Date de publication : 24/02/2026

Formation : RSSI (Responsable de la sécurité du système d'information), niveau 1

Cours de synthèse - 4j - 28h00 - Réf. RSD
Prix : 3130 CHF H.T.

NEW

La formation RSSI prépare les professionnels à gérer la sécurité des systèmes d'information, en abordant des compétences techniques (cadre réglementaires, solutions techniques, ...).

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

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

Public concerné

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

Prérequis

Aucune connaissance particulière.

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.

Programme de la formation

PARTICIPANTS

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

PRÉREQUIS

Aucune connaissance particulière.

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.

1 Les fondamentaux de la sécurité du système d'information

- Principes de sécurité : défense en profondeur, modélisation du risque Cyber.
- La classification DICT/P : Disponibilité, Intégrité, Confidentialité et Traçabilité/Preuve.
- L'émergence du cyber-risque, évolution de la cybercriminalité.
- Le déroulement d'une cyberattaque (Kill Chain).
- Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).
- Objectif de sécurité : confidentialité, disponiblité, intégrité des données et traçabilité.

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 cyberespace.

3 Les cadres normatifs et réglementaires

- Intégrer les exigences métiers, légales et contractuelles. L'approche par la conformité.
- Les domaines de la sécurité : de la politique à la conformité en passant par la sécurité informatique.
- Un exemple de réglementation juridique : directive NIS/ Loi Programmation Militaire.
- RGPD et le rôle du RSSI.
- Les 4 axes de la sécurité vue par l'Europe et l'ANSSI : Gouvernance, Protection, Défense et Résilience.
- 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.
- Élaborer un Plan d'assurance sécurité dans sa relation client/fournisseur.
- Le pilotage cyber : tableau de bord ISO compliant.

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 cyberrisques.
- Les normes ISO 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.
- Connaître des méthodes prédéfinies : approche FR/EBIOS RM, approche US/NIST, etc.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 La sensibilisation des utilisateurs

- 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.

6 Concevoir des solutions techniques optimales – Sécurité des données

- Les techniques cryptographiques.
- Les algorithmes à clé publique et symétriques.
- Les fonctions de hachage simple, avec sel et avec clé (HMAC).
- Les architectures à clés publiques (PKI).
- Application de la cryptographie : échanges TLS, sécurité des données au repos ...
- Stratégie de sauvegardes (PCA, PRA ...).

7 Authentification et habilitation des utilisateurs

- L'IAM, un enjeu majeur.
- L'authentification biométrique et les aspects juridiques.
- Techniques d'authentification (mots de passe, certificats, standards UAF et U2F de l'alliance FIDO (Fast ID Online).
- Les différentes techniques d'attaque (brute force, keylogger, credential stuffing,...).
- L'authentification forte et à facteurs multiples (MFA).
- Les standards HOTP et TOTP de l'OATH.

8 Concevoir des solutions techniques optimales – Sécurité réseau

- Cloisonner ses réseaux sensibles, les technologies firewall réseaux et applicatif.
- La sécurité du LAN : Vlans, NAC ...
- Différences entre firewalls UTM, enterprise, NG et NG-v2.
- Les risques associés au Cloud Computing selon le CESIN, l'ENISA et la CSA.
- Le Cloud Controls Matrix et son utilisation pour l'évaluation des fournisseurs de Cloud.
- Les solutions CASB pour sécuriser les données et applications dans le Cloud.
- Sécurité du réseau d'administration : SSH, bastion, cloisonnement et bonnes pratiques.
- Risques sur les réseaux sans fil et bonnes pratiques.
- Solutions VPN.

9 Concevoir des solutions techniques optimales – Sécurité postes et serveurs

- Comprendre les menaces orientées postes clients.
- Les logiciels anti-virus/anti-spyware.
- Logiciels malveillants : charges utiles (ransomware, exploit), propagation (drive-by download, clés USB malveillantes).
- Principe de hardening.
- Comment sécuriser les périphériques amovibles ?
- Vulnérabilités des architectures virtuelles et bonnes pratiques.
- Sécurité et bonnes pratiques avec les smartphones.

10 Gestion et supervision active de la sécurité

- Les catégories d'audits, de l'audit organisationnel au test d'intrusion.
- Les tests d'intrusion (black box, gray box et white box).
- Comment qualifier ses auditeurs ? – exemple avec les PASSI en France.
- Stratégie de supervision : log, IPS (Intrusion Prevention System) et IPS NG.
- Mettre en place une solution de SIEM.
- Mettre en œuvre ou externaliser son Security Operation Center (SOC).
- Les procédures de réponse à incident et la gestion de crise.

Dates et lieux

CLASSE À DISTANCE
2026 : 26 mai, 8 sep., 24 nov.