flowlysis.

LES PREMIÈRES HEURES D'UN INCIDENT

Un tableau d'une page donne à chaque décision de crise un titulaire et un suppléant. Il s'écrit et s'exerce à froid, pour qu'au premier appel personne ne cherche qui décide pendant que le délai de notification court.

AUSSI APPELÉ tableau de crise, exercice sur table, tabletop exercise **PRINCIPE QU'IL APPLIQUE** fiche P-14 **SE PRÉPARE EN** deux réunions de 2 h

SE FAIT EN 2 à 3 h d'exercice sur table **LEVIER PRINCIPAL** Coût du retard

CE QUE ÇA RAPPORTE		CE QUE ÇA COÛTE	
Impact sur le TTM	Faible	Coût d'implémentation	Faible
Impact sur la qualité (FTR)	Moyen	Difficulté d'implémentation	Faible
Impact sur l'Opex / Capex	Élevé	Difficulté de maintien	Moyen

Faible · Moyen · Élevé · N/A (sans objet)

1 Le problème auquel ça s'applique

Et ce qu'il vous coûte chaque année

CE QUE VOUS VOYEZ DÉJÀ

- « Si on se fait chiffrer demain, qui appelle qui ? » Trois réponses.
- Le plan de crise dort sur le serveur qui tomberait le premier.
- Le dernier exercice date de l'audit. Seule l'informatique y était.

OÙ PART L'ARGENT

Tant que personne n'ose isoler, le chiffrement gagne d'autres serveurs. Le délai de l'alerte précoce court dès que l'entité a eu connaissance de l'incident important (NIS2, art. 23.4). Ce moment suit une première évaluation qui le rend raisonnablement certain, pas la fin de l'analyse.

L'ORDRE DE GRANDEUR, À LA LOUCHE

Comptez-le avec votre CISO. Un ordre de grandeur suffit pour décider d'essayer.

COMBIEN DE FOIS / AN		CE QUE ÇA COÛTE À CHAQUE FOIS		PART QU'ON ÉVITE	=	DÉPENSE ÉVITÉE / AN
alertes qui exigent d'isoler un service	×	serveurs touchés × heures de restauration	×	part des serveurs épargnés en isolant plus tôt	=	**à écrire après un exercice**

QUAND ÇA NE SERT À RIEN

Pour l'incident courant, un poste infecté par exemple : l'équipe de sécurité de garde le traite selon sa procédure. Le tableau sert quand la décision la dépasse.

2 Comment ça marche

La mécanique, en clair

L'IDÉE EN UNE PHRASE

Chaque décision des premières heures porte un nom écrit à froid. Deux chantiers partent ensemble : contenir, et préparer la notification.

LES GESTES, DANS L'ORDRE

1. Lister les décisions des premières heures, mode dégradé compris (fiche O-70).
2. Nommer titulaire et suppléant ; sans réponse en 15 min, le suppléant décide.
3. Ouvrir les deux chantiers ensemble, un point court par heure (fiche O-61).
4. Écrire le délai de chaque notification et son point de départ.
5. Garder les contacts d'urgence sur papier, hors des systèmes.
6. S'exercer sur table. L'ANSSI cite un rythme d'un exercice par an ou tous les deux ans.

CE QU'IL FAUT AVOIR SOUS LA MAIN

La qualification de l'entité, vérifiée par un juriste. Une entité financière soumise à DORA déclare ses incidents majeurs liés aux TIC selon DORA, et non selon NIS2 (DORA, art. 1.2 et 19). **En Belgique** : incident significatif au CCB, sur notif.safeonweb.be (guide v1.3, août 2025) ; données personnelles à l'APD ; DORA : à la BNB, ou à la FSMA pour les entités qu'elle seule contrôle.

LE SIGNE QUE ÇA A MARCHÉ

À l'exercice, le suppléant décide l'isolement sans chercher le titulaire.

3 Les pièges de l'implémentation

Ce qui fait rater, et ce qu'on fait à la place

AU LANCEMENT — Un plan que personne n'ouvre
Quarante pages écrites pour l'audit. Le soir de l'incident, personne ne les cherche.
→ Une page, une ligne par décision, un seul titulaire par ligne (fiche O-30).

AU LANCEMENT — Les contacts dans la messagerie
L'annuaire est chiffré avec le reste. On cherche le numéro du prestataire sur son site.
→ Une liste papier chez chaque titulaire, et les numéros dans les téléphones personnels.

PENDANT — Un exercice réservé à l'informatique
L'équipe répète la restauration. Personne n'a décidé d'informer les clients.
→ Les titulaires métier autour de la table, et chaque écart traité en A3 (fiche O-10).

PENDANT — Compter le délai depuis la fin de l'analyse
On attend d'avoir tout compris pour notifier. Le délai, lui, court dès qu'une première évaluation rend l'incident important raisonnablement certain.
→ Noter l'heure de la découverte et de la première évaluation, et préparer l'alerte.

