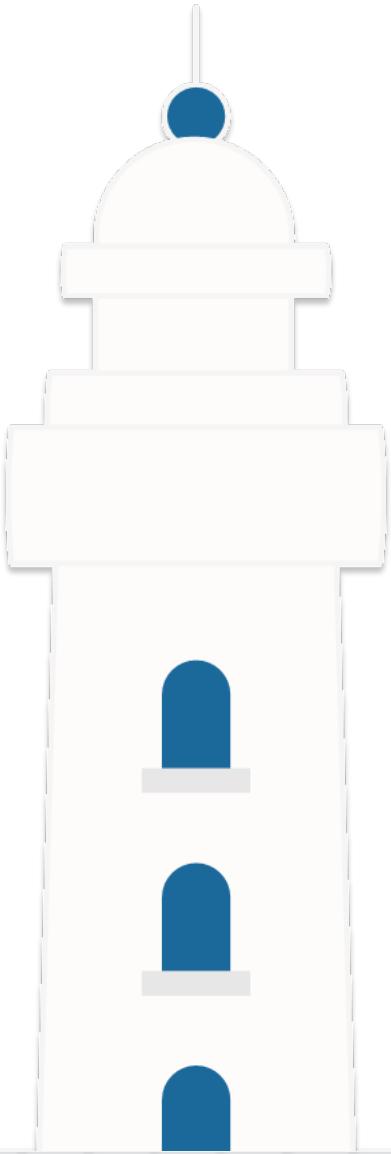
La Palmyre

26 -> 29 Mai

CSIESR

Assises 2026



Retour d’expérience cyberattaque Université Paris-Saclay

La cyberattaque 1

Premières mesures 2

Résilience 3

Retour à la normale 4

Et maintenant ? Quelques enseignements 5

Qui sommes-nous ?

L'Université Paris-Saclay est née d'une ambition commune d'universités françaises, de grandes écoles et de centres de recherches nationaux. Université de premier plan en Europe et dans le monde, elle couvre les domaines des sciences et de l'ingénierie, des sciences de la vie et de la santé, ainsi que des sciences humaines et sociales. Sa politique scientifique associe étroitement recherche et innovation, intégrant sciences fondamentales et appliquées pour répondre aux grands défis sociétaux.

Membres

- **5 facultés** : Droit-Economie-Management, Médecine, Pharmacie, Sciences, Sciences des Sports
- **3 Instituts Universitaires de Technologie (IUT):** IUT Cachan, IUT Orsay, IUT Sceaux
- **1 Ecole d'Ingénieur :** Polytech Paris-Saclay
- **4 Grandes écoles** : CentraleSupélec, AgroParisTech, Ecole Normale Supérieure Paris-Saclay, Institut d'Optique Graduate School
- **2 Universités membres associés** : Université de Versailles Saint-Quentin-en-Yvelines (UVSQ), Université Evry Paris-Saclay (UEVE)
- **7 organismes de recherche :** CEA, CNRS, IHES, INRAE, INRIA, INSERM et ONERA

