Maîtrise de NSE6 FortiWeb et Protection des Applications Web

Lien : https://innov-systems.com/formation/matrise-de-nse6-fortiweb-et-protection-des-applications-web

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC271**	**Fortinet**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les menaces spécifiques aux applications web et les principes du WAF (Web Application Firewall)
- Configurer, administrer et optimiser un FortiWeb pour une protection complète des applications web
- Mettre en œuvre des stratégies de défense contre les attaques DoS, le defacement et les attaques 0-day
- Intégrer FortiWeb dans un écosystème Fortinet (FortiGate, FortiAnalyzer, FortiSIEM)
- Déployer des politiques de sécurité conformes aux référentiels OWASP et PCI DSS
- Diagnostiquer, affiner et automatiser la détection pour réduire les faux positifs et améliorer les performances

POUR QUI ?

- Administrateurs sécurité et réseaux
- Ingénieurs systèmes responsables de la sécurité applicative
- Responsables SOC ou exploitants de solutions Fortinet
- Techniciens en charge du maintien en condition de sécurité des applications web critiques

Innov Systems

Programme détaillé

1 / INTRODUCTION AU WAF ET À FORTIWEB

- Rôle et fonctionnement d’un Web Application Firewall
- Typologie des attaques applicatives : injection, XSS, CSRF, DoS, defacement
- Positionnement de FortiWeb dans l’écosystème Fortinet
- Modes de déploiement : Reverse Proxy, Transparent, Offline, True Transparent Proxy

2 / CONFIGURATION DE BASE ET MISE EN SERVICE

- Installation et accès à l’interface d’administration
- Création d’interfaces, VLANs, routes et politiques initiales
- Gestion des utilisateurs, profils d’accès et certificats
- Premiers tests de disponibilité et validation des flux applicatifs

3 / INTÉGRATION AVEC LES SYSTÈMES DE SÉCURITÉ EXISTANTS

- Communication et synchronisation avec FortiGate
- Configuration des journaux et intégration avec FortiAnalyzer
- Connexion à un SIEM externe pour la corrélation des événements
- Bonnes pratiques de supervision et d’alerting

4 / DÉTECTION ET PROTECTION CONTRE LES ATTAQUES APPLICATIVES

- Configuration des signatures d’attaque et filtrage applicatif
- Protection contre les attaques 0-day via le moteur d’auto-apprentissage
- Gestion des faux positifs : ajustement des règles et validation du trafic
- Création de politiques de sécurité adaptées à chaque application

5 / MITIGATION DES ATTAQUES DOS ET DÉFACEMENT

Innov Systems

- Types de DoS applicatifs et méthodes de mitigation
- Protection du contenu web contre les tentatives de défiguration
- Stratégies de blocage adaptatif et limitation de taux
- Simulation et analyse d’incidents DoS

6 / CHIFFREMENT ET SÉCURISATION DES COMMUNICATIONS

- Concepts SSL/TLS et certificats X.509
- Activation du SSL Offloading sur FortiWeb
- Forcer le HTTPS et rediriger les connexions non sécurisées
- Bonnes pratiques pour la gestion du cycle de vie des certificats

7 / AUTHENTIFICATION ET CONTRÔLE D’ACCÈS

- Configuration des politiques d’authentification (formulaire, SSO, LDAP, RADIUS)
- Gestion des sessions utilisateurs et règles de restriction
- Mise en place de portails d’accès sécurisés
- Journalisation et suivi des connexions

8 / CONFORMITÉ OWASP ET PCI DSS

- Introduction aux référentiels de conformité applicative
- Vérification de la conformité PCI DSS sur FortiWeb
- Mise en œuvre des contrôles OWASP Top 10
- Rapports d’audit et traçabilité des événements

9 / OPTIMISATION DES PERFORMANCES ET DE LA DISPONIBILITÉ

- Configuration du caching et de la compression HTTP
- Load balancing et persistance de session
- Optimisation du temps de réponse et des ressources système
- Surveillance de la charge et maintenance proactive

Inov Systems

10 / AUTOMATISATION ET AUTO-APPRENTISSAGE

- Fonctionnement du moteur d’auto-apprentissage FortiWeb
- Déploiement progressif et ajustement automatique des règles
- Analyse des profils de trafic pour une meilleure détection
- Cas pratiques d’intégration en production

11 / TROUBLESHOOTING ET RÉSOLUTION D’INCIDENTS

- Méthodologie de diagnostic avancé
- Analyse des journaux, rapports et traces réseau
- Identification et correction des erreurs de configuration
- Bonnes pratiques pour la continuité de service

12 / ATELIER FINAL : CONFIGURATION COMPLÈTE ET SCÉNARIOS RÉELS

- Mise en œuvre complète d’un déploiement sécurisé FortiWeb
- Intégration avec FortiGate et FortiAnalyzer
- Tests d’attaque simulée et validation des politiques
- Évaluation et restitution des acquis

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

30 Juin au 03 Juil. 2026	Présentiel - Casablanca
25 au 28 Août 2026	Distanciel
20 au 23 Oct. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés

Innov Systems