ACADÉMIE
DE CRÉTEIL
Liberté
Égalité
Fraternité

BLOC 3 - SLAM

Propositions de ressources didactiques et technologiques

Présentation : Amal Hecker – amal.hecker@ac-creteil.fr

Sommaire

1. Structure du tableau des propositions didactiques – Réseau Certa

Bloc de compétences 1, 2 SISR , 2 SLAM, 3 SISR ou 3 SLAM – Nom du bloc			
Contexte professionnel : *Ici la description de l'entreprise prestataire de services informatiques dans laquelle l'étudiant joue le rôle de collaborateur*			
Thème : Ici le nom de la compétence globale travaillée (c*ompétence x.y*)			**Ici le semestre concerné (1, 2 ou 3-4)**
ici une explication de la compétence du point de vue du métier et des bénéfices pour l'organisation cliente. Si l'entreprise cliente est la même pour toute les séquences du cours, on peut la présenter ici.			
Séquence *numéro*	Mission confiée	Compétences travaillées	Savoirs associés
Ici durée estimée pour l'acquisition des savoirs	ici la présentation de la mission confiée pour une entreprise cliente	ici les compétences détaillées travaillées	Ici les savoirs à mobiliser ou à acquérir
	Prérequis	Indicateurs de performance	Transversalités
	ici les séquences à avoir réalisées avant de débuter cette séquence	ici les indicateurs de performance attendus, ils sont tirés du référentiel	ici les transversalités possibles avec les autres séquences du même bloc ou d'un autre bloc.
Séance 1	Travail confié	Ressources	Résultats attendus
Ici durée estimée	ici la description du travail à accomplir (réalisable dans le temps imparti)	ici la liste de ce qui doit être fourni à l'étudiant pour accomplir la tâche	ici la description de ce qui doit être produit à la fin de la séance
Séance 2…	Travail confié…	Ressources…	Résultats attendus…

2. Bloc 3 – 1ère année

a. Semestre 1

3.1. Protéger les données à caractère personnel

- Sensibilisation et communication sur les DCP
- Traitement des données à caractère personnel
- Analyse d'impact relative à la protection des données et mise en place de mesures correctives

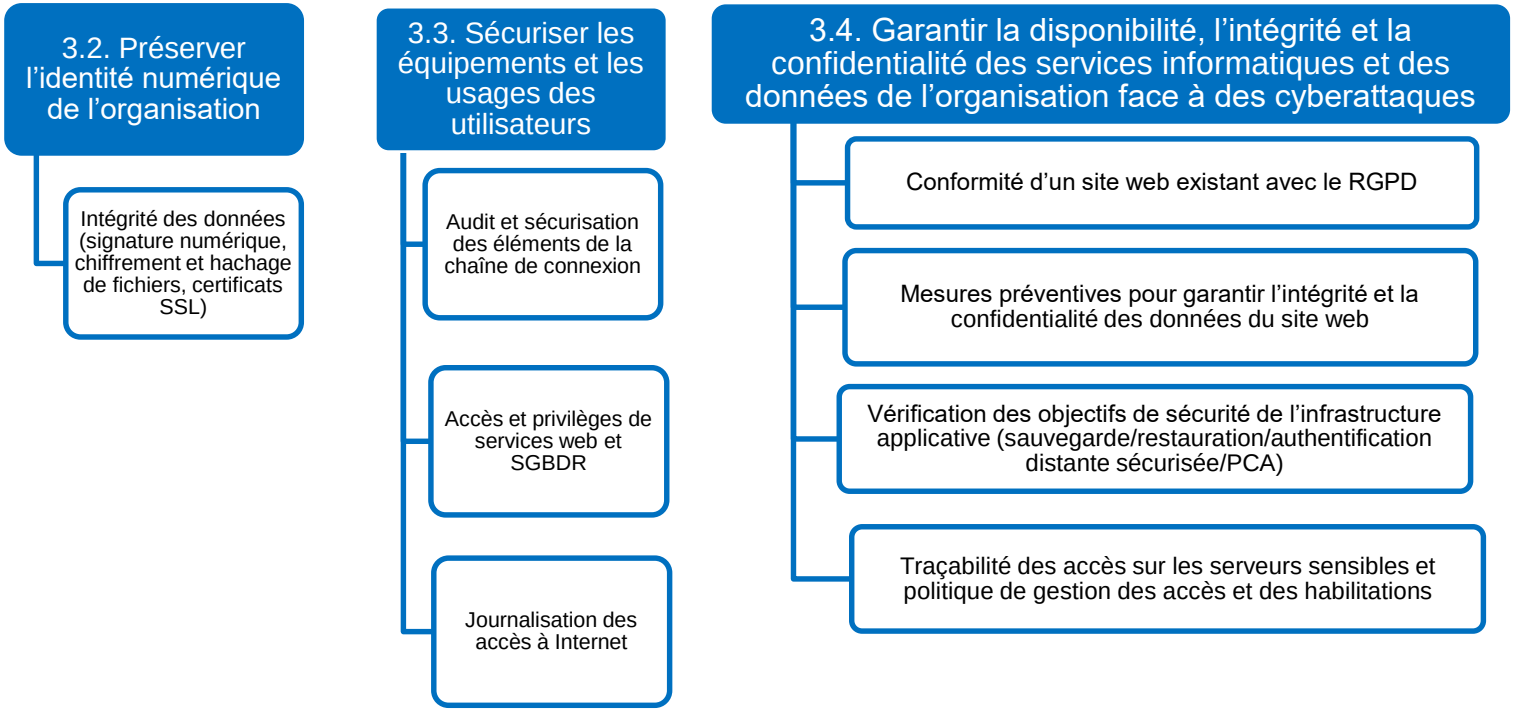
3.2. Préserver l'identité numérique de l'organisation

