TELECOM Nancy

Ingénieurs du numérique • Inspiring your digital future

ÉCOLE EN INFORMATIQUE ET SCIENCES DU NUMÉRIQUE

Syllabus
FISEA 'Cybersécurité' 2025/2026

version du 2026-02-12

WWW.TELECOMNANCY.EU

UNIVERSITÉ DE LORRAINE

LORRAINE INP

Cti Commission des titres d'ingénieur

Table des matières

Semestre S5

Activité Sportives et Culturelles 1 (ASPC1)

UE : ASPC 5

ECTS : 0.5

Responsable(s) : Ashok MAGNIFIQUE

Volume horaire : 16 heures (16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Les cours de sport répondent aux enjeux de formation du cursus Telecom Nancy en permettant à tous les élèves de construire quatre compétences qui intègrent différentes dimensions (motrice, méthodologique, sociale), en s'appuyant sur des activités physiques sportives et artistiques (APSA) diversifiées. Ces compétences sont :

- La prise en compte des enjeux de sécurité, de santé et de bien-être liés aux pratiques physiques,
- L'enrichissement du savoir-faire relationnel, et le développement du capital coopératif
- L'appropriation seul ou à plusieurs des méthodes pour apprendre et mieux se connaitre
- Le développement de la motricité et des attitudes en vue d'une meilleure efficacité.

Acquis de formation

- Mobiliser différentes ressources (motrice, physiologique, cognitive, émotionnelles) et connaissances pour agir de manière efficiente
- Acquérir des techniques spécifiques
- Savoir faire preuve d'engagement, de persévérance, savoir se dépasser
- S'intégrer dans une organisation collective, prendre part à un projet collectif
- Travailler en équipe, en groupe, coopérer
- Assumer des rôles sociaux variés
- Prendre et accepter des décisions
- Contribuer au climat de réussite
- Adapter sa communication aux autres
- Apprendre par l'action, l'observation, l'analyse de son activité et de celle des autres
- Construire et renforcer les outils d'auto-évaluation formative
- Connaître ses points forts et ses points faibles
- Savoir gérer ses ressources et définir des axes de progrès
- Se remettre en question pour évoluer dans ses pratiques
- Se fixer, conduire et réguler un projet individuel ou collectif

Advent of Code (AOC)

UE : STIC 5

ECTS : 2

Responsable(s) : Pierre-Etienne MOREAU

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

- Initier les étudiants à la résolution de problèmes algorithmiques à travers des défis progressifs.
- Accompagner la découverte d'un nouveau langage de programmation (Go) et ses paradigmes fondamentaux.
- Développer des compétences pratiques en analyse et modélisation de problèmes complexes.
- Favoriser l'autonomie et la rigueur dans la conception, le test et l'optimisation de solutions.

Acquis de formation

À l'issue du cours, l'étudiant sera capable de :

1. Analyser un énoncé algorithmique et identifier les sous-problèmes.
2. Mettre en œuvre en Go des solutions correctes et efficaces.
3. Appliquer des techniques de parsing pour traiter des données textuelles.
4. Construire et exploiter des structures de données adaptées (tableaux, listes, maps, files, piles, graphes).
5. Évaluer la complexité algorithmique et optimiser les temps d'exécution.
6. Concevoir et exécuter des jeux de tests unitaires et fonctionnels.
7. Implémenter et comparer des algorithmes d'exploration et de recherche (BFS, Dijkstra, A*).
8. Utiliser la modélisation par graphes pour résoudre des problèmes réels.
9. Développer la capacité à écrire du code rigoureux et fiable, minimisant les erreurs, de logique ou d'exécution.

Algorithmiques, Structures et Résolutions de Problèmes (ASRP)

UE : STIC 5

ECTS : 2

Responsable(s) : Pierre LUDMANN

Volume horaire : 24 heures (8h CM, 10h TD, 6h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Une part importante de l'informatique consiste à être capable de sélectionner des algorithmes adaptés à des objectifs particuliers et de les appliquer, tout en reconnaissant la possibilité qu'aucun algorithme adéquat n'existe. Cette compétence repose sur la compréhension de l'éventail d'algorithmes permettant de traiter un ensemble important de problèmes bien définis, ainsi que sur la capacité à en reconnaître les forces et les faiblesses et leur pertinence dans des contextes spécifiques. L'efficacité est un thème omniprésent dans ce domaine.

Acquis de formation

- Pour chacune des stratégies (force brute, gloutonne, diviser pour régner, retour sur trace récursif, branch-and-bound et programmation dynamique) :
  - identifier un exemple pratique auquel elle s'applique
  - l'utiliser pour résoudre un problème approprié
- Déterminer si la règle gloutonne choisie conduit à une solution optimale
- Déterminer une approche algorithmique appropriée pour un problème

- Énoncer la définition formelle du "big O". Déterminer de manière informelle la complexité en temps et en espace d'algorithmes simples
- Définir les classes P et NP. Expliquer la signification de la NP-complétude
- Fournir des exemples de problèmes classiques NP-complets
- Démontrer qu'un problème est NP-complet en réduisant un problème classique connu comme NP-complet vers celui-ci

Fondamentaux en Cyber-Sécurité 1 (FCS1)

UE : STIC 5

ECTS : 2

Responsable(s) : Rémi BADONNEL

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Ce module permet de sensibiliser et initier les étudiants aux enjeux et problèmes liés à la cyber-sécurité (cf. label CyberEdu).

Acquis de formation

- Comprendre les motivations et le besoin de sécurité des SI,
- Connaître les définitions de base et la typologie des menaces,
- Appréhender et adopter les règles de base pour les organisations et les individus,
- Comprendre les vulnérabilités inhérentes aux mécanismes réseaux et applicatifs couramment utilisés,
- Connaître le panorama des solutions techniques de sécurité,
- Appréhender les méthodes et normes de prise en compte de la sécurité de façon globale et unitaire,
- Comprendre et anticiper les difficultés en gestion de la sécurité,
- Présenter les filières métiers de la cybersécurité,
- Se familier avec les plateformes d'entraînement à la cybersécurité,
- Savoir simuler des attaques simples et s'en prémunir.

Gestion de Projet (GP)

UE : PROJET 5

ECTS : 1

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 24 heures (16h TD, 8h Projet)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Former les futur(e)s ingénieur(e)s à la gestion de projet, leur permettre d'acquérir les méthodes et maîtriser les outils à appliquer systématiquement dans tous leurs projets futurs, à l'école et dans leur vie professionnelle.

Le cours est proposé sous la forme d'un MOOC organisé par Centrale Lille (Rémi Bachelet)

Acquis de formation

- Maîtrise des fondamentaux de la gestion de projets
- Découverte et prise en main des outils et des méthodes de la gestion de projet
- Travailler en équipe : le rôle du chef de projet et la culture d'entreprise
- Gérer des réunions et des documents de projets
- Piloter et mener à bout un projet en équipe restreinte

Introduction au Hacking Éthique 1 (HACK1)

UE : STIC 5

ECTS : 2

Responsable(s) : Pierre VEUTIN

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Cette UE vise à initier les étudiants aux principes du hacking éthique et à la démarche d'audit de sécurité. Les apprenants adoptent le point de vue d'un consultant en cybersécurité chargé d'identifier des failles, de tester la robustesse d'un système, de démontrer les risques associés et de formuler des recommandations adaptées. Le cours met l'accent sur la méthodologie professionnelle, le cadre légal et la rédaction de livrables d'audit.

Acquis de formation

- Comprendre et appliquer le cadre légal, contractuel et éthique de l'audit de sécurité.
- Conduire les phases de reconnaissance, cartographie et collecte d'informations (scan passif, scan actif).
- Identifier des vulnérabilités techniques sur des services, systèmes ou applications.
- Mettre en œuvre des tests d'intrusion limités et contrôlés dans un environnement pédagogique.
- Évaluer l'impact potentiel d'une exploitation et déterminer les risques associés.
- Produire un rapport d'audit professionnel, incluant scénarios d'attaque, preuves, criticité et recommandations.
- Présenter oralement une analyse claire et argumentée à un "client" (joué dans le cadre du cours).

Introduction au Hacking Éthique 2 (HACK2)

UE : STIC 5

ECTS : 2

Responsable(s) : Thierry ARRABAL

Volume horaire : 24 heures (4h CM, 4h TD, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Ce cours permet aux étudiants d'acquérir une compréhension approfondie des vulnérabilités courantes affectant les applications web, les réseaux et les systèmes, ainsi que des méthodes d'exploitation associées.

Dans un format de classe inversée, les étudiants travaillent en groupe sur une vulnérabilité spécifique, réalisent un état de l'art, conçoivent un démonstrateur d'exploitation et proposent des solutions de mitigation.

L'objectif est de développer des compétences d'analyse de vulnérabilités, de recherche scientifique, de développement sécurisé et de présentation technique.

