EduGroupe
Accompagner pour réussir

Sécurité des systèmes et des réseaux

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'exploitation Windows et/ou Linux
- Connaissances de base des réseaux TCP/IP
- Expérience en administration système ou réseau recommandée.

PROFIL DES STAGIAIRES

- Administrateurs systèmes et réseaux
- Techniciens et ingénieurs infrastructures
- Administrateurs sécurité
- Responsables informatiques
- Exploitants et équipes de production informatique
- Toute personne souhaitant renforcer la sécurité des infrastructures systèmes et réseaux

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les principales menaces pesant sur les infrastructures informatiques.
- Identifier les vulnérabilités des systèmes et des réseaux.
- Mettre en œuvre les bonnes pratiques de sécurisation des environnements Windows et Linux.
- Renforcer la sécurité des architectures réseau.
- Déployer des mécanismes de protection des accès et des données.
- Détecter les événements de sécurité et réagir efficacement.
- Contribuer au maintien en condition de sécurité des systèmes d'information.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques, de retours d'expérience et de bonnes pratiques issues du terrain.
- Études de cas inspirées de situations réelles rencontrées par des RSSI et des responsables cybersécurité.
- Ateliers pratiques de construction d'une gouvernance sécurité, d'analyse des risques et de gestion d'incidents.
- Exercices collaboratifs de pilotage de crise cyber et de prise de décision.
- Échanges d'expériences entre participants et analyse de cas concrets d'organisations publiques et privées.

- Remise de modèles et outils directement réutilisables en entreprise (PSSI, tableaux de bord, plans d'actions, matrices de risques).

FORMATEUR

- Consultant expert en cybersécurité disposant d'une expérience significative dans l'administration sécurisée des systèmes Windows et Linux, l'architecture réseau, la gestion des vulnérabilités, la supervision de sécurité et la réponse aux incidents.

METHODE D'EVALUATION DES ACQUIS

- Évaluation initiale des connaissances en début de formation.
- Validation progressive des acquis à travers les exercices et ateliers réalisés durant les trois jours.
- Études de cas permettant de mesurer la capacité à appliquer les concepts de gouvernance, de gestion des risques et de pilotage de la cybersécurité.
- Questionnaire d'évaluation des connaissances en fin de formation.
- Débriefing collectif et individuel des travaux réalisés..

CONTENU DU COURS

Jour 1 : Comprendre les menaces et sécuriser les systèmes (7h)

Module 1 : Panorama des menaces et fondamentaux de la cybersécurité (2h)

Objectifs

- Comprendre les principales menaces actuelles.
- Identifier les impacts potentiels sur les systèmes d'information.
- Assimiler les principes fondamentaux de la sécurité informatique.

Contenu

- Évolution de la cybercriminalité.
- Typologie des cyberattaques.
- Ransomwares, phishing, malwares et attaques ciblées.
- Menaces internes et externes.
- Principes de confidentialité, intégrité et disponibilité (CIA).
- Défense en profondeur et réduction de la surface d'attaque.
- Principe du moindre privilège.

Mise en pratique

Brainstorming collectif :

- Analyse d'incidents cyber récents.
- Identification des vulnérabilités exploitées et des mesures préventives associées.

Module 2 : Sécuriser les systèmes Windows et Linux (3h)

Objectifs

- Renforcer la sécurité des systèmes d'exploitation.
- Réduire les risques liés aux mauvaises configurations.
- Appliquer les bonnes pratiques de durcissement.

Contenu

- Gestion des comptes utilisateurs et des privilèges.
- Configuration sécurisée des postes et serveurs.
- Hardening des systèmes Windows et Linux.
- Gestion des mises à jour et correctifs.
- Désactivation des services inutiles.

- Journalisation et audit des événements.
- Protection contre les logiciels malveillants.

Mise en pratique

Atelier technique :

- Analyse d'une configuration système.
- Identification des faiblesses de sécurité.
- Élaboration d'un plan de durcissement.

Module 3 : Gestion des vulnérabilités système (1h)

Objectifs

- Comprendre le cycle de vie des vulnérabilités.
- Prioriser les actions de correction.

Contenu

- Vulnérabilités, failles et exposition aux risques.
- Notions de CVE et CVSS.
- Veille de sécurité.
- Gestion des correctifs.
- Priorisation des traitements.

Mise en pratique

Étude de cas :

- Analyse d'un bulletin de sécurité et définition des actions correctives.

Module 4 : Atelier de synthèse systèmes (1h)

Objectifs

- Consolider les acquis de la première journée.

Mise en pratique

Cas pratique :

- Audit simplifié d'un serveur présentant plusieurs défauts de configuration.

Jour 2 : Sécuriser les infrastructures réseau (7h)

Module 5 : Fondamentaux de la sécurité réseau (2h)

Objectifs

- Comprendre les principes d'une architecture réseau sécurisée.
- Identifier les points d'exposition d'un réseau.

Contenu

- Architecture réseau et zones de confiance.
- Segmentation et cloisonnement.
- DMZ et réseaux internes.
- Principes du modèle Zero Trust.
- Réduction des surfaces d'exposition.

Mise en pratique

Atelier :

- Analyse critique d'une architecture réseau d'entreprise.

Module 6 : Contrôle et filtrage des flux réseau (2h)

Objectifs

- Maîtriser les mécanismes de contrôle des communications.
- Construire une politique de filtrage efficace.

Contenu

- Fonctionnement des pare-feu.

- ACL et filtrage réseau.
- Proxy et filtrage applicatif.
- VPN et accès distants sécurisés.
- Sécurisation des accès d'administration.

Mise en pratique

Travail en groupe :

- Construction d'une matrice de flux réseau autorisés.

Module 7 : Sécurisation des services réseau (2h)

Objectifs

- Sécuriser les principaux services réseau.
- Réduire les risques liés aux protocoles exposés.

Contenu

- DNS et DHCP sécurisés.
- Sécurisation des services Web.
- Protocoles sécurisés : HTTPS, SSH, SFTP.
- Gestion des certificats.
- Désactivation des protocoles obsolètes.

Mise en pratique

Atelier :

- Analyse de services réseau exposés et recommandations de sécurisation.

Module 8 : Atelier d'architecture sécurisée (1h)

Objectifs

- Mettre en application les notions de sécurité réseau.

Mise en pratique

Cas pratique :

- Conception d'une architecture réseau sécurisée pour une PME.

Jour 3 : Gestion des accès, supervision et protection des données (7h)

Module 9 : Gestion des identités et des accès (IAM) (2h)

Objectifs

- Contrôler efficacement les accès aux ressources.
- Réduire les risques liés aux comptes à privilèges.

Contenu

- Authentification et autorisation.
- Gestion des rôles et des habilitations.
- Comptes privilégiés.
- Authentification multifacteur (MFA).
- Gestion du cycle de vie des identités.

Mise en pratique

Atelier :

- Construction d'une matrice d'habilitation.

Module 10 : Protection des données et chiffrement (2h)

Objectifs

- Sécuriser les données sensibles de l'organisation.
- Comprendre les mécanismes de chiffrement.

Contenu

- Classification des données.

- Chiffrement des données au repos et en transit.
- Gestion des certificats.
- Protection des sauvegardes.
- Prévention des pertes de données.

Mise en pratique

Étude de cas :

- Choix des mécanismes de protection adaptés à différents types de données.

Module 11 : Supervision et détection des incidents (2h)

Objectifs

- Identifier les événements suspects.
- Comprendre les principes de la supervision de sécurité.

Contenu

- Journaux systèmes et réseau.
- Collecte des événements.
- Corrélation des logs.
- Introduction aux SIEM.
- Indicateurs de compromission (IoC).
- Détection des comportements anormaux.

Mise en pratique

Atelier :

- Analyse d'extraits de journaux de sécurité.
- Identification d'activités suspectes.

Module 12 : Atelier de détection d'incidents (1h)

Objectifs

- Mettre en pratique les méthodes de supervision.

Mise en pratique

Cas pratique :

- Investigation d'un scénario de compromission à partir de journaux système et réseau.

Jour 4 : Réagir aux incidents et renforcer la résilience (7h)

Module 13 : Gestion des vulnérabilités et maintien en condition de sécurité (2h)

Objectifs

- Structurer un processus de gestion des vulnérabilités.
- Maintenir durablement le niveau de sécurité.

Contenu

- Identification des vulnérabilités.
- Veille de sécurité.
- Scans de vulnérabilités.
- Priorisation des corrections.
- Gestion du cycle de remédiation.

Mise en pratique

Atelier :

- Construction d'un plan de traitement des vulnérabilités.

Module 14 : Réponse aux incidents de sécurité (2h)

Objectifs

- Organiser une réponse efficace face à un incident.
- Limiter les impacts opérationnels.

Contenu

- Cycle de vie d'un incident.
- Détection et qualification.
- Confinement.
- Éradication.
- Retour à la normale.
- Retour d'expérience.

Mise en pratique

Simulation :

- Gestion d'un incident de type ransomware.

Module 15 : Continuité d'activité et résilience (2h)

Objectifs

- Préparer l'organisation à faire face à une interruption majeure.
- Renforcer la résilience des infrastructures.

Contenu

- Sauvegardes et restauration.
- PCA et PRA.
- Gestion de crise.
- Tests de reprise.
- Amélioration continue.

Mise en pratique

Atelier :

- Construction d'un scénario de reprise d'activité.

Module 16 : Cas pratique de synthèse (1h)

Objectifs

- Mobiliser l'ensemble des compétences acquises.

Mise en pratique

Exercice fil rouge :

À partir d'un système d'information fictif :

- Analyse des vulnérabilités.
- Identification des risques.
- Définition des mesures de protection.
- Élaboration d'un plan de sécurisation.
- Présentation des recommandations au groupe.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.