- Identité numérique d'une entreprise et évaluation des menaces associées à sa présence digitale
- Initiation aux techniques, méthodes et moyens de la preuve électronique

3.3. Sécuriser les équipements et les usages des utilisateurs

- Sensibilisation des utilisateurs aux cyber menaces, risques et promotion des bonnes pratiques de sécurité numérique
- Techniques de sécurisation du poste de travail (identification et authentification, mise à jour des OS, anti-virus, pare-feu)
- Accès et privilèges appropriés pour les utilisateurs

b. Semestre 2


3.2. Préserver l'identité numérique de l'organisation
Intégrité des données (signature numérique, chiffrement et hachage de fichiers, certificats SSL)
3.3. Sécuriser les équipements et les usages des utilisateurs
Audit et sécurisation des éléments de la chaîne de connexion
Accès et privilèges de services web et SGBDR
Journalisation des accès à Internet
3.4. Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques
Conformité d'un site web existant avec le RGPD
Mesures préventives pour garantir l'intégrité et la confidentialité des données du site web
Vérification des objectifs de sécurité de l'infrastructure applicative (sauvegarde/restauration/authentification distante sécurisée/PCA)
Traçabilité des accès sur les serveurs sensibles et politique de gestion des accès et des habilitations

c. Ressources documentaires

Détail des séquences : https://reseaucerta.org/didactique/scenarios-pedagogiques-cned/

ANSSI : Kit de l'ANSSI de la « sécurité des données », « Recommandations pour la sécurisation des sites Web

MOOC SecNumEdu : chapitres 2 - 4

Manuel CEJM – Thème 4 – question 2 : le numérique dans l'entreprise et la protection des données – Edition Foucher

Pochette SIO Cybersécurité – Edition Delagrave

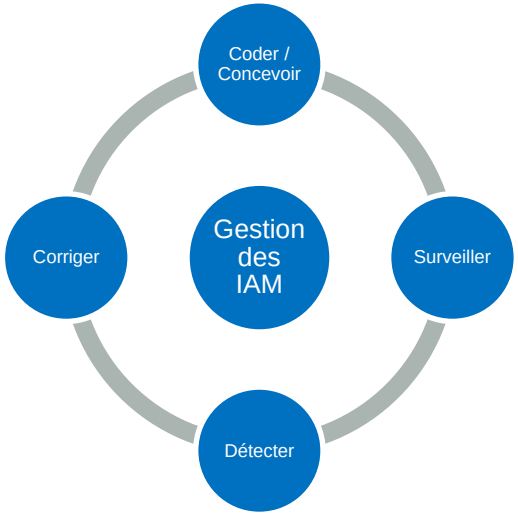
Introduction à la cybersécurité, Camille de sagazan, Ellipses

CERT-FR : centre gouvernemental de veille, d'alertes et de réponse aux attaques informatiques

CNIL :

- MOOC RGPD
- Fiche « sécurité des données : les règles essentielles pour démarrer »
- Fiche de registre des DCP / AIPD – Analyse d'impact relative à la protection des données
- Guide du développeur

3. Bloc 3 – SLAM - 2ème année



3.5B – Assurer la cybersécurité d'une solution applicative et de son développement - compétences

Participer à la vérification des éléments contribuant à la qualité d'un développement	Prendre en compte la sécurité dans un projet de développement d'une solution applicative	Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité
Prévenir les attaques	Analyser les connexions (logs)	Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures

a. Propositions de séquences – Ressources didactiques – Réseau Certa

Sensibiliser à la sécurité des applications web	Réaliser un audit de sécurité basé sur les tests d'intrusion d'une application web	Corriger les vulnérabilités recensées dans un rapport d'audit de sécurité
Participer au cycle de développement sécurisé d'une solution applicative	Mettre en œuvre une solution de gestion des identités et des autorisations	Sécuriser une base de données NoSQL

a. Sensibiliser à la sécurité des applications web

Compétences / Savoirs	Labo	Outils / Ressources
• Prévenir les attaques • Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures	• Tester les attaques XSS, XML, les injections SQL et upload • Analyser le code correspondant aux trois niveaux de sécurité	• Application web vulnérable : DVWA, OWASP Mutillidae II (Github) Metasploitable 2 • Exploit-db.com • www.xss-payloads.com/ • https://owasp.org/www-project-top-ten • Productions OWASP sur le réseau Certa (P. Dignan)
• Sécurité du développement d'application : tests de sécurité, audit de code • Vulnérabilités et contre-mesures sur les problèmes courants de développement		

b. Réaliser un audit de sécurité basé sur les tests d'intrusion d'une application web

