

# CYBERSÉCURITÉ

## référentiel, objectifs et déploiement

CODE STAGE

IN-CYB01

TARIF

3 700 €



DUREE : 5 JOURS



PRÉSENTIEL



DATES : nous consulter



### PROGRAMME

#### Journée 1 : Concepts et enjeux

- Approche d'amélioration continue suivant 3 fondements : Se connaître et adopter une stratégie - Faire un plan d'actions - Contrôler le plan d'actions
- Principe de la défense systémique
- Modèle attaque défense : Cible/mesure/menace/attaquant/contre-mesure/action/TdB
- Analyse des enjeux de sécurité du SI (DSI), enjeux de l'attaquant, enjeux du RSSI (FEROS)
- Travaux Pratiques: simulation d'une attaque (via une plateforme dédiée )

#### Journée 2: Mise en place opérationnelle de l'organisation de sécurité

- Notion de périmètre (frontière) d'application et d'applicabilité (qui et quoi dans la PSSI : OS, réseaux, responsables d'équipes, processus, application,...)
- Notion de parties prenantes internes et externes de la cyber (écosystèmes (type d'entreprises (conseil), usagers du système), métiers et missions (les activités) de la cyber et contractualisations
- Notion de réglementation (pyramide des lois : lois, décrets, .....,normes, référentiels des bonnes pratiques ) : positionner ce qui va être appris (Normes ISO ), zoom sur OIV, OSE, NIS, RGS, DNS
- Travaux dirigés et pratiques d'analyse de risques : Etude de cas (avec EBIOS)

#### Journée 3: de l'implémentation vers la supervision opérationnelle

- Déploiement des objectifs de la PSSI,
- Référentiel ISO 27002 (modélisation, mesurage, mesures de sécurité...)
- Travaux dirigés et pratiques de la mise en place d'une PSSI: choix de périmètre et élaboration d'indicateurs de supervision (organisationnel et technique)

#### Journée 4: De la supervision vers le maintien et l'amélioration de la sécurité

- Centre opérationnel de sécurité: cycle de vie de l'incident
- Outils: d'anticipation – Outils Pendant : détection et visualisation des flux, incident – Outils d'Après : investigation et forensic - Outils de corrélation d'incident et d'analyse des Log: SIEM
- Travaux dirigés et pratiques: étude de cas (identification des Indicateurs de compromission )

#### Journée 5:

- La résilience : Plan de secours informatique
- Consolidation des acquis et mise en situation
- contrôle des connaissances

#### OBJECTIFS

Savoir mener, argumenter et déployer une politique de sécurité informatique dans une entreprise en lien avec une analyse de risque.

#### PUBLIC

Responsables sécurité informatique, Auditeurs, sécurité informatique, Administrateurs sécurité, Gérants d'entreprise, Managers.

#### PRÉ-REQUIS

Notions de réseaux informatiques et d'internet

#### MODALITÉS PÉDAGOGIQUES

##### Préparation de votre formation

Questionnaire d'analyse des attentes

##### Moyens pédagogiques pendant votre formation:

Utilisation de cas concrets  
Entraînement et mise en situation,  
Simulations sur simulateur  
Echanges entre les participants et notre expert.

##### Accompagnement et suivi de la formation

Elaboration de son plan d'actions personnalisé  
Possibilité de joindre le formateur post formation

#### MODALITÉS D'ÉVALUATION

##### Évaluation des compétences

Tests, cas pratiques, exercices  
Examen de validation de l'Unité d'Enseignement

##### Évaluation de la formation

Questionnaire de satisfaction stagiaire  
Synthèse fin de stage du formateur

#### VALIDATION

Attestation de fin de formation  
Attestation de présence



Contactez-nous : 01 60 79 87 74