CRA · NIS2 · RGPD

Les 24 premières heures : un modèle d'alerte précoce pour le CRA, NIS2 et le RGPD

Sortez cette fiche dès que quelqu'un dit « cette vulnérabilité est exploitée » ou « cet incident a l'air important ». Elle liste ce que doit contenir chaque premier message, et ce qu'il faut garder prêt pour la suite.

1. Lancer le chronomètre

Notez la date, l'heure et le fuseau horaire auxquels vous en avez eu connaissance. Les délais du CRA et de NIS2 partent de ce moment, pas du tri du ticket ni de la fin de l'enquête.

Notez qui a décidé, et les faits connus à ce moment-là. On vous les demandera plus tard.

2. CRA : une vulnérabilité activement exploitée dans votre produit (fabricants)

Envoyé via la plateforme unique de signalement de l'ENISA au CSIRT désigné comme coordinateur. Obligation de signalement applicable depuis le 11 septembre 2026.

Alerte précoce · 24 heures	La présence d'une vulnérabilité activement exploitée dans le produit ; le cas échéant, les États membres où vous savez que le produit a été mis à disposition. (art. 14, § 2, a)
Notification de la vulnérabilité · 72 heures	Informations générales sur le produit ; nature générale de l'exploitation et de la vulnérabilité ; mesures correctives ou d'atténuation prises, et celles que les utilisateurs peuvent prendre ; degré de sensibilité que vous attribuez à ces informations. (art. 14, § 2, b)
Rapport final · 14 jours après la mise à disposition d'une correction ou d'une atténuation	Description de la vulnérabilité, avec sa gravité et son impact ; le cas échéant, informations sur tout acteur malveillant ; détails de la mise à jour de sécurité ou des autres mesures correctives. (art. 14, § 2, c)

> Un incident grave ayant un impact sur la sécurité de votre produit suit les mêmes étapes à 24 et 72 heures (avec, dans l'alerte précoce, s'il est soupçonné d'être causé par des actes illicites ou malveillants) et un rapport final dans un délai d'un mois après la notification d'incident (art. 14, § 3 et 4). Informez les utilisateurs concernés, et si besoin tous les utilisateurs, de la vulnérabilité ou de l'incident et des mesures qu'ils peuvent prendre (art. 14, § 8).

3. NIS2 : un incident important (entités essentielles et importantes)

Envoyé à votre CSIRT ou à votre autorité compétente, selon la transposition nationale.

Alerte précoce · 24 heures	Si l'incident est soupçonné d'être causé par des actes illicites ou malveillants, et s'il pourrait avoir un impact transfrontière. (art. 23, § 4, a)
Notification d'incident · 72 heures	Mise à jour de l'alerte précoce ; évaluation initiale, avec gravité et impact ; indicateurs de compromission, s'ils sont disponibles. (art. 23, § 4, b)
Rapport intermédiaire	À la demande du CSIRT ou de l'autorité compétente. (art. 23, § 4, c)

Rapport final · un mois après la notification	Description détaillée, avec gravité et impact ; type de menace ou cause profonde probable ; mesures d'atténuation appliquées et en cours ; impact transfrontière, le cas échéant. Si l'incident est toujours en cours : un rapport d'avancement à la place, puis le rapport final un mois après son traitement. (art. 23, § 4, d et e)

4. RGPD : une violation de données personnelles

Autorité de contrôle · 72 heures, si possible	Sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes. Nature de la violation, avec les catégories et le nombre approximatif de personnes et d'enregistrements concernés ; point de contact ; conséquences probables ; mesures prises ou proposées. Les informations peuvent être données en plusieurs fois. (art. 33, § 1, 3 et 4)
Personnes concernées · dans les meilleurs délais	Quand la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés. (art. 34)
Chaque violation, notifiée ou non	Documentée : faits, effets et mesures prises. (art. 33, § 5)

5. À remplir maintenant

Connaissance le (date, heure, fuseau)	
Décidé par	
Produit ou service, et versions	
S'applique : vulnérabilité CRA · incident grave CRA · NIS2 · RGPD · autre (ex. DORA : délais de votre superviseur financier, non traités ici)	
Actes illicites ou malveillants soupçonnés ?	
Impact transfrontière ? États membres	
Échéance des 24 heures	
Échéance des 72 heures	
Envoyé le, par qui, référence reçue	
Utilisateurs informés (quand, comment)	

Dans Jira : Clearlane CRA décompte chaque délai du CRA depuis l'heure de connaissance enregistrée, prépare chaque champ à coller dans la plateforme de l'ENISA et garde le texte exact envoyé. Clearlane Breach & Incident Reporting (bientôt disponible) fera de même pour NIS2, le RGPD et DORA. **clearlaneapps.com/fr/solutions/cyber**

Une aide de travail, pas un avis juridique. Vérifiez le texte de chaque règlement et les consignes de votre autorité nationale. Références : règlement (UE) 2024/2847 (CRA), article 14 ; directive (UE) 2022/2555 (NIS2), article 23 ; règlement (UE) 2016/679 (RGPD), articles 33 et 34.