Université Paris-Saclay – Quelques chiffres

50 000
étudiants

8 100
chercheurs et personnels académiques

9
prix Nobel

11
médailles Fields

13%
recherche française

220
laboratoires

350
plateformes expérimentales

50
startups créées chaque année

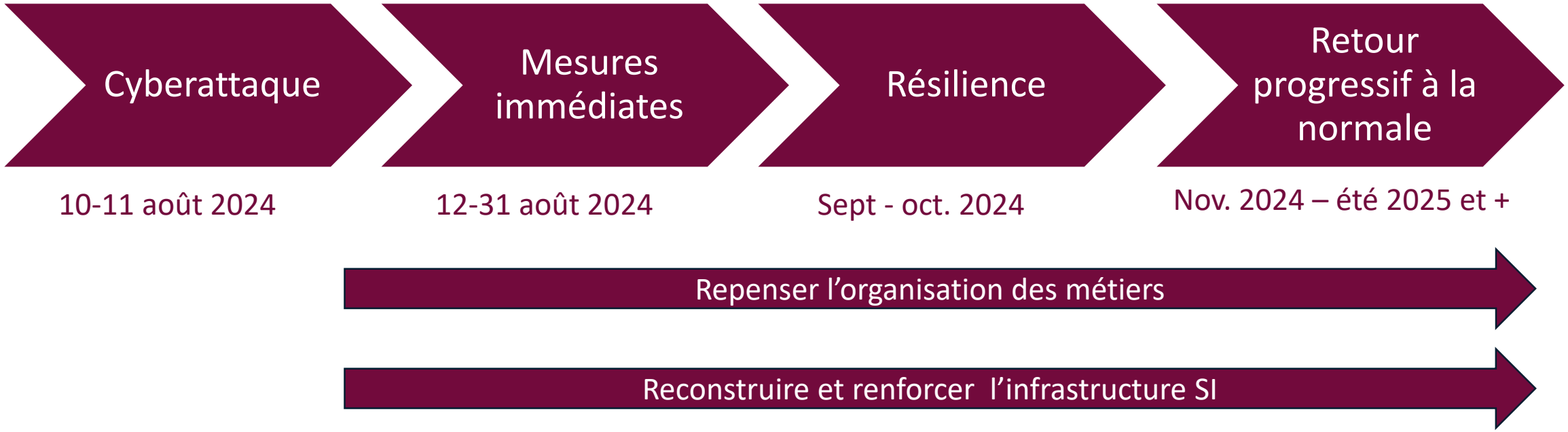
+500
partenariats industriels

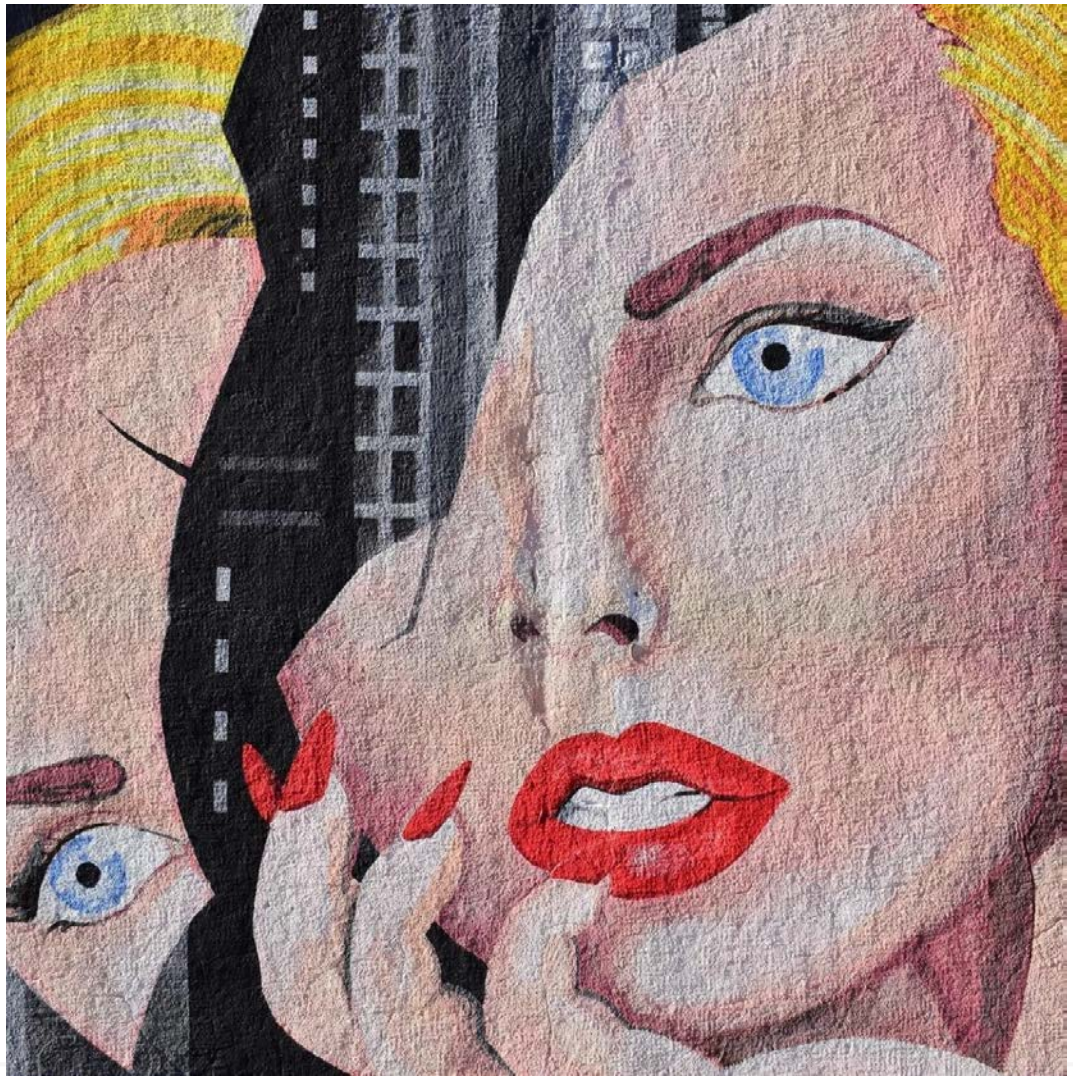
6
incubateurs

+800
partenariats universitaires internationaux

8 500
personnels administratifs et techniques

L’année 2024-2025 sous le signe d’une cyberattaque





Chapitre 1

La cyberattaque

Que s’est-il passé ?

Dans la nuit du 10 au 11 août 2024, deux semaines avant la rentrée universitaire, l’Université Paris-Saclay a été victime d’une cyberattaque majeure.

La situation du « jour d’après »

- Toute l’infrastructure centrale est HS
  - sites web de l’université et de ses labos, intranet, messagerie, Apogée, Siham, Sifac, authentification centralisée, etc.
- L’annuaire Active Directory est compromis
- Les serveurs de fichiers sont inaccessibles
- Les sauvegardes sont chiffrées (sauvegardes sur disque) ou effacées (sauvegardes sur bande)
- Notes de rançon de RansomHouse mentionnant les cryptolockers White Rabbit et Mario
- Les systèmes externes, p. ex. les services SaaS, ne sont pas touchés mais sont indisponibles (pas d’authentification SSO)
