



# ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

## Formation Cours Responsable infrastructure

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

### Résumé

Pour faire face à la montée en puissance des nouvelles menaces qui pèsent sur nos systèmes d'information, le monde de la sécurité doit s'adapter, et est de fait en perpétuelle évolution aussi bien sur le plan des technologies que des méthodes et modèles conceptuels sous-jacents. Ce séminaire de 3 jours dresse un état de l'art complet des outils organisationnels, méthodologiques et techniques de maîtrise du risque informatique. Il permettra aux participants de disposer des informations nécessaires à l'élaboration d'une feuille de route menant à la mise en place d'une politique de sécurité efficace.

### Objectifs

- | Savoir hiérarchiser les points importants des réseaux d'aujourd'hui
- | Comprendre les offres des différents opérateurs du marché
- | Mesurer les enjeux relatifs aux aspects sécurité et disponibilité
- | préconiser des choix en matière de réseaux
- | Comprendre les principes et les stratégies de virtualisation
- | Connaître et différencier les différentes solutions du marché
- | Savoir où et comment implémenter les infrastructures virtuelles
- | Pouvoir décider de l'éligibilité des ressources à virtualiser
- | Harmoniser la production virtuelle avec la production traditionnelle
- | Être informé des règles de l'art dans la gestion des infrastructures virtuelles
- | Connaître les différents types de Cloud
- | Identifier les technologies concernées par le Cloud
- | Anticiper les impacts directs et indirects du Cloud sur l'entreprise et son système d'informations
- | mener un projet de Cloud Computing
- | Comprendre les aspects techniques et les méthodes d'analyse permettant d'intégrer le transport de la voix dans un réseau IP
- | Savoir situer les caractéristiques des différents protocoles
- | Pouvoir réaliser les calculs de dimensionnement
- | Maîtriser les concepts de qualité de service, réservation (RSVP) et d'architecture Diffserv
- | choisir des technologies VOIP adaptées à ses besoins
- | Comprendre les enjeux liés au stockage des données et à ses évolutions
- | identifier les solutions proposées en fonction de l'évolution des technologies du stockage
- | Apprendre à connaître les concepts de base, les technologies, les architectures et les meilleures pratiques à mettre en oeuvre
- | Disposer d'informations permettant d'identifier le besoin en stockage dans l'organisation
- | Pouvoir bénéficier de conseils pour réussir votre projet d'évolution du stockage
- | Savoir éviter les principaux pièges en la matière
- | 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 notre disposition
- | Pouvoir améliorer la communication entre la maîtrise d'ouvrage, la maîtrise d'oeuvre et la SSI
- | effectuer des choix techniques

Référence	MET037
Durée	15 jours (105h)
Tarif	13 480 €HT

### SESSIONS PROGRAMMÉES

#### A DISTANCE (FRA)

- le 17 août 2026
- le 12 octobre 2026
- le 23 novembre 2026

#### PARIS

- le 17 août 2026
- le 12 octobre 2026
- le 23 novembre 2026

#### AIX-EN-PROVENCE

- le 12 octobre 2026

#### BORDEAUX

- le 17 août 2026

#### LILLE

- le 12 octobre 2026

#### LYON

- le 17 août 2026

#### ROUEN

- le 17 août 2026

#### SOPHIA-ANTIPOLIS

- le 17 août 2026

#### STRASBOURG

- le 17 août 2026

#### TOULOUSE

- le 17 août 2026
- le 12 octobre 2026

## Public

| Professionnels désirant comprendre la structure des réseaux de données et la transmission dans les réseaux LAN et WAN Consultant, RSI ayant besoin d'une vision globale des technologies réseaux Toute personne souhaitant disposer d'une vision globale et synthétique des techniques réseaux

## Prérequis

| connaissance générale des réseaux et en particulier du protocole IP

## Programme de la formation

### **PARTIE 1 - Panorama des technologies réseaux**

#### **Les réseaux locaux**

| Les réseaux locaux  
| Les principaux organismes  
| Les réseaux usuels  
| Classification des réseaux  
| Le modèle OSI  
| Les différents composants d'un réseau

#### **Ethernet**

| Présentation  
| Méthode d'accès CSMA/CD  
| Les adresses MAC  
| Les différentes topologies  
| Connecteurs et câblage  
| Le format des trames Ethernet II et 802.2, 802.3

#### **La commutation**

| Les extensions Ethernet  
| Les pontages  
| Le spanning tree : STP, PVST, RSTP, MSTP, PVRST  
| La commutation de niveau II  
| Les VLANs  
| La norme 802.1q  
| La commutation de niveaux 3 et 4

#### **Les technologies ATM, XDSL et LRE**

| Réseau ATM : Présentation, structure ATM, les circuits virtuels, la commutation, AAL, les classes de service, ATM et IP  
| xDSL : Les principes, les familles, ADSL, SDSL, les composants, PPOA et PPPoE  
| LRE : Principes et composants

#### **Les réseaux WiFi**

| Présentation  
| Les réseaux sans-fil  
| Les Wireless Area Network : WLAN  
| Les différentes topologies  
| L'importance du SSID  
| Les extensions des WLAN  
| Les méthodes de commutation  
| Les normes associées  
| La sécurité : Clés WEP, WPA, WPA2, EAP et RADIUS

#### **Les réseaux étendus**

| Définitions  
| Le protocole HDLC  
| Le réseau téléphonique commuté : RTC  
| Le réseau numérique à intégration de services : RNIS  
| Le protocole PPP, sa structure, PAP, CHAP, OTP

#### **Routage et MPLS**

| Présentation du routage  
| Fonctionnement et limitation du routage

- | Présentation du MPLS
- | Les mécanismes du MPLS : VRF, Sécurité, QoS

### **Les réseaux BGP**

- | Présentation
- | Structure
- | Fonctionnement
- | Limitations

### **Voix sur IP (VOIP)**

- | Présentation
- | Numérisation de la voix et codecs
- | Contraintes de la VoIP et Gigue
- | RTP / RTCP
- | Les protocoles : H323 / SIP / MGCP

### **Téléphonie sur IP : TOIP)**

- | Présentation
- | Composants
- | FXS / FXO
- | RNIS
- | QSIG
- | Passerelles
- | Topologies

### **Qualité de service : QoS)**

- | Définitions
- | Mécanismes de congestion
- | Les causes de la congestion
- | Les différents modèles de QoS
- | Classification et marquage : 802.1p vs CoS, IP precedence vs DSCP, EXP MPLS
- | Integrated Services Model : RSVP, COPS
- | Differentiated Services Model : IP Precedence, DSCP
- | Les différents modes de gestion de files d'attente : FIFO, PQ, CQ, WFQ, LLQ, CBWFQ
- | La prévention de la congestion : RED, WRED
- | Policing et shaping
- | Intégration CoS, DSCP, MPLS, BGP

### **Multicast**

- | Présentation
- | Principes
- | Adressage
- | IGMP
- | Routage
- | Protocoles de routage : PIM SM, DM et SSM, MOSPF, DVMRP, MBGP

### **Gestion des réseaux**

- | Présentation
- | Fonctions de l'administration des réseaux
- | Analyseurs matériels
- | Analyseurs de trafic réseau
- | SNMP

### **La sécurité des réseaux**

- | Les bases de la sécurité réseau
- | Principales attaques réseaux
- | Éléments de la sécurité réseau : pare-feux, proxies, sondes, outils de corrélation
- | Traduction d'adresses : PAT, NAT et SATVPN / VPDN
- | Principaux protocoles : GRE, L2TP, PPTP et IPSec

## **PARTIE 2 - Etat de l'art de la virtualisation**

### **Présentation**

- | L'histoire de la virtualisation
- | Évolution du marché de la virtualisation

- | La rationalisation des services IT par la virtualisation
- | Concepts de l'infrastructure virtuelle
- | Les principaux gains
- | L'adoption d'une infrastructure virtuelle

### **Les technologies de virtualisation des systèmes x86**

- | Tour d'horizon des approches de virtualisation
- | L'Hyperviseur
- | Les composants d'une infrastructure virtuelle

### **Les solutions du marché**

- | Offre Microsoft
- | Offre Citrix
- | Offre VMware
- | Comparatif des solutions
- | Les implémentations types
- | Démonstrations

### **La gestion d'une infrastructure virtuelle**

- | Gestion des environnements de test et de développement
- | Virtualisation du poste de travail
- | Sauvegarde et continuité de service d'une infrastructure virtuelle
- | Plan de reprise d'activité

### **Solutions complémentaires liées à la virtualisation**

- | Analyse des systèmes
- | Les outils de migration X2X du marché
- | La sauvegarde des machines virtuelles
- | La réplication de machines virtuelles
- | Le suivi des performances de l'infrastructure virtuelle

### **Les bonnes pratiques de mise en oeuvre d'un projet de virtualisation**

- | Le déroulement d'un projet de virtualisation
- | Analyse TCO/ROI
- | La mise en oeuvre : risques et recommandations

## **PARTIE 3 - Cloud - La synthèse**

### **Définition opérationnelle du Cloud**

- | Concept et définition opérationnelle
- | Caractéristiques essentielles qui font le succès du Cloud public
- | Quatre technologies fondamentales des plateformes Cloud, définies par le NIST Classification générique de Cloud : IaaS, PaaS, SaaS, FaaS, SaaS
- | Déploiement du Cloud : public, privé, hybride, virtuel, communautaire
- | Exemple de plates-formes de chaque type
- | Usages et apports fondateurs du Cloud

### **Technologies de référence des plates-formes de Cloud**

- | Architecture technique du Cloud : Microservices/Apps et API et différences avec de l'architecture traditionnelle
- | Deux composants essentiels du Cloud : Openstack et Plateforme de développement : Cloud Foundry, OpenShift, GCE
- | Technologies de l'OpenStack : composants principaux et socle de l'écosystème
- | Technologies de la plateforme de développement pour la création et le déploiement d'applications : IaC, Ansible, Terraform, Kubernetes, Docker, etc.)
- | Conception d'une plateforme générique de Cloud à partir des composants techniques de l'écosystème
- | Architecture opérationnelle de bout en bout d'un Cloud

### **Niveau de performance d'une plate-forme Cloud IaaS**

- | Principales métriques pour évaluer la performance technique
- | Capacité technique de la plateforme à supporter les applications avancées
- | Infrastructure virtuelle pour déployer le système informatique des entreprises et organisations
- | Architecture de stockage et de traitement distribués pour déployer le Big Data Solutions complètes pour déployer l'Internet des Objets : télémétrie, IoT, M2M
- | Architecture pour le déploiement de la Blockchain
- | Dispositifs pour exploiter l'Intelligence artificielle et la Machine Learning / Informatique quantique

## **Niveau de sécurité d'une plate-forme Cloud IaaS**

- | Capacité technique de la plateforme à sécuriser les applications déployées
- | Sécurité conventionnelle recommandée par le CSA : Cloud Sécurité Alliance : Firewall, NGFW, IDS/IPS
- | Sécurité opérationnelle et architecturale du Cloud à considérer: segmentation
- | Solutions techniques de sécurité de base pour protéger les données, la virtualisation, d'intégrité des applications
- | Solutions avancées de sécurité pour répondre aux caractéristiques techniques spécifiques des environnements Cloud : sécurité définie par logiciel : Software Defined Security' IA/OPS et apprentissage automatique, informatique quantique

## **Plates-formes majeures Cloud Public du marché**

- | Amazon Web Services : AWS
- | Google Cloud Platform : GCP
- | Microsoft Azure
- | Particularités et différences de chaque plateforme
- | Positionnement concurrentiel des acteurs

## **Migration des applications dans le Cloud public : retour d'expérience**

- | Définir la stratégie Cloud : Cloud public, Cloud hybride : Cloud public + Cloud privé avec OpenStack ou solution de virtualisation propriétaire), multicloud
- | Validation des apports réels
- | Facteurs clés de succès et Causes d'échec et risques
- | Détermination des termes des contrats SLA et PLA
- | Référentiels et normes sur lesquels s'appuyer: RGPD, CSA, Cloud Act, SecNumCloud, Data Act
- | Exemple de cas de migration selon les workflows, outils de travail

