

✧ Évènement - Entreprise

## Évènement 01

Phase 1 - Tour 1

### Indisponibilité généralisée des services

Début de l'incident

#### Suite d'évènements :

- **Agendas bloqués** : plusieurs employés et le secrétariat ne peuvent plus accéder aux agendas et gérer les rendez-vous avec les clients. Un client mécontent que son rendez-vous en visio, déjà reporté plusieurs fois, ait été raté, menace de rompre le contrat.
- **Système de paie et fichiers internes inaccessibles** (contrats, commandes) – le technicien support investigate sur les causes du problème.
- **Site web indisponible** : des collaborateurs constatent que le site web n'est plus accessible.

Face à cette situation, votre mission est de prendre les meilleures décisions pour répondre aux demandes des collaborateurs.

✧ Évènement - Entreprise

## Évènement 02

Phase 1 - Tour 2

### Inquiétude générale

Nous sommes à + 45min après l'incident

#### Suite d'évènements :

- **Indisponibilité de l'outil de gestion des livraisons** : Les camions se présentant à l'entrepôt ne peuvent plus être redirigés.
- **Exigence des investisseurs** : un investisseur, informé par un client, s'inquiète de la panne informatique et exige un **point de situation toutes les 20 min.**
- **Gestion de la paie** : l'indisponibilité implique un risque de non-versement **sous 72h** pour les agents.
- **Volet technique** : les investigations sont en cours, mais prennent du temps : un seul technicien est mobilisé

## Évènement 03

Phase 2 - Tour 1

### Confirmation d'une cyber attaque

Nous sommes à +1h30 après l'incident

#### Suite d'évènements :

- **La cyberattaque (rançongiciel) est confirmée :**
  - **Les systèmes sont bloqués :** paie, gestion des congés et des absences, outil de gestion logistique, site web, et certains fichiers hébergés sur les serveurs internes.
  - Le technicien est débordé : **des renforts sont nécessaires.**
- **Gestion dégradée :**
  - Les équipes dans l'entrepôt se trouvent en sous-effectif pour gérer les commandes sans outils.
  - Un client exige de désactiver l'outil de gestion logistique pour éviter une propagation vers son propre système.
- **Risques sociaux :** Les représentants du personnel **menacent d'utiliser leur droit de retrait** à cause du manque d'information disponible.
- **Volet médiatique :** Des journalistes tentent d'obtenir des informations auprès des collaborateurs.

## Évènement 04

Phase 2 - Tour 2

### Constat de l'ampleur de l'impact

Nous sommes à +3h après l'incident

#### Suite d'évènements :

- **Volet technique :** les sauvegardes sont compromises, la **récupération s'avère incertaine et lente.**
- **Demande de rançon :** une demande de **rançon de 500 000 euros** a également été publiée par les attaquants.
- **Inquiétudes :** les clients s'inquiètent très fortement du **retard induit** par l'indisponibilité des outils.
- **Gestion dégradée :** les équipes demandent des renforts et la **mise en place d'un système de repos** pour tenir dans la durée.

✱ Évènement - Entreprise

## Évènement 05

Phase 3 - Tour 1

### Détection de fuite de donnée

Nous sommes à +6h après l'incident

#### Suite d'évènements :

- **Fuite de données** : un collaborateur signale que **les attaquants revendiquent avoir volé et publié des données** sur le dark web (analyse en cours).
- **Volet technique** : La dernière sauvegarde saine date d'une semaine. Il faudra **3 jours pour la réinstaller**, puis relancer progressivement les applications.
- **Volet médiatique** : un client **dénonce le manque d'investissements** en matière de cybersécurité sur les réseaux sociaux

✱ Évènement - Entreprise

## Évènement 06

Phase 3 - Tour 2

### Adaptation en mode dégradé

Nous sommes à +7h après l'incident

#### Suite d'évènements :

- **Volet technique** :
  - **100% des serveurs sont chiffrés** : un **rachat est nécessaire** pour reconstruire une infrastructure saine.
  - **Plus de 50% des postes sont infectés** → 70 postes sont à remplacer.
  - **La fuite de données est confirmée** (contrats, noms, mails - clients/ collaborateurs).
- **Gestion dégradée** :
  - **3 semaines minimum** prévues.
  - La commande des **chèques-vacances** doit être validée sous 24h, mais le fichier de **commandes est inaccessible**.
- **Volet médiatique** :
  - 2 journalistes relancent les collaborateurs.
  - 1 tweet et 1 article local ont été publiés sur la **fuite de données** et le **risque de retard de livraisons**.