Semestre 1

Module **Ethique de l'Ingénieur**		
Cours : 3h	Cours appliqués : 12h	Travail personnel : 10h

De la charte d'éthique de l'ingénieur à l'éthique dans la sécurité de l'information, l'étudiant sera invité à s'autodéterminer en termes de valeurs et de déontologie.

Objectifs d'apprentissage

- Ethique et morale, de l'antiquité à nos jours
- Quel est le rôle de l'ingénieur (DD/RSE)
- La place de la sécurité de l'information au sein de la société
- Hacking éthique et Red Team
- Profession de foi du RSSI/RSI et Blue Team

Compétences visées

La notion d'éthique est fondamentale pour un ingénieur en regard de sa fonction dans la société. Il s'agit de permettre aux étudiants d'en prendre toute la mesure et cela particulièrement dans les métiers de la sécurité de l'information au sein d'une société devenue cyber dépendante sur bien des aspects.

Module **Méthodologie Projet**		
Cours : 6h	TD : 9h	Travail personnel : 10h

Un projet, quelle que soit sa nature, possède une logique en propre. Il s'agit d'introduire l'étudiant à cette logique

Objectifs d'apprentissage

- Architecture de l'entreprise
- La place du projet dans une entreprise
- Outils de gestions de projet
- Prise en compte de la sécurité dans les projets
- Gestion du risque (ISO31000)
- Résilience (ISO28000)

Compétences visées

La prise en compte de tous les facteurs clé autorisant la réussite d'un projet, incluant les aspects de sécurité, de gestion du risque et de résilience.

Module **Machine Learning**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce cours fournit une introduction à l'apprentissage automatique, à la classification et à la reconnaissance de formes statistiques. Le cours mettra également l'accent sur de nombreuses applications de base.

Objectifs d'apprentissage

- Apprentissage supervisé :
  Régression : régression linéaire simple et multiple.
  Classification : Régression logistique, Analyse Discrimante Linéaire et Quadratrique, Naive Bayes, Support Vector Machines.
- Apprentissage non supervisé :
  Réduction de la dimensionalité : analyse en composantes principales.
  Clustering : Kmeans, modèles gaussiens, maximisation des attentes.

Compétences visées

Savoir décrire et choisir un modèle approprié dans une situation donnée.
Formuler un modèle et l'implémenter dans une solution d'entreprise.

Module **Network**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce module couvre l'architecture générique des réseaux (modèle OSI et TCP/IP) dans une approche centrée sur la sécurité.

Objectifs d'apprentissage

- Types et classification des réseaux
- Modèle OSI
- Modèle TCP/IP
- Encapsulation et protocoles
- Eléments de Sécurité (Cryptographie, certificats, pare feu, IDS et IPS, VPN et SSH, DDL et TLS, outils de hack et contremesures)

Compétences visées

Comprendre le fonctionnement des principaux protocoles de la famille TCP/IP.
Répartir les fonctions réseautiques selon les différentes couches d'une architecture de réseau donnée.
Effectuer des choix judicieux d'architectures et de protocoles selon les besoins à satisfaire et les problèmes à résoudre.
Comprendre les enjeux de sécurité liés aux réseaux.

Module **Operating Systems**		
Cours : 6h	TD : 9h	Travail personnel : 10h

Ce cours à pour but de donner une connaissance des instructions Linux.

Objectifs d'apprentissage

- IOS, shell commands et scripting
- Linux virtual machine installation
- Linux commands, permissions, configuration
- Bash commands
- Shell scripts

Compétences visées

A l'issue de ce cours l'étudiant sera à l'aise avec l'utilisation de Linux.

Module **Scrum**		
Cours : 6h	TD : 9h	Travail personnel : 10h

Ce cours développe les spécificités d'une gestion de projet agile de type Scrum. Il débouche sur une certification. Ce cours est en blended learning pour la certification.

Objectifs d'apprentissage

- Principes de la gestion de projet agile.
- Agile vs Cycle en V ?
- Limites et apports de Scrum.
- Le rôle du Scrum Master.
- La prise en compte de la sécurité dans les projets en mode agile.

Compétences visées

A l'issue de ce cours l'étudiant sera à même de choisir une méthodologie adaptée à son projet (Scrum ou waterfall/cycle en V) en y incluant la prise en compte de la sécurité.

