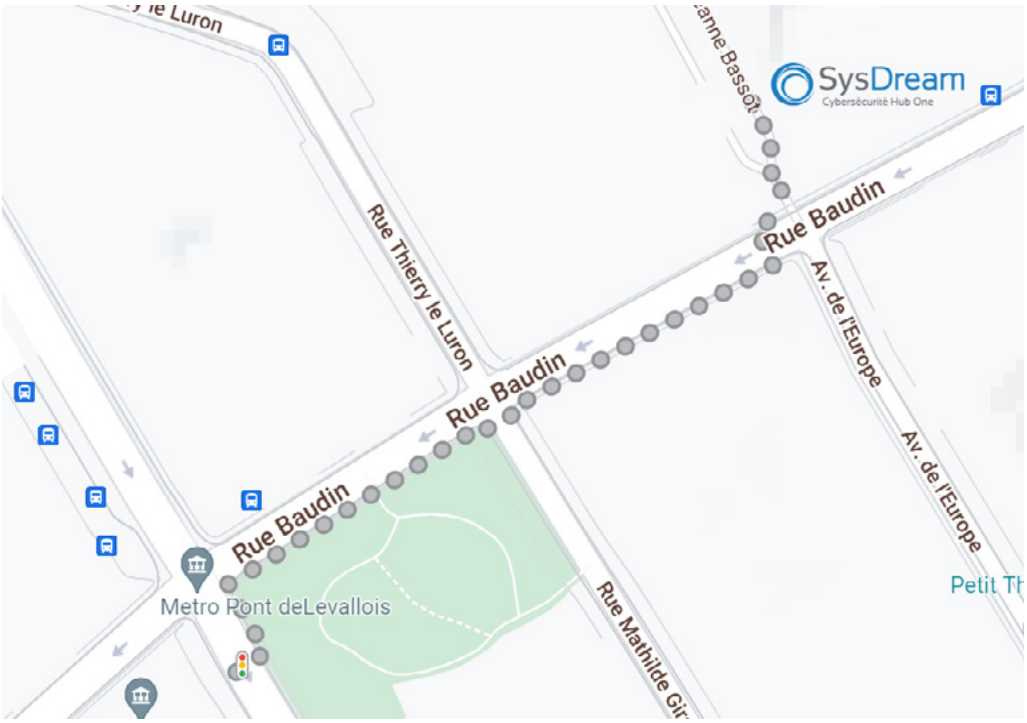
- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- 20% d'exercices pratiques
- 1 PC par personne / Internet

LE CENTRE DE FORMATION

SysDream

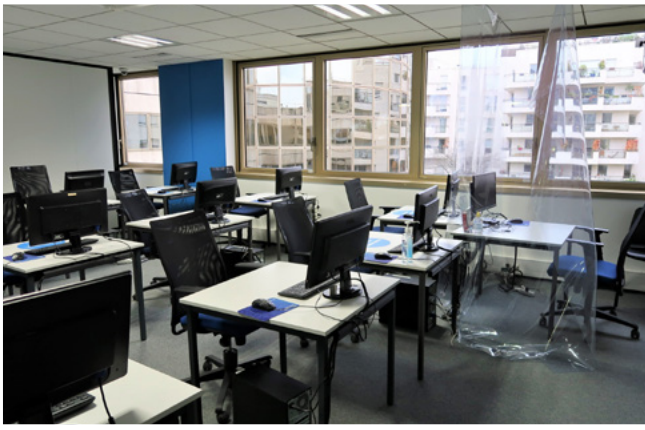
14 place Marie-Jeanne Bassot,
92300 Levallois-Perret
France

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. Toutes nos salles sont lumineuses et climatisées.



Un espace détente est mis à disposition de nos clients.

ÉVÈNEMENT SYSDREAM

SysDream organise depuis 2011 son événement Hack In Paris dans le but de rassembler, sur 5 jours, les professionnels de la Sécurité Informatique (CISO, CIO, DSI, RSSI, RSI) et experts techniques du hacking, autour de conférences internationales de haut niveau et de formations en sécurité informatique.

Retrouver le programme de cette année sur www.hackinparis.com

SysDream
Cybersécurité Hub One

SYSDREAM S.A.S

14 place Marie-Jeanne Bassot,
92300 Levallois-Perret, France

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

@sysdream