Gestion des incidents et des crises cyber

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'information et des infrastructures réseau.
- Connaissances de base en cybersécurité.
- Une expérience dans l'exploitation informatique, l'administration système ou la sécurité est recommandée.

PROFIL DES STAGIAIRES

- RSSI et responsables cybersécurité
- DSI et responsables informatiques
- Responsables infrastructures et exploitation
- Analystes SOC et équipes CERT/CSIRT
- Responsables PCA/PRA
- Responsables risques et conformité
- Chefs de projets sécurité
- Managers impliqués dans la gestion de crise.

OBJECTIFS

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

- Comprendre les mécanismes et les impacts des incidents de cybersécurité.
- Mettre en œuvre un processus structuré de gestion des incidents.
- Organiser une cellule de gestion de crise cyber.
- Coordonner les actions techniques, organisationnelles et de communication.
- Gérer efficacement les différentes phases d'une crise cyber.
- Assurer la continuité des activités et le retour à la normale.
- Réaliser un retour d'expérience et améliorer durablement la résilience de l'organisation.
- Construire un dispositif de réponse aux incidents adapté aux enjeux de l'entreprise.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et de retours d'expérience terrain.
- Études de cas basées sur des incidents cyber réels.
- Exercices collaboratifs et mises en situation.
- Simulations progressives de gestion d'incidents et de crises.
- Jeux de rôle impliquant les différentes parties prenantes.
- Cas fil rouge permettant de mettre en œuvre l'ensemble des compétences acquises.

FORMATEUR

- Consultant expert en cybersécurité disposant d'une expérience significative dans la gestion d'incidents de sécurité, la réponse à incident, la gestion de crise cyber, la continuité d'activité et l'accompagnement des organisations confrontées à des cyberattaques majeures.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation continue des acquis à travers les ateliers et simulations.
- Quiz intermédiaires de contrôle des connaissances.
- Évaluation des compétences lors des exercices de gestion d'incident.
- Cas pratique fil rouge de gestion de crise.
- Questionnaire d'évaluation des acquis en fin de formation.

CONTENU DU COURS

Jour 1 : Comprendre les incidents cyber et structurer la réponse (7h)

Module 1 : Panorama des incidents et menaces cyber (2h)

Objectifs

- Comprendre les principales menaces actuelles.
- Identifier les impacts potentiels sur les activités de l'entreprise.

Contenu

- Évolution de la menace cyber.
- Typologie des incidents de sécurité.
- Ransomwares.
- Compromissions de comptes.
- Fuites de données.
- Attaques par déni de service.
- Impacts financiers, juridiques et opérationnels.

Mise en pratique

Brainstorming collectif :

- Analyse de cyberattaques médiatisées.
- Identification des facteurs ayant aggravé ou limité les impacts.

Module 2 : Organiser la gestion des incidents de sécurité (2h)

Objectifs

- Structurer un processus de gestion des incidents.
- Définir les rôles et responsabilités.

Contenu

- Détection et signalement.
- Qualification des incidents.
- Classification et priorisation.
- Processus d'escalade.
- Constitution d'une équipe de réponse.
- Coordination entre métiers et équipes techniques.

Mise en pratique

Atelier :

- Construction d'un processus de gestion d'incident adapté à son organisation.

Module 3 : Détection, analyse et qualification des incidents (2h)

Objectifs

- Comprendre les mécanismes de détection.
- Identifier les indicateurs de compromission.

Contenu

- Sources d'information.
- Journaux et événements de sécurité.
- SIEM et supervision.
- IoC (Indicators of Compromise).
- Qualification et criticité.
- Collecte des premières preuves.

Mise en pratique

Étude de cas :

- Analyse d'événements de sécurité et qualification d'incidents.

Module 4 : Atelier de gestion d'incident (1h)

Objectifs

- Appliquer les notions étudiées durant la journée.

Mise en pratique

Simulation :

- Traitement d'un incident de sécurité depuis sa détection jusqu'à sa qualification.

Jour 2 : Répondre efficacement à un incident cyber (7h)

Module 5 : Confinement et limitation des impacts (2h)

Objectifs

- Limiter la propagation d'un incident.
- Préserver les capacités opérationnelles.

Contenu

- Stratégies de confinement.
- Isolement des systèmes.
- Protection des actifs critiques.
- Arbitrages opérationnels.
- Gestion des accès compromis.

