

PROGRAMME DE FORMATION

Gestion des incidents informatiques et de cybersécurité

Préparer, détecter, traiter et apprendre : de la qualification de l'incident au post-mortem

Durée	5 jours – 35 heures	Horaires	9h00-12h30 / 13h30-17h00
Modalité	Présentiel (ou classe virtuelle)	Effectif	4 à 12 stagiaires
Niveau	Intermédiaire	Sanction	Attestation de fin de formation
Tarif	[à compléter] € HT / stagiaire – intra sur devis	Référence	MGK-GI-01 – v1.0 – 18/10/2026

01 OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le stagiaire sera capable de :

- Définir un incident informatique et un incident de cybersécurité, et les distinguer des notions voisines (événement, problème, demande).
- Élaborer les éléments clés d'un plan de réponse aux incidents : actifs critiques, responsabilités, ressources et stratégies.
- Appliquer le cycle de vie complet d'un incident : détection, enregistrement, classification, priorisation, investigation, résolution et clôture.
- Prioriser un incident à l'aide d'une matrice impact × urgence (P0 à P3) dans le respect des SLA.
- Organiser une équipe de réponse et attribuer les rôles (gestionnaire d'incident, CSIRT, rôles spécialisés).
- Configurer un outil de gestion des incidents et piloter le processus à l'aide d'indicateurs (MTTR, MTTD, respect des SLA...).
- Identifier les obligations légales (RGPD, NIS 2) et préserver les preuves selon les règles de la chaîne de possession.
- Conduire une analyse post-mortem selon une approche « sans reproche » et formuler des actions d'amélioration continue.

02 PUBLIC VISÉ ET PRÉREQUIS

Public visé	▪ Techniciens support et administrateurs systèmes et réseaux ▪ Analystes SOC, membres de CSIRT, responsables sécurité (RSSI, adjoints) ▪ Responsables de production, chefs de projet et managers IT ▪ Toute personne amenée à participer à la gestion d'incidents
Prérequis	▪ Connaissances générales en informatique (systèmes, réseaux, notions de sécurité) ▪ Une première expérience en environnement informatique professionnel est recommandée ▪ Prérequis vérifiés lors de l'entretien préalable et du quiz de positionnement

03 PROGRAMME DÉTAILLÉ

La formation alterne apports théoriques, ateliers, exercices et travaux pratiques. Les journées 3 et 4 sont consacrées en priorité à la mise en pratique ; l'après-midi de la journée 5 est réservé à l'évaluation finale.

JOUR 1

Fondamentaux et préparation

Module 1 – Introduction à la gestion des incidents · Module 2 – Préparation et planification

Objectif de la journée : Maîtriser le vocabulaire et les enjeux de la gestion des incidents, et identifier les éléments constitutifs d'un plan de réponse.

Horaire	Séquence et contenus	Modalité
9h00 – 9h45	Accueil et positionnement - Présentation de la formation, des objectifs et du déroulé - Recueil des attentes et du contexte professionnel de chaque stagiaire - Quiz de positionnement (évaluation des acquis d'entrée)	Évaluation Échange
9h45 – 12h30	Qu'est-ce qu'un incident ? - Définition d'un incident informatique : pannes matérielles, dysfonctionnements logiciels, erreurs humaines, problèmes de performance - L'incident de cybersécurité et les critères DICP : disponibilité, intégrité, confidentialité, preuve - Incident, événement, problème, demande : bien distinguer les notions (référentiel ITIL) - Objectifs de la gestion des incidents : restauration rapide, minimisation de l'impact, optimisation des ressources, satisfaction utilisateurs - Principes fondamentaux : préparation, détection, confinement, atténuation, reprise, apprentissage	Apport Échange
Pause déjeuner – 12h30 / 13h30		
13h30 – 15h15	Préparation : les fondations d'une gestion efficace - Principes clés : traçabilité, engagement de la direction, implication collective, documentation vivante - Sauvegardes isolées et conservation des journaux - Premiers éléments juridiques : recevabilité des preuves et obligations de notification	Apport
15h15 – 17h00	Le plan de réponse aux incidents - Inventaire des actifs critiques : gouvernance, processus métiers, informations sensibles, applications, infrastructure - Attribution des responsabilités et des pouvoirs de décision - Ressources et capacités : expertise interne / externe, forensique, moyens de communication alternatifs - Stratégies opérationnelles : confinement, communication, notification (CERT, APD), restauration, tests - Atelier : identifier les actifs critiques d'une organisation fictive	Apport Atelier

JOUR 2
Le cycle de vie de l'incident et le cadre juridique
Module 3 – De la détection à la clôture · Module 4 – Aspects juridiques et obligations de notification

Objectif de la journée : Décrire et appliquer chaque étape du cycle de vie d'un incident et identifier les obligations légales associées.

