PARCOURS CERTIFIANT PASI
PILOTER ET ANIMER LA SÉCURITÉ INFORMATIQUE

Le parcours PASI est une formation certifiante d'une durée totale de 31 jours (217 heures) s'étalant sur environ 6 mois. Cette formation vise à donner aux professionnels les clés pour piloter la sécurité informatique au sein de leur organisation, en alliant connaissance technique, gestion de projet, gouvernance, et animation des équipes. La validation s'effectue par la réalisation d'un dossier professionnel et une soutenance orale devant jury.

TARIF : 19 530 € HT | **RÉF. :** PASI

OBJECTIFS

- Comprendre les concepts fondamentaux de la sécurité des systèmes et réseaux.
- Maîtriser la mise en œuvre de solutions de sécurisation adaptées.
- Connaître et appliquer la réglementation et les normes en cybersécurité.
- Savoir piloter un plan d'action stratégique et collaborer efficacement avec les parties prenantes.
- Animer la sensibilisation et développer la culture cybersécurité au sein des équipes

PRÉ-REQUIS

- Avoir une bonne connaissance des systèmes d'exploitation (Windows, Linux) et des réseaux informatiques (TCP/IP, protocoles, topologies).
- Disposer d'un ordinateur personnel avec capacité de virtualisation (pour exécuter des environnements simulés) et d'une connexion internet haut débit stable.
- Maîtriser les concepts de base en cybersécurité est un plus, pour mieux profiter des travaux pratiques sur des cas réels.
- Être capable d'utiliser des outils bureautiques classiques (tableurs Excel, outils de reporting) et prêt à se familiariser avec des outils spécialisés de sécurité (SIEM, solutions de sécurité réseau).

PUBLIC VISÉ

RSSI, DSI, responsables sécurité, chefs de projet cybersécurité et professionnels souhaitant évoluer vers des responsabilités en pilotage de la sécurité.

PROGRAMME DÉTAILLÉ

Le parcours est organisé autour de 7 axes majeurs, couvrant théorie, pratique et cas concrets.

Axe 1 : Les fondamentaux de la sécurité des systèmes et des réseaux

Durée : 5 jours - 35 heures
Objectifs : Permettre aux stagiaires de maîtriser les principales failles, menaces, équipements de sécurité et solutions pour sécuriser les systèmes et réseaux, tout en développant une veille active dans le domaine de la cybersécurité.
Contenu :

- Spécificités et failles des différents systèmes d'information (Windows, Linux, Mac, Android, iOS).
- Principaux risques et menaces actuels : ransomware, phishing, attaques DDoS.
- Architectures de sécurité : PKI, cryptographie.
- Principes de sécurité des données et sécurisation des échanges (protocoles, VPN, chiffrement).
- Méthodes et outils de veille technique, technologique et réglementaire (ANSSI, CVE).
- Travaux pratiques : identification et classification des actifs, analyse de logs issus de notre SOC, étude de cas réels sur attaques.

Axe 2 : Les fondamentaux de la réglementation sur la cybersécurité

Durée : 1 jour - 7 heures
Objectifs : Permettre aux stagiaires de comprendre les enjeux réglementaires liés à la protection des données et à la sécurité, notamment le RGPD et les normes ISO associées.
Contenu :

- Enjeux liés à la conformité réglementaire : cybercriminalité, vol de données, etc.
- Présentation du RGPD : principes clés, champ d'application, rôle du DPO, sanctions.
- Correspondances entre normes ISO 27001, 27005 et RGPD.
- Autres réglementations sectorielles et obligations des OIV et OSE.
- Travaux pratiques : analyse d'impact sur la vie privée (PIA), évaluation de la conformité, rédaction de plans d'atténuation.

Axe 3 : Pilotage d'un plan d'action cybersécurité

Durée : 10 jours - 70 heures
Objectifs : Former à la mise en œuvre, gestion et animation d'un plan d'action stratégique en cybersécurité en lien avec la gouvernance d'entreprise.
Contenu :

- Politique de sécurité (PSSI), acteurs, contraintes et documentation.
- Rédaction et structure d'un plan d'action basé sur ISO 27001.
- Collaboration avec parties prenantes (DSI, RSSI, DPO, prestataires).
- Gestion de projet : tâches, ressources, budget, outils (Trello, MS Project).
- Animation de réunions, communication avec la direction.
- Travaux pratiques : analyse de maturité, élaboration de tableaux de bord, rédaction et présentation d'un plan stratégique.

Axe 4 : Analyse et évaluation des risques de sécurité

Durée : 6 jours - 42 heures
Objectifs : Maîtriser l'analyse de risques cyber selon ISO 27005 et EBIOS Risk Manager, de l'inventaire des actifs à la priorisation et au plan de traitement.
Contenu

- Cadre normatif et DICP: ISO/IEC 27000, ISO 27005, SMSI; principes d'analyse des risques.
- Menaces et cartographie: STRIDE, OWASP, sous-traitance; TOGAF/CMDB et dépendances critiques.
- EBIOS RM: contexte, événements redoutés, scénarios, risques, mesures.
- Priorisation et outils: matrices impact/probabilité, carto des risques, ISO 27001/27002, guide ANSSI.
- Cas pratique: scénarios MITRE ATT&CK, priorisation et plan de traitement

Axe 5 : Organisation et coordination des réponses incident

Durée : 2 jours - 14 heures
Objectifs : Organiser et coordonner la réponse aux incidents, formaliser les processus de crise et de continuité, et piloter la reprise d'activité pour maintenir les fonctions critiques.
Contenu :

- Réponse aux incidents et continuité (PRA/PCA) : objectifs, structure, équipes, procédures.
- Gouvernance de crise et parties prenantes : rôles, responsabilités, alerte/escalade.
- Exécution opérationnelle et coordination interéquipes, outils de suivi/reporting.
- Communication de crise interne/externe : messages, canaux, coordination direction/régulateurs.
- Travaux Pratiques : rédaction d'un PRA/PCA, exercices de crise, scénarios ransomware/phishing.

Axe 6 : Actions de contrôle et évaluation de la sécurité

Durée : 2 jours - 14 heures
Objectifs : Savoir déployer des mesures de contrôle et auditer la mise en place des actions de sécurisation.
Contenu :

- Réalisation d'audits techniques et organisationnels.
- Tests d'intrusion, exploitation des résultats.
- Analyse des plans d'actions, définition de métriques d'efficacité.
- Rédaction de rapports et recommandations d'amélioration continues.

Axe 7 : Tests d'intrusion et audits techniques

Durée : 2 jours
Objectifs : Maîtriser les méthodes et outils pour réaliser des tests d'intrusion et audits techniques en environnement sécurisé.
Contenu :

- Techniques d'évaluation des vulnérabilités.
- Exploitation de failles, documentation d'incidents.
- Élaboration de rapports détaillés et recommandations.
- Exercices pratiques en environnement virtualisé.

ÉVALUATION DES ACQUIS

- L'acquisition des compétences est validée par un dossier professionnel à constituer par chaque stagiaire.
- Soutenance orale devant un jury, où le candidat défend son dossier et répond aux questions des experts.
- Tout au long de la formation, des quiz réguliers permettent de valider la compréhension des concepts théoriques.
- Les travaux pratiques (labs) sont très détaillés et immersifs : inventaire des actifs, analyse de logs, configuration d'outils de sécurité (pare-feu, SIEM, VPN), détection et documentation d'attaques réelles simulées (ransomware, phishing).
- Chaque TP est livré sous forme de rapports, tableaux synthétiques, plans d'action, ou rapports d'audit. Ces livrables constituent aussi une base d'évaluation.
- L'évaluation intègre la capacité à appliquer des méthodologies (ex : DICP, ISO 27001, RGPD), ainsi que la pertinence et précision des recommandations émises.

MÉTHODES PÉDAGOGIQUES

- Alternance d'apports théoriques, démonstrations, retours d'expérience et études de cas.
- Travaux pratiques intensifs avec outils réels (SIEM, outils de veille).
- Évaluation continue par quizz, travaux pratiques, dossier professionnel et soutenance.

POINTS FORTS

- Données réelles et outils avancés issus du SOC ACG Cybercampus
- Formateurs experts certifiés avec expérience terrain concrète.
- Bilan personnalisé et plan d'amélioration validés par jury.

Ce parcours certifiant fait partie de l'offre CampusAtlas, **il est reconnu et financé jusqu'à 100% par l'Opco Atlas**, avec des démarches simplifiées, une garantie de qualité et l'accompagnement sur-mesure dont bénéficient les entreprises adhérentes.