Fortianalyser

Le prix ne comprend pas le passage de la certification

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Outils

Rubrique : Fortinet - Shibboleth

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Apprendre à utiliser la FortiAnalyzer.
Explorer l'interface d'administration,
Inscrire de nouveaux équipements et sécuriser les communications avec le FortiAnalyzer.
Manipuler les logs et les achives, les rapports existants
Configurez des rapports personnalisés

Public visé

coordinateurs, managers, chefs de projets

Pré-requis

Aucun

PROGRAMME

JOUR 1

Introduction au FortiAnalyzer (Durée : 1 heure)
Présentation du FortiAnalyzer et de son rôle dans l'infrastructure de sécurité réseau
Principales fonctionnalités et avantages du FortiAnalyzer
Vue d'ensemble de l'architecture et des composants du FortiAnalyzer

TP 1 : Installation et configuration initiale du FortiAnalyzer.
TP 2 : Exploration de l'interface utilisateur du FortiAnalyzer et navigation dans les différents menus et options.

Configuration et administration (Durée : 2 heures)
Configuration initiale du FortiAnalyzer : accès, paramètres de base, etc.
Gestion des utilisateurs et des groupes d'utilisateurs
Gestion des politiques de sécurité et des rôles
Surveillance et gestion des performances du système
Sauvegarde et restauration de la configuration

TP 1 : Création et gestion des utilisateurs et des groupes d'utilisateurs sur le FortiAnalyzer.
TP 2 : Configuration des politiques de sécurité et des rôles pour définir les niveaux d'accès des utilisateurs.
TP 3 : Surveillance et gestion des performances du système en utilisant les outils disponibles sur le FortiAnalyzer.
TP 4 : Sauvegarde et restauration de la configuration du FortiAnalyzer.

Inscription des équipements qui enverront leurs logs sur le FortiAnalyzer (Durée : 1,5 heures)
Présentation des différentes méthodes d'inscription des équipements (via FortiGate, FortiSwitch, etc.)
Configuration des équipements pour l'envoi des logs vers le FortiAnalyzer
Vérification de la connectivité et de la réception des logs

TP 1 : Configuration d'un FortiGate pour envoyer ses logs vers le

Code de formation : NE225

€ Tarifs

Prix public : 1870 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 7 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

FortiAnalyzer.
TP 2 : Configuration d'un FortiSwitch pour envoyer ses logs vers le FortiAnalyzer.
TP 3 : Vérification de la connectivité et de la réception des logs sur le FortiAnalyzer.

Les logs et les archives (Durée : 1,5 heures)
Compréhension des différents types de logs générés par les équipements
Analyse des logs en temps réel
Utilisation des filtres pour la recherche et la récupération des logs spécifiques
Archivage des logs et gestion de l'espace de stockage

TP 1 : Analyse des logs en temps réel sur le FortiAnalyzer.
TP 2 : Utilisation des filtres pour rechercher des logs spécifiques sur le FortiAnalyzer.
TP 3 : Configuration de l'archivage des logs et gestion de l'espace de stockage sur le FortiAnalyzer.

Les rapports (Durée : 1 heure)
Génération de rapports prédéfinis et personnalisés
Personnalisation des rapports en fonction des besoins de l'organisation
Analyse des données des rapports pour l'optimisation de la sécurité réseau
Planification et automatisation de la génération des rapports

TP 1 : Génération de rapports prédéfinis sur le FortiAnalyzer.
TP 2 : Personnalisation des rapports en fonction des besoins spécifiques de l'organisation.
TP 3 : Analyse des données des rapports pour identifier les tendances de sécurité et les points d'amélioration.
TP 4 : Planification et automatisation de la génération des rapports sur le FortiAnalyze

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.