INTITULE DE LA FORMATION :

Symantec Data Loss Prevention 15.5 Administration

REF. COURS : SYM_DLP15

DUREE : 5 JOURS (35H)

- Formation inter-entreprise ou intra-entreprise
- Formation en présentiel ou distanciel
- Horaires : 9h-12h30 – 14h-17h30

PRIX PUBLIC INTERENTREPRISES : 4500€ HT / PERS

DESCRIPTION :

Le cours d'administration de Symantec Data Loss Prevention 15.5 est conçu pour vous fournir les connaissances fondamentales nécessaires à la configuration et à l'administration de la plate-forme Symantec Data Loss Prevention Enforce. Les ateliers pratiques comprennent des exercices pour configurer le serveur Enforce, les serveurs de détection et les agents DLP, ainsi que la création de stratégies et la détection d'incidents, la réponse aux incidents, les rapports d'incidents et l'administration des utilisateurs et des rôles. De plus, vous découvrirez les meilleures pratiques de déploiement et les produits Symantec Data Loss Prevention suivants : Network Monitor, Network Prevent, Cloud Service for Email, Network Discover, Network Protect, Cloud Storage, Endpoint Prevent et Endpoint Discover. Notez que ce cours est dispensé sur une plate-forme Microsoft Windows.

OBJECTIFS PEDAGOGIQUE :

À la fin de ce cours, vous serez en mesure de configurer et d'utiliser Symantec Data Loss Prevention 15.5.

Ce cours comprend des exercices pratiques qui vous permettent de tester vos nouvelles compétences et de commencer à utiliser ces compétences dans un environnement de travail.

COMPETENCE VISEE :

PUBLIC :

Ce cours est destiné à toute personne responsable de la configuration, de la maintenance et du dépannage de Symantec Data Loss Prevention. De plus, ce cours est destiné aux utilisateurs techniques responsables de la création et de la maintenance des politiques Symantec Data Loss Prevention et de la structure de réponse aux incidents.

PRE-REQUIS :

Vous devez avoir une connaissance pratique des systèmes d'exploitation et des commandes de classe serveur Windows, ainsi que des concepts de mise en réseau et de sécurité réseau.

PROGRAMME :

Module 1 : Vue de la prévention des pertes de données
- Vue de prévention des pertes de données
- Gestion des risques de perte de données
- Cas d'utilisation réels de la prévention des pertes de données

Module 2 : Présentation de Symantec Data Loss Prevention
- Suite de prévention contre la perte de données Symantec
- Architecture Symantec Data Loss Prevention

Module 3 : Identification et description des données confidentielles
- Identification des données confidentielles
- Configuration de Symantec Data Loss Prevention pour reconnaître les données confidentielles
- Correspondance du contenu décrit (DCM)
- Correspondance exacte des données (EDM)
- Correspondance de documents indexés (IDM)
- Apprentissage automatique des vecteurs (VML)
- Reconnaissance d'images sensibles
- Détection de type de fichier personnalisé

Travaux pratiques :

visiter la console Enforce, créer des groupes de stratégies, configurer une stratégie pour la détection des informations personnelles identifiables (PII), configurer une stratégie pour la conformité PCI, configurer une stratégie pour protéger les documents confidentiels, configurer une stratégie pour protéger le code source, configurer une stratégie ou une reconnaissance de formulaire, utiliser un modèle pour ajouter une stratégie DLP, exporter des stratégies à utiliser sur un site de reprise après sinistre (DR), configurer la reconnaissance optique de caractères (OCR)

Module 4 : Localisation des données confidentielles stockées sur site et dans le cloud

- Déterminer où rechercher des données confidentielles
- Localisation des données confidentielles sur les référentiels d'entreprise
- Localisation des données confidentielles dans le Cloud
- Localisation des données confidentielles sur les ordinateurs d'extrémité

Travaux pratiques :

Exécuter une analyse d'énumération de contenu, analyser une cible Windows, analyser les ordinateurs d'extrémité à la recherche de données confidentielles.

Module 5 : Comprendre comment les données confidentielles sont utilisées

- Surveillance des données confidentielles circulant sur le réseau
- Surveillance des données confidentielles utilisées sur les ordinateurs d'extrémité

Travaux pratiques :

Configurer Network Prevent for Email pour surveiller les messages SMTP, utiliser Network Prevent for Email pour surveiller les messages SMTP, surveiller l'activité des points de terminaison.

Module 6 : Former les utilisateurs à adopter des pratiques de protection des données

- Mise en place d'une formation en entreprise sur les politiques de protection des données
- Fournir des notifications de violations de la politique des utilisateurs

Travaux pratiques :

Configurer le plug-in de recherche Active Directory, configurer les notifications par e-mail, configurer les notifications à l'écran.

Module 7 : Prévention de l'exposition non autorisée de données confidentielles

- Utilisation de règles de réponse pour empêcher l'exposition de données confidentielles
- Protection des données confidentielles en mouvement
- Protection des données confidentielles en cours d'utilisation
- Protection des données confidentielles au repos

Travaux pratiques :

Configurer le blocage SMTP, tester la reconnaissance optique de caractères (OCR) et la politique « HIPAA et HITECH (y compris PHI) », configurer le blocage des points de terminaison, configurer l'annulation de l'utilisateur du point de terminaison, analyser et mettre en quarantaine les fichiers sur une cible de partage de fichiers de serveur, analyser et mettre en quarantaine les fichiers sur une cible de point de terminaison

Module 8 : Corriger les incidents de perte de données et suivre la réduction des risques

- Examen des cadres de gestion des risques
- Utilisation des options de rapport d'incident pour identifier et évaluer les risques
- Créer des outils qui soutiennent le processus de réduction des risques de l'organisation
- Communiquer les risques aux parties prenantes • Comprendre les options de reporting et d'analyse avancées.

Travaux pratiques :

Configurer les rôles et les utilisateurs, utiliser des rapports pour suivre l'exposition et la réduction des risques, définir les statuts d'incident et les groupes de statuts, configurer et utiliser les réponses intelligentes, planifier et envoyer des rapports.

Module 9 : Améliorer la prévention des pertes de données avec les intégrations

- Mécanismes d'intégration Symantec DLP
- Sécurité centrée sur l'information Symantec
- Intégrations supplémentaires avec les solutions Symantec Enterprise

Travaux pratiques :

Créer le schéma de vues et l'utilisateur, exécuter le script de configuration de la vue des données d'incident, vérifier la création des vues de données d'incident, utiliser les vues de données d'incident

Module 10 : Révision du cours

- Examen des produits et de l'architecture Symantec DLP
- Examen des étapes d'une mise en œuvre de la prévention des pertes de données

TEST AND CERTIFICATION :

EVALUATION DE LA FORMATION :

- Avant la formation : Auto-positionnement du stagiaire selon les prérequis
- Pendant la formation (démarche formative) : évaluation continue des connaissances, travaux pratiques.
- À l'issue de la formation (démarche sommative) : questionnaire de satisfaction du stagiaire,
- A 6 mois : évaluation différée

INTERVENANT :

- Consultant/ Formateur habilité et certifié SYMANTEC

LIEU ET DELAI D'ACCES

- Lieu en présentiel : **38 rue Victor Hugo – 92400 COURBEVOIE ou autre site préciser dans la convocation**
- **Présentiel** : groupe de 4 participants minimum et 12 participants maximum
- **Distanciel** : groupe de 4 participants minimum et 10 participants maximum
- **Le délai estimé** entre la demande du bénéficiaire et le début de la prestation est estimé entre 3 mois et 1 jour (financement CPF).

METHODES MOBILISEES EN DISTANCIEL

ARROW ECS Education adapte ses modules en distanciel avec l'outil TEAMS (autre selon contraintes techniques), autour de l'organisation et des principes pédagogiques suivants:

- Un référent technique adresse en amont aux participants les informations techniques nécessaire et un tuto pour suivre la formation à distance avec l'outil TEAMS. Il valide avec chacun le bon fonctionnement des connections audio et vidéo lors d'un RV technique collectif. Il pose également les règles du jeu d'un fonctionnement en virtuel et gère d'éventuelles problématiques techniques.

  Par ailleurs il est disponible la première demi-journée de formation en cas de soucis technique des participants, pour gérer individuellement d'éventuels ajustements liés à l'outil « en ligne ».
- Des documents sont envoyés en amont (par mail) : questionnaire, supports bénéficiaires, auto-tests éventuels, boite à outils …
- La « classe virtuelle » permet aux participants d'avoir accès aux mêmes ressources techniques qu'en présentiel. Chaque participant aura accès à un support de cours et un environnement technique accessible via le Cloud. Cette démarche vise à renforcer la dimension opérationnelle des sessions à distance, tout en gardant la richesse du partage en intelligence collective.

  Au-delà de l'animation en plénière, l'outil en ligne permet l'organisation de sous-groupes virtuels de travail dans le déroulé de la formation et le formateur passe d'un groupe à l'autre en soutien. De même les mises en situation sont maintenues.

Une messagerie (chat) permet aux participants d'interagir par écrit, au-delà des échanges interactifs.

MOYENS PEDAGOGIQUES ET TECHNIQUES

- Supports en Anglais : les participants recevront le support de la formation en format numérisé. Un lien d'accès à une plateforme de téléchargement dédiée leur sera adressé avant la formation, leur permettant de télécharger l'ensemble des supports, documentations et outils de la formation.
- Matériel nécessaire pour la formation en présentiel :

✓ Une salle dont la taille est compatible avec le plan gouvernemental de lutte contre l'épidémie de COVID-19 en vigueur au moment de la formation
✓ Un vidéo projecteur et la possibilité de sonorisation
✓ 1 paperboard
✓ Une connexion internet
✓ Un PC

- Matériel nécessaire pour la formation en distanciel :

✓ Un ordinateur comprenant un micro, une enceinte et si possible un double écran.
✓ Une connexion Internet.

MODALITES DE SUIVI

- La convocation et le livret d'accueil sont envoyés à l'apprenant 10 jours avant le début de la formation.
- L'intervenant ou ARROW ECS Education remet le règlement intérieur, signe et fait signer la feuille d'émargement au stagiaire par demi-journées.
- L'attestation de formation est remise au stagiaire à la fin de la formation.
- Le livret d'accueil et le règlement intérieur sont consultables sur notre site https://edu.arrow.com/fr/ rubrique « ressources ».

- Suivi post formation : le participant envoie sa demande au formateur par écrit à l'adresse mail suivante : training.ecs.fr@arrow.com . Le formateur lui répond par retour de mail, sous 3 jours en fonction de ses disponibilités. Selon le niveau de complexité de la demande, il peut également lui proposer un rendez-vous téléphonique dans les cinq jours pour approfondir la question et solutionner sa problématique. Cette assistance est mise en place durant trois mois, à partir de la fin de la session.

ACCESSIBILITE ET PRISE EN COMPTE DES SITUATIONS DE HANDICAP

- Pour nos formations, nous faisons une étude préalable à la formation pour adapter nos locaux, nos modalités pédagogiques et d'animation en fonction de la situation de handicap portée à notre

connaissance. En fonction des besoins spécifiques, nous mettrons tout en œuvre avec nos partenaires spécialisés pour être en capacité de réaliser la prestation.

- Pour toute demande, merci de bien vouloir contacter notre référent handicap Cédric BOUTROS par mail : cedric.boutros@arrow.com

MOYENS D'ENCADREMENT

- **Assistance pédagogique** : Thierry DESOUCHE – thierry.desouche@arrow.com – 06 85 34 81 53 - du lundi au vendredi (9h30-13h, 14h-17h30)
- **Assistance technique :** Jean Yves BORG – jean-yves.borg@arrow.com - – 06 76 98 76 61 - du lundi. au vend.(9h30-13h,14h-17h30)
- **Intervenant** : (préciser son nom) training.ecs.fr@arrow.com – 01 49 97 49 51 du lundi au vendredi (9h30-13h, 14h-17h30)
- **Référent handicap** : Cédric. BOUTROS – cedric.boutros@arrow.com – 06 38 14 03 69 (9h30-13h, 14h-17h30)

DEBOUCHES ET SUITE DU PARCOURS

En France et dans l'OCDE les mutations économiques, technologiques mais aussi sociétales s'accélèrent depuis ces dernières années et incitent les entreprises à modifier en profondeur leur organisation du travail, pour anticiper les changements et de s'y adapter. Dans ce contexte, le développement et l'adaptation des compétences à ces évolutions prend une dimension primordiale, pour permettre aux équipes d'être en adéquation avec la mutation technologique en perpétuelle évolution et des nouvelles compétences techniques nécessaires.

L'accompagnement des équipes dans un environnement apprenant est devenu aujourd'hui un enjeu majeur pour permettre aux structures de déployer et réussir la transformation, mais aussi pour donner la capacité aux individus à maintenir leur employabilité ou à intégrer le marché du travail.

Cette formation vous permet de développer vos compétences et d'être en capacité de configurer et d' administrer la plate-forme Symantec Data Loss Prevention Enforce.