

Bachelor en Sciences et Ingénierie, spécialité(s) :

Rapport de mission d'audit

Campagne d'évaluation Bachelor 2025

Nom de l'école : Ecole supérieure d'informatique, électronique, automatique
Acronyme : ESIEA
Académie : Paris
Sites (3) : Paris(siège) / Laval / Ivry-sur-Seine
Réseau, groupe : UGEI

Composition de l'équipe d'audit

Timothée TOURY (Membre de la CTI, Rapporteur principal)
Noël BOUFFARD (Expert de la CTI, Corapporteur)
Nabil LITAYEM (Expert international)
Thomas ROBERT (Expert élève)

Binôme de relecteurs :

Marie Madeleine LE MARC
Pascal BIDAN

Dossier présenté en séance plénière de la CTI le 18-19 novembre 2025 ;

Pour information :

*Les textes des rapports de mission de la CTI ne sont pas justifiés pour faciliter la lecture par les personnes dyslexiques.

I. Périmètre de la mission d'audit

Demande(s) d'attribution du grade de licence à une ou plusieurs formations de Bachelor d'une école d'ingénieurs.

Catégorie de dossier	Diplôme	Voie	Site	Antériorité
PE (Périodique, renouvellement d'accréditation)	Bachelor en Sciences et Ingénierie spécialité Cybersécurité	FISEA	Ivry-sur-Seine	
NV (Nouvelle voie d'accès à une formation existante)	Bachelor en Sciences et Ingénierie spécialité Cybersécurité	Formation initiale sous statut d'étudiant	Ivry-sur-Seine	

II. Suivi des recommandations précédentes de la CTI

Avis	Recommandation	Statut
Avis n° 2022/11 - CTI	Augmenter la part des enseignements réalisés par des enseignants vacataires issus du monde socioéconomique	Réalisée
Avis n° 2022/11 - CTI	Préciser les objectifs de la politique sociale et les actions mises en œuvre pour les atteindre	Réalisée

Conclusion

Les recommandations ont été suivies effectivement.

III. Description, analyse et évaluation de l'équipe d'audit

L'école et sa gouvernance

L'ESIEA est un établissement privé reconnu par l'État, EESPIG, porté par l'association "Groupe ESIEA" (loi 1901) dont la gouvernance est historiquement marquée par l'implication de ses alumni, majoritaires au conseil d'administration ; l'école revendique ainsi une indépendance de décision et une autonomie financière fondée principalement sur les frais de scolarité et l'apprentissage.

Elle est implantée sur trois sites : Paris/Ivry sur Seine (où se déploient ingénieur et Bachelor), Laval (ingénieur) et Agen (programmes RNCP) ; le Bachelor cybersécurité n'est opéré qu'à Paris/Ivry sur Seine.

Le positionnement "numérique/informatique" de l'école (créée en 1958) et son historique en cybersécurité contribuent à une identité claire pour un Bachelor BSI en cybersécurité.

Une stratégie RSE formalisée en 2020, avec des objectifs opérationnels (handicap, égalité F/H, lutte contre les violences/harcèlement), un bilan carbone (2022) et des investissements alignés (rénovation/ construction de campus).

Pour le Bachelor cybersécurité, l'école met en avant un adossement à l'écosystème francilien et grand ouest, avec appuis de partenaires industriels et institutionnels (dont l'ANSSI et le ministère de l'Intérieur) et une appartenance à Puissance Alpha Bachelor (19 écoles).

Le RAE mentionne l'absence de formations de même niveau sur le site et indique des passerelles ou coopérations.

Un CA (jusqu'à 25 membres avec les alumni structurellement majoritaires : 13 alumni, 2 étudiants, 1 représentant salariés, jusqu'à 9 extérieurs) fixe les orientations, vote le budget et nomme le DG. Le bureau du CA se réunit mensuellement ; le CA bimestriellement. Le comité de direction (9 directeurs) se réunit toutes les deux semaines ; un Conseil stratégique de perfectionnement (CSP) annuel associe entreprises, enseignants et représentants étudiants.

Le RAE décrit une répartition claire des rôles et processus CA/bureau/DG-CODIR/CSP, cohérente avec l'attendu A.3 associant comme il se doit les parties prenantes.

