EduGroupe
Accompagner pour réussir

# Parcours certifiant Détecter et traiter des incidents de sécurité informatiquedents de sécurité

Référence : **SECDTISI**

Durée : **23 jours (161 heures)**

Certification : **Certification professionnelle Détecter et traiter des incidents de sécurité informatique**

## Connaissances préalables

- Il est impératif de justifier d'une expérience professionnelle dans le domaine visé par la certification, acquise au sein de la Direction des systèmes d'information d'une entreprise ou d'une ESN (Entreprise de Services du Numérique) ou de justifier d'un diplôme ou d'une certification de niveau 5 (par exemple : BTS Services Informatiques aux Organisations, BTS Systèmes numériques, DUT informatique, Licence Porfessionnelle Métiers de l'informatique, BUT Informatique, Titres à finalité professionnelle, CQP Administrateur Systèmes et Réseaux, etc.)
- Plus explicitement :
- Connaître le guide d'hygiène sécurité de l'ANSSI ou connaître les bonnes pratiques telles qu'elles sont décrites dans ce guide
- Fondamentaux réseaux : Modèle OSI - Equipement réseaux - Fonctionnement TCP/UDP - Service applicatif commun (http, DNS, SMTP, SSL)
- Fondamentaux système : Compréhension de base Windows (Service, fonctionnement) - Compréhension de base Linux (CLI, Service, fonctionnement)
- La compréhension de l'anglais est un plus

## Profil des stagiaires

- Ce parcours certifiant s'adresse à des personnes titulaires d'une certification de niveau 5 ou 6 dans le domaine de l'informatique, dont la cybersécurité n'est pas la seule fonction (techniciens systèmes et réseaux, assistance technique dans les ESN, différents profils de la DSI)
- Le périmètre de la certification correspond aux activités des professionnels qui exercent dans les métiers de la gestion des incidents et des crises de sécurité.

## Objectifs

- A l'issue de la formation, le participant sera capable de :
- Détecter des incidents de sécurité informatique
- Traiter des incidents de sécurité informatique de premier niveau
- Contribuer opérationnellement à la gestion de crise
- Travailler en équipe au sein d'un SOC, CSIRT, d'un CSERT

## Certification préparée

- Aucune

## Méthodes pédagogiques

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

## Formateur

- Consultant-formateur expert en Cybersécurité

## Méthodes d'évaluation des acquis

- Évaluations formatives : Quiz et mises en situation tout au long des 2 jours de formation
- Évaluation finale : Etude de cas pratique en groupe
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

## Contenu du cours

### 1. Module 1 : les fondamentaux de la cybersécurité (14 heures)

### 2. Jour 1 : Introduction et concepts de base (7 heures)

- Accueil et introduction au module (30 min)
- Introduction à la cybersécurité : Définitions, concepts clés, acteurs, chaîne cybercriminelle (1h30)
- Risques et enjeux de la cybersécurité : Analyse des impacts des menaces (1h15)
- Typologie des cyberattaques (Partie 1) : Introduction aux types d'attaques (ransomware, phishing, etc.) (1h30)
- Typologie des cyberattaques (Partie 2) : Étude approfondie des vecteurs d'attaque (1h15)
- 💡 *Quiz et discussion (30 min)*

### 3. Jour 2 : Réglementations, normes et criticité des incidents (7 heures)

- Révision et questions (15 min)
- Réglementations et normes en cybersécurité : Présentation des normes ISO 2700X, RGPD, OWASP Top 10 (1h30)
- Gestion de la criticité des incidents : Méthodologie pour évaluer la gravité des incidents (1h30)
- 💡 *Cas pratiques : Analyse de scénarios d'attaque fictifs pour identifier des solutions (1h30)*
- 💡 *Discussion sur les bonnes pratiques : Échanges sur des retours d'expériences (1h15)*
- 💡 *Évaluation finale : Étude de cas pratique et validation des acquis (30 min)*

