

Formation : Parcours certifiant Manager la cybersécurité des systèmes, applications et bases de données

Bloc de compétences du titre RNCP 40573

Cours pratique - 26j - 182h00 - Réf. ZCN

Prix : 13310 € H.T.

NEW

Ce parcours de formation représente le quatrième bloc de compétences constituant le titre certifié de niveau 7 (Bac +5) " Expert en informatique et système d'information - Option Cybersécurité" reconnu par l'État.



Objectifs pédagogiques

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

- ✓ Maîtriser le processus de gouvernance de la sécurité
- ✓ Maîtriser la sécurité du Cloud, des applications, des postes clients
- ✓ Identifier et analyser les menaces et les risques qui pèsent sur un SI
- ✓ Cartographier les risques
- ✓ Réaliser un test de pénétration
- ✓ Rédiger un rapport final suite à un test d'intrusion
- ✓ Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- ✓ Analyser l'intrusion a posteriori

Public concerné

Toutes personnes souhaitant manager la cybersécurité des systèmes, applications et bases de données.

Prérequis

Être titulaire d'un diplôme ou titre de niveau 6 (équiv. Bac + 3/4) en spécialité informatique ou justifiant d'une expérience professionnelle équivalente.
Être titulaire d'un diplôme ou titre de niveau 7 (équiv. Bac + 5) en spécialité scientifique ou justifiant d'une expérience professionnelle équivalente.

PARTICIPANTS

Toutes personnes souhaitant manager la cybersécurité des systèmes, applications et bases de données.

PRÉREQUIS

Être titulaire d'un diplôme ou titre de niveau 6 (équiv. Bac + 3/4) en spécialité informatique ou justifiant d'une expérience professionnelle équivalente.

Être titulaire d'un diplôme ou titre de niveau 7 (équiv. Bac + 5) en spécialité scientifique ou justifiant d'une expérience professionnelle équivalente.

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.

Certification

Chaque bloc de compétences est validé par un examen écrit sous forme d'étude de cas. Bloc de compétences « Manager la cybersécurité des systèmes, applications et bases de données », de la certification professionnelle « Expert en informatique et systèmes d'information », délivrée par 3W ACADEMY.

Enregistrée au répertoire national des certifications professionnelles, sous le numéro 40573, par décision du directeur général de France Compétences en date du 30/04/2025.

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.

Composition du parcours

Ce parcours est composé des modules suivants :

Sécurité des systèmes d'information, synthèse

Réf. SSI - 3 jours  4 / 5

Cybersécurité réseaux/Internet, synthèse

Réf. SRI - 3 jours  4 / 5

Sécurité SI, mise en œuvre pratique d'une analyse de risques

Réf. CUR - 2 jours  4 / 5

Risk Manager - Méthode EBIOS

Réf. EBU - 2 jours  4 / 5

Hacking et sécurité, niveau 1

Réf. HAC - 5 jours  4 / 5

Tests d'intrusion, organiser son audit

Réf. TEI - 4 jours  4 / 5

Cybersécurité, tester ses environnements

Réf. CTE - 3 jours  3 / 5

Analyse Forensic

Réf. AFB - 3 jours  4 / 5

Certification Manager la cybersécurité des systèmes, applications et bases de données.

Réf. ZSB - 1 jour

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.

Mentions légales

- Retrouvez le détail des mentions légales sur le titre RNCP de référence [Titre RNCP Expert en informatique et systèmes d'information - Option Cybersécurité - Réf.XCS](#)

Programme de la formation

1 Sécurité des systèmes d'information, synthèse

- Les fondamentaux de la sécurité du système d'information.
- La task force SSI : de multiples profils métiers.
- Les cadres normatifs et réglementaires.
- Le processus d'analyse des risques.
- Les audits de sécurité et la sensibilisation des utilisateurs.
- Le coût de la sécurité et les plans de secours.
- Concevoir des solutions techniques optimales.
- Supervision de la sécurité.
- Les atteintes juridiques au système de traitement automatique des données.
- Recommandations pour une sécurisation "légale" du SI.

2 Cybersécurité réseaux/Internet, synthèse

- Sécurité de l'information et cybercriminalité.
- Firewall, virtualisation et Cloud Computing.
- Sécurité des postes clients.
- Fondamentaux de la cryptographie.
- Authentification et habilitation des utilisateurs.
- La sécurité des flux réseaux.
- Sécurité Wi-Fi.
- Sécurité des Smartphones.
- Sécurité des applications.
- Gestion et supervision active de la sécurité.

3 Sécurité SI, mise en œuvre pratique d'une analyse de risques

- La notion de risque en sécurité des informations.
- L'identification des biens informationnels.
- L'analyse de risque.
- Les méthodes utiles.
- Les normes.
- Construction du plan de traitement des risques.

4 Risk Manager - Méthode EBIOS

- La méthode EBIOS risk manager.
- Cadrage et socle de sécurité.
- Sources de risques.
- Scénarios stratégiques.
- Scénarios opérationnels.
- Traitement du risque.

5 Hacking et sécurité, niveau 1

- Le Hacking et la sécurité.
- Sniffing, interception, analyse, injection réseau.
- La reconnaissance, le scanning et l'énumération.
- Les attaques Web.
- Les attaques applicatives et post-exploitation.

6 Tests d'intrusion, organiser son audit

- Les menaces.
- Méthodologie de l'audit.
- Les outils de Pentest.
- Rédaction du rapport.
- Mises en situation.

7 Cybersécurité, tester ses environnements

- Les attaques Web.
- Détecter les intrusions.
- La collecte des informations.

8 Analyse Forensic

- Comment gérer un incident ?
- Analyser les incidents pour mieux se protéger : L'analyse Forensic.
- Analyse forensic d'un système d'exploitation Windows.

Titres RNCP associés

Pour aller plus loin et renforcer votre employabilité, découvrez les titres RNCP qui contiennent ce parcours certifiant.

- [Titre RNCP Expert en informatique et systèmes d'information - Option Cybersécurité - Réf. XCS](#)

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.

Découvrez-les sur notre page [Comment financer sa formation](#) ou [contactez votre conseiller formation](#).

Horaires

Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts.

Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

Dates et lieux

CLASSE À DISTANCE

2026 : 16 juin, 23 juin, 29 sep., 6 oct., 17 nov., 24 nov.

PARIS LA DÉFENSE

2026 : 16 juin, 29 sep., 17 nov.