

Configuring F5 Advanced WAF (Web Application Firewall)

Référence : **SEC-F5AWAF**

Durée : **4 jours**

Certification : **Aucune**

CONNAISSANCES PREALABLES

- 1-Connaître la suite de produits F5 BIG-IP et, en particulier, les procédures de paramétrage et de configuration d'un système BIG-IP LTM, y compris concernant les serveurs virtuels, les pools, les profils, les réseaux VLAN et les adresses « self-IP ».
- 2-Il est vivement conseillé aux personnes qui ne connaissent pas le système BIG-IP de suivre la formation « Administering BIG-IP » au préalable.

PROFIL DES STAGIAIRES

- Administrateurs réseaux et sécurité chargés de l'installation et de la maintenance quotidienne du module Application Security Manager.

OBJECTIFS

- Être capable de configurer le mode de protection le plus adapté à leurs applications Web.
- Être capable de différencier les modèles de sécurité négative des modèles de sécurité positive.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Paramétrage du système BIG-IP

Traitement du trafic à l'aide du module Local Traffic Manager (LTM)

Concepts liés aux applications Web

Vulnérabilités liées aux applications Web

Déploiement des politiques de sécurité

Signatures des attaques

Mise en place d'une sécurité positive

Cookies et autres en-têtes

Génération de rapports

Rôles utilisateur et administration

Gestion avancée des paramètres

Modèles d'application

Outil Real Traffic Policy Builder

Analyseurs de vulnérabilités

Saisie obligatoire des informations de connexion et suivi de sessions

Détection d'anomalies

ASM et iRules

Prise en charge des formats AJAX et JSON

Prise en charge du format XML et des services Web

Notre **référént handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.