Microtel
Training institute

FORMATION CONFIGURATION ET DÉPLOIEMENT DE FORTIWEB

Cette formation FortiWeb vous apprendra 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

CURSUS:
SÉCURITÉ DES SYSTÈMES D'INFORMATION

CODE DE LA FORMATION:
FT-SC-FORTIWEB

ÉDITEUR OU CONSTRUCTEUR:
FORTINET

DURÉE:
3 JOURS

PRÉREQUIS:
Pour suivre cette formation, il est important de posséder des connaissances des couches OSI et du protocole HTTP. Il est également demandé de maîtriser les bases des langages HTML et JavaScript, ainsi qu'un langage de page dynamique côté serveur (par exemple, PHP).Un maîtrise de base du transfert de port FortiGate est vivement conseillé.

PUBLIC:
Ce cours cible les professionnels des réseaux et de la sécurité chargés de l'administration et l'assistance FortiWeb

OBJECTIFS:
Concrètement à l'issue de ce cours vous serez en mesure de :

- 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 liés au flux du trafic (y compris le flux FTP/SSH).
- Diagnostiquer les faux positifs et personnaliser les signatures

- Optimiser les performances

CONTENU:

- Introduction
- Configuration de base
- Intégration SIEM externe
- Intégration répartiteurs de charge et SNAT
- Défacement et attaques par déni de service
- Signatures, assainissement et auto-apprentissage
- SSL et TLS
- Authentification et contrôle d'accès
- Conformité à la norme PCI DSS 3.0
- Mise en cache et compression
- Réécriture & redirections
- Résolution des problèmes
- Diagnostic