- Les systèmes locaux (p. ex. les SI des labos ou les PC des agents) ne sont pas touchés
- L’infrastructure réseau n’est pas touchée

Timeline

5 Août 2024	18:00	Premières traces de la cyberattaque
6 Août 2024	13:00	Scan de réseau / mouvements latéraux
7 Août 2024	10:00	Accès stockage
10 Août 2024	23:30	Début chiffrement serveurs Windows
11 Août 2024	0:30	Début chiffrement ESX
12 Août 2024	22:00	Fin de l'attaque

Chapitre 2

Premières mesures – préparation de l'année universitaire 2024-2025

Les deux premiers jours…

Dimanche 11/08
8h : détection d'un incident messagerie par membres DSI
10h : plus d'accès à l'administration à distance – Intervention sur site et détection du chiffrement des serveurs
12h : Information du CERT-FR
Isolation du système d'information central

Lundi 12/08

- Prédéclaration à la CNIL de l'incident
- Analyse de l'étendue des dégâts : **catastrophique**
  - Plus de moyens de communication
  - Plus d'applications métiers disponibles
    - => Retour au « mode papier » - Black-out complet du SI de l'Université
- Contact ANSSI : mise en place d'équipes d'intervention sur les volets investigation et remédiation
- Mise en place d'une cellule de crise autour du Président
- Isolation des filers non chiffrés

Les deux premières semaines…

Semaine 1 : 14, 15 (férié),16 août

- Opération « commando » avec l'ANSSI pour remonter une infrastructure AD sécurisée
  - Plage horaire ANSSI & DSI 7h–24h
  - 2 serveurs physiques compromis, mais non chiffrés
  - Mise en place de l'infrastructure Tiers 0 pour remonter les 2 forêts AD UPS et UPSAY
  - Remontée des 2 AD non chiffrés en les sécurisant et supprimant toutes les traces de la compromission

Semaine 2 : 19-23 août

- Dépôt de plainte en gendarmerie
- Intervention prestataire récupération de données
- Des snapshots non chiffrés de VM disponibles par recoupement
- « filers » non chiffrés
- Chaque image de VM (et données) de toute l'infra virtualisée est figée à une date antérieure à l'attaque (début août)
- Restauration des VM : faire une sauvegarde avant toute intervention sur les serveurs (1 Po de données)
- Commande d'une baie de stockage en urgence

Décisions et actions initiales

Priorité à la réouverture des canaux de communication

- Continuité de service organisée autour des solutions de communication externes (dont réseaux sociaux) déjà utilisés avec focus sur les sujets immédiats : support aux étudiants internationaux (groupe WhatsApp existant préalablement), logement et accueil des étudiants etc.
- Mais possibilités limitées : pas de liste des étudiants inscrits, pas de possibilité de finaliser les inscriptions, pas d'emplois du temps disponibles, pas de moyen de contacter les intervenants pédagogiques.
- Création d'un site web public temporaire
- Ouverture d'une messagerie basée sur MS 365 (avec MFA obligatoire)

Maintien des dates de rentrée

Pas de suite donnée à la demande de rançon

Conformément à la politique générale de l'Etat

Chapitre 3

Résilience

Quelques mesures de contournement pour les SI

Communication

- Bascule sur une messagerie externe, non souveraine (MS365)
- Création d'un site web spécifique

Etudiants

- Adaptation d'un logiciel existant pour permettre une inscription minimale des étudiants
- Tous les étudiants qui se présentent en début d'année sont réputés avoir le droit de s'inscrire
- Pas de paiement des frais d'inscription avant d'avoir remis en service le SI Financier
- Création d'adresses mail spécifiques pour les étudiants sur une plateforme dédiée
- Création de comptes locaux pour les enseignants sur le Moodle de l'Université

Finance

- Utilisation de procédures « manuelles » basées sur Excel pour les commandes
- Remise en service de l'application DVP (DGFiP) pour le paiement des factures

RH

- Réutilisation pour les premiers mois de la bande de virement pré-cyberattaque + ajustements manuels
- Remise en service de Winpaie qui avait été abandonné au profit de Siham Preliq
- Injection manuelle des nouveaux arrivants

Reconstruction de l'outil de travail

Définition de 3 phases générales

- Eléments cœur du SI : messagerie, authentification, accès aux fichiers partagés, site web – cible fin octobre 2024
- Applications métier principales, permettant de traiter les opérations de base : Finances, RH, Scolarité – cible fin décembre 2024
- Tout le reste – à partir de janvier 2025
- Une priorisation plus fine est établie par la DSI à l'intérieur de chaque phase

Ressources humaines

Support

- Mise en place d’un dispositif de soutien psychologique (entretiens individuels et de groupe)
- Recrutement de personnel administratif pour accélérer les saisies de données

Course contre la montre !

