RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

MINES Saint-Étienne | Institut Mines-Télécom

ESUP-DAYS 41
5 MAI 2026 @Paris

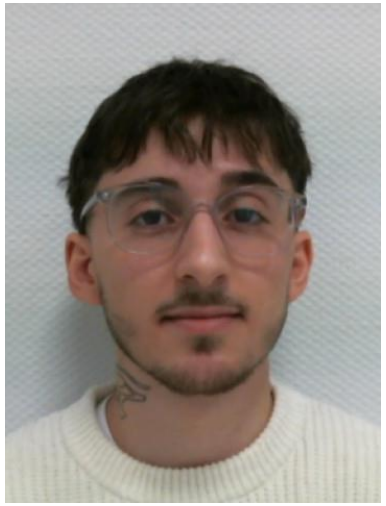
Retour d’expérience

Sur la mise en œuvre et l’utilisation de la solution MFA Esup-OTP

QUI SOMMES-NOUS ?

Dominique BERTHET

FONCTION : DSI - RSSI



Pierre-Louis DE OLIVEIRA

FONCTION : Ingénieur systèmes et réseaux

MINES SAINT-ETIENNE

ÉCOLE FONDÉE EN 1816

4 CAMPUS

Historique · Saint-Étienne
Santé · Saint-Étienne
Aix-Marseille-Provence
Numérique · Lyon

480 PERSONNELS
DONT 150 ENSEIGNANTS-CHERCHEURS

+ 9 000 Alumni

2500 ÉTUDIANTS

- 27 % Internationaux
- 25 % Femmes
- 31 % Boursiers

Plateformes technologiques de pointe

- Diwii
- MedTechLab
- Salle blanche
- Fabrication additive métallique
- ...

VIE ÉTUDIANTE

532 LOGEMENTS étudiants

35 associations étudiantes

CULTURE SCIENTIFIQUE

LA ROTONDE
Centre de culture scientifique

60 000 VISITEURS

À LA POINTE DE LA RECHERCHE

5 centres de formation et de recherche

- Centre Ingénierie et Santé
- Centre Microélectronique de Provence
- Institut Henri Fayol
- Sciences des Matériaux et des Structures
- Sciences des Processus Industriels et Naturels

300 publications internationales

20 M € chiffre d'affaires

Classement Mondial Standford
9 chercheurs dans le Top 2% des chercheurs influents

7 ERC

11e École d'Ingénieurs Française au classement de l'Étudiant

TOP 100 MONDIAL
sur 3 ODD
dont « lutte contre les changements climatiques »

52,8 M€ de budget
dont 41 % de ressources propres

INTERNATIONAL

140 Partenariats dans 50 pays

T.I.M.E. Top International Managers in Engineering

EULiST EUROPEAN UNIVERSITY

LABELLISÉ DD&RS

BIENVENUE EN FRANCE

NR NIVEAU 1 RÉSEAU NUMÉRIQUE RESPONSABLE

ECA Certificate Quality in Internationalisation

Collège d'ingénierie LYON · SAINT-ÉTIENNE

Collège des hautes études Lyon — Sciences

INNOVATION

TEAM
Incubateur d'accompagnement à la maturation technologique

101 start-up accompagnées

80 % taux de survie à 5 ans

FORMATIONS

6 Diplômes d'ingénieurs

- Ingénieur Civil des Mines + FUSION
- Ingénieur Systèmes Microélectronique et Informatique
- Ingénieurs en apprentissage en partenariat avec l'ISTP

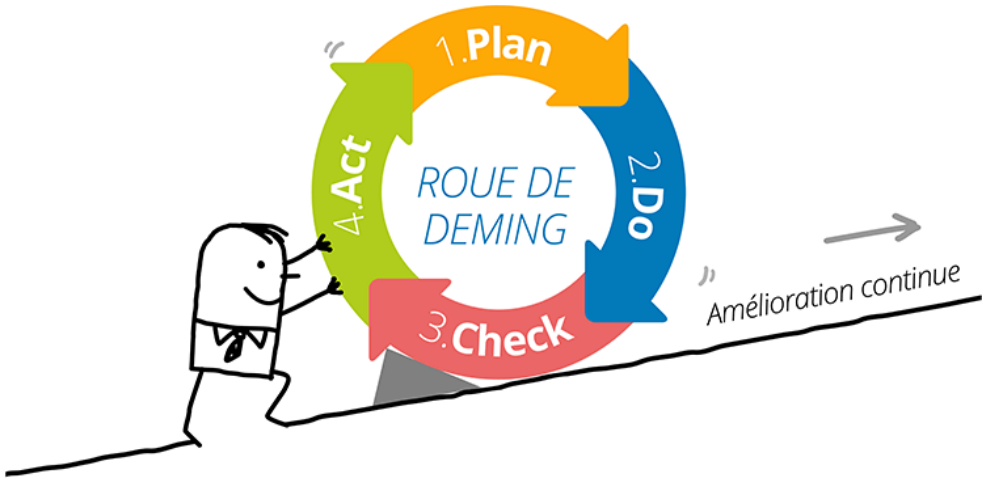
Génie industriel
Génie des Installations Nucléaires
Valorisation Énergétique
Systèmes Eléctroniques Embarqués

42 doubles diplômes
« Ingénieur-pharmacien »
« Ingénieur-médecin »
...