Module **Securing Embedded Software**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce cours enseigne les concepts essentiels de la qualité, de la sûreté et de la sécurité des logiciels embarqués.

Objectifs d'apprentissage

- Définitions de base : systèmes embarqués, logiciels embarqués, bugs logiciels, qualité des logiciels embarqués, sûreté et sécurité (MISRA, CERT, ...)
- Vérification de logiciels avec des outils d'analyse statique et dynamique (SonarQube, Valgrind, ...)
- Notions de base sur l'architecture des ordinateurs, la compilation, la manipulation des bits, la représentation des nombres entiers, des chaînes de caractères et des nombres flottants (Data Lab)
- Assemblage x86 (Bomb Lab + Attack Lab)

Compétences visées

Comprendre les abstractions entre le programme et la plate-forme d'exécution, ainsi que certains détails d'implémentation pour trouver et éliminer efficacement les bogues et protéger les systèmes embarqués des attaques qui peuvent nuire à leur sûreté et leur sécurité.

Module **HW Virtualization and Trust**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce cours s'intéresse à la virtualisation du hardware et comment cette technique contribue à la sécurité. Ce cours est centré sur Pike OS connue pour sa robustesse et son usage dans les systèmes embarqués temps-réel critiques.

Objectifs d'apprentissage

- Eléments de Hardware
- Hardware Consolidation
- Abstraction matérielle
- Multiple Independent Levels of Security
- Root of Trust and Chain of Trust
- PikeOs Separation Kernel

Compétences visées

Comprendre les différents niveaux d'abstraction du matériel et leur impact sur la sécurité des systèmes embarqués.

Module **OS Architecture**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce cours a pour but de donner une compréhension fondamentale du rôle et du fonctionnement d'un système d'exploitation. Le cours est centré sur linux dont l'usage est très majoritaire dans toutes les couches d'un écosystème IoT.

Objectifs d'apprentissage

- OS : objectifs et grandes lignes (exécution de processus, principales architectures, quelques familles et Linux)
- Mémoire (adressage, stack, heap, gestion, concurrence, distribution)
- Modules (principe, architecture, points d'entrée, dépendances, phases d'insertion)
- Processus, tâches et interruptions (systèmes de traitement et calcul vs systèmes embarqués, processus et tâches, IPC, classes d'ordonnancement, interruptions, Multi-CPU, multi-cœurs, gestion de la concurrence, préemption)
- Sous-systèmes et généricité (VFS, PCI, stacks réseau, USB, Industrial IO)
- Droits d'accès et sécurité
- Etudes de quelques failles connues, exploit et patch.

Compétences visées

A l'issue de ce cours l'étudiant sera à même de comprendre le fonctionnement de Linux en détail et aura une idée des principaux enjeux de sécurité des OS.

Module **Cybersecurity Landscape**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module introduit les notions fondamentales de la cybersécurité

Objectifs d'apprentissage

- Principes généraux
- Vocabulaire (virus, ver, cheval de Troie, root kit, …)
- Problèmes liés à l'architecture réseaux
- Problèmes liés aux systèmes d'exploitation
- Les failles web
- Les risques par catégorie
- Les acteurs de la cybersécurité
- Sociologie du cybercrime
- Législation

Compétences visées

A l'issue de ce cours les étudiant auront une vue générale de l'écosystème de la cybersécurité (acteurs, enjeux et vocabulaire).

Module **Projet pour l'Innovation Industrielle (1/2)**		
Cours : 10h		Travail personnel : 115h

Dans ce module les étudiants sont mis en équipe d'au moins 4 étudiants et sont mis en situation de prestation de service pour un « partenaire » (entreprise, laboratoire de recherche, association, etc…). C'est une mission de type « forfait » et non « régie », contrairement au stage, mais le principe reste très proche.

Les partenaires suivent l'équipe par des réunions d'avancement. Le projet s'étale sur les semestres 1 et 2 et aboutis à un livrable et une évaluation sur le niveau de satisfaction du partenaire.

Ces projets doivent contenir **une part significative de sécurité** pour être validés pour les étudiants de la majeure.

Objectifs d'apprentissage

- Gestion de projet
- Compétences professionnelles en situation de service
- Autoformation (les sujets doivent idéalement explorer des aspects non abordés en cours)

Compétences visées

Toutes les compétences d'un ingénieur en prestation de service chez un client : communication, suivi des tâches, points d'avancement, planification, prise en compte et gestion des risques, réalisation des testes et des recettes, documentation, acquisition de nouvelles compétences techniques…

Module **Advanced Database Mangement**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce module traite des questions de performance et de volumétrie caractéristiques des grands systèmes d'information actuels en introduisant les techniques d'optimisation des index et des requêtes.
Il traite également les questions de la sécurité des données et la gestion d'accès aux données.

