Formation Piloter et animer la sécurité informatique

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Le parcours certifiant Piloter et animer la sécurité informatique s'adresse aux professionnels issus des systèmes et réseaux ou de la DSI souhaitant monter en compétence et obtenir une reconnaissance métier dans le domaine de la cybersécurité. Structuré sur 217 heures (31 jours sur 6 mois maximum), il permet de maîtriser les fondamentaux techniques, réglementaires et organisationnels nécessaires à la mise en oeuvre d'une stratégie de sécurité informatique.
Ce programme intensif et progressif est organisé en 7 modules couvrant l'ensemble du cycle de la sécurité : de la sécurisation des systèmes et réseaux, à l'analyse des risques (notamment avec EBIOS Risk Manager), en passant par la gestion de crise, l'audit, la conformité RGPD, et la sensibilisation des utilisateurs. Les apprenants alternent apports théoriques, ateliers pratiques, études de cas, mises en situation, et simulations de pilotage.
Grâce à une pédagogie mixte et professionnalisante, les participants développent leurs compétences techniques et comportementales : animation de réunions, rédaction de préconisations, coordination de plans d'action, accompagnement au changement. L'usage d'outils de veille, de logiciels de gestion de projet ou d'audit complète leur savoir-faire opérationnel.
À l'issue du parcours, les stagiaires sont préparés à la certification professionnelle Piloter et animer la sécurité informatique. Ils repartent avec une vision stratégique, des outils concrets, et une capacité renforcée à contribuer activement à la cybersécurité des organisations.

Référence	SECPASI
Durée	31 jours (217h)
Tarif	16 241 €HT
Certification	- €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 1er juin au 15 juillet 2026
du 8 sept. au 22 octobre 2026
du 16 nov. au 30 décembre 2026

PARIS

du 1er juin au 15 juillet 2026
du 8 sept. au 22 octobre 2026
du 16 nov. au 30 décembre 2026

VOIR TOUTES LES DATES

Objectifs

| mettre en oeuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.
| Être en mesure de mettre en place une stratégie de cybersécurité à partir d'une analyse du risque
| Être capable de sécuriser des réseaux, des protocoles, des terminaux et des serveurs
| Pouvoir animer et évaluer la mise en oeuvre de la stratégie de cybersécurité

Public

| Ce parcours certifiant à des personnes titulaires d'une certification de niveau 5 ou 6 dans le domaine de l'informatique, dont la cybersécurité n'est pas la seule fonction (techniciens systèmes et réseaux, assistance technique dans les ESN, différents profils de la DSI)
| Le périmètre de la certification correspond aux activités des professionnels qui exercent dans les métiers de la Gestion de la sécurité et du pilotage des projets de sécurité ou dans les métiers du Conseil, services et recherche

Prérequis

| Il est impératif de justifier d'une expérience professionnelle dans le domaine visé par la certification, acquise au sein de la Direction des systèmes d'information d'une entreprise ou d'une ESN (Entreprise de Services du Numérique) ou de justifier d'un diplôme ou d'une certification de niveau 5 (par exemple : BTS Services Informatiques aux Organisations, BTS Systèmes numériques, DUT informatique, Licence Porfessionnelle Métiers de l'informatique, BUT Informatique, Titres à finalité professionnelle, CQP Administrateur Systèmes et Réseaux, etc.)
| Plus explicitement :

| Connaître le guide d'hygiène sécurité de l'ANSSI ou connaître les bonnes pratiques telles qu'elles sont décrites dans ce guide.
| Fondamentaux réseaux : Modèle OSI - Equipement réseaux - Fonctionnement TCP/UDP - Service applicatif commun (http, DNS, SMTP, SSL).
| Fondamentaux système : Compréhension de base Windows (Service, fonctionnement) - Compréhension de base Linux (CLI, Service, fonctionnement).
| La compréhension de l'anglais est un plus

