esea
LA E-SANTÉ NOUVELLE-AQUITAINE

URPS PHARMACIENS Nouvelle-Aquitaine

Pharmacies d'officine : Sensibilisation aux bonnes réactions en cas de cyber attaque



Présentation : Mathieu DUCOS (Esea)

Introduction : Dr Marie-Hélène TESSIER
(Présidente de l'URPS Pharmaciens NA)

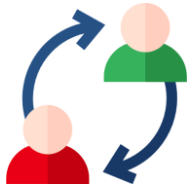
Pendant le webinaire :



- Vos micros sont fermés



- Vous pouvez poser vos questions à l'écrit dans le tchat, nous y répondrons après chaque fin de partie



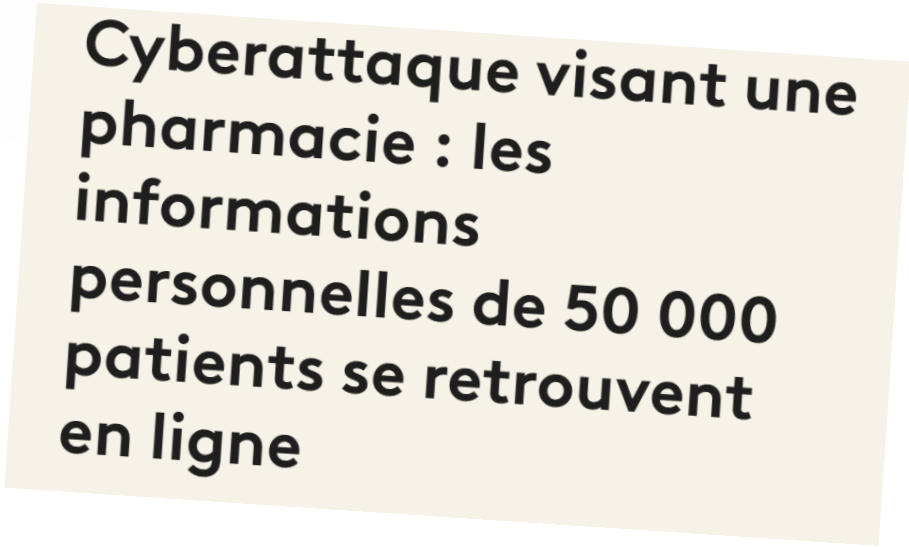
- Un temps d'échange est également prévu à la fin de la présentation

Quelques exemples de situation


OFFICINE

7 novembre 2026 · 4 min de lecture

Trois pharmacies piratées : l'accès à distance en cause, les gestes à faire tout de suite


Cyberattaque visant une pharmacie : les informations personnelles de 50 000 patients se retrouvent en ligne


25 septembre 2026 à 15h50 · Attaque

PHARMALAND : PRÈS DE 6 800 FICHES LIÉES AUX PHARMACIES EN FUITE

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

1 Qu’est-ce qu’une crise / incident cyber ?

2 Quelles sont les actions à réaliser ?

3 Quelques exemples d’attaques types



Qu’est-ce qu’une crise / incident cyber ?



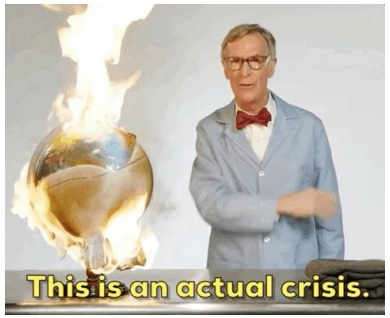
Qu’est-ce qu’une crise ?

Anomalie, Incident, Crise ?

Une Anomalie _____ est un événement de courte durée qui perturbe involontairement le fonctionnement nominal d'un système, sans conséquences majeures pour la structure.

Un incident _____ est un événement compromettant la disponibilité, l'intégrité ou la confidentialité des données engendrant un dysfonctionnement significatif pour la structure ou la mise en danger d'un patient.

