DOCAPOSTE Institute

Formation FORTINET NSE5, FortiAnalyzer Administrator

Présentation

Ce programme de formation sur FortiAnalyzer couvre la présentation de ses fonctionnalités principales et de son architecture, ainsi que la configuration initiale. Il inclut la gestion et la configuration des logs de sécurité, l'analyse des logs et des rapports, et la surveillance et les alertes en temps réel. Le programme aborde également la gestion des incidents et des réponses, l'optimisation et le dépannage, ainsi que l'intégration avec d'autres produits Fortinet.
Ce cours prépare au passage de la certification
L'achat du voucher pour passer la certification est en option.

Durée : 7,00 heures (1 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Comprendre et maîtriser l'administration de FortiAnalyzer pour centraliser, analyser et corréler les logs de sécurité.
- Configurer, gérer et personnaliser les rapports et les alertes de sécurité avec FortiAnalyzer.
- Intégrer FortiAnalyzer avec d'autres solutions Fortinet pour une gestion de la sécurité unifiée et optimale.
- Appliquer des stratégies avancées pour le dépannage et la surveillance des événements de sécurité réseau.

Prérequis

- Connaissances de base en réseaux et sécurité (idéalement avec FortiGate et autres produits Fortinet).
- Expérience dans la gestion des logs et la surveillance de la sécurité.
- Certification Fortinet NSE4 ou expérience avec des solutions FortiGate est recommandée.

Public

- Administrateurs réseau et sécurité.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Ingénieurs et responsables de la gestion de la sécurité, cherchant à analyser et centraliser les logs de Fortinet.
- Administrateurs de solutions FortiGate, FortiSIEM, FortiWeb, et autres outils Fortinet, souhaitant renforcer la surveillance et l'analyse de la sécurité.

Programme de la formation

Introduction à FortiAnalyzer et à son architecture

- Présentation de FortiAnalyzer et de ses fonctionnalités principales
- Architecture de FortiAnalyzer pour centraliser les logs et événements
- Configuration initiale de FortiAnalyzer et de l'interface d'administration

Gestion et configuration des logs de sécurité

- Configuration de la collecte de logs à partir de dispositifs Fortinet (FortiGate, FortiSwitch, etc.)
- Personnalisation des paramètres de collecte, des filtres de logs et des événements spécifiques
- Stockage des logs et gestion de la rétention des données

Analyse des logs et des rapports de sécurité

- Exploration des logs de sécurité pour détecter les incidents et anomalies
- Création de rapports personnalisés pour l'analyse de la sécurité réseau
- Mise en place de rapports sur les incidents, les menaces et les activités suspectes

Surveillance et alertes en temps réel

- Configuration des alertes et notifications basées sur des événements spécifiques de sécurité
- Intégration avec FortiSIEM pour une surveillance avancée et une gestion des incidents
- Utilisation de FortiAnalyzer pour l'analyse en temps réel des événements de sécurité

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Gestion des incidents et des réponses

- Mise en place de processus pour répondre aux incidents et aux alertes générées par FortiAnalyzer
- Gestion des réponses aux menaces et incidents de sécurité détectés via les logs
- Meilleures pratiques pour utiliser FortiAnalyzer dans les environnements de sécurité opérationnels

Optimisation et dépannage

- Résolution des problèmes courants de collecte de logs et de performance des rapports
- Optimisation des configurations pour améliorer la visibilité et la réactivité du système
- Utilisation de FortiAnalyzer pour le dépannage et l'identification des points de faiblesse réseau

Intégration avec d'autres produits Fortinet

- Intégration de FortiAnalyzer avec FortiGate, FortiSIEM, FortiWeb, et autres produits Fortinet
- Collaboration entre FortiAnalyzer et FortiManager pour la gestion centralisée
- Automatisation de la collecte et de la gestion des logs à travers la Security Fabric de Fortinet

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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- 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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France