Compétences / Savoirs	Labo	Outils / Ressources
• Prévenir les attaques • Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures • Participer à la vérification des éléments contribuant à la qualité d'un développement informatique	• Installer et configurer l'environnement applicatif pour les tests d'intrusion • Construire le modèle de menaces de l'architecture applicative • Générer le rapport des menaces des éléments du diagramme de flots de données • Réaliser un test d'intrusions (*pentest Greybox, WhiteBox*) • Rédiger le rapport du test d'intrusions	• Outils de pentest : https://www.lemondeinformatique.fr/actualites/lire-10-outils-de-pen-test-pour-hackers-ethiques-75526.html • Architecture applicative présentant des vulnérabilités • MITRE : CVE / CWE • Outil de modélisation des menaces basée sur les vulnérabilités connues (Microsoft Threat Modeling Tool, OWASP Threat Dragon) • Modèle de menaces STRIDE
• Sécurité du développement d'application • Vulnérabilités et contre-mesures sur les problèmes courants de développement		

c. Corriger les vulnérabilités recensées dans un rapport d'audit de sécurité

Compétences / Savoirs	Labo	Outils / Ressources
• Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité • Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures	• Analyser le rapport de tests d'intrusion et effectuer les corrections logicielles nécessaires • Réaliser un test post-audit des vulnérabilités les plus critiques après correction	• Outils de pentest : https://www.lemondeinformatique.fr/actualites/lire-10-outils-de-pen-test-pour-hackers-ethiques-75526.html • Architecture applicative présentant des vulnérabilités • MITRE : CVE / CWE • OWASP Top-10
• Sécurité du développement d'application • Vulnérabilités et contre-mesures sur les problèmes courants de développement		

d. Participer au cycle de développement sécurisé d'une solution applicative

Compétences / Savoirs	Labo	Outils / Ressources
• Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité • Participer à la vérification des éléments contribuant à la qualité d'un développement informatique	• Appliquer les bonnes pratiques de sécurité dans la conception • Réaliser une revue de code de sécurité d'une solution applicative • Mettre en place le suivi des bugs de sécurité • Créer un pipeline CI/CD en intégrant les tests de sécurité • Traiter/rédiger un récit de risque • Traiter/rédiger un récit de sécurité	• SAFECode • Secure coding guidelines for Java SE • Livre blanc Cybersecurity by design de Thalès • Fuzzing • Outil de scan de vulnérabilités et de tests par injection de données aléatoires (fuzzing) • Outil d'analyse de code SonarQube • Récits de risque • Récits de sécurité
• Sécurité du développement d'application • Environnement de développement et de production		

e. Mettre en œuvre une solution de gestion des identités et des accès

Compétences / Savoirs	Labo	Outils / Ressources
• Analyser les connexions • Prévenir les attaques • Participer à la vérification des éléments contribuant à la qualité d'un développement informatique	• Installer et configurer une solution IAM • Configurer la gestion des accès et des autorisations des utilisateurs • Journaliser les accès • Mettre en place une authentification SSO sécurisée • Configurer la connexion à une application en utilisant des fournisseurs d'authentification externes	• Solutions d'IAM (keycloak, OpenID Connect, OAuth2) • UMLSec
• Sécurité du développement d'application : authentification, habilitations et privilèges des utilisateurs		

f. Sécuriser une base de données NoSQL

Compétences / Savoirs	Labo	Outils / Ressources
• Analyser les connexions • Prévenir les attaques • Participer à la vérification des éléments contribuant à la qualité d'un développement informatique	• Installer et configurer l'architecture applicative • Réaliser un audit de sécurité de la base de données et du serveur • Journaliser les accès • Rédiger un rapport d'audit (documenter les vulnérabilités et proposer un plan d'action des mesures correctives) • Corriger les vulnérabilités de l'architecture applicative	• Base de données NoSQL • Outils d'audit de sécurité et de tests (nosqlmap)
• Sécurité du développement d'application : authentification, habilitations et privilèges des utilisateurs		

Autres pistes …

Sécurité client lourd, mobile

Sécurisation de l’environnement de développement

Réponse à incident de sécurité logicielle et exploitation des logs

Tolérance aux intrusions

Sécurité des applications dans le cloud

Ressources

Les séquences proposées se trouvent sur le site du réseau Certa dans la rubrique Didactique, cliquer ici.
Il est vivement recommandé d'utiliser des machines virtuelles pour l'installation des applications vulnérables et l'exécution des tests d'intrusion afin de ne pas compromettre la sécurité de vos systèmes physiques.

L'ensemble des ressources exploitées pour la production de ces scénarios pédagogiques est répertorié dans mon pearltrees :

https://www.pearltrees.com/hecker_sio/cybersecurite/id38274889