USRS7R - Risques et certifications Cyber pour le "Supply Chain Management"

Mis à jour le 13-05-2024

Code : USRS7R

Unité spécifique de type mixte

4 crédits

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

USRS3V Analyse des enjeux principes, doctrines de sécurité - Description de la menace, attaques, vulnérabilités
USRS3P Système d'exploitation : principes, virtualisation, introduction aux automates et systèmes embarqués
USRS3Q Réseaux et protocoles, Réseaux industriels
USRS3S Base de donnée et structures de données des SI : ERP, des systèmes industriels, SCADA, MES,
USRS3X Dispositifs de sécurité : DMZ, Pare-feu, IDS, principes généraux et configuration du SI

Objectifs pédagogiques

L'objectif est de prendre en compte les spécificités informatiques du "Supply Chain" Management. Dans ce contexte, certains maillons de la chaîne logistique semblent jouer un rôle particulier, les systèmes d'information du "Supply Chain" (IS-SC) des organisations civiles ou régaliennes deviennent de plus en plus critiques car ils complexes et interconnectés via des réseaux informatiques en nuage qui comportent une multitude de composants informatiques, dont des datacenters, des objets connectés, des capteurs qui vont permettre de suivre l'avancée du processus logistique.

Cette complexité expose les IS-SC à de nombreuses vulnérabilités, par ailleurs, les chaines d'approvisionnement sont au coeur des préoccupation des cyber attaquants par l'interet qu'elles représentent. Les cyberattaques sur la chaîne d'approvisionnement peuvent entraîner d'importantes pertes financières et de réputation. Par conséquent, les organisations doivent mettre en œuvre des mesures de cybersécurité.

L'objectif pédagogique du cours sera d'apprendre, concevoir et appliquer les principes fondamentaux de la sécurité des systèmes d'information logistiques de la Supply Chain, de modifier leurs configurations en réponse aux enjeux ou incidents, enfin d'analyser les normes et cadres réglementaires à partir d'une connaissance des architectures et techniques des SI-SC (TMS, WMS, ERP, etc.). Le cours apprendra également une méthodologie de référence pour intégrer la sécurité dans les projets.

Une partie est largement consacrée aux risques et certifications pour le "Supply Chain Management », elle intégrera en outre une application concrète pour prendre en compte les risques sur la SC liées au changement climatique au travers de travaux dirigés sur les thématiques suivantes :

- USRS7R TD1 TE Travail dirigé : identifier l'introduction des éléments de l'impact écologiqies dans la chaine d'approvisionnement (prendre connaissance de l'article ou similaire de "Gera, Rajat, Priyanka Chadha, Manmeet Bali Nag, Sahiba Sharma, Heena Arora, Anjum Parvez, and Lebedinskaya Yuliya Sergeevna. "A systematic review of green supply chain management practices in firms." *Materials Today: Proceedings* 69 (2022): 535-542.").
- USRS7R TD2 TE : L'objectif est d'élaboter un indicateur de performance environnementale dans la SC et l'organisation.
- USRS7R TD3 TE Travail dirigé TE : positionnement des questions environnementales dans le processus cyber et SC
- USRS7R TD4 TE : Audit d'un composant du SI, estimation via un indicateur environnemental.
- USRS7R TD F TE Evaluation des risques environnementaux et leur classification pour la SC

Compétences

La clé de la maturité cyber d'une entreprise repose sur la capacité d'appliquer les bonnes pratiques cyber de façon adaptée à l'organisation, la mise en place d'un cycle de certification et la connaissance et les capacités d'appliquer les référentiels. Les compétences visées seront :

- Identifier par une analyse technique les enjeux des systèmes de défense appliqués au systèmes industriels,
- Modéliser et configurer les zones de sécurité (zones et conduits),
  Identifier et évaluer les architectures techniques de sécurité complexes de cloisonnement et autres principes de sécurité,
- Savoir maintenir en situation d'incident ou même de crise les conditions de sécurité opérationnelles.