La crise _____ génère une déstabilisation majeure de l'organisation et des métiers, provoquant des impacts multiformes et importants, jusqu’à engendrer parfois des dégâts irréversibles ou des risques pour la vie.



INCIDENT

Dès le constat d' une anomalie majeure, identifiez le **scénario** pour adopter le bon réflexe technique :

SCÉNARIO A : Bug ou Panne Logicielle

- Redémarrer le poste. Si le problème persiste, **éteindre l'ordinateur**.
- Sortir le classeur **"Mode dégradé"**.

SCÉNARIO B : Suspicion de cyberattaque (Écran bloqué, fichiers cryptés)

- **NE PAS ÉTEINDRE LE PC** (pour conserver les preuves techniques).
- **Déconnecter immédiatement le câble réseau** (Ethernet) ou **couper le Wi-Fi.**
- Alerter votre support informatique et passer en mode 100% papier.

Quelles sont les actions à réaliser? (administratif)



Gestion de la crise

Quels sont les éléments à intégrer dans une main courante ?

- ❑ Recommandations pour sanctions disciplinaires
- ☒ Horaire (début, avancement et fin de la crise)
- ☒ Lieu (serveur machine ou lieu physique)
- ❑ Estimation budgétaire des réparations
- ☒ Rédacteur de la main courante
- ☒ Contexte de l'incident
- ☒ Les impacts sur le SI
- ❑ Score de conformité RGPD de l'incident

Main courante et relevé d'actions

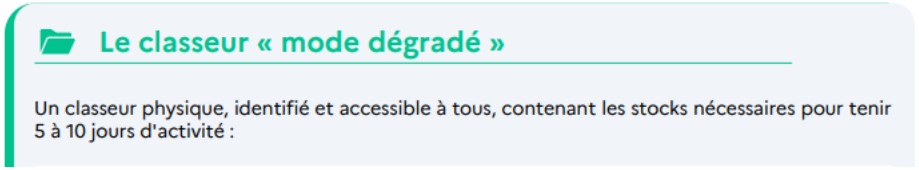
Cette main courante constitue la trace écrite de tous les événements se déroulant entre le déclenchement et la fin de la crise

Ouverture de la main courante :	Date :	Heure :
Fermeture de la main courante :	Date :	Heure :
Rédacteur(s) de la main courante :		
Responsable de la cellule :		

#	Date	Heure	Type *Information / Décision / Action*	Description	Porteur	Statut *Non initié / En cours / Finalisé / Annulé*	Echéance	Commentaires *Suivi des actions et résolution*
1								
2								
3								

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Gestion de la crise



L'objectif :