Acquis de formation

À la fin du cours, les étudiants seront capables de :

- Analyser en profondeur une vulnérabilité (mécanisme, prérequis, surface d'attaque).
- Réaliser un état de l'art : articles scientifiques, CVE, incidents publics.
- Concevoir et exploiter un démonstrateur mettant en jeu une vulnérabilité réelle.
- Élaborer des contre-mesures pertinentes et évaluer leur efficacité.
- Présenter leurs travaux de manière structurée et professionnelle lors d'une soutenance.
- Collaborer efficacement en groupe dans un court projet (16-18h).
- Adopter une démarche responsable dans la manipulation de codes vulnérables.

Langue obligatoire - Anglais S5 (AN5)

UE : SEHS 5

ECTS : 1.5

Responsable : Muriel DUVAL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Obtention du score TOEIC demandé par l'école
- Approfondissement des quatre compétences langagières (expression orale et écrite, compréhension orale et écrite) en vue d'atteindre au minimum le niveau B2 du Cadre Européen Commun de Référence pour les Langues (CECRL) en fin de 1ère année

Acquis de formation

Groupe standard

- Comprendre le contenu essentiel de sujets concrets ou abstraits lors d'une discussion
- Comprendre une grande gamme de textes longs et complexes, ainsi que saisir des significations implicites

Groupe de perfectionnement :

- S'exprimer spontanément et couramment sans trop apparemment devoir chercher ses mots
- Utiliser la langue de façon efficace et souple dans sa vie sociale, professionnelle ou académique
- S'exprimer sur des sujets complexes de façon claire et bien structurée et manifester sa maîtrise des outils d'organisation, d'articulation et de cohésion du discours

Logique Mathématique (LOG)

UE : SFA 5

ECTS : 2

Responsable(s) : Pierre-Adrien TAHAY

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Il s'agit d'un cours d'informatique théorique. L'objectif principal est d'être capable de traduire des assertions exprimées dans un langage naturel (français, anglais…) dans un langage compréhensible par une machine avec des variables, des connecteurs logiques (logique des propositions) et des quantificateurs (logique du premier ordre). Ce formalise permet ensuite de résoudre des problèmes logiques de manière formelle à l'aide d'algorithmes de mise sous forme clausale et de résolution dans des systèmes formels (Robinson particulièrement).

Acquis de formation

- Savoir définir un ensemble par induction, des fonctions récursives et faire des preuves par induction.
- Traduire des énoncés simples de la langue naturelle dans le langage de la logique des propositions et le langage de la logique du premier ordre.
- Mener des démonstrations dans des systèmes formels fondés sur la règle de résolution.

Management des Organisations 1 (MO1)

UE : SEHS 5

ECTS : 1.5

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 24 heures (6h CM, 18h TD)

Méthode d'évaluation : QCM + Etude de cas + soutenance

Objectifs

Comprendre les organisations et l'entreprise en particulier, et ses spécificités.

Acquis de formation

- Comprendre les fondements d'une organisation et s'y situer : logique managériale et entrepreneuriale,
- Savoir décrire une entreprise (outil méthodologique),
- Prendre en compte la finalité RSE des entreprises,
- Savoir analyser la performance d'une organisation : management stratégique et opérationnel et la place des parties prenantes (notions de gouvernance),
- Comprendre les phénomènes générés par le processus de production et son histoire en vue d'arriver à un processus d'amélioration continue
- Comprendre les principes de la propriété intellectuelle

Mathématiques Appliquées : Probabilités (MAP-A)

UE : SFA 5

ECTS : 2

Responsable(s) : Sophie MÉZIÈRES

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Initier au raisonnement probabiliste, connaître les résultats de base les plus importants, et savoir les appliquer à la modélisation probabiliste de problèmes concrets simples

Acquis de formation

- Comprendre la notion de probabilité sur un ensemble fini ou infini
- Manipuler les variables aléatoires discrètes et continues
- Savoir modéliser des situations concrètes avec des probabilités

Programmation Web et Bases de Données (WEBBD)

UE : STIC 5

ECTS : 2

Responsable(s) : Gérald OSTER

Volume horaire : 24 heures (8h CM, 8h TD, 8h TP)

Méthode d'évaluation : Examen Terminal

Objectifs

This course introduces the fundamental principles of relational databases and the basics of web programming. Students will learn to design, query, and normalize relational databases using both theoretical and practical approaches. They will also gain foundational knowledge of web technologies, including HTTP, HTML, CSS, and server-side programming with Flask, to develop simple web applications that interact with a relational database.

Acquis de formation

- Explain the principles of database systems and the relational model.
- Design conceptual database schemas using the Entity-Relationship (E/R) model.
- Translate E/R schemas into relational schemas.
- Write and optimize queries using relational algebra and SQL.
- Apply normalization techniques to ensure data consistency and reduce redundancy.
- Understand the fundamentals of the web: architecture, HTTP, and client-server interactions.
- Write structured web pages using HTML and CSS.
- Develop simple dynamic web applications with Flask that interact with a relational database.

Projet Pluridisciplinaire d'Informatique Intégrative Cyber (PPII5)

UE : PROJET 5

ECTS : 5

Responsable(s) : Gérald OSTER

Volume horaire : 100 heures (100h Projet)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Ce projet vise à placer les élèves-ingénieurs en situation de développement complet d'un système informatique sur le thème de la cybersécurité intégrant :

- la conception algorithmique,
- la modélisation et l'implémentation de données,
- la réalisation d'un service web avec front-end et back-end,
- la gestion de projet collaboratif.

Les étudiants mettent en œuvre les compétences acquises dans les différentes UEs du semestre, et, notamment les enseignements traitant de l'algorithmique, des bases de données, de la programmation web, de la gestion de projet et de la cybersécurité.

Acquis de formation

À l'issue du projet, les étudiants seront capables de :

- Volet Gestion de projet :
  - Définir les besoins fonctionnels et techniques à partir d'un cahier des charges simplifié.
  - Planifier et suivre un projet (outils agiles, gestion des versions, documentation).
  - Utiliser des outils collaboratifs (Git, GitLab, Trello/Jira, Wiki, etc.).
  - Rédiger et présenter un rapport de projet clair et professionnel.
- Volet Algorithmique :
  - Analyser un problème et identifier les algorithmes pertinents.
  - Évaluer la complexité et la correction des solutions envisagées.
  - Implémenter et tester des algorithmes efficaces en Python.
- Volet Base de données :
  - Concevoir un modèle de données relationnel (MCD, MLD).
  - Normaliser et documenter le schéma de la base.
  - Implémenter et interroger une base relationnelle (PostgreSQL/MySQL/SQLite).
  - Gérer les interactions entre la base et l'application via une API.
- Volet Web :
  - Concevoir une architecture client-serveur.
  - Développer une API REST avec Flask.
  - Concevoir un front-end léger (HTML/CSS/JS ou framework minimal).
  - Connecter le front-end à l'API.
  - Déployer et tester une application web fonctionnelle.

Séminaire Esprit d'Équipe (SEM)

UE : SEM 5

ECTS : 1

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle continu

Objectifs

L'esprit d'équipe est une qualité indispensable dans toute forme d'organisation du travail, en particulier au niveau ingénieur.

- Encourager l'esprit de promotion et de faciliter l'intégration,
- Apprendre à s'affirmer et à communiquer au sein d'un groupe (atelier théâtre),
- Responsabiliser les étudiants sur l'organisation d'événements.

Acquis de formation

- Comprendre sa place dans un groupe
- Savoir se comporter dans le groupe
- Savoir organiser un événement comportant plus de 100 personnes

Socle Commun en Informatique (SCINFO)

UE : STIC 5

ECTS : 2

Responsable(s) : Christophe BOUTHIER

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Acquérir les savoirs et savoirs-faire indispensables en informatique pour le reste de la formation à TELECOM Nancy

Acquis de formation

- Savoir utiliser la ligne de commande pour naviguer dans le système de fichiers et gérer les permissions
- Savoir configurer un environnement de développement Python et l'utiliser pour résoudre un problème simple
- Savoir manipuler les données au niveau binaire (opérations bit à bit)
- Savoir utiliser Git pour les opérations de base : add, commit, push
- Comprendre les mécanismes fondamentaux des réseaux TCP/IP : adresses IP, DNS, URL
- Savoir ce qu'est un processus et comprendre son rôle dans un système
- Savoir utiliser une expression régulière simple

Techniques d'Expression et de Communication (TEC)

UE : SEHS 5

ECTS : 1.5

Responsable(s) : Isabelle HEUDIARD

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Maîtriser tous les aspects de la prise de parole devant un groupe : choix du contenu et des supports, gestuelle et élocution
- Développer des capacités de synthèse, à l'oral comme à l'écrit
- Identifier et comprendre les types d'arguments utilisés dans différents supports (textuels, iconographiques)
- Améliorer sa communication interpersonnelle

Acquis de formation

- Réaliser des supports clairs et pertinents au service d'une présentation orale de qualité
- Maîtriser tous les aspects de la communication non-verbale
- S'exprimer à l'oral avec aisance et améliorer la qualité de l'expression écrite
- Connaître et respecter les règles de la nétiquette
- Gérer le stress
- Identifier les informations essentielles contenues dans divers documents et les restituer de manière synthétique et argumentée
- Développer son esprit critique
- Interagir avec une équipe pour préparer un exposé

Semestre S6

Activité SPortives et Culturelles 2 (ASPC2)

UE : ASPC 6

ECTS : 0.5

Responsable(s) : Ashok MAGNIFIQUE

Volume horaire : 16 heures (16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Les cours de sport répondent aux enjeux de formation du cursus TELECOM Nancy en permettant à tous les élèves de construire quatre compétences qui intègrent différentes dimensions (motrice, méthodologique, sociale), en s'appuyant sur des activités physiques sportives et artistiques (APSA) diversifiées. Ces compétences sont :

- La prise en compte des enjeux de sécurité, de santé et de bien-être liés aux pratiques physiques,
- L'enrichissement du savoir-faire relationnel, et le développement du capital coopératif
- L'appropriation seul ou à plusieurs des méthodes pour apprendre et mieux se connaitre
- Le développement de la motricité et des attitudes en vue d'une meilleure efficacité.

Acquis de formation

- Mobiliser différentes ressources (motrice, physiologique, cognitive, émotionnelles) et connaissances pour agir de manière efficiente
- Acquérir des techniques spécifiques
- Savoir faire preuve d'engagement, de persévérance, savoir se dépasser
- S'intégrer dans une organisation collective, prendre part à un projet collectif
- Travailler en équipe, en groupe, coopérer
- Assumer des rôles sociaux variés
- Prendre et accepter des décisions
- Contribuer au climat de réussite
- Adapter sa communication aux autres
- Apprendre par l'action, l'observation, l'analyse de son activité et de celle des autres
- Construire et renforcer les outils d'auto-évaluation formative
- Connaître ses points forts et ses points faibles
- Savoir gérer ses ressources et définir des axes de progrès
- Se remettre en question pour évoluer dans ses pratiques
- Se fixer, conduire et réguler un projet individuel ou collectif

Assembleur (ASM)

UE : STIC 6

ECTS : 2

Responsable(s) : Christophe BOUTHIER

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Comprendre l'architecture hardware d'un ordinateur. Comprendre l'assembleur ARM 32 bits et la gestion mémoire de la pile.

Acquis de formation

- Apprendre les instructions de l'assembleur ARM 32 bits
- Maîtriser la gestion de la mémoire
- Maîtriser la gestion des cadres d'appels (stack frames)
- Maîtriser la manipulation des bits
- Comprendre le fonctionnement d'un programme écrit en assembleur ARM 32 bits

Fondamentaux en Cybersécurité 2 (FCS2)

UE : STIC 6

ECTS : 2

Responsable(s) : Jean-Marc MISERT

Volume horaire : 24 heures (8h CM, 4h TD, 12h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Approfondir les connaissances acquises dans le module *Fondamentaux Cyber-Sécurité 1* en se familiarisant à la gestion des accès et des identités, et explorant des problématiques plus avancées de cybersécurité.

Acquis de formation

- Comprendre les concepts liés à la gestion des accès et des identités, notamment dans le contexte d'un service d'annuaire (*active directory*).
- Connaître les vulnérabilités, attaques et contre-mesures liées à la gestion des accès et des identités.
- Explorer par groupe des thématiques actuelles liées à la cybersécurité (ruptures technologies, nouvelles menaces, attaques avancées, réglementations, aspects humains et organisationnels).

Formation à la Recherche d'Emploi / Apprentissage (FRE)

UE : SEHS 6

ECTS : 1

Responsable(s) : Isabelle HEUDIARD

Volume horaire : 12 heures (12h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Favoriser une réflexion sur le projet personnel et professionnel.
- Préparer l'insertion dans la vie professionnelle à l'issue du diplôme d'ingénieur.

- Aider à la recherche des stages de 2e et 3e année.

Acquis de formation

- Élaborer son projet professionnel
- Décrypter une offre
- Construire son CV
- Rédiger une lettre de motivation pertinente et efficace
- Se préparer à l'entretien de recrutement

Langage C (LGC)

UE : STIC 6

ECTS : 2

Responsable(s) : Olivier FESTOR

Volume horaire : 24 heures (8h CM, 8h TD, 8h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Ce module a pour objectif de présenter les principes fondamentaux du langage C ainsi que la représentation des données en mémoire

Acquis de formation

- Maîtriser les concepts fondamentaux du langage C
- Maîtriser la gestion de la mémoire en C
- Savoir créer un programme C fonctionnel résolvant un problème spécifique
- Savoir gérer et corriger les erreurs et failles courantes d'un programme C
- Maîtriser son environnement de programmation (éditeur de texte, débugger, processus de compilation, makefile)

Langue obligatoire - Anglais S6 (AN6)

UE : SEHS 6

ECTS : 1.5

Responsable(s) : Muriel DUVAL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Obtention du score TOEIC demandé par l'école
- Approfondissement des quatre compétences langagières (expression orale et écrite, compréhension orale et écrite) en vue d'atteindre au minimum le niveau B2 du Cadre Européen Commun de Référence pour les Langues (CECRL) en fin de 1ère année.

Acquis de formation

Groupe standard

- Comprendre le contenu essentiel de sujets concrets ou abstraits lors d'une discussion.
- Comprendre une grande gamme de textes longs et complexes, ainsi que saisir des significations implicites.

Groupe de perfectionnement :

- S'exprimer spontanément et couramment sans trop apparemment devoir chercher ses mots.
- Utiliser la langue de façon efficace et souple dans sa vie sociale, professionnelle ou académique.
- S'exprimer sur des sujets complexes de façon claire et bien structurée et manifester sa maîtrise des outils d'organisation, d'articulation et de cohésion du discours

Management des Organisations 2 (MO2)

UE : SEHS 6

ECTS : 1.5

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Comprendre les organisations et leurs spécificités à travers leurs stratégies sur différents marchés

Acquis de formation

- Etablir des diagnostics stratégiques d'entreprises et proposer des solutions (
- Définir la stratégie globale et par domaine d'activité,
- Analyser la croissance d'une entreprise,
- Réaliser le mix-marketing produit (méthodologie des 4P, etc.)

Mathématiques Appliquées Numériques et Analyse de Données - A (MAN-A)

UE : SFA 6

ECTS : 2

Responsable(s) : Jean-François SCHEID

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Examen final

Objectifs

Dans ce cours on introduit les notions et outils classiques de l'analyse numérique qui interviennent dans les problèmes d'analyse de données. Ces méthodes font partie de la culture indispensable à tout ingénieur du numérique.

Acquis de formation

- Identifier les problèmes potentiels d'arithmétique flottante intervenant dans un calcul numérique.
- Analyser la stabilité d'un calcul numérique.
- Identifier le type de décomposition matricielle à réaliser en fonction des propriétés des matrices.
- Connaitre différentes factorisations matricielles usuelles.
- Analyser la stabilité de la solution d'un système linéaire
- Connaitre les principes de la classification non-hiérarchique.

Méthodologies et Outils DevOps (DEVOPS)

UE : STIC 6

ECTS : 2

Responsable(s) : Christophe BOUTHIER

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Acquis de formation

- Explorer les fonctionnalités avancées de Git pour gérer des *workflows* de développement collaboratifs plus complexes
- Comprendre l'architecture et le fonctionnement interne de git
- Utiliser docker pour créer, gérer et déployer des applications conteneurisées
- Concevoir et implémenter des pipelines d'Intégration et de déploiement continus (CI/CD) avec gitLab CI/CD
- Appliquer ces concepts et outils à un projet logiciel concret

Modèles des Systèmes à Événements Discrets (MSED)

UE : SFA 6

ECTS : 2

Responsable(s) : Zahra RONDEAU

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Epreuve Terminale

Objectifs

- Comprendre les concepts fondamentaux et les contraintes des systèmes à évènements discrets.
- Maîtriser les méthodes, modèles et outils utilisés pour l'analyse et la conception de ces systèmes.

Acquis de formation

- comprendre et prendre en compte les caractéristiques et contraintes des systèmes à évènements discrets

- identifier évènements, états et transitions dans un système discret.
- résoudre des problèmes élémentaires à l'aide de la modélisation
- modéliser des problèmes réels sous forme graphique
- acquérir les connaissances liées à la conception et réalisation de systèmes complexes
- maîtriser les méthodes, modèles et outils pour la conception et la réalisation de systèmes discrets
- choisir les méthodes et modèles appropriés
- modéliser des systèmes discrets pour étudier leur comportement
- expliquer les modes de représentation de systèmes discrets
- analyser et construire un modèle discret pour la commande d'un système
- prendre en compte les contraintes liées aux interactions et synchronisation

Programmation Orientée Objet (POO)

UE : STIC 6

ECTS : 2

Responsable(s) : Gérald OSTER

Volume horaire : 24 heures (8h CM, 8h TP, 8h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Acquérir les concepts fondamentaux de la programmation orientée objets (abstraction, encapsulation, héritage, polymorphisme) et les mettre en œuvre en Java.
- Développer des logiciels simples, testés, lisibles et maintenables (TDD, refactoring, patterns élémentaires).
- Utiliser l'écosystème professionnel : Git, Gradle, JUnit 5, outils d'analyse statique et intégration continue.

