

Durée : 3 jours soit 21 heures

Référence : DOCPOS-FORTIWEB-NSE



Public visé :

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



Pré-requis :

- 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.



Objectifs pédagogiques :

- 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.



Compétences acquises à l'issue 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.



Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.



Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel



Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique



Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert...).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquis ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.



Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :

Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr

Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.

Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- [AGEFIPH](#)
- [FIPHFP](#)
- MDPH de votre département

Description / Contenu

Module 1 : 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
- Conformité avec les standards de sécurité (PCI DSS, GDPR, etc.)
- Génération de rapports d'audit pour le suivi des actions de sécurité

Module 2 : 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)

Module 3 : 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

Module 4 : 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

Module 5 : 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

Module 6 : 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

Module 7 : Rapports et conformité

- Création de rapports de sécurité pour les applications web