FORMATION LABELLISÉE SECNUMEDU-FC

Tronc commun pour tous

Module 1
Cybersécurité : notions de bases, enjeux et droit commun

Module 2
L'hygiène informatique pour les utilisateurs

Module 3
Gestion et organisation de la cybersécurité

Module 4
Protection de l'innovation et cybersécurité

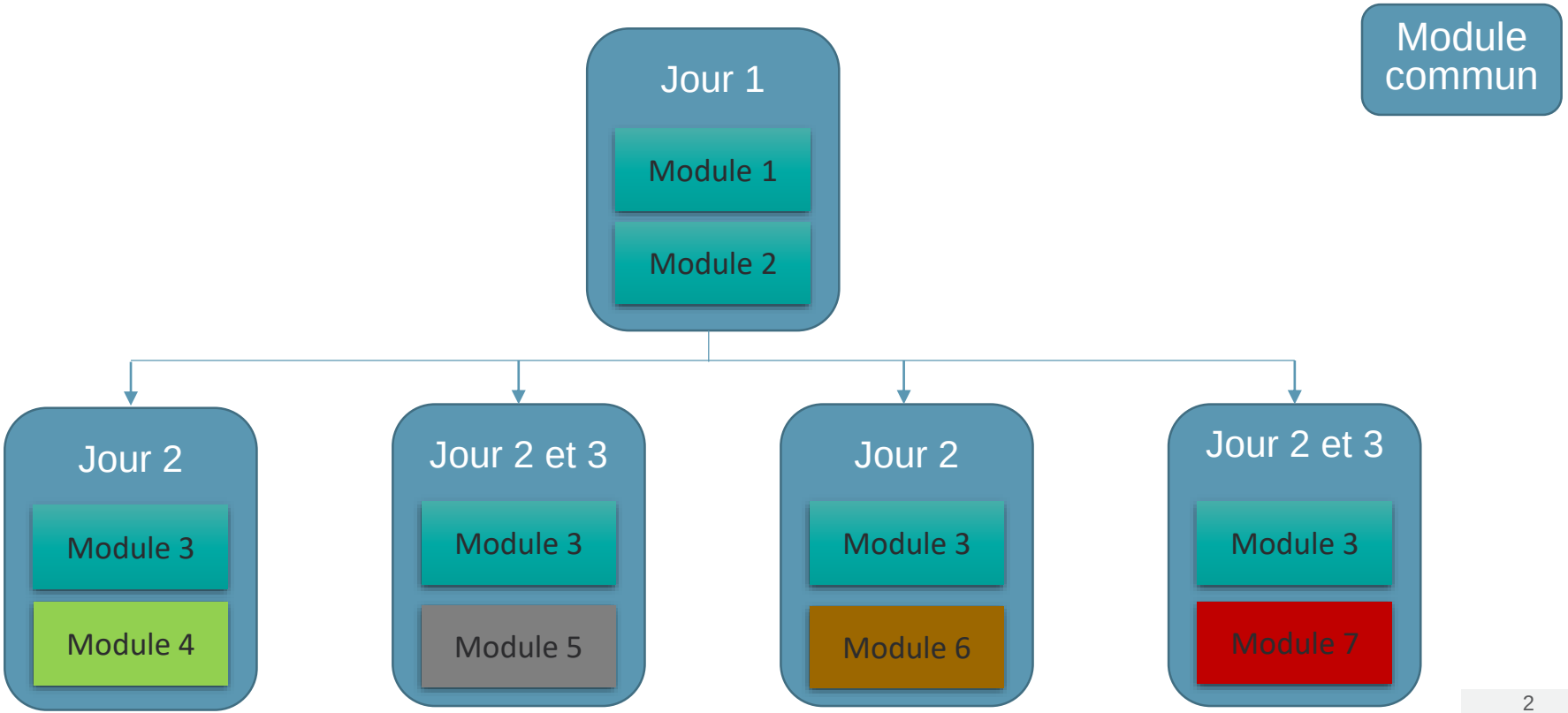
Module 5
Administration sécurisée du SI interne d'une entreprise