Offre de formation. Mission affichée : former des professionnels du numérique maîtrisant enjeux scientifiques/techniques et impact sociétal ; l'offre est structurée autour du programme ingénieur (5 majeures dont cybersécurité), du Bachelor BSI cybersécurité, d'un MS cybersécurité (CGE), d'un MSc IA en partenariat SKEMA, de BADGE en cybersécurité et de titres RNCP "experts".

Cohérence d'ensemble. L'école revendique et met en oeuvre une cohérence verticale (Bac+3 → Bac+5) et thématique (cybersécurité, IA, VR, embarqué, software), ainsi qu'un ancrage fort aux besoins métiers (conseil de perfectionnement, enquêtes, livres blancs).

Recherche et adossement. Une unité de recherche unique, esieaLab, évaluée par le HCERES en octobre 2023, structurée en 4 équipes (Cybersécurité ; ML & Robotique ; Systèmes complexes & information quantique ; Réalité virtuelle & systèmes immersifs). Le RAE aligne objectifs et indicateurs (publications, personnels docteurs/EC impliqués) pour l'adossement au Bachelor.

Ressources humaines

L'école recense 167 permanents (109 sur le site d'Evry) et détaille la répartition par fonctions et sites ; intervenant en Bachelor : 18 enseignants permanents (55 %), 10 docteurs (35 %), 8 EC (30 %) et 14 intervenants issus du monde socio-économique (34 %).

Locaux et ressources matérielles

Paris 5e (~2 000 m²) et Ivry-sur-Seine (~5 700 m²) constituent le site principal ; le déménagement est annoncé en novembre 2025 vers un nouveau campus de 8 000 m² à Ivry. Les bâtiments sont en conformité ERP avec suivi sécurité.

Systèmes d'information et moyens numériques.

Le SI de scolarité et l'infrastructure sont en refonte : déploiement Proxmox VE, serveurs CPU/GPU, forge GitLab, serveur JupyterHub, accès à des bibliothèques numériques (ScholarVox, O'Reilly, ENI, etc.).

Budget et traçabilité.

Le RAE renvoie à un rapport des commissaires aux comptes pour les éléments budgétaires applicables aux Bachelors

SWOT global sur la partie : L'école et sa gouvernance

Points forts

- Gouvernance impliquée et lisible, avec forte place des alumni et dispositifs de dialogue.
- Expérience et réputation de l'ESIEA en cybersécurité, labelisations et large portefeuille de formations dans le domaine.
- Adossement à l'écosystème (Campus Cyber/PEC, partenaires industriels, ANSSI/MI), et appartenance à Puissance Alpha pour la visibilité en recrutement.
- Équipe pédagogique mixte (permanents/docteurs/EC + professionnels) et adossement à esieaLab

Points faibles

- Site d'Ivry actuel jugé moins attractif avant le basculement sur le nouveau campus (novembre 2025)
- Relatif isolement dans l'écosystème de l'ESR
- Visibilité internationale à renforcer

Risques

- Concurrence croissante des formations post-bac (non CTI) en cybersécurité, complexifiant la lisibilité du paysage.
- Aléas liés à la refonte du SI (migration) et au déménagement de novembre 2025 (continuité pédagogique/technique).
- Évolution rapide des métiers (IA/Cloud) pouvant déplacer les attentes de compétences visées, exigeant une forte réactivité

Opportunités

- Dynamique nationale en cybersécurité (Campus Cyber) et marché de l'emploi porteur ; apprentissage en 3e année.
- Partenariats académiques (PSB – ouverture du programme commun annoncée en septembre 2025 ; SKEMA ; CentraleSupélec) pour diversifier passerelles et co-diplômes.
- Nouveau campus d'Ivry (8 000 m², novembre 2025) comme levier d'attractivité et de modernisation des environnements d'apprentissage.

Le management de l'école : son pilotage, son fonctionnement et son système qualité

Le management de l'ESIEA repose sur une gouvernance autonome et impliquée, favorisant une bonne structuration organisationnelle. Toutefois, le système qualité requiert des améliorations sur l'implication active des étudiants dans l'évaluation des services.

Renforcer la sensibilisation des étudiants et former davantage les collaborateurs permettrait d'améliorer la qualité des services proposées et favoriserait une culture qualité mieux intégrée, essentielle pour garantir l'efficacité du processus d'amélioration continue.

SWOT global sur la partie : Le management de l'école : son pilotage, son fonctionnement et son système qualité

Points forts

- Dispositif Qualité et RSE dédié, bien aligné sur les cadres qualité (ESG/CTI/HCERES/CGE/Qualiopi) et piloté en PDCA.
- Pilotage transparent et participatif (dialogue régulier avec représentants étudiants, outils d'amélioration continue)

Points faibles

- Mobilisation étudiante inégale dans les évaluations ; boucle de rétroaction encore peu valorisante, limitant l'engagement durable.
- Culture qualité perçue par une partie des équipes comme « conformité » ; fréquence/efficacité des échanges à renforcer avec les représentants étudiants.

Risques

- Evolution très rapide du secteur demandant une évolution rapide, donc un suivi constant de la qualité
- Pression réglementaire multi-référentielle

Opportunités

- Suites des audits CTI & HCERES 2024 pour consolider la reconnaissance externe et ancrer l'amélioration continue
- Refonte du SI (2026) pour un pilotage plus efficace

Les ancrages et partenariats

L'école a un ancrage parisien (Paris/Ivry) et régional (Laval et Agen, Dax fermant fin juillet 2025). Elle développe une collaboration spécifique avec la mairie d'Ivry-sur-Seine, qui souhaitant conserver une école d'ingénieur sur son territoire, soutient l'école dans la construction de son nouveau campus d'Ivry lequel doit ouvrir fin 2025. Des collaborations existent avec d'autres établissements de formation et de recherche (Universités de Paris 1 et de Versailles). Au delà des partenariats actifs avec SKEMA Business School et Paris Business School, l'école étudie un projet de coopération avec Centrale Supélec.

L'école est très active dans ce domaine avec environ 75 partenariats d'entreprises dont une quinzaine font l'objet d'accords pluriannuels. 6 chaires d'entreprises soit thématiques soit pédagogiques sont opérationnelles en coopération avec de grandes organisations (Accenture, Airbus, SII...).

Tant sur Paris/Ivry qu'à Laval, l'école, par les actions de son référent entrepreneuriat, soutient les projets d'innovation et d'entrepreneuriat dans le cadre de partenariats avec les PEPITES. A L'école a créé à Paris et à Laval, l'OpenLab, un espace de fabrication pour des réalisations innovantes. Ceci permet de mettre en lien divers acteurs (partenaires académiques, des chercheurs, des professionnels...) dans le cadre de projets.

L'école est investie dans des réseaux nationaux en étant membre d'organisations et d'associations relevant de ses domaines d'activité (UGEI, CDEFI, CGE, associations diverses, Campus Cyber, PEC, etc.). Par ailleurs elle a des accords spécifiques avec SKEMA Business School et Paris Business School.

Pour l'ensemble de ses formations, l'école a signé des accords de partenariats avec une soixantaine d'établissements d'enseignement supérieur dans le monde. Pour la formation Bachelor Cybersécurité, l'école a ciblé l'Université de Zagreb pour l'immersion internationale obligatoire de ses apprenants et l'Université du Québec pour une convention de double diplôme. L'école gagnerait à donner un choix plus large de pays à ses élèves bachelors et à mettre en oeuvre une immersion internationale individuelle.

SWOT global sur la partie : Les ancrages et partenariats

Points forts

- Réseau des 10 000 Alumni actif et engagé
- Relations avec les entreprises
- Réseau des partenaires internationaux présents sur tous les continents

Points faibles

- Immersion internationale non individuelle pour les élèves
- Partenariat recherche avec d'autres laboratoires

Risques

- Concurrence liée au nombre de formations sur la Cybersécurité

Opportunités

- Besoins des entreprises en terme de compétences Cybersécurité
- Campus Cyber

La formation Bachelor en sciences et ingénierie

Bachelor en Sciences et Ingénierie spécialité Cybersécurité

FISEA (FISEA) sur le site de Ivry-sur-Seine

Formation initiale sous statut d'étudiant (FISE) sur le site de Ivry-sur-Seine

Le programme a été élaboré en étroite collaboration avec des partenaires industriels, institutionnels et académiques, dans le but de répondre précisément aux besoins spécifiques et évolutifs du secteur de la cybersécurité. Cette co-construction témoigne d'une volonté d'ancrer la formation dans les réalités du terrain et de garantir une forte adéquation avec les exigences du marché du travail, tout en assurant une veille constante face aux évolutions technologiques rapides.

