Réf : ET_SEC_CYB / ET2_SEC_CYB

Cyberdéfense

Construction d'une stratégie de défense

Objectif

Disposer de compétences défensives est aujourd'hui indispensable dans le maintien opérationnel d'un système d'information. Elles permettent de prévenir et de bloquer les menaces, de plus en plus croissantes et complexes. L'objectif de cette formation est donc de vous transmettre les connaissances sur la cyberdéfense, tant d'un point de vue organisationnel que technique, pour que vous soyez en mesure de construire une stratégie de défense efficace.

Public	Prérequis	Durée estimée pour le suivi des modules indispensables
Informaticiens	Des connaissances en système et réseau Microsoft ainsi que des notions en gestion et suivi de projet sont nécessaires.	Durée des vidéos : 5h55 Durée des TP : 9h30

Contenu pédagogique

Les modules indispensables

Présentation du cours

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h02.

- Présentation du cours

Introduction à la cybersécurité en France

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h13.

- Objectifs du module
- Introduction aux menaces pesant sur les organisations françaises
- Les profils d'attaquants
- Vision des dirigeants vis-à-vis de la cybersécurité
- Zoom sur L'ANSSI
- Démonstration - Présentation des guides de sécurité ANSSI
- La cybersécurité sur le plan européen
- Conclusion

Audit de la cybersécurité des systèmes d'information

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h30.

- Objectifs du module
- Séquencement d'un projet d'audit de la sécurité de l'information et réalisation d'un rapport
- Identifier la maturité des processus
- TP à réaliser - Identifier les mesures de sécurité
- Auditer et identifier les écarts vis-à-vis du guide d'hygiène de l'ANSSI - partie 1
- Démonstration - Présentation ISO 27002
- Auditer et identifier les écarts vis-à-vis du guide d'hygiène de l'ANSSI - partie 2
- Démonstration - Présentation du Guide d'hygiène de l'ANSSI
- Auditer et identifier les écarts vis-à-vis du guide d'hygiène de l'ANSSI - partie 3
- TP à réaliser - Alignement des mesures de sécurité vis-à-vis du guide d'hygiène ANSSI
- Présentation des points stratégiques du rapport auprès de la direction/hiérarchie
- TP à réaliser - Réaliser une présentation pour la restitution d'audit au CODIR
- Conclusion

Durcissement des infrastructures Windows

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 2h44.

- Objectifs du module
- Sécurité des droits d'administration
- Durcissement postes et serveurs
- Durcissement des protocoles réseau
- IA, ATA et Threat Intelligence
- Journalisation et surveillance avancée - partie 1
- Journalisation et surveillance avancée - partie 2
- Démonstration - Présentation de PingCastle
- TP à réaliser - Mettre en œuvre un renforcement de sécurité en environnement Microsoft
- TP à réaliser - Auditer son architecture et préparer un plan de contre-mesure
- Conclusion

Une défense alignée sur les attaques

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h24.

- Objectifs du module
- Revue de la segmentation des phases d'un attaquant
- Présentation des différents groupes APT
- Etude avancée des étapes d'une attaque APT à travers ATT&CK
- Démonstration - Présentation de la MITRE ATT&CK
- Conclusion