

Formation Cybersécurité : Fondamentaux de la sécurité Systèmes et Réseaux

■ Durée :	5 jours (35 heures)
■ Tarifs inter-entreprise :	2 475,00 CHF HT (standard) 1 980,00 CHF HT (remisé)
■ Public :	Tous
■ Pré-requis :	Connaissance des protocoles réseaux
■ Objectifs :	Comprendre les enjeux de la sécurité d'un réseau informatique et savoir la mettre en œuvre
■ 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 :	RÉS445-F
■ Note de satisfaction des participants:	4,70 / 5
■ 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

Introduction

Enjeux de la sécurité

Évaluation des risques

Critères de sécurité

Normes liées à la sécurité

Plans de continuité ou de reprise d'activité

Analyse du risque et des menaces

Analyse des risques et élaboration des scénarios

Caractérisation des menaces (sources, vulnérabilités, objectif)

Savoir faire un inventaire des menaces caractéristiques

Adéquation risque-menace et disponibilité

Atelier pratique : Mise en situation d'un laboratoire de pentest dans le cadre d'une équipe red team sur les attaques courantes, puis une équipe blue team pour les contre-mesures

Les différents niveaux de gestion de la sécurité

Sécuriser les données, les échanges, et le réseau

Sécurité du système d'exploitation, réduction de la surface d'attaque

Sécurité des applications

Gestion des identités

Auditer un système

Sécurité des données

Les problématiques de l'accès physique

Identification des ressources critiques

Chiffrer les données

Sécurité des échanges de données

Contraintes de sécurité : intégrité, confidentialité, non-répudiation

Principes de chiffrement, symétrique, asymétrique (clés privées, secret partagé..)

Contraintes liées au support (espionnage, liaisons sans fil..)

VPN, TLS

Sécurisation de Linux

Permissions standards et étendues

Gestion des profils de sécurité et des limitations des applications

Utilisation de PAM

Mise en place du pare-feu sur Linux

Manipulation du chiffrement disque sur Linux

Gestion des intrusions et des journaux (logs)

Sécurisation de Windows

Gestion des droits

Gestion des services

Accès problématiques pour le réseau et les périphériques

Configuration du pare-feu, et réflexions

Possibilités de chiffrement

Gestion du journal d'évènement et des audits

Audit d'un système

Analyse externe au niveau réseau

Inventaire des risques opérationnels

Vérification du cloisonnement applicatif et utilisateur

Risques liées à la maintenance du système (versions des logiciels, mauvaises configurations)

Tentatives d'intrusion ciblées

Sécurité réseau

VLAN, 802.1x, NAC

Firewall

Proxy

IDS/IPS/DPI

SIEM, SOAR, SOC

Sécurité du cloud

Sécurité Wifi