FORMATION EN PRESENTIEL ET/OU EN DISTANCIEL (SELON LE THEME)

SÉMINAIRE PSSI - SÉCURITÉ DES SYSTÈMES D'INFORMATION

Dernière mise à jour le 15/10/2024.

OBJECTIF

Savoir assurer la sécurité de votre SI ainsi que l'analyse des risques à la mise en œuvre optimale de solutions de sécurité.

Tarif	2290 € HT par participant

Réf.	SSI

Contact	0465260114 contact@univlearn.fr https://univlearn.fr/

COMPÉTENCES DÉVELOPPÉES

- Planifier un plan d'actions pour atteindre les objectifs de la politique de sécurité
- Connaître le cadre juridique français et européen (LPM, NIS, RGPD, …)
- Maîtriser le processus de gouvernance de la sécurité
- Utiliser les référentiels métiers et les normes associées de la série ISO 27K
- Elaborer une riposte adéquate et proportionnée pour réduire les risques cyber

PUBLIC CONCERNÉ

Ingénieurs prenant les fonctions de RSSI, directeurs ou responsables informatiques, ingénieurs ou correspondants sécurité, chefs de projet intégrant des contraintes de sécurité.

PRÉ-REQUIS

- Avoir des connaissances de base en système d'information et en réseau

MODALITÉS ET DÉLAIS D'ACCÈS

Vous pouvez vous inscrire pour suivre une de nos formations jusqu'à la veille de la date de démarrage si la formation est financée directement par votre entreprise ET si le nombre maximum de participants n'est pas atteint. Si la formation est financée via un OPCO, vous devez au préalable avoir obtenu un accord de ce dernier.

MÉTHODES ET MOYENS MOBILISÉS

Evaluation des acquis tout au long de la formation à travers des Tps, des Quizz ; Evaluation de satisfaction de fin de formation ; Attestation de fin de formation précisant les modules acquis et en cours d'acquisition ; Support de cours remis en fin de session.

MODALITÉS DE DÉROULEMENT DE L'ACTION DE FORMATION

Formation présentielle ou distancielle dispensée par un formateur expérimenté. La formation alterne des exposés théoriques, des démonstrations et la mise en pratique au travers d'exercices et de cas concrets.

Niveau	Modalité	Effectif par session	Durée
Autres formations professionnelles continues	**Présentiel**	**2 mini > 6 maxi**	**21 heures / 3 jour(s)**

PROGRAMME

Module 1 - Les fondamentaux de la sécurité du système d'information

La définition des actifs processus/information et actifs en support (informatique).
La classification DICT/P : Disponibilité, Intégrité, Confidentialité et Traçabilité/Preuve.
La définition du risque SSI et ses propriétés spécifiques (vulnérabilités, menaces).
Les différents types de risques : accident, erreur, malveillance.
L'émergence du cyber risque, les APT, se préparer à une cyber crise.
Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).

Module 2 - La task force SSI : de multiples profils métiers

Le rôle et les responsabilités du RSSI / CISO, la relation avec la DSI.
Vers une organisation structurée et décrite de la sécurité, identifier les compétences.
Le rôle des "Assets Owners" et l'implication nécessaire de la direction.
Les profils d'architectes, intégrateur, auditeurs, pen-testeurs, superviseurs, risk manager, etc.
Constituer un équipe compétente, formée et réactive aux évolutions du cyber espace.

Module 3 - Les cadres normatifs et réglementaires

Intégrer les exigences métiers, légales et contractuelles. L'approche par la conformité.
Un exemple de réglementation métier : PCI DSS pour protéger ses données sensibles.
Les mesures de sécurité pour atteindre un objectif de confidentialité, intégrité des données.
Un exemple de réglementation juridique : directive NIS/ Loi Programmation Militaire.
Les 4 axes de la sécurité vue par l'Europe et l'ANSSI : Gouvernance, Protection, Défense et Résilience.
Les mesures de sécurité pour atteindre un objectif de disponibilité, intégrité des processus.
La norme ISO 27001 dans une démarche système de management (roue de Deming/PDCA).
Les bonnes pratiques universelles de la norme ISO 27002, la connaissance minimale indispensable.
Les domaines de la sécurité : de la politique à la conformité en passant par la sécurité informatique.
Elaborer un Plan d'Assurance Sécurité dans sa relation client/fournisseur.

Module 4 - Le processus d'analyse des risques

Intégration de l'Analyse des risques au processus de gouvernance de la sécurité.
Identification et classification des risques, risques accidentels et cyber risques.
Les normes ISO 31000 et 27005 et la relation du processus risque au SMSI ISO 27001.
De l'appréciation des risques au plan de traitement des risques : les bonnes activités du processus.
Connaitre des méthodes pré définies : approche FR/EBIOS RM, approche US/NIST, etc.

Module 5 - Les audits de sécurité et la sensibilisation des utilisateurs

Les catégories d'audits, de l'audit organisationnel au test d'intrusion.
Les bonnes pratiques de la norme 19011 appliquées à la sécurité.
Comment qualifier ses auditeurs ? – exemple avec les PASSI en France.
Sensibilisation à la sécurité : Qui ? Quoi ? Comment ?
De la nécessité d'une sensibilisation programmée et budgétisée.
Les différents formats de sensibilisation, présentiel ou virtuelle ?
La charte de sécurité, son existence légale, son contenu, les sanctions.
Les quiz et serious game , exemple avec le MOOC de l'ANSSI.

Module 6 - Le coût de la sécurité et les plans de secours

Les budgets sécurité, les statistiques disponibles.

La définition du Return On Security Investment (ROSI).
Les techniques d'évaluation des coûts, les différentes méthodes de calcul, le calcul du TCO.
La couverture des risques et la stratégie de continuité.
Plans de secours, de continuité, de reprise et de gestion de crise, PCA/PRA, PSI, RTO/RPO.
Développer un plan de continuité, l'insérer dans une démarche sécurité.

Module 7 - Concevoir des solutions techniques optimales

Structurer sa protection logique et physique. Savoir élaborer une défense en profondeur.
Les trois grands axes de la sécurité informatique (réseaux, données, logiciels).
Cloisonner ses réseaux sensibles, les technologies firewall réseaux et applicatif.
Rendre ses données illisibles pendant le stockage et le transport, les techniques cryptographiques.
Sécuriser ses logiciels par le durcissement et une conception secure.
Gestion des vulnérabilités logicielles, savoir utiliser CVE/CVSS.

Module 8 - Supervision de la sécurité

Indicateurs opérationnels de gouvernance et de sécurité.
Le pilotage cyber : tableau de bord ISO compliant.
Préparer sa défense (IDS, détection incidents, etc.).
Traitement des alertes et cyber forensics, le rôle des CERT.

Module 9 - Les atteintes juridiques au Système de Traitement Automatique des Données

Rappel, définition du Système de Traitement Automatique des Données (STAD).
Types d'atteintes, contexte européen, la loi LCEN. Le règlement RGPD.
Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

Module 10 - Recommandations pour une sécurisation "légale" du SI

La protection des données à caractère personnel, sanctions prévues en cas de non-respect.
De l'usage de la biométrie en France.
La cybersurveillance des salariés : limites et contraintes légales.
Le droit des salariés et les sanctions encourues par l'employeur.

LES PLUS

Consultant formateur expert en cybersécurité

INTERVENANT(S)	ÉVALUATION	ATTRIBUTION FINALE
Consultant Formateur Cybersécurité	Questions posées par le formateur tout au long de la formation à l'oral ou à travers un QCM	Attestation Individuelle de Formation