Management des risques sur les actifs critiques exposés aux cybermenaces à l'aide de la méthode EBIOS Risk Manager

Durée : 3 jours **Prix :** 2 450 € HT

Contexte

L'analyse de risques est incontournable dans la stratégie de cybersécurité d'une organisation. Elle permet entre autres de faire le point sur les menaces qui planent sur l'organisation, les vulnérabilités des systèmes, et l'importance de l'actif qui pourrait être endommagé.

Une analyse de risques a de nombreux bénéfices pour l'organisation. Elle permet d'une part de prendre conscience des actifs importants de l'organisation. D'autre part, l'identification des menaces, des vulnérabilités, des impacts et de leur probabilité permet d'avoir une vision d'ensemble sur les risques qui planent sur l'organisation.

L'analyse de risques va aussi permettre d'harmoniser les efforts de protection aux objectifs de l'entreprise. Elle aidera à prendre des décisions sur les protections à déployer, et notamment de s'inscrire dans une démarche de cyber-résilience.

Cette formation de haut niveau vise à renforcer les capacités de l'organisation sur les techniques et méthodes d'analyse des risques de cybersécurité sur les actifs de l'organisation.

Objectifs

- Découvrir les enjeux de la cybercriminalité et de la cybersécurité.
- Découvrir les aspects organisationnels et techniques de la cybersécurité (défense en profondeur).
- Identifier et définir les actifs de l'organisation.
- Calculer la valeur des actifs de l'organisation.
- Appliquer la méthode EBIOS Risk Manager pour analyser les risques cyber sur les actifs organisationnels.
- Construire une riposte adéquate et proportionnée pour réduire les risques cyber.

Public visé

Top Management, Managers, Responsables de la sécurité des systèmes, Gestionnaires et Exploitants des Assets, Cadres et toute personne intéressée par la stratégie de cybersécurité.

Prérequis

Aucun.

Modalités pratiques

Méthodologie pédagogique

Exposé, échanges d'expérience, études de cas.

Méthodologie d'évaluation

Le stagiaire reçoit en amont de la formation un questionnaire permettant de mesurer les compétences, profil et attentes du stagiaire. Tout au long de la formation, les stagiaires sont évalués au moyen de différentes méthodes (quizz, ateliers, exercices et/ou de travaux pratiques, etc.) permettant de vérifier l'atteinte des objectifs. Un questionnaire d'évaluation à chaud est soumis à chaque stagiaire en fin de formation pour s'assurer de l'adéquation des acquis de la formation avec les attentes du stagiaire. Une attestation de réalisation de la formation est remise au stagiaire.

Programme

Module 1 : Comprendre les enjeux de la cybercriminalité

- Le modèle économique de la cybercriminalité
- Les différents types de menaces
- Les motivations des attaquants
- Panorama des cyberattaques contre les entreprises et les infrastructures critiques
- Les crypto-monnaies au service de l'industrie de la cybercriminalité
- Questionnement sur les SOC (Security Operations Center)
- Analyse de la rentabilité d'un programme de Cybersécurité
- C'est quoi la gestion des risques ?
- Objectifs de la gestion de la gestion des risques

Module 2 : Les principes fondamentaux de la cybersécurité

- Méthodes et techniques des cyberattaquants
- Les différents types d'actifs exposés aux cybermenaces
- Panorama des vulnérabilités sur les actifs, leurs impacts, et leurs conséquences
- La défense en profondeur
- Les référentiels ISO (27001, 27002, 27005)
- Les sources d'informations incontournables (ANSSI, ENISA, NIST, CIS, CSA, OWASP, CESIN, …)

Module 3 : Les spécificités des technologies opérationnelles

- Définition
- Évolution des OT
- Les systèmes basés sur l'IOT et leurs interdépendances
- Systèmes et Composants OT
- Convergence des système OT et IT
- Contraintes spécifiques des OT en matière de cybersécurité

Module 4 : Les fondamentaux de la méthode EBIOS Risk Manager

- Historique
- Objectifs de la méthode
- Les concepts de la gestion des risques
- Le modèle CID (Confidentialité, Intégrité, Disponibilité) pour les technologies IT
- Le modèle CIDS (Confidentialité, Intégrité, Disponibilité, Sécurité) pour les technologies OT
- Processus d'analyse de risque
- Carte d'identité de la méthode EBIOS Risk Manager
- Principes directeurs de la méthodes EBIOS Risk Manager

Module 5 : Cadrage et Socle de sécurité

- Définir le cadre de l'étude
- Définir le périmètre métier et technique
- Identifier les événements redoutés
- Déterminer le socle de sécurité

Module 6 : Sources de risque

- Identifier les sources de risque (SR) et les objectifs visés (OV)
- Evaluer le couple SR/OV
- Sélectionner les couples SR/OV

Module 7 : Scénarios stratégiques

- Cartographier l'écosystème
- Elaborer les scénarios stratégiques
- Définir les mesures de sécurité sur l'écosystème

Module 8 : Scénarios opérationnels

- Elaborer les scénarios opérationnels
- Evaluer la vraisemblance des scénarios opérationnels

Module 9 : Traitement du risque

- Réaliser une évaluation des risques
- Décider de la stratégie de traitement du risque
- Définir les mesures de sécurité
- Évaluer et documenter les risques résiduels
- Mettre en place le cadre de suivi des risques

Module 10 : Surveillance et contrôle des risques

- Les avantages de la méthode EBIOS Risk Manager
- Audit des risques
- Examen de la situation
- Analyse des données
- Réévaluation des risques
- Réponse au risque