Azurtem
15 Rue du Maréchal Joffre, FR-06000 NICE +33.(0)6.88.20.00.04
https://shop.azurtem.com / shop@azurtem.com

*Déclaration d'activité enregistrée sous le numéro **93060803406** auprès du préfet de région de Provence Alpes Côte d'Azur*

Stage de formation

Mikrotik Certified Network Associate (MTCSE)

Durée	2 jours (9h-12h30 et 13h30-17h)
Modalités et délais d'accès	Le programme de formation chez Mikrotik est déjà établi; que l'on soit en situation intra ou inter-entreprise le contenu de la formation sera identique. L'inscription peut avoir lieu jusque une semaine avant le démarrage de la session sous réserve de places disponibles. Les inscriptions et la planification de la session seront confirmées auprès du client dès la réception du devis accepté par celui-ci.
Tarifs	Le coût forfaitaire par personne et par session s'élève à 920€ H.T. Dans le cas d'une session se déroulant au sein de l'entreprise de l'apprenant.e, des frais supplémentaires liés au déplacement et à l'hébergement du formateur viendront s'ajouter à ce coût forfaitaire. Une session assurée en intra-muros se calcul sur une base de quatre pax.
Public visé	Ingénieurs et techniciens réseau souhaitant déployer et maintenir des réseaux sécurisés basés sur des équipements MikroTik.
Accessibilité et aménagements	En cas de présence d'un.e ou plusieurs apprenant.e.s handicapé.e.s, et ce quel que soit le lieu de la formation, nous tenterons de déterminer ensemble les aménagements et dispositions spécifiques qui seront nécessaires lors de la formation. Référent handicap Azurtem: Yann SHUKOR [training@azurtem.com / +33(0)6.88.20.00.04]
Prérequis	L'apprenant.e doit avoir une bonne compréhension du jeu de protocoles TCP/IP et pour se certifier doit avoir obtenu au préalable le certificat MTCNA.
Equipement nécessaire	Un ordinateur portable équipé d'interfaces Ethernet et Wifi capable d'exécuter des applicatifs sous Windows
Objectif	À la fin de cette session de formation, l'apprenant.e sera capable de planifier et de mettre en œuvre les mesures de sécurité appropriées pour sécuriser un réseau.
Formateur et Contact formation	Consultant/formateur Mikrotik: Yann Shukor [training@azurtem.com / +33(0)6.88.20.00.04] Certifié: MTCNA, MTCSWE, MTCRE, MTCWE, MTCINE, MTCWE, MTCIPv6E, MTCSE

Modalités pédagogiques	La formation alterne entre apports théoriques et pratiques. Le formateur dispense la partie théorique accompagnée de diapositives affichées sur un grand écran. L'apprenant.e aura à sa disposition un routeur qui servira lors des nombreux travaux pratiques de mises en situations ; individuelles et en groupes. Le formateur profitera de ces exercices de mises en pratiques pour s'assurer que chaque apprenant.e a bien assimilé le contenu du chapitre en cours de présentation.
Éléments remis à l'apprenant.e	L'apprenant.e recevra dès le début de la session une copie électronique du support de cours (PDF).
Modalité d'évaluation initiale	Une invitation est transmise en amont aux apprenant.e.s afin de recueillir les sujets qui pourraient requérir davantage d'attention lors du déroulement de la session. Avant la session l'apprenant.e pourra tester ses connaissances réseaux à l'aide du test d'évaluation mis à disposition par Mikrotik : https://mikrotik.com/client/example_test
Quiz du matin	Tous les matins l'apprenant.e devra répondre à une quinzaine de questions, proposées lors du quiz du matin, à propos des sujets couverts la veille. Cela permettra de revenir sur certains sujets mal compris voire d'insister sur quelques points importants.
Modalité d'évaluation finale	Le dernier jour, à la fin de la session de formation, aura lieu l'examen de certification. Chaque apprenant.e aura une heure pour répondre à vingt-cinq questions (EN/FR). Pour être certifié il faudra obtenir au minimum soixante pour cent de bonnes réponses.
Niveau de satisfaction et taux de réussite	Nous tentons de recueillir l'avis des apprenants suite à chaque session de formation : [avis]. Un indicateur de réussite est également affiché, et maintenu, sur le site de chez Mikrotik : https://mikrotik.com/training/centers/europe/france

Matinée (amX)

Après-midi (pmX)

Titre	Objectif
Module 1 Introduction *(am1)*	• Attaques, mécanismes et services • Les menaces les plus courantes • Déploiement de la sécurité RouterOS • **Module 1 labo**
Module 2 Parefeu *(am1)*	• Flux de paquets, chaînes de pare-feu • Pare-feu dynamique • Table RAW • Atténuation des inondations SYN à l'aide de la table RAW • Configuration par défaut de RouterOS • Meilleures pratiques pour l'accès de gestion • Détection d'attaques contre des services réseaux critiques • Filtres du pont • Options avancées des filtres du pare-feu • Filtrage ICMP • **Module 2 labo**
Module 3 Attaques des couches OSI *(pm1)*	• Attaques MNDP et prévention • DHCP : serveurs 'rogue', attaques d'épuisement et prévention • Attaques TCP SYN et prévention • Attaques UDP et prévention • Attaques "Smurf ICMP" et prévention • Attaques FTP, Telnet et brute-force SSH et prévention • Détection et prévention du balayage des ports • **Module 3 labo**

Module 4
Chiffrement
(am2)
	• Introduction au chiffrement et à la terminologie
	• Méthodes de chiffrement
	• Algorithmes - symétrique, asymétrique
	• Infrastructure à clé publique (PKI)
	• Certificats
	  ◦ Certificats auto-signés
	  ◦ Certificats valides et gratuits
	  ◦ Utilisation des certificats dans RouterOS
	• **Module 4 labo**

Module 5 Sécurisation du Routeur *(pm2)*	• Port knocking • Connexions sécurisées (HTTPS, SSH, WinBox) • Ports par défaut des services • Construction d'un tunnel au travers de SSH • **Module 5 labo**

Module 6 Tunnels Sécurisés *(pm2)*	• Introduction à IPsec • L2TP + IPsec • SSTP avec certificats • **Module 6 labo**

-=oOo=-