Les compétences ciblées par la formation incluent la maîtrise des outils et techniques de cybersécurité, la gestion des risques informatiques, la sécurité logicielle et matérielle, la cryptographie, ainsi que des compétences transverses en communication, travail en équipe et capacité d'adaptation aux changements technologiques.

La formation vise également à développer chez les étudiants un sens critique, une éthique professionnelle et une ouverture à l'innovation.

Le programme présente une architecture pédagogique cohérente et progressive, alignée avec les exigences du secteur. Organisé sur trois années, il propose un équilibre entre enseignements théoriques, travaux pratiques et périodes en entreprise, favorisant une professionnalisation réelle des étudiants. Les modules de spécialisation en cybersécurité sont complétés par des enseignements transversaux. L'alternance possible en troisième année renforce l'acquisition de compétences opérationnelles.

Le programme comprend des stages obligatoires et des périodes en apprentissage. Ces expériences professionnelles sont encadrées et évaluées par des tuteurs académiques et professionnels, assurant une acquisition progressive des compétences professionnelles pratiques et théoriques attendues.

Cette immersion structurée en entreprise favorise une appropriation concrète des réalités du secteur et renforce la capacité d'adaptation des étudiants face aux évolutions et exigences du marché de la cybersécurité.

Les étudiants sont initiés à la recherche à travers des projets collaboratifs avec des enseignants-chercheurs actifs.

En s'appuyant sur l'intégration à des équipes de recherche et la participation à des travaux de pointe en cybersécurité, la formation encourage une posture d'investigation permanente, essentielle pour accompagner la transformation rapide des technologies et alimenter une culture de recherche scientifique au sein de l'établissement.

La formation inclut des modules dédiés à la responsabilité sociétale et environnementale (RSE), sensibilisant les étudiants aux enjeux éthiques, sociaux et environnementaux liés aux technologies numériques.

Cette approche vise à forger chez les futurs professionnels une conscience critique et un engagement actif, les incitant à intégrer les principes du développement durable et de l'inclusion dans la conception et la mise en œuvre de solutions technologiques, en cohérence avec les attentes sociétales.

L'ESIEA propose des cours et ateliers spécifiques dédiés à l'innovation et à l'entrepreneuriat, permettant aux étudiants de développer un esprit entrepreneurial, des compétences en gestion de projet et en valorisation de l'innovation technologique.

Cette démarche s'appuie sur des partenariats solides avec des entreprises et des dispositifs institutionnels, offrant ainsi aux étudiants un environnement propice à l'expérimentation, à la prise d'initiative et à la concrétisation de projets innovants.

La formation encourage fortement la maîtrise des langues, notamment l'anglais technique, et propose des opportunités de mobilité internationale grâce aux partenariats et réseaux internationaux tels que Puissance Alpha Bachelor. Des échanges culturels et académiques enrichissent cette ouverture internationale.

Cette dynamique internationale permet aux étudiants d'acquérir une véritable agilité interculturelle, condition essentielle pour évoluer avec succès dans un secteur numérique globalisé.

Le programme est conçu pour assurer une parfaite adéquation entre les compétences visées et les contenus pédagogiques proposés. Cette cohérence est garantie par un suivi régulier et des ajustements continus basés sur les retours d'expérience des étudiants et des entreprises partenaires. Cette approche permet d'anticiper les évolutions des métiers du numérique et de la cybersécurité, et de renforcer l'employabilité des diplômés, en alignant constamment la formation avec les attentes du marché.

La formation combine enseignements théoriques, travaux pratiques, projets professionnels et périodes en entreprise. Le contenu pédagogique est structuré afin d'assurer une montée en compétence continue et cohérente, avec un équilibre optimal entre théorie et pratique.

Cette organisation modulaire et évolutive favorise l'autonomie, l'esprit d'initiative et l'adaptabilité des étudiants, tout en intégrant régulièrement les innovations du secteur et les besoins exprimés par les parties prenantes.

