# Détecter et traiter des incidents de sécurité informatique

**Durée: 23 Jours** **Réf de cours: DTISI** **Méthodes d'apprentissage: Classe à distance**

## Résumé:

Global Knowledge en partenariat avec ACG Cybersecurity lance un nouveau parcours certifiant :
Le parcours de formation DTISI (Détecter et traiter des incidents de sécurité informatique) vise à permettre aux candidats à la certification d'acquérir les connaissances, savoir-faire et compétences nécessaires pour la détection et le traitement des incidents de sécurité informatique.

L'unité d'intervention CyberSquad : vous voulez apprendre à détecter, analyser et répondre aux cyberattaques ? Avec le parcours DTISI comprenant 50% de pratique et un accompagnement expert, devenez un agent d'élite, capable de neutraliser les menaces et de protéger les systèmes grâce à une expertise technique concrète.

Objectifs: Détecter - Analyser - Répondre
Compétences clés:
- SOC & SIEM, corrélations, hunting
- Gestion d'incidents, confinement, reprise
- Forensics systèmes/réseaux, preuves
- Gestion de crise et reporting exécutif

*Mis à jour 23/09/2025*

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

## Public visé:

Le parcours de formation DTISI 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), ou aux professionnels ayant une expérience équivalente.

## Objectifs pédagogiques:

- Le parcours de formation permet aux candidats la maîtrise des compétences inscrites au référentiel de la certification. L'obtention de la certification doit permettre aux professionnels qui exercent dans les métiers de la gestion des incidents et des crises de sécurité d'être capables de :
- Comprendre les fondamentaux cyber & référentiels clés (ISO 27001, RGPD, OWASP…)
- Exploiter un SOC et des outils SIEM (Elastic, Splunk…)
- Détecter des incidents de sécurité informatique
- Traiter des incidents de sécurité informatique de premier niveau
- Identifier, analyser et répondre à un incident en conditions réelles
- Apporter une contribution opérationnelle à la gestion de crise
- Mener une investigation numérique et sécuriser les preuves
- Piloter une cellule de crise cyber
- Travailler en équipe au sein d'un SOC, CSIRT, d'un CSERT
- Sensibiliser les équipes et mettre en place une veille efficace

## Pré-requis:

Justifier d'un diplôme ou d'une certification de niveau 5 (par

## Test et certification

Certification : A l'issue du parcours de formation, l'acquisition des

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)

compétences sera validée par un jeu de rôle élaboré sur la base d'une situation réelle ou proche de la réalité (3 heures), et d'une soutenance orale devant un  jury (30 minutes),

## Contenu:

Axe 1 : Les fondamentaux de la cybersécurité – 2 jours (14 heures)

- Identification de l'écosystème de l'espace cyber et de la sécurité numérique : acteurs au sein d'une organisation, chaîne cybercriminelle, cybercriminalité (profils, motivations, modus operandi, etc.)
- Définition et appréhension des concepts de base de la cybersécurité : compréhension des risques (cybercriminalité, atteinte à l'image, espionnage, sabotage, etc.), enjeux et impacts des menaces et attaques sur une organisation, les moyens d'action d'une organisation, les systèmes d'information impactés par la cybersécurité (SI d'entrepri
- Les différents types d'attaque, scénarios d'attaque et techniques de propagation : ransomware, hameçonnage, documents malveillants, déni de service, ingénierie sociale, attaque de mots de passe.
- Les principaux vecteurs d'attaque : messagerie, navigation Internet, connexions sans fil, logiciels malveillants
- La réglementation et les normes en vigueur dans la cybersécurité : ISO 2700X, (27001, 27005...), RGPD
- Les référentiels standards : les 10 vulnérabilités du Top 10 OWASP, STRIDE.

Axe 2 : Etat de l'art du SOC – 4 jours (28 heures)

- Les principes fondamentaux du SOC
- Définition et rôle du SOC
- Organisation du SOC et ses processus
- Panorama des fonctions d'un SOC
- Politique de gestion d'un incident de sécurité : Définition, objectifs, services,
- périmètres, moyens associés.
- Découverte et mise en place du SIEM
- Présentation du SIEM : objectifs, principes de fonctionnement, missions
- Présentation des outils du SIEM : outils de collecte, corrélateur d'événements, outils d'analyse, outils de reporting (par exemple : Elastic, Logstash et Kibana, Splunk...)
- Recommandations de l'ANSSI sur la journalisation.
- Framework de réponses à incident : le NIST, le CERT, norme ISO 27035 (gestion des incidents de sécurité de l'information, journalisation, usages et bonnes pratiques).

