INTITULE DE LA FORMATION :

SG UTM : Administrator

REF. COURS : SOP_SG_UTM

DUREE : 3 JOURS (21H)

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

PRIX PUBLIC INTERENTREPRISES : 1800€ HT / PERS

DESCRIPTION :

Ce cours est conçu pour les professionnels techniques qui administreront Sophos SG UTM et fournit les compétences nécessaires pour gérer les tâches courantes au quotidien.

Il se compose de présentations et d'exercices pratiques en laboratoire pour renforcer le contenu enseigné, et des copies électroniques des documents justificatifs du cours seront fournies à chaque stagiaire via le portail en ligne.

Le cours devrait durer 2 jours, dont environ la moitié sera consacrée aux exercices pratiques.

OBJECTIFS PEDAGOGIQUE :

A l'issue de cette formation, les stagiaires seront capables de :

- Reconnaître les principales capacités techniques et leur protection contre les menaces
- Effectuer les tâches de configuration courantes
- Sauvegarder et restaurer le système
- Accomplir des tâches courantes au quotidien
- Afficher et gérer les journaux et les rapports

COMPETENCE VISEE :

PUBLIC :

PRE-REQUIS :

il n'y a pas de prérequis pour ce cours ; Cependant, il est recommandé aux stagiaires de :

Avoir des connaissances en réseau équivalentes à CompTIA N+ ou mieux

Connaître les bonnes pratiques de sécurité

Être capable de configurer un serveur Windows

Avoir de l'expérience dans la configuration et la gestion de périphériques de passerelle réseau

Avoir une connaissance des réseaux généraux Windows et Microsoft Active Directory

Si vous ne savez pas si vous remplissez les conditions préalables nécessaires pour suivre ce cours, veuillez nous envoyer un e-mail à training.ecs.fr@arrow.com et nous serons heureux de vous aider.

PROGRAMME :

Module 1 : Menaces de sécurité et comment l'UTM s'en protège
- Identifier les menaces courantes
- Reconnaître la protection fournie par Sophos UTM

Module 2 : Premiers pas avec XG Firewall
- Effectuer la configuration de base du système
- Créer des définitions de réseau, de service et de temps
- Configurer les interfaces sur l'UTM
- Configurer comment plusieurs liens Internet sont utilisés par l'UTM

Laboratoires
- Configurer un UTM à l'aide de l'assistant de configuration
- Naviguer dans WebAdmin
- Configurer les paramètres système
- Créer des définitions
- Configurer les interfaces et le routage

Module 3 : Protection du réseau
- Créer des règles de pare-feu et NAT
- Configurer la prévention des intrusions et la protection avancée contre les menaces (ATP)

Laboratoires
- Créer des règles de pare-feu

- Configurer le NAT
- Démontrer la protection avancée contre les menaces
- Configurer la prévention des intrusions (IPS)

Module 4 : Connexions de site à site

- Expliquer les options VPN disponibles pour les connexions de site à site
- Configurer un VPN de site à site SSL et IPsec
- Comprendre le déploiement et la configuration de RED

Laboratoires

- Configurer un VPN SSL de site à site
- Configurer un VPN de site à site IPsec

Module 5 : Authentification

- Décrire les méthodes d'authentification disponibles sur l'UTM
- Configurer les utilisateurs et groupes locaux
- Activer l'authentification des services d'annuaire
- Configurer l'authentification unique pour le filtrage Web
- Activer les mots de passe à usage unique

Laboratoires (40 min)

- Configurer l'authentification locale et le Portail Utilisateur
- Configurer l'authentification externe à l'aide d'Active Directory
- Activer les mots de passe à usage unique
- Configurer Active Directory SSO pour le filtrage Web

Module 6 : Protection Web et contrôle des applications

- Décrire les principales fonctionnalités du module Web Protection
- Configurer le filtrage Web avec plusieurs politiques
- Activer le contrôle des applications et créer des règles pour bloquer les applications

Laboratoires

- Déployer le certificat CA HTTPS
- Configurer les actions de filtrage
- Gérer les sites Web
- Configurer les politiques Web
- Configurer les profils Web
- Configurer le contrôle des applications

Module 7 : Protection des e-mails

- Activer le rapport de quarantaine
- Configurer une simple protection des e-mails
- Configurer la protection des données
- Configurer le cryptage SPX
- Configurer les profils SMTP

Laboratoires (65 min)

- Activer et configurer les résumés de quarantaine
- Configurer une politique de protection des e-mails pour le mode MTA

- Crypter les e-mails qui correspondent à une liste de contrôle des données à l'aide de SPX
- Gérer les éléments mis en quarantaine en tant qu'utilisateur

Module 8 : Accès sans fil et à distance

- Décrire les principales capacités de la protection sans fil
- Configurer les points d'accès sans fil
- Créer des points d'accès
- Configurer l'accès à distance SSL
- Activer le portail VPN HTML5
- Décrire la prise en charge des clients VPN Cisco natifs

Laboratoires (25 min)

- Configurer un VPN d'accès distant SSL
- Configurer le portail VPN HTML5

Module 9 : Protection des terminaux et contrôle mobile

- Installer et lancer le client de point de terminaison
- Gérer les terminaux protégés
- Décrire l'intégration entre Sophos Mobile Control et l'UTM
- Répertorier les types de configuration pouvant être poussés vers Sophos Mobile Control

Module 10 : Journalisation, rapports et dépannage

- Comprendre la surveillance et la gestion à distance dans l'UTM
- Examiner les options de journalisation
- Comprendre les rapports intégrés et iView
- Examiner les outils de dépannage disponibles

Laboratoires (30 min)

- Exécuter, personnaliser et planifier des rapports
- Afficher et gérer les fichiers journaux
- Utiliser des outils d'assistance intégrés

TEST AND CERTIFICATION :

Attestation

Pour devenir Sophos Certified Administrator, les stagiaires doivent passer et réussir une évaluation en ligne. L'évaluation teste leurs connaissances à la fois du contenu présenté et du contenu pratique. La note de passage pour l'évaluation est de 80 % et est limitée à 4 tentatives.

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 SOPHOS

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 gérer les tâches courantes au quotidien.