

INTITULE DE LA FORMATION :**Trend Micro Deep Security 20****REF. COURS:** TRM_DS**DUREE :** 3 JOURS (21H)

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

PRIX PUBLIC INTERENTREPRISES : 2250€ HT / PERS**DESCRIPTION :**

La formation Deep Security 20 pour les professionnels certifiés est une formation de trois jours,

cours de formation dirigé par un instructeur. Les participants apprendront à utiliser Trend Micro Deep Security pour une sécurité cloud hybride avancée sur les sites physiques, virtuels et basés sur le cloud les serveurs. Ce cours détaille l'architecture de base du Deep sur site Solution de sécurité, options de déploiement, modules de protection, configuration des politiques et l'administration du système. Dans le cadre du cours, les participants déploieront Deep Security agents sur une variété de Windows Server, ainsi que Deep Security Virtual Appareil. Meilleures pratiques et détails de dépannage pour une mise en œuvre réussie et la maintenance à long terme du système sont discutées.

Ce cours est dispensé par des formateurs certifiés Trend Micro et intègre une variété d'exercices pratiques en laboratoire, permettant aux participants de mettre le contenu de la leçon en action.

OBJECTIFS PEDAGOGIQUE :

Après avoir terminé cette formation, les participants pourront :

- Décrire le but, les caractéristiques, fonctions et capacités de Deep Sécurité 20
- Définir et installer les composants qui composent la sécurité profonde
- Mettre en œuvre la sécurité en activant des modules de protection
- Décrire la configuration disponible et les options d'administration
- Tenter la certification Trend Micro Professionnel pour la sécurité profonde

Examen de certification

COMPETENCE VISEE :

PUBLIC :

Ce cours est conçu pour les professionnels IT responsables de la protection réseaux, point de terminaison, cloud ou menaces de sécurité xSP.

Ce stage concerne également les administrateurs systèmes, les ingénieurs réseaux, les ingénieurs vente / avant-vente, les gestionnaires de comptes techniques (TAM), les ingénieurs Support, ingénieurs Intégration et les architectes Solution & Sécurité.

PRE-REQUIS :

Il n'y a pas de prérequis pour suivre ce cours, cependant, une connaissance pratique de Trend Micro produits et services, ainsi qu'une compréhension des concepts de base des réseaux et les principes seront utiles.

Une connaissance de base des sujets suivants est également bénéfique :

- Serveurs et clients Windows
- Pare-feu et dispositifs d'inspection de paquets
- VMware® ESXi/vCenter/NSX
- Amazon Web Services/Microsoft® Azure®/VMware vCloud®/Google Cloud Platform™
- Technologies de virtualisation

Les participants sont tenus d'apporter un ordinateur portable avec une résolution d'écran recommandée d'au moins 1980 x 1080 ou plus et une taille d'affichage de 15" ou plus.

PROGRAMME :

Sujets couverts:

- Présentation du produit
- Introduction à la Deep Security
- Modules de protection Deep Security
- Options de déploiement de Deep Security
- Composants de Deep Security Trend Micro
- Serveur, système d'exploitation et base de données exigences
- Architecture du gestionnaire de Deep Security

- Installation et mise à niveau de Deep Security Directeur
- Déploiement d'agents de Deep Security
- Architecture des agents de Deep Security
- Déploiement d'agents Deep Security
- Gestion des agents de Deep Security
- Opérations en ligne de commande
- Réinitialisation des agents
- Agents protecteurs
- Affichage de l'état de protection de l'ordinateur
- Mise à niveau des agents Deep Security
- Organisation des ordinateurs à l'aide de groupes et Dossiers intelligents
- Maintenir la sécurité approfondie à jour
- Mises à jour de sécurité
- Mises à jour de logiciel
- Relais de sécurité profonde Trend Micro
- Services Smart Protection utilisés par Deep Security
- Configuration de la source Smart Protection Stratégies
- Héritage et remplacement des stratégies
- Création de nouvelles politiques
- Exécution d'analyses de recommandations
- Protéger les serveurs contre les logiciels malveillants
- Techniques d'analyse anti-malware
- Activation de la protection anti-malware
- Analyse Intelligente
- Blocage des sites Web malveillants
- Activation de la réputation de sites Web
- Réglage du niveau de sécurité
- Filtrage du trafic à l'aide du pare-feu
- Activation du pare-feu Deep Security
- Règles de pare-feu
- Analyse du trafic
- Ordre d'analyse du trafic
- Analyse des ports
- Protéger les serveurs contre les vulnérabilités
- Correctif virtuel
- Détection d'une activité réseau suspecte
- Protection des applications Web
- Activation de la prévention des intrusions
- Règles de prévention des intrusions
- Filtrage SSL (Security Sockets Layer)

- Protéger les applications Web
- Détection des modifications apportées aux serveurs protégés
- Activation de la surveillance de l'intégrité
- Exécution d'analyses de recommandations
- Détection des modifications apportées aux objets de la ligne de base
- Blocage des logiciels non approuvés
- Modes d'exécution
- Activation du contrôle des applications
- Détection des modifications logicielles
- Création d'un inventaire des logiciels approuvés
- Pré-approbation des modifications logicielles
- Inspection des journaux sur les serveurs protégés
- Activation de l'inspection des journaux
- Exécution d'analyses de recommandations
- Événements et alertes
- Transfert d'événement
- Alertes
- Marquage d'événement
- Rapports
- Protéger les conteneurs
- Intégration continue/déploiement continu
- Développement de logiciels à l'aide de conteneurs
- Protéger les conteneurs avec Deep Security
- Automatisation des opérations de sécurité approfondie
- Tâches planifiées
- Tâches basées sur des événements
- Modèles de démarrage rapide
- Faire de l'agent Deep Security un Amazone
- Interface de programmation d'applications
- Détecter les programmes malveillants émergents via
- Défense contre les menaces connectées
- Phases de défense contre les menaces connectées
- Analyseur Trend Micro™ Deep Discovery™
- Trend Micro Apex Central™
- Configuration de la sécurité profonde pour les connectés
- Défense contre les menaces
- Suivi des soumissions
- Sujets de l'annexe
- Activation et gestion de plusieurs locataires
- Protéger les machines virtuelles à l'aide du Deep
- Appliance virtuelle de sécurité
- Dépannage des problèmes courants de Deep Security

TEST AND CERTIFICATION :

À la fin de ce cours, les participants peuvent choisir de passer l'examen de certification obtenir la désignation en tant que Trend Micro Certified Professional for Deep Security.

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 TREND MICRO

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, boîte 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'accroissent 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 d'utiliser Trend Micro Deep Security pour une sécurité cloud hybride avancée sur les sites physiques, virtuels et basés sur le cloud les serveurs.