Acquis de formation

- Utiliser le langage Java pour implémenter et tester des algorithmes pour résoudre des problèmes simples.
- Concevoir et implémenter des classes.
- Utiliser les mécanismes d'encapsulation orientés objet tels que les interfaces et les membres privés.
- Appliquer les techniques de décomposition pour découper un programme complexe en morceaux plus simples et réutilisables.
- Utiliser l'héritage pour concevoir des hiérarchies simples de classes permettant aux sous-classes de réutiliser du code.
- Raisonner sur le flot de contrôle dans un programme faisant intervenir la liaison dynamique.
- Tracer l'exécution de segments de code variés et de résumer leur effets en terme de calcul.
- Manipuler les collections & génériques, exceptions, entrées/sorties.
- Tester (JUnit), déboguer, profiler et améliorer la qualité (SOLID, refactoring, code smells).

Projet Pluridisciplinaire d'Informatique Intégrative Cyber 2 (PPII6)

UE : PROJET 6

ECTS : 4

Responsable(s) : Gérald OSTER

Volume horaire : 100 heures (100h Projet)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Ce projet vise à placer les élèves-ingénieurs en situation de développement complet d'une application logicielle performante et modulaire en langage C pour la cybersécurité. Il mobilise des compétences en algorithmique avancée, en programmation système basique, en gestion de la mémoire, en gestion de projet collaboratif, et en cybersécurité.

Les étudiants mettent en œuvre les connaissances acquises dans les UEs du semestre, notamment celles portant sur la programmation en C, les structures de données avancées, les concepts de chaîne de compilation, la gestion de projet logiciel, et la cybersécurité.

Un cas d'application typique consiste à concevoir ou à sécuriser un logiciel en s'appuyant sur la bibliothèque SDL, tout en respectant une démarche d'ingénierie logicielle rigoureuse.

Acquis de formation

À l'issue du projet, les étudiants seront capables de :

- Volet Gestion de projet
  - Identifier et formaliser les besoins fonctionnels et techniques d'un projet logiciel.
  - Définir une architecture logicielle adaptée et planifier les étapes de développement.
  - Utiliser des outils de gestion de versions et de suivi (Git, GitLab, Trello/Jira).
  - Documenter et présenter les choix techniques et le produit réalisé.
- Volet Programmation en C
  - Concevoir et développer un programme structuré, modulaire et lisible en C.
  - Maîtriser la gestion dynamique de la mémoire (allocation, libération, vérification).
  - Utiliser efficacement les pointeurs, structures, tableaux dynamiques et listes chaînées.
  - Gérer les entrées/sorties, les fichiers, et les interactions avec une bibliothèque graphique (SDL).
  - Mettre en œuvre un makefile et assurer la portabilité du code.
- Volet Algorithmique et structures de données avancées
  - Choisir et implémenter des structures de données adaptées (arbres, graphes, files de priorité, etc.).
  - Évaluer la complexité algorithmique des solutions proposées.
  - Optimiser les performances du code (temps d'exécution, mémoire, modularité).
  - Tester et valider les algorithmes sur des jeux de données représentatifs.
- Volet Ingénierie logicielle
  - Concevoir une première architecture logicielle.
  - Appliquer les principes de modularité et d'encapsulation.
  - Intégrer des tests unitaires et de validation.
  - Assurer la robustesse et la maintenance du code sur la durée du projet.

Réseaux (RES)

UE : STIC 6

ECTS : 2

Responsable(s) : Thibault CHOLEZ

Volume horaire : 24 heures (8h CM, 4h TD, 12h TP)

Méthode d'évaluation : Examen Terminal

Objectifs

Acquérir les connaissances de base sur les réseaux informatiques. Comprendre l'architecture en couches du modèle OSI et son instanciation dans le monde Internet (TCP/IP).

Acquis de formation

- Connaître l'architecture d'Internet à différents niveaux (physique, économique, logique)
- Savoir décrire le fonctionnement des protocoles associés aux principales applications internet
- Savoir identifier le niveau d'encapsulation d'un protocole et déchiffrer son en-tête protocolaire
- Modéliser un protocole de transport
- Concevoir un plan d'adressage IP et configurer un routage statique
- Configurer et déboguer une pile réseau
- Évaluer la qualité de service d'un réseau
- Utiliser un analyseur de trafic

Stage Ouvrier (STA1A)

UE : STAGE 1A

ECTS : 1.5

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 4 à 8 semaines

Méthode d'évaluation : Examen Terminal

Objectifs

Le stage de première année a pour but d'apporter une première expérience en entreprise avec un travail de type opérateur. Plus précisément, il a vocation à permettre de :

- connaître la structure organisationnelle d'une entreprise ou d'une association et savoir la caractériser,
- comprendre la notion de secteur et de filière, l'environnement social, matériel, historique d'une entreprise, les problèmes rencontrés au quotidien et leurs résolutions
- conforter les qualités professionnelles et tout particulièrement l'aptitude à travailler au sein d'un groupe
- Adapter ces aptitudes et qualités aux exigences organisationnelles, techniques et humaines d'un emploi d'opérateur.

Acquis de formation

Le stage 1A permet de développer principalement les compétences suivantes :

- connaître l'entreprise (contexte socio-économique, se situer dans la structure et dans l'environnement hiérarchique, identifier les personnes-ressources dans l'entreprise),
- comprendre l'environnement spécifique du monde du travail (hygiène et sécurité, conditions matérielles, conditions humaines, normes en vigueur),
- s'intégrer dans un contexte professionnel en être capable de se conformer aux contraintes de l'activité, aux normes associées et apporter une valeur ajoutée à l'organisme d'accueil,
- mettre en perspective le rôle de l'ingénieur dans un contexte industriel,
- valoriser l'expérience et développer les qualités rédactionnelles au travers d'un rapport de stage.

Structures de Données (SD)

UE : STIC 6

ECTS : 2

Responsable(s) : Olivier FESTOR

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Ce module est consacré aux structures de données essentielle de l'informatique.

Il a pour objectifs de permettre aux élèves de maîtriser les structures de données principales de l'informatique au travers de leur spécification, test, implémentation dans une langage de bas niveau.

Acquis de formation

- Connaître, savoir choisir et utiliser les structures de données usuelles,
- Être capable de spécifier les structures usuelles de manière algébrique,
- Ecrire et dériver des tests à partir des spécifications,
- Maîtriser l'implémentation des structures et des algorithmes associés en langage C,
- Comparer les performances des structures de données standard et des algorithmes associés.

Théorie des Langages (TLA)

UE : SFA 6

ECTS : 2

Responsable(s) : Pierre-Adrien TAHAY

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Deux examens intermédiaires de 30 minutes et un examen final de 2h.

Objectifs

L'objet de ce cours est, en grande partie, une introduction à la théorie des langages, les automates finis et les grammaires algébriques. Les étudiants doivent être familiers avec les différentes notions, les définitions, les différentes méthodes effectives pour construire un automate fini et inversement déterminer le langage rationnel qu'il dénote, le rendre déterministe et minimiser le nombre d'états à l'aide d'algorithmes. La fin du cours introduit la notion de grammaires algébriques avec différents exemples afin de préparer les étudiants au module de compilation au S7.

Acquis de formation

- Acquérir la notion de langages et connaître les opérations sur les langages
- Déterminiser et minimiser un automate fini
- Reconnaître si un langage est régulier
- Savoir écrire une grammaire algébrique répondant à une spécification donnée
- Savoir mener une analyse LL(1) d'une grammaire algébrique

Semestre S7

Analyse d'attaques et de défenses (AAD)

UE : STIC 7

ECTS : 2

Responsable(s) : Pierre VEUTIN

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

L'objectif de ce cours est de permettre aux étudiants d'identifier, analyser et comprendre des attaques informatiques réelles, en s'appuyant sur l'étude de traces numériques issues de différents systèmes d'exploitation (Linux et Windows). Le cours met l'accent sur la détection, l'interprétation et la reconstitution d'un scénario d'attaque, ainsi que sur les principales mesures de défense associées.

Acquis de formation

- Analyser des logs et artefacts systèmes pour reconstituer un incident de sécurité.
- Identifier les techniques d'attaque courantes sur Linux et Windows.
- Détecter des comportements anormaux ou malveillants (malware, exploitation, persistance).
- Utiliser des outils d'analyse, de triage et d'investigation numérique.
- Proposer des contre-mesures et bonnes pratiques pour limiter les risques et renforcer les défenses du système.

