# Incident Responder (CIR) : gérer les incidents et répondre aux cyberattaques

## Date et durée

Code formation : ARI001FR
Durée : 4,5 jours
Nombre d'heures : 31 heures

## Formation avec certification

PECB Certified Incident Responder

## Description

Dans un contexte où les cyberattaques sont plus rapides et plus complexes, la capacité d'une organisation à réagir en quelques minutes fait toute la différence. Cette **formation PECB CIR intensive de 4,5 jours** vous transforme en référent incident : vous apprenez à détecter précocement une menace, à coordonner les équipes techniques, juridiques et communications, puis à restaurer les services en conditions sûres.
Construite autour du cadre NIST et enrichie des retours d'expérience des plus grands CSIRT, la session alterne exposés, **travaux pratiques sur machines dédiées et mises en situation** réaliste (ransomware, persistance avancée, intrusion réseau). Vous manipulez des SIEM, des forensers open-source et des play-books automatisés pour contenir, éradiquer et documenter chaque phase d'un incident, sans coupure business.
Après avoir suivi ces cours PECB, vous serez en mesure de gérer les indicateurs de compromission, de conserver la chaîne de preuves, de communiquer en situation de crise et de tirer des leçons pour améliorer en permanence les mesures de sécurité. Ce programme de formation prépare et permet également de **passer l'examen de certification PECB Certified Incident Responder** (*en savoir+ dans l'onglet Certification*).

## Objectifs

*À l'issue de cette formation en analyse & réponse aux incidents, vous atteindrez les objectifs de compétences suivants :*

- concevoir une stratégie de réponse coordonnée entre équipes et outils, puis l'orchestrer en temps réel pour limiter l'ampleur d'un incident ;
- cartographier les vecteurs ransomware, choisir les contre-mesures adaptées et faire exécuter un scénario de réponse qui réduit l'impact au strict minimum ;
- décomposer les comportements malveillants, établir un plan de correction sur mesure et appliquer des méthodes de traçage forensic pour neutraliser le code ;
- détecter précocement les menaces périphériques, les confiner par des dispositifs automatiques et des play-books ciblés avant qu'elles n'atteignent le cœur du réseau ;
- éradiquer les mécanismes de persistance avancés et bâtir un programme de remédiation qui empêche la réapparition des menaces identifiées ;
- se préparer efficacement à l'examen de certification PECB Certified Incident Responder (CIR) .

## Points forts

- **Certification PECB incluse :** cette formation vous prépare spécifiquement à l'examen PECB Certified Incident Responder (CIR). Le coût de votre participation inclut les frais d'examen et de certification.
- **Expertise d'un formateur certifié :** votre formateur est un expert en réponse aux incidents. Il alterne théorie, anecdotes et astuces issues de projets qu'il a réellement pilotés pour que chaque concept devienne immédiatement applicable.
- **Des crédits de développement professionnel :** votre participation à cette formation vous donne droit à 31 crédits de développement professionnel continu (CPD/CPE), ce qui vous permet de maintenir à jour vos compétences et certifications.
- **Une seconde chance à l'examen :** en cas de besoin, vous avez la possibilité de repasser l'examen une fois gratuitement dans les 12 mois suivant la date initiale.

Certification

*Cette formation vous permet de passer la certification professionnelle PECB Certified Incident Responder. Un code coupon vous sera fourni afin que vous puissiez programmer votre examen en ligne sur le site du PECB.*

## Modalités de l’examen PECB Incident Responder

L’examen d’une durée de **1 heure** est disponible en plusieurs **langues (français, anglais, etc.)**. Il est conforme aux exigences du programme d’examen et de certification du PECB et couvre les domaines de compétence suivants :

- les concepts fondamentaux et les principes de la réponse aux incidents de sécurité ;
- la corrélation entre la norme PECB CIR et les autres normes ou cadres réglementaires ;
- l’approche par processus pour une réponse efficace aux incidents de sécurité de l’information.

Après avoir réussi cet examen (**70 % de bonnes réponses minimum**), vous pourrez demander la certification PECB Certified Incident Responder.
Pour en savoir plus sur les modalités, consulter le règlement d'examen PECB ainsi que le règlement de certification PECB.

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

*Suivre cette formation PECB nécessite les prérequis suivants :*

- **Connaissances fondamentales en cybersécurité** : il est essentiel d’avoir une bonne compréhension des principes de base de la cybersécurité, c’est-à-dire connaître les notions de menace, vulnérabilité et risque, savoir identifier les principaux types d’attaques (malware, phishing, déni de service) et comprendre les fonctions premières des dispositifs de défense (pare-feu, antivirus, contrôle d’accès, chiffrement).
- **Maîtrise des bases de la réponse aux incidents** : une familiarité avec les concepts de base de la réponse aux incidents est nécessaire pour suivre efficacement la formation ; il faut donc connaître les grandes phases du cycle de vie d’un incident (préparation, détection, containment, eradication, recovery, leçons apprises) et avoir déjà manipulé un ticket d’alerte ou participer à un exercice de table-top.
- **Expériences professionnelles** : 2 ans d'expérience pratique dans le domaine de la réponse aux incidents ou de la cybersécurité sont nécessaires pour obtenir la certification PECB CIR.

Public

*Cette formation s'adresse à toute personne impliquée dans la gestion de la sécurité des systèmes d'information, incluant :*

- Les **professionnels de la cybersécurité** qui désirent renforcer leurs compétences en réponse aux incidents.
- Les **architectes de la sécurité et les gestionnaires de risque** qui souhaitent intégrer des plans de réponse aux incidents dans leurs stratégies.
- Les **analystes de sécurité** et les **consultants en sécurité** qui souhaitent valider leur expertise en obtenant un certification reconnu.
- Les **auditeurs** et les **professionnels de la conformité** qui veulent comprendre le processus de gestion des incidents.

Programme

## Jour 1 : comprendre et planifier la réponse aux incidents

- La compréhension du cycle de vie de la réponse aux incidents.
- La mise en place d'une stratégie et d'un plan de réponse aux incidents.
- La formation de l'équipe de réponse (IR Team).
- La gestion des parties prenantes et de la communication en cas de crise.

*Travaux pratiques*

- Définir des rôles et des responsabilités au sein d'une équipe de réponse aux incidents.

## Jour 2 : répondre aux incidents de ransomware et de malware

- L'analyse des vecteurs d'attaque des ransomwares et des malwares.
- Les techniques de confinement et d'éradication des menaces.
- La récupération des systèmes et des données après une infection.

*Étude de cas*

- Analyser des données d'un incident de ransomware pour déterminer sa nature et son impact.

**Jour 3 : détecter, analyser et répondre aux menaces du périmètre**

- L'identification des indicateurs de compromission (IoC) liés aux menaces externes.
- Le tri et la hiérarchisation des incidents de sécurité.
- Les techniques d'analyse des journaux (logs) et des événements.
- La mise en place de mesures de confinement sur un scénario d'attaque du périmètre.

## Jour 4 : enquêter, documenter et s'améliorer continuellement

- La réponse aux incidents liés aux mécanismes persistants (APT).
- La collecte et la préservation des preuves numériques (forensic).
- L'analyse post-mortem et l'amélioration du processus de réponse.
- La documentation des incidents et la rédaction des rapports.

*Travaux pratiques*

- Simuler une communication de crise et rédiger un rapport post-incident.

**Dernière demi-journée : se préparer à la certification PECB CIR**

- Présentation de la structure et du format de l'examen.
- Conseils et astuces pour réussir l'examen. PECB CIR.

*Contenu de formation proposé en partenariat avec PECB*