Les méthodes pédagogiques privilégiées incluent l'apprentissage par projet, la pédagogie inversée et des travaux pratiques intensifs. Un équilibre entre présentiel et distanciel est assuré, tout comme entre travail personnel et collectif, favorisant ainsi l'autonomie et l'esprit d'équipe des étudiants.

Cette diversité méthodologique, alliée à une forte contextualisation des apprentissages, permet de développer chez les étudiants une capacité d'analyse critique et d'adaptation.

L'équipe pédagogique est constituée d'enseignants-chercheurs experts dans leurs domaines respectifs (avec des critères de recrutement compétitifs), permettant d'assurer un enseignement de qualité aligné sur les dernières avancées technologiques. L'encadrement est renforcé par des intervenants professionnels apportant leur expertise du terrain.

Il convient de souligner que, malgré la pénurie nationale d'enseignants spécialisés en cybersécurité, l'ESIEA parvient à maintenir une équipe hautement qualifiée, garante du niveau académique.

SWOT global sur la partie : La formation Bachelor en sciences et ingénierie

Points forts

- Positionnement clair, adossé aux besoins industriels et institutionnels ; partenariats structurants (ANSSI, MI) et contribution active des acteurs au design et à l'évaluation du programme.
- Pédagogies actives et hybrides (projets, inversée) articulant théorie–pratique–immersion ; usage d'environnements numériques spécialisés (ex. TryHackMe) et campus moderne favorisant l'innovation.
- Équipe pédagogique reconnue (enseignants-chercheurs/experts) et attractive malgré la pénurie nationale en cybersécurité.

Points faibles

- RSE/numérique responsable à approfondir ; internationalisation (mobilités, exposition interculturelle) en-deçà des ambitions.
- Accompagnement individuel et reconnaissance des initiatives étudiantes à structurer davantage.

Risques

- Obsolescence rapide des contenus/outils face au rythme technologique ; pression multi-référentielle accroissant la charge administrative.
- Concurrence accrue pour recruter/fidéliser des experts en cybersécurité, avec risque d'instabilité d'équipe et d'érosion d'expertise.

Opportunités

- Environnement et réseau solide de l'école permettant un vivier d'intervenants de qualité (jouant également un rôle d'accompagnement continu d'évolution de la formation)
- Développer les alliances internationales, recherche appliquée et projets industriels ; capter la dynamique nationale/UE cybersécurité (réseaux, financements).

Recrutement des élèves

L'ESEIA recrute des élèves après le Bac en 1re année de formation via le concours Puissance Alpha, accessible par Parcoursup. Un recrutement en 2e année de Bachelor est également mis en place pour compléter les effectifs démissionnaires ou en échec (ceux-ci étant majoritaires en 1re année).

Des bourses publiques (Crous) et propres à l'école sont disponibles pour assurer une diversité sociale.

L'école affiche un taux d'étudiantes sur le campus entre 8 et 10% selon les années.

L'école effectue un suivi approprié des résultats de son recrutement, notamment sur la diversité sociale et la féminisation de sa formation.

SWOT global sur la partie : Recrutement des élèves

Points forts

- Recrutement sur concours via Parcoursup
- Promotions remplies
- Bon support à la diversité sociale
- Label SecNumEdu décerné par l'ANSSI

Points faibles

- Peu de visibilité parmi toute l'offre de formation Parcoursup

Risques

- Voir le taux de féminisation de la formation continuer à diminuer
- Peu d'attractivité des formations Bac+3 par rapport aux formations Bac+5

Opportunités

- Promouvoir la féminisation de l'ESEIA via les actions de promotion extérieure
- Domaine cybersécurité attractif en Europe spécifiquement comme à l'international

La vie étudiante et la vie associative des élèves

L'école propose un guide d'accueil détaillé à ses nouveaux élèves de Bachelor et en programme ingénieur, ainsi qu'une semaine d'intégration conjointe.

Les étudiants de Bachelor participent aux activités des mêmes associations que les élèves-ingénieurs, notamment au sein de l'association d'informatique de l'école. Les associations bénéficient d'un financement de l'école pour leurs projets et de locaux fournis par l'école.

L'engagement étudiant est reconnu avec compensation en crédits ECTS.