14 MASTERS dont 8 en anglais

1 ÉCOLE DOCTORALE 200 docteurs

SOMMAIRE



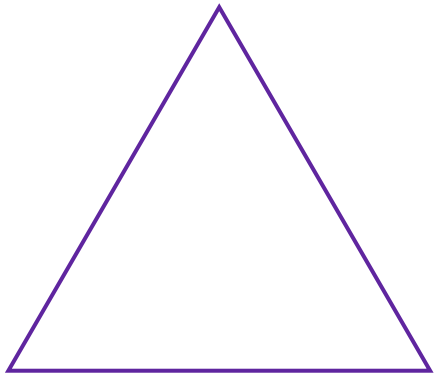
CONTEXTE ET ENJEUX DE SECURITE

Type d'utilisateurs :

- Etudiants, doctorants, vacataires,
- Enseignants-chercheurs,
- Personnels techniques et administratifs.

Accès multiples :

- Intranet,
- VPN,
- Messagerie,
- Applications Métier / SI.

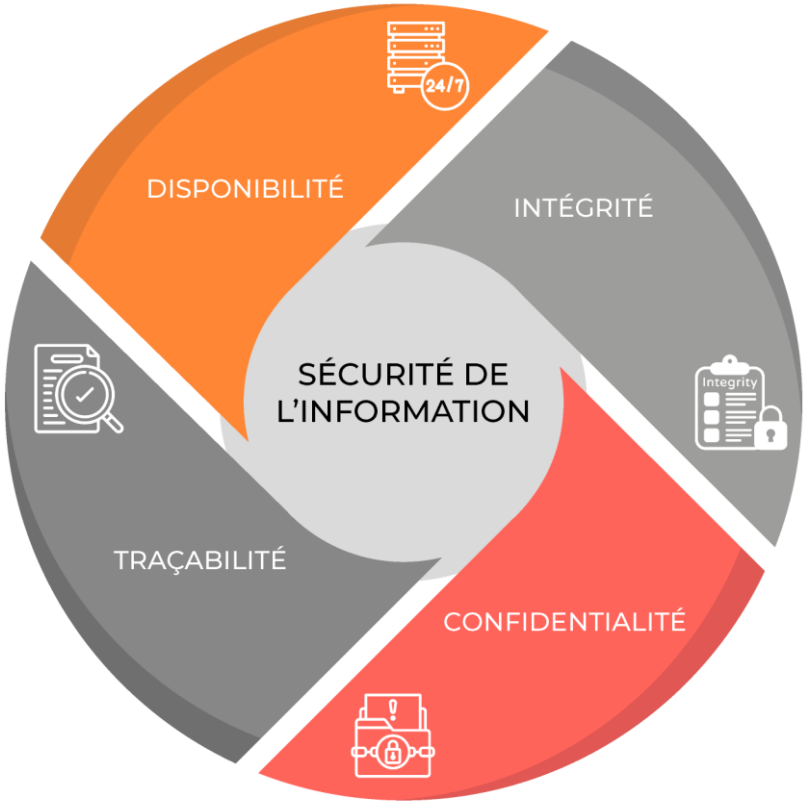


Données sensibles :

- Données personnelles (RGPD),
- Données de recherche (confidentielles / stratégiques / propriété intellectuelle),
- Données administratives (financières, RH).

Enjeux de sécurité (DICT) :

- **Disponibilité :** assurer l'accès,
- **Intégrité :** garantir leur fiabilité,
- **Confidentialité :** protéger les données,
- **Traçabilité :** suivre les actions.



R I S Q U E S I D E N T I F I E S

ISO 27005

Vulnérabilités :

- Simple authentification,
- Utilisateurs (manquement de sensibilisation).

Menaces :

- Déchiffrement (mot de passe faible, attaque hybride, Rainbow table…),
- Ingénierie sociale (famille phishing, OSINT…),
- Exploitation technique (malware, interception…),
- Imprudence utilisateur (partage involontaire, réutilisation de mot de passe…).

Risques :

- Violation des données personnelles,
- Sanctions financières,
- Atteinte à l'image,
- Suspension de financements ou partenariats,
- Responsabilité juridique / atteinte à la propriété intellectuelle.