Horaire	Séquence et contenus	Modalité
9h00 – 10h30	Détection et enregistrement - Vue d'ensemble du cycle : détection, classification, investigation, résolution, clôture - Sources de détection : supervision, utilisateurs, observation directe, journaux, notifications externes - Enregistrement dans un outil de tickets : informations obligatoires, référence unique, accusé de réception	Apport
10h30 – 12h30	Classification et priorisation - Catégorisation : type, composant, service impacté, cause apparente - Évaluation de l'impact et de l'urgence - Matrice impact × urgence et niveaux de priorité P0 à P3 - Mise en pratique guidée : prioriser une série de cas courts	Apport Exercice
Pause déjeuner – 12h30 / 13h30		
13h30 – 15h00	Investigation, résolution et clôture - Mesures d'urgence : confinement, préservation des preuves, communication ciblée, journal de bord - Analyse approfondie : vecteur, périmètre, chronologie, vulnérabilités exploitées - Le dilemme investigation / rétablissement - Résolution : diagnostic, solution de contournement ou définitive, mise en œuvre, vérification des sauvegardes - Critères de clôture (ISO/IEC 20000) et contenu du rapport de synthèse	Apport
15h00 – 17h00	Aspects juridiques et obligations de notification - RGPD : notification à la CNIL sous 72 heures, information des personnes concernées, sanctions encourues - Directive NIS 2 et réglementations sectorielles (finance, santé, télécoms) - Obligations contractuelles et assurance cyber-risques - Collecte des preuves et chaîne de possession (chain of custody) - Dépôt de plainte et collaboration avec les services spécialisés - Quiz de fin de journée sur les modules 1 à 4	Apport Évaluation

JOUR 3
Organisation, outils et indicateurs – mise en pratique
Module 5 – Rôles et responsabilités · Module 6 – Outils · Module 7 – KPI · Exercices et TP

Objectif de la journée : Organiser une équipe de réponse, outiller le processus et le piloter par les indicateurs, au travers d'exercices et de travaux pratiques.

Horaire	Séquence et contenus	Modalité
9h00 – 10h15	Rôles et responsabilités - Le gestionnaire d'incident (Incident Manager) : coordination, évaluation, communication, amélioration - L'équipe de réponse (CSIRT / ISIRT) : équipe de base, étendue, cellule de crise - Rôles spécialisés : responsable technique, responsable communication, responsable post-mortem	Apport
10h15 – 12h30	Exercice 1 – Construire l'organisation de réponse - À partir d'une étude de cas (PME de 200 salariés), définir l'organigramme de la cellule de réponse - Élaborer la matrice RACI des activités du cycle de vie - Définir la chaîne d'escalade et les critères de déclenchement de la cellule de crise - Restitution en groupe et correction commentée	Exercice Atelier
Pause déjeuner – 12h30 / 13h30		
13h30 – 15h30	TP 1 – Mise en place d'un outil de gestion des incidents - Panorama des outils : suivi (Jira, GLPI), alertes et astreintes (Opsgenie), communication (Slack, Teams), pages de statut - Configuration d'un outil de ticketing (GLPI ou équivalent) : catégories, matrice de priorité, SLA, files d'attente - Paramétrage des notifications et des règles d'escalade automatique - Traitement d'un lot de 15 tickets : enregistrement, catégorisation, priorisation, affectation	TP
15h30 – 17h00	TP 2 – Indicateurs de performance - KPI clés : MTTR, MTTD, taux de respect des SLA, résolution au niveau 1, détection proactive - Indicateurs de qualité et de charge : récurrence, mauvaise catégorisation, escalades inutiles, volumes - Calcul des indicateurs à partir d'un export de tickets (tableur) - Construction d'un tableau de bord de pilotage et interprétation des tendances	TP Exercice

JOUR 4
Simulation d'incident majeur et post-mortem
Module 8 – Gestion de crise · Module 9 – Post-mortem et culture organisationnelle · Exercices et TP

Objectif de la journée : Conduire la réponse à un incident de sécurité majeur de bout en bout, puis en tirer les enseignements par une analyse post-mortem.

Horaire	Séquence et contenus	Modalité
9h00 – 9h30	Briefing de la simulation - Présentation du scénario : attaque par rançongiciel sur le SI d'une organisation fictive - Répartition des rôles : gestionnaire d'incident, responsable technique, communication, juridique, direction	Échange
9h30 – 12h30	Exercice 2 – Simulation de crise sur table (tabletop) - Injections successives d'événements par le formateur (alertes, appels, fuite de données, pression médiatique) - Qualification et priorisation de l'incident, décision de confinement (déconnexion vs investigation) - Tenue de la main courante horodatée et suivi du ticket d'incident - Décisions de notification : CNIL, CERT, assureur, clients - Rédaction des communications de crise interne et externe	Simulation Exercice
Pause déjeuner – 12h30 / 13h30		
13h30 – 15h00	TP 3 – Confinement et préservation des preuves - Isolement d'un poste compromis en environnement virtualisé (segmentation VLAN, règles de filtrage) - Collecte des journaux système et réseau, calcul d'empreintes (hash) et horodatage - Rédaction d'une fiche de chaîne de possession - Vérification de l'intégrité d'une sauvegarde avant restauration	TP
15h00 – 17h00	TP 4 – Analyse post-mortem de la simulation - Le processus de post-mortem : collecte, analyse des causes racines, actions correctives, partage - Application des méthodes des 5 Pourquoi et du diagramme d'Ishikawa au scénario du matin - Culture « sans reproche » : centrer l'analyse sur les systèmes et les processus - Rédaction du rapport post-mortem à partir d'un modèle fourni - Restitution des groupes et débriefing collectif	TP Atelier

