PARCOURS CERTIFIANT DTISI - DÉTECTER ET TRAITER DES INCIDENTS DE SÉCURITÉ INFORMATIQUE

Formation certifiante de 23 jours (161 heures) sur environ 4 mois, le parcours DTISI forme à la détection, qualification et gestion des incidents dans un SOC ou CERT. Le parcours associe théorie approfondie, exercices pratiques immersifs et simulation de gestion de crise, validés par un jeu de rôle final et une soutenance devant jury.

TARIF : 14 490 € HT | **RÉF. :** DTISI

OBJECTIFS

- Maîtriser les concepts fondamentaux et acteurs de la cybersécurité.
- Identifier et analyser les vecteurs, techniques et scénarios d'attaques.
- Utiliser efficacement les outils SIEM et méthodes SOC d'analyse et détection.
- Gérer les incidents avec des processus structurés en conformité avec les normes (ISO 27035).
- Participer à la gestion de crise et à la sensibilisation des équipes.

PRÉ-REQUIS

- Disposer de connaissances générales en informatique et des fondamentaux de la cybersécurité (notions sur les attaques, vecteurs, risques).
- Connaître le guide de sécurité de l'ANSSI ou avoir suivi un module de formation équivalent (exemple : Mooc SecNumacadémie de l'ANSSI) est recommandé mais non obligatoire.
- Posséder un ordinateur personnel avec une connexion internet et capacité d'exécuter des outils de cybersécurité avancés (SIEM, outils forensic).
- Être familiarisé avec les environnements réseaux et systèmes, et disposer d'une capacité d'analyse et de synthèse pour traiter des données complexes issues des logs de sécurité.
- Engagement à participer activement aux ateliers pratiques et simulations d'incidents pour valider les compétences.

PUBLIC VISÉ

Analystes SOC, techniciens de sécurité, experts en gestion d'incidents, coordinateurs d'équipes CERT.

PROGRAMME DÉTAILLÉ

Le parcours est organisé autour de 7 axes majeurs, couvrant théorie, pratique et cas concrets.

Axe 1 : Les fondamentaux de la cybersécurité

Durée : 2 jours - 14 heures
Objectifs : Permettre aux stagiaires de maîtriser les concepts clés de la cybersécurité, identifier les risques, les vecteurs d'attaque, et comprendre le cadre réglementaire applicable.
Contenu :

- Identification de l'écosystème cyber : acteurs, chaîne cybercriminelle, profils et motivations des attaquants.
- Concepts fondamentaux : risques, impacts sur l'organisation, systèmes d'information concernés.
- Types d'attaques : ransomware, phishing, déni de service, ingénierie sociale, mots de passe compromis.
- Principaux vecteurs : messagerie, navigation web, connexions sans fil, logiciels malveillants.
- Cadre réglementaire : normes ISO 27001, 27005, RGPD.
- Référentiels de sécurité : Top 10 OWASP, STRIDE.
- Travaux pratiques : identification des vecteurs d'attaque sur une architecture fictive, catégorisation des incidents selon leur criticité, quiz de validation.

Axe 2 : État de l'art du SOC

Durée : 4 jours - 28 heures
Objectifs : Former à la connaissance du SOC, à ses outils et méthodes, notamment le SIEM, ainsi qu'aux principaux frameworks de gestion des incidents.
Contenu :

- Définition, rôle et organisation d'un SOC.
- Panorama des fonctions : surveillance, analyse, réponse aux incidents.
- Introduction aux outils SIEM (Elastic Stack, Splunk), leur architecture et fonctionnalités.
- Présentation et démonstration IDS/IPS.
- Recommandations de l'ANSSI sur la journalisation.
- Frameworks de réponse à incident : NIST, CERT, ISO 27035.
- Travaux pratiques : installation et configuration de SIEM, analyse des logs, création de règles de corrélation, étude de cas (temps réel phishing).

Axe 3 : Gestion des incidents

Durée : 10 jours - 70 heures
Objectifs : Apprendre à déployer et gérer efficacement le processus complet de gestion des incidents de sécurité, des détections initiales à la remédiation.
Contenu :

- Principes et rôles des IDS, IPS, UTM.
- Classification des incidents selon leur criticité, fonctionnement des bases de données d'incidents.
- Phases de réaction : détection, catégorisation, confinement, éradication, récupération.
- Méthodes d'analyse forensic, outils Kansa, GRR.
- Procédures et outils pour répondre aux incidents mineurs et majeurs.
- Travaux pratiques : simulations complètes, rédaction de rapports, analyse des causes racines.