Mise en pratique

Atelier :

- Définition des mesures de confinement adaptées à différents scénarios.

Module 6 : Investigation et analyse de l'incident (2h)

Objectifs

- Comprendre les causes et le périmètre de compromission.

Contenu

- Investigation numérique.
- Chronologie des événements.
- Recherche de traces.
- Identification du vecteur d'attaque.
- Détermination du périmètre impacté.

Mise en pratique

Étude de cas :

- Reconstitution d'une chronologie d'attaque à partir d'éléments techniques.

Module 7 : Éradication et retour à la normale (2h)

Objectifs

- Supprimer les causes de compromission.
- Restaurer les services de manière sécurisée.

Contenu

- Éradication des éléments malveillants.
- Correction des vulnérabilités.
- Vérification de l'intégrité des systèmes.
- Réintégration progressive des services.
- Contrôles post-rétablissement.

Mise en pratique

Atelier :

- Élaboration d'un plan de remédiation et de rétablissement.

Module 8 : Simulation de réponse à incident (1h)

Objectifs

- Mobiliser les compétences acquises.

Mise en pratique

Exercice scénarisé :

- Gestion complète d'un incident de type ransomware.

Jour 3 : Organiser et piloter une crise cyber (7h)

Module 9 : Comprendre la gestion de crise cyber (2h)

Objectifs

- Identifier les spécificités d'une crise cyber.
- Comprendre les enjeux décisionnels.

Contenu

- Différence entre incident et crise.
- Critères de déclenchement d'une cellule de crise.
- Gouvernance de crise.
- Prise de décision sous contrainte.
- Coordination des parties prenantes.

Mise en pratique

Brainstorming :

- Identification des critères de déclenchement d'une cellule de crise.

Module 10 : Structurer une cellule de crise cyber (2h)

Objectifs

- Organiser efficacement les rôles et responsabilités.

Contenu

- Composition de la cellule de crise.
- Rôle de la direction.
- Rôle du RSSI.
- Coordination juridique, RH et communication.
- Pilotage des actions.

Mise en pratique

Atelier :

- Construction d'une cellule de crise adaptée à une organisation.

Module 11 : Communication de crise cyber (2h)

Objectifs

- Maîtriser la communication interne et externe.

Contenu

- Communication avec les collaborateurs.
- Communication avec les clients et partenaires.
- Communication réglementaire.
- Relations avec les autorités.
- Gestion de la communication médiatique.

Mise en pratique

Jeu de rôle :

- Préparation de communications de crise selon différents scénarios.

Module 12 : Exercice de gestion de crise (1h)

Objectifs

- Mettre en œuvre les mécanismes de pilotage de crise.

Mise en pratique

Simulation :

- Activation et animation d'une cellule de crise cyber.

Jour 4 : Résilience, continuité d'activité et retour d'expérience (7h)

Module 13 : Continuité et reprise d'activité (2h)

Objectifs

- Préparer l'organisation à maintenir ses activités essentielles.

Contenu

- PCA et PRA.
- Analyse d'impact métier.
- Priorisation des activités critiques.
- Stratégies de reprise.
- Tests et exercices.

Mise en pratique

Atelier :

- Construction d'un scénario simplifié de continuité d'activité.

Module 14 : Retour d'expérience et amélioration continue (2h)

Objectifs

- Capitaliser sur les incidents et crises.

Contenu

- Méthodologie RETEX.
- Analyse des causes profondes.
- Identification des axes d'amélioration.
- Mise à jour des procédures.
- Renforcement de la posture de sécurité.

Mise en pratique

Étude de cas :

- Réalisation d'un RETEX complet à partir d'un incident simulé.

Module 15 : Cas fil rouge : Gestion complète d'une crise cyber (2h)

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Mise en pratique
Exercice de synthèse :

- Détection.
- Qualification.
- Gestion d'incident.
- Activation de la cellule de crise.
- Communication.
- Reprise d'activité.
- Retour d'expérience.

Module 16 : Restitution et débriefing (1h)

Objectifs

- Présenter les décisions prises.
- Évaluer la pertinence des actions menées.

Mise en pratique
Présentation orale :

- Restitution des travaux devant le groupe.
- Débriefing collectif.
- Identification des bonnes pratiques et axes d'amélioration.

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.