Parcours DTISI

Détecter et traiter des incidents de sécurité informatique

Catégorie : Sécurité Informatique
Durée : 23 Jours (161 heures de formation)
Certification : Certification professionnelle Détecter et traiter des incidents de sécurité informatique
Référence : ACGDTISI

Objectifs pédagogiques

Acquérir les connaissances, savoir-faire et compétences nécessaires pour la détection et le traitement des incidents de sécurité informatique

- Détecter des incidents de sécurité informatique
- Traiter des incidents de sécurité informatique de premier niveau
- Apporter une contribution opérationnelle à la gestion de crise
- Travailler en équipe au sein d'un SOC, CSIRT, d'un CSERT

Public

Le parcours de formation est ouvert aux candidats 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).

Pré-requis

- Justifier d'un diplôme ou d'une certification de niveau 5 (par exemple : BTS Services Informatiques aux Organisations, BTS Systèmes numériques, DUT informatique, Licence Professionnelle métiers de l'Informatique, BUT Informatique, Titres à Finalité Professionnelle, CQP dont le CQP Administrateur Systèmes et Réseaux, etc.)

OU

- Justifier d'une expérience acquise au sein de la Direction des systèmes d'information d'une entreprise ou d'une ESN (Entreprise de Services du Numérique)

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 vecteursd'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 et fonctionnement d'un SOC

Durée : 4 jours – 28 heures

Objectifs : Former à la connaissance du SOC, à ses outils et méthodes, notamment le SIEM, ainsi qu'aux principauxframeworks 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 decas (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, desdétections 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 **:** Donner les bases indispensables de l'analyse forensic pour traiter les incidents et identifier les causes racines.

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 **:** Renforcer les compétences en traitement avancé des incidents, planification des réponses et remédiation.

Contenu :

- Définition et organisation de la gestion de crise : identification des enjeux (réputation, fonctionnement, finances), rôles des parties prenantes, et bonnes pratiques des cellules de crise.
- Politique d'escalade : compréhension des types d'escalades (managériales, fonctionnelles) et des mécanismes de déclenchement.
- Procédures de gestion de crise : logistique, référentiels (ex. PRIS), étapes clés du déroulement, et formalisation du retour d'expérience.
- Continuité d'activité (PCA/PRA) : cadre réglementaire, typologie des risques, rôles des acteurs, et mesures de sécurisation des actifs et des réseaux.
- Communication et gestion du stress : architecture des échanges, indicateurs de suivi, outils de pilotage, et techniques de régulation en période de crise.

Travaux pratiques : élaboration de fiches réflexes, gestion coordonnée d'incidents majeurs.

Axe 6 : Sensibilisation des équipes et amélioration continue
Durée : 2 jours – 14 heures

Objectifs **:** Maîtriser les techniques avancées d'analyse des journaux, construction de scénarios de détection et réponsesrapides.

Contenu :

- Thématiques de communication : menaces courantes (phishing, ransomware, piratage…), exposition des données personnelles, sécurité des mots de passe et des moyens d'authentification.
- Bonnes pratiques de protection : mise à jour des logiciels, sauvegarde des données, signalement des fraudes, sécurité en télétravail, gestion des mots de passe.
- Outils de communication : intranet, emails, MOOC ANSSI, outils de veille, formats collaboratifs comme le World Café.
- Adaptation aux profils utilisateurs : salariés, prestataires, personnes en situation de handicap.
- Supports pédagogiques : rédaction de procédures et modes opératoires pour les utilisateurs, en lien avec la politique de sécurité.
- Campagnes de sensibilisation : conception de scénarios simples d'ingénierie sociale (ex. hameçonnage) pour illustrer les risques et renforcer la vigilance.

Travaux pratiques : Elaborer un kit de sensibilisation, organiser une campagne de sensibilisation.

Axe 7 : La veille en Cybersécurité
Durée : 1 jour – 7 heures

Objectifs **:** Savoir à utiliser les outils et sources de veille adaptés aux enjeux de la cybersécurité et identifier les impacts liés à la veille dans les pratiques de l'entreprise.

Contenu :

- Compréhension de l'OSINT et du paysage des menaces : introduction aux usages de l'OSINT, évolution des cybermenaces, rôle du cycle PDCA et outils d'anticipation.
- Sources et techniques de veille : exploitation de sources réglementaires et techniques (ANSSI, CERT-FR, NIST, éditeurs, Dark Net…), recherche de publications (CVE), identification des failles réseau.
- Capitalisation et diffusion de la veille : archivage via le Knowledge Management, communication via intranet, supports internes et tableaux de bord.
- Implication des parties prenantes : direction, cellules de crise, utilisateurs, pour intégrer la veille dans les pratiques de sécurité de l'entreprise.

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 investigationsforensics, 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 d'évaluation des acquis

- Alternance d'apports théoriques, démonstrations, retours d'expérience et études de cas.
- Travaux pratiques intensifs avec outils réels (SIEM, outils de veille).
- Évaluation continue par quizz, travaux pratiques, dossier professionnel et soutenance.

EXPERTISE TERRAIN

Formateurs en poste : analystes SOC, auditeurs PASSI, consultants cyber. Vous apprenez avec celles et ceux qui font face aux menaces au quotidien.

50 % DE PRATIQUE, 100% D'IMPACT – «LEARNING BY DOING»

Labs, mises en situation, simulations d'attaque : ici, on apprend en faisant.Apprenez la cybersécurité autrement : intégrer le Cyber Squad, c'est transformer la théorie en pratique.

L'ALLIANCE DES COMPÉTENCES TECHNIQUES ET STRATÉGIQUES

Grâce aux parcours DTISI et PASI, les équipes du Cyber Squad se complètent : les agents techniques neutralisent les menaces en temps réel, pendant que les leaders stratégiques préparent et pilotent la vision à long terme. Ensemble, ils bâtissent une véritable forteresse numérique.

Accessibilité de la formation :

ACG Cybersecurity s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap.

Notre réfèrent handicap se tient à votre disposition par mail à referent.handicap@acgcybersecurity.fr pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.