Compilation 1 (COMPIL1)

UE : SFA 7

ECTS : 2

Responsable(s) : Suzanne COLLIN

Volume horaire : 56 heures (8h CM, 16h TD, 32h Projet)

Méthode d'évaluation : Examen Terminal

Objectifs

- Connaissances des techniques de base de la compilation des langages : analyse lexicale et syntaxique, contrôles sémantiques, mémoire à l'exécution et génération de code.

Acquis de formation

- Maîtrise du fonctionnement de l'analyseur lexical
- Spécification et réalisation d'un analyseur syntaxique ascendant SLR et LALR
- Construire des structures d'arbre abstrait et de table des symboles
- Décrire, analyser et exploiter la représentation des objets en mémoire à l'exécution
- Représenter la pile à l'exécution d'un programme écrit dans un langage impératif

Comptabilité Gestion (CGE)

UE : SEHS 7

ECTS : 1.5

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Epreuve Terminale

Objectifs

- Appréhender les bases du fonctionnement financier et comptable de l'entreprise ainsi que l'évaluation de sa situation financière et fonctionnelle
- Comprendre les techniques de gestion financière appliquées à la problématique du choix des investissements

Acquis de formation

- Lire un compte de résultat, un bilan et les annexes de la liasse fiscale
- Élaborer un diagnostic financier et fonctionnel de l'entreprise
- Lire et comprendre une fiche de paie

Cryptographie et Authentification (ICRYP)

UE : SFA 7

ECTS : 2

Responsable(s) : Jannik DREIER

Volume horaire : 44 heures (8h CM, 16h TD, 20h Projet)

Méthode d'évaluation : Epreuve Terminale

Objectifs

Donner aux étudiants les bases de la cryptographie pour appréhender le domaine de la protection de l'information et ouvrir à certains concepts de la sécurité des systèmes d'information.

Acquis de formation

- Maîtriser les enjeux de la cryptographie dans la protection de l'information
- Connaître les objectifs cryptographiques de base (confidentialité, intégrité, authenticité)
- Maîtriser le vocabulaire de la cryptographie
- Comprendre les principaux algorithmes de chiffrement symétrique et asymétrique et les garanties fournies
- Connaître les principales fonctions de hachage cryptographique associées et les garanties fournies
- Connaître les principaux algorithmes de signature et MAC et les garanties fournies
- Comprendre les limites de la protection assurée par la cryptographie

Graphes et Recherche Opérationnelle (GRO1)

UE : SFA 7

ECTS : 2

Responsable(s) : Bruno PINÇON

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Epreuve Terminale

Objectifs

L'objectif principal de ce cours est de doter les élèves d'un ensemble de compétences nécessaires en aide à la décision.

Il s'agit dans un premier temps de modéliser et de formaliser un certain nombre de problèmes types d'optimisation. Certains de ces problèmes sont ensuite étudiés d'un point de vue théorique et des méthodes de résolution sont présentées et analysées. Ce premier module insiste sur l'aspect pratique en utilisant le solveur gurobi.

Acquis de formation

- Identification et modélisation d'un problème de type recherche opérationnelle.
- Bases théoriques sur certains de ces problèmes appelés programmes linéaires (PL)
- Quelques méthodes pour résoudre ces problèmes de façon exacte ou approchée (via une ou des heuristiques) ou en combinant méthodes heuristique et exacte.

Intelligence Artificielle 1 (IA1)

UE : SFA 7

ECTS : 2

Responsable(s) : François BUET

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Epreuve Terminale (2 h)

Objectifs

Permettre aux étudiants d'avoir une connaissance générale des objectifs et des domaines d'applications de l'intelligence artificielle, et d'entrevoir le fonctionnement et les conditions d'utilisation des principaux outils numériques du domaine.

Acquis de formation

- Modéliser un problème (variables, espace de recherche, opérateurs, prise en compte des coûts, de l'incertitude, des contraintes…)
- Concevoir une heuristique.
- Définir un critère d'optimalité.
- Appliquer une méthode de recherche de solution.
- Sélectionner, implémenter et comparer des algorithmes de machine learning/deep learning adaptés au problème étudié.

Langue obligatoire - Anglais S7 (AN7)

UE : SEHS 7

ECTS : 1.5

Responsable(s) : Muriel DUVAL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Améliorer la maîtrise des quatre compétences langagières (expression orale et écrite, compréhension orale et écrite) pour maintenir ou parfaire un niveau B2, C1 ou C2
- Développer les compétences professionnelles nécessaires pour travailler en entreprise dans un contexte international

Acquis de formation

- Avoir une meilleure connaissance de soi, de son projet professionnel et savoir l'exposer en anglais
- Savoir lire une offre d'emploi rédigée en anglais
- Savoir rédiger un CV, une lettre de motivation, une « follow-up letter », lorsqu'on souhaite postuler à l'étranger
- Être préparé à un entretien d'embauche en anglais

Modélisation Objet et Conception des systèmes d'Information - Analyse (MOCI1)

UE : STIC 7

ECTS : 2

Responsable(s) : François CHAROY

Volume horaire : 24 heures (8h CM, 4h TD, 12h TP)

Méthode d'évaluation : Contrôle Continu

Objectifs

À l'issue du cours, l'étudiant doit être capable d'identifier clairement les besoins fonctionnels et non fonctionnels d'un système, de maîtriser les techniques de recueil et d'analyse des besoins. Rédiger un cahier des charges structuré et exploitable, de valider et vérifier les exigences recueillies auprès des parties prenantes, et d'utiliser des outils standards d'ingénierie des besoins (ex. diagrammes UML, user stories).

Acquis de formation

- Lister les composants d'un cas d'utilisation
- Décrire comment le processus d'ingénierie des besoins permet leur élicitation et leur validation
- Interpréter un cahier des charges pour un système logiciel
- Décrire les problèmes fondamentaux et les techniques classiques utilisées pour l'élicitation des besoins
- Décrire les éléments principaux d'un modèle de données
- Identifier les besoins fonctionnels et non-fonctionnels dans un document de spécification des besoins
- Conduire une revue d'un document de spécification pour en déterminer la qualité

Modélisation Objet et Conception des systèmes d'Information - Conception (MOCI2)

UE : STIC 7

ECTS : 2

Responsable(s) : François CHAROY

Volume horaire : 24 heures (8h CM, 4h TD, 12h TP)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Connaître les différentes principes et modèles de conception (Fonctionnel, Objet, Event Based)
- Savoir concevoir en utilisant une approche orientée objets - introduction à GRASP
- Connaître les patrons de conception
- Découvrir l'architecture logicielle à partir des patrons d'architecture de base

Acquis de formation

- Comprendre les principes de conceptions classiques
- Appliquer un paradigme de conception pour concevoir un logiciel simple et savoir l'expliquer
- Utiliser un paradigme de conception de façon appropriée pour concevoir un logiciel simple
- Dans le contexte d'un paradigme de conception, décrire un ou plusieurs patrons de conceptions qui pourraient être mis en œuvre.
- Créer des modèles structurels et comportementaux appropriés pour un logiciel à partir d'un cahier des charges
- Identifier une architecture logicielle à partir d'une conception de haut niveau
- Mettre en œuvre des design patterns simple lors de la conception d'un logiciel

Projet d'Entreprise S7 (PE7)

UE : PE 7

ECTS : 4

Responsable(s) : Thibault CHOLEZ

Volume horaire : 109 heures (4h TD, 3x35H en entreprise au S7)

Méthode d'évaluation : Épreuve Terminale (Notes de Travail, Rapport, Soutenance)

Objectifs

- Montrer que l'apprenti est autonome pour résoudre les problèmes d'un assistant-ingénieur.
- Mener à bien une mission de cybersécurité en entreprise.
- Analyser un problème de cybersécurité en entreprise.
- Mise en œuvre d'une solution de cybersécurité appropriée.

Acquis de formation

Compétences métiers

- Réaliser un développement technique sur la base d'un cahier des charges dans un cadre contraint,
- Programmer dans un langage informatique spécifique,

- Appliquer des procédures intégrées et instrumentées d'une chaîne de production logicielle,
- Documenter, tester et valider un développement technologique,
- Réaliser un état de l'art sur une méthode ou une technologie particulière développée ou mise en oeuvre dans le stage;

Compétences transverses

- Développer sa capacité d'auto-apprentissage pour approfondir ses connaissances et compétences sur un champ particulier (MOOC, SPOC, tutoriel, formation en entreprise, ...)
- Présenter un projet technique et sa réalisation au travers d'un rapport et d'une soutenance
- Mesurer, journaliser les ressources associées
- Travailler dans une équipe, (savoir présenter ses idées, savoir écouter, et comprendre les autres, dialoguer et rendre compte, coopérer pour arriver à des objectifs)
- Maîtriser les outils et pratiques d'ateliers et de réunions de travail (assurer la prise de note, rédiger des comptes rendus et plans d'action, ...)
- identifier les lieux et les personnes ressources, créer et développer la collaboration à l'échelle du projet

Projet d'Innovation Cyber (INOV)

UE : INOV

ECTS : 7

Responsable(s) : Thibault CHOLEZ

Volume horaire : 182 heures (7h TD, 5x35H en entreprise au S7)

Méthode d'évaluation : Épreuve Terminale (Notes de Travail, Rapport, Soutenance)

Objectifs

- Découvrir le fonctionnement général d'un département R&D, d'un bureau d'étude, ou tout service chargé de faire de la veille technologique.
- Découvrir un thème de recherche et développement particulier ou de veille technologique en cybersécurité.
- Réfléchir sur un sujet très précis et limité dans le cadre du thème étudié.
- Apprendre la méthodologie scientifique de réalisation d'état de l'art, de présentation et d'évaluation des résultats.
- Comprendre le fonctionnement des processus de publication et d'évaluation des travaux de recherche.