Clôture de l'année universitaire 2023-2024

- Obligation de tenir les jurys dans les délais → besoin des listes d'étudiants et des notes

Etudiants boursiers

- Envoi de données vers Aglaé avant décembre

Médecine

- Examen national EDN mi-octobre

Arrivée massive de nouveaux collègues à la rentrée

Formation continue

- Facturation sur l'exercice 2024

Clôture de l'exercice financier 2024 et préparation du budget 2025

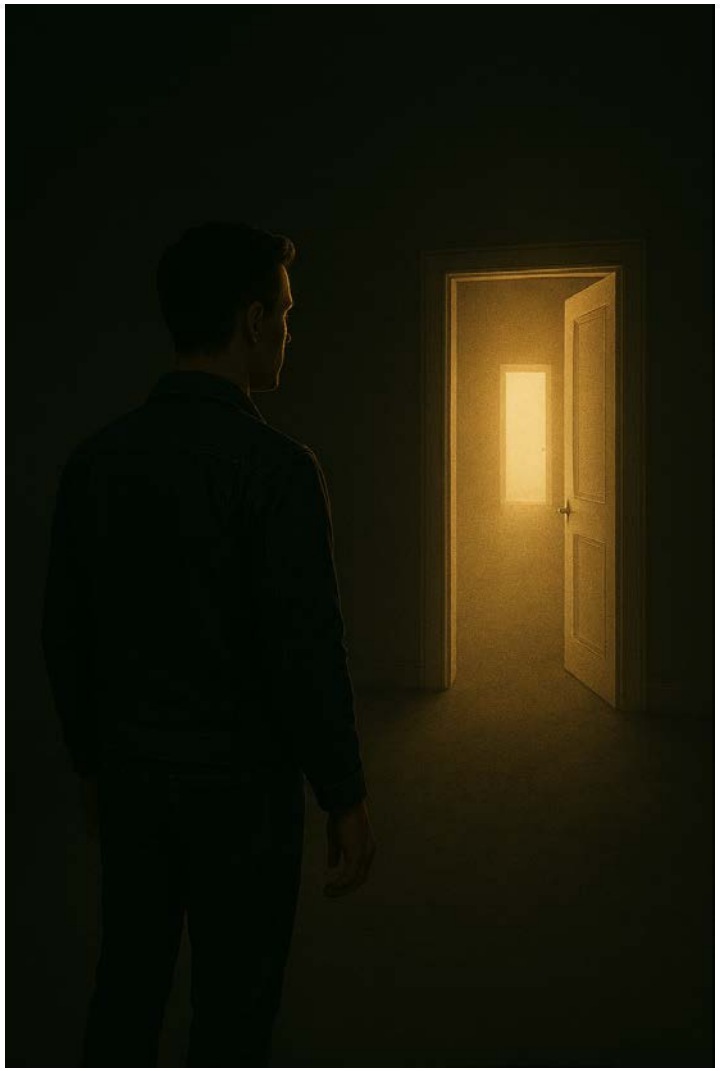
Cerises sur le gâteau…

Inondation du campus – octobre 2024

- Le campus est entièrement inondé pendant une dizaine de jours
- Tous les bâtiments doivent être évacués y compris des logements de fonction
- Plus d'électricité dans les bâtiments
- Difficultés pour ravitailler les groupes électrogènes
- Des équipements scientifiques détruits pour plusieurs millions d'€

Divulgation de données

- RansomHouse publie en octobre 2024 un échantillon de données exfiltrées et le jeu complet en novembre 2024
- 70.000 personnes (candidats en master) sont concernés par la fuite



Dernier chapitre

« l'histoire sans fin » : Retour à la normale ?

