

RADWARE DEFENSEPRO

Les fondamentaux

Référence : ISSRDWDPRO

PLAN DE COURS

Objectifs : installer et déployer DefensePro en suivant les instructions ; comprendre et configurer les différentes possibilités de protection ; utiliser APSolute Vision et Vision Reporter	
Prérequis : Bonnes connaissances en sécurité et réseau	
Public : Administrateurs, responsables de la sécurité du SI	
Niveau : Débutant	Durée standard préconisée : 3 jrs (dont 1 Vision Reporter)
Pédagogie : alternance d'apports théoriques et nombreux exercices de mise en pratique	
Moyens pédagogiques : un ordinateur multimédia par apprenant, ordinateur et vidéoprojecteur pour l'animateur	Évaluation des acquis : Mise en pratique à l'aide d'exercices en autonomie puis corrigés individuellement et collectivement
Suivi après formation : • Certificat de stage • Bilan de formation rempli par le formateur	• Évaluation de satisfaction à chaud remplie par l'apprenant • Un ouvrage de référence (remis en formation)

Détail des objectifs

Cocher les OBJECTIFS

	définis lors du tour de table	traités durant la formation
Appréhender la problématique et RADWARE DefensePro	<input type="checkbox"/>	<input type="checkbox"/>
Réaliser les actions fondamentales (connexion, administration et politique de sécurité).....	<input type="checkbox"/>	<input type="checkbox"/>
Administrer et réaliser une configuration initiale.....	<input type="checkbox"/>	<input type="checkbox"/>
Installer DefensePro.....	<input type="checkbox"/>	<input type="checkbox"/>
Se connecter en utilisant APSolute Insite.....	<input type="checkbox"/>	<input type="checkbox"/>
Administrer DefensePro.....	<input type="checkbox"/>	<input type="checkbox"/>
Protéger son réseau	<input type="checkbox"/>	<input type="checkbox"/>
Appréhender la protection DoS (Denial of Service).....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer la protection DoS avec la protection DNS.....	<input type="checkbox"/>	<input type="checkbox"/>
Prévenir la propagation par vers.....	<input type="checkbox"/>	<input type="checkbox"/>
Définir une protection Anti-Scanning.....	<input type="checkbox"/>	<input type="checkbox"/>
Se protéger contre les attaques SYN Flood.....	<input type="checkbox"/>	<input type="checkbox"/>
Définir des limites de connexion.....	<input type="checkbox"/>	<input type="checkbox"/>
Protéger les serveurs	<input type="checkbox"/>	<input type="checkbox"/>
Mettre en place une protection Server Cracking.....	<input type="checkbox"/>	<input type="checkbox"/>
Mettre en place une protection HTTP Mitigator.....	<input type="checkbox"/>	<input type="checkbox"/>
Mettre en place la Signature Protection	<input type="checkbox"/>	<input type="checkbox"/>
Définir les profils.....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les signatures des clients.....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les exceptions de sécurité (Black 1 White listes).....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les ACL (Access Control List).....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer la bande passante.....	<input type="checkbox"/>	<input type="checkbox"/>
Déployer.....	<input type="checkbox"/>	<input type="checkbox"/>
Utiliser APSolute Vision (3^{ème} jour)	<input type="checkbox"/>	<input type="checkbox"/>
Appréhender APSolute Vision.....	<input type="checkbox"/>	<input type="checkbox"/>
Utiliser APSolute Vision.....	<input type="checkbox"/>	<input type="checkbox"/>
Mettre en œuvre Vision Reporter.....	<input type="checkbox"/>	<input type="checkbox"/>

Compléments :

.....

.....