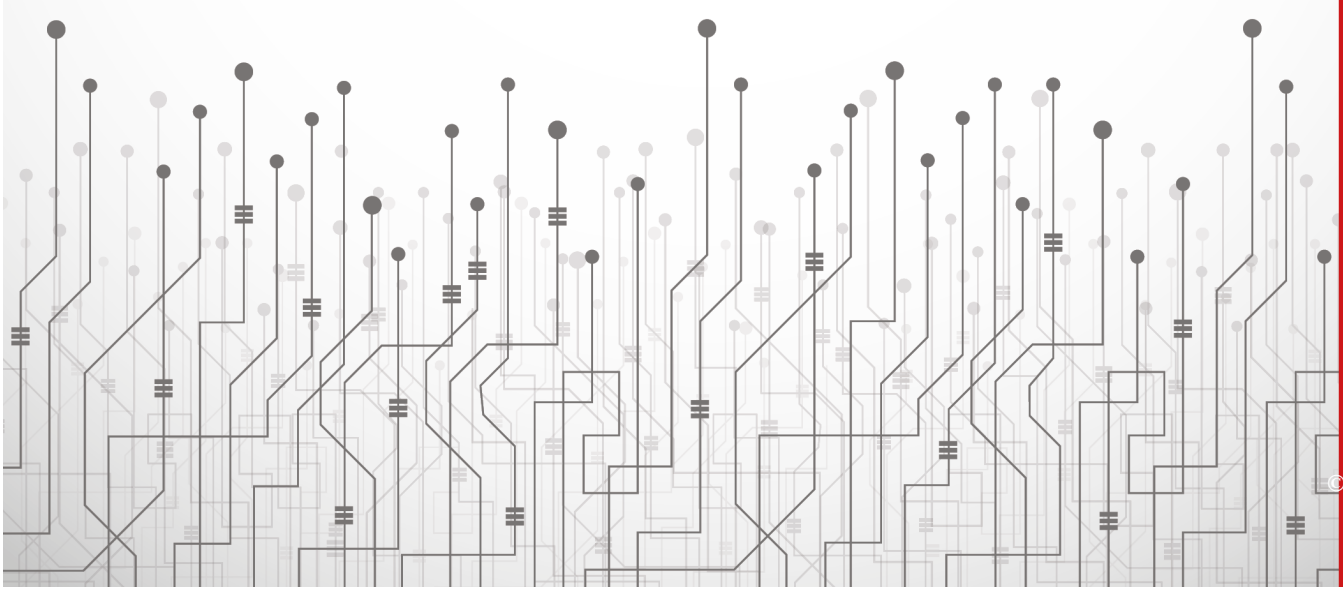
<ÉCOLE
DE LA FILIÈRE
NUMÉRIQUE/>

imie

Syllabus

Cybersécurité - Majeure 3

Année 2018-2019



Cycle de vie du document

<ÉCOLE DE LA FILIÈRE NUMÉRIQUE/> imie	Syllabus - CYB Advanced Année 2018-2019		
Formation concernée :	Cursus A5 (initial et alternance)		
Diffusion du document :	IMIE Services Formateurs (internes & externes) CM, RE et TM Apprenants		
Service responsable :	Service pédagogique		
Rédigé par :	**Nicolas MORICET** **François-Xavier WAWRZYNIAK** Responsable de filière DEV & OPS	Date de création :	16-Oct-2018
Relecture par :	**Johanne BERTHIER** Responsable académique	Date de relecture :	16-Oct-2018
Validé par :	**Arnaud BERTHIER** Chief Management Officer	Date d'application :	16-Oct-2018
Diffusion approuvée par :	**Arnaud BERTHIER** Chief Management Officer	Date de péremption :	Guide valable jusqu'au 31/08/2019

TABLE DES MATIÈRES

1. VULGARISATION DU MODULE

LA cybersécurité touche a un périmètre large en informatique : lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies.

Ces domaines peuvent dépendent des états et des organisations.

Dans ce modules nous aborderons tout ces points dont un chef de projet en informatique doit avoir connaissance.

2. PRÉ-REQUIS PÉDAGOGIQUE

L'apprenant aura suivi le module suivant pour accéder à ce module :

Aucun prérequis pédagogique

3. OBJECTIFS DU MODULE

- Connaitre les lois (et les acteurs de ces lois) informatiques applicable en entreprise.
- Pouvoir sensibilisé les employés d'une entreprise à ces lois.
- Savoir appliquer la lois pour la conservation des données des employés en entreprise.
- Connaitre les lois de la propriété intellectuelle.
- Savoir rédigé une politique de sécurité informatique
- Connaitre une méthode de gestion de projet de sécurité informatique
- Connaissance des acteurs du marché de la cybersécurité pour faire appelle à une prestation en cas de besoin

4. PLAN DU MODULE

- Sensibilisation à la cybersécurité (orienté employer, TPE et PME)
- Le contexte géopolitique de la France face à la cybersécurité
- Les acteurs de la cybersécurité (ANSSI, Europe, CNIL, CLUSIF, législation française)
- Les principales loi de l'informatique

- Les droit en entreprise (droit de rétractation, la conservation des logs, la messagerie et les mails)
- Le RGPD
- Le forensic
- La méthode EBIOS
- L'achat raisonné de la sécurité dans une entreprise

5. DESCRIPTION ET RECOMMANDATIONS TECHNIQUES

Méthode EBIOS

6. RESSOURCES

En vue de préparer le module, l'apprenant aura pris connaissance ou/et installer les ressources suivantes :

Une sensibilisation à la cybersécurité et des cours plus approfondis :

https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/

La méthode EBIOS :

https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

la méthode EBIOS Risk manager :

https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

Les logiciel préconiser par l'ANSSI :

https://www.ssi.gouv.fr/particulier/logiciels-preconises-par-lanssi-2/

le CERT-FR :

https://www.cert.ssi.gouv.fr/

7. CRITÈRES D'ÉVALUATION

- L'apprenant sait déterminer le périmètre de sécurité de l'entreprise
- L'apprenant sait sécurisé le métier client
- L'apprenant rédige une politique de sécurité cohérente avec le métier client
- L'apprenant met en place ou achète une sécurité raisonnée en fonction du métier client
- L'apprenant sait sensibilisé l'entreprise (directeur, équipe et sous-traitant) à la cybersécurité
- L'apprenant sait expliquer l'enjeu de la cybersécurité pour l'entreprise

8. TYPE(S) D'ÉVALUATION(S)

En fonction des critères d'évaluations ci-dessus vous pouvez mettre en place le(s) type(s) d'évaluation(s) :

Projet avec présentation

9. SAVOIRS, SAVOIR-FAIRE TECHNIQUES, SAVOIR-FAIRE RELATIONNELS, SAVOIR-FAIRE ORGANISATIONNELS

- L'apprenant connait les lois (et les acteurs de ces lois) informatiques applicable en entreprise.
- L'apprenant sait sensibilisé les employés d'une entreprise à ces lois.
- L'apprenant sait appliquer la lois pour la conservation des données des employés en entreprise.
- L'apprenant connait les lois de la propriété intellectuelle.
- L'apprenant sait rédiger une politique de sécurité informatique
- L'apprenant connait de gestion de projet de sécurité informatique
- L'apprenant connait les acteurs du marché pour faire appel à une prestation en cas de besoin

10. QUESTIONS ET RETOURS

Si vous avez des questions, sur le contenu pédagogique de ce module, veuillez contacter le service pédagogique : support-pedagogique@imie.fr.