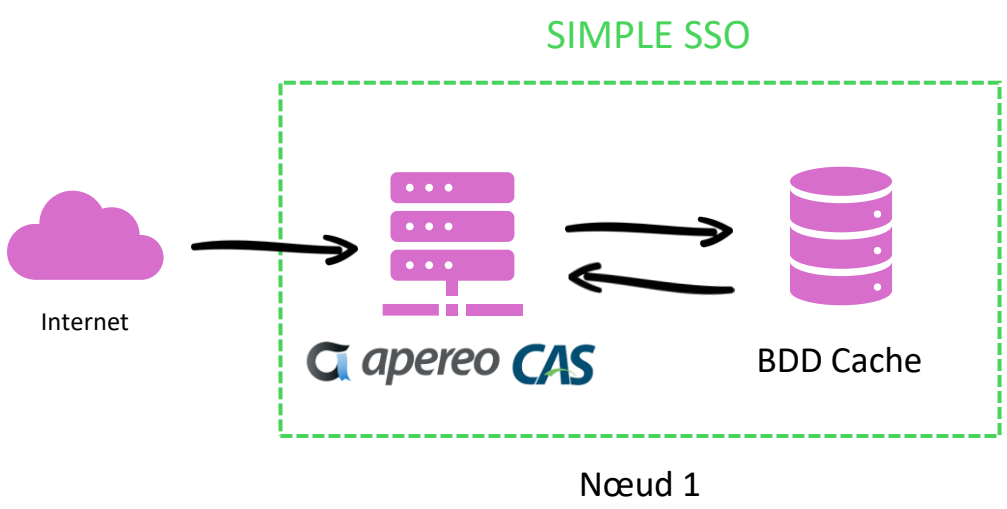
OBJECTIFS DU PROJET

Spécifique :	Déployer la 2FA pour tous les utilisateurs.
Mesurable :	100 % personnels / 100 % étudiants.
Atteignable :	Solution compatible SI existant.
Réaliste :	Réduction des risques de sécurité.
Temporel :	2025 **(tous personnels)** / 2026 **(étudiants)**.

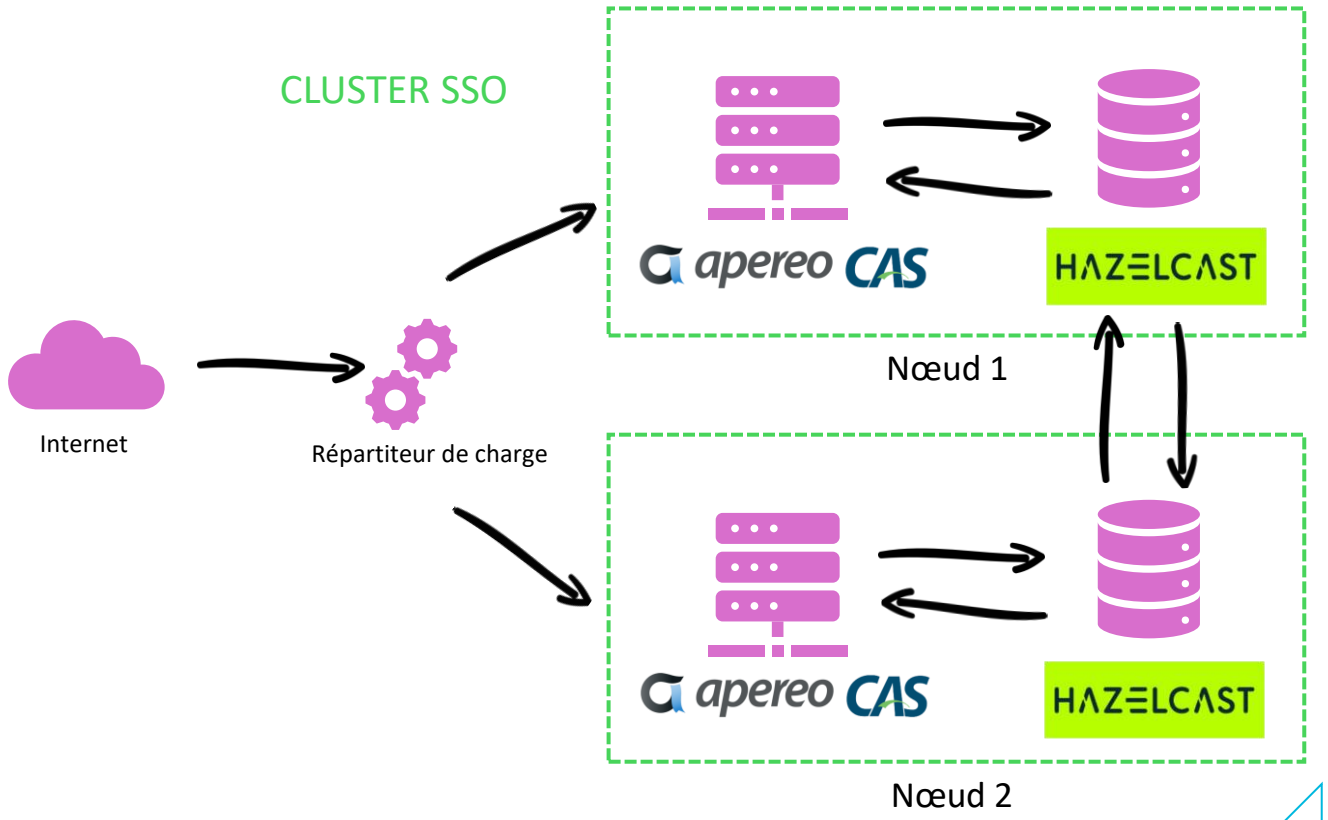
OBJECTIFS :
Opérationnel
Sécuriser les accès sans dégrader la vie numérique des utilisateurs.
Gouvernance
Faire porter le projet par la direction.

