F5 Configuration BIG-IP Advanced Web Application Firewall (AWAF)

Durée: 4 Jours **Réf de cours: AWAF** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Ce cours de 4 jours permet aux étudiants d'acquérir une compréhension fonctionnelle du déploiement, du réglage et de l'utilisation de F5 Advanced Web Application Firewall pour protéger leurs applications web des attaques basées sur le protocole HTTP.
Le cours comprend des parties magistrales, des travaux pratiques et des discussions sur les différents outils de F5 Advanced Web Application Firewall pour la détection et l'atténuation des menaces provenant de multiples vecteurs d'attaque tels que le web scraping, le déni de service de la couche 7, la force brute, les bots, l'injection de code et les exploits de type "zero day".
Mis à jour 14/01/2025

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Ce cours est destiné au personnel SecOps responsable du déploiement, du réglage et de la maintenance quotidienne de F5 Advanced WAF.

Objectifs pédagogiques:

- Les participants obtiendront un niveau fonctionnel d'expertise avec F5 Advanced WAF, y compris la configuration complète de la politique de sécurité et du profil, l'évaluation du client et les types d'atténuation appropriés.
- A l'issue de cette formation, les participants seront en mesure de :
- Décrire le rôle du système BIG-IP en tant que proxy complet dans un réseau de distribution d'applications
- Dimensionner le F5 Advanced Web Application Firewall
- Définir un pare-feu d'application Web
- Décrire comment F5 Advanced Web Application Firewall protège une application web en sécurisant les types de fichiers, les URL et les paramètres
- Déployer F5 Advanced Web Application Firewall à l'aide du modèle de déploiement rapide (et d'autres modèles) et définir les contrôles de sécurité inclus dans chacun d'eux
- Définir les paramètres d'apprentissage, d'alarme et de blocage dans le cadre de la configuration de F5 Advanced Web Application Firewall
- Définir les signatures d'attaque et expliquer pourquoi la mise en scène des signatures d'attaque est importante
- Déployer des campagnes de lutte contre les menaces pour se protéger contre les menaces CVE
- Contraster la mise en oeuvre de politiques de sécurité positives et négatives et expliquer les avantages de chacune d'entre elles
- Configurer le traitement de la sécurité au niveau des paramètres d'une application Web
- Déployer F5 Advanced Web Application Firewall à l'aide de l'éditeur de politique automatique
- Ajuster une politique manuellement ou permettre l'élaboration automatique d'une politique
- Intégrer les résultats d'un scanner de vulnérabilité d'application tiers dans une politique de sécurité
- Configurer l'application de la connexion pour le contrôle du flux
- Atténuer le bourrage d'informations d'identification (credential stuffing)
- Configurer la protection contre les attaques par force brute
- Déploiement d'une défense avancée contre les robots racleurs de sites web, tous les robots connus et d'autres agents automatisés
- Déployer DataSafe pour sécuriser les données côté client

Pré-requis:

Il n'y a pas de pré-requis spécifique à la technologie F5 pour ce cours. Cependant, il serait très utile pour les étudiants ayant une expérience limitée de l'administration et de la configuration de BIG-IP d'avoir les connaissances équivalentes à la formation Administration BIG-IP ou la Certification F5 Certified BIG-IP Administrator I

Il est recommandé d'avoir les connaissances et l'expérience générales suivantes en matière de technologie de réseau :

- OSI model encapsulation
- Routing and switching
- Ethernet and ARP
- TCP/IP concepts
- IP addressing and subnetting
- NAT and private IP addressing 3
- Default gateway
- Network firewalls
- LAN vs. WAN
- Une expérience avec LTM n'est pas nécessaire.
- Une connaissance préalable du WAF n'est pas requise.

Contenu:

- Chapter 1: Setting Up the BIG-IP System
- Chapter 2: Traffic Processing with BIG-IP
- Chapter 3: Web Application Concepts
- Chapter 4: Web Application Vulnerabilities
- Chapter 5: Security Policy Deployment
- Chapter 6: Policy Tuning and Violations
- Chapter 7: Attack Signatures and Threat Campaigns
- Chapter 8: Positive Security Policy Building
- Chapter 9: Securing Cookies and Other Headers
- Chapter 10: Visual Reporting and Logging
- Chapter 11: Lab Project 1
- Chapter 12: Advanced Parameter Handling
- Chapter 13: Automatic Policy Building
- Chapter 14: Web Application Vulnerability Scanner Integration
- Chapter 15: Deploying Layered Policies
- Chapter 16: Login Enforcement and Brute Force Mitigation
- Chapter 17: Reconnaissance with Session Tracking
- Chapter 18: Layer 7 DoS Mitigation
- Chapter 19: Advanced Bot Defense
- Chapter 20: Form Encryption using DataSafe
- Chapter 21: Review and Final Labs

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.
Le cours de formation autodirigée (SDT) gratuit suivant, bien que facultatif, est utile pour tout étudiant ayant une expérience limitée de l'administration et de la configuration de BIG-IP : Commencer avec BIG-IP

Ce module est disponible gratuitement et en anglais sur le site Exclusive Network France via ce lien F5 Training Programs and Online Classes | F5

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.