Remise en service des SI

Remise en service

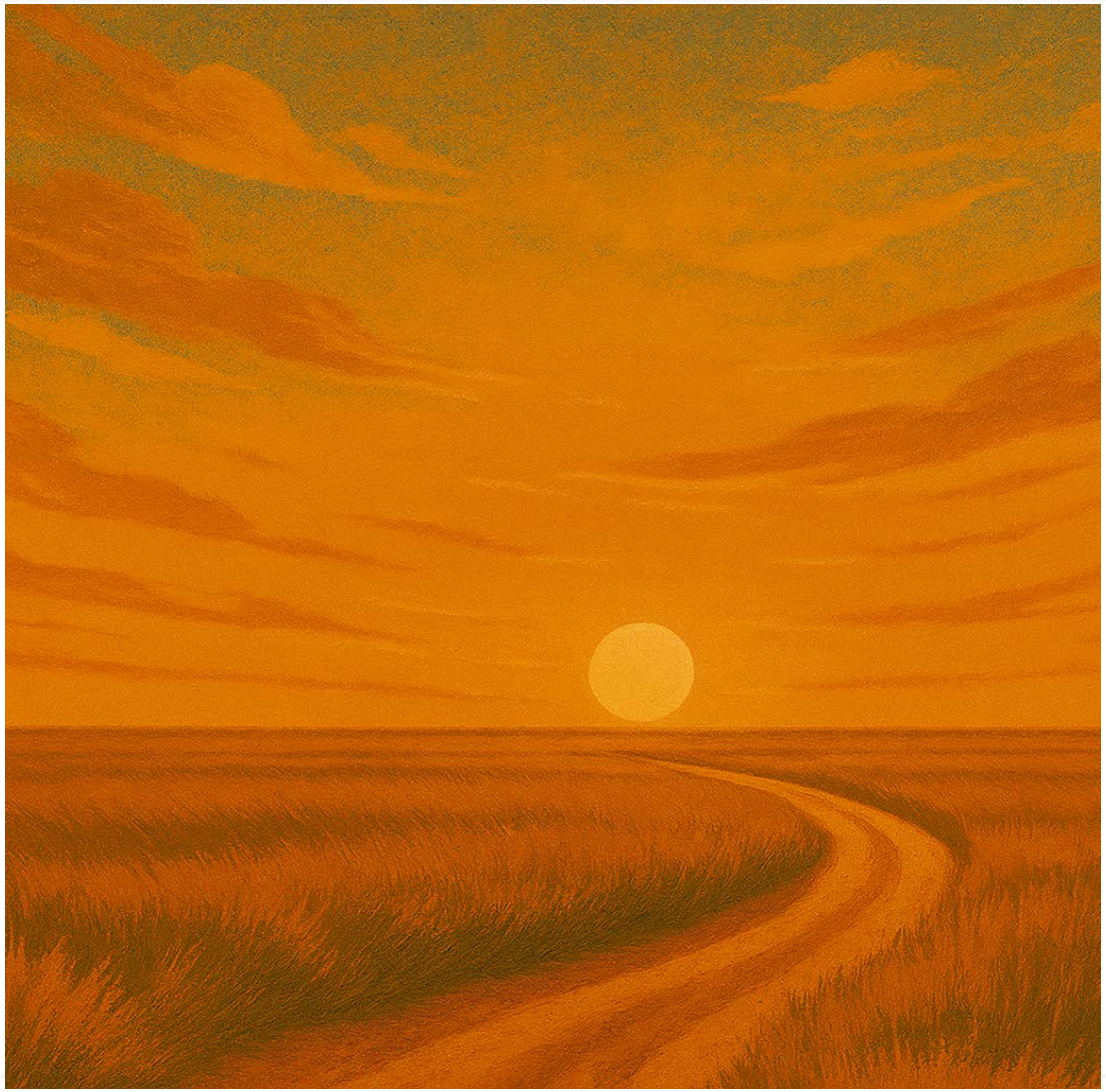
- Remise en service technique des SI après 3-5 mois

- Remise en service effective pour tous les utilisateurs 2-4 mois plus tard
  - Apogée : réouverture progressive janvier – mars 2025
  - Sifac : ouverture large avril 2025
  - Siham : ouverture large juin 2025

- Pour les autres SI : remise en service pour l'essentiel au premier semestre 2025

Gérer la fin d'utilisation des SI temporaires

- L'objectif initial de réintégrer automatiquement les données entrées dans les SI temporaires n'a pas pu être tenu : les données ont été majoritairement re-saisies manuellement.
- Certains systèmes et mesures temporaires ont été maintenues pendant toute l'année universitaire pour éviter d'ajouter de nouvelles perturbations en cours d'année.
  - Modalités d'accès à Moodle
  - Adresses mail temporaires pour les étudiants prolongées jusqu'à fin 2025



Et maintenant ?