- Pouvoir continuer à travailler malgré une panne ou une cyber attaque

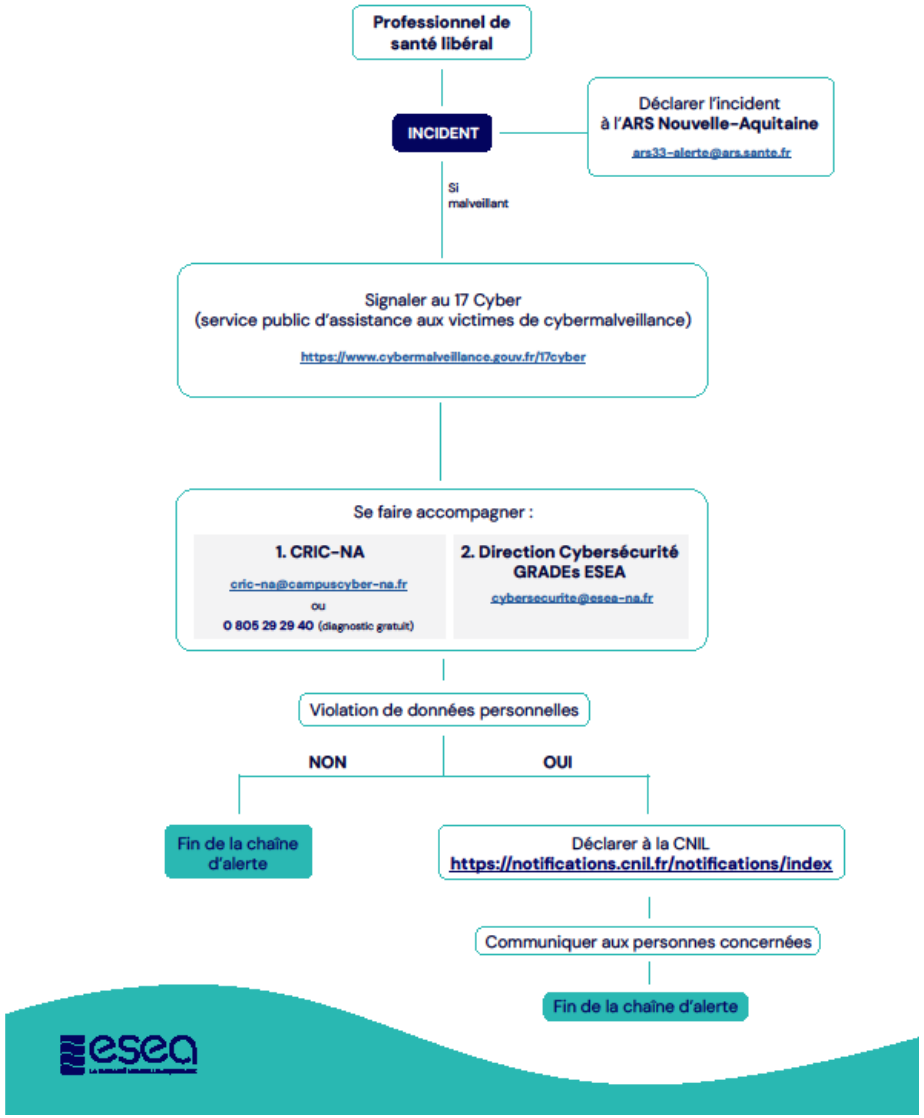
Le secret l'anticipation !!

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Chaîne d'alerte en cas d'incident

PROFESSIONNEL DE SANTÉ LIBÉRAL

Mai 2025



Accessible ici

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Déclaration de l'incident

Si Malveillant

Signaler au 17 Cyber
(service public d'assistance aux victimes de cybermalveillance)

https://www.cybermalveillance.gouv.fr/17cyber

Déclarer l'incident
à l'**ARS Nouvelle-Aquitaine**

ars33-alerte@ars.sante.fr

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Se faire accompagner

Se faire accompagner :

1. CRIC-NA

cric-na@campuscyber-na.fr

ou

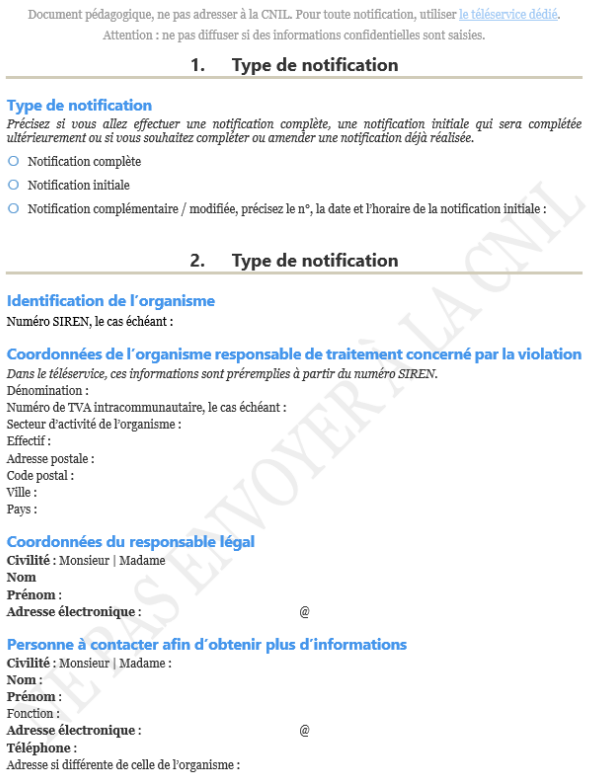
0 805 29 29 40 (diagnostic gratuit)

2. Direction Cybersécurité GRADEs ESEA

cybersecurite@esea-na.fr

Signalement à la CNIL

Déclarer à la CNIL
https://notifications.cnil.fr/notifications/index



Document pédagogique, ne pas adresser à la CNIL. Pour toute notification, utiliser le téléservice dédié.
Attention : ne pas diffuser si des informations confidentielles sont saisies.

1. Type de notification

Type de notification

Précisez si vous allez effectuer une notification complète, une notification initiale qui sera complétée ultérieurement ou si vous souhaitez compléter ou amender une notification déjà réalisée.

- ○ Notification complète
- ○ Notification initiale
- ○ Notification complémentaire / modifiée, précisez le n°, la date et l'horaire de la notification initiale :

2. Type de notification

Identification de l'organisme

Numéro SIREN, le cas échéant :

Coordonnées de l'organisme responsable de traitement concerné par la violation

Dans le téléservice, ces informations sont préremplies à partir du numéro SIREN.

Dénomination :
Numéro de TVA intracommunautaire, le cas échéant :
Secteur d'activité de l'organisme :
Effectif :
Adresse postale :
Code postal :
Ville :
Pays :

Coordonnées du responsable légal

Civilité : Monsieur | Madame
Nom
Prénom :
Adresse électronique : @

Personne à contacter afin d'obtenir plus d'informations

Civilité : Monsieur | Madame :
Nom :
Prénom :
Fonction :
Adresse électronique : @
Téléphone :
Adresse si différente de celle de l'organisme :

PAS ENVOYER À LA CNIL

Le signalement implique :

- Identifier la violation de données personnelles
- Tenir un registre des violations
- Notifier la violation à la CNIL
- Communiquer la violation aux personnes concernées

Communiquer aux personnes concernées

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Interlude RGPD

Quels sont les obligations RGPD pour une officine ?

- Désignation d'un DPO activité globale annuelle de plus de 2 600 000 € HT (conseillé dans tous les cas)
- Avoir un registre de traitement des données personnelles
- Informer les personnes dont vous traitez les données
- Avoir défini des durées de conservation des données

https://www.cnil.fr/sites/cnil/files/2023-09/guide-rgpd-cnop_cnil.pdf

Quelques exemples d'attaques types



Phishing



LInkedin

Bonjour Alexandre,

Vous avez ajouté une nouvelle adresse e-mail à votre compte LinkedIn.

Pour confirmer cette adresse veuillez cliquer sur ce lien ou le coller dans votre navigateur :

https://www.linkedin.com/psettings/sign-in-and-security

Nous vous demanderons ensuite de vous identifier. Assurez-vous d'utiliser l'adresse e-mail sur laquelle vous souhaitez recevoir les messages, les invitations et les demandes.

Merci d'utiliser LinkedIn !
L'équipe LinkedIn

Se désinscrire | Aidez-moi

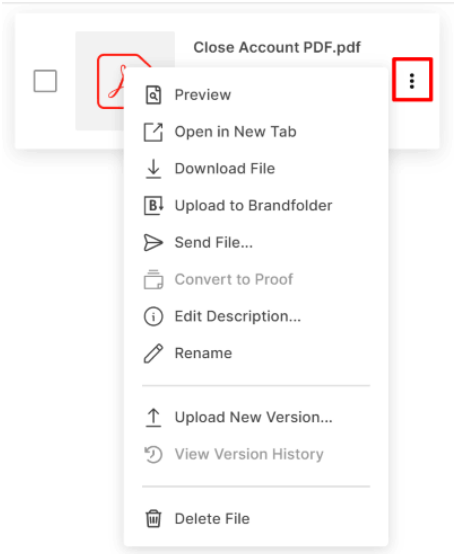
La pharmacie se fait pirater une boite mail via un mail de phishing.

