ap Expert 360°

CABINET DU FUTUR - DCLIC

TOULOUSE

30 SEPTEMBRE 2026

Piraté à 8h00

Ce que vous devez faire avant midi

ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

30 SEPTEMBRE 2026

TOULOUSE

ORDRE DES EXPERTS-COMPTABLES RÉGION OCCITANIE

ap Expert 360° CABINET DU FUTUR - DCLIC

Jessica Ramond

Responsable commerciale PME · ITrust



30 SEPTEMBRE 2026
TOULOUSE

ORDRE DES EXPERTS-COMPTABLES RÉGION OCCITANIE

ap Expert 360° CABINET DU FUTUR - DCLIC

Chiffres-clés

57%

Entreprises françaises ciblées

par au moins 1 cyberattaque au cours des 12 derniers mois.

60%

Font faillite

(entreprises ayant subi une cyberattaque dans les 18 derniers mois).

59 600€

Coût moyen

d'une cyberattaque.

+27%

Hausse des attaques

1 347 cyberattaques revendiquées visant la France en 2025, contre 1 062 en 2024

(Sources : Rapport annuel sur la cybercriminalité 2026, rapport du gouvernement, BNP Entreprise, étude Hiscox 2025, rapport cyber Hiscox, Paul Curwell)

30 SEPTEMBRE 2026

TOULOUSE



ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

ap Expert 360°
CABINET DU FUTUR - DCLIC

Objectif

Partager un protocole de crise en 4 étapes-clés

- **Comment réagir dans les premières minutes**
- **Quels systèmes isoler**
- **Qui prévenir**
- **Comment limiter les dégâts**

30 SEPTEMBRE 2026

TOULOUSE

Agenda

01

Les 10 premières minutes

Ne pas aggraver la situation

02

Mobiliser en interne

03

Les obligations légales

RGPD, ANSSI, police…

04

Reprendre le contrôle

La sortie de crise

05

Q&A

30 SEPTEMBRE 2026

TOULOUSE



ORDRE DES EXPERTS-COMPTABLES RÉGION OCCITANIE

ap Expert 360° CABINET DU FUTUR - DCLIC

01- Les 10 premières minutes :

ne pas aggraver la situation

1 - Reconnaître les signaux d'une attaque en cours

Signaux évidents

- Message de rançon affiché à l'écran avec un compte à rebours
- Fichiers renommés avec une extension inconnue (.locked, .encrypted, .xxx)
- Alertes en cascade de l'antivirus mais plus de blocage
- Utilisateurs éjectés de leurs sessions simultanément

Signaux suspects

- Poste anormalement lent
- Connexions réseau sortantes inhabituelles, vers des IPs inconnues (nuit, weekend)
- Tentatives de connexion échouées répétées sur des comptes admin (brute force)
- Réception de mail confirmant un changement de mot de passe non demandé
- Disparition de fichiers ou copie vers un cloud non autorisé (OneDrive perso, Dropbox...)
- Accès RDP ou VPN depuis une localisation géographique / à un horaire incohérent

2 - Le réflexe n°1 : isoler sans éteindre

Pourquoi ne pas éteindre ? Éteindre = effacer toutes les infos précieuses (processus malveillants en cours d'exécution, clés de chiffrement potentiellement récupérables, connexions réseau actives vers les serveurs des attaquants, identifiants utilisés pour se déplacer latéralement dans le réseau).

Que signifie "isoler" ?

Débrancher le câble réseau

Désactiver Wi-Fi et Bluetooth

Ne pas déconnecter les USB

Les périphériques déjà branchés peuvent contenir des logs précieux.

Laisser la machine allumée

3 - Déconnexion réseau sans supprimer les logs

Préserver en priorité :

- Les journaux d'événements Windows (Event Viewer) ou Linux (/var/log/)
- Les logs du pare-feu et du proxy
- Les logs de l'Active Directory
- Les logs VPN et accès distants
- Les emails suspects reçus dans les heures/jours précédents

Comment les préserver sans risque :

Depuis un poste non compromis, faire une copie des logs sur un support externe (ex : clé USB propre).

Ne jamais copier les logs depuis la machine compromise elle-même.

30 SEPTEMBRE 2026
TOULOUSE

ORDRE DES EXPERTS-COMPTABLES RÉGION OCCITANIE

ap Expert 360° CABINET DU FUTUR - DCLIC

4 - Identifier le périmètre

⚠ Au moment de la détection, l'attaquant est probablement présent sur le réseau depuis plusieurs semaines.

Serveurs partagés ou NAS ?

Ce poste est-il connecté à des serveurs partagés ou à un NAS ?

Droits admin ? Données sensibles ?

L'utilisateur concerné a-t-il des droits admin ou accès à des données sensibles (de type R&D) ?

Autres utilisateurs impactés ?

D'autres utilisateurs signalent-ils des comportements anormaux ?

Sauvegardes ?

Y a-t-il des sauvegardes connectées en permanence au réseau ?

