# F5 BIG-IP : configuration avancée WAF

*Lien : https://innov-systems.com/formation/f5-big-ip-configuration-avancee-waf*

| DURÉE | RÉFÉRENCE | CATÉGORIE |
| --- | --- | --- |
| **5 jours (35h)** | **RST167** | **F5 Networks** |

## OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Etre capable de différencier les modèles de sécurité négative des modèles de sécurité positive
- Configurer le mode de protection le plus adapté à leurs applications Web

## POUR QUI ?

- Administrateurs réseaux et sécurité

## Programme détaillé

### 1 / Présentation du système BIG-IP

- Découvrir les produits et les ressources F5 Networks
- Vue d'ensemble du système BIG-IP

### 2 / Paramétrage du système BIG-IP

- Configuration de base du système
- Archiver la configuration du système BIG-IP
- Utiliser les ressources et outils de support F5

### 3 / Traiter le trafic avec BIG-IP

- Les objets de traitement de trafic BIG-IP
- Appréhender les profils
- Vue d'ensemble des stratégies de trafic local
- Afficher le flux de requêtes HTTP

### 4 / Concepts liés aux applications Web

- Vue d'ensemble du traitement des demandes d'application Web
- FireWall d'application Web
- Contrôles de sécurité de la couche 7
- Présentation des éléments de communication Web
- Présentation de la structure de requêtes HTTP
- Examen des réponses HTTP
- Analyse des types de fichiers, des URL et des paramètres
- Utiliser le proxy HTTP Fiddler

### 5 / Vulnérabilités liées aux applications Web

- Une taxonomie des attaques : le paysage des menaces
- Exploits communs contre les applications Web

### 6 / Déployer des politiques de sécurité

- Vue d'ensemble de modèles de sécurité positifs et négatifs
- Le workflow de déploiement
- Attribution d'une stratégie au serveur virtuel
- Utiliser les paramètres avancés du Workflow de déploiement
- Configuration des technologies de serveur

### 7 / Les signatures d'attaque

- Afficher les demandes
- Contrôles de sécurité proposés par le déploiement rapide
- Définir les signatures d'attaque

### 8 / Réglage des stratégies et infractions

- Traiter le trafic post-déploiement
- Comment les infractions sont catégorisées
- Taux d'infraction : échelle de menace
- Définition de la mise en scène et l'application
- Définition du mode d'application
- Définition de la période de préparation à l'application
- Revue de la définition de l'apprentissage
- Définition des suggestions d'apprentissage
- L'apprentissage automatique ou manuel
- Les paramètres d'apprentissage, d'alarme et de blocage
- Interprétation du résumé de l'état de préparation à l'application
- Configurer la page de réponse de blocage

## 9 / Signatures des attaques

- Présentation des signatures d'attaque
- Vue d'ensemble des bases de la signature d'attaque
- Créer les signatures d'attaque définies par l'utilisateur
- Les modes d'édition simples et avancés
- Les ensembles de signature d'attaque
- Les pools de signature d'attaque
- Les signatures d'attaques et la mise en scène des attaques
- Mettre à jour les signatures d'attaque
- Définir les campagnes contre les menaces
- Déployer les campagnes contre les menaces

## 10 / Mise en place d’une sécurité positive

- Les composants de stratégie de sécurité
- Le joker (Wildcard)
- Le cycle de vie de l'entité
- Choix du programme d'apprentissage
- Affichage des suggestions d'apprentissage et de l'état d'avancement
- Score d'apprentissage
- Adresses IP approuvées et non approuvées
- Compact

## 11 / Cookies et autres en-têtes

- Le but des cookies WAF avancés F5
- Les cookies autorisés et appliqués
- Sécuriser les en-têtes HTTP

## 12 / Génération de rapports

- Affichage des données récapitulatives de sécurité des applications

- Rapports : créer votre propre vue
- Rapports : graphique basé sur des filtres
- Statistiques sur la force brute et le Web Scraping
- Affichage des rapports de ressources
- Conformité PCI : PCI-DSS 3.0
- Analyse des demandes
- La journalisation locale
- Afficher les journaux dans l'utilitaire de configuration
- Définir le profil de journalisation
- Configurer la journalisation des réponses

## 13 / Gestion avancée des paramètres

- Les types de paramètres
- L paramètres statiques
- Les paramètres dynamiques
- Les niveaux de paramètres
- Autres considérations relatives aux paramètres

## 14 / Élaboration automatique de stratégies

- Aperçu de l'élaboration automatique de stratégies
- Les modèles qui automatisent l'apprentissage
- Le relâchement des stratégies
- Le resserrement des stratégies
- La vitesse d'apprentissage : échantillonnage du trafic
- Les modifications du site de suivi

## 15 / Intégration du scanner de vulnérabilité d'applications web

- Intégrer la sortie du scanner
- Import des vulnérabilités

- Résoudre les vulnérabilités
- Fichier XSD du scanner XML générique

## 16 / Stratégies en couches

- Stratégie parent
- L'héritage
- Cas du déploiement

## 17 / La connexion et atténuation de la force brute

- Les pages de connexion pour le contrôle de flux
- Configurer la détection automatique des pages de connexion
- Les attaques par force brute
- Configurer la protection de la force brute
- Atténuer la force brute basée sur la source
- Remplissage des informations d'identification
- Atténuation du remplissage des informations d'identification

## 18 / Suivi de session

- Définition du suivi de session
- Configurer les actions en cas de détection de violation

## 19 / Atténuation DoS de la couche 7

- Les attaques par déni de service
- Le profil de protection DoS
- La protection DoS basée sur TPS
- Créer un profil de journalisation DoS
- Application des atténuations TPS
- La détection comportementale et basée sur le stress

### 20 / Bots defense avancés

- Classifier les clients avec le profil Bot Defense
- Les signatures de bot
- L'empreinte digitale F5
- Les modèles de profil Bot Defense
- La protection des micro-services

### 21 / Chiffrement de formulaire à l'aide de DataSafe

- Ciblage des éléments de la livraison d'applications
- Exploitation du modèle d'objet de document
- Protection des applications à l'aide de DataSafe
- L'ordre des opérations pour la classification des URL

## Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

## Prochaines dates programmées

| | |
|---|---|
| 17 au 21 Août 2026 | Distanciel |
| 12 au 16 Oct. 2026 | Distanciel |

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.



**Réservation & Renseignements**

**Téléphone :** +212 522 247 210
**Email :** contact@innov-systems.com
**Web :** https//www.innov-systems.com