**Ref :** DNDAESD04 | **Durée :** 5 jours | **Tarif :** 2 €HT

# Introduction à la cyberdéfense

**Formation en visioconférence**

**Objectifs :**

Comprendre les menaces courantes pesant sur les systèmes d'information en vue d'établir un plan de défense en profondeur adapté aux différents types de menaces actuelles.

**Jour 1 matin**

Section 1 - Introduction à la cybersécurité en France
Introduction aux menaces pesant sur les organisations ces dernières années
Vision des dirigeants vis-à-vis de la cybersécurité
Présentation des différents corps d'état liés à la cybersécurité Française

**Jour 1 après-midi**

Zoom sur l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : PSSIE, Homologations ANSSI, Les visas, Le RGS, Instruction 901, Ebios RM
La cybersécurité sur le plan Français et Européen
TP 1 / Rédiger une présentation concise de ce qu'est le RGS dans son contenu et son fonctionnement

**Jour 2 matin**

Section 2 - Audit de la cybersécurité des systèmes d'information
Séquencement d'un projet d'audit de la sécurité de l'information et réalisation d'un rapport
Étude de maturité des processus défensifs
TP 2 / Étude de cas - Identification des mesures de sécurité existante et de leur maturité

**Jour 2 après-midi**

Auditer et Identifier les écarts vis-à-vis du guide d'hygiène de l'ANSSI
TP 3 / Étude de cas - Alignement des mesures de sécurité (maturité, raisons de l'écart) vis-à-vis du guide d'hygiène de l'ANSSI (cf. TP2)

**Jour 3 matin**

Présentation des points stratégiques du rapport auprès de la direction/hiérarchie
TP 4 / Étude de cas - Réaliser une présentation pour la restitution d'audit au CODIR (cf. TP2)

**Jour 3 après-midi**

Section 3 - Étude avancée des différents couches d'une défense en profondeur
Présentation des différentes couches
Couche 1 : Les données : chiffrement, DLP, ACL, Classification et marquage
Couche 2 : Les applications : SLA's, scan et identification des vulnérabilités, gestion des mises à jour

**Jour 4 matin**

Couche 3 : Les hôtes : HIDS/HIPS, Antivirus, pare-feu, gestion des mises à jour, chiffrement, restriction logicielle
Couche 4 : Le réseau : Gestion des mises à jours, NAC, segmentation logique/physique, pare-feu, NIDS/NIPS
Couche 5 : Le périmètre : Pare-feu, Anti-DDoS, Accès distant, Filtrage web, honeypot
Couche 6 : Le cloud : SLA's,

**Jour 4 après-midi**

Couche 7 : La sécurité physique : Contrôle d'accès, sécurité des bâtiments (video, alarme, sécurité salle serveur)
TP 5 / Étude de cas - Proposition d'une stratégie de défense adaptée (cf. TP2)

**Jour 5**

Section 4 - Une défense alignée aux attaques
Revue de la segmentation des phases d'un attaquant
Présentation des différents groupes APT
Étude avancée des étapes d'une attaque APT au travers ATT&CK
Pour aller plus loin (IA, Threat Intelligence)
TP 6 / Étude de l'APT 41 au travers de ATT&CK

## Public

Administrateur système, consultant en sécurité de l'information.

## Pré-requis

Connaissances générales en système et réseau.

## Méthodes pédagogiques

Alternance d'apports théoriques, d'exercices pratiques et d'études de cas.