

FORMATION SPECIALISEE DE SITE
DES LYCEES ET DU CREPS
Réunion du 5 mars 2026

RAPPORT POUR INFORMATION

Cyberattaque sur le système d'information des lycées
Etat de situation au 26 janvier 2026

Rappel du contexte évoqué lors de la FSS de novembre 2025

- Une cyberattaque d'ampleur a impacté, vendredi 10 octobre 2025, une large partie du système d'information des lycées publics par ransomware, revendiquée par le groupe Qilin, hackers de dimension internationale.
- Dès la détection de l'attaque du domaine edu.hdf par le service Urbanisation du SI du Département du Numérique Educatif (Direction des Politiques éducatives, Pôle PEAJ), les services ont alerté la hiérarchie, ainsi que les autorités académiques et la DRAAF, et se sont organisés collégialement pour limiter l'impact de l'attaque par arrêt des serveurs.
- Un prestataire, Orange Cyber Défense (service d'expertise en cyber sécurité), et la DSI accompagnent, depuis la détection, les services du DNE et ce afin de contenir l'attaque, sécuriser les infrastructures et protéger les données, dans le souci constant des usagers.
- Le plan d'actions à mettre en œuvre afin de rétablir le service dans les meilleurs délais a été aussitôt défini avec Orange Cyber Défense.

Plan général d'actions

Sécurisation primaire :

- Premières mesures conservatoires et d'isolement avec extinction des équipements situés dans les datas center, centres névralgiques de l'infrastructure réseaux lycées, des serveurs et des sauvegardes (488) sur 237 sites. Dans le même temps il a été demandé l'extinction de tous les ordinateurs des lycées.
- La déclaration de la cyberattaque a été réalisée dès le vendredi 10 octobre à l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et à la CNIL. Une plainte a été déposée auprès de la Gendarmerie nationale.
- Organisation de cellules de gestion technique de crise entre les services régionaux et Orange cyber défense pour la mise en place des opérations techniques, et organisation de cellules opérationnelles et décisionnelles (Région, ministère de l'éducation nationale, ANSSI, COSIM et partenaires académiques, DRAAF), ces cellules pouvant se réunir plusieurs fois par jour afin de définir collégialement les enjeux, les risques, les points d'étape, la priorisation, la méthodologie et la communication.

Etat d'avancement au 26 janvier

Plan de remédiation :

Dès que la gendarmerie a donné l'autorisation à la Région de reconstruire les infrastructures, soit à partir du 28 octobre :

1^{ère} phase :

Remise en fonctionnement dégradé de l'administratif et du fonctionnement des lycées

Dans un premier temps et pour permettre aux services administratifs (priorité arrêtée en cellule de crise décisionnelle) de fonctionner à nouveau en mode dégradé, il a été convenu de déployer une application de protection. Cet outil peut être vu comme un antivirus de nouvelle génération avec analyse comportementale.

Une extrême vigilance et une très grande prudence ont été observées dans le rétablissement progressif des services, les hackers ayant tenté des récidives.

7100 postes informatiques ont ainsi été protégés et ont pu accéder à internet dès début novembre.

Une stratégie de solution d'impression a minima pour les postes administratifs et d'enseignants a également été conçue.

Le rétablissement des services de restauration, a également été effectué à cette période.

Remise en fonctionnement dégradé de la pédagogie :

Parallèlement, les équipes ont protégé et réactivé l'accès à internet des **90 000 ordinateurs pédagogiques dès le 28 novembre**.

Les **250 000 comptes utilisateurs ont été réinitialisés**, avec des mots de passe complexifiés (12 caractères au lieu de 8).

L'agent de protection est à ce jour déployé sur plus de **100 680** équipements informatiques.

2^{ème} phase :

Reconstruction de l'infrastructure centrale

La reconstruction de l'infrastructure centrale a débuté par le nettoyage, le durcissement, et la reconstruction de l'annuaire technique par Orange Cyber Defense. Cet annuaire permet aux utilisateurs de se connecter aux ordinateurs des lycées. Il a été remis en service durant la deuxième semaine des vacances scolaires.

De nouveaux équipements de sécurité réseaux ont été installés sur le site d'Amiens. De nouveaux serveurs centraux ont été livrés et installés physiquement.

3^{ème} phase :

Reconstruction des infrastructures locales sur la base des serveurs existants

L'infrastructure centrale est désormais opérationnelle.

La création des serveurs virtuels locaux est achevée sur l'ensemble des 237 sites.

