le cnam
Auvergne – Rhône-Alpes

Cybersécurité : référentiel, objectifs et déploiement

Cybersécurité : référentiel, objectifs et déploiement

SEC101

Planning

Période	Modalité
Information Indisponible - Information Indisponible	Formation ouverte et à distance (FOAD)

CONDITIONS D'ACCES / 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 VISÉES

- 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.

Contenu de la formation

- ----------
- 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 et d’évaluation

Contrôle continu: Contrôle de connaissances et de savoirs qui se déroule tout le long du temps de l'enseignement

Examen final: Examen final portant sur l'ensemble des connaissances et des savoirs de l'enseignement

Accompagnement et suivi:

Prise en charge des auditeurs inscrits à une unité d’enseignement, depuis l’inscription jusqu’au déroulement effectif de la formation.

Parcours

Cette UE est constitutive des diplômes suivants:

[{"code":"CC15700A","code_suivi":1028,"date_debut_validite":"2020-09-01","date_fin_validite":"9999-08-31","date_limite_utilisation":"9999-08-31","affichable":true},{"code":"CC13800A","code_suivi":794,"date_debut_validite":"2021-09-01","date_fin_validite":"9999-08-31","date_limite_utilisation":"9999-08-31","affichable":true},{"code":"LG02501A","code_suivi":260,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CYC9101A","code_suivi":430,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CYC9102A","code_suivi":431,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CYC9104A","code_suivi":429,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CYC9105A","code_suivi":220,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CYC9106A","code_suivi":1031,"date_debut_validite":"2024-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CRN0801A","code_suivi":601,"date_debut_validite":"2023-12-21","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CRN0802A","code_suivi":971,"date_debut_validite":"2023-12-21","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true},{"code":"CRN0803A","code_suivi":972,"date_debut_validite":"2023-09-01","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true}]

ECTS:

Volume Horaire indicatif	Financement individuel hors tiers financeur et CPF	Tarif de référence (Employeur)
45 heures	450.00	900.00

Infos Pratiques

Durée indicative	Modalité	Période	Date de début des cours	Date de fin des cours
45 heures	Formation ouverte et à distance (FOAD)	Premier semestre	Information Indisponible	Information Indisponible

Dernière mise à jour: 02/07/2025 10:21:41