
CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (C.C.T.P)

Marché 2026.03 : Accord-cadre relatif à des prestations de réponse à incident de cybersécurité pour
l'Université de Lille

Le contexte :

Aux vues de l'accroissement des risques cyber, l'Université de Lille souhaite se préparer au mieux à faire face à une éventuelle crise d'origine cyber.

Pour cela, elle a déjà engagé plusieurs chantiers de sécurisation de son système d'information et travaille à améliorer son niveau de résilience face aux risques.

Toutefois, le risque d'une crise majeure qui paralyserait tout ou une partie de notre système d'information ne peut être complètement exclu.

Une telle situation, si elle devait se produire, pourrait avoir des impacts forts sur notre capacité à assurer nos missions, voire même mettre l'établissement dans l'incapacité de fonctionner correctement pendant une période plus ou moins longue.

Préventivement, il nous semble donc nécessaire de contractualiser au travers de ce marché avec une équipe spécialisée en réponse à incident d'origine cyber (CSIRT) pour venir en appui des équipes de la DGDNUM (Direction Générale du Numérique de l'Université de Lille) en cas de crise majeure.

Environnement et chiffres clés :

L'université de Lille compte actuellement environ :

- 9 500 personnels
- 80 000 étudiants
- 15 facultés, écoles et instituts, répartis sur 6 campus sur l'ensemble du Nord, Pas de Calais.
- 64 unités de recherche
- 25 000 postes de travail (Windows, macOS et Linux)
- 2000 serveurs (Linux, Windows).

L'environnement du système d'information de l'établissement :

- La plupart de nos serveurs sont virtualisés au travers de la solution VMware NSX
- L'ensemble de nos serveurs fait l'objet d'une redondance sur 2 sites physiques différents, un dispositif de sauvegarde Off-Line est également mis en place.

- Nos postes clients utilisent la solution antivirus EPP/EDR de WithSecure. Actuellement, environ 18 500 postes sont déjà protégés par cette solution.
- Nos serveurs sont protégés par la solution EDR Cortex de PaloAlto.
- Ces 2 solutions EDR (WithSecure et Cortex) remontent leurs résultats vers notre SOC externalisé qui assure une prestation en 24/7.
- Des audits de sécurité (pentest) sont organisés au moins une fois par an afin d'éprouver la solidité de notre SI et en particulier de notre AD.
- Un travail de sensibilisation au phishing est en place depuis l'automne 2024, il permet au travers de mises en situation de tester chaque mois l'ensemble des personnels et des étudiants de l'établissement
- Un projet d'authentification multi-facteurs est en cours de déploiement au sein de l'établissement, avec pour objectif final de renforcer l'authentification sur le VPN et sur les applications les plus sensibles.

La prestation attendue :

En cas de crise majeure et de mobilisation de l'équipe « réponse à incident », celle-ci assurera au sein de la cellule de crise un rôle qui pourra évoluer en fonction de la situation.

Néanmoins, dans la plupart des cas, voici ce qui est attendu de la part du prestataire :

- Une disponibilité en 24/7.
- Le déclenchement de l'alerte et de la prestation doit pouvoir être réalisé par un moyen simple et rapide (exemple : numéro unique d'appel téléphonique).
- L'interlocuteur prenant l'appel doit être en mesure d'appréhender au mieux la situation et de comprendre les concepts, technologies et vocabulaire du secteur d'activité.
- Dès le déclenchement de l'alerte et pendant l'ensemble de la prestation, tous les échanges se feront exclusivement en français (à l'écrit et à l'oral)
- Une fois l'événement qualifié, l'équipe de réponse à incident commencera à travailler sans délai sur l'événement ; toutefois, au moins une personne de l'équipe « réponse à incident » doit pouvoir être mobilisée sur site obligatoirement dans un délai maximum de 4h y compris le week-end et les jours fériés afin d'apporter conseil et expertise à la cellule de crise.
- L'équipe « réponse à incident » accompagnera et conseillera les membres de la cellule de crise dès la mise en place de celle-ci. Elle travaillera en coopération avec les équipes internes de la Direction Générale Déléguée au Numérique (DGDNUM) qui sont à même de traiter les aspects techniques de la crise. Son objectif ne sera donc pas de fournir un renfort technique pour la remise en service, mais plutôt d'assurer un rôle de conseil et d'accompagnement sur la gestion de la crise.
- Elle apportera néanmoins du conseil et une assistance technique sur la recherche du ou des chemins de compromission et du patient zéro.
- Elle contribuera de manière active à proposer des moyens d'endiguement de la menace.
- L'équipe « réponse à incident » assurera si nécessaire la négociation avec le ou les attaquants, dans le but de découvrir si des informations ont été exfiltrées et le type d'informations concernées. Cela permettra plus facilement d'identifier le ou les serveur(s) compromis.

- Elle apportera une assistance à la réalisation du plan de sortie de crise.

Format de la réponse du candidat :

Le candidat présentera sa société et la manière dont elle est organisée pour répondre à la demande. Il fournira aussi des informations comme :

- La date de création de l'entreprise,
- Le nombre de collaborateurs dans l'entreprise
- Le nombre de dossiers traités sur les 12 derniers mois
- Il indiquera s'il est en mesure de répondre à la prestation en s'appuyant sur ses seules équipes en interne ou s'il fait appel à des partenaires extérieurs.

Le candidat doit proposer une offre forfaitaire incluant de suite un minimum de 5 jours-hommes pour démarrer la prestation de réponse à incident.

Toutefois, comme il n'est pas possible d'évaluer la durée exacte de la crise ni le nombre de jours-hommes nécessaire, le candidat doit prévoir la possibilité d'ajouter un nombre de jours-hommes à la prestation une fois que la crise a démarré.

L'offre doit faire apparaître clairement le coût jour-homme supplémentaire.

Cette manière de procéder permettra d'estimer plus finement le nombre de jours nécessaires à la réalisation exacte de la prestation.

- Pour ce faire, l'offre comportera donc une ligne de forfait annuel (forfait de 5 jours-hommes).
- Une ligne indiquant le coût pour toute journée supplémentaire.

Si un surcoût est à prévoir pour les périodes de travail en heure non ouvrées (HNO), ce surcoût doit apparaître dans l'offre.

Dans l'hypothèse où le forfait annuel n'a pas été mobilisé, le prestataire indiquera s'il est possible de convertir la partie non-consommée en une participation à un exercice de crise d'une durée maximale d'une journée.

Le candidat indiquera si la prestation inclut une veille proactive sur les actifs exposés de l'établissement, avec la possibilité d'être alerté en cas de détection de vulnérabilité.

Chaque candidat devra fournir les CV détaillés des experts qui seraient en mesure d'intervenir à l'Université.