



## **Programme détaillé de l'enseignement sur 3 ans**

## Groupe des activités pratiques indépendantes et/ou transverses

|     | Activité pratique permanente | # instances | Début | Prof | Dépendances | Groupe des activités pratiques indépendantes et/ou transverses  |
|-----|------------------------------|-------------|-------|------|-------------|---|
| ALT | Alternance                   | 6           | S5    |      |             | Représente la part de l'alternance en entreprise  |
| MQ  | Main Quest                   | 6           | S5    |      |             | La quête principal représente la séquence d'atelier, de projet en groupe structurant la formation   |
| SQ  | Side Quests                  | 5           | S6    |      |             | <p>Les quêtes secondaires représentent plusieurs choses au sein de la formation:</p> <ul style="list-style-type: none"> <li>- Projet individuel ou en groupe d'étudiant de la même ou de différente promos</li> <li>- Proposé par l'étudiant ou par l'école</li> <li>- Opportuniste ou planifier (hackathon, ctf, ...) tout au long de la formation</li> <li>- Technique ou non (associatif)</li> <li>- Crédit variable à évaluer en début de projet avec validation personnalisé (soutenance du travail effectué ou autre)</li> <li>- L'étudiant doit valider son quota de crédit de SQ en fin de formation, c'est à dire que d'un semestre sur l'autre le nombre de crédit en SQ validé peut varier.</li> </ul> |

## Groupe de cours non technique

| Code Cours  | Connaissance non technique                                  | #Instances | Début | Enseignant | Dépendances | Groupe de cours non technique  |
|-------------|---|------------|-------|------------|-------------|--|
| ANG         | Anglais   | 6          | S5    | DEE        |             | Programme possible :<br>- Cours de conversation et compréhension, technique et non technique<br>- Révision grammatical<br>- Préparation TOEIC  |
| SOFT SKILLS | Communication / Expression écrite / Développement personnel | 4          | S5    | IMP?       |             | Comme le package entreprise, module de cours orienté vers un résultat -> Développer les étudiants sur un plan personnel<br>- Communication écrite/orale en milieu professionnel<br>- Développement personnel, leadership<br>- Associatif<br>- Activité Culturel<br>Peut se dérouler à 50% comme des SQ   |
| RISQPCA     | Risque sécurité et plan de continuité                       | 2          | S9    |            |             | Analyse de risque en cybersécurité et étude de cas EBIOS, et plan de continuité d'activité<br>- Management des systèmes d'information et normalisation<br>- Problématique de la SII et analyse de risques<br>- Plans de Continuité d'Activité et plans de secours informatique<br>- Gestion Opérationnelle de la Sécurité : processus et outillage<br>- Système de Management de la sécurité du SI<br>- Anticipation et gestion des crises<br>- Média training |
| DC          | Droit Cybersécurité   | 1          | S7    |            |             | Programme en cours de définition :<br>- Législation spécifique aux risques cybers<br>- Pour le secteur privé et pour le secteur public<br>- Aspects réglementaires et juridiques pour la protection des données (RGPD, ...)<br>- Protection du patrimoine immatériel de l'entreprise   |

|         |                                  |   |    |             |  |  |
|---------|----------------------------------|---|----|-------------|--|--|
|         |                                  |   |    |             |  | - Droit d'internet et de l'information (hacking éthique<br><a href="https://www.silicon.fr/hacker-ethique-legislation-francaise-claire-160842.html">https://www.silicon.fr/hacker-ethique-legislation-francaise-claire-160842.html</a> )   |
| PACKENT | Package entreprise               | 2 | S5 | IMP?<br>AD? |  | Cours "package entreprise" contenant ce qu'il faut pour créer, gérer son entreprise et pour les salariés:<br>- Contrat, financement, Lean Canevas, BP<br>- Notion de droit généraliste<br>- Droit des affaires, du travail, droits d'auteur<br>- Compta, liasse fiscale, etc..   |
| METHOD  | Méthode de l'entreprise          | 1 | S5 |             |  | Programme possible :<br>- Méthode ITIL<br>- Démarche Qualité<br>- Fonctionnement interne managérial  |
| GEOCYB  | Géopolitique de la cybersécurité | 2 | S9 |             |  | Programme possible :<br>- Guerre de l'information, Intelligence et Veille économique<br>- Espionnage industriel<br>- Fuites d'informations<br>- Panorama géopolitique des cybermenaces<br>- Intelligence stratégique et contre-ingérence<br>- Les entreprises face aux risques numériques (APT)<br>- Enjeux de la veille sur le Dark Net et le Black-Market<br>- La cybercriminalité : une vision à 360 degrés<br>- Cybersécurité interne et compromission<br>- Des signaux faibles au renseignement<br>- Cybercriminalité, menaces et attaques<br>- (voir TVAEGE) |