Acquis de formation

- Comprendre l'organisation et les processus de la recherche et développement.
- Réaliser un état de l'art sur un sujet scientifique et/ou technologique précis.
- Développer une contribution ciblée en cybersécurité et l'évaluer avec rigueur.
- Présenter un travail sous la forme d'un rapport.
- Présenter le travail à l'oral devant des pairs.
- Gestion d'un projet de recherche

Systèmes 1 (SYS1)

UE : STIC 7

ECTS : 2

Responsable(s) : Moufida MAIMOUR

Volume horaire : 56 heures (8h CM, 8h TD, 8h TP, 32h Projet)

Méthode d'évaluation : Épreuve Terminale

Objectifs

- Comprendre le rôle et l'évolution des systèmes d'exploitation dans un système informatique.
- Maîtriser les notions fondamentales de processus, d'adressage et de gestion de la mémoire, ainsi que les mécanismes de communication interprocessus
- Identifier les mécanismes matériels et logiciels assurant la protection et la sécurité des ressources.

Acquis de formation

- Décrire l'organisation, les fonctions et les composants essentiels d'un système d'exploitation.
- Manipuler les processus et les mécanismes d'entrée/sortie sous UNIX/Linux.
- Mettre en œuvre les principaux mécanismes de communication interprocessus (signaux, tubes, fichiers).
- Expliquer les principes de la gestion mémoire, de la pagination et de la mémoire virtuelle.
- Identifier les mécanismes de protection de base et découvrir les notions introductives de forensic mémoire.
- Mettre en pratique la programmation système en C sous UNIX/Linux.
- Concevoir et implémenter un mini-shell intégrant l'exécution de commandes, les redirections et les pipes.
- Manipuler les appels systèmes liés aux processus, à la gestion de la mémoire et aux entrées/sorties.
- Appliquer les notions fondamentales des systèmes d'exploitation abordées en cours de système à travers une réalisation concrète

Semestre S8

Droit 2A (DROIT)

UE : SEHS 8

ECTS : 1.5

Responsable(s) : Anne-Claire HEURTEL

Volume horaire : 24 heures (6h CM, 18h TD)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Initier aux principes de base de l'organisation juridique française, au droit des affaires, au droit social et au droit numérique.

Acquis de formation

- Se référer à la législation en vigueur pour la négociation des contrats
- Observer la particularité du contrat de travail et les droits et obligations qui en découlent
- Amener les étudiants à prendre conscience des différentes situations de la vie professionnelle (formation, modification du contrat, rupture de la relation de travail)
- Comprendre les enjeux liés au droit du numérique (protection des données personnelles, propriété intellectuelle et identité numérique, cybercriminalité et responsabilité des acteurs du numérique)
- Réfléchir aux motivations pour le choix d'une structure juridique.

Investigation Numérique, Réponse à Incidents (INV)

UE : STIC 8

ECTS : 2

Responsable(s) : Mickael JENFT

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Présenter un ensemble de techniques relatives à l'investigation numérique permettant la préservation, la recherche et la restitution de la preuve numérique.

Acquis de formation

- Savoir dans quel contexte il est nécessaire d'appliquer une procédure d'investigation numérique
- Etre capable de réaliser une sécurisation de données de n'importe quel équipement numérique
- Connaître les éléments qu'il est possible d'analyser, avec quels outils
- Savoir mettre en œuvre une méthodologie permettant une analyse rigoureuse d'un média

Langue obligatoire - Anglais S8 (AN8)

UE : SEHS 8

ECTS : 1.5

Responsable(s) : Muriel DUVAL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Améliorer la maîtrise des quatre compétences langagières (expression orale et écrite, compréhension orale et écrite) pour maintenir ou parfaire un niveau B2, C1 ou C2
- Développer les compétences professionnelles nécessaires pour travailler en entreprise dans un contexte international

Acquis de formation

- Réussir son entretien d'embauche en anglais
- Savoir conduire une réunion en anglais ou y participer de façon professionnelle, savoir faire un compte-rendu de réunion ou rédiger un ordre du jour
- Savoir présenter un projet informatique réalisé en binôme, à l'aide d'un support visuel (PowerPoint) et savoir répondre aux questions posées à l'issue de sa présentation

Méthodologie, Droit et Organisation en Cyber-Sécurité (MDO)

UE : STIC 8

ECTS : 2

Responsable(s) : Vivien MAINTENANT, Jean-Marc MISERT

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Aborder les aspects organisationnels, juridiques, économiques et sociaux spécifiques au domaine de la cyber-sécurité.

Acquis de formation

- Connaître les principales normes et guides organisationnels en cyber-sécurité (ANSSI EBIOS, ITIL Gestion des Incidents, NIST SCAP, NSA/CCS)
- Appréhender le droit et la réglementation spécifique à la cyber-sécurité (DSSI, ENISA, NIS)
- Comprendre les schémas de certification et d'évaluation de produits (ISO, CSPN premier niveau)
- Connaître l'organisation et les principaux processus relatifs à la cyberdéfense (réaction, traitement, coordination, gestion de crise, communication), stratégie et souveraineté nationale
- Savoir évaluer les impacts économiques et sociaux liés à la cyber-sécurité

Projet d'Entreprise S8 (PE 8)

UE : PE 8

ECTS : 11

Responsable(s) : Thibault CHOLEZ

Volume horaire : 571 heures (11h TD, 16x35H en entreprise au S8)

Méthode d'évaluation : Épreuve Terminale (Notes de Travail, Rapport, Soutenance)

Objectifs

- Montrer que l'apprenti est autonome pour résoudre les problèmes d'un assistant-ingénieur.
- Mener à bien une mission de cybersécurité en entreprise.
- Analyser un problème de cybersécurité en entreprise.
- Mise en œuvre d'une solution de cybersécurité appropriée.

Acquis de formation

Compétences métiers

- Réaliser un développement technique sur la base d'un cahier des charges dans un cadre contraint,
- Programmer dans un langage informatique spécifique,
- Appliquer des procédures intégrées et instrumentées d'une chaîne de production logicielle,
- Documenter, tester et valider un développement technologique,
- Réaliser un état de l'art sur une méthode ou une technologie particulière développée ou mise en oeuvre dans le stage;

Compétences transverses

- Développer sa capacité d'auto-apprentissage pour approfondir ses connaissances et compétences sur un champ particulier (MOOC, SPOC, tutoriel, formation en entreprise, ...),
- Présenter un projet technique et sa réalisation au travers d'un rapport et d'une soutenance,
- Mesurer, journaliser les ressources associées,
- Travailler dans une équipe, (savoir présenter ses idées, savoir écouter, et comprendre les autres, dialoguer et rendre compte, coopérer pour arriver à des objectifs),
- Maîtriser les outils et pratiques d'ateliers et de réunions de travail (assurer la prise de note, rédiger des comptes rendus et plans d'action, ...),
- identifier les lieux et les personnes ressources, créer et développer la collaboration à l'échelle du projet.

Renseignement d'Origine en Source Ouverte (OSINT)

UE : STIC 9

ECTS : 2

Responsable(s) : Jean-Philippe AUZELLE

Volume horaire : 24 heures (8h CM, 4h TD, 12h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Former les étudiants aux techniques et méthodologies du renseignement d'origine en source ouverte (OSINT), permettant la collecte, l'analyse et la restitution d'informations pertinentes provenant de sources accessibles au public.

Acquis de formation

- Savoir identifier les situations nécessitant le recours à l'OSINT
- Être capable de collecter des informations pertinentes depuis diverses sources ouvertes (médias, réseaux sociaux, bases de données publiques, web profond)
- Connaître les outils et techniques d'analyse permettant de transformer des données brutes en renseignement exploitable
- Savoir présenter et restituer les informations collectées de manière claire, structurée et éthique

Réseaux Avancés (RA)

UE : STIC 8

ECTS : 2

Responsable(s) : Rémi BADONNEL

Volume horaire : 36 heures (6h CM, 6h TD, 12h TP, 12h Projet)

Méthode d'évaluation : Epreuve Terminale

Objectifs

- Approfondir et mettre en application les connaissances sur le fonctionnement des réseaux, leurs mécanismes internes, et analyser de façon détaillée les protocoles de l'Internet.