SOLUTION RETENUE

Ancienne infrastructure SSO :



Nouvelle infrastructure :



Cahier des charges :

SOLUTION MFA :

- Open source,
- Souverain,
- Communautaire,
- Confiance,
- Interopérabilité.

GUIDE ANSSI :

- R8 : Ne pas faire usage du facteur « SMS »,
- R10 : Limiter le nombre de connexions,
- R12 : Limiter la durée des sessions,
- R24 : Appliquer une politique de « Rate limiting »,
- R31 : Mettre à disposition un coffre-fort de mot de passe,
- R39- : Utiliser un facteur de possession intégrant un composant de sécurité.

EXISTENTIEL :

- Prévenir toute rupture technique avec les équipes,
- Garantir la continuité des usages pour les utilisateurs,
- S’appuyer sur le plan de reprise d’activité (PRA) interne,
- Se conformer aux conformités ANSSI et aux normes ISO 27001 / 27005, dans une démarche méthodique PDCA.

SOLUTION RETENUE

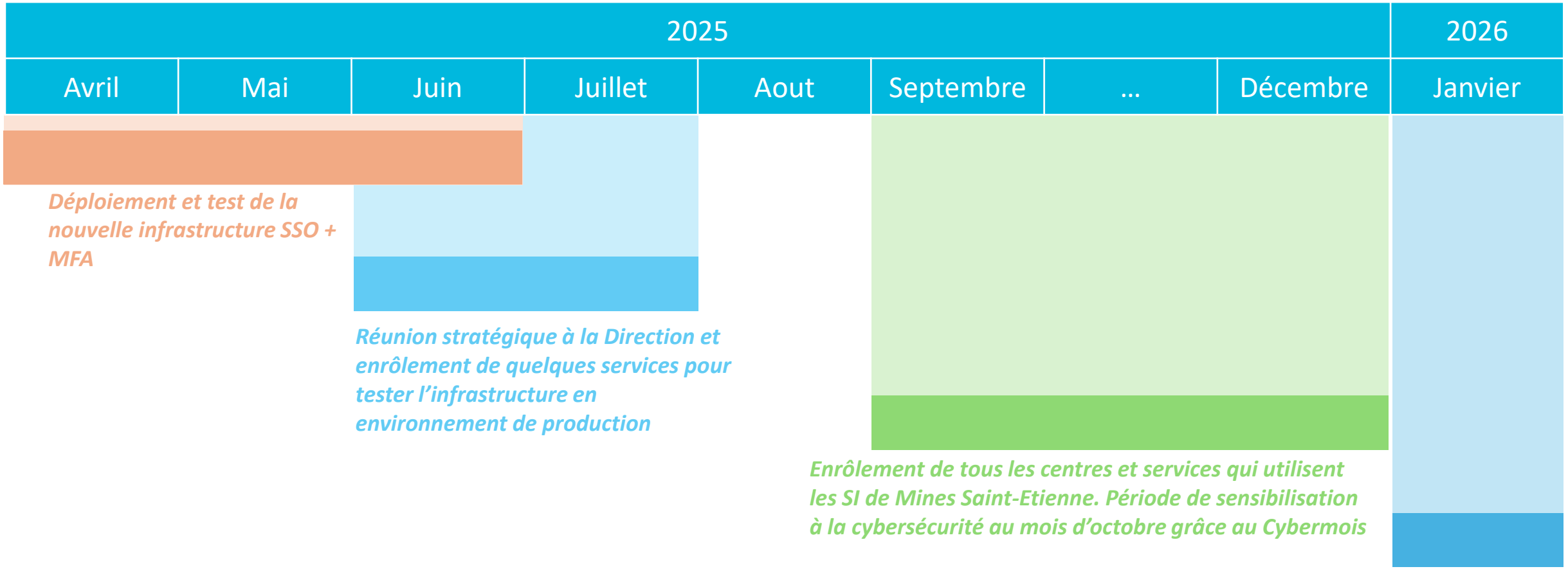
Avantages :

- Développée par le consortium ESUP-Portail,
- Open source,
- Souverain,
- Grande communauté,
- Présentée plusieurs fois aux JRES,
- RETEX positif de l'Université Jean Monnet,
- Large choix de méthodes d'authentification,
- Compatible avec Apereo CAS.

Configuration adopté :

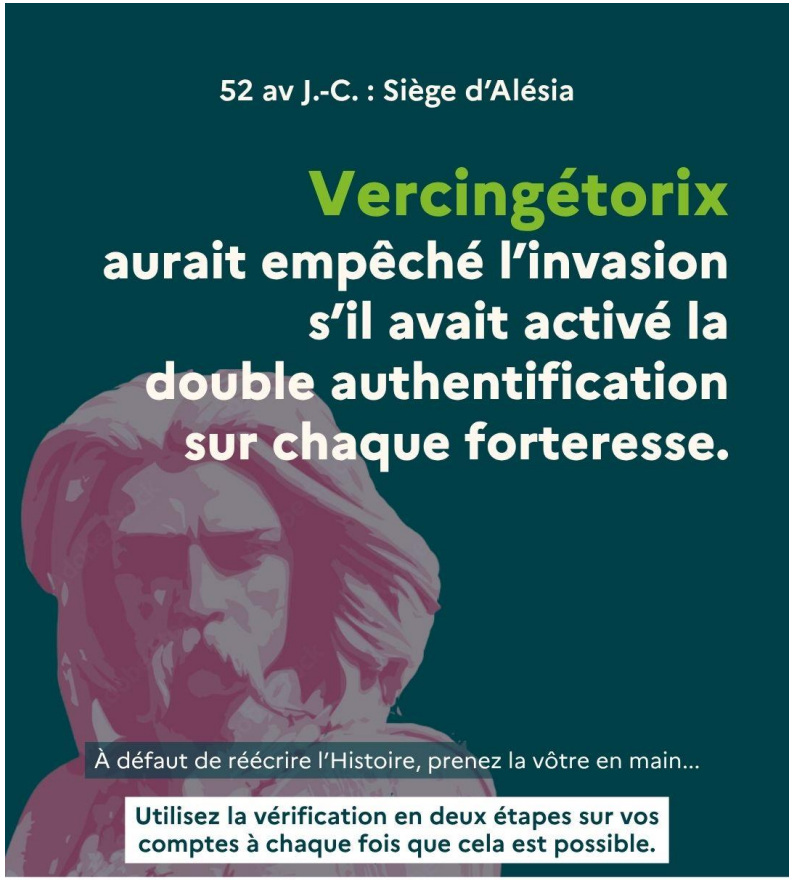
- Minimum 2 facteurs d'authentification :
  - un facteur principal,
  - le deuxième sert uniquement de secours.
- Méthodes adoptées :
  - TOTP,
  - WebAuthn,
  - Push avec Esup-Auth,
  - Grille de codes (méthode de secours pour tous le monde).
- Accès à l'UI de management restreint au réseau interne uniquement,
- Couplage de Esup-OTP avec l'implémentation Trusted MFA d'Apereo CAS,
- Utilisation d'un attribut LDAP pour facilité la mise en production.

MISE EN OEUVRE



ACCOMPAGNEMENT ET EXPLOITATION CONTINUE :

- Mise à disposition d'une documentation technique pour les utilisateurs,
- Support via la plateforme HELPMines,
- Communication par mail et via le portail interne,
- Vidéo de sensibilisation et d'explication lié à l'intégration de la MFA sur notre plateforme de diffusion ESUP-POD,
- Plastification de la grille de codes (format banque).



