

Formation FORTINET NSE6, FortiWeb

Présentation

Ce programme de formation sur FortiWeb et son architecture couvre la présentation des fonctionnalités de sécurité des applications web, le déploiement initial et la configuration de base. Il inclut la protection contre les attaques web courantes, la configuration des politiques de sécurité, et la gestion des performances et de la haute disponibilité. Le programme aborde également l'intégration avec d'autres solutions Fortinet, la surveillance et le dépannage, ainsi que la création de rapports et la conformité.

Ce cours prépare au passage de la certification

L'achat du voucher pour passer la certification est en option.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Comprendre et déployer FortiWeb pour la protection des applications web contre les menaces et attaques.
- Configurer et gérer les règles de sécurité pour protéger les applications contre les attaques courantes (XSS, injection SQL, etc.).
- Intégrer FortiWeb avec des solutions Fortinet pour une gestion complète de la sécurité des applications.
- Appliquer des stratégies de gestion des performances et de haute disponibilité des applications web.

Prérequis

- Connaissances de base en réseaux et en sécurité informatique.
- Expérience avec les solutions Fortinet (idéalement FortiGate et FortiWeb).
- Compréhension des menaces courantes et des concepts de sécurité des applications web.

Public



- Administrateurs réseau et sécurité.
- Ingénieurs en sécurité des applications et des infrastructures.
- Responsables de la gestion de la sécurité des applications web.

Programme de la formation

Introduction à FortiWeb et architecture

- Présentation de FortiWeb et des fonctionnalités de sécurité des applications web
- Déploiement initial de FortiWeb dans un environnement de production
- Configuration de l'interface et des paramètres de base

Protection contre les attaques web courantes

- Prévention des attaques par injection SQL, XSS, CSRF, et autres
- Configuration des règles de sécurité pour la protection des applications
- Détection et prévention des attaques DDoS (Distributed Denial of Service)

Configuration des politiques de sécurité

- Création et gestion des politiques de sécurité pour les applications web
- Paramétrage des règles personnalisées et des protections contre les vulnérabilités spécifiques
- Utilisation des profils de sécurité pour un filtrage approfondi du trafic web

Gestion des performances et haute disponibilité

- Configuration de l'équilibrage de charge pour les applications web
- Optimisation des performances des applications avec FortiWeb
- Mise en place d'une haute disponibilité (HA) pour les déploiements FortiWeb

Intégration avec d'autres solutions Fortinet

- Intégration avec FortiGate pour une gestion unifiée de la sécurité réseau et des applications
- Surveillance et gestion des logs via FortiAnalyzer
- Automatisation de la réponse aux incidents de sécurité des applications avec FortiSIEM

Surveillance et dépannage

- Analyse des logs d'attaque et des alertes générées par FortiWeb
- Surveillance du trafic web et des menaces potentielles
- Techniques de dépannage courantes pour FortiWeb

Rapports et conformité

- Création de rapports de sécurité pour les applications web
- Conformité avec les standards de sécurité (PCI DSS, GDPR, etc.)
- Génération de rapports d'audit pour le suivi des actions de sécurité

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.