CISCO

CCNA SECURITY

DESCRIPTION DU COURS

Cisco Certified Network Associate Security (CCNA® Security) valide les connaissances et les acquis, nécessaires à la sécurisation des réseaux Cisco. Avec une certification sécurité CCNA, un professionnel du réseau démontre qu'il détient les compétences requises pour développer une infrastructure de sécurité, reconnaître les menaces et les vulnérabilités des réseaux et atténuer les menaces de sécurité. Le cursus sécurité CCNA met l'accent sur les principales technologies de sécurité, l'installation, le dépannage et la surveillance des périphériques réseau afin de maintenir l'intégrité, la confidentialité et la disponibilité des données et des périphériques, ainsi que sur les compétences des technologies utilisées par Cisco dans sa structure de sécurité.

CCNA Security prépare les participants au monde du travail et à la certification Cisco CCNA Security reconnue dans le monde entier. En outre, la National Security Agency (NSA, Agence de sécurité nationale américaine) et le Commitee on National Security Systems (CNSS, Comité américain des systèmes de sécurité nationale) valident la conformité aux normes de formation CNSS 4011 de la certification Cisco CCNA Security.

DEROULEMENT DE LA FORMATION

- **Période : Du 18 Janvier au 13 Avril 2019**
- **Durée**
  - ✓ **3 Mois**
  - ✓ **2 jours / Semaine (Vendredi et Samedi)**
  - ✓ **3H / Jour**
  - ✓ **6H / Semaine**
  - ✓ **Cours du Soir : 18h30 – 21h30**
- **Langue**
  - **Cours avec instructeur : FRANCAIS**
  - **Support sur la plateforme CISCO : ANGLAIS**
  - **Tests et examens sur la plateforme CISCO : ANGLAIS**

CONTENU

CHAPTER 1: MODERNS NETWORK SECURITY THREATS

- Securing Networks
- Network Threats
- Mitigating Threats

CHAPTER2: SECURING NETWORK DEVICES

- Securing Device Access
- Assigning Administrative Roles
- Monitoring and Managing Devices
- Using Automated Security Features
- Securing the control plane

CHAPTER 3: AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

- Purpose of AAA Authentication
- Server-Based AAA
- Server-Based AAA Authentication
- Server-Based AAA Authorization and Accounting

CHAPTER 4: IMPLEMENTING FIREWALL TECHNOLOGIES

- Access Control Lists
- Firewall Technologies
- Zone-Based Policy Firewall

CHAPTER 5 : IMPLEMENTING INTRUSION PREVENTION

- IPS Technologies
- IPS Signatures
- Implement IPS

CHAPTER 6 : SECURING THE LOCAL AREA NETWORK

- Endpoints Security
- Layer 2 Security Considerations

CHAPTER 7 : CRYPTOGRAPHIC SYSTEMS

- Cryptographic Services
- Basic Integrity and Authenticity
- Confidentiality
- Public Key Cryptography

CHAPTER 8 : IMPLEMENTING VIRTUAL PRIVATE NETWORKS

- VPNs
- IPsec VPN Components and Operation
- Implementing Site-to-Site IPsec VPN with CLI

CHAPTER 9 : IMPLEMENTING THE CISCO ADAPTIVE SECURITY APPLIANCE

- Introduction to the ASA
- ASA Firewall Configuration

CHAPTER 10: ADVANCED CISCO ADAPTIVE SECURITY APPLIANCE

- ASA Security Device Manager
- ASA VPN Configuration

CHAPTER 11: MANAGING A SECURE NETWORK

- Network Security Testing
- Developing a Comprehensive Security Policy

MATERIELS DE TRAVAUX PRATIQUE :

Matériels **CISCO**

Pour tout autre renseignement veuillez contacter le **25380845 / 60502222** ou par mail à **info@isisec.net**.

Une attestation est délivrée à la fin de la formation en cas de validation.

Personne responsable :

MOUMOUNI ABOU Mahaman Laoual
62 10 68 67
77 09 30 55 (Whatsapp)