### 4. Module 2 : Etat de l'art du SOC (28 heures)

### 5. Jour 1 : Introduction et principes du SOC (7 heures)

- Accueil et introduction au module (30 min)
- Les principes fondamentaux du SOC : Définition, rôle et organisation (1h30)
- Panorama des fonctions du SOC : Surveillance, détection et réponse aux incidents (1h15)
- Politique de gestion des incidents : Définition, périmètres et moyens associés (1h30)
- Exemples pratiques de gestion des incidents au sein d'un SOC (1h15)
- 💡 *Quiz et discussion (30 min)*

### 6. Jour 2 : Découverte et mise en œuvre du SIEM (7 heures)

- Révision et questions (15 min)
- Introduction au SIEM : Objectifs, principes et missions (1h30)
- Présentation des outils SIEM (Elastic, Kibana, Splunk) (1h30)
- Recommandations de l'ANSSI sur la journalisation (1h30)
- 💡 *Exercices pratiques sur l'utilisation d'un SIEM (1h15)*
- 💡 *Quiz et discussion (30 min)*

## 7. Jour 3 : Frameworks de réponse à incident (7 heures)

- Révision et questions (15 min)
- Introduction aux frameworks NIST et CERT : Présentation de l'organisation et des étapes clés (1h30)
- Présentation du framework ISO 27035 : Gestion des incidents de sécurité (1h30)
- Référentiel MITRE ATT&CK : Organisation, techniques et tactiques (1h30)
- Comparaison des frameworks (NIST, CERT, ISO 27035, MITRE) (1h15)
- 💡 *Quiz d'évaluation des frameworks (30 min)*

## 8. Jour 4 : Application pratique et consolidation (7 heures)

- Introduction à la journée (15 min)
- 💡 *Utilisation combinée des frameworks : Cas pratiques de sélection des frameworks selon les besoins (1h30)*
- 💡 *Exploration approfondie du référentiel MITRE ATT&CK : Études de cas sur des scénarios d'attaques courants (1h30)*
- 💡 *Exercice pratique sur le SIEM : Détection et journalisation d'un incident fictif (1h30)*
- Élaboration d'un rapport d'incident : Synthèse des actions réalisées et des recommandations
- 💡 *Quiz final et feedback*

## 9. Module 3 : Gestion des incidents de sécurité (70 heures)

## 10. Jour 1 : Introduction et bases de la gestion des incidents (7 heures)

- Introduction au module (15 min)
- Définition des incidents de sécurité : Typologies (mineurs, majeurs) et impacts organisationnels (1h30)
- Interactions entre incidents et organisation : PCA, PRA, continuité d'activité (1h30)
- Présentation des outils IDS/IPS/UTM : Fonctionnalités de base et principes d'utilisation (1h30)
- 💡 *Exercice pratique : Configuration de base d'un IDS (1h15)*
- 💡 *Synthèse et quiz (30 min)*

## 11. Jour 2 : Outils avancés de détection et journalisation (7 heures)

- Fonctionnement des logiciels de collecte et d'analyse (Elastic, Kibana, Splunk). (1h45)
- Pratiques de journalisation recommandées (ANSSI) (1h30)
- 💡 *Exercice pratique : Collecte de données à partir d'un SIEM (1h30)*
- 💡 *Étude de cas : Analyse de journaux d'événements pour détecter un incident (1h15)*
- Synthèse et feedback (30 min)

## 12. Jour 3 : Qualification et priorisation des incidents (7 heures)

- Critères de qualification des incidents : Gravité, impact, et priorité (1h45)
- Utilisation des tableaux de bord pour la gestion des incidents (1h30)
- 💡 *Exercice pratique : Qualification et priorisation d'incidents sur un tableau de bord (1h30)*
- Introduction à l'analyse des causes racines (Root Cause Analysis) (1h15)
- 💡 *Quiz et discussion (30 min)*