Objectifs d'apprentissage

- Administration : Architecture Oracle, Gestion des utilisateurs, Schéma Oracle
- Optimisation de la base de données : Gestion du stockage, Plan d'exécution, Indices, Vues matérialisées
- PL/SQL : Fonctions et procédures de stockage, Déclencheurs

Compétences visées

Maitriser l'optimisation des bases de données. Résoudre les problèmes liés à la grosse volumétrie. Maitriser la sécurité des données. Maitriser la gestion des accès à la base de données.

Module **Node and React Developpement**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce module traite du développement Web avec les langages Node.js et React, et donne **les bonnes pratiques** de développement pour sécuriser le code.

Objectifs d'apprentissage

- Mise en œuvre des langages
- Node.js vs React : Pro et cons
- Bonnes pratiques de développement

Compétences visées

Développer "proprement" une interface Web (**security by coding**).

Module **Software Engineering**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Le génie logiciel s'intéresse aux procédures systématiques qui permettent de répondre aux attentes des clients, d'être **fiable**, d'avoir de faibles coûts de maintenance et d'être performant tout en respectant les délais et les coûts de construction.

Ce cours a pour objectif d'enseigner aux étudiants les fondamentaux du génie logiciel.

Objectifs d'apprentissage

- Modélisation de logiciels
- Modèles de conception de logiciels
- Méthodologies logicielles classiques
- Pratiques et méthodologie pour le développement sécurisé
- Sécurité intrinsèque des différents langages de programmation

Compétences visées

Être capable de faire des conceptions logicielles correctes et **fiables**.
Être capable d'adopter les meilleures pratiques en matière de programmation de logiciels et d'avoir une approche **security by design**.

Semestre 2

Module **Projet pour l'Innovation Industrielle (2/2)**		
Cours : 21h		Travail personnel : 104h

Dans ce module les étudiants sont mis en équipe d'au moins 4 étudiants et sont mis en situation de prestation de service pour un « partenaire » (entreprise, laboratoire de recherche, association, etc…). C'est une mission de type « forfait » et non « régie », contrairement au stage, mais le principe reste très proche. Les partenaires suivent l'équipe par des réunions d'avancement. Le projet s'étale sur les semestres 1 et 2 et aboutis à un livrable et une évaluation sur le niveau de satisfaction du partenaire.

Ces projets doivent contenir **une part significative de sécurité** pour être validés pour les étudiants de la majeure.

Objectifs d'apprentissage

- Gestion de projet
- Compétences professionnelles en situation de service
- Autoformation (les sujets doivent idéalement explorer des aspects non abordés en cours)

Compétences visées

Toutes les compétences d'un ingénieur en prestation de service chez un client : communication, suivi des tâches, points d'avancement, planification, prise en compte et gestion des risques, réalisation des testes et des recettes, documentation, acquisition de nouvelles compétences techniques…

Module **Méthodologie Recherche**		
Cours : 6h	TD : 9h	Travail personnel : 10h

La méthodologie de recherche est un aperçu de la façon dont une recherche donnée est effectuée. Elle définit les techniques ou les procédures utilisées pour identifier et analyser les informations concernant un sujet de recherche spécifique. La méthodologie de recherche a donc à voir avec la façon dont un chercheur conçoit son étude de façon à pouvoir obtenir des résultats valides et fiables et atteindre ses objectifs de recherche.

L'application de la méthodologie recherche se fera sur un sujet contenant une **part significative de sécurité des systèmes émergeants** pour les élèves de la majeure.

Objectifs d'apprentissage

- Type de méthodologie : qualitative, quantitative, mixte
- Rédaction d'une méthodologie : approche, collecte de données, méthode d'analyse et justification des choix.

Compétences visées

A l'issue de ce module l'étudiant pourra mener et défendre un travail de recherche.

Module **Computional Modeling**		
Cours : 9h	TD : 18h	Travail personnel : 23h

De trop nombreux échecs nous ont appris ce qu'il en coûte de traiter simplement des questions complexes, c'est-à-dire de réduire à des modèles simplistes la foisonnante complexité de la vie, de la société, de la connaissance.

