VISIO - Gérer vos incidents de cybersécurité pour les collectivités

TOO141GICC

En Visio-conférence, de 9h00 à 17h00

A distance - Synchrone

Inscrivez-vous au moins 2 mois avant le début du stage pour bénéficier d'un tarif préférentiel
Délai d'accès : Inscription jusqu'à la veille du démarrage de la session
Contactez Gaëlle (01 53 39 14 18,gaelle.ducher@adiaj.org) ou Julien (01 53 39 14 24, julien.laudat@adiaj.org) pour réaliser cette formation en INTRA

Objectifs

- Comprendre les étapes de gestion d'un incident de cybersécurité
- Apprendre à détecter, répondre et remédier efficacement à une cyberattaque
- Élaborer un plan de gestion des incidents pour les collectivités

Public Visé

Responsables informatiques, agents techniques, et gestionnaires de crise dans les collectivités territoriales

Pré Requis

Avoir des connaissances en cybersécurité, avoir suivi la formation "Fondamentaux de la cybersécurité pour les collectivités territoriales", ou justifier d'une expérience suffisante.

Objectifs pédagogiques

Comprendre les étapes de gestion d'un incident de cybersécurité
Apprendre à détecter, répondre et remédier efficacement à une cyberattaque
Élaborer un plan de gestion des incidents pour les collectivités

Méthodes et moyens pédagogiques

- Apports de connaissances théoriques
- Cas pratiques
- Echanges autour des questions/réponses
- Support documentaire via PADLET (présentation, fiches méthodologiques, modèle de plan de gestion des incidents adapté aux collectivités, liste des outils recommandés pour surveiller et gérer les incidents (IDS, SIEM, etc.), contact des organismes compétents (ANSSI, Cybermalveillance.gouv.fr)
- Encadrement assuré par l'ADIAJ Formation et/ou le formateur

Déroulement pédagogique et prérequis techniques de la classe virtuelle, à distance

- Chaque jour est séquencé en 4 séquences d'1h30. Pause de 15 à 30 minutes le matin et l'après-midi. Pause méridienne d'une heure.
- Chaque stagiaire sera invité à rejoindre une salle digitale, via un lien d'accès, un ID de réunion communiqué par mail, au minimum 15 minutes avant le début de la session, pour permettre de paramétrer sereinement sa connexion.
- Chaque stagiaire reste maître de sa connexion visuelle (caméra) et sonore (son), pour permettre de suivre en toute autonomie et dans le respect de tous.
- Matériel nécessaire : un ordinateur par stagiaire, une connexion internet, un navigateur compatible, une webcam et un micro.

Qualification Intervenant.e.s

Formatrice experte en intelligence artificielle, numérique et

Parcours pédagogique

MATINEE (3H30)

• 9h00 – 9h30 : Introduction et contexte
- Présentation des objectifs de la formation et des participants.
- Pourquoi se préparer ?
  . Les collectivités, cibles privilégiées des cyberattaques.
  . Impacts des incidents sur les services publics et la confiance des citoyens.
- Étude de cas : Exemples concrets d'incidents récents dans les collectivités (ransomware, vol de données).

• 9h30 – 10h30 : Comprendre les incidents de cybersécurité
- Types d'incidents courants :
  . Phishing, ransomware, attaques par déni de service (DDoS), vol d'identifiants.
- Les signes d'un incident :
  . Ordinateurs ralentis, fichiers cryptés, comportements anormaux du système.
- Cycle de vie d'un incident :
  1. Préparation
  2. Détection et analyse
  3. Contention
  4. Éradication et récupération
  5. Apprentissage post-incident

• 10h30 – 10h45 : Pause

• 10h45 – 12h15 : Détection et analyse des incidents
- Détecter une menace :
  . Outils et techniques pour surveiller les systèmes (journaux, systèmes de détection d'intrusion).
  . Indicateurs de compromission (IoC).

- Atelier pratique : Étudier un cas fictif
  . Analyse d'un incident simulé (ex. une attaque par phishing ou ransomware).
  . Identifier les indicateurs de compromission et prioriser les actions.

• 12h15 – 12h30 : Synthèse de la matinée
- Récapitulatif des étapes de détection et analyse.
- Introduction aux réponses à adopter en cas d'incident.

cybersécurité

• 12h30 – 13h30 : Pause déjeuner

APRES-MIDI (3H30)

• 13h30 – 14h30 : Réponse et gestion de l'incident

- Agir rapidement et efficacement :
  . Contenir l'incident pour limiter les impacts.
  . Identifier les systèmes affectés et isoler les éléments compromis.
- Communication en situation de crise :
  . Informer les parties prenantes internes et externes.
  . Interactions avec les autorités compétentes (ANSSI, police).
- Atelier pratique : Simulation de gestion d'un incident
  . Les participants réagissent à un scénario d'attaque en suivant un protocole.

• 14h30 – 15h30 : Récupération et retour à la normale

- Éradication de la menace :
  . Suppression des malwares et restauration des systèmes compromis.

- Plan de reprise après sinistre (PRS) :
  . Récupération des données à partir de sauvegardes.
  . Validation de l'intégrité des systèmes avant leur remise en production.
- Atelier pratique : Élaborer une stratégie de reprise
  . Les participants élaborent un plan de récupération à partir d'un scénario fictif.

• 15h30 – 15h45 : Pause

• 15h45 – 16h45 : Préparation et planification proactive

- Établir un plan de gestion des incidents :
  . Élaborer des procédures écrites pour chaque étape.
  . Identifier les rôles et responsabilités (DSI, agents techniques, décideurs).
- Tests et simulations :
  . Importance des exercices réguliers pour valider le plan.
  . Retour d'expérience (post-mortem) pour améliorer les processus.
- Atelier final : Créer un mini-plan de gestion des incidents
  . Chaque participant rédige une ébauche adaptée à son contexte local.

• 16h45 – 17h00 : Conclusion et évaluation

- Synthèse des apprentissages.

- Questionnaire d'évaluation de la formation.

- Remise d'un guide pratique (modèle de plan de gestion des incidents, fiches outils).

Apprenez à gérer efficacement les incidents de cybersécurité avec la formation ADIAJ. Protégez votre collectivité face aux cybermenaces.

Méthodes et modalités d'évaluation

Chaque stagiaire est invité à émarger sur EasySign, grâce à un mail d'invitation. L'émargement est obligatoire. L'équipe de l'ADIAJ est à votre disposition pour toute aide technique.
Modalités d'évaluation : Chaque stagiaire est invité par mail à compléter :
- Avant la formation : un questionnaire de positionnement via EvalOne, afin que chacun puisse nous faire remonter ses attentes.
- Après la formation : une Evaluation de la satisfaction des stagiaires via EvalOne.
Attestations de la formation : Certificat de réalisation à l'employeur et Attestation de fin de formation à l'apprenant.

Modalités d'Accessibilité

ADIAJ Formation est en capacité d'accueillir ou réorienter toute personne en situation de handicap. Pour assurer un suivi optimal, merci de nous contacter.
Référent handicap : Volodia TOURTCHINE - 01 53 39 14 17 - volodia.tourtchine@adiaj.org

Durée

7.00 Heures

1 Jour

Effectif

De 3 à 14 Personnes

Tarifs (net de taxes)

Inter (Par personne) :	**680.00**
Inter Adhérent (Par personne) :	**640.00**

Contactez-nous !

Gaëlle DUCHER
Responsable Ingénierie Formation
Tél. : 0153391418
Mail : gaelle.ducher@adiaj.org