DOCAPOSTE Institute

Formation Parcours introductif à la Cybersécurité

Présentation

Ce parcours intensif de 10 jours offre une immersion complète dans les fondamentaux de la cybersécurité, ses enjeux, ses normes et ses outils.
Il permet d'acquérir une vision globale des risques, des cadres réglementaires et des bonnes pratiques, tout en découvrant les principaux métiers du domaine.
Grâce à une pédagogie active, il prépare les participants à intervenir efficacement dans un environnement numérique sécurisé.
À travers des cas concrets et des ateliers, les participants acquièrent les compétences nécessaires pour l'ancrage des objectifs de la formation.

Durée : 70,00 heures (10 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

A l'issue de la formation, le stagiaire sera capable de mettre en œuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.

- Détenir 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

Prérequis

Avoir des connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI.

Public

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Toutes personnes souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux.

Programme de la formation

Jour 1. Introduction à la cybersécurité et à son environnement
QCM de positionnement : Évaluer les représentations initiales de la cybersécurité.

- Enjeux de la cybersécurité à l'ère numérique
- Typologie des cybermenaces
- Écosystème des acteurs (ANSSI, CNIL, CERT, etc.)
- Terminologies essentielles
- Notions de sécurité informatique vs cybersécurité

Exercices : Identifier des menaces dans des scénarios fictifs

Jour 2. Gouvernance, conformité et cadre réglementaire

- Le RGPD en profondeur et ses obligations
- Les normes clés : ISO 27001 / 27005 / 27701 / 27035 / 27037
- Responsabilités légales et cybersécurité

Débat guidé : Faut-il privilégier ISO 27001 ou RGPD en priorité ?

Jour 3. Gestion des risques

- Méthodes d'analyse des risques : ISO 27005, EBIOS RM
- Identification, évaluation, traitement, acceptation des risques
- Risques résiduels et continuité des activités
- Outils de gestion des risques

QCM : Sur la terminologie ISO 27005 et le cycle de gestion des risques

Jour 4. Systèmes de management de la sécurité de l'information (SMSI)

- Définition et composantes d'un SMSI (ISO 27001)
- Déploiement d'un programme de sécurité
- Indicateurs, audit, plan d'amélioration continue

Étude de cas : Audit de maturité sécurité

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Jour 5. Fondamentaux de la cryptographie

- Principes : chiffrement symétrique/asymétrique
- Hashing, signature numérique, certificats
- Applications concrètes (VPN, TLS/SSL, emails sécurisés)
- Cryptanalyse et failles classiques

Étude de cas : Analyser une faille cryptographique

Jour 6. Défense – Mécanismes de sécurité informatique

- Sécurisation des postes clients et serveurs (Windows, Linux)
- Hardening et bonnes pratiques système
- Firewall, antivirus, SIEM, IDS/IPS
- Gestion des accès et privilèges

Démo : Analyse de logs avec un outil type Graylog / Splunk

Jour 7. Gestion des cyberattaques

- Cycle de vie d'une attaque
- Scénarios d'attaques types : ransomware, phishing, APT
- Réaction à incident : détection, confinement, éradication, restauration
- Méthodologie ISO 27035 – Gestion des incidents

Cas pratique : Analyse d'un rapport d'incident (ex. ransomware)

Jour 8. Sécurité offensive (Pentest & Red Team)

- Introduction au hacking éthique
- Étapes d'un test d'intrusion (Kali Linux, Metasploit, Nmap…)
- Ateliers pratiques : reconnaissance, exploitation, post-exploitation
- Outils et reporting d'un pentest

Lab pratique : Reconnaissance réseau (Nmap), analyse de vulnérabilités

Jour 9. Plan de Continuité et de Reprise d'Activité (PCA / PRA)

- Différence entre PCA et PRA
- Analyse d'impact métier (BIA)
- Élaboration d'un plan de continuité
- Tests de reprise, retour d'expérience (REX)

QCM : Sur la différence entre PCA, PRA et sauvegarde

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Jour 10. Cas pratiques et simulation globale

- Application transversale : simulation de crise cyber
- Création d'un plan de sécurité, gestion d'un incident, analyse post-mortem
- Débriefing collectif, recommandations, évaluation finale

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétence.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Équilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Tout au long de la formation

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Évaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

NB : dans le cadre d'une Action collective, chaque stagiaire bénéficiaire sera contacté par un prestataire choisi par l'Opco Atlas afin d'évaluer « à chaud » la qualité de la formation suivie.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France