
# FORMATION Intégrateur Sécurité Réseaux Niveau 1

*Ref.* ***CISR1-10***
*Durée : 5.0 jour(s) / 35.0 heures*

Dans toute entreprise se trouve un système d'information. Il peut être infogéré, dans le Cloud, ou gérer via une DSI, dans tous les cas il représente le point central de toute activité de l'entreprise. Le protéger des malveillance et assurer son bon fonctionnement tout en préservant les performances est un enjeu crucial.

Cette certification permet l'acquisition des savoirs fondamentaux pour pouvoir intégrer une sécurisation des réseaux d'entreprises. Elle s'inscrit dans un shéma de certifications visant à valider les savoirs nécessaires pour les fiches métiers de l'ANSSI suivantes : RSSI, Chef sécurité de projet, Architecte sécurité, Spécialiste sécurité d'un domaine technique, Administrateur de solutions de sécurité, Auditeur de sécurité technique, consultant en cybersécurité, Formateur en cybersécurité.

## Pré-requis :

Connaissance du fonctionnement des réseaux informatique

## Personnes concernées :

Techniciens et administrateurs systèmes et réseaux
Architectes sécurité
Intégrateur sécurité et réseau
Ingénieur sécurité
Responsable sécurité
Chef de projet sécurité

ECSF METIERS ASSOCIE :
Chief Information Security Officer, Cybersecurity Architect, Cybersecurity implementor, Cybersecurity auditor

## Objectifs :

À l'issue de la formation, le participant sera en mesure de :
Acquériir les bonnes pratiques de sécurisation des réseaux
Identifier les menaces liées aux réseaux
Appliquer les bonnes pratiques de sécurisation des systèmes et réseaux
Choisir les mesures de sécurité adaptées
Elaborer une politique de sécurité des réseaux

## Programme :

**JOUR 1**

**Introduction SSI**
Le numérique en entreprise
La convergence des réseaux
Etat des menaces sur les réseaux en 2021
Les typologies des attaquants
Les outils d'attaques
Les typologies d'attaques
Les CVE & CVSS
Les attaques APT
The Unified Kill Chain
Les piliers de la sécurité
Les principes généraux de la sécurité
La sécurité dans le cyber-espace
Les acteurs de la cybersécurité
La sécurité offensive
**Les bases de la cryptographie**
Vocabulaire
Objectifs
Chiffrement de César & chiffrement de Vigenère
Principe de Kerckhoffs
Le chiffrement symétrique
Le chiffrement asymétrique
Les recommandations de sécurité
Fonction de hash

**QUIZZ sur Introduction et cryptographie**

**JOUR 2**

**Virtual Private Network & Accès sécurisé**
Définition
Les implémentations VPN
Les protocoles VPN
IPSEC
TLS
Autres protocoles sécurisés : SSH
**TD  Mise en place du VPN IPSec & mise en  place de SSH**
**IAM**
Gestion des identités et des accès
IAAA
Les méthodes d'authentification
Cycle de vie des accès
Stratégie de gestion des identités
LDAP
Les modèles de contrôle des accès
Les implémentations
Focus sur Kerberos
**TP mise en place Kerberos**

**JOUR 3**

**Pare-feu**
Définition
Place du pare-feu dans le modèle OSI
Règles de pare-feu
Pare-feu Stateless & Statefull
Politique de filtrage
Les limites des pare-feux traditionnels
Les pare-feux nouvelles génération
Méthodologie de la mise en place d'une politique de filtrage
Bonnes pratiques d'ordre général
**TP : Etude d'une cartographie et mise en place d'une politique de filtrage**

**Proxy**
Définition
Pourquoi un serveur mandataire ?
Le filtrage URL
Les types de proxy
Les implémentations de proxy
**TP : Mise en place d'un proxy et de règles de filtrage**

**JOUR 4**

**Les architectures de passerelle d'interconnexion**
Le concept
La passerelle d'interconnexion selon les niveaux de sécurité
**Sécurité des équipements réseau**
Administration
Cloisonnement des réseaux
Sécurisation des ports
Mécanismes liés à la disponibilité
Synchronisation horaire et horodatage
Journalisation
TD : Durcissement de commutateurs et routeurs, quizz global

**JOUR 5**

Examen blanc : Quizz sur l'ensemble des points abordés, mise en place d'une architecture sécurisée, réalisation d'une politique de filtrage

Examen final : QCM sur SSI, bonnes pratiques de sécurisation des réseaux, cryptographie. Etude de cas sur la mise en place d'une architecture sécurisée. Points spécifiques sur politiques filtrages, durcissements des équipements, mise en place VPN

## Démarche pédagogique :

Formation orientée sur la pratique
70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

## Evaluation et validation :

**EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES**
Partie théorique et pratique
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.
Il peut se dérouler à distance.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'Europpean union agency for cybersecurity via l'European Cybersecurity Skills Framework