L'intégration des logiciels et applicatifs sur les serveurs pédagogiques est effective sur les 237 sites dont 170 sites totalement traités depuis le 7 janvier.

Les opérations à suivre dans les semaines qui viennent sont les serveurs d'impression, le stockage des fichiers et leur sauvegarde.

Parallèlement, dès que cela est possible, des travaux de récupération de données se poursuivent ainsi que des opérations techniques.

A ce jour :

193 opérations de récupération de données historiques sur les anciens serveurs ont été réalisées. Cela a engendré :

- 126 opérations réussies en administratif, soit 82 récupérations complètes et 43 partielles = taux de réussite de 73%
- 98 opérations réussies en pédagogie, soit 59 récupération complètes et 39 partielles = taux de réussite de 75%

Une communication régulière et adaptée

Des consignes à respecter dans la remise en service progressive ont été données aux établissements, la Foire aux Questions, co-rédigée par les autorités académiques et les services régionaux, est régulièrement mise à jour.

Les services académiques ont élaboré un kit de ressources regroupant les informations et outils essentiels pour les personnels. Les corps d'inspection élaborent également un plan de continuité pédagogique pour accompagner au mieux les enseignants dans cette période compliquée.

Les responsables d'établissements, ainsi que les enseignants reçoivent des informations et communication régulièrement de la part des autorités académiques et de la Région.

L'enquête est menée par la Gendarmerie nationale et est encore en cours.

Des communiqués de presse conjoints avec les autorités académiques sont publiés régulièrement depuis le 10 octobre et mis à disposition sur l'ENT.

Des communiqués internes sont également adressés aux agents des lycées, via la direction des ressources humaines, et une FSS/FSC exceptionnelle s'est tenue le jeudi 6 novembre 2025. Un prochain point de situation est fait ce 5 mars 2026.

Une première délibération exceptionnelle portant sur la sécurisation des infrastructures des lycées a été présentée à la **commission permanente du 27 novembre**. Elle porte sur deux mesures fortes dans le cadre de la mise en œuvre du plan de remédiation :

- Premièrement, l'acquisition de la solution Cortex qui vise à protéger les postes et serveurs de façon optimale, couplée à un service central opérationnel en charge de surveiller, analyser et répondre aux incidents de cybersécurité en temps réel, utilisant des technologies d'automatisation pour détecter et prioriser les menaces.
- Deuxièmement, l'acquisition de baies de sauvegardes immuables à destination des établissements.

Cette délibération porte sur un montant global de 3 250 000€.

Une seconde délibération exceptionnelle a été présentée en décembre 2025 pour le plan de remédiation. Celui-ci s'étalera sur 2026 pour un montant global de 19 250 000 €.

Elle ouvre une nouvelle phase de remédiation et de sécurisation qui permettra de corriger les vulnérabilités identifiées et renforcer la sécurité des SI conformément aux recommandations

de l'ANSSI, au rapport de l'audit de sécurité et aux exigences réglementaires et techniques en vigueur.

Aussi, il est proposé d'intervenir sur les infrastructures centrales en acquérant de nouveaux serveurs complémentaires à ceux achetés en 2025 et de mettre en œuvre la nouvelle stratégie de sauvegarde.

Un renforcement global de la sécurité des SI se poursuivra avec l'acquisition de solutions d'audit de traçabilité, la protection renforcée de l'active directory (AD), l'achat d'équipements actifs réseau, le renouvellement de l'agent EDR, ainsi que la remédiation sur les postes informatiques non compatibles avec Windows 11, considérés comme vulnérables aux cyberattaques.

Le plan global de remédiation s'élève à 22 500 000€.

Une communication régulière envers l'ensemble des collègues mobilisés

Les cellules de crise réunissant les autorités académiques et la Région sont maintenues à hauteur de deux fois par semaine. La cellule technique se réunit quant à elle une à deux fois par semaine selon nécessité.

L'ensemble des agents est informé de l'évolution de la remédiation, reçoit les protocoles techniques et est destinataire des différentes communications auprès des établissements.

Un séminaire regroupant l'ensemble des agents a été organisé en visio le 5 décembre 2025 afin de présenter un point d'étape, le nouveau schéma d'architecture du système d'information des lycées et de répondre aux questions de chacun. Ce temps a également été l'occasion pour Giovanni Sorano, Directeur Général Adjoint du pôle de remercier les équipes pour le travail accompli et l'investissement de chacun.

Un deuxième séminaire a été organisé le jeudi 22 janvier 2026.