5 — Ce qu'il ne faut surtout pas faire

- **Payer la rançon immédiatement**
- **Redémarrer les machines**
- **Communiquer sur les canaux internes compromis**
- **Informer tout le monde immédiatement**
- **Effacer les traces**

30 SEPTEMBRE 2026

TOULOUSE



ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

ap Expert 360°
CABINET DU FUTUR - DCLIC

02- Mobiliser en interne

30 SEPTEMBRE 2026
TOULOUSE

ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

cap Expert 360°
CABINET DU FUTUR - DCLIC

1 - Qui prévenir ?

1. **RSSI / Responsable IT / Prestataire informatique**
   Dans les 5 premières minutes, pour prendre les premières décisions techniques.

2. **Directeur Général**
   Dans les 10 premières minutes, pour prendre les décisions stratégiques.

3. **DPO (Data Protection Officer)**
   Dans les 15 premières minutes, pour évaluer si des données personnelles sont concernées.

4. **Conseil juridique / DAF**
   Pour déclencher la couverture assurance cyber et documenter les décisions prises.

5. **Directeur Communication**
   Pour une communication de crise externe et interne maîtrisée.

Ces personnes constitueront a minima la cellule de crise.

2 - Documenter dès la première minute

Pourquoi documenter ?

Pour la plainte pénale, l'activation de l'assurance et la notification CNIL.
Chaque minute compte et chaque action doit être tracée.

Ce qu'il faut noter, en temps réel :

- L'heure exacte à laquelle l'incident a été détecté et par qui
- Les symptômes observés, poste par poste (captures d'écran si possible, photos)
- Chaque action prise : qui a fait quoi, sur quel système, à quelle heure
- Chaque appel passé : qui, quand, ce qui a été dit
- L'état des systèmes à chaque étape (fonctionnel, isolé, chiffré, restauré)

3 - Externaliser ou gérer en interne ?

Quand faut-il externaliser auprès d'un CSIRT ?

- Plusieurs postes ou serveurs simultanément touchés
- Suspicion d'une exfiltration de données sensibles
- Pas d'équipe sécurité en interne
- Message de rançon
- Notification requise auprès de la CNIL ou des clients (une analyse forensique est souvent demandée)

Quand une gestion interne est-elle envisageable ?

- Un seul poste isolé, sans propagation réseau
- Équipe IT expérimentée avec des outils de détection en place
- Données non critiques ou non personnelles

Un CSIRT (Computer Security Incident Response Team) est une équipe spécialisée dans l'analyse forensique et la remédiation d'incidents cyber.

30 SEPTEMBRE 2026

TOULOUSE



ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

cap Expert 360°
CABINET DU FUTUR - DCLIC

03- Les obligations légales :
RGPD, ANSSI, police…

30 SEPTEMBRE 2026
TOULOUSE

ORDRE DES EXPERTS-COMPTABLES RÉGION OCCITANIE

ap Expert 360° CABINET DU FUTUR - DCLIC

1 - RGPD : la notification CNIL en 72h

Quand notifier la CNIL ? Si des données personnelles sont compromises, consultées, volées, chiffrées, détruites ou modifiées sans autorisation (ex : dans une attaque ransomware ou une exfiltration).

72h, à partir de quand ? Dès que vous avez "connaissance" de la violation.

Ce que doit contenir la notification CNIL :

- La nature de la violation
- Si possible, les catégories et le nombre approximatif de personnes concernées par la violation
- Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés
- La description des conséquences probables de la violation de données
- La description des mesures prises ou envisagées pour éviter que cet incident se reproduise ou atténuer les conséquences négatives

Faut-il notifier les personnes concernées ?

Oui, dans certains cas : risque élevé pour les droits et libertés des personnes.

Sanctions en cas de non-notification

Amendes allant jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial.

Où se renseigner, comment notifier ? https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles

2 - Déclarer à la police ou à la gendarmerie

Pourquoi le faire ?

- Condition contractuelle de votre assurance cyber (dépôt de plainte = pré-requis à l'indemnisation)
- Trace officielle de l'incident qui protège l'entreprise en cas de litige ultérieur avec des tiers (clients, partenaires ou investisseurs)
- Enrichissement des bases de renseignement sur les groupes cybercriminels actifs

Où porter plainte ?

- Au commissariat de police ou à la gendarmerie
- En ligne : cybermalveillance.gouv.fr
- Directement auprès de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)

Délai recommandé : dans les 24 à 48h suivant la détection de l'incident, idéalement après avoir préservé les preuves et avoir une première vision du périmètre.

3 - Contacter l'ANSSI *Agence Nationale de la Sécurité des Systèmes d'Information*

Les entreprises qui ont une obligation de signalement à l'ANSSI :

- Les Opérateurs d'Importance Vitale (OIV) : secteurs défense, énergie, santé, transport, eau, finance
- Les Opérateurs de Services Essentiels (OSE) : environ 500 entités en France
- Depuis NIS2 : entités essentielles et entités importantes

Comment contacter l'ANSSI ?

- 3218 ou +33 9 70 83 32 18
- cert-fr@ssi.gouv.fr

Pour en savoir + : https://club.ssi.gouv.fr/#/declarations

Ce que NIS2 change :

Les obligations NIS2 incluent :

- La mise en place de mesures de gestion des risques
- La notification des incidents significatifs sous 24h (alerte initiale) puis 72h (notification complète)
- Des sanctions : max 10 millions d'euros ou 2% du CA mondial

30 SEPTEMBRE 2026

TOULOUSE



ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

cap Expert 360°
CABINET DU FUTUR - DCLIC

04- Reprendre le contrôle : la sortie de crise

Investiguer avec un prestataire qualifié

Un **CERT** ou **CSIRT** vise à accompagner des équipes dans le cadre de réponses à incident de sécurité informatique. Pour cela, il est amené à réaliser différentes missions et analyses :

DFIR
Digital Forensics Incident Response

Études de malware

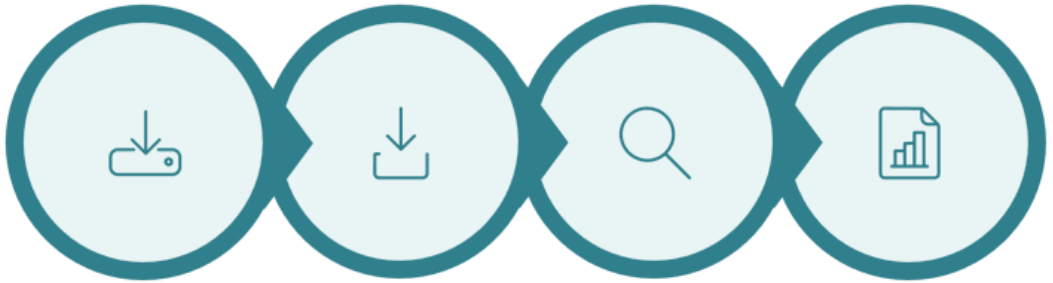
Accompagnement de crise

Support au SOC

> La réponse à incident est un travail **linéaire et cyclique** de recherche, de remédiation jusqu'à éviction complète des menaces. L'ensemble des actions effectuées par le CERT n'ont qu'un objectif : **remédier au maximum l'incident et limiter sa résurgence.**



L'analyse forensique



Acquisition **Parsing** **Analyse** **Restitution**

Acquisition et collecte

Suite au cadrage, un scope d'incident et de collecte a été défini. Le CERT récupère les données à chaud ou à froid :

- **Données complètes :** images disques, snapshots VMs…
- **Collecte partielle** via outils

Analyses d'artefact

Les systèmes disposent de différents mécanismes assurant leur bon fonctionnement :

- Journaux de sécurité
- Supervision de l'utilisation des ressources
- Historique des fichiers
- Lancement régulier d'applications

Parsing et ingestion

Les artefacts forensiques ne sont pas nécessairement exploitables en l'état :

- Bases de données ESE
- Registres Windows
- Fichiers NTFS

Restitution

Rapport d'analyse, présentation des preuves récoltées, des recherches réalisées et recommandations

30 SEPTEMBRE 2026

TOULOUSE

ORDRE DES EXPERTS-COMPTABLES RÉGION OCCITANIE

ap Expert 360° CABINET DU FUTUR - DCLIC

Les autres actions

1 Sécuriser avant de reconstruire

Avant de remettre le moindre système en service, assurez-vous que le vecteur d'entrée est identifié et fermé, et que les sauvegardes que vous allez restaurer sont saines.

2 Mettre en application son PRA

Mettre en application son Plan de Reprise d'Activité, le compléter si nécessaire.

3 Tirer les enseignements

Réunir la cellule de crise pour analyser ce qui s'est passé, identifier les failles et renforcer les défenses.

4 Planifier la communication de crise

Définir les messages, les canaux et les destinataires pour une communication maîtrisée vers les clients, partenaires et médias.

30 SEPTEMBRE 2026

TOULOUSE



ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

ap Expert 360°
CABINET DU FUTUR - DCLIC

Q&A

MERCI À NOS PARTENAIRES

ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE

BANQUE POPULAIRE OCCITANE

agiris.

BNCplus
Tout savoir sur la fiscalité du libéral

CAUDIA

LE LABEL CO-PILOTES

Cotélib

Dext By IRIS

ECMA

fulll

illinks GED DESIGNER

weekera

l'agence des experts-comptables

LVC

MyUnisoft

Pennylane

septeo Solutions Experts-Comptables

Tiime

SVP

Trajectoire

finthesis

inqom by VISMA

MyCompanyFiles

ap Expert 360°

CABINET DU FUTUR - DCLIC

TOULOUSE

30 SEPTEMBRE 2026

ORDRE DES EXPERTS-COMPTABLES
RÉGION OCCITANIE