Dans ce module, plutôt que de simplifier la complexité en la mutilant, nous nous proposons de commencer par l'assumer en la modélisant.

Pour la partie pratique de ce module, les cas étudiés auront une **part significative de sécurité** envisagée sous l'angle de la complexité (surface d'attaque de l'IoT par exemple).

Objectifs d'apprentissage

- La modélisation : concevoir des modèles.
- Les logiques de la modélisation systémique.
- La modélisation projective de l'action complexe.
- L'organisation, propriété des systèmes complexes. La symbolisation des opérations complexes.
- Le processus de décision des systèmes complexes.

Compétences visées

Être capable de saisir une problématique systémique dans toute sa complexité, d'en offrir un modèle et à partir de celui-ci d'en extraire les décisions les plus adaptées.

Module **Applied Cryptography**		
Cours : 9h	TD : 18h	Travail personnel : 23h

L'objet de ce module est d'exposer les méthode et principes de base pour conserver un secret, et notamment la cryptographie. Il s'agit de montrer les différentes applications concrètes dans un système IT.

Objectifs d'apprentissage

- Le secret
- Stéganographie et tatouage
- Clé privée et publique, et échanges de clé.
- Algorithmes de cryptographie symétrique et asymétrique.
- Certificats, signature et non répudiation.
- Usages dans les protocoles (TLS/HTTPS, VPN, IPsec…)

Compétences visées

Être capable de saisir une problématique systémique dans toute sa complexité, d'en offrir un modèle et à partir de celui-ci d'en extraire les décisions les plus adaptées.

Module **NoSql**		
Cours : 9h	TD : 18h	Travail personnel : 23h

L'objectif de ce cours est de fournir une introduction aux méthodologies et aux outils pour les bases de données NOSQL.
Il traite également les questions de la sécurité des données et la gestion d'accès aux données.

Objectifs d'apprentissage

- Modéliser des collections d'objets NoSQL
- NoSQL orienté documents : Cassandra, MongoDB
- NoSQL orienté colonnes : Elasticsearch
- NoSQL orienté graphes : Neo4j

Compétences visées

Concevoir et utiliser des architectures NoSQL database.
Interroger un moteur de recherche avec Elasticsearch.
Visualiser des données avec Kibana.
Assurer l'intégrité des données dans une base NoSql.

Module **OS Hardening**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module traite du durcissement des systèmes d'exploitation.
Il s'agit de minimiser l'exposition d'un ordinateur aux menaces actuelles et futures en configurant entièrement le système d'exploitation et en supprimant les applications inutiles.

Objectifs d'apprentissage

- Evaluation des systèmes d'exploitation en termes de niveau de risque.
- Evaluations de vulnérabilité.
- Tests de pénétration pour identifier les failles.
- Détermination du niveau et de l'étendue du durcissement nécessaire pour sécuriser entièrement un système.
- Classification des meilleures pratiques par rapport à l'impact qu'elles auront sur les opérations.
- Implémenter les changements nécessaires.

Compétences visées

A l'issue de ce cours les étudiant sauront évaluer l'état d'un OS et décider ou non d'une campagne de durcissement, voir mener cette campagne eux-mêmes.

Module **Network Security**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module couvre l'ensemble des enjeux de la sécurité des réseaux.

Objectifs d'apprentissage

- Menaces et contremesures propres à chaque couche du modèle OSI
- Sécurité matérielle Firewall, NGFW, WAF, NAC et proxy
- IDS et IPS
- SSL et TLS
- SSH, VPN et IpSec
- Usage et Sécurité des SDWAN
- Outils de hack réseau

Compétences visées

A l'issue de ce module l'étudiant aura toutes les connaissances pour aborder les enjeux de sécurité dans les réseaux. Il sera à même d'identifier les failles les plus communes et de proposer des contre-mesures.

Module **Connectivity Security**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce cours donne tous les éléments nécessaires au choix d'une connectivité IoT (réseaux sans fils) au regard des enjeux de sécurité et des enjeux business.

Objectifs d'apprentissage

- Normes de connectivité
- Vulnérabilités et exploit connus dans les réseaux sans fils IoT.
- Very Short Range connectivity : NFC, RFID
- Short Range connectivity : Wifi, Bluetooth, Zigbee, Zwave
- Long Range Connectivity : Lorawan, LTE-M, NB IoT
- Cellular Connectivity : 4G, 5G
- Sécurité des passerelles (gateway) incluant la sécurité physique des équipements.

