SEC101 - Cybersécurité : référentiel, objectifs et déploiement

Mis à jour le 19-04-2024

Code : SEC101

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

EPN05 - Informatique
2 rue Conté
accès 33.1.13B
75003 Paris
01 40 27 28 21
Mmadi Hamida
hamida.mmadi@lecnam.net

Présentation

Prérequis

Niveau Bac + 2 en informatique, il est conseillé de suivre ou d'avoir suivi l'unité d'enseignement SEC001.

Objectifs pédagogiques

- L'objectif pédagogique principal du cours est de permettre la compréhension des principes élémentaires du processus de la cybersécurité dans une organisation ainsi que ses spécificités en fonction des organisations, qu'elles soient régaliennes ou non, à dimension nationale ou internationale.
- Le cours vise l'enseignement de 3 composants clés du processus : "Analyse de risque", "Politique de sécurité", "Gestion opérationnelle de la sécurité ». L'objectif de chacun sera de permettre à l'apprenant de découvrir les aspects méthodologiques, normatifs ainsi que les éléments de langage et les concepts.
- A l'issue, l'apprenant sera en mesure d'élaborer, défendre et accompagner la mise en oeuvre d'une analyse de risque, de mesures de sécurité et de les évaluer, ainsi qu'une gestion opérationnelle des incidents de sécurité. Les travaux pratiques mettront l'apprenant face à ces situations.

Compétences

- Participer et accompagner la mise en place de la gouvernance de la cybersécurité d'une organisation, régalienne ou industrielle, à dimension nationale ou internationale,
- Participer à l'analyse de risque de l'organisation et piloter la mise en place de la mission d'analyse de risque cyber,
- Identifier, communiquer et présenter un rapport des risques cyber de l'organisation,
- Participer à l'élaboration et à la mise à jour des politiques de cybersécurité auprès des entités concernées du périmètre de l'organisation, national ou international,
- Identifier, élaborer et assurer la diffusion des mesures de sécurité adaptées à l'organisation et son périmètre, identifier les parties prenantes, exposer et les expliquer,
- Participer à l'optimisation et la mise en place des mesures et contrôles de sécurité, intervenir dans leur gestion opérationnelle,
- Accompagner ou participer ou mener des audits de vulnérabilités et d'intrusion sur les services du système d'information de l'organisation en apportant,
- Participer à l'analyse des différentes situations d'incidents, y compris de crise.

Programme

Contenu

- ----------
- Temps 1 : Principaux enjeux de la sécurité pour la société numérique
- ----------
- Écosystème
- Éléments clés de l'intelligence de la menace (géopolitique,…)
- Éléments clés des obligations normatives françaises et internationales (RGS, Homologation, LPM, ISO27, RGPD, etc.),
- Intégration de ces éléments clés dans le processus d'analyse de risque, de mise en place

de la cyber et de supervision de la cybersécurité,
- Organisation des métiers de la cybersécurité dans l'entreprise.
- ----------
- Temps 2 : l'Analyse de risque cyber (AR)
- ----------
- Principes fondamentaux de l'analyse de risque,
- Éléments de langage et définitions des concepts de l'AR,
- Application de l'AR à la cyber, surfaces d'exposition et surface d'attaques,
- Les processus d'analyse de risque (global/ciblé),
- Application d'une méthodologie (ISO27001-ISO27005, EBIOS, MEHARI,…),
- Le métier de gestionnaire de risque (RSSI, Risk manager).
- ----------
- Temps 3 : les politiques cyber : les mesures, contremesures et leurs mesures (PSSI)
- ----------
    - Définition et principes de la PSSI (définition et mise en place de bonnes pratiques, notions d'architectures,…),
    - Analyse d'une mesure de sécurité (mesures techniques, organisationnelles) (stratégiques, opérationnelles)(application ISO27002, RGS),
    - Analyse d'une mesure à partir d'une architecture technique ("threat modelling"),
    - Application d'un référentiel de mesures de sécurité à une architecture technique et à l'organisation,
    - Évaluation de la cyber (indicateurs et métriques),
    - Le métier de RSSI.
- ----------
- Temps 4 : la sécurité opérationnelle (SECOPS)
- ----------
    - L'amélioration continue en cybersécurité (anticiper, lever le doute, corriger, capitaliser) (ISO27035) en vue du maintien des conditions opérationnelles de sécurité,
    - Principe de la SECOPS et de la gestion opérationnelle de la cyber (procédures opérationnelles, ...)
    - Le cycle de vie d'un incident de sécurité et de ses éléments clés(du signal faible à la crise, en passant les alertes)
    - La gestion opérationnelle des vulnérabilités (IoC, …),
    - La gestion opérationnelle des contrôles de sécurité (les accès, mesures de la PSSI, conformité, etc.),
    - La gestion opérationnelle de l'outillage SECOPS,
    - La gestion opérationnelle de campagnes de mises à jour critiques,
    - La gestion opérationnelle avec l'AR et la PSSI, détection et réponse (traitement, confinement, acceptation).
- ----------

Modalités de validation

- Contrôle continu
- Examen final

Description des modalités de validation

Le contrôle continu se fera par le biais d’un dossier en AR, PSSI, description de mesures ISO27002 ou similaire et d’indicateurs ISO27004 ou similaire, SECOPS, description d’un outillage SECOPS et de ses principes.

La note de contrôle continu permettra d'améliorer la note de l'examen final.

L'examen final doit présenter la moyenne de 3 notes des 3 modules : AR, PSSI, SECOPS et ne pas présenter de note inférieure à 10/20 à l'un des 3 modules.

La session 2 ne prend pas en compte le contrôle continu.

Bibliographie

Titre	Auteur(s)
Tableaux de bord de la sécurité réseau », Editeur(s) : Eyrolles, Nbp: 562 , 26/08/2010, 3°ed., EAN13 : 9782212128215	Cédric Llorens, Laurent Levier, Denis Valois, Benjamin Morin
Management de la sécurité de l'information, Implémentation ISO 27001 , Editeur(s)	Alexandre Fernandez-Toro
analyse de la norme ISO27035 , « La gestion des risques Concepts et méthodes 2009	Plusieurs documents du CLUSIF sont disponibles à cette adresse : / https://cl