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

Planning prévu au 19/12/24

SEC105-Architectures et Bonnes Pratiques de la sécurité des Réseaux, des Systèmes, des Données et des Applications

UE	Intervenant	Date	Début	Fin	Durée	H	
SEC105	LACOMME François	19/12/2024	13:30	17:30	04:00	4	
SEC105	LACOMME François	21/01/2025	13:30	17:30	04:00	4	
SEC105	PAULHAC Michaël	23/01/2025	08:15	12:15	04:00	4	
SEC105	PAULHAC Michaël	18/02/2025	08:00	12:00	04:00	4	
SEC105	PAULHAC Michaël	18/02/2025	13:30	17:30	04:00	4	
SEC105	LACOMME François	20/02/2025	13:30	17:30	04:00	4	
SEC105	LACOMME François	18/03/2025	10:00	12:00	02:00	2	
SEC105	LACOMME François	18/03/2025	13:30	17:30	04:00	4	
SEC105	PAULHAC Michaël	19/03/2025	13:30	17:30	04:00	4	
SEC105	PAULHAC Michaël	20/03/2025	08:00	12:00	04:00	4	
SEC105	LACOMME François	15/04/2025	09:00	12:00	03:00	3	
SEC105	LACOMME François	15/04/2025	13:30	17:30	04:00	4	
SEC105	PAULHAC Michaël	16/04/2025	08:00	12:00	04:00	4	
SEC105	PAULHAC Michaël	16/04/2025	13:30	17:30	04:00	4	
SEC105	PAULHAC Michaël	20/05/2025	08:00	12:00	04:00	4	
SEC105	LACOMME François	21/05/2025	13:30	16:30	03:00	3	
Total						**60**	

15 séances de 4h => 60h, dont examen

SEC105 - Cours Michaël PAULHAC et François LACOMME
Programme prévisionnel

001 - Sécurité et Réseaux -Introduction.pdf - 78 p.

Notions de base et enjeux de la sécurité

Les enjeux de la sécurité du S.I.
Les besoins de sécurité.
Vulnérabilités, menaces, attaques.
Panorama de quelques menaces.
Droits et organisation de la Cybersécurité en France.

002 - cyberedu_module_4_cybersecurite_organisation_02_2017.pdf - 62 p

La gestion de la cybersécurité au sein d'une organisation.

1.Intégrer la sécurité au sein d'une organisation
2.Intégrer la sécurité dans les projets
3.Difficultés liées à la prise en compte de la sécurité
4.Métiers liés à la cybersécurité

003 - cyberedu_module_3_reseau_et_applicatifs.pdf - 40 p.

Les aspects réseau et applicatifs (1re partie)

1. La sécurité du protocole IP
2. Sécurisation d'un réseau

003 - cyberedu_module_3_reseau_et_applicatifs.pdf - 39 p.

Les aspects réseau et applicatifs (2e partie)

3. Les bases de la cryptographie
4. La sécurité des applications web

004 - SEC105 - Dispo et sûreté de fonctionnement.pdf

Disponibilité et sureté de fonctionnement - 32 p.

Définitions
Les Datacenter
ANSI/TIA-942
Disponibilité et Haute disponibilité
Les composantes de la haute disponibilité
RTO / RPO
PCA / PRA

005 - SEC105 – Architectures et protocoles de sécurité pour les accès au SI.pdf - 22 p.

Contexte ; Risques d'attaque ; Défauts de conception
Standard 802.1x
AAA

006 - SEC105 – Gestion et maintien des conditions de sécurité des identités, comptes utilisateurs droits et privilèges.pdf - 32 p.

Gestion de l'identité numérique

L'identité personnelle

Identity & Access Management ; fondamentaux ; Composantes ; Les normes d'identité

007 - SEC105 – Controle d'accès et sécurité de l'information.pdf - 36 p.

Le contrôle d'accès

Modèles d'accès

Principe de moindre privilège

008 - SEC105 – Sécurité de base des matériels et systèmes d'exploitation.pdf - 15 p.

Maintien en Condition de Sécurité

Mise en place de mesures : Matériel ; OS

009 - SEC105 – Sécurité de base des matériels et systèmes d'exploitation - Virtualisation & cloud.pdf - 23 p.

Préambule ; Rappels ; Périmètre

Risques

Règles de contrôle

Et le Cloud ?

010 - SEC105 – Architectures et protocoles de sécurité pour la messagerie.pdf - 23 p.

Préambule

Identifier le besoin

Connaitre l'architecture

Cloisonner et filtrer

Antispam et de recherche de contenu malveillant

Utiliser des canaux de transport sécurisés

Se protéger contre les courriels illégitimes

011 - SEC105 – Architectures et protocoles pour la protection des données travail, domicile et mobilité.pdf - 34 p.

Risque

Démarche de réduction des risques

L'utilisateur nomade

L'équipement d'accès

Le canal d'interconnexion

Passerelles d'interconnexion

Les ressources du SI de l'entité

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

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