Compétences visées

A l'issue de ce module l'étudiant aura une connaissance des différents réseaux (courte protée, longue protée et cellulaire) en usage dans l'IoT. L'étudiant aura développé une expertise particulière sur la sécurité de ces réseaux.

Module **Containerization Technoplogies**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Docker est une plateforme ouverte pour le développement, le déploiement et l'exécution d'applications. Il permet d'embarquer et d'exécuter une application dans un environnement cloisonné appelé conteneur. Ce module présente cette technologie et les recommandations qui sont relatives à son usage selon l'ANSSI.

Objectifs d'apprentissage

- Docker, containérisation et déploiement de conteneurs
- Cloisonnement du conteneur
- Cloisonnement des ressources
- Restriction des privilèges
- Limitation des accès aux ressources
- Journalisation du conteneur

Compétences visées

Mettre en œuvre et déployer des containers Docker de façon sécurisée.

Module **Decentralization Technologies**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce cours introduit à la blockchain comme "élément de confiance" (par exemple pour la gestion de l'identité numérique, ou comme plateforme décentralisée dans l'IoT assurant une meilleure résilience, etc…) et explore ses développements en cours (NFT, WEB 3.0).

Objectifs d'apprentissage

- Définir la blockchain, expliquer la structure et les aspects opérationnels.
- Comparer les différents types de blockchains.
- Les éléments de confiance dans la blockchain et le protocole de consensus.
- La structure et les concepts de base d'un contrat intelligent.
- Écrire, compiler et déployer des smart contracts.
- Transmettre les informations capturées et stocker les données sur une blockchain privée.
- Introduction à Hyperledger de la Fondation Linux.
- Compréhension de l'infrastructure de blockchain Hyperledger Fabric.
- Définition des actifs, des participants, des transactions et des listes de contrôle d'accès à l'aide de Hyperledger Composer.
- Développement de la blockchain (web 3.0, NFT, etc…).

Compétences visées

Prendre en compte les architectures décentralisées comme **élément de confiance et de résilience** numérique dans l'élaboration de produit numériques.

Module **Explainability AI**		
Cours : 9h	TD : 18h	Travail personnel : 23h

L'intelligence artificielle a un énorme potentiel pour sécuriser le cybermonde. De nombreuses recherches sont menées dans le domaine de l'intelligence artificielle en matière de cybersécurité, mais leur adoption dans le monde réel est extrêmement limitée.
Le manque d'interprétabilité et de précision des modèles d'intelligence artificielle constitue une restriction à la mise en œuvre, car l'utilisateur doit être sûr que le système d'intelligence artificielle utilisé pour la prise de décision est fiable.

L'**Explainability AI** permet de surmonter cette difficulté et constitue une étape importante vers une intelligence artificielle fiable et prévisible. Elle est l'objet de ce module.

Objectifs d'apprentissage

- Équité et dévalorisation : Gérez et surveillez l'équité. Analyser le déploiement pour détecter les biais potentiels.
- Atténuation de la dérive du modèle : Analyser le modèle et faire des recommandations en fonction du résultat le plus logique. Alerter lorsque les modèles s'écartent des résultats escomptés.
- Gestion du risque de modèle : Quantifier et atténuer le risque lié au modèle. Être alerté lorsqu'un modèle ne fonctionne pas correctement. Comprendre ce qui s'est passé lorsque les écarts persistent.
- Automatisation du cycle de vie : Construire, exécuter et gérer des modèles dans le cadre de services intégrés de données et d'IA. Unifier les outils et les processus sur une plateforme pour surveiller les modèles et partager les résultats. Expliquer les dépendances des modèles d'apprentissage automatique.
- Le multi-cloud : Déployer des projets d'IA sur des clouds hybrides, notamment des clouds publics, des clouds privés et sur site. Favoriser la **confiance** avec l'IA explicable.

Compétences visées

Être capable d'évaluer une IA en fonction d'un cas d'usage définit et d'envisager une démarche d'explicabilité pour assurer les résultats et éviter les biais.