**Groupe de cours ayant pour objectif d'offrir le socle technique minimal  
comme pré-requis à la sécurité informatique.**

| Code Cours | Fondement de l'informatique                            | #Instances | Début | Enseignant     | Dépendances | Groupe de cours qui a pour objectif d'offrir le socle technique minimal comme pré-requis à la sécurité infos.<br>Chaque matière doit inclure pour chaque notion abordé son volet sécu/hack d'un point de vue ludique...<br>Par contre seulement d'un point de vue introductif, le détail sera vue dans des cours spécifiques  |
|------------|--|------------|-------|----------------|-------------|---|
| FI_LOGIN   | Prise en main du système de l'école                    | 1          | S5    | LA<br>AM<br>MP |             | Apprendre à utiliser et comprendre les différents outils fournis par l'école.<br>LMS, Mail, Chat, Connexion, Shell unix et commande de base, Git, Moulinette, ...<br><br>Jeux sécu : escalade des droits via sudoers  |
| FI_MICRO   | Architecture, microprocesseurs                         | 1          | S5    | LA<br>AM<br>MP | FI_LOGIN    | Reprends le contenu de LA d'APPING et l'étends.<br>Principalement, présente l'architecture d'une machine (bus, périphérique) et du processeur en particulier.<br>Commence par les mécanismes de représentation de valeur (base numérique, hexa), nombre flottant, unicode...<br>Introduit les concepts d'ISA et du décodage d'instruction du processeur, notion de pipeline, notion d'ILP, Instruction scheduling (inorder/outoforder), modèle d'exécution et pile d'appel. |
| FI_ASM     | Fondamentaux Assembleur (Mise en pratique de FI_MICRO) | 1          | S5    | LA<br>AM<br>MP | FI_MICRO    | Cours d'assembleur classique visant les processeurs Intel.<br>Avec mise en pratique par l'implémentation de petit projet en ia32, x86_64<br>Voir aussi code 16 bit (comme dépendance au cours kernel, dépends si kernel 32 ou kernel 64,  |

|          |                             |   |    |                |                      |   |
|----------|-----------------------------|---|----|----------------|----------------------|---|
|          |                             |   |    |                |                      | <p>Mais aussi pour un modèle SANS protection mémoire</p> <p>Jeux sécu : jeu avec l'adresse de retour sur la pile, code auto-répliquant (16 bit)</p>   |
| FI_SEXP  | Système d'exploitation      | 2 | S5 | LA<br>AM<br>MP | FI_MICRO             | <p>Reprends le contenu de LA d'APPING et l'étends.</p> <p>Cad, présente a quel besoin fonctionnel répond un SEXP à travers un historique.</p> <p>Ensuite, présente les différentes concepts constitutifs d'un SEXP sur plusieurs cours.</p> <p>Architecture d'un SEXP, Métaphore de l'usine, Appels Systèmes, Userland/Kernel Land et mode d'exécution</p> <p>Sous-systèmes : Mémoire, Briques de synchronisation, VFS et Block, Net</p> <p>Pilote de périphérique (registre de périphérique, IO Port et MemIO, datasheet).</p> |
| FI_PROGC | Programmation C             | 1 | S5 | LA<br>AM<br>MP | FI_LOGIN<br>FI_MICRO | <p>Reprends le contenu de LA d'APPING et l'étends.</p> <p>Bref, Bootstrap de programmation en C (piscine), à travers plusieurs exos et mini-projets.</p>  |
| FI_ALGO  | Algo, structure de données. | 2 | S5 | LA             |                      | <p>Cours généraliste sur les algos classiques et les structures de données associées</p>  |
| FI_MATH  | Math pour l'informatique    | 1 | S6 |                |                      | <p>Cours généraliste des maths utiles pour l'informatique :</p> <ul style="list-style-type: none"> <li>- Polynome, AL</li> <li>- Analyse</li> <li>- Notion de complexité</li> <li>- Analyse</li> </ul> <p>Basé sur des projets petits projets mettant l'emphasis sur les notions abordés par la pratique</p>  |

