État de l'art de la sécurité des Systèmes d'Information

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Fondamentaux de la cybersécurité

Rubrique : Fondamentaux

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Connaître les principes et les normes de chaque domaine de la SSI
- Disposer d'informations sur les tendances actuelles au niveau des menaces et des solutions à notre disposition
- Pouvoir améliorer la communication entre la maitrise d'ouvrage, la maitrise d'oeuvre et la SSI
- Être en mesure d'effectuer des choix techniques

Public visé

- Directeurs des systèmes d'information ou responsable informatique, RSSI, chefs de projet sécurité, architectes informatiques

Pré-requis

- Bonne connaissance générale des systèmes d'information

PROGRAMME

1. **Introduction**

2. Évolutions des menaces et les risques

- Statistiques sur la sécurité
- Tendances dans l'évolution des menaces

3. Modèle d'approche et maturité effective de l'organisme

- Identification des acteurs : organisation et responsabilités
- Exigences SSI : obligations légales métiers, responsabilités civiles, responsabilités pénales, règlements, délégations

4. L'identification des besoins DICP consécutifs aux enjeux

- Classification SSI : informations, données et documents, processus, ressources, les pièges
- Identification des menaces et des vulnérabilités : contextuelles métiers, contextuelles IT
- Cartographie des risques : gravité / vraisemblance, niveaux, traitement du risque, validation des risques résiduels

5. L'état de l'art des méthodologies et des normes

- Bonnes pratiques SSI : les acteurs, les textes de référence, avantages et inconvénients ;

Code de formation : CYB504

€ Tarifs

Prix public : 2420 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 21 heures

Rythme : 3 jours. 14 au 16 Décembre 2026

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 1/11/2026

les règles d'hygiène ANSSI, les fiches CNIL, le chapitre 7 RGS
- Approche enjeux : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27002
- Approche SMSI : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27001

6. Modélisation des niveaux de maturité des technologies SSI

- Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
- La sécurité des accès : filtrage réseau, identification, authentification (faible, moyenne, forte), gestion des identités vs. SSO, habilitation, filtrage applicatif (WAF, CASB et protection du Cloud), détection/protection d'intrusion, journalisation, supervision
- La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP, les recommandations ANSSI
- Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation
- Le cas du DLP : architecture

7. Nomadisme

- Sécurité des postes nomades : problèmes de sécurité liés au nomadisme
- Protection d'un poste vs. Solutions spécifiques
- Mise en quarantaine
- Accès distants
- VPN : concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

8. Les architectures de cloisonnement

- La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité périphérique à la sécurité en profondeur

9. La sécurité des end point

- Le durcissement : postes de travail, ordi phones, serveurs
- L'adjonction d'outils : postes de travail, ordi phones, serveurs
- La sécurité des applications : les standards et les bonnes pratiques

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 1/11/2026