Auditer et contrôler la sécurité de son système d'information

Date et durée

Code formation : GSI003FR
Durée : 2 jours
Nombre d'heures : 14 heures

Description

Dans un contexte où les **menaces cybernétiques** se complexifient, la simple mise en place de protections ne suffit plus : il faut vérifier leur efficacité. Cette courte formation vous apprendra à structurer une démarche d'audit rigoureuse pour évaluer la conformité et la robustesse de votre système d'information face aux **exigences des normes et des standards** (ISO, NIST et ANSSI).
Loin de se limiter à la théorie, le programme vous plongera dans la réalité opérationnelle du **contrôle interne**. Vous concevrez vos propres tableaux de bord pour piloter la performance de la sécurité et apprendrez à orchestrer différents types d'audits, de **l'analyse configurationnelle** aux tests d'intrusion, afin d'identifier les failles avant qu'elles ne soient exploitées.
À l'issue de cette formation, vous disposerez des clés pour transformer les **résultats d'audit** en plans d'action correctifs concrets. Vous serez en mesure d'instaurer une boucle d'amélioration continue, garantissant ainsi la pérennité et la résilience de votre **gouvernance SSI**.

Objectifs

À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants :

- définir les enjeux de gouvernance et les obligations liées à la sécurité des SI ;
- élaborer une stratégie d'audit adaptée aux risques et au contexte de votre entreprise ;
- construire des tableaux de bord pertinents pour le pilotage de la sécurité ;
- réaliser des audits d'architecture, de configuration et des audits organisationnels ;
- piloter des campagnes de tests d'intrusion et gérer les plans de remédiation.

Points forts

- **Ancrage normatif** : vous maîtriserez les standards incontournables du marché (ISO 27001, NIST) pour légitimer vos audits.
- **Vision à 360°** : vous balayerez l'ensemble du spectre de l'audit, du contrôle organisationnel jusqu'aux tests d'intrusion techniques, pour ne laisser aucune zone d'ombre.
- **Outils de pilotage** : vous repartirez avec des méthodes concrètes pour construire des tableaux de bord qui parlent à la direction.
- **Expertise terrain** : vous bénéficierez du retour d'expérience de formateurs experts certifiés et spécialistes des audits réels.

Modalités d'évaluation

Travaux Pratiques

Etude de cas

Pré-requis

Suivre cette formation nécessite le prérequis suivant :

- **Théorique :** une bonne connaissance des concepts fondamentaux de la cybersécurité et des normes ISO 2700x est recommandée pour suivre le rythme de la formation.

Public

Cette formation s'adresse aux professionnels de la sécurité et de la conformité. Le public inclut notamment :

- les **RSSI et DSI** qui doivent garantir la conformité et piloter la stratégie de sécurité globale ;
- les **auditeurs SSI et consultants** qui réalisent des missions de contrôle et de conseil en cybersécurité ;
- les **responsables conformité et risques** qui intègrent le volet sécurité dans leur cartographie des risques ;
- les **ingénieurs et administrateurs sécurité** qui participent aux audits techniques et à la mise en œuvre des corrections.

Programme

Module 1 : appréhender la gouvernance et les normes SSI

- Les enjeux stratégiques et les obligations réglementaires du pilotage de la sécurité.
- La définition des rôles et des responsabilités au sein de la gouvernance.
- L'application des référentiels majeurs : ISO 27001, ISO 27005, NIST et recommandations de l'ANSSI.

Étude de cas

- Analyser le contexte normatif d'une entreprise fictive et identifier les référentiels applicables.

Module 2 : conduire une démarche d'audit de sécurité

- Le panorama des typologies d'audits : organisationnel, physique, architecture, configuration et code source.
- L'application des méthodologies éprouvées et des bonnes pratiques d'audit.
- La structuration et l'élaboration d'un plan d'audit SSI cohérent.

Travaux pratiques

- Simuler la planification d'un audit de sécurité sur un périmètre donné.

Module 3 : piloter la performance par la donnée

- La méthodologie de construction d'indicateurs de sécurité (KPIs, KRIs).
- La conception et l'exploitation de tableaux de bord décisionnels pour la SSI.
- L'utilisation des métriques pour ajuster la stratégie de pilotage.

Travaux pratiques

- Concevoir une maquette de tableau de bord pour un RSSI.

Module 4 : orchestrer les contrôles et tests techniques

- Les différentes approches de tests d'intrusion : boîte noire, grise et blanche.

- L'analyse des rapports de vulnérabilités et l'interprétation des résultats techniques.
- La priorisation des risques et la définition des plans d'action correctifs.

Module 5 : pérenniser l'amélioration continue

- L'intégration des résultats d'audit dans la gestion de projet et le cycle de vie applicatif.
- La communication efficace des résultats aux parties prenantes.
- Le suivi de la mise en conformité et des actions de remédiation dans la durée.

Travaux pratiques

- Élaborer un plan d'amélioration continue suite à un rapport d'audit défavorable.