SWOT global sur la partie : La vie étudiante et la vie associative des élèves

Points forts

- Reconnaissance de l'engagement étudiant développée
- Échanges entre étudiants de Bachelor et élèves-ingénieurs
- Financement de la vie étudiante par l'école

Points faibles

- Peu de femmes présentes sur le campus

Risques

- La voie FISA réduit de fait la participation des étudiants Bachelor 3A à la vie étudiante

Opportunités

- Le nouveau campus de l'école, avec son espace plus important et l'accueil de plus d'étudiants

L'insertion professionnelle des diplômés

Elle est réalisée par l'école qui fait entre autres intervenir des conférenciers issus d'entreprises partenaires. Il faut souligner que les 12 diplômés de la première promotion 2021-2024 ont poursuivi leurs études en M1

Pas d'insertion professionnelle constatée pour la 1ère promotion

Pas de diplômés en entreprise : ceux que nous avons interviewé lors de l'audit ont bien confirmé que les entreprises attendaient des jeunes avec un diplôme bac+5 pour le domaine de la cybersécurité...

SWOT global sur la partie : L'insertion professionnelle des diplômés

Points forts

- Contenu de la formation adapté et très technique
- 3ème année en apprentissage devant faciliter l'insertion professionnelle

Points faibles

- Poursuite des études des 12 diplômés de la 1ère promotion

Risques

- Bachelor perçu comme une préparation à la poursuite d'études

Opportunités

- Attentes des entreprises en matière de compétences Cybersécurité

Bilan global de l'évaluation

Données fournies par l'école conformément à l'arrêté du 27 janvier 2020 relatif au cahier des charges des grades universitaires de licence et de master

Bachelor en Sciences et Ingénierie spécialité Cybersécurité

FISEA sur le site de Ivry-sur-Seine

Formation initiale sous statut d'étudiant sur le site de Ivry-sur-Seine

1. Garantir la qualité académique et un adossement à la recherche	
nombre et part des enseignants permanents dans la formation	18 permanents : 55 % (> 40%)
nombre et part des enseignants docteurs, de la ou des disciplines pertinentes, dans la formation	10 docteurs : 35 % (> 25%)
nombre et part des personnels enseignants-chercheurs, de la ou des disciplines pertinentes, dans le corps enseignant de la formation	8 enseignants-chercheurs : 30 % (>25%)
nombre et qualité des publications scientifiques par enseignant du programme	17, dans le cadre de l'unité ESIEA N&S – Numérique et société auditionnée par l'HCERES
autres indicateurs de productions scientifiques (brevets...) liés aux domaines de formations correspondant au diplôme	1 ouvrage
nombre de diplômés s'inscrivant dans le diplôme de niveau supérieur (niveau master ou doctorat)	Les 12 diplômés de la promo 2024 ont tous poursuivi leurs études (généralement en Mastère et Master, dans des voies plutôt professionnalisantes)
2. Préparer l'insertion professionnelle	
part des professionnels issus du monde socioéconomique du programme	14 intervenants : 34% (>25%)
taux d'emploi à 18 mois et à 30 mois des diplômés du programme	Pas encore de diplômés en recherche d'emploi (première promotion 2014, en poursuite d'études)
taux de poursuite d'études à un niveau supérieur	Les 12 diplômés de la promo 2024 ont tous poursuivi leurs études.
part des diplômés en emploi en CDI à 18 mois et à 30 mois	Non concerné car 1ère promotion diplômée en 2024
3. Favoriser la réussite de tous les étudiants	
part des étudiants en situation de handicap	4.5 % d'étudiants en situation de handicap pour l'école (100 sur 2200 étudiants / 7 étudiants pour le Bachelor cybersécurité)
part des étudiants en apprentissage	26 % des 3 promotions en 2024/2025
part des étudiants bénéficiant d'un accompagnement pédagogique ou d'un parcours de formation personnalisé	Aucun actuellement
4. Définir une politique sociale pour permettre l'accès de tous à la formation	
part des étudiants boursiers sur critères sociaux	En 2024-25 : 24% (>20%)
part des étudiants du programme soutenus par l'établissement	3% (<20%)
montant des aides de l'établissement distribuées au sein du programme	2000 € en 2024-2025 (10 000 € cumulés depuis 2022)
5. Inscrire son offre de formation dans la politique de site	
part des étudiants du programme poursuivant leurs études dans les formations du site hors de l'établissement d'origine	58%