Acquis de formation

- Connaître les principales familles de protocoles de routage, en comprendre le fonctionnement, ainsi que les avantages et les inconvénients,
- Maîtriser les principes du contrôle de congestion mis en œuvre par le protocole TCP, et connaître les différents algorithmes associés à ce protocole
- Savoir programmer des applications communicantes en C (sockets), et maîtriser les interfaces et paradigmes avancés liés à cette programmation
- Configurer des équipements réseaux et des systèmes pour réaliser des interconnexions et des services de base sur une plateforme cyber-range
- Comprendre l'évolution des architectures et protocoles réseaux (protocole IPv6…)

Sécurité des Applications (SECAP)

UE : STIC 8

ECTS : 2

Responsable(s) : Elliot BRETT, Thierry ARRABAL

Volume horaire : 24 heures (4h CM, 8h TD, 12h Projet)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Aborder les problèmes de sécurité spécifiques au développement de logiciels

Acquis de formation

- Connaître les failles et attaques de sécurité liées aux langages de programmation, au développement d'applications web et aux systèmes de gestion de bases de données
- Connaître et savoir mettre en œuvre les bonnes pratiques liées au développement logiciel
- Connaître et mettre en œuvre des méthodologies pour rechercher des failles de sécurité
- Savoir utiliser des outils usuels pour la sécurisation de code informatique (analyse statique, analyse dynamique)

Sécurité des Architectures (SECARCH)

UE : STIC 8

ECTS : 2

Responsable(s) : Pierre VEUTIN

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Ce module vise à doter les étudiants des connaissances et compétences nécessaires pour concevoir, analyser et améliorer des architectures techniques sécurisées. Le cours introduit les principes fondamentaux de la sécurité by design, de la segmentation réseau, de la gestion des flux, de la défense en profondeur et de l'intégration de mécanismes de protection dans des environnements hybrides (on-premise, virtualisés, cloud).

L'étudiant adopte la posture d'un architecte sécurité capable de proposer des choix techniques argumentés et adaptés aux risques.

Acquis de formation

- Analyser une architecture informatique existante et identifier ses faiblesses.
- Concevoir une architecture sécurisée intégrant les principes fondamentaux :
  - défense en profondeur
  - segmentation réseau
  - gestion des accès et des identités
  - durcissement des composants
- Définir et modéliser les flux réseau et les zones de sécurité.
- Intégrer des solutions de sécurité adaptées (pare-feu, proxy, WAF, IDS/IPS, VPN, IAM, etc.)
- Justifier des choix d'architecture en fonction des menaces, contraintes et besoins métiers.
- Produire une documentation technique claire : schémas, règles, principes directeurs,

Supervision, Contrôle et Internet (SCI)

UE : STIC 8

ECTS : 2

Responsable(s) : Rémi BADONNEL

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

- Découvrir les concepts clés de la supervision de réseaux et services.
- Mettre en œuvre ses concepts avec différents outils (du monitoring à la configuration), en considérant différentes aires fonctionnelles (FCAPS).

Acquis de formation

- Comprendre les enjeux de la supervision de réseaux et services,
- Connaître des concepts, architectures et protocoles clés du domaine,
- Savoir comment est représentée l'information de gestion et réaliser des requêtes,
- Etre familiarisé avec l'utilisation et le paramétrage d'une solution de supervision.

Systèmes Avancés (SYS2)

UE : STIC 8

ECTS : 2

Responsable(s) : Moufida MAIMOUR

Volume horaire : 24 heures (8h CM, 8h TD, 8h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

- Comprendre les principes de fonctionnement du noyau liés à la création, la planification et la coordination des processus.
- Maîtriser les mécanismes de synchronisation et leurs implémentations concrètes (sémaphores, mutex, etc.).
- Développer des applications concurrentes multi-threadées robustes et efficaces sous Linux (pthreads)

Acquis de formation

- Comprendre la gestion et l'implantation des processus sous UNIX/Linux.
- Identifier et comparer les principaux algorithmes d'ordonnancement, et analyser le comportement des politiques de scheduling.
- Maîtriser les mécanismes de synchronisation, d'exclusion mutuelle et de communication entre processus.
- Manipuler les processus et threads en langage C sous Linux.
- Utiliser lespthreads et les primitives de synchronisation POSIX.

Semestre S9

Big-Data et Intelligence Artificielle pour la Cyber-Sécurité (BDIA)

UE : STIC 9

ECTS : 2

Responsable(s) : Christophe BIANCO

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Avoir une vue d'ensemble sur les différents principes en œuvre dans la collection, le traitement et l'analyse de données volumineuses, changeantes, structurées et non structurées pour déterminer des situations et des tendances parmi des volumes de données.

Acquis de formation

- Comprendre le concept de logs et des technologies associées (SIEM, Big Data, etc.)
- Identifier les principes de traitements (corrélation, normalisation, etc.)
- Acquérir les principes de définition et de gestion de cas d'usage
- Définir des rapports et indicateurs au sein de tableaux de bord
- Techniques de traitement des données (analyse comportementale, machine learning, deeep learning, modèles statistiques) appliquées à la cybersécurité
- Environnement réglementaire sécurité et vie privée

Cryptographie Avancée (ACRYP)

UE : SFA 9

ECTS : 2

Responsable(s) : Jannik DREIER

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Présenter des méthodes et outils cryptographiques avancés et leurs cas d'utilisation

Acquis de formation

- Connaître le fonctionnement et les objectifs de méthodes et outils cryptographiques avancés comme les preuves à divulgation nulle, chiffrements avancés ou homomorphiques, le calcul multipartite sécurisé, les réseaux de mélange, les preuves de travail
- Comprendre l'utilisation de ces méthodes et outils dans des applications comme la blockchain et les contrats intelligents, les protocoles de vote électronique, les protocoles d'authentification (multi-facteurs)
- Être en mesure d'évaluer la pertinence d'une solution cryptographique avancée.

Exercice de Gestion de Crise Cyber (CW)

UE : CW

ECTS : 1.5

Responsable(s) : Rémi BADONNEL

Volume horaire : 36 heures (36h Projet)

Méthode d'évaluation : Contrôle Continu

Objectifs

Aborder une gestion de crise cyber, à travers un exercice fictif, mais réaliste de cyber wargame, mêlant à la fois des compétences organisationnelles et techniques.

Acquis de formation

- Etre capable de s'organiser en équipe, d'établir des roulements, et de gérer l'effort face à une situation de crise cyber
- Savoir protéger des infrastructures et services informatiques, et réagir face à des attaques ou tentatives d'attaques cyber, en étant placé dans des conditions réalistes
- Rechercher des failles de sécurité et réaliser des attaques simulées sur des systèmes virtuels ou physiques pouvant être complexes
- Connaître et expérimenter les enjeux d'une lutte informatique d'influence

Ingénierie Centre Opérationnel Cyber Sécurité (SOC)

UE : STIC 9

ECTS : 2

Responsable(s) : Christophe BIANCO

Volume horaire : 36 heures (10h CM, 26h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Présenter aux étudiants les méthodes et outils liés à la gestion de la sécurité au travers de cas concrets, tout en abordant également les problématiques liées à la sécurité physique et matérielle dans ce contexte.

Acquis de formation

- Comprendre les principes de gestion de risque
- Concevoir et mettre en place une politique de sécurité du système d'information (PSSI)
- Maîtriser les méthodes et outils permettant sa supervision et son contrôle (SMSI intégré à un système Analytique)
- Appréhender les éléments de la politique relative à la sécurité physique et matérielle du système d'information
- Comprendre le fonctionnement d'un SOC (Security Operating Center) et les différentes étapes liées à la gestion des incidents de sécurité.
- Mettre en place les concepts liés à cette gestion au travers de travaux pratiques (Blue team versus Red team)

Langue obligatoire - Anglais S9 (AN9)

UE : SEHS 9

ECTS : 1.5

Responsable(s) : Muriel DUVAL

Volume horaire : 24 heures (24h TD)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Améliorer sa prise de parole devant un auditoire de façon formelle et informelle
- Réaliser des supports clairs et pertinents si nécessaire

Acquis de formation

- S'exprimer à l'oral avec aisance, clarté et rigueur dans tout type de contextes (présentations formelles, informelles, conduites de débats et interactions en petits groupes)
- Maîtriser les bases de la phonétique anglaise pour améliorer la qualité de sa production orale

Malware et Rétro-ingénierie de Code (MLW)

UE : STIC 9

ECTS : 2

Responsable(s) : Guillaume BONFANTE

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Présenter aux étudiants les méthodes et outils liés à la virologie informatique
et à la rétro-ingénierie de code

Acquis de formation

- Savoir évaluer les vulnérabilités d'un système au regard de la menace induite par les logiciels malveillants
- Savoir évaluer la dangerosité d'un programme, en décrire les anomalies
- Savoir analyser les protections d'un malware (obfuscation) et les contourner
- Etre capable de rechercher la « payload » d'un malware par analyse statique (IDA) ou dynamique (pintool), et en retourner les fonctionnalités
- Décrire les dégâts provoqués par un malware sur un système

Projet d'Entreprise S9 (PE9)

UE : PE 9

ECTS : 12

Responsable(s) : Thibault CHOLEZ

Volume horaire : 362 heures (12h TD, 10x35H en entreprise au S9)

Méthode d'évaluation : Épreuve Terminale (Notes de Travail, Rapport, Soutenance)

Objectifs

Permettre l'acquisition des compétences indispensables, dans les domaines de la gestion et du management, à l'exercice du métier d'ingénieur de spécialité cybersécurité.

