Formation Configuring F5 Advanced WAF

(previously licensed as ASM)

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Le cours BIG-IP Application Security Manager (4 jours) offre aux participants une compréhension fonctionnelle de la procédure de déploiement, de réglage et d'utilisation du gestionnaire ASM (BIG-IP Application Security Manager) afin de protéger leurs applications Web contre les attaques HTTP.
Le cours comprend des conférences, des travaux pratiques et des discussions sur différents composants ASM permettant de détecter et d'atténuer les menaces provenant de plusieurs vecteurs d'attaque tels que le grattage de la toile, le déni de service de couche 7, la force brute, les bots, l'injection de code et les exploits zero day.

Référence	F5N-BIG-AWF-CFG
Durée	4 jours (28h)
Tarif	3 800 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 21 au 24 mai 2024*
du 24 au 27 juin 2024
du 2 au 5 septembre 2024
du 28 au 31 octobre 2024
du 12 au 15 novembre 2024
du 17 au 20 décembre 2024

VOIR TOUTES LES DATES

(*) session confirmée

Objectifs

| Décrire le rôle du système BIG-IP en tant que périphérique proxy complet
| Définir un pare-feu d'application Web
| Déployer le pare-feu et définir les contrôles de sécurité
| Définir les paramètres d'apprentissage, d'alarme et de blocage
| Définir les signatures d'attaque
| Déployer des campagnes de menaces pour se protéger contre les menaces CVE
| Comparer la mise en oeuvre des politiques de sécurité positives et négatives
| Configurer le traitement de la sécurité au niveau des paramètres d'une application Web
| Déployer le pare-feu à l'aide du générateur de politique automatique
| Régler une politique manuelle ou automatique
| Intégrer la sortie du scanner de vulnérabilité des applications tierces dans une politique de sécurité
| Configurer l'application de la connexion pour le contrôle de flux
| Limiter le credential stuffing
| Configurer la protection contre les attaques par force brute
| Déployer Advanced Bot Defense contre les scrapers Web, tous les bots connus et autres agents automatisés

Public

| tout étudiant ayant une expérience limitée de l'administration et de la configuration BIG-IP

Prérequis

| Il est recommandé de posséder des connaissances générales en réseau suivantes :
| Encapsulation du modèle OSI
| Routage et commutation
| Ethernet et ARP
| Notions TCP/IP
| Adressage IP et sous-réseaux
| NAT et adressage IP privé
| Passerelle par défaut
| Pare-feu réseau
| LAN vs WAN

Programme de la formation

Traitement du trafic avec le gestionnaire de trafic local BIG-IP (LTM)
| Identifying BIG-IP Traffic Processing Objects
| Understanding Profiles
| Overview of Local Traffic Policies
| Visualizing the HTTP Request Flow

Concepts d'application Web
| Web Application Firewall: Layer 7 Protection
| Layer 7 Security Checks
| Overview of Web Communication Elements
| Overview of the HTTP Request Structure
| Examining HTTP Responses
| How F5 Advanced WAF Parses File Types, URLs, and Parameters
| Using the Fiddler HTTP Proxy

Vulnérabilités des applications Web
| A Taxonomy of Attacks: The Threat Landscape
| Common Exploits Against Web Applications

Déploiement de la politique de sécurité Réglage de la politique de sécurité
| Defining Learning
| Comparing Positive and Negative Security Models
| The Deployment Workflow
| Assigning Policy to Virtual Server
| Deployment Workflow: Using Advanced Settings
| Configure Server Technologies
| Defining Attack Signatures
| Viewing Requests
| Security Checks Offered by Rapid Deployment
| Post-Deployment Traffic Processing
| How Violations are Categorized
| Violation Rating: A Threat Scale
| Defining Staging and Enforcement
| Defining Enforcement Mode
| Defining the Enforcement Readiness Period
| Reviewing the Definition of Learning
| Defining Learning Suggestions
| Choosing Automatic or Manual Learning
| Defining the Learn, Alarm and Block Settings
| Interpreting the Enforcement Readiness Summary
| Configuring the Blocking Response Page

Signatures d'attaque
| Defining Attack Signatures
| Attack Signature Basics
| Creating User-Defined Attack Signatures
| Defining Simple and Advanced Edit Modes
| Defining Attack Signature Sets
| Defining Attack Signature Pools
| Understanding Attack Signatures and Staging
| Updating Attack Signatures
| Defining Threat Campaigns
| Deploying Threat Campaigns

Le renforcement de la sécurité positive
| Defining and Learning Security Policy Components
| Defining the Wildcard
| Defining the Entity Lifecycle
| Choosing the Learning Scheme
| How to Learn: Never (Wildcard Only)
| How to Learn: Always
| How to Learn: Selective

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Reviewing the Enforcement Readiness Period: Entities
| Viewing Learning Suggestions and Staging Status
| Defining the Learning Score
| Defining Trusted and Untrusted IP Addresses
| How to Learn: Compact

Sécurisation des cookies et autres en-têtes
| The Purpose of F5 Advanced WAF Cookies
| Defining Allowed and Enforced Cookies
| Securing HTTP headers

Reporting et journalisation
| Viewing Application Security Summary Data
| Reporting: Build Your Own View
| Reporting: Chart based on filters
| Brute Force and Web Scraping Statistics
| Viewing Resource Reports
| PCI Compliance: PCI-DSS 3.0
| Analyzing Requests
| Local Logging Facilities and Destinations
| Viewing Logs in the Configuration Utility
| Defining the Logging Profile
| Configuring Response Logging

Rôles d'utilisateur
Modification, fusion et exportation de règles
Gestion avancée des paramètres
| Defining Parameter Types
| Defining Static Parameters
| Defining Dynamic Parameters
| Defining Parameter Levels
| Other Parameter Considerations

Utilisation de modèles d'application
| Defining Templates Which Automate Learning
| Defining Policy Loosening
| Defining Policy Tightening
| Defining Learning Speed: Traffic Sampling
| Defining Track Site Changes

Utilisation du générateur de règles automatique
Intégration aux scanners de vulnérabilité Web
| Integrating Scanner Output
| Importing Vulnerabilities
| Resolving Vulnerabilities
| Using the Generic XML Scanner XSD file

Application de la connexion et suivi de session
| Defining Login Pages for Flow Control
| Configuring Automatic Detection of Login Pages
| Defining Brute Force Attacks
| Brute Force Protection Configuration
| Source-Based Brute Force Mitigations
| Defining Credential Stuffing
| Mitigating Credential Stuffing

Détection et atténuation du Web scraping
Suivi de session
| Defining Session Tracking
| Configuring Actions Upon Violation Detection

Application de la géolocalisation et exceptions d'adresse IP
Protection DoS de couche 7
| Defining Denial of Service Attacks

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Defining the DoS Protection Profile
| Overview of TPS-based DoS Protection
| Creating a DoS Logging Profile
| Applying TPS Mitigations
| Defining Behavioral and Stress-Based Detection

ASM et iRules
Utilisation de profils de contenu pour les applications AJAX et JSON
Bot avancée de détection et de défense - Bot défense proactive - Mode d'édition simple pour les signatures d'attaque
| Classifying Clients with the Bot Defense Profile
| Defining Bot Signatures
| Defining F5 Fingerprinting
| Defining Bot Defense Profile Templates
| Defining Microservices protection

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785