part des enseignants-chercheurs de la formation inscrits dans les équipes de recherche du site	100% (>50%)
nombre de projets de recherche dans le domaine de la formation partagés avec d'autres établissements de formation et de recherche du site	3 (>1)
6. Favoriser la mobilité internationale	
part des étudiants en mobilité entrante/sortante	Sortante : Bachelor 2A : 100 % (=100%) Entrante : Bachelor 3A : 2 canadiens en 2023-2024 Entrante : Bachelor 3A : 1 canadien en 2025-2026
part des enseignants-chercheurs et enseignants en mobilité entrante/sortante	Mobilité entrante = 5 % - 2 enseignants chercheurs de FOI (Croatie) Mobilité sortante = 3 % - 1 enseignant chercheur à l'UQAC (Canada)
nombre et qualité des partenariats étrangers	2 partenariats actifs et pertinents : Faculty of Organization and Informatics (FOI) - Croatie Université de Québec à Chicoutimi (UQAC) - Canada
7. Mettre en œuvre une démarche qualité afin d'assurer l'amélioration continue de la formation	
fréquence des enquêtes	1 enquête de satisfaction globale par an + évaluation systématique des tous les enseignements
proportion des répondants	Bachelor 1 : 65% (<75%) Bachelor 2 : 82% (>75%) Bachelor 3 : 99% (>75%)

Conclusion globale de l'audit Bachelor

Ce Bachelor est crédible et bien positionné dans l'écosystème cybersécurité. La gouvernance, lisible et réactive, s'appuie sur une culture associative et un dialogue structuré avec les étudiants ; elle constitue un facteur de stabilité et de vitesse d'exécution apprécié dans un domaine mouvant. Le pilotage qualité/RSE est installé, avec des dispositifs et indicateurs qui soutiennent la dynamique d'amélioration continue. À ce titre, l'école dispose d'atouts pour maintenir l'alignement sur les standards attendus pour le grade de licence.

Sur le plan managérial, la mécanique PDCA est tangible (enquêtes récurrentes, suivis, itérations), mais son appropriation reste inégale côté étudiants : les taux de réponse contrastés invitent à renforcer l'engagement et la « valeur perçue » de l'évaluation des enseignements. Le pilotage gagnera à consolider des boucles de rétroaction plus visibles (restitution, décisions, effets) afin d'ancrer une culture partagée de la qualité au-delà de la conformité. Parallèlement, deux chantiers structurants, nouveau campus et refonte du SI, sont des leviers majeurs de transformation, à condition d'en maîtriser les risques de migration et de continuité pédagogique.

L'ancrage externe est solide : liens étroits avec l'écosystème (Campus Cyber, partenaires industriels, ANSSI/MI) et dispositifs de co-construction qui assurent une forte pertinence métier. C'est un déterminant central de l'employabilité et de la lisibilité du diplôme. L'exposition internationale et la mobilité sortante restent cependant encore modestes ; leur montée en puissance est une priorité pour conforter l'attractivité et l'ouverture interculturelle du programme.

La formation elle-même présente une architecture claire et progressive, combinant fondamentaux, mises en situation et professionnalisation (stages/alternance). L'usage de pédagogies actives (projets, hackathons, labs) et l'outillage numérique (GitLab, JupyterHub, bibliothèques) soutiennent l'apprentissage par la pratique et la montée en autonomie. L'adossement à la recherche via esieaLab et la présence d'enseignants-chercheurs apportent de la profondeur scientifique au cursus. Ces choix pédagogiques sont cohérents avec les compétences visées et la demande du marché.

Plusieurs points de vigilance appellent toutefois une action volontariste. D'abord, la mobilisation étudiante dans les évaluations doit être consolidée (incitations, formats, restitution courte), faute de quoi la boucle qualité perd en granularité et en réactivité. Ensuite, l'internationalisation (mobilités, parcours entrants/sortants, visibilité des partenariats) doit franchir un palier pour rejoindre les niveaux attendus. Enfin, l'intégration plus explicite de la RSE/numérique responsable dans les acquis d'apprentissage, ainsi que la reconnaissance formalisée des initiatives étudiantes, renforceront l'alignement avec les attentes sociétales et la motivation des promotions.