JOUR 5
Amélioration continue et évaluation finale
Module 10 – Défis, maturité et amélioration continue · Évaluation des acquis

Objectif de la journée : *Bâtir une démarche d'amélioration continue adaptée à son organisation et valider les compétences acquises.*

Horaire	Séquence et contenus	Modalité
9h00 – 10h30	Défis et culture organisationnelle - Obstacles courants : engagement de la direction, définition des SLA, compétences, outils inadaptés, adhésion des équipes - Attributs d'une organisation mature : acceptation de l'échec, apprentissage, collaboration transversale, transparence	Apport Échange
10h30 – 12h30	Amélioration continue et maturité - Le cycle PDCA appliqué à la gestion des incidents : révision, ajustements, compétences, intégration stratégique - Les cinq niveaux de maturité : réactif, basique, structuré, proactif, optimisé - Atelier : autodiagnostic de maturité et plan d'action à 6 mois pour sa propre organisation - Synthèse de la formation et séance de questions-réponses	Apport Atelier
Pause déjeuner – 12h30 / 13h30		
13h30 – 16h15	Évaluation finale des acquis - Partie 1 – QCM de 30 questions portant sur l'ensemble des modules (45 min) - Partie 2 – Étude de cas individuelle (2 h) : qualifier et prioriser un incident, proposer les mesures de confinement, identifier les obligations de notification, rédiger une synthèse post-incident - Seuil de validation : 70 % de réussite globale	Évaluation
16h15 – 17h00	Bilan et clôture - Correction collective du QCM et retours individualisés - Évaluation de la satisfaction à chaud - Remise de l'attestation de fin de formation	Évaluation Échange

04 MÉTHODES ET MOYENS PÉDAGOGIQUES

Méthodes	▪ Pédagogie active : environ 50 % de mise en pratique sur l'ensemble de la formation ▪ Apports théoriques illustrés de cas réels ▪ Ateliers en sous-groupes, exercices, travaux pratiques et simulation de crise sur table ▪ Retours d'expérience du formateur et échanges entre pairs
Moyens techniques	▪ Salle équipée : vidéoprojecteur, tableau blanc, connexion Internet ▪ Un poste de travail par stagiaire avec accès à l'environnement de TP virtualisé ▪ Outil de ticketing (GLPI ou équivalent), tableur, machines virtuelles de TP ▪ En distanciel : classe virtuelle, partage d'écran et environnement de TP accessible à distance
Supports remis	▪ Support de cours au format numérique ▪ Modèles : plan de réponse, fiche de chaîne de possession, rapport post-mortem, matrice de priorisation ▪ Énoncés et corrigés des exercices et TP

05 MODALITÉS D'ÉVALUATION ET DE SUIVI

Avant la formation	Entretien préalable et quiz de positionnement pour évaluer le niveau d'entrée et adapter le parcours.
Pendant la formation	Évaluation formative : quiz de fin de journée, exercices et TP corrigés, observation lors de la simulation de crise.
Évaluation finale	Jour 5 après-midi : QCM de 30 questions et étude de cas individuelle. Validation à partir de 70 % de réussite globale.
Satisfaction	Questionnaire de satisfaction à chaud en fin de formation et évaluation à froid à 3 mois.
Suivi et sanction	Feuilles d'émargement signées par demi-journée. Remise d'une attestation de fin de formation mentionnant les objectifs et les résultats de l'évaluation des acquis.

06 ACCÈS, DÉLAIS ET ACCESSIBILITÉ

Modalités d'accès	Inscription après entretien préalable (téléphone ou visioconférence) et signature de la convention ou du contrat de formation.
Délai d'accès	Entrée possible jusqu'à 15 jours avant le début de la session, sous réserve de places disponibles.
Lieu	[à compléter] – ou en intra-entreprise dans vos locaux

Accessibilité	Formation accessible aux personnes en situation de handicap. Le référent handicap étudie chaque situation afin de proposer les adaptations nécessaires (pédagogiques, matérielles, organisationnelles). Contact référent handicap : [à compléter]
Financement	Plan de développement des compétences, OPCO, financement personnel. [à compléter selon les éligibilités]

07 INTERVENANT ET CONTACT

Formateur	Expert en cybersécurité et cloud, plus de dix ans d'expérience opérationnelle, enseignant en cybersécurité, systèmes et réseaux du BTS au Master 2.
Contact	MGK Formation – [adresse] – [téléphone] – [e-mail]
Indicateurs de résultats	Taux de satisfaction, taux de réussite et taux d'abandon : [à compléter – mis à jour annuellement]

MGK Formation – Organisme de formation certifié Qualiopi au titre de la catégorie « Actions de formation ». N° de déclaration d'activité : [à compléter] – SIRET : [à compléter]. Ce numéro ne vaut pas agrément de l'État.