Fondamentaux Cybersécurité et SOC

Durée : 3 jours (21 heures)

CONNAISSANCES PREALABLES

- Connaissances générales de l'environnement informatique.
- Notions de base en systèmes et réseaux.
- Une première expérience dans l'administration ou le support informatique constitue un plus.

PROFIL DES STAGIAIRES

- Futurs analystes SOC
- Techniciens et administrateurs systèmes et réseaux
- Techniciens support informatique
- Responsables informatiques souhaitant développer leurs compétences en cybersécurité
- Collaborateurs en reconversion vers les métiers de la cybersécurité
- Toute personne souhaitant comprendre les fondamentaux de la cybersécurité opérationnelle et du fonctionnement d'un SOC.

OBJECTIFS

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

- Comprendre les fondamentaux de la cybersécurité et les principales menaces.
- Identifier les vulnérabilités courantes des systèmes d'information.
- Comprendre les principes de défense en profondeur.
- Découvrir le fonctionnement d'un Security Operations Center (SOC).
- Comprendre les mécanismes de détection des incidents de sécurité.
- Analyser des événements de sécurité et des journaux d'activité.
- Identifier les indicateurs de compromission (IoC).
- Participer à la détection et à la qualification d'incidents cyber.
- Comprendre le rôle de l'analyste SOC dans une organisation.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et de démonstrations.
- Études de cas inspirées d'incidents réels.
- Exercices d'analyse d'événements de sécurité.
- Ateliers collaboratifs de qualification d'incidents.
- Mises en situation d'analyste SOC.
- Cas fil rouge permettant de suivre le cycle complet d'un incident cyber.

FORMATEUR

- Consultant expert en cybersécurité opérationnelle disposant d'une expérience significative dans les domaines du SOC, de la supervision de sécurité, de la gestion des incidents, de la détection des menaces et de la réponse aux cyberattaques.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation continue des acquis à travers les ateliers et exercices.
- Quiz de validation des connaissances.
- Évaluation des compétences lors des analyses d'incidents.
- Cas pratique de synthèse en fin de formation.
- Questionnaire d'évaluation des acquis.

CONTENU DU COURS

Jour 1 : Comprendre les fondamentaux de la cybersécurité (7h)

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

Objectifs

- Comprendre les enjeux de la cybersécurité.
- Identifier les principales menaces visant les organisations.

Contenu

- Définition de la cybersécurité.
- Évolution des cybermenaces.
- Cybercriminalité et acteurs de la menace.
- Ransomwares.
- Phishing et ingénierie sociale.
- Malwares et attaques ciblées.
- Conséquences opérationnelles, financières et réglementaires.

Mise en pratique

Brainstorming collectif :

- Analyse de cyberattaques récentes et identification des facteurs de compromission.

Module 2 : Comprendre les vulnérabilités et les mécanismes d'attaque (2h)

Objectifs

- Identifier les principales vulnérabilités exploitées par les attaquants.
- Comprendre les différentes phases d'une attaque.

Contenu

- Vulnérabilités systèmes.
- Vulnérabilités réseau.
- Vulnérabilités applicatives.
- Cycle de vie d'une attaque.
- Kill Chain.
- MITRE ATT&CK (introduction).
- Surface d'attaque.

Mise en pratique

Atelier :

- Cartographie d'un scénario d'attaque selon les différentes phases de compromission.

Module 3 : Les principes de protection des systèmes d'information (2h)

Objectifs

- Comprendre les mécanismes de défense utilisés dans les organisations.

Contenu

- Confidentialité, intégrité et disponibilité.
- Défense en profondeur.
- Gestion des accès.
- Authentification multifacteur.
- Gestion des correctifs.
- Sauvegardes et résilience.
- Sensibilisation des utilisateurs.

Mise en pratique

Étude de cas :

- Identification des mesures de sécurité adaptées à différents scénarios de risques.

Module 4 : Atelier de synthèse cybersécurité (1h)

Objectifs

- Consolider les acquis de la première journée.

Mise en pratique

Cas pratique :

- Analyse globale de la posture de sécurité d'une PME fictive.

Jour 2 : Découvrir le fonctionnement d'un SOC (7h)

Module 5 : Introduction au Security Operations Center (SOC) (2h)

Objectifs

- Comprendre le rôle et l'organisation d'un SOC.

Contenu

- Missions d'un SOC.
- Organisation et niveaux d'analystes.
- Processus de supervision.
- Détection et qualification des incidents.
- Relations avec les équipes CERT, CSIRT et RSSI.

Mise en pratique

Brainstorming :

- Définition des fonctions essentielles d'un SOC moderne.

Module 6 : Collecte et supervision des événements de sécurité (2h)

Objectifs

- Comprendre comment sont collectées et exploitées les données de sécurité.

Contenu

- Journaux systèmes et réseaux.
- Sources de logs.
- Centralisation des événements.
- Corrélation des données.
- Présentation des SIEM.
- Cas d'usage de supervision.

Mise en pratique

Atelier :

- Analyse d'événements de sécurité issus de différentes sources.

Module 7 : Détection des menaces et qualification des alertes (2h)

Objectifs

- Identifier les événements suspects.
- Comprendre le processus de qualification d'une alerte.

Contenu

- Indicateurs de compromission (IoC).
- Faux positifs et faux négatifs.
- Qualification des alertes.
- Priorisation des incidents.
- Escalade et gestion des tickets.

Mise en pratique

Travaux pratiques :

- Qualification d'alertes de sécurité simulées.

Module 8 : Atelier Analyste SOC Niveau 1 (1h)

Objectifs

- Mettre en pratique les missions d'un analyste SOC.

Mise en pratique

Simulation :

- Analyse d'un flux d'alertes et qualification des événements.

Jour 3 : Détecter et investiguer un incident de sécurité (7h)

Module 9 : Analyse et investigation des incidents cyber (2h)

Objectifs

- Comprendre les méthodes d'investigation.
- Identifier les éléments utiles à l'analyse.

Contenu

- Cycle de gestion d'un incident.
- Recherche d'indices de compromission.
- Analyse des événements.
- Reconstitution d'une chronologie.
- Collecte des preuves.

Mise en pratique

Étude de cas :

- Investigation d'un incident simulé.

Module 10 : Réponse aux incidents et coordination opérationnelle (2h)

Objectifs

- Comprendre les actions mises en œuvre lors d'un incident.

Contenu

- Détection.
- Confinement.
- Éradication.
- Rétablissement.
- Retour d'expérience.
- Rôle des équipes de réponse à incident.

Mise en pratique

Atelier :

- Élaboration d'un plan d'action face à une compromission.

Module 11 : Threat Intelligence et veille cyber (2h)

Objectifs

- Comprendre l'apport du renseignement sur les menaces.

Contenu

- Concepts de Threat Intelligence.
- Sources de renseignement.
- Indicateurs techniques.
- Veille de sécurité.
- Utilisation des IoC dans un SOC.

Mise en pratique

Travaux pratiques :

- Analyse d'indicateurs de compromission issus d'une campagne d'attaque.

Module 12 : Cas pratique de synthèse – Simulation SOC (1h)

Objectifs

- Mobiliser l'ensemble des compétences acquises.

Mise en pratique

Exercice fil rouge :

À partir d'un scénario de compromission :

- Analyse des alertes.
- Qualification des événements.
- Identification des IoC.
- Investigation de l'incident.
- Proposition d'actions de remédiation.
- Présentation des conclusions 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.