Phishing

Quelles sont les actions à réaliser dans ce cas :

- [x] Contacter votre prestataire informatique pour désactiver la boite mail. Et connaître les actions réalisées par l'attaquant
- [ ] Supprimer immédiatement tous les mails suspects et vider la corbeille.
- [x] Contacter les personnes à qui des mails de phishing ont été envoyé
- [ ] Attendre de voir si le pirate utilise à nouveau la boîte mail avant d'intervenir.
- [ ] Signaler systématiquement l'incident à la CNIL dans les 72 heures, quel que soit son impact.
- [ ] Continuer à utiliser normalement la messagerie en attendant que le problème se règle.

Poste corrompu

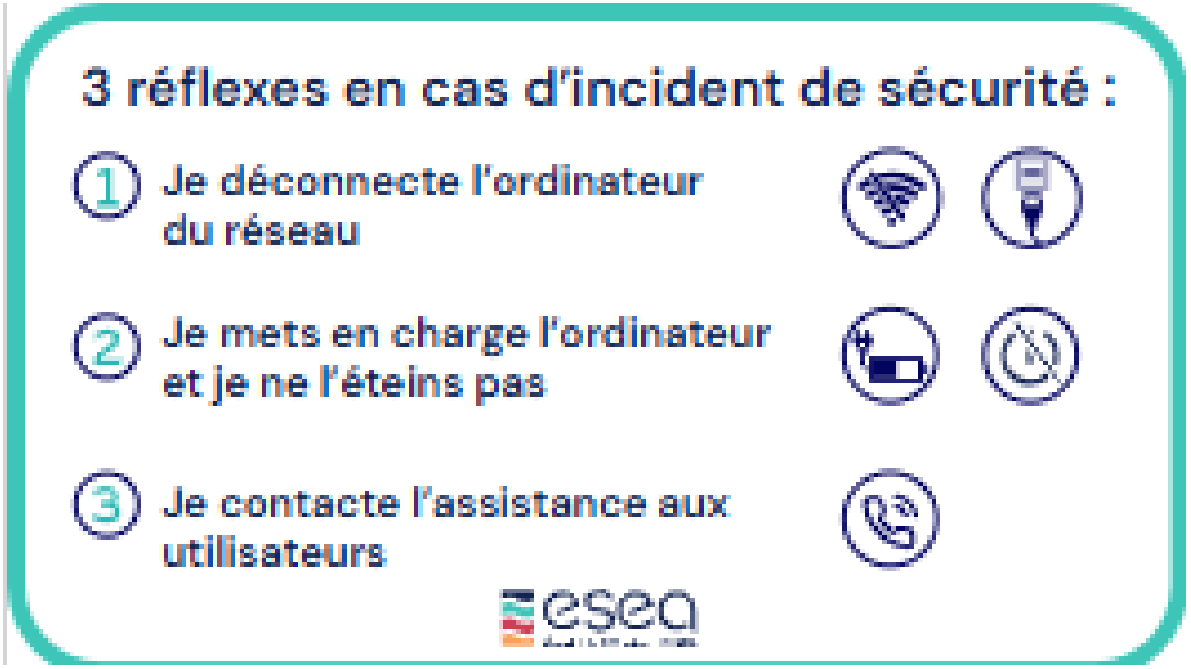






esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Poste corrompu



- Contacter votre prestataire informatique si vous en avez un.
- Isoler le poste du reste du réseau
- Réaliser les actions juridiques

Quelques exemples de situation

OFFICINE 7 novembre 2026 · 4 min de lecture

Trois pharmacies piratées : l'accès à distance en cause, les gestes à faire tout de suite

Fuite de données via des accès distants:



TeamViewer

AnyDesk

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

Fuite de données via des accès distants:

À vérifier au sein de l'officine :

- Avec vos prestataires et éditeurs, identifiez les outils de prise en main à distance installés (AnyDesk, Splashtop, TeamViewer, RustDesk, VNC, etc.) et le prestataire qui utilise chacun d'eux. Faites désinstaller tout outil inutilisé ou dont vous ne pouvez pas identifier le prestataire.
- Pour chaque outil conservé, **désactivez l'option « accès sans surveillance »** et activez la **validation manuelle depuis l'officine avant chaque connexion**. Vérifiez l'identité de l'intervenant avant d'accepter sa demande.
- Changez sans délai les mots de passe d'accès de tous les outils de prise en main à distance conservés.

