

## Formation Cisco : Supervision et sécurisation d'un réseau TCP/IP

<b>Durée :</b>	3 jours
<b>Public :</b>	Administrateurs de systèmes et réseaux locaux
<b>Pré-requis :</b>	- Capacité à administrer des réseaux locaux d'entreprises fonctionnant sous TCP/IP - Capacité à utiliser un poste sous Linux en ligne de commande et avec une interface graphique
<b>Objectifs :</b>	- Analyser les flux échangés sur un réseau - Contrôler l'accès au réseau - Surveiller les accès au réseau
<b>Sanction :</b>	Attestation de fin de stage mentionnant le résultat des acquis
<b>Taux de retour à l'emploi:</b>	Aucune donnée disponible
<b>Référence:</b>	RéS917-F
<b>Note de satisfaction des participants:</b>	Pas de données disponibles

### Les concepts

Les problèmes qui menacent un réseau informatique  
Les journaux d'événements  
Recueil d'informations et d'alertes  
Points de mesure  
Techniques de surveillance.

Mot-clés : *TCP/IP, NetFlow/IPFIX, SNMP, NDIS/IDS*

**Atelier pratique : mise en oeuvre de SNMP**

### Les outils d'analyse et de synthèse des flux

La capture de trames  
L'analyse de flux  
La mesure de performance

**Ateliers pratiques : mise en oeuvre de wireshark, ntopng, MRTG, Munin et cacti**

### Les outils de contrôle d'accès aux réseaux

Le contrôle l'accès aux ressources  
Le filtrage de trames  
Les parefeux

IPSec

**Ateliers pratiques : mise en oeuvre de nmap et ipcop**

### **Les outils de renforcement de la sécurité**

Surveillance de l'accès à des fichiers

Détection des failles de sécurité

Détection des intrusions sur le réseau

**Ateliers pratiques : mise en oeuvre de tripwire, SNORT, NESSUS**