FICHE TECHNIQUE DE FORMATION
Réponse aux Incidents

Objectifs de la Formation:

Comprendre les principes et les méthodologies de réponse aux incidents.

Développer des compétences pour détecter, analyser et répondre aux incidents de sécurité.

Maîtriser les techniques et les outils pour une gestion efficace des incidents.

Public Cible:

Responsables de la sécurité, administrateurs réseau, analystes SOC, toute personne impliquée dans la gestion des incidents de sécurité.

Prérequis:

Connaissances de base en cybersécurité et en gestion des systèmes d'information.

Méthodologie Pédagogique:

Exposés théoriques, démonstrations pratiques, ateliers interactifs, études de cas.

Programme de la Formation:

1. Introduction à la Réponse aux Incidents

Concepts de Base : Comprendre les principes de la réponse aux incidents.

Cycle de Vie des Incidents : Présentation des étapes du cycle de vie de la réponse aux incidents.

2. Préparation à la Réponse aux Incidents

Plan de Réponse aux Incidents : Élaboration d'un plan de réponse aux incidents.

Équipe de Réponse aux Incidents (IRT) : Formation et organisation de l'équipe de réponse.

3. Détection des Incidents

Techniques de Détection : Utilisation des techniques pour détecter les incidents de sécurité.

Outils de Surveillance : Introduction aux outils de surveillance pour la détection des incidents (SIEM, IDS).

4. Analyse des Incidents

Techniques d'Analyse : Techniques pour analyser et comprendre les incidents.

Analyse Forensique : Utilisation des techniques forensiques pour l'analyse des incidents.

5. Containment, Eradication et Récupération

Containment des Incidents : Stratégies pour contenir les incidents.

Eradication des Menaces : Techniques pour éradiquer les menaces et récupérer les systèmes compromis.

6. Communication des Incidents

Rapports d'Incidents : Techniques pour rédiger des rapports d'incidents.

Communication avec les Parties Prenantes : Stratégies pour communiquer avec les parties prenantes pendant un incident.

7. Leçons Apprises et Amélioration

Analyse Post-Incident : Techniques pour analyser les incidents après leur résolution.

Amélioration Continue : Stratégies pour améliorer les processus de réponse aux incidents.

8. Applications Pratiques

Ateliers de Détection et Analyse : Exercices pratiques pour détecter et analyser les incidents.

Simulations de Réponse aux Incidents : Jeux de rôle pour pratiquer la réponse aux incidents.

9. Outils de Réponse aux Incidents

Introduction aux Outils Forensiques : Présentation des outils forensiques pour l'analyse des incidents.

Automatisation de la Réponse aux Incidents : Techniques pour automatiser la réponse aux incidents.

10. Évaluation Finale