Semestre 3

Module **Projet pour l'Innovation Industrielle**		
		Travail personnel : 100h

Dans ce module les étudiants sont mis en équipe d'au moins 4 étudiants et sont mis en situation de prestation de service pour un « partenaire » (entreprise, laboratoire de recherche, association, etc…). C'est une mission de type « forfait » et non « régie », contrairement au stage, mais le principe reste très proche. Les partenaires suivent l'équipe par des réunions d'avancement. Le projet s'étale sur les semestres 1 et 2 et aboutis à un livrable et une évaluation sur le niveau de satisfaction du partenaire.

Ces projets doivent contenir **une part significative de sécurité** pour être validés pour les étudiants de la majeure.

Objectifs d'apprentissage

- Gestion de projet
- Compétences professionnelles en situation de service
- Autoformation (les sujets doivent idéalement explorer des aspects non abordés en cours)

Compétences visées

Toutes les compétences d'un ingénieur en prestation de service chez un client : communication, suivi des tâches, points d'avancement, planification, prise en compte et gestion des risques, réalisation des tests et des recettes, documentation, acquisition de nouvelles compétences techniques…

Module **Data Protection Management**		
Cours : 9h	TD : 18h	Travail personnel : 23h

La protection de la donnée est au cœur des enjeux du numérique. Il s'agit dans ce module d'en montrer tous les tenants et les aboutissants.
Ce module conduit à une certification RGPD.

Objectifs d'apprentissage

- Aspects juridiques nationaux et européens (RGPD et NIS2)
- Le modèle EU vs USA, état des échanges.
- Principes et outils de la protection des données.
- Protection des données et cybersécurité (CIA)
- Fonction de DPO

Compétences visées

Être capable d'évaluer le niveau de protection des données dans une entreprise et de mettre celui-ci à jour en fonction des normes et les lois.

Module **CyberResilience**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce module introduit à la démarche de cyber résilience. Il donne le cadre normatif et juridique, le périmètre et les enjeux de la cyber résilience.

Objectifs d'apprentissage

- Introduction, définition et vocabulaire
- La norme ISO 22301
- Le framework NIST,
- La continuité d'activité Business
- La continuité d'activité IT
- le business Impact Analysis (BIA)
- Le Plan de continuité d'Activité (PCA)
- Le Plan de Reprise d'Activité (PRA)
- Les architectures IT résilientes : On-Prem - Cloud
- les solutions de sauvegarde, le Recovery

Compétences visées

Être capable de mettre en œuvre une politique de cyber résilience.

Module **BI**		
Cours : 9h	TD : 18h	Travail personnel : 23h

La Business Intelligence (BI) est un processus technologique permettant d'analyser des données et de fournir des informations exploitables qui aident les cadres, les gestionnaires et les travailleurs à prendre des décisions commerciales éclairées.

Objectifs d'apprentissage

- Qu'est-ce que la business intelligence ?
- Comment fonctionne la BI ?
- Avantages de la BI
- Exemples de BI
- Comment créer une stratégie BI
- Catégories d'analyse BI
- Avantages et inconvénients de la BI
- Plateformes BI
- BI et big data
- Le rôle futur de la BI

Compétences visées

Être capable de mettre en œuvre une démarche de Business intelligence.

Module **Dataviz**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Le but de ce module est de proposer une approche complète de la visualisation de données.

Objectifs d'apprentissage

- Visualisation de données : une approche sémiologique
- Les outils de l'entreprise pour la visualisation de données
- Les frameworks web pour la visualisation

Compétences visées

Comprendre les enjeux de la visualisation de données pour l'entreprise.
Utiliser et adapter les outils de visualisation de l'entreprise.

Module **Governance Risk and Compliance**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module couvre l'ensemble des enjeux de la gouvernance, de la gestion du risque et de la conformité.

Ce module conduit à deux certifications (ISO27001 et ISO27005) en blended learning.

Objectifs d'apprentissage

- Connaissance des normes (ISO 27001, ISO27005)
- Mise en place d'un SMSI
- Ateliers pratiques d'analyse des risques (selon EBIOS RM)
- Méthodologie d'audit

Compétences visées

A l'issue de ce module l'étudiant aura toutes les connaissances pour aborder les tâches de consulting (suivant les normes ISO27001 et 27005, ou RM EBIOS) en gouvernance de la cybersécurité et/ou audit.

Module **Sémiologie et OSINT**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module aborde le social engineering et les aspects psychologiques qui lui donne assise (Biais Cognitifs, grille comportementale etc…). L'OSINT y est présenté comme un moyen de préparation au SE mais également comme un moyen de débusquer les fake et deep fake news.

