Piloter et animer la sécurité informatique

Durée: 31 Jours **Réf de cours: PASI** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Global Knowledge en partenariat avec ACG Cybersecurity lance un nouveau parcours certifiant:
Le parcours de formation PASI (Piloter et animer la sécurité informatique) vise à permettre aux candidats à la certification d'acquérir les connaissances, savoir-faire et compétences nécessaires au pilotage à l'animation de la sécurité informatique.
Le centre de commandement : vous souhaitez diriger la stratégie de cybersécurité et assurer la résilience ?
Avec le parcours PASI, apprenez à piloter le Cyber Squad, anticipez les crises, dirigez les opérations, et bâtissez une sécurité durable pour votre organisation.
Objectifs: Planifier - Anticiper - Piloter
Compétences clés:
- Gouvernance & PSSI, KPIs, comités
- Risques EBIOS RM, ISO 27005
- Conformité RGPD/ISO 27001/27701
- Gestion de crise, PCA/PRA, communication
Mis à jour 23/09/2025

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Le parcours de formation est ouvert aux candidats 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) ou aux participants disposant d'une expérience professionnelle équivalente.

Objectifs pédagogiques:

- L'obtention de la certification doit permettre aux 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 d'être capables de :
- Mettre en place une stratégie de cybersécurité à partir d'une analyse du risque
- Animer et évaluer la mise en œuvre d'une stratégie de cybersécurité
- Élaborer et piloter une politique de cybersécurité (PSSI, projets, budget)
- Sécuriser les systèmes, réseaux et architectures (PKI, cryptographie, Linux, Windows…)
- Appliquer les référentiels et obligations (RGPD, ISO 27001/27005)
- Cartographier les risques avec EBIOS RM
- Coordonner la gestion de crise et la réponse aux incidents
- Contrôler l'efficacité de la sécurité (audits, tests d'intrusion, correctifs)
- Sensibiliser, former, et faire monter en compétence les équipes

Pré-requis:

Justifier d'un diplôme ou d'une certification de niveau 5 (par exemple : BTS Services Informatiques aux Organisations, BTS Systèmes numériques, DUT informatique, Licence Professionnelle métiers de l'Informatique, BUT Informatique, Titres à Finalité

Test et certification

Certification: A l'issue du parcours, l'acquisition des compétences sera validée par l'élaboration d'un dossier professionnel et d'une soutenance orale devant un jury.

Professionnelle, CQP dont le CQP Administrateur Systèmes et

Justifier d’une expérience acquise au sein de la Direction des systèmes d’information d’une entreprise ou d’une ESN (Entreprise de Services du Numérique)

Contenu:

Axe 1 : Les fondamentaux de la sécurité des systèmes et des réseaux - Durée 5 jours (35 heures)

Les spécificités et les failles des différents SI :

- Les principaux risques et menaces
- Les architectures de sécurité (PKI et Crypto)
- Les principes de la sécurité des données
- Les principes de la sécurité des échanges
- Les principes de la sécurisation d'un système (principalement Windows et Linux)

Les ressources et la démarche de recherche d'informations sur les failles d'autres systèmes que Windows et Linux : Mac, Android, IOS, etc.

- La veille technique, technologique et règlementaire en matière de cybersécurité :
- Les principales sources d'information : ANSSI, etc.
- Les techniques de veille : construire un référentiel et capitaliser les informations
- Analyse, curation et outils de communication (intrant d'entreprise, supports de communication

Axe 2 : Les fondamentaux de la règlementation sur la cybersécurité - 1 jours (7 heures)

- Les enjeux liés à la mise en conformité règlementaire des SI en matière de cybersécurité : cybercriminalité, vol de données, etc.
- Le RGPD et ses liens avec la sécurité de l'information et la gestion de risques : objectifs, champ d'application, grands principes, PIA (étude d'impact sur la vie privée), rôle du DPO, sanctions en cas de violation de la réglementation
- Les correspondances entre les exigences des normes ISO (27001 et 27005) et le RGPD
- Les autres règlementations : règlementations sectorielles, obligations des OIV et OSE

Axe 3 : Pilotage d'un plan d'action de cybersécurité - 10 jours (70 heures)

- La PSSI : acteurs internes et externes, contraintes, mesures, plan d'action et documentation
- Le plan d'action stratégique et les préconisations : objectifs, structure et règles de rédaction (ISO 27001)
- La collaboration avec les différents acteurs : posture, techniques et modes de communication, techniques d'animation de réunion
- Les méthodologies et les outils de gestion de projets
- Le marché de la sécurité informatique et la sélection des prestataires : labels, niveaux de certification, etc.

