

Audit et analyse des réseaux

Cours Synthèse de 2 jours - 14h

Réf : AUR - Prix 2024 : 1 950CHF HT

Le trafic sur les réseaux de données est composé de nombreuses applications dont les volumes sont en général inversement proportionnels à l'importance qu'ils revêtent pour l'entreprise. Ce cours se propose de donner les clés, techniques et pratiques, de l'analyse des réseaux.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

- Comprendre l'art d'analyser les flux réseau
- Connaitre les impacts de métrologie active et passive
- Identifier les outils utiles à la gestion du trafic
- Appréhender les méthodes d'audit appliquées à la sécurité
- Identifier les outils utiles pour surveiller la Qos

LE PROGRAMME

dernière mise à jour : 05/2021

1) Les architectures de réseaux

- Rappels sur les architectures de protocoles.
- Le réseau d'entreprise, les réseaux virtuels, les techniques de VPN. Le réseau longue distance, les services des ISP.
- Les réseaux d'accès : xDSL, fibre, WiFi, WiMax, 4G/5G.
- Les paramètres clés du réseau. Notion d'échantillonnage, problématiques de la mesure.
- Les débits, valeurs moyennes, rafales. Le nombre de paquets par seconde (PPS).
- L'analyse des goulets d'étranglement.

2) La métrologie

- Métrologie active vs métrologie passive.
- Métrologie : l'impact des couches du modèle en couches.
- Les approches purement réseau (niveau 2-3-4).
- Les approches applicatives (niveau 7).
- L'impact applicatif sur le réseau.
- Les groupes de l'IETF : IPSAMP, IPPM, IPFIX. Pourquoi tant d'efforts différents ?
- Les approches SNMP.
- Les corrélations statistiques.

3) La gestion du trafic

- Les outils. Les méthodes de contrôle d'admission.
- Impact des technologies sur les comportements.
- Capacity planning. Prévoir les évolutions. Garantir les performances.
- Des outils pour la gestion de parcs informatiques. Analyse des systèmes d'exploitation.
- Analyse des applications. Découverte de topologies.

4) La sécurité

- Les principes de sécurité liés au trafic : les firewalls.

PARTICIPANTS

Ce cours s'adresse aux architectes de réseaux, aux chefs de projets, aux responsables de systèmes d'information, aux ingénieurs réseaux.

PRÉREQUIS

Connaissances de base dans le domaine des réseaux.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Les différents types de filtrages : Stateful, Stateless et applicatif (proxy ou proxying applicatif).
- Les limites des systèmes actuels.
- La détection d'intrusion : un audit en temps réel.
- La conformité du trafic aux règles du firewall.

5) La méthodologie

- Les étapes importantes.
- Pourquoi une méthodologie ?
- L'audit permanent.

6) La qualité de service

- Notions de SLA. QoS vs CoS.
- Le modèle de bout en bout.

7) Les outils d'audit et de Qos

- Les audits ponctuels. Pour quoi faire ? Exemple.
- Les performances et l'impact financier.
- Analyseurs, systèmes de gestion, le traffic shaping (régulation de flux), un état du marché.
- Les outils : PRTG, Wireshark/TCPdump...
- Qosmos. Qosmetrix. NetFlow, Ntop...
- Bilan et comparaison synthétique.

LES DATES

CLASSE À DISTANCE
2024 : 04 juil., 17 oct., 19 déc.