Programme

Contenu

TEMPS 1 Le IS-SC et ses enjeux cybersécurité

Le processus de cybersécurité d'une Supply chain (IS-SC) via la certification
Intégration dans un management des risques de l'organisation
Positionnement de la certification d'un IS-SC dans ce processus.
Eléments de langage : expression des exigences de sécurité - évaluation complète - attente d'une certification et de contrôles - mise en oeuvre de contrôles - validation et vérification - conformité.
Perte de disponibilité, intégrité, condfidentialité et traçabilité (DICT),
Perte de "vie privée"
Processus de l'analyse de risques cyber : enjeux, processus et bien informationnels

Le IS-SC , la gestion des risques cyber (2) :

Modèle ISO 27x
Identification des risques cyber
Estimation des risques
Mise en place d'indicateurs,
Evaluation des métriques vis à vis du DICT,Perte de "vie privée"

TD1 : Travail dirigé : reconstitution d'une chaine d'approvisionnement, identification de la normalisation cyber, apprentissage de l'écosysteme cyber
TD2 : Audit d’un composant du SI, obtention d'un indicateur de compromission, analyse CVSS.

TEMPS 2 Anatomie d'un référentiel

éléments de langage, clauses, objectifs de sécurité, mesures de sécurité, bonnes pratiques
Exemples de certification : homologation, principes.
Scenario opérationnel et stratégique,
Estimation du risque (qualitatif, quantitatif)(vraissemblance)
Analyse d'un indicateur de risque : CVSS,

TD3 : cas concret de l'analyse CVSS et calcul du risque

TEMPS 3 Référentiels et certifications

Application de l'analyse de risque au IS-SC
Analyse de risques du IS-SC d'une organisation
Généralités et éléments de langage - définitions
Cartographie des actifs,
Méthodologie et méthode (EBIOS-RM , AMDEC)
Identification des risques dans la SC
TD4 : Recherche bibliographique sur les analyses de risque
TD4 : Exemple d'une homologation

Transition écologique et supply chain

Intégration des risques environnementaux à l'IS-SC.
Les transitions numérique et écologique sont du ressort du supply manager de l'organisation, il doit désormais ajouter la traçabilité environnementale des produits à ses activités, l'IS-SC intégrera des fonction de gestion optimale de flux de matières premières et des coûts environnementaux, en optimisant les choix d'implantation de la SC et donc de l'IS-SC. Ce TD/TP au travers d'un cas d'étude permettra de décrire ces obligations métiers.
TD1 TE Travail dirigé : identifier l'introduction des éléments de l'impact écologiqies dans la chaine d'approvisionnement (prendre connaissance de l'article ou similaire de "Gera, Rajat, Priyanka Chadha, Manmeet Bali Nag, Sahiba Sharma, Heena Arora, Anjum Parvez, and Lebedinskaya Yuliya Sergeevna. "A systematic review of green supply chain management practices in firms." Materials Today: Proceedings 69 (2022): 535-542.").
TP1 : découverte d'un IS-SC et ses spécificités
TD2 TE : L'objectif est d'élaboter un indicateur de performance environnementale dans la SC et l'organisation.
TD3 TE Travail dirigé TE : positionnement des questions environnementales dans le processus cyber et SC
TD4 TE : Audit d'un composant du SI, estimation via un indicateur environnemental.

Maintenir la et envisager éventuellement des évolutions de programme et des interventions, pour s'adapter aux nouveaux enjeux d'assurabilité dus notamment au dérèglement climatique, mais aussi aux modifications des métiers amenés par l'intelligence artificielle par exemple,
- Développer également des formations courtes, permettant notamment aux professionnels du secteur de satisfaire aux exigences règlementaires tout en suivant un programme de qualité,
- Veiller à une offre accessible sur l'ensemble du territoire.

Modalités de validation

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

Description des modalités de validation

controle continu : 50 %

devoir sur table : 50 %