Axe 4 : Analyse et évaluation des risques de sécurité - 6 jours (42 heures)

- Les fondamentaux de la gestion des risques en sécurité de l'information :
- Le cadre normatif en gestion des risques : les normes de la famille ISO/IEC 27000 (27005)
- Typologie des risques : OWASP, STRIDE, risques spécifiques à la sous-traitance, etc.
- Politique de cybersécurité et SMSI
- Les notions clés : Disponibilité, Intégrité, Confidentialité, Preuve
- Les principes d'une analyse de risques
- Le Système de management de la sécurité de l'information (SMSI)
- Les méthodes et outils pour la cartographie du SI : principes de TOGAF, outils de gestion de parc, etc.
- La méthode d'analyse des risques EBIOS RM : établissement du contexte, étude d'événements redoutés, études

Axe 5 : Organisation et coordination des réponses à incident - 2 jours (14 heures)

- Les fondamentaux de la gestion des risques en sécurité de l'information :
- Les enjeux liés à l'organisation de la réponse à incident et à la gestion de la continuité
- Les parties prenantes en cas d'incident de sécurité ou de crise cyber
- Les plans de réponse à incident, de continuité et de reprise de l'activité (PCA / PRA) :
- La mise en œuvre des procédures
- La communication interne / externe dans la gestion des incidents
- Les outils de suivi et de reporting dans la gestion des incident

Axe 6 : Mise en œuvre d'actions de contrôle de cybersécurité - 3 jours (21 heures)

- L'organisation des actions de contrôle : objectifs, planification, préparation
- L'encadrement réglementaire des actions de contrôle
- Les outils et techniques d'audit disponibles : recettage, test utilisateur, test d'intrusion, test de bon fonctionnement, audit de configuration, etc.
- La détection des vulnérabilités
- Le marché de la sécurité informatique et la sélection de prestataires d'audits techniques
- Le choix des procédures d'évaluation en fonction des objectifs : PTES, CVA
- La supervision et l'administration des actions de contrôle : reporting et outils de suivi
- La veille technologique

Axe 7 : Sensibilisation et formation des équipes - 4 jours (28 heures)

- Le changement et la conduite du changement
- Les sujets sur lesquels communiquer, par exemple : les menaces courantes, la diffusion des données personnelles sur le web, la gestion des mots de passe, etc.
- Les règles d'hygiène informatique et mesures de protection à mettre en place
- Les outils de communication : intranet, mails, MOOC de l'ANSSI, les outils de veille (ANSSI), World Café, etc.
- L'adaptation des outils de communication aux utilisateurs : salariés, personnes en situation de handicap.
- La rédaction d'une fiche technique : rédaction et présentation de procédures, modes opératoires à destination des utilisateurs, mise à jour en lien avec la politique et le dispositif de sécurité.

	des scénarios des menaces, étude des risques, étude des mesures de sécurité	■ Les outils d'accompagnement : sélection et mise à disposition de ressources (MOOC, moyens de sensibilisation : le transfert de compétences, la sollicitation et la sélection d'un OF en lien avec les RH, etc. ■ Le rôle du professionnel dans le déploiement d'un plan de formation ciblé destiné aux professionnels des SI : identification des besoins en formation, appui à la sélection des formations et des prestataires

Méthodes pédagogiques :

Formateurs de terrain et cas réels, pour une application immédiate. **50% de pratique** et "Learning by Doing" pour ancrer les réflexesMéthode pédagogique :1ère journée en présentiel, autres journées à distanceUn support de cours officiel sera fourni aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement