SEC202 - SACE Sécurité d'Architectures Complexes et Émergentes

Mis à jour le 15-07-2026

Code : SEC202

Unité d'enseignement de type cours

6 crédits

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

Responsabilité nationale : EPN03 - Electroniques, électrotechnique, automatique et mesure (EEAM) / Véronique LEGRAND

Contact national :

EPN03 Equipe pédagogique Systèmes éco-électriques

292 rue Saint-Martin
21-0-41
75003 Paris
01 58 80 85 01
Alexandre Pigot
alexandre.pigot@lecnam.net

Présentation

Prérequis

Les auditeurs doivent présenter les pré-requis suivants, l'absence de ces prérequis peut constituer un frein à la réussite de l'UE : :

bac+4 informatique requis impérativement

en outre les connaissances avancées en sécurité sont requises dans les domaines des architectures, protocoles des systèmes, systèmes d'exploitation, réseaux avancés, ceux qui ont validé SEC107, SEC108 ont reçu ces enseignements.

*TM : threat modelling

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 la menace de systèmes émergents (SE) (Cloud, Fog, Edge) avec des outils TM*

Comprendre et concevoir la sécurité de ces nouvelles architectures et protocoles : réseaux et systèmes d'informations complexes et émergents (Cloud, datacenter, Applications Web, …) 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'entreprise :

- 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 la modélisation de la menace (analyse de causes avec différents outils des différents domaines: OWASP, AMDEC) ainsi qu'à l'analyse de mauvaises pratiques .

Programme

Contenu

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

TEMPS 2 : LA SÉCURITÉ DES IoT ET DES SYSTÈMES INDUSTRIELS COMME NOUVEAUX SYSTÈMES INFORMATIQUES ÉMERGENTS

TEMPS 3 : PRÉSENTATION DE MODÈLES D'ARCHITECTURES DE SÉCURITÉ ET DE MODÈLES "THREAT MODELLING" (APPROCHE SECTORIELLE, PAR TYPE D'APPLICATIONS).

A) LA SÉCURITÉ DES SYSTÈMES D'INFORMATION VÉHICULAIRES CONNECTÉS ET AUTONOMES (COURS+TD+TP)
B) LA SÉCURITÉ DES SYSTÈMES DRONES (COURS+TD+TP)
C) LA SÉCURITÉ DES SYSTÈMES VIA LA BLOCKCHAIN ET DES SMART CONTRACTS (COURS+TD+TP)

TEMPS 4 RECHERCHE BIBLIOGRAPHIQUE D'UN SUJET CHOISI OU IMPOSÉ

TEMPS 5 CONTRÔLE FINAL

Modalités de validation

- Contrôle continu
- Projet(s)
- Mémoire
- Examen final

Description des modalités de validation

CONTRÔLE CONTINU (TRAVAUX PRATIQUES OU DIRIGÉS)

MINI-PROJET : Recherche bibliographique individuelle

EXAMEN FINAL PRESENTIEL