Axe 3 : Gestion des incidents – 10 jours ( 70 heures)

- Le suivi du système d'information :
- IDS (système de détection des intrusions) : Définition et principes de fonctionnement
- IPS (système de prévention des intrusions) : Définition et principes de fonctionnement
- UTM (Unified Threat and Management) :

Axe 4 : Les fondamentaux de l'investigation numérique – 1 jour (7 heures)

- Etat de l'art de l'investigation numérique
- Introduction et processus du Forensics
- Preuve numérique : définition, rôle, préservation de la preuve
- Vocabulaire et taxonomie
- Sur qui s'appuyer : acteurs internes (DSI, RSSI) et externes (ANSSI et forces de l'ordre)

Axe 5 : La gestion de crise en cybersécurité – 3 jours (21 heures)

- La gestion de crise : définition, rôle des parties prenantes et enjeux pour l'organisation (réputation, fonctionnement, impacts financiers...), cellules de gestion de crise (bonnes pratiques et usages)
- La politique de gestion de l'escalade et des types d'escalades (managériales/fonctionnelles).
- Les procédures de gestion de crise : logistique, référentiel (ex. PRIS), déroulement et étapes clés, retour d'expérience
- PCA/PRA : définition, cadre réglementaire, feuille de route, typologie et analyse des risques, procédures du plan de continuité (acteurs, rôles, mesures de protection de l'information et de sécurisation des réseaux et des actifs)
- La communication de crise : mapping de l'architecture logicielle et matérielle, rôle et impacts des réunions de crise, périodicité des échanges et de la remontée des indicateurs et événements, outils et tableaux de bord
- Mise en pratique : La gestion du stress en période de crise : techniques de régulation et de communication

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

- Sur quoi communiquer :
- Les menaces courantes (fishing, hoax, pièces jointes, ransomware, piratage de compte et d'identité, ciblage publicitaire...)
- La diffusion des données personnelles sur le web : exposition des données sensibles, RGPD
- La gestion des mots de passe et les moyens d'authentification, les clés de chiffrement (cryptage, vérification d'intégrité), le https, les certificats SSL, le paiement en ligne...
- Le nomadisme (filtre de confidentialité, VPN, bloqueur smartphone...)
- Les bonnes pratiques et mesures de

Axe 7 : La veille en cybersécurité – 1 jour (7 heures)

- Introduction à l'OSINT : Périmètres et usages
- Evolution du paysage des cybermenaces : enjeux de la veille, PDCA (identification et rôle), les outils pour identifier, comprendre et anticiper les nouvelles menaces ou les nouveaux attaquants.
- Principales sources réglementaires et techniques de veille : ANSSI, éditeurs (alertes et patchs, mise à jour des bases, etc.), CERT-FR, NIST, ChatGPT, Dark Net, Le Clusif...
- Techniques de veille : recherche de publications sur les incidents et patchs associés (CVE), identification des failles sur son réseau
- Archivage et stockage de la veille (Knowledge Management)
- Les outils de communication d'une veille sur la cybersécurité : intranet d'entreprise, supports de communication.
- Parties prenantes d'une veille : direction, cellules de crise, utilisateurs.

Définition et principes de fonctionnement
- La criticité d'un incident : définition d'incident mineur/majeur
- Les actifs concernés et connectivités (serveurs, bases de données, IoT, OS, application, réseaux et téléphonie...)
- Tableaux de bord de la gestion des incidents : base de données incident (Elastic Search)/journal d'évènement/ticket
- Mise en pratique de la gestion d'incident :
- Compréhension des principes de fonctionnement et utilisation d'un IDS, IPS et UTM, règles de base
- Les logiciels de collecte et d'analyse
- Les incidents de sécurité
- Les intrusions externes/internes
- Tactiques de réaction aux incidents : les phases de réaction aux incidents (détection, catégorisation, classification)
- Analyse des causes racines : outils, méthodes, indicateurs.
- Traitement d'un incident mineur : procédure de réponse aux incidents (fiches réflexes), outils de réponse (Linux, Windows, Kansa, GRR), actions correctives

protection (bloqueurs de pubs et de sites malveillants, installation et mise à jour des logiciels, sauvegarde de données, signalement des fraudes, télétravail, gestionnaire de mots de passe...)
- Les bons outils de communication : intranet, mails, MOOC de l'ANSSI, les outils de veille (ANSSI), World Café,
- Les profils utilisateurs : salariés de l'organisation, prestataires de services, personnes en situation de handicap.
- Rédaction et présentation de procédures, modes opératoires de scénarios de réponse à des incidents à destination d'utilisateurs, mise à jour en lien avec la politique et le dispositif de sécurité.

## Méthodes pédagogiques :

**Formateurs de terrain** et cas réels, pour une application immédiate. **50% de pratique** et "Learning by Doing" pour ancrer les réflexes. Modalité pédagogique : 1ère journée en présentiel, les autres jours à distance. Un support de cours officiel sera fourni aux participants.

## Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement