



## 1. VOS ATTENTES

Dans le cadre de votre politique de formation, vous désirez augmenter le niveau de compétence de vos adhérents chargés de l'installation des systèmes de sûreté. L'évolution de ces systèmes demande des connaissances sur les réseaux informatiques pour en permettre l'intégration, ainsi que la dimension du risque cyber qui ne peut être ignoré.

## 2. NOTRE PROPOSITION

### Objectifs généraux de la formation

L'action de formation doit permettre aux participants de :

- ✓ Identifier les composants et le fonctionnement d'un réseau informatique
- ✓ Définir les besoins avec le service informatique
- ✓ Intégrer un équipement de sécurité sur un réseau informatique

### Public

Les adhérents du groupement GPMSE  
INSTALLATION

### Pré-requis

- ✓ Connaissances en électronique et/ou électrotechnique
- ✓ Connaissances du fonctionnement et de l'installation des équipements de sécurité (détection intrusion, vidéosurveillance, contrôle d'accès)

### Durée, dates et lieux de formation

3,5 jours soit 24,5 heures de formation

Dates à définir en fonction des disponibilités de chacune des deux parties

Déroulement de la formation dans les locaux de CNPP SAINT MARCEL



### 3. LA CONCEPTION PEDAGOGIQUE

Elle consiste en l'étude de la part de l'intervenant du parcours pédagogique et à la préparation des documents remis aux stagiaires pendant la formation.

### 4. CONTENU DE LA FORMATION

<b>Première journée</b> 8H30 - 17H00	<ul style="list-style-type: none"><li>- Les réseaux informatiques</li><li>- Débit et bande passante</li><li>- Raccordement de matériel sur le réseau</li><li>- Raccordement physique (support d'interconnexion)</li></ul>
<b>Deuxième journée</b> 8H30 - 17H00	<ul style="list-style-type: none"><li>- Définition de la cybermenace</li><li>- Présentation des principales vulnérabilités des systèmes</li><li>- Démonstration : attaques sur matériels de sécurité / sûreté</li><li>- Recommandations pour la mise en sécurité d'une installation</li><li>- Démonstration : mise en sécurité d'une installation de sécurité / sûreté</li></ul>
<b>Troisième journée</b> 8H30 - 17H00	<ul style="list-style-type: none"><li>- Vidéosurveillance sur IP</li><li>- De l'analogique vers le Numérique</li><li>- Technologie numérique</li><li>- Construire son système vidéo numérique</li><li>- Contrôle d'accès / détection intrusion</li><li>- Mise à jour et paramétrage des différents composants</li><li>- Travaux pratiques</li></ul>
<b>Quatrième journée</b> 8H30 - 12H00	<ul style="list-style-type: none"><li>- Travaux pratiques (suite)</li><li>- Obtention d'une attestation de connaissances à l'issue d'une épreuve écrite de type QCM</li></ul>



## 5. PROGRAMME DETAILLE

.....1<sup>ère</sup> journée

8h30 – 17h00

### Les réseaux informatiques

- ✓ Architecture
- ✓ Matériel

### Débit et bande passante

### Raccordement de matériel sur le réseau

- ✓ Conséquences
- ✓ Avantages/inconvénients

### Raccordement physique (support d'interconnexion)

- ✓ Câble
- ✓ Fibre optique
- ✓ Liaison hertzienne

### Paramétrage : configuration d'adresse d'un matériel sur un réseau

### Démonstration (mise en œuvre d'un réseau et interconnexion de matériel)

.....2<sup>ème</sup> journée

8h30 – 17h00

### Définition de la cybermenace

### Présentation des principales vulnérabilités des systèmes

### Démonstration : attaques sur matériels de sécurité / sûreté

### Recommandations pour la mise en sécurité d'une installation

### Démonstration : mise en sécurité d'une installation de sécurité / sûreté

8h30 – 17h00

#### Vidéosurveillance sur IP

- ✓ Qu'est ce que la vidéo sur IP
- ✓ Identification des matériels : caméra, serveur vidéo, logiciel...

#### De l'analogique vers le Numérique

- ✓ Comment faire évoluer son système analogique vers un système numérique
- ✓ Analyse des fonctions principales : prise de vue, transmission, visualisation, enregistrement

#### Technologie numérique

- ✓ Prise de vue capteur CCD, CMOS, Mégapixel
- ✓ Compression différents algorithmes et Normes (Mpeg4/Mpe2/wavelet...)
- ✓ Les différentes résolutions

#### Construire son système vidéo numérique

- ✓ Calcul de la bande passante
- ✓ Calcul de stockage et définition du type d'archive (Raid, Nas, ...)
- ✓ Gestion vidéo (Hypervision, Supervision IHM)
- ✓ Définition de ces besoins réseaux

#### Contrôle d'accès / détection intrusion

- ✓ Intégration sur le réseau
- ✓ Bande passante
- ✓ Définition des besoins
- ✓ Interopérabilité

#### Mise en jour et paramétrage des différents composants

#### Travaux pratiques

- ✓ Intégration des différents composants (contrôle d'accès, vidéosurveillance et détection intrusion) sur un réseau informatique (définition des besoins de bande passante, mise en œuvre)

8h30 – 12h30

#### Travaux pratiques (SUITE)

- ✓ Intégration des différents composants (contrôle d'accès, vidéosurveillance et détection intrusion) sur un réseau informatique (définition des besoins de bande passante, mise en œuvre)

#### Contrôle des connaissances

- ✓ Obtention d'une attestation de connaissance à l'issue d'une épreuve écrite de type QCM

## 6. MOYENS PEDAGOGIQUES NECESSAIRES

### Fournis par CNPP

- ✓ Une salle de cours équipée des moyens suivants :
  - Un vidéo projecteur
  - Un tableau blanc
  - Un paper board
  - Maquettes
- ✓ Différentes maquettes de systèmes électroniques de lutte contre la malveillance de divers constructeurs et le matériel nécessaire à la construction d'un réseau informatique
- ✓ Une documentation spécifique par stagiaire





## 7. MODALITES D'EVALUATION

### Un suivi qualitatif par l'évaluation

#### **EVALUATION EN COURS DE FORMATION**

L'interactivité et certaines séquences pédagogiques, provoquant la re-formulation par les stagiaires des enseignements, permettent à l'intervenant d'évaluer la transmission des savoirs et savoir-faire et d'estimer l'atteinte des objectifs de formation.

#### **EVALUATION EN FIN DE FORMATION**

L'évaluation sera réalisée par un test théorique de types QCM en fin de formation. La réussite des tests théoriques permet l'obtention d'une attestation de connaissance.

#### **BILAN DE LA FORMATION**

A l'issue de la formation, un questionnaire de satisfaction est envoyé au commanditaire de la formation. Cette évaluation nous permet de mesurer l'efficacité de nos formations et d'améliorer nos processus de production. Un questionnaire de satisfaction est également complété par chaque stagiaire en fin de formation.

## 8. NOS INTERVENANTS

Notre dispositif de formation est piloté par un responsable de filière, expert dans son domaine d'activité et garant de l'adéquation entre notre réponse pédagogique et votre besoin.

Il sélectionne et accompagne nos intervenants dans les missions de préparation, d'organisation, de conception, d'animation et d'évaluation de l'efficacité de nos actions.

La prestation sera réalisée par des intervenants possédant les qualités suivantes :

- ✓ expérience professionnelle significative dans les fonctions de la sécurité
- ✓ vision concrète de la prévention des risques industriels ou tertiaires
- ✓ capacité à transmettre un savoir à un public varié
- ✓ animation et dynamique de groupe

Le parcours pédagogique est adapté aux professionnels en formation et aux exigences de l'entreprise.



## 9. LES AVANTAGES DE CNPP

### L'expertise à votre service

CNPP c'est 60 années d'activités dans l'expertise en matière de prévention et de maîtrise des risques :

- Laboratoire pour les essais de conformité des produits de sécurité malveillance (centrales d'alarme, détecteurs de mouvements, sirènes, enregistreurs vidéo numériques, caméras, moniteurs, coffres et systèmes bancaires (DAB, GAB), systèmes de neutralisation de billets, serrures, fermetures, protections des bâtiments, antivols de véhicules, ... ;
- Organisme certificateur des entreprises de service en matière de sécurité (installateurs, mainteneurs);
- Membre actif des comités de normalisation français, européens et internationaux ;
- Rédacteur de règles techniques.

Le "Département Formation" est placé au cœur des activités de CNPP. Il profite de la participation de nos experts pour nourrir ses actions de formation et faire profiter à nos clients de notre retour d'expérience.

### La qualité à votre service

Les processus de formation de CNPP répondent aux normes OPQF et ISO 9001 et garantissent un haut niveau de prestation.

Le service qualité du département formation est à votre service pour toute réclamation ou suggestion d'amélioration non traitée par vos interlocuteurs habituels au 02.32.53.64.93.