Axe 4 : Les fondamentaux de l'investigation numérique

Durée : 1 jour - 7 heures
Objectifs : Acquérir les fondamentaux de l'investigation numérique: préservation de la preuve, collecte, analyse et rapport.
Contenu

- Processus d'investigation numérique, définition et rôle des preuves.
- Taxonomie et méthodologies forensics.
- Collaboration avec acteurs internes et externes (ANSSI, forces de l'ordre).
- Travaux pratiques : collecte, préservation et analyse des preuves numériques, rédaction de rapports forensic.

Axe 5 : La gestion de crise en Cybersécurité

Durée : 3 jours - 21 heures
Objectifs : Structurer, piloter et entraîner la réponse organisationnelle en situation de crise cyber, du déclenchement au RETEX.
Contenu :

- Cellule de crise: rôles, escalade, coordination.
- PCA/PRA: périmètre, dépendances, activation, synchronisation des actions.
- Communication: messages, canaux, tableaux de bord.
- Travaux pratiques : mise en place cellule, exercice ransomware, kit messages, RETEX

Axe 6 : Sensibilisation des équipes et amélioration continue

Durée : 2 jours - 14 heures
Objectifs : Concevoir, déployer et mesurer des actions de sensibilisation pour renforcer durablement la posture cyber
Contenu :
Thématiques clés et supports: phishing, mots de passe, nomadisme.
Méthodes d'animation et relais managériaux.
KPI et tableaux de bord de sensibilisation.
Travaux pratiques : mini-campagne + dashboard et plan d'amélioration

Axe 7 : La veille en Cybersécurité

Durée : 1 jour - 7 heures
Objectifs : Savoir mettre en place une veille opérationnelle efficace pour anticiper les menaces et adapter les dispositifs de sécurité.
Contenu :

- Sources de veille : ANSSI, CERT-FR, OSINT, CVE.
- Méthodes d'analyse et exploitation des alertes.
- Rédaction et communication des recommandations.
- Travaux pratiques : mise en place de processus de veille, analyse des résultats, formulation de plans d'amélioration continue.

ÉVALUATION DES ACQUIS

- Validation des acquis par un jeu de rôle final, suivi d'une soutenance orale devant jury.
- Évaluations régulières avec quiz et auto-tests intégrés au fil des modules.
- Travaux pratiques approfondis utilisant des outils SOC (SIEM Splunk, Elastic Stack), forensic (Kansa, GRR), et simulation d'incidents (phishing, ransomware).
- Travaux pratiques centrés sur l'identification, catégorisation, analyse et réponse aux incidents.
- Livrables : rapports d'analyse, classification des incidents, documentation des investigations forensics, et plans de remédiation.
- Les Travaux pratiques portent aussi sur la configuration avancée et la personnalisation d'outils de détection, ainsi que sur la gestion coordonnée d'incidents complexes.
- Les compétences évaluées incluent la maîtrise des standards ISO 27035, NIST CSF, les processus SOC et CERT, ainsi que l'analyse approfondie des journaux d'événements.

MÉTHODES PÉDAGOGIQUES

- Cours théoriques enrichis par études de cas réels et retour d'expérience.
- Exercices pratiques avec outils SOC, enquêtes sur logs, simulations d'incidents.
- Jeux de rôles et soutenance pour valider les compétences opérationnelles.

POINTS FORTS

- Formateurs certifiés PASSI, experts SOC et Forensics.
- Mise en œuvre d'outils professionnels leaders (SIEM, Elastic, Splunk).
- Approche pragmatique avec simulations et scénarios réels.
- Alignement aux recommandations ANSSI, ISO 27035 et NIST.
- Ce cursus est éligible au financement OPCO Atlas

Ce parcours certifiant fait partie de l'offre CampusAtlas, **il est reconnu et financé jusqu'à 100% par l'Opco Atlas**, avec des démarches simplifiées, une garantie de qualité et l'accompagnement sur-mesure dont bénéficient les entreprises adhérentes.