Programme de la formation

1 - Module 1 : Les fondamentaux de la cybersécurité (35 heures)
2 - Jour 1 : Introduction à la cybersécurité
| Matin : Enjeux de la sécurité des systèmes et réseaux ; Analyse des cyberattaques récentes
| Après-midi : Identification de failles sur des scénarios prédéfinis

3 - Jour 2 : Architecture et moyens de protection
| Matin : Principes d'architecture sécurisée ; Équipements de sécurité : firewalls, proxys
| Après-midi : Mise en place d'un firewall et test de configurations

4 - Jour 3 : Sécurisation des systèmes
| Matin : Sécurisation des systèmes Windows et Linux ; Configurations des politiques de groupe
| Après-midi : Atelier de durcissement d'un système Linux

5 - Jour 4 : Veille technologique et menaces émergentes
| Matin : Introduction à la veille technologique ; Exploration des bases de données de vulnérabilités
| Après-midi : Mise en place d'un processus de veille personnalisé

6 - Jour 5 : Synthèse et mise en pratique
| Matin : Synthèse des acquis ; Discussion sur les bonnes pratiques de veille et sécurisation
| Après-midi : Révision globale des concepts abordés
| Après-midi : Finalisation des projets pratiques ; Activité collaborative : brainstorming en petits groupes pour récapituler et partager les bonnes pratiques identifiées au cours du module.

7 - Module 2 : les fondamentaux de la réglementation de la cybersécurité (7 heures)
| Matin : Cadre réglementaire ; Introduction à la réglementation : RGPD et normes ISO ; Étude des obligations liées aux données personnelles
| Après-midi : Application et bonnes pratiques
| Après-midi : Cas pratiques : analyse d'une étude d'impact (PIA) ; Atelier collaboratif : élaboration d'une politique de conformité adaptée ; Synthèse et réponses aux questions des participants

8 - Module 3 : Pilotage d'un plan d'action en cybersécurité (70 heures)
9 - Jour 1-2 : Introduction à la PSSI et planification
| Matin : Principes et structure de la PSSI
| Après-midi : Identification des contraintes et ressources

10 - Jour 3-5 : Gestion de projet appliquée
| Planification des tâches et gestion des ressources
| Utilisation d'outils pratiques : création d'un projet type

11 - Jour 6-7 : Communication et collaboration
| Animation de réunions : scénarios et jeux de rôle
| Gestion des parties prenantes : études de cas

12 - Jour 8-9 : Rédaction et recommandations
| Préparation d'un rapport stratégique
| Simulation de présentation à un comité fictif

13 - Jour 10 : Synthèse et évaluation
| Bilan global du module
| QCM et étude de cas final pour valider les acquis

14 - Module 4 : Analyse et évaluation des risques de sécurité (42 heures)
15 - Jour 1-2 : Fondamentaux de la gestion des risques
| Matin : Introduction aux concepts clés et typologie des risques
| Après-midi : Exploration des normes ISO et SMSI

16 - Jour 3-4 : Cartographie des actifs et analyse des risques
| Matin : Techniques de cartographie et identification des actifs critiques
| Après-midi : Atelier sur l'établissement d'un contexte de gestion des risques

17 - Jour 5 : Analyse et évaluation des risques
| Matin : Application de la méthode EBIOS
| Après-midi : Rédaction des recommandations et plans d'action

18 - Jour 6 : Synthèse et validation
| Matin : Discussion sur les plans de gestion des risques
| Après-midi : Évaluation finale (cas pratique et QCM)

19 - Module 5 : Organisation et coordination des réponses à incident (14 heures)
20 - Jour 1 : Introduction et plans de continuité
| Matin : Principes de gestion des incidents et présentation des PCA/PRA
| Après-midi : Atelier de constitution d'équipes et de rédaction de procédures

21 - Jour 2 : Mise en situation et synthèse
| Matin : Simulation de gestion de crise avec analyse des incidents
| Après-midi : Discussion sur les bonnes pratiques et évaluation finale

