	Responsable / *Responsible* : Ladislas HAJNAL & Nicolas LARRIEU	Ingénieur ENAC Année scolaire 2021/2022
S9-S10 **MSc-SSIR** **Formation** **TLS-SEC**	**Master Mention Réseaux et Télécommunications** **Parcours Sécurité des Systèmes d'Information et des Réseaux**	AVI SAT SITA

OBJECTIFS / *OBJECTIVES*

TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

Remarque : cette formation se présente comme une année de substitution complète réalisée dans les locaux de l'ENSEEIHT.

Les étudiants inscrits à la formation TLS-SEC ont la possibilité de s'inscrire également au parcours de MASTER R&T parcours SSI et des réseaux. Ceci se traduit par un module supplémentaire intitulé « gouvernance de la SSI » qui sera dispensé à l'université de Toulouse. A l'issue de l'année TLS-SEC, les étudiants qui auront également suivi le module supplémentaire « gouvernance de la SSI » se verront délivrés deux diplômes : diplôme TLS-SEC d'ingénieur et diplôme de MASTER parcours SSIR de l'université de Toulouse.

La formation TLS-SEC sera dès la première année adressée à un public diversifié, venant de la formation initiale et de la formation continue. Au niveau de la formation initiale les étudiants arrivent d'écoles d'ingénieurs et de parcours différents. Plus précisément il y aura potentiellement des élèves venant des formations :
- informatique et réseaux de l'INSA Toulouse ;
- automatique et électronique de l'INSA Toulouse ;
- génie mathématique et modélisation de l'INSA Toulouse ;
- des ingénieurs de l'ENAC ;
- télécommunications et réseaux de l'INP-ENSEEIHT ;
- informatique mathématiques et applications de l'INP-ENSEEIHT ;
- et des élèves de divers départements d'autres écoles de l'INP, des Mines d'Albi, et du Centre Universitaire Jean-François Champollion.

Pour en savoir plus / *For more information* : http://formations.enac.fr/fr/formations/feuilleter-le-catalogue/sciences-technologies-sante-STS/formation-d-ingenieur-classique-FI/ingenieur-enac-program-47517.html

Pour s'adapter à un public aussi diversifié nous intégrerons dans la formation diverses techniques pédagogiques..

Autoformation : les étudiants disposent d'une salle à l'année avec des ordinateurs récents et haut de gamme et de nombreux éléments actifs derniers cri (switchs, routeurs, ASAs, etc.). De nombreuses références sont données aux étudiants pour permettre de ser remettre à niveau et d'approfondir leurs connaissances en auto-formation.

Projets : dès le démarrage de l'année scolaire les étudiants seront regroupés équipes avec des profils variés au niveau des compétences d'entrée (électronique, réseau, système, programmation, mathématiques). L'évaluation sera en grande partie par projets, où les équipes seront en concurrence.

Challenges : il est habituel dans les formations en sécurité de participer aux challenges en ligne nationaux ou internationaux. Un des principaux objectifs que nous nous sommes donnés est la participation à ces challenges. De nombreuses ressources en ligne sont disponibles pour préparer ces challenges et nous avons déjà donné des pointeurs vers ces ressources aux étudiants qui ont déjà déposé leur dossier de candidature. Nous avons également des challenges que nous avons développé nous-mêmes. Ces *challenges* seront structurés sous la forme d'une suite de défis qui permettent aux étudiants de pénétrer au fur et à mesure au coeur d'un système d'informations ou d'un réseau vulnérable. Cette méthode d'apprentissage active permet aux étudiants de mieux cerner les stratégies d'attaque que des personnes malveillantes peuvent adopter lors d'une attaque informatique. Elle présente alors l'avantage de leur faire réaliser les enjeux, défis et difficultés de leur futur métier.

Conférences : un ensemble de conférences est mis en place pour permettre à des intervenants industriels et gouvernementaux d'illustrer les concepts théoriques vus lors des différents enseignements. Cette forme d'apprentissage permet aux étudiants 1) d'être sensibilisé aux implications de la mise en place de la sécurité informatique au sein d'une entreprise et au sein d'un état, et 2) de mettre en perspective leurs acquis vis-à-vis des problématiques concrètes rencontrées dans le monde industriel ou gouvernemental.

Structure générale de la formation

1er semestre :

- 400h d'enseignements.
- dont 100h de TP et 60h Compétences professionnalisantes (Anglais, Conférences)

380h distribués sur 4 modules plus 20h d'Anglais :

- 80h Module d'Entrée : Bases de la Sécurité
- 95h Module Réseau
- 105h Module Logiciel / Système / Matériel
- 100h Module de Sortie : Cas pratiques

2ème semestre : Projet long (rapport et soutenance en Anglais), certifications, stage de 6 mois

Calendrier :

- Rentrée : fin septembre
- Fin premier semestre : fin janvier
- Début stage : mars
- Fin stage : septembre

Répartition des modules dans l'année :

- Module d'Entrée : trois semaines à partir de la rentrée, temps complet
- Module de Sortie : jeudis matin (conférences) et trois semaines complètes en janvier
- Module Réseau : lundis et mardis de mi-octobre à fin décembre
- Module Logiciel / Système / Matériel : mercredis et vendredis de mi-octobre à fin décembre

Modalité de candidature :

Les étudiants de deuxième année intéressés par cette filière doivent faire parvenir leur lettre

de motivation aux points de contact ENAC (Ladislas Hajnal et Nicolas Larrieu) avant la fin du mois de mai.
Leur dossier devra contenir les pièces suivantes (il sera collecté à la fin du mois de mai) :

- Lettre de motivation pour expliciter le choix de la filière TLS SEC

Une réponse sur leur candidature sera donnée fin juin pour un début de troisième année TLS SEC vers la mi-septembre.