SEC202 - SACE Sécurité d'Architectures Complexes et Émergentes

Mis à jour le 04-12-2024

Code : SEC202

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Contact national :

EPN05-Informatique

2 rue Conté
33.1.10A
75003 Paris

Marlène DEFFON
marlene.deffon@lecnam.net

Présentation

Objectifs pédagogiques

L'objectif de cette Unité d'Enseignement sera d'une part d'approfondir les principes de sécurité globale et de défense en profondeur appliquées aux architectures de sécurité rencontrés dans les réseaux complexes et émergents, et d'autre part d'acquérir des savoir-faire pour la conception, planification et gestion de leur sécurité dans les centres opérationnels de sécurité (SOC).

Compétences

Le cursus vise 3 grandes compétences :

Appréhender et analyser les situations de menaces des systèmes émergents (SE) (Cloud, Fog, Edge)

Comprendre et concevoir la sécurité de ces nouvelles architectures et protocoles : réseaux et systèmes d'informations complexes et émergents (Cliuod, datacenter,...), IoT, dont les systèmes véhiculaires, les systèmes drones, la chaine de blocs,

Appliquer des exigences, normes et méthodes de conception, d'analyse adaptées à chacune de ces 3 niveaux d'architectures et en particulier les IoT, dont les systèmes véhiculaires, les systèmes drones, la blockchain,

Exemples de compétences demandées par l'entrperise :

- Participer à la définition de l'architecture cloud,
- Faciliter l'intégration des nouveaux produits connectés en assurant des spécifications / interfaces fonctionnelles cohérentes avec les produits constituant le tableau électrique et l'architecture
  cloud.
- Participer à l'AMDEC système et aux analyses de mauvais usages et de positions de repli.

Programme

Contenu

TEMPS 1 : NOUVEAUX CHALLENGES DE LA SÉCURITÉ DES ARCHITECTURES ÉMERGENTES (CLOUD, FOG, EDGE)

TEMPS 2 : LA SECURITE DES IoT, DES SYSTEMES INDUSTRIELS COMME NOUVEAUX SYSTÈMES INFORMATIQUES ÉMERGENTS

TEMPS 3 : PRÉSENTATION DE MODELES D'ARCHITECTURES DE SECURITE ET DE MODELES THREAT MODELLING (APPROCHE VERTICALE PAR TYPE D'APPLICATIONS

LA SECURITE DES SYSTÈMES D'INFORMATION VÉHICULAIRES CONNECTÉS ET AUTONOMES (COURS+TD+TP)
LA SECURITE DES SYSTÈMES DRONES (COURS+TD+TP)
LA SECURITE DES SYSTÈMES VIA LA BLOCKCHAIN ET DES SMARTCONTRACTS (COURS+TD+TP)

TEMPS 4 RECHERCHE BIBLIOGRAPHIQUE D'UN SUJET CHOISI OU IMPOSÉ

Modalités de validation

- Contrôle continu
- Projet(s)
- Mémoire

Description des modalités de validation

Controle continu

Recherche bibliographique individuelle