

Configuring F5 Advanced WAF

Réf. BIG-WAF · F5 · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
4 jours	Avancé	Présentiel · Live · Intra	Inclus

Présentation

Ce cours F5 officiel apprend à déployer, configurer et administrer F5 Advanced WAF (anciennement BIG-IP ASM) pour sécuriser les applications web. Les participants construisent des politiques de sécurité, se défendent contre les attaques OWASP Top 10, les bots et les attaques DoS applicatives. Il prépare aux fonctions de sécurité applicative et à la certification F5.

Objectifs pédagogiques

- Déployer F5 Advanced WAF et comprendre son architecture de traitement du trafic
- Construire et affiner des politiques de sécurité applicatives
- Se protéger contre les attaques OWASP Top 10 et les injections
- Configurer la défense anti-bots et l'atténuation des DoS L7
- Mettre en œuvre le blindage des identifiants et la protection contre le brute-force
- Exploiter le logging, le reporting et le réglage des faux positifs

Programme détaillé

1. Module 1 — Provisionnement et traitement du trafic

- Architecture BIG-IP et provisionnement Advanced WAF
- Concepts de proxy et de virtual servers
- Flux de traitement des requêtes HTTP
- Configuration réseau initiale

2. Module 2 — Politiques de sécurité applicatives

- Déploiement rapide et modèles de politiques
- Signatures d'attaque et mise à jour
- Apprentissage automatique et affinage des politiques
- Gestion des faux positifs

3. Module 3 — Défense contre les attaques web

- Protection OWASP Top 10 (injections, XSS...)
- Blindage des paramètres, URL et cookies
- Protection des identifiants et anti-brute-force
- DataSafe et chiffrement côté client

4. Module 4 — Bots, DoS et supervision

- Défense anti-bots (Bot Defense)
- Atténuation des attaques DoS applicatives (L7)
- Logging, événements et reporting
- Bonnes pratiques d'exploitation et de maintenance

Prérequis

Avoir suivi le cours Administering BIG-IP ou disposer d'une expérience équivalente, ainsi que des connaissances HTTP/HTML et de sécurité web. La connaissance de BIG-IP LTM est un atout.

Public visé

Administrateurs sécurité, ingénieurs réseau et sécurité applicative, administrateurs F5 et responsables de la protection des applications web.

Ce qui est inclus

- Support de cours officiel F5
- Labs sur environnement BIG-IP dédié
- Exercices de construction de politiques WAF
- Attestation de fin de formation et préparation à la certification F5
- Pauses et déjeuner inclus

Certification

Cours préparant à la certification F5 Certified Technology Specialist (ASM/Advanced WAF), examen 303 délivré via Pearson VUE. Advancia Training est centre d'examen agréé Pearson VUE.

1 500 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible