INVICTIS

2025

CYBER-ATTACKS PLAYBOOK

QUE FAIRE DANS LES 60 PREMIÈRES MINUTES ?

Réagir vite. Protéger votre activité. Limiter l'impact.

CYBER ATTACK

QUE FAIRE DANS LES **60 PREMIÈRES MINUTES ?**

Chaque minute compte lors d'une attaque informatique.
Les cybercriminels ne dorment jamais, et les incidents surviennent toujours plus vite qu'on ne l'imagine. Beaucoup d'organisations perdent leurs moyens au pire moment.

Chez **Invictis**, nous avons accompagné de nombreuses entreprises lors de cybercrises majeures. **Une certitude : Ce que vous faites dans la première heure détermine l'impact de l'attaque.**

OBJECTIF : PROTÉGER, DOCUMENTER, REMONTER L'INFORMATION ET REPRENDRE LE CONTRÔLE.

PLAN D'ACTION

60 min

ÉTAPE 1 – ISOLER, PROTÉGER, CONTENIR (0–10 MINUTES)

- Déconnecter **uniquement les postes compromis ou suspects du réseau**
- **Bloquer les sessions** utilisateurs **compromises**
- Suspendre les accès distants si nécessaire (VPN, PAM…)
- **Interdire toute suppression ou nettoyage de systèmes**
- Conserver les logs et preuves numériques

- Message interne immédiat : « *Nous avons détecté un incident. Ne redémarrez aucun poste. Attendez les instructions de la cellule de crise.* »

ÉTAPE 2 – ALERTER LES BONNES PERSONNES (10–20 MINUTES)

Activation de la cellule de crise cyber :

- Responsable de Crise – CEO / RSSI : **Décision & arbitrage**
- Responsable technique DSI / SOC : **Confinement, suppression de la menace, restauration priorisée.**
- Juridique – DRH & DPO / Compliance : **Notification CNIL ≤ 72h si données personnelles**
- Assurance cyber – Courtier : **Déclenchement immédiat du sinistre & Experts agréés.**
- Équipes Métiers – Managers : **Coordination avec direction pour impact client**

À prévenir :

- DPO pour évaluation RGPD / CNIL
- ANSSI / CERT-FR selon statut OIV/OSN
- Assurance cyber (Si souscrite)
- Police / Gendarmerie pour dépôt de plainte

ÉTAPE 3 – DOCUMENTER CHAQUE ACTION (20–40 MINUTES)

Checklist :

- Heure de détection
- Symptômes
- Systèmes impactés
- Décisions prises
- Actions techniques réalisées
- Preuves collectées (logs, captures d'écran, mails)

Chaque minute compte comme preuve juridique. **Cette documentation est essentielle pour la CNIL, l'assureur, l'enquête judiciaire et RETEX.**

Votre préparation est insuffisante ? Faites appel à **INVICTIS** !

INVICTIS
Agir vite, Agir juste. ©

Contactez-nous : contact@invictis.fr | www.invictis.fr

CYBER ATTACK

QUE FAIRE DANS LES **60 PREMIÈRES MINUTES ?**

60 min

ÉTAPE 4 – COMMUNIQUER SANS PANIQUER (40–60 MINUTES)

Règles d'or :

1. **Dire ce qui est vrai, uniquement**
2. Garder le contrôle du narratif

Exemple de communication interne :
Objet : Incident de sécurité en cours – consignes immédiates

Nous avons détecté un incident. Ne redémarrez pas vos équipements et attendez les consignes officielles.

Un groupe dédié pilote la situation.

Exemple de communication externe :
Objet : Information – Mesures de sécurité en cours

Un incident est en cours d'analyse. Les mesures nécessaires ont été immédiatement engagées avec nos experts.

À ce stade, aucune preuve de compromission des données sensibles n'est confirmée.

OBLIGATIONS LÉGALES ET SANCTIONS

- **CNIL** : Notification sous 72h si violation de données personnelles
- **ANSSI / CERT-FR** : Notification si systèmes critiques, OIV / OSN
- **Assurance cyber** : Notification immédiate
- **Police / Gendarmerie** : Dépôt de plainte conseillé

CONSÉQUENCES POSSIBLES

- **Entreprise** : Amendes jusqu'à **4 % du CA (RGPD)**, perte de contrats, réputation compromise, mise sous surveillance réglementaire.
- **Dirigeant / DPO** : Responsabilité pénale et civile, auditions par autorités, risque de sanctions en cas de négligence avérée.
- **Clients** : Perte de confiance, préjudice, recours collectifs.
- **Collaborateurs** : Interruption de l'activité, exposition de données RH (Carte ID, N° SS, Numéro, E-mail, Adresse personnelle) / Action en responsabilité civile de collaborateurs lésés. Possibilité de dommages-intérêts.

RETEX POST-INCIDENT

À réaliser dans les 10 jours :

- Comment l'incident a-t-il été détecté ?
- Quelles mesures ont fonctionné ?
- Qu'aurait-on pu mieux faire ?
- Actions correctives et plan d'amélioration continue

Objectif : Transformer la crise en amélioration continue.

CONCLUSION

Les 60 premières minutes sont déterminantes. Les entreprises qui réagissent vite, documentent, alertent les autorités et tirent les leçons sont celles qui survivent et prospèrent.

Invictis vous accompagne :

- **Avant l'attaque** : Audit, renforcement, simulation.
- **Pendant l'attaque** : Gestion de crise, investigations.
- **Après l'attaque** : Remédiation, rapports CNIL/assurance, formation des équipes.

Contactez-nous : hello@invictis.fr | www.invictis.fr

INVICTIS
Agir vite, Agir juste. ©