Parcours introductif à la Cybersécurité

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Fondamentaux de la cybersécurité

Rubrique : Fondamentaux

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

- Disposer d'une vision globale de la cybersécurité et son environnement (enjeux, écosystème...)
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Appréhender les métiers liés à la cybersécurité
- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifier les bonnes pratiques en matière de sécurité informatique

Public visé

- Toute personne souhaitant apprendre les fondamentaux de la sécurité informatique et/ou souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux

Pré-requis

- Connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI

PROGRAMME

Jour 1 matin (phase 1 - Etat de l'art cyber)

Chapitre 1: Les tendances de la cybercriminalité

- L'évolution de la cybercriminalité en France et dans le monde
- L'impact économique de la cybercriminalité
- Le modèle économique "Hacking as a Service"
- Caractéristiques, Coûts, Usages

Chapitre 2 : Base de la sécurité de l'information

- SSI & SI
- DICP et les critères de sécurité
- La sécurité en profondeur
- Le security by design
- Approche par les risques
- Vulnérabilités & menaces

Chapitre 3 : Gestion des cyberattaques

- Tests d'intrusion, mesure d'anticipation incontournable
- SOC (Security Operation Center)
- La gestion des incidents
- Les plans de continuité d'activité
- Métier de la gouvernance cyber

Code de formation : SECINT

€ Tarifs

Prix public : 6645 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

- **Le plan de développement des compétences** de votre entreprise : rapprochez-vous de votre service RH.
- **Le dispositif FNE-Formation**.
- **L'OPCO** (opérateurs de compétences) de votre entreprise.
- **Pôle Emploi** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
- **CPF** -MonCompteFormation

Contactez nous pour plus d'information

Lieux & Horaires

Campus : Ensemble des sites

Durée : 70 heures

Délai d'accès :
Jusqu'à 8 jours avant le début de la formation

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 23 / 09 / 2024
  : Ensemble des sites
  ✓ : Distanciel possible
  : 70 heures
  : 10 jours
- 21 / 10 / 2024
  : Ensemble des sites
  ✓ : Distanciel possible
  : 70 heures
  : 10 jours
- 21 / 10 / 2024
  : Ensemble des sites
  ✓ : Distanciel possible
  : 70 heures
  : 10 jours
- 18 / 11 / 2024
  : Ensemble des sites
  ✓ : Distanciel possible
  : 70 heures

- Les exercices Red, Blue et Purple Teaming
- Recourir à une société spécialisée de détection des incidents

Jour 1 après-midi (phase 1 - Etat de l'art cyber)

Chapitre 4 : Gestion d'incidents et riposte face à une cyberattaque

- La notion de preuve dans le monde informatique
- Recherche, collecte et structuration de preuves
- Méthodologie de gestion d'incidents
- Les CERT (Computer Emergency Response Team) : des organismes qui facilitent la tâche
- Le cadre juridique des ripostes à une cyberattaque
- Organiser et gérer une cellule de crise
- Importance de la veille en cybersécurité
- Gestion des vulnérabilités et patch management

Jour 2 matin (phase 1 - état de l'art cyber)

Chapitre 5 : Identifier les acteurs de la lutte contre la cybercriminalité

- Cyber-délits en France et Europe : quel dispositif ?
- Les services spécialisés du ministère de l'Intérieur
- OCLCTIC, BEFTI, IRCGN, BFMP, DGSI, etc.

Chapitre 6 : Les bonnes pratiques

- Gouvernance de la cybersécurité
- Défense en profondeur
- Gestion des incidents de cybersécurité

Jour 2 après-midi (phase 1 - état de l'art cyber)

Chapitre 7 : Loi, normes, référentiels, organisme qui régit la cybersécurité

- RGPD
- Article 321 du code pénal
- ISO/IEC 27001/2
- Guide d'hygiène ANSSI, CIS, MITRE
- Prestataires certifiés obligatoires (PDIS, PRIS)
- Audit de sécurité par l'ANSSI
- Auditeurs certifiés (PASSI, LPM)
- Le rôle spécifique de l'ANSSI, la CNIL, l'ARJEL et l'ENISA
- Directive européenne : Network and Information Security
- Règlement européen : Cybersecurity Act
- Loi de programmation militaire (2016)
- Les organismes de l'Union européenne
- Les associations
- Les entreprises privées au service de la lutte contre la cybercriminalité

Jour 3 matin (phase 2 - Introduction aux différents métiers du cyber offensive)

Chapitre 8 : La sécurité offensive et le pentesting

- Principes de la sécurité de l'information
- Les différentes phases d'une attaque
- Définition d'un test d'intrusion
- Aspects légaux et réglementaires liés aux tests d'intrusion
- Méthodes et framework pour un test d'intrusion

TD/ Framework pentest ESD Academy
TP 1/ Questionnaire de pré-engagement
TP 2/ Rédaction d'un contrat de pré-engagement

Chapitre 9 : Préparer son test d'intrusion

- Préparation d'une machine pour test d'intrusion
- Automatisation et scripting
- Outils matériel connus

TD/ Rubber Ducky

- Templating de documents

TD/ Suivi test d'intrusion

Chapitre 10 : Collecte d'informations

- Ingénierie des sources publiques (OSINT)

: 10 jours

- 18 / 11 / 2024
: Ensemble des sites
: Distanciel possible
: 70 heures
: 10 jours

- 16 / 12 / 2024
: Ensemble des sites
: Distanciel possible
: 70 heures
: 10 jours

- 16 / 12 / 2024
: Ensemble des sites
: Distanciel possible
: 70 heures
: 10 jours

- Relevé passif et actif d'informations sur l'organisation cible

TD/ Présentation des outils d'OSINT
TP 3/ Relevé d'informations & Reconnaissance

Jour 3 après-midi (phase 2 - Introduction aux différents métiers du cyber offensive)

Chapitre 11 : Énumération de l'infrastructure

- Énumération du périmètre
- Evasion sur infrastructure sécurisée
- Enumération des protocoles

TD/ Présentations des outils d'énumération
TP 4/ Enumération de l'infrastructure

Chapitre 12 : Analyse des vulnérabilités

- Scan de vulnérabilités
- Présentation des différents outils

TD/ Présentation OpenVAS

- Les vulnérabilités connues

TP 5/ Identification des vulnérabilités

Jour 4 matin (phase 2 - Introduction aux différents métiers du cyber offensive)

Chapitre 13 : Exploitation

- Recherche d'Exploits
- Présentation des outils/frameworks d'attaques

TD/ Présentation metasploit

- Déploiement et exécution de charges

TP 6/ Exploitation des vulnérabilités

- Écoute passive et active des infrastructures
- Bruteforcing

Jour 4 après-midi (phase 2 - Introduction aux différents métiers du cyber offensive)

Chapitre 14 : Post-Exploitation

- Désactivation des éléments de traçabilité
- Élévation de privilèges (Méthodes, outils, vulnérabilités linux, ...)
- Etude des persistances (ADS, base de registre, planificateur de tâches, services)
- Mouvements latéraux et pivoting
- Nettoyage des traces

Jour 5 matin (phase 3 - Introduction aux différents métiers du cyber défensive)

Chapitre 15 : Métiers, support de travail et référentiels

- La blue team
- Ingénieur en sécurité, intégrateur de solution, le SOC, le CSIRT
- Le SOC au coeur de la blue team
- Audit de la cybersécurité des systèmes d'information

Chapitre 16 : Durcissement des infrastructures Windows

- Durcissement des postes et serveurs
- Durcissement des protocoles réseaux
- ATA, IA et threat intelligence
- Journalisation et surveillance avancée

TP / Mettre en œuvre un renforcement de sécurité en environnement Microsoft
TP / Auditer son architecture et préparer un plan de contre mesure

Jour 5 après-midi (phase 3 - Introduction aux différents métiers du cyber défensive)

Chapitre 17 : Ouverture à l'investigation numérique avec la collecte de données

- Les outils du marché (Kape, Arsenal, FTKimager, Plaso,Hindsight..)
- Collecte des données physique et virtualisation
- Présentation du Lab
- TD / Collecte de données (En continue)

Jour 6 matin (phase 3 - Introduction aux différents métiers du cyber défensive)

Chapitre 18 : Recherche d'artefacts et reporting

- Différents artefacts internet
- Pièces jointes
- Open/Save MRU
- Flux ADS Zone.Identifier
- Téléchargements
- Historique Skype
- Navigateurs internet
- Historique
- Cache
- Sessions restaurées
- Cookies

TP / Analyse d'un disque

Jour 6 après-midi (phase 3 - Introduction aux différents métiers de la cyber défensive)

- Différents artefacts exécution
- UserAssist
- Timeline Windows 10
- RecentApps
- Shimcache
- Jumplist
- Amcache.hve
- BAM/DAM
- Last-Visited MRU
- Prefetch

TD / Chaîne de custody et création d'un rapport sur une étude de cas

Jour 7 matin (phase 4 - Introduction aux différents métiers du cyber - manager du risque)

