FORMATION RÉUSSIR LA CERTIFICATION FORTINET NSE4 FORTIGATE SECURITY & INFRASTRUCTURE

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Sécurité défensive

Rubrique : SOC (Security Operations Center)

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Vous former dans un centre de formation agréé Fortinet vous assure le meilleur niveau de maîtrise de vos équipements Fortinet.

Public visé

Toute personne qui doit administrer régulièrement un firewall Fortigate.

Pré-requis

Notions TCP/IP et des connaissances des concepts firewall.

PROGRAMME

A l'issue de cette session de trois jours

Vous serez en mesure de : - décrire les fonctionnalités des UTM du FortiGate,
- neutraliser les menaces véhiculées au travers des malwares, les applications nocives et limiter les accès aux sites inappropriés,
- contrôler les accès au réseau selon les types de périphériques utilisés,
- authentifier les utilisateurs au travers du portail captif personnalisable,
- mettre en œuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise,
- mettre en œuvre un VPN IPsec pour l'accès des utilisateurs nomades au réseau de l'entreprise,
- appliquer de la PAT, de la source NAT et de la destination NAT,
- interpréter les logs et générer des rapports - utiliser la GUI et la CLI,
- mettre en œuvre la protection anti-intrusion,
- maîtriser l'utilisation des applications au sein de votre réseau…

A l'issue de cette session de deux jours

vous serez en mesure de : - configurer de la SD-Wan,
- monitorer le statut de chaque lien de la SD-Wan
- configurer de la répartition de charge au sein de la SDWan
- déployer un cluster de FortiGate,
- inspecter et sécuriser le trafic réseau sans impacter le routage,
- analyser la table de routage d'un FortiGate,
- diviser un FortiGate physique en plusieurs FortiGates virtuels indépendants, via la mise en œuvre des Virtual Domains,
- étudier et choisir une architecture de VPN IPsec
- comparer les VPN IPsec en mode Interface (routebased) ou Tunnel (Policy-based)
- implémenter une architecture de VPN IPSec redondée,
- troubleshooter et diagnostiquer des problématiques simples sur le FortiGate,
- mettre en œuvre l'identification utilisateur ou l'authentification transparente dans les environnements Active Directory…

Code de formation : SP78033

€ Tarifs

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Campus : Ensemble des sites

Durée : 35 heures

Délai d'accès :
Jusqu'à 8 jours avant le début de la formation

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 18 / 11 / 2024
: Ensemble des sites
: Distanciel possible
: 35 heures
: 5 jours

- 09 / 12 / 2024
: Ensemble des sites
: Distanciel possible
: 35 heures
: 5 jours

MODALITÉS

Modalités

Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.