Les risques les plus significatifs tiennent à la vitesse d'évolution des métiers (IA/Cloud), à la pression concurrentielle des offres post-bac, à la rareté des ressources humaines expertes et aux aléas des chantiers SI/campus. Ils nécessitent une veille renforcée, une gouvernance agile des maquettes (itérations semestrielles assumées), des politiques RH proactives (attractivité/fidélisation des intervenants) et une conduite de projet outillée sur les migrations techniques, avec plans de contingence clairement établis. La charge multi-référentielle accroît par ailleurs la complexité opérationnelle ; la réussite passera par une priorisation explicite et une automatisation accrue de la collecte d'indicateurs.

En miroir, les opportunités sont substantielles : tension durable du marché cybersécurité, montée de l'apprentissage en 3^e année, nouveau campus écoconçu (fin 2025) et refonte SI (2026) propices à l'attractivité, au pilotage et à l'expérience étudiante. L'effet de réseau (partenaires, Campus Cyber, alumni) peut être davantage capitalisé pour des projets structurants et une visibilité nationale/européenne accrue. À court terme, la digitalisation des processus pédagogiques et administratifs permettra d'amplifier le suivi individualisé et l'agilité des parcours.

En conclusion, ce Bachelor présente une cohérence d'ensemble, une pertinence métier et une dynamique d'amélioration qui justifient une appréciation globalement favorable. La trajectoire est bien orientée au regard du référentiel CTI des BSI ; la consolidation des points de vigilance évoqués — engagement étudiant, internationalisation, intégration RSE, sécurisation des chantiers SI/campus, assurera le franchissement d'un cap de maturité. Si l'école transforme ses chantiers

structurants en gains concrets de qualité perçue et de pilotage, elle pourra non seulement sécuriser l'atteinte des attendus du grade de licence, mais aussi se distinguer durablement sur un marché de plus en plus compétitif.

SWOT global de l'audit Bachelor

Points forts

- Gouvernance associative stable, autonome et proche des étudiants
- Pilotage qualité/RSE outillé et alignement sur plusieurs référentiels (ESG, CTI, HCERES, CGE, Qualiopi)
- Démarche d'amélioration continue déployée à l'échelle de l'école, appuyée par des projets structurants
- Ancrages et partenariats forts (ANSSI, ministère de l'Intérieur, Campus Cyber, entreprises), adossés à un grand réseau d'alumni
- Positionnement métier clair et 3^e année en apprentissage favorisant l'insertion
- Pédagogies actives et hybrides (projets, hackathons, labs, équilibre présentiel/distanciel)
- Environnement numérique en modernisation (Proxmox VE, GitLab, JupyterHub, bibliothèques numériques)

Points faibles

- Participation des étudiants inégal aux enquêtes
- Internationalisation perfectible : peu de mobilités sortantes/rentantes à ce stade, visibilité internationale à renforcer.
- RSE/numérique responsable à approfondir dans la formation.
- Accompagnement individuel et reconnaissance des initiatives étudiantes à mieux structurer.
- Pas de conseil de perfectionnement spécifique à ce Bachelor

Risques

- Mutation rapide des métiers (IA, cloud) pouvant déplacer les compétences attendues
- Programme récent, pas encore installé durablement auprès de toutes les entreprises
- Concurrence post-bac en cybersécurité (tout type d'offre) brouillant la lisibilité du paysage
- Aléas de migration liés à la refonte du SI (calendrier et intégrations).
- Pression multi-référentielle et charge administrative accrues.
- Pénurie nationale de profils enseignants-chercheurs en cybersécurité (recrutement/fidélisation).

Opportunités

- Nouveau campus écologique et très équipé (livraison prévue novembre 2025) renforçant attractivité et conditions d'apprentissage
- Refonte du SI (2026) pour un pilotage et des services plus efficaces
- Marché cybersécurité en forte croissance
- Montée en puissance de l'apprentissage (3^e année) et des stages pour l'employabilité immédiate
- Présence/implication dans Campus Cyber et partenariats (MI, PwC, Gatewatcher, Wallix...).
- Déploiement/élargissement de collaborations internationales
- Outillage numérique pédagogique (GitLab, JupyterHub, labs) propice à l'innovation pédagogique.