EduGroupe
Accompagner pour réussir

Etat de l'art de la sécurité des systèmes d'information

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

Opcommerce

CONNAISSANCES PRÉALABLE

- Disposer de bonnes connaissances générales sur les SI

PROFIL DES STAGIAIRES

- Directeurs des systèmes d'information ou responsable informatique, RSSI, chefs de projet sécurité, architectes informatiques

OBJECTIFS

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Connaître les principes et les normes de chaque domaine de la SSI
- Disposer d'informations sur les tendances actuelles au niveau des menaces et des solutions à notre disposition
- Pouvoir améliorer la communication entre la maitrise d'ouvrage, la maitrise d'oeuvre et la SSI
- Être en mesure d'effectuer des choix techniques

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Pédagogie active et ancrée dans le réel : Alternance d'apports théoriques courts et d'exercices pratiques ; Apprentissage par l'action et la réflexion collective ; Approche métier et contextualisation ; Évaluation continue
- Formats et adaptation selon le contexte : Présentiel (inter à Paris, Lyon, Nantes, Rennes, Toulouse, Pau / Intra partout en France) ; Distanciel synchrone (classe virtuelle) ; Distanciel asynchrone (complément e-learning) ; Inter / Intra
- Dimension innovante : Serious Game Cellule de crise SSI ; Auto-diagnostic de maturité SSI ; Veille dynamique ; Plan d'action personnalisé ; Continuité pédagogique post-formation
- Moyens pédagogiques et techniques mobilisés : Salle équipée (ou plateforme en ligne sécurisée) ; Supports numériques complets ; Plateforme Internet pour héberger ressources, quiz et documents collaboratifs ;
- Évaluation des acquis en continu

FORMATEUR

- Consultant-formateur expert en cybersécurité et gouvernance SSI, garantissant une approche pragmatique et un transfert de compétences concret

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture
- Pendant la formation : évaluations formatives sous diverses formes
- Fin de formation : évaluation sommative sous forme de quiz général ou étude de cas ; évaluation satisfaction
- Après la formation : Evaluation à froid, un mois après la session de formation

CONTENU DU COURS

1. Jour 1 — Contexte, enjeux et évolution des menaces (7h)

2. Matin (3 h 30) - Introduction à la SSI et à la gestion des risques

- Définitions : sécurité, fiabilité, intégrité, disponibilité, confidentialité
- Rôle et responsabilité des acteurs (DSI, RSSI, MOA/MOE)
- Les grands principes de gouvernance de la SSI : PDCA, approche par les risques
- 💡 *Brainstorming collectif : Quels sont les risques majeurs pour notre SI ?*
- 💡 *Quiz interactif : vocabulaire et typologie des menaces*

3. Après-midi (3 h 30) - Panorama des menaces et tendances actuelles

- Cybermenaces émergentes : ransomware, supply chain attack, IA malveillante, deepfake, exfiltration cloud
- Facteurs d'exposition : nomadisme, shadow IT, télétravail, IoT
- Les grandes tendances des solutions de protection (EDR/XDR, SASE, ZTNA, IA défensive)
- 💡 *Étude de cas en binôme : analyse d'un incident réel (attaque supply chain, fuite de données)*
- 💡 *Débrief collectif : leçons à tirer, mesures correctives*

4. Jour 2 — Méthodologie, normes et maturité SSI (7h)

5. Matin (3 h 30) - Modèles d'approche et évaluation de la maturité

- Modèles de maturité : CMMI, ISO 27001, NIST CSF, ANSSI PAM
- Diagnostic de maturité SSI : axes, niveaux, outils et indicateurs
- Cartographie des risques : identification, évaluation, traitement
- 💡 *Atelier pratique : auto-évaluation de la maturité de son organisation à l'aide d'une grille fournie*
- 💡 *Restitution en groupe : priorisation des axes d'amélioration*

6. Après-midi (3 h 30) - Normes, référentiels et méthodes de gestion des risques

- Présentation synthétique : ISO 27001/27002, EBIOS Risk Manager, RGPD, RGS, PCI-DSS, NIS2
- Alignement stratégique : comment relier exigences métiers, contraintes techniques et référentiels
- Élaboration d'un plan de gouvernance SSI adapté à la taille de l'organisation
- 💡 *Étude de cas fil rouge : mise en conformité simplifiée d'un SI à partir d'un scénario donné*
- 💡 *Quiz technique : Quel référentiel pour quelle situation ?*

7. Jour 3 — Architecture, nomadisme et sécurité opérationnelle (7h)

8. Matin (3 h 30) - Technologies et architectures de sécurité

- Cloisonnement réseau et segmentation : principes, modèles, exemples (Zero Trust, micro-segmentation)
- Sécurité des endpoints et des environnements mobiles
- Architecture SASE, VPN, ZTNA et solutions d'accès sécurisés
- Intégration des services Cloud et SaaS : gestion des identités et des accès (IAM, MFA, PAM)
- 💡 *Atelier technique guidé : conception d'un schéma d'architecture sécurisée pour une entreprise multi-sites*
- 💡 *Mise en commun / débrief : choix techniques et justification*

9. Après-midi (3 h 30) - Nomadisme, collaboration et communication SSI

- Gestion du nomadisme : risques et contre-mesures (Wi-Fi public, BYOD, mobilité internationale)
- Communication entre MOA, MOE et SSI : langage commun et gouvernance
- Intégration sécurité dès la conception (Security by Design)
- Synthèse et plan d'action individuel
- 💡 *Jeu de rôle : simulation d'un comité de sécurité — échange MOA/MOE/RSSI pour la prise de décision*
- 💡 *Plan d'action personnel : chaque participant rédige la feuille de route SSI adaptée à son organisation*
- 💡 *Évaluation finale : QCM + restitution orale*

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 .