Formation Gestion des incidents de sécurité & réponse à incident (CSIRT)

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : GISI

Niveau : Moyen

intra

Mise à jour le 30/12/25

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en cybersécurité
- Compréhension des systèmes d'information
- Expérience IT ou sécurité recommandée

Objectifs

Objectifs pédagogiques :

- Comprendre le rôle et les missions d'un CSIRT
- Identifier les différents types d'incidents de sécurité
- Comprendre le cycle de vie de la gestion d'incident
- Connaître les bonnes pratiques de réponse à incident
- Appréhender les enjeux organisationnels et humains d'un incident cyber

Objectifs opérationnels :

- Détecter et qualifier un incident de sécurité
- Appliquer une méthodologie de réponse à incident
- Contenir et limiter l'impact d'un incident
- Organiser la communication interne et externe
- Contribuer à l'amélioration continue de la sécurité après incident

Programme

Jour 1 – Fondamentaux de la gestion d'incident & organisation CSIRT

Introduction à la gestion des incidents de sécurité

Qu'est-ce qu'un incident de sécurité ?
Différence incident / alerte / crise cyber
Typologies d'incidents (malware, intrusion, fuite, ransomware…)
Impacts techniques, métiers, juridiques et image

Organisation CSIRT / CERT

Rôle et missions d'un CSIRT
CSIRT interne vs externe
Processus et responsabilités
Coordination avec les équipes IT, métiers et direction

Cycle de vie d'un incident de sécurité

Préparation
Détection et analyse
Confinement
Éradication
Rétablissement
Retour d'expérience (RETEX)

Atelier pratique

Analyse de scénarios d'incidents réels
Qualification du type d'incident
Identification des parties prenantes

Jour 2 – Réponse à incident, communication et retour d'expérience

Détection et analyse des incidents

Formation Gestion des incidents de sécurité & réponse à incident (CSIRT)

Sources de détection (logs, alertes, utilisateurs)
Qualification et priorisation des incidents
Analyse initiale et collecte d’informations
Notions de preuves et traçabilité

Contention, éradication et reprise

Actions de confinement
Limitation de la propagation
Nettoyage et correction
Retour à un état opérationnel sécurisé

Communication et gestion de crise

Communication interne
Communication externe (clients, partenaires)
Interaction avec les autorités et prestataires
Documentation de l’incident

Retour d’expérience et amélioration continue

Analyse post-incident
Identification des causes racines
Plans d’actions correctifs
Mise à jour des procédures et sensibilisation

Atelier pratique

Simulation complète d’un incident de sécurité
Élaboration d’un plan de réponse à incident
Restitution collective et RETEX