DAWAN

Plan de la formation

www.dawan.fr

# Formation Cybersécurité : Synthèse technique et souveraineté numérique

| | |
|---|---|
| **Durée :** | 3 jours (21 heures) |
| **Tarifs inter-entreprise :** | 2 275,00 CHF HT (standard)<br>1 820,00 CHF HT (remisé) |
| **Public :** | Tout manager de la DSI impliqué dans la sécurité (responsables de domaine, responsables infrastructures, applications, production…) - RSSI / CISO, responsables SSI, DSI et directions générales souhaitant disposer d'une vision synthétique et stratégique |
| **Pré-requis :** | Bonne connaissance générale du système d'information de l'établissement (architecture globale, applications majeures, enjeux métiers). |
| **Objectifs :** | Connaître l'étendue des risques qui pèsent sur les informations de l'établissement - Comprendre l'évolution des analyses de risque pour faire face aux nouvelles menaces - Identifier les risques associés à l'émergence de nouvelles technologies (cloud, IoT, IA, OT, mobilité…) - Savoir mettre en œuvre une gouvernance de sécurité efficace - Comprendre l'intérêt de disposer d'une surveillance et d'une gestion des incidents de dernière génération - Comprendre les enjeux de la souveraineté numérique et de l'indépendance vis-à-vis des fournisseurs et législations extra-européennes - Préparer l'indépendance numérique de son organisation en identifiant les leviers, ressources et choix technologiques clés. |
| **Modalités pédagogiques, techniques et d'encadrement :** | • Formation synchrone en présentiel et distanciel.<br>• Méthodologie basée sur l'Active Learning : 75 % de pratique minimum.<br>• Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat.<br>• Un formateur expert. |

| | |
|---|---|
| **Modalités d’évaluation :** | • Définition des besoins et attentes des apprenants en amont de la formation.<br>• Auto-positionnement à l'entrée et la sortie de la formation.<br>• Suivi continu par les formateurs durant les ateliers pratiques.<br>• 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 :** | CYB102742-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 |

## Analyser l’état de l’art et l’évolution de la cybersécurité

Cartographier les grandes familles de menaces actuelles : ransomware, espionnage, sabotage, fraude, compromission de comptes, supply chain
Comprendre l’évolution des attaquants : opportunistes, cybercriminalité organisée, groupes étatiques, menaces internes
Relier ces menaces aux différents environnements du SI : datacenter, cloud, OT, postes, mobilité, partenaires
Identifier les grandes tendances de la cybersécurité : défense en profondeur, Zero Trust, automatisation, XDR, SASE
**Atelier fil rouge : partir d’un incident réel ou médiatisé et reconstituer les grandes étapes techniques et organisationnelles de l’attaque**

## Faire évoluer ses analyses de risques face aux nouvelles menaces

Revoir les principes des analyses de risques SSI et leur articulation avec les analyses métiers
Intégrer de nouveaux facteurs de risques : dépendance au cloud, interconnexions

massives, API, données massives, mobilité
Adapter les méthodes de risque : scénarios, criticité métier, vraisemblance, gravité, risques résiduels, risques systémiques
Relier les résultats de l'analyse de risques aux arbitrages d'investissement, aux priorités de projets et aux plans de traitement
**Atelier fil rouge : réaliser une mini-analyse de risques sur un périmètre SI donné et prioriser trois actions de réduction de risques**

## Structurer une gouvernance de la sécurité efficace

Définir les rôles et responsabilités : direction générale, DSI, RSSI, DPO, métiers, prestataires, comités de pilotage
Mettre en place les instances de gouvernance : comité sécurité, comité risques, revue des incidents, revue des projets sensibles
Structurer les documents et référentiels : politique de sécurité, chartes, procédures, registres, plans de continuité
Intégrer la sécurité dans les processus de l'entreprise : achats, projets, gestion de crise, gestion des changements et des vulnérabilités
**Atelier fil rouge : dessiner la gouvernance SSI cible de son organisation et identifier les manques principaux à combler**

## Intégrer les évolutions technologiques dans sa stratégie de sécurité

Identifier les impacts des évolutions technologiques : virtualisation, conteneurs, cloud public/privé, SaaS, IoT, 5G, IA
Appréhender les risques spécifiques liés à ces technologies : surface d'attaque, dépendances, exposition, réglementations
Adapter les architectures de sécurité : segmentation, micro-segmentation, accès conditionnels, gestion des identités et des accès
Prévoir les compétences, outils et partenariats nécessaires pour sécuriser ces nouvelles briques technologiques
**Atelier fil rouge : analyser un projet de migration ou de transformation (ex : cloud, mobilité) et identifier les décisions de sécurité structurantes**

## Mettre en place une surveillance et une gestion des incidents de dernière génération

Comprendre le rôle de la supervision et de la détection : journaux, corrélation, scénarios d'alerte, détection comportementale
Découvrir les socles techniques : SIEM, SOC, EDR, NDR, XDR, SOAR et services managés de sécurité

Organiser la gestion des incidents : classification, priorisation, communication, coordination technique et métier, gestion de crise
Relier la détection et la réponse aux exigences de conformité (notification, rapports, traçabilité, audits)
**Atelier fil rouge : construire un schéma de chaîne de détection et de réponse pour un incident type, du signal faible à la résolution**

## Comprendre les enjeux de la souveraineté numérique

Définir la souveraineté numérique : maîtrise de ses données, de ses infrastructures, de ses dépendances technologiques et juridiques
Comprendre les enjeux de localisation des données, des lois extraterritoriales et des dépendances à certains fournisseurs majeurs
Identifier les liens entre souveraineté, continuité d'activité, résilience et cybersécurité
Situer son organisation dans cet écosystème : secteurs critiques, exigences réglementaires, attentes des clients, enjeux d'image
**Atelier fil rouge : cartographier les dépendances numériques majeures de l'organisation (cloud, logiciels, prestataires, données critiques)**

## Articuler indépendance numérique, choix des fournisseurs et cybersécurité

Analyser les critères de choix des fournisseurs au prisme de la souveraineté : localisation, juridiction, transparence, réversibilité, standards ouverts
Évaluer les bénéfices et limites des offres dites « souveraines » ou « de confiance »
Intégrer les considérations de souveraineté dans les contrats, les appels d'offres et la gestion du cycle de vie des services numériques
Mettre en cohérence la stratégie de cybersécurité avec la stratégie de sourcing et d'infogérance
**Atelier fil rouge : définir une grille de critères souveraineté / sécurité à utiliser dans le choix ou la révision d'un fournisseur clé**

## Identifier les technologies clés et préparer l'indépendance numérique de son organisation

Repérer les technologies clés et les briques critiques : identité, chiffrement, infrastructure, messagerie, collaboration, stockage, sauvegarde
Identifier les marges de manœuvre pour réduire certaines dépendances sans dégrader le service rendu aux métiers
Prioriser les chantiers d'indépendance numérique réalistes : diversification des fournisseurs, standardisation, réversibilité, open source, solutions locales
Élaborer une feuille de route combinant sécurité, résilience et souveraineté numérique
**Atelier fil rouge : formaliser un plan d'action synthétique « cybersécurité et**

**souveraineté numérique » sur 12 à 24 mois**