## 13. Jour 4 : Techniques avancées d'analyse des incidents (7 heures)

- Analyse avancée des journaux d'événements : Utilisation d'outils forensics et de logs (1h45)
- 💡 *Exercice pratique : Détection d'une intrusion à partir des journaux (1h30)*
- Techniques de containment, éradication et récupération (1h30)
- 💡 *Étude de cas : Gestion complète d'un incident de sécurité (1h15)*
- 💡 *Quiz et retour collectif*

## 14. Jour 5 : Approfondissement des frameworks NIST et ISO 27035 (7 heures)

- Introduction à la journée (15 min)
- Présentation du framework NIST : Étapes clés (détection, containment, récupération) (1h30)
- Présentation du framework ISO 27035 : Organisation, étapes, amélioration continue (1h30)
- 💡 *Exercice pratique : Comparaison entre les frameworks NIST et ISO 27035 sur un cas réel (1h30)*
- 💡 *Quiz sur les frameworks NIST et ISO 27035 (1h15)*
- Synthèse et feedback

## 15. Jour 6 : Études de cas et outils IDS/IPS (7 heures)

- Révision des journées précédentes et introduction (15 min)
- Configuration avancée d'un IDS : Surveiller des activités malveillantes (1h30)
- 💡 *Étude de cas : Analyse des alertes générées par un IDS (1h30)*
- Présentation et configuration d'un IPS : Prévention des intrusions (1h30)
- 💡 *Exercice pratique : Containment d'une intrusion détectée par un IPS (1h15)*
- 💡 *Quiz et retour collectif (30 min)*

## 16. Jour 7 : Gestion des incidents complexes (7 heures)

- Introduction aux incidents complexes (15 min)
- 💡 *Étude de cas : Analyse d'un incident complexe sur un système distribué (1h15)*
- Techniques avancées de containment : Limiter l'impact d'une attaque en temps réel (1h30)
- Récupération après un incident : Restaurer les systèmes et vérifier leur intégrité (1h30)
- 💡 *Exercice pratique : Mise en œuvre d'un containment et récupération (1h15)*
- 💡 *Quiz et feedback collectif (30 min)*

## 17. Jour 8 : Investigation et Root Cause Analysis (7 heures)

- Introduction à la journée (15 min)
- Techniques d'analyse forensics : Méthodes et outils pour reconstituer un incident (1h30)
- 💡 *Exercice pratique : Analyse des journaux pour identifier l'origine d'un incident (1h30)*
- Introduction au Root Cause Analysis (RCA) : Méthodologie et outils associés (1h30)
- 💡 *Étude de cas : RCA d'un incident critique et élaboration de recommandations (1h15)*
- 💡 *Quiz et discussion*

## 18. Jour 9 : Élaboration de rapports d'incidents (7 heures)

- Introduction à la journée (15 min)
- Structure d'un rapport d'incident : Analyse, recommandations, retour d'expérience (1h30)
- 💡 *Étude de cas : Élaboration d'un rapport complet sur un incident donné (1h30)*
- Recommandations post-incident : Formalisation des enseignements pour améliorer la posture (1h30)
- 💡 *Exercice pratique : Présentation des rapports d'incidents en groupe (1h15)*
- Feedback collectif et synthèse

## 19. Jour 10 : Simulation complète et validation des acquis (7 heures)

- 💡 *Introduction à la simulation (15 min)*
- 💡 *Détection de l'incident : Identification des anomalies à partir des outils disponibles (1h30)*
- 💡 *Réponse à l'incident : Containment, éradication et récupération des systèmes (1h30)*
- 💡 *Élaboration d'un rapport complet : Analyse, recommandations, et plan d'amélioration (1h30)*
- 💡 *Présentation des résultats et évaluation finale (1h15)*
- Clôture et feedback final (30 min)

