EduGroupe
Accompagner pour réussir

Cybersécurité - Synthèse technique

Référence : **SECSYNTH** Durée : **3 jours (21 heures)** Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Aucune connaissance préalable

PROFIL DES STAGIAIRES

- Tout manager de la DSI impliqué dans la sécurité

OBJECTIFS

- Connaître l'entendue des risques qui pèsent sur les informations de l'établissement
- Comprendre l'évolution des analyses de risque pour faire face aux nouvelles menaces
- Identifier les risques associés à l'émergence de nouvelles technologies
- Savoir mettre en oeuvre une gouvernance efficace
- Comprendre l'intérêt de disposer d'une surveillance et d'une gestion des incidents de dernière génération

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Pédagogie active, interactive et expérientielle : Alternance d'apports conceptuels, de démonstrations et d'ateliers pratiques ; Études de cas réels inspirées d'incidents et de projets de transformation numérique ; Ateliers collaboratifs ; Évaluations formatives continues
- Distinction selon les formats et types de formation : Présentiel (inter Paris, Lyon, Nantes, Rennes, Toulouse, Pau/ intra partout en France) ; Distanciel synchrone (classe virtuelle) ; Distanciel asynchrone
- Dimension innovante et immersive : Serious game Cyber Crisis Challenge ; Auto-diagnostic de maturité cybersécurité ; Fil rouge Cyber-lab virtuel ; Coaching post-formation (option)
- Moyens pédagogiques et techniques : Plateforme Internet intégrant quiz, ressources téléchargeables et suivi des acquis ; Supports pédagogiques numériques ; Outils techniques de démonstration ; Encadrement par un formateur expert en cybersécurité certifié ISO 27001 / EBIOS RM / CEH, garantissant une approche pragmatique et à jour des dernières évolutions technologiques et réglementaires

FORMATEUR

- Consultant-formateur expert en cybersécurité certifié ISO 27001 / EBIOS RM / CEH

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : les évaluations formatives sous plusieurs formes (exercices, quiz...)
- A la fin de la formation : Evaluation sommative sous forme de quiz général ou étude de cas qui permet de s'assurer de l'atteinte des objectifs de la formation ; Evaluation satisfaction remplie par chaque apprenant
- Après la formation : Evaluation à froid, un mois après la session de formation
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Jour 1 – État de l'art et évolution de la cybersécurité (7h)

2. Matinée : Contexte et panorama (3h30)

- Évolution historique de la cybersécurité : des périmètres fermés aux environnements hybrides
- Nouvelles menaces : ransomware-as-a-service, attaques supply chain, IA générative et deepfakes
- Panorama des acteurs de la menace (APT, hacktivisme, cybercriminalité organisée)
- État de l'art des cadres de référence (NIS2, RGPD, ISO 27001/27005, DORA, LPM, ANSSI)

3. Après-midi : Transformation de la sécurité des SI (3h30)

- Cyberdéfense et résilience numérique : les nouveaux paradigmes (Zero Trust, Secure by Design)
- Approches sectorielles : commerce, santé, industrie, services numériques
- 💡 *Atelier : cartographier les principales menaces et vulnérabilités de son organisation*
- 💡 *Quiz interactif : panorama des cyberattaques récentes et leçons à retenir*

4. Jour 2 – Analyse des risques et gouvernance de la sécurité (7h)

5. Matinée : Évolution des méthodes d'analyse des risques (3h30)

- Méthodologies : EBIOS RM, ISO 27005, MEHARI, FAIR
- Intégration des analyses de risques dans la gouvernance globale de l'entreprise
- Quantification du risque cyber : indicateurs, probabilités, impacts
- 💡 *Cas pratique : identification et hiérarchisation de risques sur un scénario réel (supply chain, cloud)*

6. Après-midi : Gouvernance, rôles et responsabilités (3h30)

- Gouvernance cyber : structures, comités, reporting, communication à la direction
- Rôles clés : direction générale, RSSI, DPO, métiers, IT, conformité
- Politique de sécurité, plan de continuité, indicateurs de pilotage (KPI/KRI)
- 💡 *Atelier collaboratif : créer une matrice RACI de la gouvernance sécurité*
- 💡 *Exercice de synthèse : construire une feuille de route de gouvernance pour une PME*

7. Jour 3 – Évolutions technologiques, surveillance et gestion des incidents (7h)

8. Matinée : Évolutions technologiques et nouveaux modèles (3h30)

- Technologies émergentes : Cloud computing, Edge, IoT, 5G, IA, Blockchain, Quantum
- Risques et opportunités : gestion des identités, chiffrement, souveraineté des données, architectures Zero Trust
- Sécurité du développement (DevSecOps), automatisation, détection comportementale (UEBA)
- 💡 *Démonstration / étude de cas : sécurité d'un service cloud exposé, bonnes pratiques et contre-mesures*

9. Après-midi : Surveillance, détection et gestion des incidents (3h30)

- SOC, SIEM, EDR/XDR : principes, déploiement, supervision des alertes
- Gestion des incidents : phases NIST (préparation, détection, réponse, retour d'expérience)
- Coopération avec l'ANSSI / CERT / autorités sectorielles
- 💡 *Exercice pratique : simulation d'un incident – détection, confinement, communication*
- Synthèse : établir un plan d'amélioration continue et de surveillance durable

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible .