le cnam
Nouvelle-Aquitaine

Fiche récapitulative

SEC105 | Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications

51
Total d'heures d'enseignement

6
Crédits ECTS

Date non définie
Début des cours prévu

Programme

Programme du cours Architectures et Protocoles de Sécurité du SI

Introduction aux architectures, leur sécurisation et l'application des principes de défense en profondeur

Objectif : comprendre les besoins en stratégies et tactiques cyber, défense en profondeur, études des menaces, vulnérabilités, techniques d'attaques & de défense : mesure et contre-mesure.
Compétence : Gestion de la sécurité des données, des réseaux et des systèmes.

Notion de donnée, information et connaissance.

Les 12 bonnes pratiques de sécurité, tableau de bord.

Lien avec les cours avancés techniques et organisationnel

Présentation des sujets 1 à 7 pour le mémoire.

Architectures et protocoles de sécurité pour les accès au SI (AAA : authentification, Autorisations, Accounting)

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base pour accéder aux réseaux d'entreprise et protéger les accès aux actifs essentiels et support de l'entreprise : gestion des mots de passe, de ses informations personnelles, professionnelles et de son identité numérique.
Compétence : Gestion et maintien des conditions de sécurité des identités, comptes utilisateurs, droits et privilèges y compris pour le paiement électronique ou les architectures d'authentification tiers.
1/Identité numérique

2/Architecture d'autorisation : Annuaire, etc?

3/Architecture d'authentification

4/Stratégies de groupe
Ce dernier point s'effectuera sous forme d'exercice où il s'agit par une recherche bibliographique de mieux connaitre les attaques, vulnérabilités et outils de gestion pour appliquer les stratégies de groupes en conformité avec les bonnes pratiques

5/ Architectures et protocoles de sécurité pour le paiement électronique sur Internet pour comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base liées au paiement électronique (Oauth, tier de confiance,...)

Sécurité de base des matériels et des systèmes d'exploitation

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité, expliquer DICT, la différence avec la sureté de fonctionnement, mettre en place les mesures de base sur tout système, OS.
Compétence : Gestion et maintien des conditions de sécurité de base des matériels et systèmes d'exploitation.

Les mesures de sécurité avancées seront abordée en SEC108.

Architectures et protocoles de sécurité pour la virtualisation
Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les besoins de sécurité d'une machine virtuelle,

étendue des mesures de sécurité au Datacenters, Cloud (SaaS,IaaS,?),
Compétence : Applications des mesures de sécurité de base aux environnements virtualisés : VM, BYOD, ...

Appliquer les mesures de base.

Architectures et protocoles de sécurité pour les réseaux locaux, les mobiles et Internet

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base pour les réseaux, mettre en place la sécurité des VLAN, GSM (évolutions 3G/4G).
Compétence : Gestion et maintien des conditions de sécurité des réseaux.

Architectures et protocoles de sécurité pour la messagerie

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base sur les messages (stockage et transport) et architectures de messageries (Windows Exchange, Web, IMAP, configuration port SSL), des interactions avec les services de résolution de nom, d'adresse, d'authentification et d'annuaire.
Compétence : Gestion et maintien des conditions de sécurité de la messagerie.
Architectures et protocoles de sécurité pour la sauvegarde des données, des applications, des bases de données

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de base pour la protection des données en particulier l'application des mesures de sécurité via des architectures de sauvegardes (SAN, mécanismes, protocoles (SCSI, Zoning FC et LUN,FCoE et iSCSI).
Compétence : Gestion et maintien des conditions de sécurité des sauvegardes.

Architectures et protocoles de sécurité pour les architectures applicatives

Objectif : comprendre le fonctionnement et les vulnérabilités, développer, superviser les exigences de sécurité de base liées au déploiement et téléchargement d'applications, d'architectures API, Client serveur, front/back end, intergiciels, EAI,?,

Compétence : Gestion et maintien des conditions de sécurité des applications et logiciels.
Architectures et protocoles pour la protection des données : travail, domicile & mobilité

Objectif : comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base sur les donnés stockées et véhiculées dans les systèmes mobiles, lors de synchronisations d'ordinateur, Cloud des données personnelles, professionnelles, identifiants numériques en mobilité.
Compétence : Gestion et maintien des conditions de sécurité des données.

Révision

Objectifs : aptitudes et compétences

Objectifs :

Comprendre les objectifs, exigences et contraintes spécifiques à l'application des bonnes pratiques de la sécurité informatique

- Comprendre les mécanismes informatiques réseau, système, data et applicatifs de base,

- Apprendre les architectures techniques, protocoles et configuration en lien avec les bonnes pratiques de base à déployer sur un SI en vue de garantir une hygiène informatique de base,

- Apprendre les différents outils et techniques pour valider l'adéquation et la mise en place des bonnes pratiques, les tester.

- Apprendre à garantir des conditions opérationnelles de sécurité d'un système conformément aux politiques de sécurité organisationnelles, opérationnelles et techniques,

- Apprendre à intégrer la composante technique dans les procédures accompagnant la mise en place des bonnes pratiques,

- Être en mesure de prendre les décisions pour que l'entreprise mette en oeuvre des mesures techniques en réponse aux bonnes pratiques,

Compétences :

- Maintenir la sécurité du système de base conformément aux politiques organisationnelles,

- Appliquer les bonnes pratiques et mesures de sécurité de base,

- Déployer les solutions techniques adaptées aux bonnes pratiques de base sur un SI pour une hygiène informatique de base,

- Déployer les solutions techniques adaptées en fonction des contraintes de confidentialité, d'intégrité et de disponibilité des applications en entreprise,

- Sensibiliser aux objectifs de sécurité, les bonnes pratiques, leurs applications et les mesures adaptées,

- Prendre les décisions pour la mise en oeuvre des bonnes pratiques dans l'entreprise,

- Mettre en oeuvre les mécanismes informatiques réseau et développement logiciel de base,

- Rédiger et mettre en oeuvre des procédures de base pour la mise en place des bonnes pratiques,

- Vérifier la mise en place des bonnes pratiques,

- Tester les mesures et évaluer leur robustesse.

Prérequis

Bac+2 informatique, BAC + 2 SI ou SHS
UTC501, UTC502,UTC503,UTC504
UTC505 et RSX101.
L2 ou Bac+2

Il est conseillé de suivre SEC101 avant SEC105.

Délais d'accès

Le délai d'accès à la formation correspond à la durée entre votre inscription et la date du premier cours de votre formation.

- UE du 1er semestre et UE annuelle : inscription entre mai et octobre
- UE du 2e semestre : inscription de mai jusqu'à mi-mars

Exemple : Je m'inscris le 21 juin à FPG003 (Projet personnel et professionnel : auto-orientation pédagogique). Le premier cours a lieu le 21 octobre. Le délai d'accès est donc de 4 mois.

Planning

Légende:

Cours en présentiel

Cours 100% à distance

Mixte: cours en présentiel et à distance

Modalités	Lieux	Disponibilités	Prochaines sessions *	Tarif indicatif
	En ligne	Semestre 1	Prévue en 2025-2026	De 0 à 1.020 €
	En ligne	Semestre 2	Prévue en 2025-2026	De 0 à 1.020 €
	En ligne	Semestre 1	Prévue en 2026-2027	De 0 à 1.020 €
	En ligne	Semestre 2	Prévue en 2026-2027	De 0 à 1.020 €
	En ligne	Semestre 1	Prévue en 2027-2028	De 0 à 1.020 €
	En ligne	Semestre 2	Prévue en 2027-2028	De 0 à 1.020 €

*Selon les UEs, il est possible de s'inscrire après le début des cours. Votre demande sera étudiée pour finaliser votre inscription.

Modalités

Modalités pédagogiques :

Pédagogie qui combine apports académiques, études de cas basées sur des pratiques professionnelles et expérience des élèves. Équipe pédagogique constituée pour partie de professionnels. Un espace numérique de formation (ENF) est utilisé tout au long du cursus.

Modalités de validation :

Dossier
Ou examen sur table
Ou les 2
Pour valider cette UE, vous devez obtenir une note minimale de 10/20

Tarif

Mon employeur finance	1.020 €
Pôle Emploi finance	510 €
Je finance avec le co-financement Région	Salarié : 156 €
Je finance avec le co-financement Région	Demandeur d'emploi : 124,80 €

Plusieurs dispositifs de financement sont possibles en fonction de votre statut et peuvent financer jusqu'à 100% de votre formation.

Salarié : Faites financer votre formation par votre employeur

Demandeur d'emploi : Faites financer votre formation par Pôle emploi

Votre formation est éligible au CPF ? Financez-la avec votre CPF

Si aucun dispositif de financement ne peut être mobilisé, nous proposons à l'élève une prise en charge partielle de la Région Nouvelle-Aquitaine avec un reste à charge. Ce reste à charge correspond au tarif réduit et est à destination des salariés ou demandeurs d'emploi.

Pour plus de renseignements, consultez la page Financer mon projet formationopen_in_new ou contactez nos conseillers pour vous accompagner pas à pas dans vos démarches.

Passerelles : lien entre certifications

- CRN0803A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Cybersécurité
- LG025B21 - Bloc Informatique : Concevoir et réaliser l'architecture applicative d'un système d'information
- CYC9101A - Diplôme d'ingénieur Architecture et ingénierie des systèmes et des logiciels (AISL)
- CYC9104A - Diplôme d'ingénieur Informatique, réseaux, systèmes et multimédia (IRSM)

- CYC9106A - Diplôme d'ingénieur Cybersécurité
- CRN0802A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Systèmes d'information (SI)
- LG02501A - Licence 3 Informatique générale
- CRN0801A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Systèmes et réseaux
- CRN0803A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Cybersécurité
- CRN0801A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Systèmes et réseaux
- CRN0802A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Systèmes d'information (SI)

Avis des auditeurs

Les dernières réponses à l'enquête d'appréciation de cet enseignement :

↓ Fiche synthétique au format PDF

Taux de réussite

Les dernières informations concernant le taux de réussite des unités dcenseignement composant les diplômes

↓ Taux de réussite