Fluctuat nec mergitur

La cyberattaque a beaucoup secoué l'université mais l'a également renforcée

- Tout est revenu à la normale (en apparence)
- Le soutien de la gouvernance auprès de toutes les équipes a été sans faille tout au long de l'année
- Mise en place d'un projet collectif pour sauver l'année universitaire
- Le SI est désormais plus résilient et robuste

Les conséquences à moyen et long terme sur la communauté sont difficiles à évaluer

- Beaucoup d'énergie dépensée et de tension accumulée
- Possible perte de confiance vis-à-vis de l'institution

Bénéfices techniques

Accélération ou anticipation de projets prévus à moyen terme

- Architecture Active Directory
- Portables dédiés à l'administration technique
- Remplacement des baies de stockage

Renforcement de l'infrastructure SI

- Meilleure segmentation des réseaux
- Campagne de mise à jour des mots de passe
- Adoption du MFA
- Déploiement massive d'un EDR avec un microSOC
- Déploiement d'un bastion

En cours

- Sauvegarde offline
- Mise en place d'un SIEM et d'un NSOC 24x7

Quelques enseignements

Epreuve à tous les niveaux de l'organisation et dans tous les métiers

- « crise d'origine cyber » plutôt que « crise cyber »
- Nécessite une forte adaptation de toutes les équipes métier
- Très déstabilisant pour tous

Points d'attention techniques

- Segmenter le réseau et l'infrastructure, y compris les postes de travail, pour limiter les possibilités de latéralisation
- Les systèmes de réplication et de sauvegarde sont exposés dès lors qu'ils sont sur le réseau → importance de disposer d'une sauvegarde hors ligne.
- La documentation technique et organisationnelle, incluant un annuaire de crise (équipes et prestataires à mobiliser en cas de crise) doit être disponible sous forme numérique et/ou physique dans un emplacement sécurisé et indépendant
- Une plateforme de communication indépendante et de large diffusion, comme Signal, permet de faciliter les communications de crise.
- Améliorer les capacités de surveillance de l'activité SI et de réponse aux incidents

Quelques enseignements

Facteurs facilitants

- Prendre du recul
- Soutien de la gouvernance et des tutelles
- Ne pas se placer en « recherche de coupable »
- Entraide aux différents niveaux de la communauté
- Protéger les équipes opérationnelles

Aborder la sortie de crise comme un projet

- Evaluer le temps nécessaire et se placer sur le temps long
- Fixer les priorités et les grandes étapes de la sortie de crise, et s'y tenir
- Définir les rôles et périmètres d'intervention de chacun
- Tenir des cellules de crise très régulières niveau technique et gouvernance
- Rendre compte régulièrement de la situation – y compris les retards ou difficultés

La reconstruction induit des évolutions massives de l'infrastructure SI

- Et des coûts associés

Anticiper ce qui peut l'être

Infrastructure technique

- A faire évoluer pour réduire à la fois le risque d'une attaque réussie, et son impact si elle réussit
- Coût humain et budgétaire

Plan de continuité d'activité

- Définir les priorités de remise en service si rien ne marche, les données les plus importantes, les compromis acceptables
- Document essentiellement métier et non technique

Conformité

- RGPD
- NIS2
- Audits techniques et organisationnels réguliers

Organisation de crise

- Cellule de crise : qui, où, quels moyens d'échange entre les membres
- Premiers gestes en cas de crise
- Annuaire
- Evaluer le besoin d'une assistance technique et organisationnelle ex. PRIS
- Mettre en place des exercices de crise (cyber ou non) réguliers

Merci