Formation Détecter et traiter des incidents de sécurité informatique

Parcours certifiant

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Le parcours certifiant Détecter et traiter des incidents de sécurité informatique est conçu pour les professionnels IT souhaitant se spécialiser dans la réponse aux cyberincidents. Accessible aux titulaires d'un diplôme ou d'une expérience en systèmes et réseaux, ce programme de 161 heures (23 jours) en format mixte offre une montée en compétences concrète et certifiante, alignée sur les réalités opérationnelles du métier.
La formation couvre les fondamentaux de la cybersécurité, les principes de fonctionnement d'un SOC (Security Operations Center), l'usage des outils de supervision (SIEM), les méthodologies de gestion des incidents (NIST, ISO 27035), et les techniques d'investigation numérique. Les participants apprennent à détecter, qualifier et traiter des incidents, à analyser les causes racines, à gérer la documentation et à communiquer efficacement en contexte de crise.
Un volet important du parcours est consacré à la gestion de crise cyber, à la sensibilisation des équipes aux menaces, ainsi qu'à la veille technologique. Les participants développent des compétences transversales : élaboration de PCA/PRA, animation d'une cellule de crise, création de supports de sensibilisation, réalisation d'une veille active via des outils OSINT (Shodan, TheHarvester, Maltego...).
Grâce à une pédagogie axée sur la pratique (ateliers, simulations, cas concrets), les apprenants sortent formés pour intégrer un SOC, CSIRT ou CERT, et piloter efficacement les réponses aux menaces dans tout environnement professionnel. La certification obtenue atteste de leur capacité à gérer les incidents de sécurité dans leur globalité, de la détection à la résolution.

Référence	SECDTISI
Durée	23 jours (161h)
Tarif	13 280 €HT
Certification	- €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 1er juin au 3 juillet 2026
du 9 sept. au 11 octobre 2026
du 16 nov. au 18 décembre 2026

PARIS

du 1er juin au 3 juillet 2026
du 9 sept. au 11 octobre 2026
du 16 nov. au 18 décembre 2026

VOIR TOUTES LES DATES

Objectifs

| 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

Public

| 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.

Prérequis

| 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

Programme de la formation

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

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)

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

Découverte et mise en oeuvre 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)

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)

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

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

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)

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)

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

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

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)

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 oeuvre d'un containment et récupération (1h15)
| Quiz et feedback collectif (30 min)

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

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

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)

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

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

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

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)

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

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)

Module 7 : 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)

Détail des dates de session
| Session du 04 mars au 12 juin 2026 : Mars : 04 au 06 + 19 et 20 + 30 au 31 Avril : 01 + 13 au 15 + 22 au 24 + 29 au 30 Mai : 11 au 13 mai + 21 au 22 Juin : 01 +02 + Jury les 11 et 12
| Session du 01 juin au 25 août 2026 : Juin : 01 au 02 + 10 au 12 + 22 au 25 Juillet : 01 au 03 + 07 au 10 + 20 au 23 + 29 au 31 Août : Jury les 24 et 25
| Session du 09 septembre au 08 janvier 2027 Septembre : 09 au 11 + 24 au 25 + 28 au 30 Octobre : 12 au 13 + 26 au 27 Novembre : 09 au 10 + 19 au 20 + 30 Décembre : 01 au 02 + 10 au 11 + 17 au 18 Janvier 2027 : Jury les 07 et 08
| Session du 16 novembre au 11 juin 2027 Novembre : 16 au 18 Décembre : 03 au 04 + 14 au 16 Janvier 2027 : 06 au 08 + 21 au 22 + 28 au 29 Février 2027 : 10 au 12 + 24 au 26 Mars 2027 : 04 au 05 Juin 2027 : Jury les 10 et 11

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

Détecter et traiter des incidents de sécurité informatique
Certification professionnelle Détecter et traiter des incidents de sécurité informatique de l'OPCO Atlas.
La certification se compose de 2 épreuves :

| Le jeu de rôle - 3h30. Il comprend 3 phases :
| Phase 1 : compréhension du contexte d'intervention et détection des incidents (1 heure). EduGroupe fournira au candidat les informations et documents permettant de définir son rôle, ses missions et le contexte d'exercice de l'entreprise fictive donnée. Le candidat s'appuie sur un questionnaire défini par l'organisme de formation et synthétise les informations demandées.
| Phase 2 : détection et traitement d'un incident de sécurité maximum (1h30). Une simulation d'attaque informatique est déclenchée par le jury d'évaluation. Le candidat doit résoudre à l'aide des outils et logiciels à sa disposition un incident de sécurité informatique mineur impactant la fonctionnalité de l'entreprise.
| Phase 3 : débriefing avec la direction et amélioration continue (30 minutes). A la suite de la simulation, le candidat effectue un retour d'expérience sur l'événement survenu, sa contribution à la gestion de crise et les axes d'amélioration et évolutions à apporter à l'organisation de l'entreprise et au dispositif de sécurité en matière de cybersécurité.
| La soutenance orale - 0h30. Elle fait suite au jeu de rôle et est distincte du retour d'expérience qui fait partie intégrante du jeu de rôle. La soutenance orale a pour objectif de démontrer la capacité du candidat à présenter une analyse critique de son travail : 15 minutes de présentation par le candidat + 15 minutes d'échanges avec le jury.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).

| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.