+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 06/09/2024

S'inscrire

Formation FortiWeb de Fortinet (NSE6)

3 jours (21 heures)

Présentation

Les applications Web non protégées constituent une passerelle d'entrée pour les hackers et les attaques. L'approche multicouche et corrélée de FortiWeb protège vos applications Web contre de nombreuses vulnérabilités et notamment celles du Top 10 OWASP. Lorsque associé au service de sécurité des applications web des FortiGuard Labs, vous êtes protégé contre les vulnérabilités applicatives, bots et URL malveillantes. Nos deux moteurs de détection heuristique sécurisent vos applications contre des menaces évoluées telles que l'injection SQL, le cross-site scripting, le dépassement de tampon, le cookie poisonning, les sources malveillantes et les attaques de déni de service.

Dans cette formation d'une durée de trois jours, vous apprendrez à déployer, à configurer et à dépanner le pare-feu d'application Web de Fortinet : FortiWeb.Les formateurs vous présenteront les concepts-clés liés à la sécurisation des applications web. Ils vous proposeront des exercices en laboratoire, vous permettant d'explorer les fonctionnalités de protection et de performances de FortiWeb.Vous travaillerez sur des simulations d'attaques utilisant des applications web réelles. À partir de simulations du trafic, vous apprendrez à répartir la charge des serveurs virtuels sur les serveurs réels, tout en appliquant des paramètres logiques, en inspectant le flux et en sécurisant les cookies de session HTTP. Comme toujours, nous vous enseignerons la dernière version de l'outil à savoir FortiWeb 7.6.

Objectifs

- Comprendre les menaces guettant les couches applicatives
- Lutter contre les défacements et attaques par déni de service
- Prévenir les attaques 0-day sans perturber le trafic direct
- Rendre les applications rétroactivement compatibles avec
- OWASP Top 10 2013 et PCI DSS 3.0
- Découvrir les vulnérabilités de vos serveurs et applications Web hébergées pour une protection personnalisée et efficace.
- Configurer FortiGate avec FortiWeb, pour une sécurité renforcée des applications HTTP et XML
- Empêcher le contournement accidentel des scans, tout en autorisant les protocoles FTP et le SSH
- Configurer le blocage et le reporting pour un FortiADC ou FortiGate externe, et pour FortiAnalyze
- Choisir le mode de fonctionnement adéquat

- Équilibrer la charge au sein d'un pool de serveurs
- Sécuriser les applications « nues » : protocoles SSL/TLS, authentification et contrôle d'accès sophistiqué.
- Façonner FortiWeb pour protéger vos applications spécifiques.
- Dresser une liste noire des suspects : hackers, participants aux attaques DDoS et gratteurs de contenu.
- Effectuer un dépannage en cas de problème lié au flux du trafic (y compris le flux FTP/SSH).
- Diagnostiquer les faux positifs et personnaliser les signatures
- Optimiser les performances

Public visé

À tous ceux qui administrent régulièrement des Politiques de Filtrage déployées sur des Fortigates via FortiManager.

Pré-requis

- Connaissance des couches OSI et du protocole HTTP
- Maîtrise de base des langages HTML et JavaScript, ainsi que d'un langage de page dynamique côté serveur (par exemple, PHP)
- Maîtrise de base du transfert de port FortiGate

Programme de notre formation FortiWeb

1. Introduction 2. Configuration de base 3. Intégration SIEM externe 4. Intégration répartiteurs de charge et SNAT 5. Défacement et attaques par déni de service 6. Signatures, assainissement et auto-apprentissage 7. SSL et TLS 8. Authentification et contrôle d'accès 9. Conformité à la norme PCI DSS 3.0 10. Mise en cache et compression 11. Réécriture & redirections 12. Résolution des problèmes 13. Diagnostic

Certification

Ce cours vous prépare à l'examen de spécialiste FortiWeb 7. Il fait également partie des cours préparant l'examen de certification NSE 6.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être

problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.