Acquis de formation

- Compétences métiers
  - Rédiger une note de cadrage
  - Définir des spécifications techniques et/ou des modèles,
  - Déterminer des choix techniques (architecture logicielle et matérielle) et sélectionner des technologies
  - Réaliser une solution fonctionnelle et/ou technique,
  - Appliquer les méthodes de validation « southbound » (tests techniques, tests fonctionnels, preuves, métrologie) et « northbound » (conformité de la solution au cahier des charges et attentes des usagers)
  - Maîtriser la conduite de projet (planifier, identifier, définir et hiérarchiser les activités à accomplir, réaliser les actions, s'adapter aux contraintes et aux changements, évaluer les résultats)
  - Respecter les délais et les procédures
  - Rendre compte aux parties-prenantes
  - Maîtrise de l'organisation et de la conduite de réunions
  - Gérer une configuration multi-acteurs (encadrement académique, encadrement industriel, membres du groupe-projet)
  - Savoir travailler en équipe (s'engager, savoir motiver et impliquer les autres, gérer les conflits et les différents points de vue, négocier les compromis)
  - Maîtriser la communication professionnelle (présenter un produit abouti à l'oral et à l'écrit en français et en anglais, animer une formation, etc.)
- Compétences transverses
  - Maîtriser la conduite de projet (planifier, identifier, définir et hiérarchiser les activités à accomplir, réaliser les actions, s'adapter aux contraintes et aux changements, évaluer les résultats)
  - Respecter les délais et les procédures
  - Rendre compte aux parties-prenantes
  - Maîtrise de l'organisation et de la conduite de réunions
  - Gérer une configuration multi-acteurs (encadrement académique, encadrement industriel, membres du groupe-projet)
  - Savoir travailler en équipe (s'engager, savoir motiver et impliquer les autres, gérer les conflits et les différents points de vue, négocier les compromis)
  - soutenir la prise de décision en situation de management d'entreprise (organiser, anticiper, choisir, calculer, budgéter, contrôler, corriger)
  - Maîtriser la communication professionnelle (présenter un produit abouti à l'oral et à l'écrit en français et en anglais, animer une formation)

Protocoles de Sécurité et Vérification (PSV)

UE : SFA 9

ECTS : 2

Responsable(s) : Jannik DREIER

Volume horaire : 24 heures (8h CM, 16h TD)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Présenter aux étudiants les protocoles de sécurité (ou protocoles cryptographiques), et les méthodes et outils liés à leur vérification.

Acquis de formation

- Comprendre la conception et la description des protocoles cryptographiques
- Être en mesure d'anticiper les attaques
- Comprendre les modèles d'attaquant, en évaluer les conséquences pratiques
- Savoir spécifier un protocole et ses propriétés de sécurité
- Connaître un logiciel de vérification de protocoles

Sécurité des Réseaux et Services (SRS)

UE : STIC 9

ECTS : 2

Responsable(s) : Jérôme FRANÇOIS

Intervenant(s) : Jérôme FRANÇOIS, Vincent LECUIRE

Volume horaire : 24 heures (8h CM, 4h TD, 12h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

Étudier et d'approfondir les problèmes de sécurité spécifiques aux réseaux et aux logiciels informatiques en s'appuyant sur les connaissances des systèmes d'exploitation et des protocoles de l'Internet.

Acquis de formation

- Connaître les principales menaces contre les réseaux informatiques et les vulnérabilités liées aux couches/protocoles,
- Comprendre les principes d'exploitation des vulnérabilités réseaux,
- Appréhender les outils de scan et d'analyse réseau, ainsi que ceux utilisés pour l'interception et l'altération de trames.
- Être capable de configurer des règles de filtrage, et d'utiliser différents outils de protection des réseaux (pare-feux, systèmes de détection d'intrusion, VPN sécurisés…)

Séminaire 3A (SEM3A)

UE : SEM 9

ECTS : 1

Responsable(s) : Zahra RONDEAU

Volume horaire : 36 heures (36h Projet)

Méthode d'évaluation : Contrôle Continu

Objectifs

- Permettre l'acquisition des compétences indispensables, dans les domaines de la gestion et du management, à l'exercice du métier d'ingénieur.

Acquis de formation

- Élaborer son projet professionnel
- Analyser et structurer ses savoirs, savoir-faire et savoir-être et les présenter
- Construire son argumentation lors de l'entretien d'embauche

Technologies du Continuum Numérique (TCN)

UE : STIC 9

ECTS : 2

Responsable(s) : Thierry ARRABAL

Volume horaire : 24 heures (8h CM, 16h TP)

Méthode d'évaluation : Épreuve Terminale

Objectifs

L'objectif du cours est d'acquérir à la fois les connaissances et les compétences liées au continuum numérique, du cloud à l'internet des objets, et en maîtriser leurs spécificités ainsi que les risques associés.

Acquis de formation

- Connaître le fonctionnement des principaux protocoles de l'Internet des Objets
- Comprendre les principes du cloud computing et les patrons architecturaux associés.
- Simuler un réseau de capteurs sans fil, modifier et compiler le *firmware* d'un capteur, déployer et superviser un réseau de capteurs sans fil
- Connaître des caractéristiques du système d'exploitation Android et les principales fonctionnalités du *framework* de développement, concevoir et développer une application Android
- Savoir déployer et configurer un ou plusieurs service(s) dans une infrastructure cloud courante (IaaS)
- Maîtriser les risques de cybersécurité liés à ces environnements

Semestre S10

Projet de Fin d'Etudes (PFE10)

UE : PFE 10

ECTS : 30

Responsable(s) : Thibault CHOLEZ

Volume horaire : 953 heures (8h TD, 27x35H en entreprise au S10)

Méthode d'évaluation : Épreuve Terminale (Notes de Travail, Rapport, Soutenance)

Objectifs

Mettre l'élève ingénieur en situation professionnelle sur un projet d'envergure en cybersécurité et lui permettre de mobiliser l'ensemble des compétences et connaissances acquises dans sa formation et de les mettre en œuvre au service d'un projet d'envergure en cybersécurité au sein d'une organisation.

Acquis de formation

- Compétences métiers
  - Appliquer les techniques d'analyse des besoins et des problèmes,
  - Élaborer un cahier des charges fonctionnel
  - Définir des spécifications techniques et/ou des modèles
  - Réaliser ou piloter la réalisation d'une solution fonctionnelle et/ou technique (gérer les risques, les situations imprévues, les sources d'erreur)
  - Appliquer les méthodes de validation « southbound » (tests techniques, tests fonctionnels, preuves, métrologie) et « northbound » (conformité de la solution au cahier des charges et attentes des usagers)
  - Maîtriser le déploiement, la sécurité, la sûreté de fonctionnement, la performance, le suivi et la maintenance en production de la solution,
  - Intégrer l'ensemble des dimensions temporelles et capacitaires d'un système informatique (évolutivité, passage à l'échelle)
- Compétences transversales
  - Être capable de mobiliser ses connaissances scientifiques
  - Analyser et résoudre un problème complexe
  - Savoir travailler en autonomie (gérer son temps, planifier, anticiper, prendre des décisions)
  - Être force de proposition
  - Maîtriser la conduite de projet (définition de la problématique, identifier, définir et hiérarchiser les activités à accomplir, réaliser les actions, s'adapter aux changements, évaluer les résultats)
  - Maîtrise de l'organisation et de la conduite de réunions
  - Savoir travailler en équipe (s'engager, savoir motiver et impliquer les autres, gérer les conflits et les différents points de vue, négocier les compromis)
  - Savoir travailler en réseaux (créer, développer la collaboration avec les personnes et les organisations, organiser et enrichir un réseau)
  - Maîtriser la communication professionnelle (rédiger clairement et efficacement, connaître et utiliser différents supports de communication, préparer un exposé, s'exprimer en public, s'adapter à des publics différents, gérer le stress)
  - Assurer une veille technologique permanente (identifier les besoins d'information, mettre en œuvre les stratégie de recherche, évaluer la pertinence des informations collectées, l'exploiter de façon efficace)

TELECOM Nancy
193 avenue Paul Muller
54600 Villers-lès-Nancy - France
Tél. +33 (0)3 72 74 59 00
www.telecomnancy.eu
contact@telecomnancy.eu

Facebook : TELECOM Nancy
X : @TELECOMNancy

Coordonnées GPS : 48°40'8" N - 06°09'25" E