

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

## Présentation

### Prérequis

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

### Objectifs pédagogiques

**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 œuvre des mesures techniques en réponse aux bonnes pratiques,

### Compétences

1. Maintenir la sécurité du système de base conformément aux politiques organisationnelles,
2. Appliquer les bonnes pratiques et mesures de sécurité de base,
3. Déployer les solutions techniques adaptées aux bonnes pratiques de base sur un SI pour une hygiène informatique de base,
4. Déployer les solutions techniques adaptées en fonction des contraintes de confidentialité, d'intégrité et de disponibilité des applications en entreprise,
5. Sensibiliser aux objectifs de sécurité, les bonnes pratiques, leurs applications et les mesures adaptées,
6. Prendre les décisions pour la mise en œuvre des bonnes pratiques dans l'entreprise,
7. Mettre en œuvre les mécanismes informatiques réseau et développement logiciel de base,
8. Rédiger et mettre en œuvre des procédures de base pour la mise en place des bonnes pratiques,
9. Vérifier la mise en place des bonnes pratiques,
10. Tester les mesures et évaluer leur robustesse.

## Programme

### Contenu

#### 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.

Mis à jour le 26-04-2024



**Code : SEC105**

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 33.1.11B

75003 Paris

01 40 27 28 21

Mmadi Hamida

[hamida.mmadi@lecnam.net](mailto:hamida.mmadi@lecnam.net)

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 connaître 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 données 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

## Modalités de validation

- Projet(s)
- Examen final

## Description des modalités de validation

Dossier

Ou examen sur table

Ou les 2

## Bibliographie

Titre	Auteur(s)
« Sécurité informatique : Pour les DSI, RSSI et administrateurs », Ed. 5, Eyrolles, 2016, p. 645, ISBN: 978-2-212-11849-0	Laurent Bloch, Christophe Wolfhugel, Ary Kokos, G�r�me Billois, Arnaud Soulli�, Alexandre Anzala-Yamajako, Thomas Debize
« Cybers�curit� » : S�curit� informatique et r�seaux Ed. 5 - Editeur Dunod, 2016, ISBN: 978-2-10-074734-4	Gheraouti, Solange