Management des risques sur les actifs critiques exposés aux cybermenaces

Durée : **5** jours **Prix :** 3 800 € 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

- Valoriser les actifs de l'organisation.
- Identifier et analyser les menaces et les risques qui pèsent sur les actifs de l'organisation.
- Appréhender les concepts fondamentaux de l'analyse de risques de cybersécurité.
- Connaitre les méthodes d'analyse disponibles pour maîtriser les risques de cybersécurité.
- Savoir conduire une analyse de risques.
- Appréhender le contenu d'un plan de traitement des risques.

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 : Introduction aux Technologies Opérationnelles (OT)

- Introduction aux Technologies Opérationnelles (OT)
- Définition
- Évolution des OT
- Les systèmes basés sur l'IOT et leurs interdépendances
- Systèmes et Composants OT
- Convergence des système OT et IT
- Analyse de la rentabilité du programme de Cybersécurité
- C'est quoi la gestion des risques ?
- Objectifs de la gestion de la gestion des risques
- Les processus de gestion des risques
- Démarche générale de la gestion des risques

Module 2 : Planification de la gestion des risques

- Cadrage de la démarche
- Appréhender le contexte général
- Définir les critères de base et méthodes d'appréciation du risque
- Définir le domaine d'application et les limites
- Décrire l'environnement du processus de gestion du risque
- Organiser et gouverner la gestion du risque

Module 3 : Appréciation des risques

- Description générale
- Identification des risques
- Analyse des risques
- Évaluation des risques

Module 4 : Traitement des risques

- Options de traitement du risque
- Fiche descriptive du risque
- Registre des risques

Module 5 : Surveillance et contrôle des risques

- Audit des risques
- Examen de la situation
- Analyse des données
- Réévaluation des risques
- Réponse au risque