## **Impact et grandes tendances**

- | Multicloud : fusion naturelle entre le système informatique de l'entreprise et les clouds publics
- | Accélération de l'usage de la virtualisation et de l'IA
- | Impacts sur les compétences des équipes informatiques et sur l'organisation de la DSI

## **PARTIE 4 - Voix et téléphonie sur IP**

### **Introduction**

- | Rappels sur la téléphonie classique
- | Voix analogique
- | Rappel RNIS

### **La voix en paquets**

- | Passage de la voix analogique à la voix numérique
- | Mise en paquet de la voix numérisée
- | Les codecs

### **Les protocoles utilisés**

- | RTP et RTCP
- | Calcul de la bande passante réelle en fonction du codec utilisé
- | Compression d'en-tête TRP : cRTP

### **Le protocole H323**

- | Présentation du modèle
- | Les Gateway, les MCU, les Gatekeeper
- | Les relais FAX et DTMF

### **SIP(Session Initiation Protocol)**

- | Description du protocole
- | Les composants UAC, UAS
- | Serveurs SIP, messages SIP et adressage SIP
- | Établissement d'un appel SIP
- | Le protocole SDP : Session Description Protocol

### **MGCP**

- | Composants call agent et media-gateway
- | Interopérabilité avec SIP et H323
- | Les commandes
- | Utilisation du protocole MGCP aujourd'hui

### **La qualité de service**

- | Contraintes liées à la voix
- | Les modèles et les outils de la QoS
- | Classification, marquage et Queueing
- | Policing, shaping et token bucket
- | Réseau opérateur MPLS et QoS

### **Dimensionnement d'un réseau de voix**

- | Rappels sur les Erlang
- | Dimensionnement des trunk
- | Calcul du dimensionnement réel en IP

### **Le marché actuel**

- | Introduction de la sécurité au niveau des postes et des serveurs
- | L'offre du marché et les différents acteurs

## **PARTIE 5 - État de l'art du stockage de données SAN/NAS**

### **Les fondamentaux du stockage de données**

- | La nouvelle pyramide hiérarchique des technologies
- | L'évolution technologique : disques et bandes magnétiques, disques optiques
- | Les interfaces et protocoles : Infiniband, FibreChannel, SCSI, SATA
- | L'évolution des architectures des systèmes de stockage : RAID, CAS, RAIN, MAID

### **Le stockage en réseau**

- | L'infrastructure SAN/Fibre Channel et SAN sur IP
- | Positionnement des architectures DAS, NAS, SAN : FC et iSCSI
- | Les phases d'évolution du stockage en réseau : convergence NAS-SAN, iSCSI
- | L'état de la standardisation et les seuils d'industrialisation : SMI, NDMP, DAFS

### **La redondance des données RAID et les critères de sélection**

- | Les niveaux de RAID
- | Critères de sélection

### **La virtualisation**

- | Les bases de la virtualisation
- | Architecture Symétrique : in-band' ou Asymétrique : out-band)
- | Les solutions de virtualisation de l'espace de stockage : disques et bibliothèques virtuelles VTL
- | La gestion de l'espace virtuel : Thin Provisionning et le Thick Provisionning
- | La gestion du stockage par niveau le "Tiering"

### **Le stockage en réseau au service des établissements**

- | Le partage de l'espace de stockage : LUN mapping, zoning, LUN masking
- | La consolidation du stockage
- | Les mouvements de données dans l'espace de stockage : HSM, copies, agents
- | La disponibilité des données : HA, clustering
- | La sécurité des données : zones sensibles
- | La gestion du stockage de données : ressources, services et règles, SMI
- | Le modèle informatique centré sur l'information : le stockage sous forme de services

### **La gestion du cycle de vie des données (ILM)**

- | Valeur et accès à l'information au cours du temps
- | Qu'est-ce que l'ILM ?
- | Principales applications
- | Solutions du marché : maturité et limites