22 - Module 6 : Mise en oeuvre d'actions de contrôle de cybersécurité (21 heures)
23 - Jour 1 : Organisation et outils d'audit
| Matin : Introduction aux objectifs et planification des actions de contrôle
| Après-midi : Présentation des outils d'audit et d'évaluation

24 - Jour 2 : Mise en pratique des audits
| Matin : Atelier d'audit de configuration et de tests utilisateurs
| Après-midi : Identification et correction des vulnérabilités

25 - Jour 3 : Supervision et synthèse
| Matin : Analyse des rapports d'audit et présentation des recommandations
| Après-midi : Synthèse et évaluation finale avec un cas pratique complet

26 - Module 7 : Sensibilisation et formation des équipes (28 heures)
27 - Jour 1 : Principes et enjeux de la sensibilisation
| Matin : Introduction aux concepts de sensibilisation et conduite du changement
| Après-midi : Atelier sur les objectifs et attentes des utilisateurs finaux

28 - Jour 2 : Supports et bonnes pratiques
| Matin : Création et personnalisation de supports de sensibilisation
| Après-midi : Simulation de sessions interactives (phishing, mots de passe)

29 - Jour 3 : Mise en place d'un plan de formation
| Matin : Analyse des besoins et élaboration de parcours
| Après-midi : Sélection et évaluation des formations

30 - Jour 4 : Synthèse et évaluation
| Matin : Simulation de sessions de sensibilisation
| Après-midi : Évaluation finale et réflexion sur l'impact des actions

31 - Détail des dates de sessions
| Session du 04 mars au 28 août : Mars : les 04 au 06 + 19 et 20 + 30 et 31 Avril : les 1er + 13 au 15 + 22 au 24 + 29 au 30 Mai : les 11 au 13 + 21 au 22 Juin : les 01 et 02 + 22 au 24 Juillet : les 06 au 08 + 20 et 21 Août : 27 et 28 (Jury)
| Session du 01 juin au 30 septembre : Juin : 01 au 04 + 10 au 12 + 15 au 18 + 24 au 26 Juillet : 01 au 03 + 07 au 10 + 20 au 23 + 29 au 31 Août : 05-06-07 Septembre : Jury les 29 et 30
| Session du 08 septembre au 12 février 2027 : Septembre : 08 au 11 + 21 au 23 + 30 Octobre : 01 au 02 + 12 au 14 + 26 au 28 Novembre : 09 au 10 + 18 au 20 + 30 Décembre : 01 au 02 + 08 au 11 + 16 au 18 Février 2027 : Jury les 11 et 12
| Session du 16 novembre au 11 juin 2027 : Novembre : 16 au 17 Décembre : 03 au 04 + 14 au 15 Janvier 2027 : 06 au 08 + 20 au 22 Février 2027 : 01 au 03 + 11 au 12 + 24 au 26 Mars 2027 : 03 au 05 + 18 au 19 + 29 au 31 Avril 2027 : 14 au 16 Juin 2027 : Jury les 10 et 11

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

Piloter et animer la sécurité informatique
Certification professionnelle Piloter et animer la sécurité informatique de l'OPCO Atlas. La certification se compose de 2 épreuves :

| La rédaction d'un dossier professionnel : Le candidat doit rédiger un dossier professionnel d'une vingtaine de pages prenant appui sur des exemples d'une ou plusieurs situations vécues, en contexte professionnel et formatif, en rapport avec la certification visée. Pour chaque compétence, le candidat fournira ainsi un ou plusieurs exemples de pratique professionnelle. Le candidat disposera d'un mois pour préparer et rédiger le dossier.
| La soutenance orale : il s'agit d'une présentation par le candidat du dossier professionnel préparé. Le candidat adressera au jury son dossier 15 jours avant la soutenance. Celle ci comprendra 15 à 20 minutes de présentation par le candidat + 10 à 15 minutes de questions du jury pour approfondir l'évaluation des compétences.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.