Module 6
La cybersécurité des entreprises ayant externalisé

Module 7
Sécurité des sites internet gérés en interne

SecNumedu
Formation continue
ANSSI

FORMATION LABELLISÉE SECNUMEDU-FC



MODULE 1
CYBERSÉCURITÉ : NOTIONS DE BASES, ENJEUX ET DROIT COMMUN

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Identifier l'articulation entre cybersécurité, sécurité économique et intelligence économique
- Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI).
- Connaître les définitions et la typologie des menaces

Durée : 3,5 heures

Contenu :

- Définitions (Intelligence économique, sécurité économique globale, cybersécurité, etc.)
- Les enjeux de la sécurité des systèmes d'informations
- Les propriétés de sécurité
- Aspects juridiques et assurantiels
- Le paysage institutionnel de la cybersécurité

SecNumedu
Formation continue
ANSSI

MODULE 2
L'HYGIÈNE INFORMATIQUE POUR LES UTILISATEURS

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Appréhender et adopter les notions d'hygiène de base de la cybersécurité pour les organisations et les individus

Durée : 3,5 heures

Contenu :

- Connaître le système d'information et ses utilisateurs
- Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes…)
- Maîtriser le réseau de partage de documents (en interne ou sur internet)
- Mettre à niveau les logiciels
- Authentifier l'utilisateur
- Nomadisme - Problématiques liées au BYOD (Bring your Own Devices)

MODULE 3
GESTION ET ORGANISATION DE LA CYBERSÉCURITÉ

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Appréhender les multiples facettes de la sécurité au sein d'une organisation.
- Connaître les métiers directement impactés par la cybersécurité
- Anticiper les difficultés courantes dans la gestion de la sécurité

Durée : 3,5 heures

Contenu :

- Présentation des publications/recommandations
- Présentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.)
- Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)
- Maîtriser le rôle de l'image et de la communication dans la cybersécurité
- Méthodologie d'évaluation du niveau de sécurité
- Actualisation du savoir du référent en cybersécurité
- Gérer un incident / Procédures judiciaires

SecNumedu
Formation continue
ANSSI

MODULE 4
PROTECTION DE L'INNOVATION ET CYBERSÉCURITÉ

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Appréhender la protection de l'innovation à travers les outils informatiques

Durée : 3,5 heures

Contenu :

- Les modalités de protection du patrimoine immatériel de l'entreprise
- Droit de la propriété intellectuelle lié aux outils informatiques
- Cyber-assurances
- Cas pratiques

MODULE 5
ADMINISTRATION SÉCURISÉE DU SYSTÈME D'INFORMATION (SI) INTERNE D'UNE ENTREPRISE

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Savoir sécuriser le SI interne
- Savoir détecter puis traiter les incidents
- Connaître les responsabilités juridiques liées à la gestion d'un SI

Durée : 6 à 9 heures

Contenu :

- Analyse de risque (Expression des besoins et identification des objectifs de sécurité -EBIOS / Méthode harmonisée d'analyse des risques - MEHARI)
- Principes et domaines de la SSI afin de sécuriser les réseaux internes
- Détecter un incident
- Gestion de crise
- Méthodologie de résilience de l'entreprise
- Traitement et recyclage du matériel informatique en fin de vie (ordinateurs, copieurs, supports amovibles, etc.)
- Aspects juridiques

SecNumedu
Formation continue
ANSSI

MODULE 6
LA CYBERSÉCURITÉ DES ENTREPRISES AYANT EXTERNALISÉ TOUT OU PARTIE DE LEUR SI

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé

Durée : 3,5 heures

Contenu :

- Les différentes formes d'externalisation
- Comment choisir son prestataire de service ?
- Aspects juridiques et contractuel

MODULE 7
SÉCURITÉ DES SITES INTERNET GÉRÉS EN INTERNE

Public : Public hétérogène parmi les salariés des entreprises, dirigeant, cadre, responsable informatique, etc.

Objectifs :

- Connaître les règles de sécurité pour gérer un site internet

Durée : 9 heures

Contenu :

- Menaces propres aux sites internet
- Approche systémique de la sécurité (éviter l'approche par patches)
- Configuration des serveurs et services
- HTTPS et Infrastructure de gestion de clés (IGC)
- Services tiers
- Avantages et limites de l'utilisation d'un Content Management et / ou développement web
- Sécurité des bases de données
- Utilisateurs et sessions
- Obligations juridiques réglementaires