### **Le stockage en réseau au service des établissements**

- | Problématiques
- | Procédures, architectures
- | Technique utilisée : la déduplication, les snapshots réplication, sauvegarde CDP
- | Le RTO : Recovery Time Objective
- | Le RPO : Recovery Point Objective
- | Reprise après sinistre et continuité d'activité : plan de retour d'activité : PRA' plan de continuité d'activité : PCA)
- | Méthodes et outils appropriés aux PRA/PCA

### **La sécurisation des données par la réplication**

- | La réplication synchrone
- | La réplication asynchrone
- | La réplication asynchrone : temps réel
- | Les protocoles de la réplication

### **L'archivage des données**

- | Concept
- | Technologies utilisées pour l'archivage numérique
- | Normes en usage : NF Z 42-013, NF Z 43-400, ISO 14641-1
- | Savoir définir et mettre en oeuvre une politique d'archivage
- | Qu'est-ce qu'une politique d'archivage
- | Votre plan d'archivage en fonction des données
- | Faut-il externaliser l'archivage ?

### **Comment maîtriser votre projet de stockage : du dimensionnement à la mise en place)**

- | Évaluer votre espace de stockage en fonction des données
- | Les contrôleurs de stockage
- | La configuration Actif/Passif par rapport à la configuration Actif/Actif
- | La mémoire cache
- | Le choix de disque dur
- | La hiérarchisation du stockage : HSM et la gestion par niveau le "Tiering"

### **Synthèse et recommandations**

- | Les 10 messages-clés pour réussir votre projet d'évolution du stockage

## **PARTIE 6 - État de l'art de la sécurité des Systèmes d'Information**

### **Introduction**

#### **Évolutions des menaces et les risques**

- | Statistiques sur la sécurité
- | Tendances dans l'évolution des menaces

#### **Modèle d'approche et maturité effective de l'organisme**

- | Identification des acteurs : organisation et responsabilités
- | Exigences SSI : obligations légales métiers, responsabilités civiles, responsabilités pénales, règlements, délégations

#### **L'identification des besoins DICP consécutifs aux enjeux**

- | Classification SSI : informations, données et documents, processus, ressources, les pièges
- | Identification des menaces et des vulnérabilités : contextuelles métiers, contextuelles IT
- | Cartographie des risques : gravité / vraisemblance, niveaux, traitement du risque, validation des risques résiduels

#### **L'état de l'art des méthodologies et des normes**

- | Bonnes pratiques SSI : les acteurs, les textes de référence, avantages et inconvénients ; les règles d'hygiène ANSSI, les fiches CNIL, le chapitre 7 RGS
- | Approche enjeux : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27002
- | Approche SMSI : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27001

#### **Modélisation des niveaux de maturité des technologies SSI**

- | Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
- | La sécurité des accès : filtrage réseau, identification, authentification : faible, moyenne, forte' gestion des identités vs. SSO, habilitation, filtrage applicatif : WAF, CASB et protection du Cloud), détection/protection d'intrusion, journalisation, supervision
- | La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP, les recommandations ANSSI
- | Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation
- | Le cas du DLP : architecture

#### **Nomadisme**

- | Sécurité des postes nomades : problèmes de sécurité liés au nomadisme
- | Protection d'un poste vs. solutions spécifiques
- | Mise en quarantaine
- | Accès distants
- | VPN : concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

#### **Les architectures de cloisonnement**

- | La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité

périphérique à la sécurité en profondeur

### **La sécurité des end point**

- | Le durcissement : postes de travail, ordi phones, serveurs
- | L'adjonction d'outils : postes de travail, ordi phones, serveurs
- | La sécurité des applications : les standards et les bonnes pratiques

### **Méthode pédagogique**

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

### **Méthode d'évaluation**

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

---

### **Suivre cette formation à distance**

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

- | Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
- | Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
- | Privilégier une connexion filaire plutôt que le Wifi.
- | Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
- | Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
- | Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
- | Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
- | Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
- | Horaires identiques au présentiel.