À vérifier auprès de chacun de vos prestataires informatiques :

- Protéger sa console de maintenance par une authentification multifacteur (MFA) et utiliser un compte nominatif pour chaque intervenant.
- Ouvrir chaque session avec un compte utilisateur standard, sans droits administrateur, et limiter les accès aux seuls besoins de l'intervention.
- Maintenir à jour les outils de prise en main à distance utilisés et désinstaller ceux devenus inutiles.

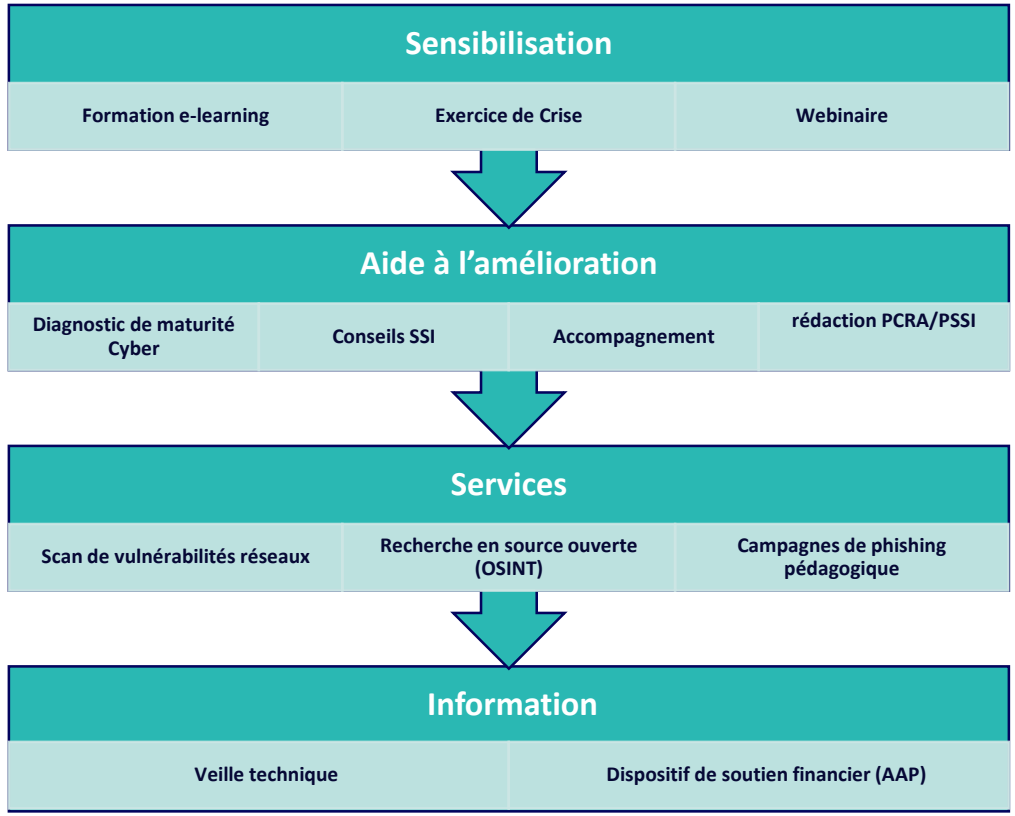
Merci de votre attention

Adresse de contact

- *cybersecurite@esea-na.fr*

Présentateurs

- Mathieu Ducos



URPS PHARMACIENS Nouvelle-Aquitaine

esea
LA E-SANTÉ NOUVELLE-AQUITAINE