Objectifs d'apprentissage

- Notions de Sémiologie
- Fake news, Deep Fake, et IA Génératives
- OSINT et Cadre juridique
- OSINT et renseignement

Compétences visées

Evaluer les risques liés à la désinformation pour une entreprise ou un état.
Avoir conscience de l'importance du facteur humain et de l'information en cybersécurité.

Module **HW security**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module fournis toutes les bases pour le hacking de matériel électronique et de système embarqué.

Objectifs d'apprentissage

- Sécurité matérielle
- Equipement de l'analyste et rétro-ingénierie de schéma électronique
- Ports de communication série, Protocoles de communication électroniques : Capture de communications SPI et I2C
- Extraction des micro-logiciels
- Debugger : Exploitation des bootloaders, Exploitation de mécanismes de mise-à-jour, Chip-off et dump
- Rétro-ingénierie de micro-logiciels : Système d'exploitation, Interruptions matérielles, Extraction de systèmes de fichiers, Désassemblage et analyse du code machine
- Recherche de vulnérabilités : Analyse de configuration, Mots de passe faibles et par défaut, Fonctionnalités cachées, Vulnérabilités système
- Backdooring : Mécanismes d'installation de porte dérobée, Compilation de portes dérobées pour architectures embarquées :
- ARM, MIPS, Persistance de la porte dérobée

Compétences visées

Être capable de mener les tests de pénétration minimaux sur de l'électronique analogique ou numérique.
Evaluer le niveau de sécurité d'un système électronique.

Module **Safety and Security**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce cours vise à souligner les spécificités du monde industriel (convergence IT/OT) en termes de cybersécurité, en relation avec la notion de sûreté.

Objectifs d'apprentissage

- De la sûreté de fonctionnement à la cybersécurité
- Cycles de vie IT/OT
- Cartographie des SI industriels
- Gestion des vulnérabilités
- Durcissement des architectures
- Détection des menaces
- Security by design
- Norme IEC 62443
- Spécificité GRC industrielle
- Gestion de crise IT/OT

Compétences visées

Être capable d'évaluer et de comprendre la spécificité des enjeux de cybersécurité dans l'industrie.
Ëtre capable de proposer des solutions adaptées aux besoin en cybersécurité de l'industrie.

Module **Psychology and Social Engineering**		
Cours : 12h	TD : 18h	Travail personnel : 20h

Ce module aborde le social engineering et les aspects psychologiques qui lui donne assise (Biais Cognitifs, grille comportementale etc…).

Objectifs d'apprentissage

- Biais cognitifs
- Comportements digitaux à risques
- Red Teaming et ciblage psychologique
- Social Engineering

Compétences visées

Evaluer les risques liés au facteur humain (social engineering) dans/pour une entreprise.
Avoir conscience de l'importance du facteur humain et de l'information en cybersécurité.

Module **Security Use case**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce module étudie différents cas d'usage en sécurité et cybersécurité.

Objectifs d'apprentissage

- Identifier les constantes dans les cas d'usage
- Etablir les règles de réponses à incidents et bonnes pratiques
- Notion de crise et de gestion de crise

Compétences visées

Comprendre de façon concrète les tenants et les aboutissants des enjeux de sécurité dans différents domaines et secteurs d'activité, en fonction de différents enjeux business.

Module **IT management/ITIL**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Ce cours permet à l'étudiant de comprendre l'utilisation des technologies de l'information dans le cadre de la stratégie d'entreprise.

Objectifs d'apprentissage

- ITIL et management IT
- BIA dans ITIL et risk management
- ITIL security Mangement

Compétences visées

Intégrer les stratégies de management informatiques et analyser leur impact stratégique.
Identifier les problèmes et les implications de la gestion informatique.
Comprendre comment l'informatique peut améliorer, voire transformer, le processus de gestion à travers l'accès à une meilleure information

Module **Veille et enjeux**		
Cours : 9h	TD : 18h	Travail personnel : 23h

Le but de ce cours est de proposer une initiation à la compréhension d'un article de recherche et de mener une veille technologique efficace.

Objectifs d'apprentissage

- Notion de traitement d'images
- Lecture et analyse d'article de recherche sur un thème donné.
  Ce thème contient une **part significative de sécurité** pour les étudiants de la majeure.

Compétences visées

Savoir analyser un article scientifique et mener une veille technologique.