## 20. Module 4 : Fondamentaux de l'investigation numérique (7 heures)

## 21. Fondamentaux de l'investigation numérique (7 heures)

- Introduction au module et objectifs (15 min)
- Introduction à l'investigation numérique : Définitions, étapes clés et contexte légal (1h30)
- Collecte et préservation des preuves numériques : Méthodes et outils (1h30)
- Méthodes d'analyse forensics et outils pratiques : Démonstrations et exercices (1h30)
- 💡 *Étude de cas : Analyse d'un incident et reconstitution des événements (1h15)*
- Synthèse et feedback collectif

## 22. Module 5 : Gestion de crise en cybersécurité (21 heures)

## 23. Jour 1 : Introduction et mise en place d'une cellule de crise (7 heures)

- Introduction au module et objectifs (15 min)
- Définition et typologies de crises cyber (1h30)
- Organisation d'une cellule de crise : Rôles et responsabilités (1h30)
- Étapes de la gestion de crise : Détection, activation, gestion, retour à la normale (1h30)
- 💡 *Exercice pratique : Mise en place d'une cellule de crise (1h15)*
- 💡 *Synthèse et quiz*

## 24. Jour 2 : Communication et continuité d'activité (7 heures)

- Introduction et objectifs de la journée (15 min)
- Stratégies de communication de crise : Interne et externe (1h30)
- Outils de communication : Tableaux de bord et gestion des médias (1h30)
- Introduction au PCA/PRA : Objectifs et méthodologie (1h30)
- 💡 *Exercice pratique : Identification des activités critiques pour un PCA (1h15)*
- 💡 *Quiz et retour collectif*

## 25. Jour 3 : Simulation de crise et retour d'expérience (7 heures)

- 💡 *Introduction à la simulation (15 min)*
- 💡 *Simulation de crise (Partie 1) : Détection et activation de la cellule de crise (1h30)*
- 💡 *Simulation de crise (Partie 2) : Coordination des actions et communication (1h30)*
- 💡 *Retour à la normale et élaboration du retour d'expérience (1h30)*
- 💡 *Exercice pratique : Rédaction d'un retour d'expérience structuré (1h15)*
- Synthèse finale et feedback collectif (30 min)

## 26. Module 6 : Sensibilisation des équipes et amélioration continue (14 heures)

## 27. Jour 1 : Introduction et création de campagnes (7 heures)

- Introduction au module et objectifs (15 min)
- Les menaces courantes et les comportements à risque des collaborateurs (1h30)
- Conception de campagnes de sensibilisation : Stratégies et messages clés (1h30)
- 💡 *Atelier pratique : Élaboration d'un plan de communication pour une campagne fictive (1h30)*
- 💡 *Exercice pratique : Création de supports interactifs (affiches, vidéos, quiz) (1h15)*
- Synthèse et discussion

## 28. Jour 2 : Diffusion et amélioration continue (7 heures)

- Introduction et objectifs de la journée (15 min)
- Introduction au cycle PDCA (Plan-Do-Check-Act) pour la sensibilisation (1h30)
- 💡 *Exercice pratique : Évaluation de l'impact d'une campagne fictive (1h30)*
- 💡 *Atelier : Ajustement des supports et messages à partir des retours collectés (1h30)*
- 💡 *Simulation de présentation des campagnes auprès de publics cibles (1h15)*
- Clôture et feedback collectif (30 min)

## 29. Module 7 : La veille en cybersécurité (7 heures)

## 30. La veille en cybersécurité (7 heures)

- Introduction au module et objectifs (15 min)
- Introduction aux sources d'information fiables : CERT-FR, MITRE, NIST, ANSSI (1h30)
- 💡 *Exercice pratique : Utilisation d'outils OSINT (Maltego, Shodan) (1h30)*
- Analyse et exploitation des informations collectées (1h30)
- 💡 *Étude de cas : Élaboration d'un rapport à partir d'une menace détectée (1h15)*
- Synthèse et feedback collectif (30 min)

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.