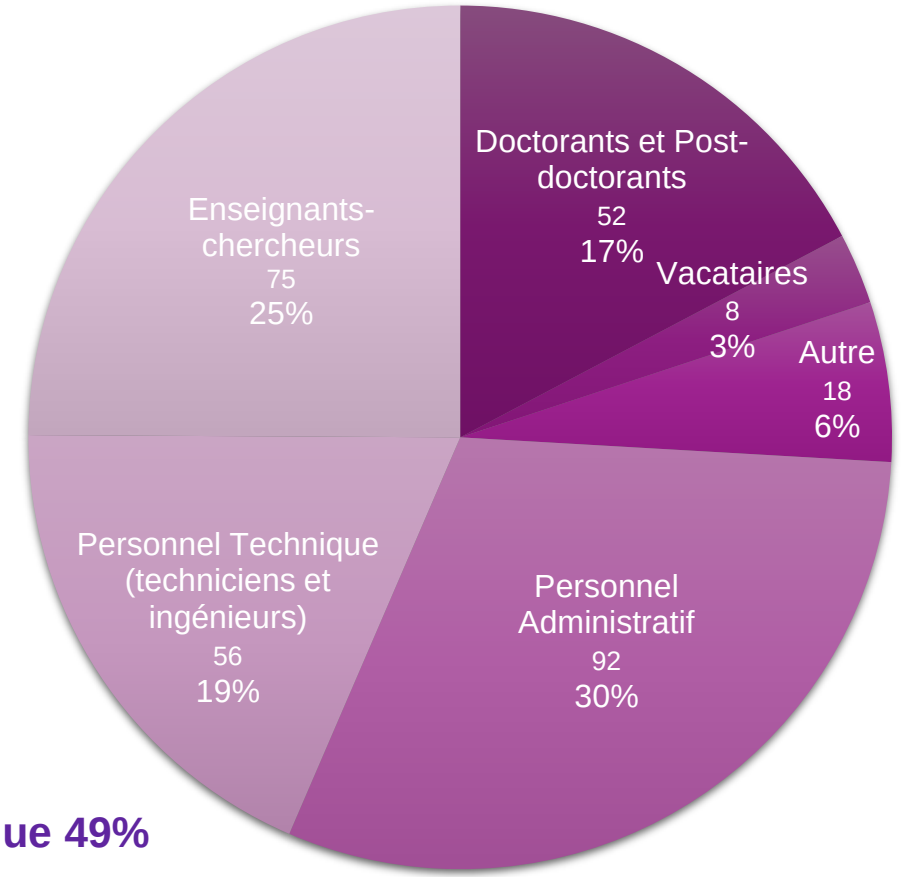
CYBER MOIS
CYBERMOIS.GOUV.FR

Indicateurs de suivi :

Total des répondants à l'enquête

	Pour 2026	
Participants	671	
Réponses complètes	**301**	**44,9%**
Soit :		
Personnel Administratif	92	30,6%
Personnel Technique (techniciens et ingénieurs)	56	18,6%
Enseignants-chercheurs	75	24,9%
Doctorants et Post-doctorants	52	17,3%
Vacataire	8	2,7%
Autre	18	6,0%

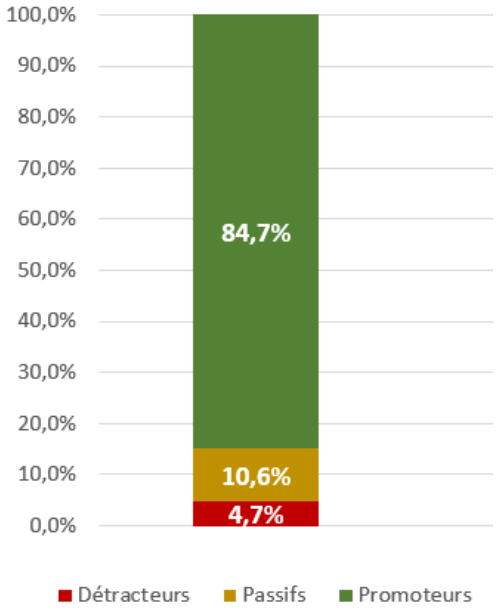
Taux de participation

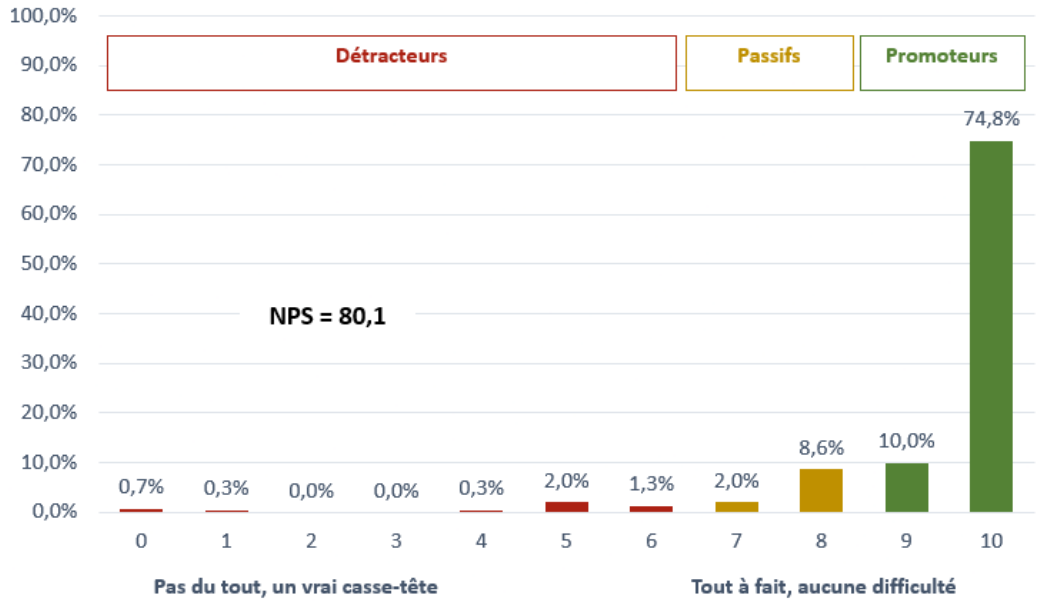


Personnel : Enseignements-Recherche 42% - Administratif et Technique 49%

Indicateurs de suivi :

L'installation et la configuration du MFA se sont déroulées sans aucune difficulté pour vous ?





93,5% Passifs - Promoteurs

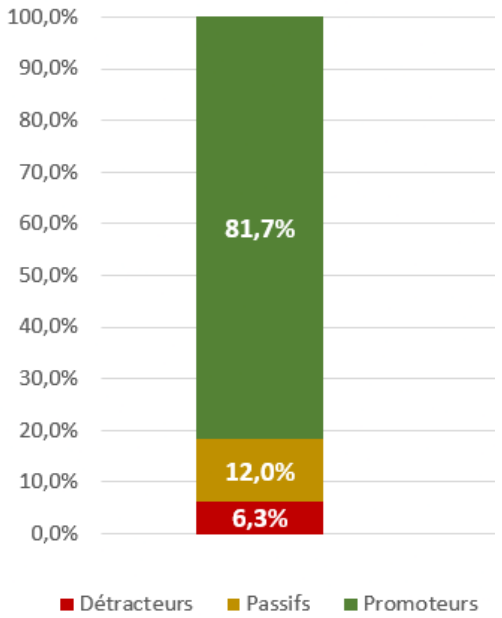
5 commentaires

Interprétation du score

- NPS > 50 : Excellent, forte fidélité.
- NPS entre 0 et 50 : Bon, mais améliorable.
- NPS < 0 : Problème de satisfaction, action urgente nécessaire.

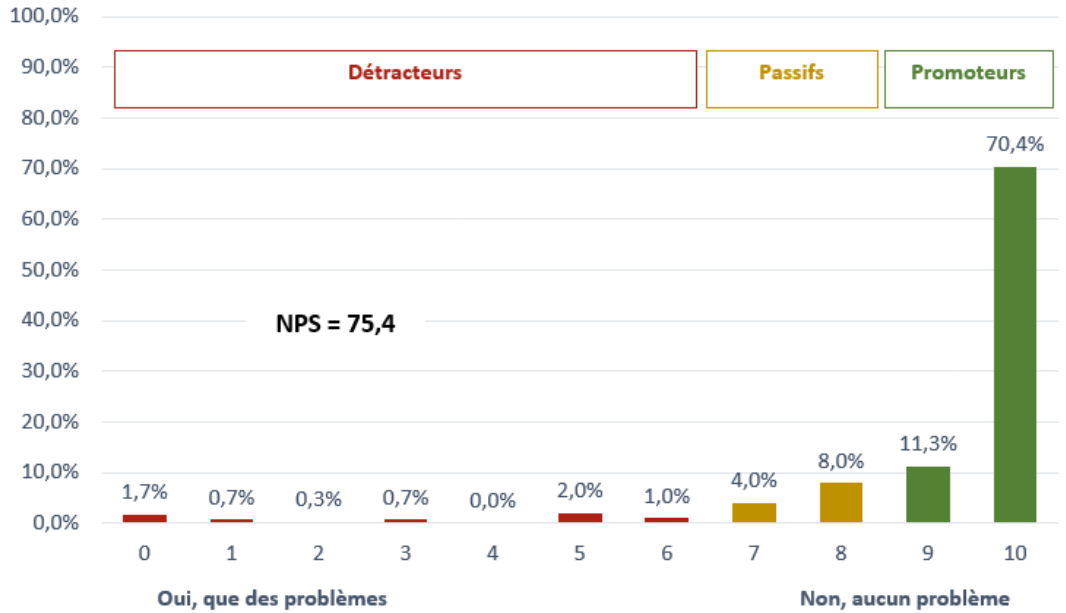
Indicateurs de suivi :

Depuis la mise en place du MFA, avez-vous rencontré des problèmes lors de son utilisation quotidienne ?



93,7% Passifs - Promoteurs

21 commentaires

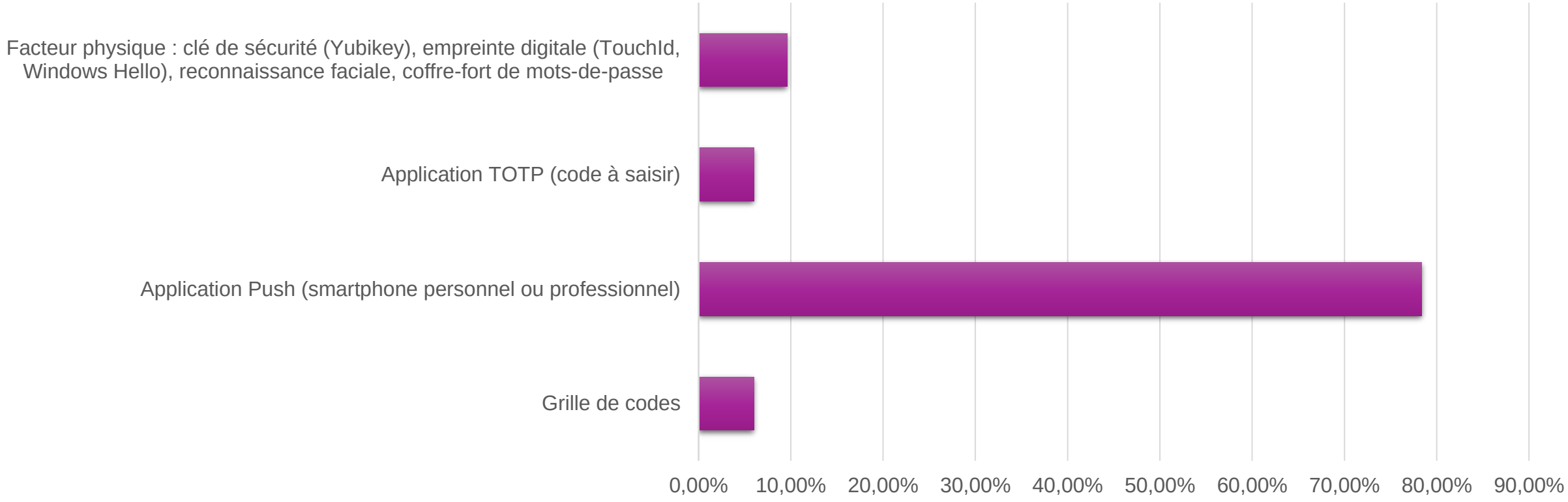


Interprétation du score

- NPS > 50 : Excellent, forte fidélité.
- NPS entre 0 et 50 : Bon, mais améliorable.
- NPS < 0 : Problème de satisfaction, action urgente nécessaire.

Indicateurs de suivi :

Quelle est votre méthode d'authentification préférée pour vous authentifier ?



Résultat du Pentest :

EVALUATION DES RISQUES :

Mineur	Pas de conséquence directe sur la sécurité du système d'information audité.
Modéré	Conséquences isolées sur des points précis du système d'information audité.
Majeur	Conséquences restreintes sur une partie du système d'information audité.
Critique	Conséquences généralisées sur l'ensemble du système d'information audité.

Facilité d'exploitation / Impact	Difficile	Complexe	Modéré	Facile
Mineur	Mineur	Mineur	Important	Majeur
Modéré	Mineur	Important	Important	Majeur
Majeur	Important	Majeur	Majeur	Critique
Critique	Important	Majeur	Critique	Critique

VULNERABILITES TROUVES :

Identifiant	Risque	Description de la vulnérabilité	Impact	Facilité d'exploitation
CAS001C	Important	Absence de Rate limiting sur les endpoints login & OTP	Majeur	Difficile
CAS002C	Important	Open-Redirect via insufficient service whitelisting	Majeur	Difficile
CAS003	Mineur	Information Disclosure via Spring Errors on cas	Mineur	Complexe
CAS004C	Mineur	Information Disclosure via Node Errors on mfa-manager	Mineur	Complexe
CAS005	Mineur	Information Disclosure via Preauth Actuators listing	Mineur	Complexe
CAS006C	Mineur	Information Disclosure via Open API exposure on mfa	Mineur	Complexe

Retour DSI :

FACTEURS DE SUCCES :

- L'adhésion de la direction et de toute la DSI,
- Utilisation de l'image du consortium ESUP grâce à Esup-Signature,
- Coopération de tous les centres et services,
- Accompagnement au plus près des utilisateurs (degré d'importance),
- Usage de la plastifieuse pour les grilles de codes,
- Simplicité de l'utilisation de l'application Esup-Auth avec sa méthode PUSH,
- L'intégration de la solution à l'infrastructure existante,
- Coût financier du projet.

CORRECTIFS APPLIQUES :

- Correction des failles de sécurités ressorties lors du Pentest,
- Expérience utilisateur avec l'intégration d'une annexe pour le remplacement du smartphone.

PERSPECTIVES D'EVOLUTION :

- Mise en place de ESUP-NFC-TAG pour faciliter l'enrôlement des étudiants,
- Exploiter les « groovy scripts » coté Apereo CAS pour conditionner l'accès à l'UI de management des facteurs d'authentification, mais aussi pour désactiver temporairement la 2FA pour les étudiants en cas d'examen national.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

MINES Saint-Étienne | Institut Mines-Télécom

Merci

Dominique BERTHET – Pierre-Louis DE OLIVEIRA

Email : dberthet@emse.fr

Email : pl.deoliveira@emse.fr

ESUP-DAYS 41
5 MAI 2026 @Paris