SEC107 - Conception d'architecture de sécurité à partir d'un audit de sécurité

Mis à jour le 02-04-2024

Code : SEC107

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

Bac+2 informatique, (ou L2)
UTC501, UTC502, UTC503, UTC504, UTC505, SEC105

Objectifs pédagogiques

Ce cours vise le soutien aux infrastructures de cyber défense, il permet d'acquérir des compétences pour permettre de déterminer comment un dispositif de sécurité complexe devrait fonctionner tant dans ses capacités de sécurité offensives que défensives comme lever les doutes, neutraliser une attaque mais également pour en comprendre le mode opératoire. Il permettra également de comprendre comment le changement de conditions, d'opérations ou d'environnement pourraient l'affecter.

il enseigne la mise en place d'outillage pour la collecte et l'analyse des flux et des données à partir de la conception et le maintien de l'outillage de cyber défense : système de détection d'intrusion, scanner de vulnérabilités, firewall, trafic réseau afin de mettre en place un système de défense plus robuste pour amélioration continue et l'atténuation de la menace.

- Comprendre les exigences et contraintes spécifiques à la mise en place d'une architecture de sécurité, en particulier le principe de traçabilité,
- Comprendre les différents dispositifs présents pour concevoir une architecture de sécurité robuste,
- Comprendre les mécanismes informatiques : réseau, système, data et applicatif nécessaires à la mise en place d'une architecture de sécurité,
- Apprendre les architectures techniques, protocoles et configurations pour mettre en place une architecture de sécurité,
- Apprendre les différents outils et techniques pour valider l'adéquation et la mise en place d'une architecture de sécurité, la tester.
- Apprendre à garantir des conditions opérationnelles de sécurité d'un Centre de Sécurité Opérationnel conformément aux politiques de sécurité organisationnelles, opérationnelles et techniques,
- Apprendre à intégrer la composante technique dans les procédures accompagnant la mise en place sécurité d'un Centre de Sécurité Opérationnel,

Compétences

1. Concevoir et optimiser une architecture de sécurité, intégrant les dispositifs de sécurité qui la composent ainsi que les composants applicatifs, réseaux et systèmes,
2. Savoir exprimer ses besoins dans un langage de modélisation (UML), et en particulier appliquer les principes de traçabilité aux exigences de l'organisation,
3. Maintenir cette architecture de sécurité conformément aux politiques de sécurité PSSI,
4. Appliquer les bonnes pratiques et mesures de sécurité de base,
5. Déployer les solutions techniques adaptées à l'architecture de sécurité d'un SI,
6. Déployer les solutions techniques de l'architecture de sécurité afin de maintenir les conditions de sécurité et de disponibilités opérationnelles de l'architecture de sécurité,
7. Intégrer l'architecture de sécurité aux objectifs de sécurité,
8. Prendre les décisions pour la mise en œuvre de l'architecture de sécurité,
9. Rédiger et mettre en œuvre des procédures de base pour la mise en place des bonnes pratiques,
10. Vérifier la mise en place des bonnes pratiques, les tester et évaluer leur robustesse.
11. Être en mesure de prendre les décisions dans un Centre de Sécurité Opérationnel pour que l'entreprise mette en œuvre une architecture de sécurité robuste et évolutive,

12. Être en mesure d’analyser la sécurité lors de l’intégration de composants techniques nouveaux ou existant tant pour des protocoles que des configurations logicielles ou utilitaires.

Programme

Contenu

Cours 0 Introduction aux architectures de sécurité pour une défense en profondeur avancée

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, bonnes pratiques de sécurité, tableau de bord.

Temps 1 - Se protéger « by design » : conception d’architectures de sécurité défensives par le cloisonnement des flux et services

Objectif : comprendre et configurer une DMZ

Cours 1 Principe de cloisonnement : bastion, filtrage & relayage

Cours 2 Firewall, règles de firewall et matrice de flux

Cours 3 Les zones : mise en place de la DMZ

Étude par projet d’une architecture complexe :

Temps 2 - Analyser : Architectures de sécurité défensive pour la centralisation des flux et des services (Centre pour les Opérations de sécurité)

Objectif : comprendre et montrer les différents services et outillages de cyberdéfense visant l’analyse au sein d’un centre de sécurité opérationnel (SOC, CERT) et d’une zone démilitarisée (DMZ).

Cours 4 : Les vulnérabilités et les scanners de vulnérabilités

Cours 5 : Les intrusions et la détection d’intrusion

Cours 6 : Corrélation pour l’analyse de sécurité (1)

Cours 7 : Corrélation pour l’analyse de sécurité (2)

Cours 8 : SOC et CERT

Étude par projet de la corrélation pour l’analyse de sécurité

Temps 3 Architecture offensive par veille et pièges

Cours 10: Principe des « pots de miel » (Honeypots)

Cours 11 : outils pour la surveillance sur Internet

Cours 12 : Révision

Modalités de validation

- Projet(s)
- Mémoire
- Examen final

Description des modalités de validation

QCM
Etude de cas
Travail personnel : Examen final Projet(s)

Bibliographie

Titre	Auteur(s)
1. Enterprise Security: A Data-Centric Approach to Securing the Enterprise	Woody, Aaron - Editeur: Packt Publishing -2013 - 324p ISBN: 978-1-84968-596-2