DANS LA DURÉE — Un tableau qui vieillit
Le suppléant est parti il y a six mois. Son numéro sonne dans le vide.
→ Revoir le tableau à chaque départ d'un titulaire et à chaque exercice.

4 Exemple

Cas type du tertiaire, du constat au résultat

LA SITUATION DE DÉPART

L'OBJET

Un prestataire de services informatiques gérés de 160 personnes, qualifié d'entité importante NIS2 par son juriste (hypothèse du cas).

CE QUI CLOCHE

Un vendredi à 19 h 40, un technicien voit des fichiers chiffrés. Personne ne sait qui peut couper l'outil qui relie l'entreprise à ses 140 clients.

CE QU'ILS REGARDAIENT AVANT

Le taux de réussite des sauvegardes, à 99 % chaque mois. Il ne disait pas qui déciderait de couper.

LES CHIFFRES DE DÉPART, LE JOUR DE L'INCIDENT

4 h 50	entre la découverte et l'isolement
39	serveurs chiffrés à l'isolement
5 h	de restauration par serveur
21 h 20	entre la découverte et l'alerte précoce

CE QU'ILS ONT FAIT

Un tableau d'une page, puis le même vendredi soir rejoué sur table avec les vrais titulaires.

LE DÉCLENCHEUR	▶	LE GESTE	▶	CE QU'ILS ONT VU	▶	LA DÉCISION
L'isolement décidé à 0 h 30, après cinq appels sans réponse.		Sept décisions, chacune avec un titulaire et un suppléant, sur une page imprimée.		Rejoué sur table : isolement à 20 h 25, alerte précoce prête à 23 h 10.		Un exercice par an, avec un scénario nouveau chaque fois.

CE QUE ÇA A DONNÉ

4 h 50 → 45 min — Le délai avant l'isolement : de 19 h 40 à 0 h 30 le jour de l'incident, de 19 h 40 à 20 h 25 au rejeu.

39 → 6 serveurs — À rythme constant : 39 en 4,83 h, soit 8 par heure ; au rejeu, 0,75 h × 8 = 6. Soit 33 × 5 h = 165 h de restauration évitables.

2 h 40 → 20 h 30 — La marge sur l'alerte précoce de 24 h (hypothèse prudente : délai compté dès 19 h 40) : 24 h − 21 h 20, puis 24 h − 3 h 30. Au rejeu, la notification s'ouvre à 20 h 05, avec la crise.

43 h — Ce que ça a coûté : deux réunions de 2 h à quatre (16 h), un exercice de 3 h à neuf (27 h).

Refaites-le avec votre scénario : un vendredi soir, vos vrais titulaires, l'heure de chaque décision notée. Posez l'écart à 24 h sous le tableau.

1 · LE TABLEAU, UNE LIGNE PAR DÉCISION

DÉCISION	TITULAIRE / SUPPLÉANT	CE QU'IL LUI FAUT
Déclarer la crise	COO / directeur général	ce qu'on voit, et où ça s'étend
Isoler ou arrêter un service	CISO / astreinte infra	ce que l'arrêt coupe, et chez qui
Passer en mode dégradé	COO / chef de service	la procédure manuelle (fiche O-70)
Informer clients et personnel	COO / communication	ce qu'on sait, ce qu'on ignore
Notifier l'autorité	juriste / COO	l'heure de la prise de connaissance, l'impact
Notifier une violation de données	juriste / COO	avec le délégué RGPD, les données touchées
Appeler la réponse à incident	CISO / responsable infra	le contrat, l'assureur, le n° d'astreinte

Contenir — titulaire : le CISO ; isoler sans effacer de preuve

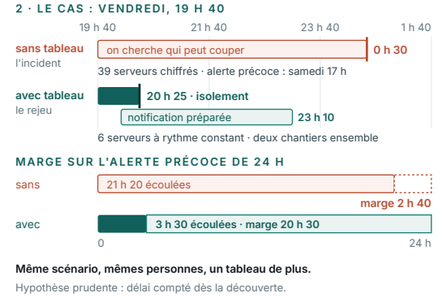
Préparer la notification — titulaire : le juriste, en même temps

L'HORLOGE NIS2 PART DE LA CONNAISSANCE (ART. 23.4)

0 (connaissance) · dans les 24 h (alerte précoce) · dans les 72 h (notification d'incident) · un mois après la notification (rapport final)

RGPD, art. 33 : violation de données personnelles, dans les meilleurs délais et si possible 72 h au plus tard après en avoir pris connaissance, sauf si elle n'est pas susceptible d'engendrer un risque.

2 · LE CAS : VENDREDI, 19 H 40



Même scénario, mêmes personnes, un tableau de plus.
Hypothèse prudente : délai compté dès la découverte.

À gauche le tableau, les deux chantiers et l'horloge NIS2. À droite les six premières heures du cas, le jour de l'incident puis au rejeu, et la marge restante sur l'alerte précoce.

L'exemple est un cas type, reconstruit à partir de situations courantes du tertiaire. Aucune situation client n'y est identifiable.