DAWAN

Plan de la formation

www.dawan.fr

Formation État de l’art de la sécurité des systèmes d’information

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 CHF HT (standard) 1 980,00 CHF HT (remisé)
Public :	Directeurs des systèmes d’information ou responsables informatiques - RSSI, chefs de projet sécurité, architectes informatiques
Pré-requis :	Disposer de bonnes connaissances générales sur les systèmes d’information et leurs architectures (infrastructures, applications, réseaux)
Objectifs :	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 disposition - Améliorer la communication entre la maîtrise d’ouvrage, la maîtrise d’œuvre et la SSI - Être en mesure d’effectuer des choix techniques cohérents avec les enjeux métier et le niveau de maturité de l’organisme
Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.

Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102751-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Clarifier les enjeux et poser le cadre de la SSI dans l’organisation

Situer la sécurité des systèmes d’information dans la stratégie globale de l’organisme
Identifier les actifs critiques : données, applications, services, infrastructures, image, conformité
Comprendre les grandes familles de risques : opérationnels, financiers, juridiques, réputationnels
Relier SSI, continuité d’activité, conformité réglementaire (RGPD, sectoriel…) et résilience globale
Atelier fil rouge : cartographier les actifs critiques de l’organisme et leurs enjeux associés

Analyser l’évolution des menaces et des risques

Observer les grandes tendances des menaces : ransomware, supply chain, espionnage, fraude, attaques ciblées
Comprendre l’évolution des attaquants : industrialisation, spécialisation, modèles économiques de la cybercriminalité

Relier les menaces aux vecteurs d’attaque : exposition internet, cloud, télétravail, partenaires, mobilité
Adapter la perception du risque : probabilité, impact, risques systémiques, risques liés à la dépendance numérique
Atelier fil rouge : confronter la cartographie d’actifs aux principales menaces pour dégager une première vision des risques majeurs

Modéliser l’approche SSI et la maturité effective de l’organisme

Découvrir les modèles d’approche de la SSI : gestion de risques, défense en profondeur, Zero Trust, approche par les services
Évaluer la maturité SSI : processus, organisation, techniques, culture, sensibilisation, gouvernance
Utiliser des grilles simples de maturité pour se situer (processus, technologies, pilotage, amélioration continue)
Identifier les écarts entre maturité souhaitée et maturité actuelle pour orienter les priorités
Atelier fil rouge : réaliser un auto-diagnostic de maturité SSI sur quelques axes clés et en dégager 3 priorités

Définir les besoins DICP à partir des enjeux métier

Revoir les notions de Disponibilité, Intégrité, Confidentialité, Preuve (DICP) et leurs impacts métier
Traduire les enjeux métier et réglementaires en exigences DICP par type d’information et de service
Hiérarchiser les exigences DICP pour guider les choix d’architecture, de contrôle et de surveillance
Mettre en cohérence les exigences DICP avec la continuité d’activité (PCA/PRA) et la gestion des incidents
Atelier fil rouge : déterminer les niveaux DICP de plusieurs services clés et en déduire les contraintes SSI prioritaires

Explorer l’état de l’art des méthodologies, normes et référentiels SSI

Découvrir les principales normes et référentiels : ISO 2700x, guides ANSSI, NIST, bonnes pratiques sectorielles
Comprendre l’apport des méthodes de gestion des risques (ex : EBIOS Risk Manager) dans la décision SSI
Situer les référentiels par rapport aux objectifs : conformité, certification, pilotage interne, sensibilisation

Choisir une combinaison pragmatique de référentiels adaptée à la taille, au secteur et aux objectifs de l'organisme
Atelier fil rouge : sélectionner les référentiels et méthodes les plus pertinents pour le contexte de son organisation

Modéliser les niveaux de maturité des technologies SSI

Cartographier les grandes familles de technologies SSI : protections périmétriques, filtrage, IAM, EDR/XDR, SIEM, chiffrement, WAF, etc.
Évaluer le niveau de maturité et de déploiement de ces technologies dans l'organisme
Identifier les redondances, les lacunes et les opportunités de rationalisation
Relier choix technologiques, contraintes budgétaires et gains de maîtrise de risque
Atelier fil rouge : construire une matrice « technologies SSI / maturité / priorités d'évolution »

Intégrer le nomadisme et les nouveaux usages numériques

Analyser les impacts du nomadisme, du télétravail et de la mobilité sur la sécurité (postes, accès, Wi-Fi, données locales)
Prendre en compte les usages cloud, SaaS, applications web et collaboratives dans la stratégie SSI
Adapter les politiques d'accès : VPN, accès conditionnels, MFA, gestion des terminaux (PC, mobiles, BYOD)
Articuler sécurité des usages nomades, expérience utilisateur et exigences DICP
Atelier fil rouge : définir quelques scénarios d'usage nomade et les exigences de sécurité associées

Concevoir des architectures de cloisonnement adaptées

Revenir sur les principes de cloisonnement : segmentation réseau, zones de sécurité, DMZ, micro-segmentation
Identifier les zones à fort enjeu : données sensibles, systèmes critiques, environnements d'administration, partenaires
Relier cloisonnement, supervision et gestion des droits d'accès
Prendre en compte la complexité croissante (cloud hybride, interconnexions, IoT, OT) dans les stratégies de cloisonnement
Atelier fil rouge : esquisser un schéma de cloisonnement cible à partir d'un SI simplifié, en priorisant quelques zones critiques

Renforcer la sécurité des end points et des postes de travail

Analyser le rôle central des postes de travail et des terminaux comme point d’entrée des attaques
Passer de l’antivirus classique à des dispositifs plus modernes (EDR/XDR, contrôle d’applications, durcissement des postes)
Intégrer la gestion des vulnérabilités, des mises à jour, des droits locaux et des usages (clé USB, cloud personnel, etc.)
Articuler sécurité des end points, sensibilisation des utilisateurs et supervision centralisée
Atelier fil rouge : définir un socle de sécurité cible pour les postes de travail en fonction du contexte de l’organisme

Pouvoir effectuer des choix techniques et améliorer la communication MOA / MOE / SSI

Traduire les enjeux métiers et DICP en exigences techniques compréhensibles par la MOE et les équipes SSI
Structurer les décisions : critères, arbitrages, justification des investissements SSI
Améliorer la communication entre maîtrise d’ouvrage, maîtrise d’œuvre et SSI : langage commun, indicateurs, tableaux de bord
Élaborer une feuille de route réaliste de transformation SSI intégrant technologies, organisation et culture
Atelier fil rouge final : formaliser une note d’orientation SSI présentant 3 à 5 choix techniques structurants pour les prochaines années