EBIOS Risk Manager, préparation à la certification LSTI

Analyse de risques cyber APT et écosystème

Séminaire de 2 jours - 14h
Réf : IVH - Prix 2024 : 2 090CHF HT

La méthode EBIOS RM (2018) permet d'apprécier et de traiter les risques relatifs à la sécurité des SI et plus particulièrement le cyber risque en se fondant sur une expérience éprouvée en matière de conseil SI et d'assistance MOA. Ce séminaire vous apportera toutes les connaissances nécessaires à sa mise en œuvre en situation réelle.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les enjeux sur les risques cyber : la cyber défense par le risque

Évaluer en quoi le nouvel EBIOS s'adapte (ou pas) aux enjeux actuels de sécurité

Comprendre l'approche de la gestion de risque proposée

Appréhender le vocabulaire et les concepts développés par l'ANSSI

Réaliser une étude complète via l'ensemble des ateliers proposés

EXEMPLE

Des études de cas dans un contexte industriel et tertiaire permettront de comprendre et pratiquer la méthode.

LE PROGRAMME

dernière mise à jour : 12/2019

1) La cybermenace dans l'actualité

- Les cyber vols et le cyber espionnage de données sensibles.
- Vers une nouvelle guerre froide Est-Ouest, USA-Chine.
- Les dénis de services d'envergure mondiale.
- Les groupes de hackers organisés, le rôle des agences de renseignements.
- Phishing/ingénierie sociale, Spear phishing : des scénarios bien rodés.
- Les APT : persistance et profondeur des attaques.
- Vol de données sensibles, intrusions réseaux, malwares, bots/botnets et ransomwares.

2) Identification et analyse de la cyber menace

- L'approche des militaires appliquée au monde cyber.
- L'approche US avec le Find, Fix, Track, Target, Engage, Assess.
- La cyber kill chain comme base de description. Exemple type : Lockheed Martin.
- Les phases Reconnaissance, Weaponization, Delivery, Exploit, Installation, Control (C2). Actions on Objectives.
- Le portrait robot d'une attaque ciblée selon l'ANSSI.
- Les phases du processus (Connaître, Rentrer, Trouver, Exploiter).
- L'identification des chemins d'attaque directs et indirects.

3) La méthode EBIOS

- Rôle de l'ANSSI et du club EBIOS.

PARTICIPANTS

RSSI ou correspondants sécurité, architectes sécurité, directeurs ou responsables informatiques, ingénieurs, chefs de projets (MOE, MOA) devant intégrer des exigences de sécurité.

PRÉREQUIS

Connaissances de base en management de risques et en cybersécurité, ou connaissances équivalentes à celles apportées par les stages BYR et ASE ou BYR et AIR.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- EBIOS face aux enjeux de la LPM.
- Apport de la nouvelle méthode EBIOS RM (2018) et EBIOS 2010.
- La compatibilité EBIOS RM versus ISO 31000 et ISO 27005.

4) Les fondamentaux de la méthode

- Valeur métier, bien supporté, écosystème, partie prenante.
- Approche par conformité versus approche par scénarios de risques.
- Prise en compte des menaces intentionnelles sophistiquées de type APT.
- Appréciation de son écosystème et des parties prenantes critiques de rang 1, 2, 3.
- EBIOS RM au processus d'homologation de la LPM et de la directive NIS.
- Règles de sécurité de l'approche par conformité (guide d'hygiène, mesures LPM/NIS…).
- Processus Gestion de Risques comme mesure de la gouvernance SSI.

5) Les objectifs de EBIOS RM

- Identifier le socle de sécurité adapté à l'objet de l'étude.
- Être en conformité avec les règlements de sécurité (métier/juridique/contractuel).
- Identifier et analyser les scénarios de haut niveau en intégrant l'écosystème et les parties prenantes.
- Identifier et impliquer les mesures de sécurité pour les parties prenantes critiques.
- Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration.
- Les axes prioritaires d'amélioration : la sécurité et les points faibles exploitables des attaquants.
- Conduire une étude de risque détaillée visant, par exemple, l'homologation type ANSSI.

6) Les activités de la méthode (1 et 2)

- 1. Atelier – Cadrage et socle de sécurité :
- Quelles valeurs métiers, bien, supports faut-il cartographier ?
- Quels événements à redouter, vus de l'activité métier ?
- Quel socle de sécurité intégrer : ANSSI, PSSI interne… ?
- Quels référentiels de réglementation identifier comme obligatoires ?
- 2. Atelier – Sources de risque et objectifs visés :
- Quelle attractivité des valeurs métiers, cyber attaquants ?
- Quelle implication des métiers dans la connaissance des sources de risques ?
- Quels critères pour évaluer les couples SR-OV : l'évaluation des ressources et motivation des groupes attaquants.

Etude de cas : Présentation des ateliers 1 et 2.

7) Les activités de la méthode (3, 4 et 5)

- 3.4. Atelier – Scénarios stratégiques et opérationnels :
- Quelles sont les parties prenantes de l'écosystème ?
- Quels scénarios vus des métiers puis vus de la technique ?
- Quels chemins d'attaques directs et indirects décrire ?
- Comment calculer les vraisemblances des scénarios : de la méthode expresse à la méthode avancée.
- 5. Atelier – Traitement du risque :
- Quels risques considérer comme inacceptables dans le contexte ?
- Quels livrables pour une étude EBIOS RM ?
- Déclaration d'applicabilité type ISO 27001, rapport d'appréciation des risques LPM/NIS, etc.

Etude de cas : Présentation des ateliers 3, 4 et 5.

8) EBIOS, étude de cas

- 1.Le contexte de l'étude : implication des métiers dans l'identification des valeurs métiers et des impacts ressentis.
- Détermination des sources de risques et des objectifs d'attaques potentiels.
- Détermination des obligations réglementaires, juridiques et l'identification des parties prenantes critiques de rang 1.

- La construction de la cartographie de menace numérique de l’écosystème dans le contexte.
- 2. Les activités des ateliers nécessaires à la construction des scénarios stratégiques puis opérationnels.
- L’évaluation des risques en termes de gravité et de vraisemblance.
- Élaboration d’une méthode de calcul de la maturité cyber et dépendance par rapport aux parties prenantes.
- 3. Élaboration du plan de traitement des risques.
- L’élaboration d’un plan d’actions.
- Les mesures de sécurité techniques (protection, défense) et organisationnelles (gouvernance, résilience).
- Le choix des mesures parmi les règles de sécurité des référentiels LPM/NIS ou ISO ou autre.
- Le choix d’un logiciel certifié ANSSI (en cours de certification : ARIMES, EGERIE, AGILE RM, FENCE, IBM OpenPages, …).
- La construction provisoire de son « logiciel » sur base tableur.

LES DATES

CLASSE À DISTANCE
2024 : 02 juil., 26 nov.