Chapitre 19 : État de l'art du management du risque

- Quelle est la définition d'un risque
- Quelle vision du risque ?
- L'ISO 31000
- L'AMRAE, le Club EBIOS
- Qu'est-ce qu'un bon risque manager
- Sensibilisation des dirigeants aux risques cybers

Chapitre 20 : Créer un programme de gestion des risques

- L'importance de contextualiser
- Contexte interne, externe
- Recette du risque
- Assets
- Vulnérabilités
- Menaces
- Mesures
- Scénarios

TP / À l'aide d'une étude de cas, identifier les scénarios de risques, vulnérabilités, menaces

Jour 7 après-midi (phase 4 - Introduction aux différents métiers du cyber - manager du risque)

Chapitre 21 : Analyser et estimation des risques

- Approche qualitative vs quantitative
- Les différentes méthodes de calcul des risques
- Calcul des risques

TP / À l'aide d'une étude de cas, analyser et estimer les scénarios de risques

Jour 8 matin (phase 4 - Introduction aux différents métiers du cyber - manager du risque)

Chapitre 22 : EBIOS

- Différence entre EBIOS 2010 et EBIOS Risk Manager
- Notions de socle de sécurité
- Visions ateliers
- Les 5 ateliers

Chapitre 23 : MEHARI

- Le CLUSIF
- Fonctionnement de MEHARI
- Les différentes phases de la méthode MEHARI

Chapitre 24 : OCTAVE

- Les trois phases d'OCTAVE
- Vue organisationnelle : création des profils de menaces sur les biens de l'entreprise ;
- Vue technique : identification des vulnérabilités d'infrastructure ;
- Développement de la stratégie : analyse de risques, mise en place des mesures de sécurité.

Jour 8 après midi (phase 4 - Introduction aux différents métiers du cyber - manager du risque)

Chapitre 25 : la méthode Bow-tie

- Représenter les relations entre les dangers leurs causes et leurs effets ;
- Évaluer la contribution de chaque cause et la gravité de chaque risque ;
- Positionner des barrières de prévention et de protection ;
- Évaluer les facteurs aggravants diminuant l'efficacité des barrières ;
- Évaluer la robustesse et la contribution des barrières à l'atténuation des risques ;
- Évaluer l'impact de ces barrières sur la cotation générale du risque.

Jour 9 matin (phase 5 - Introduction aux différents métiers du cyber - assistance à RSSI)

Chapitre 26 : métier de RSSI (responsable de la sécurité des systèmes d'information)

- Les différentes tâches d'un RSSI
- RSSI et non directeur cyber
- Les associations des RSSI
- Quelle fonction pour l'assistant RSSI
- Conformité et gestion des risques

Chapitre 27 : Savoir interpréter les référentiels, normes du marché

- ISO/IEC 27001/2
- Quelle méthode de travail pour implémenter la norme ISO
- Gestion des risques et programme de GdR
- Comment monter une PSSI (politique de sécurité de l'information

TD / exemple de PSSI

Jour 9 après-midi (phase 5 - Introduction aux différents métiers du cyber - assistance à RSSI)

Chapitre 28 : NIST Cybersecurity framework

- Les phases et les activités du NIST CF
- Identify
- Protect
- Detect
- Respond

Jour 10 matin (phase 5 - Introduction aux différents métiers du cyber - assistance à RSSI)

Chapitre 29 : Guide d'hygiène de l'ANSSI

- 42 règles de sécurité
- Comment identifier la maturité

TP / Créer un fichier de suivi

- Modèle de maturité avec CMMI
- Recommandations de l'ANSSI
- Comprendre les schémas de labellisation

Jour 10 après-midi (phase 5 - Introduction aux différents métiers du cyber - assistance à RSSI)

Chapitre 30 : Création d'un tableau de bord

- Quels indicateurs
- Maturity model vs process model
- Créer ses outils de veille

Chapitre 31 : Quid de la gouvernance du DevOps

- Quel modèle pour la sécurité application
- SDLC de Microsoft
- Stride, threat modeling et approche SSI du Devsec
- Les outils
- L'OWASP ASVS, SAM, code review

Chapitre 32 : La sécurité du monde industriel

- Les enjeux
- Différences entre SIE et SII
- Recommandations de l'ANSSI pour les indus
- Mode opératoire des attaquants et APT sur les réseaux industriels

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels

Méthode

Fin de formation : entretien individuel
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation
Assiduité : certificat de réalisation (validation des acquis)