|          |                         |   |    |                       |                      |   |
|----------|-------------------------|---|----|-----------------------|----------------------|---|
| FI_GP    | Gestion de projet       | 1 | S5 | FB?                   |                      | Essentiel pour mener un projet informatique<br>- Cycle d'un projet et Méthodes<br>- Qualité logiciel<br>- Travail en groupe<br>- Planning<br>Utilisable directement et pratiquement lors des premiers projets en binomat ou groupe  |
| FI_NET   | Fondement d'internet    | 1 | S5 | LA<br>AM<br>MP<br>FB? | FI_SEXP<br>FI_PROGP  | Essentiel du réseau avec un très gros FOCUS sur internet (autres réseaux vue dans cours spécifique)<br>- WIFI, ETH, ARP, IP, IP6, ICMP, TCP, UDP, SMTP, etc..<br>- HTTP (serveur web et site web)<br>- réseau local, global (OSPF, BGP), Routage, DNS,...<br><br>Jeux sécu : HTTP et Mail via nc, scapy en python |
| FI_PROGP | Python pour la sécurité | 1 | S5 | LA<br>AM<br>MP        | FI_LOGIN<br>FI_MICRO | Reprends le contenu de LA d'APPING et l'étends<br>Cours de programmation python préparant à son usage pour la sécurité info.<br>- python basique<br>- python avancé<br>- module standard et avancé<br><br>Jeux sécu: keylogger, parseur PE/ELF  |
| FI_BDD   | Bases de données        | 1 | S5 | LA<br>AM<br>MP        | FI_LOGIN             | Cours généraliste sur les bases de données<br>- utilités, notion de data et notion de dépendance fonctionnel<br>- SQL et NOSQL<br><br>Jeux sécu : SQL injection   |

### Groupe de cours spécifique à l'admin-sys et au devops

| Code Cours | Admin Sys et Réseaux | #Instances | Début | Enseignant            | Dépendances       | Groupe de cours spécifique à l'admin-sys et au devops  |
|------------|----------------------|------------|-------|-----------------------|-------------------|--|
| ASR_BASE   | Admin Sys et Réseaux | 1          | S6    | LA<br>AM<br>MP<br>FB? | FI_NET<br>FI_SEXP | Suis le cours de Système d'exploitation mais d'un point de vue ADMIN avec plus de mise en<br>Pratique :<br>- Account, Authorization, Authentication => Gestion de l'identité<br>- Services<br>- Tache<br>- Montage de compte d'entreprise et administration (VLAN/VPN IPsec, architecture MPLS)<br>- Use Case d'intervention temporaire (nouveau prestataire, syndication)<br>- Appliance sécu<br>Continue à poser les concepts et comparaison Win/Linux |
| ASR_WIN    | Windows              | 2          | S7    | LA<br>AM<br>MP<br>XC? | ASR_BASE          | Atelier spécifique windows, programmation powershell et automatisation des taches, Active Directory  |
| ASR_LIN    | Linux                | 2          | S7    | LA<br>AM<br>MP<br>XC? | ASR_BASE          | Atelier spécifique linux, scripting et automatisation des taches, LDAP/Kerberos  |
| ASR_CLOUD  | Cloud computing      | 1          | S8    | FB?                   | ASR_BASE          | Cours et Atelier sur le cloud computing et les infrastructures 2.0 (IaC)<br>Concepts et mise en place  |



### Groupe de cours spécifique à la sécurité info/cyberdéfense

| Code Cours | Sécurité Informatique                      | #Instances | Début | Enseignant            | Dépendances                                | Groupe de cours spécifique à la sécurité info/cyberdéfense   |
|------------|--|------------|-------|-----------------------|--|--|
| SEC_OFF    | Sécurité offensive                         | 1          | S6    | LA<br>AM<br>MP<br>XC? | ASR_BASE<br>FI_PROGC<br>FI_PROGP<br>FI_ASM | Cours généraliste qui introduira les sous-catégories suivantes:<br>Fingerprinting/identification/Osint (identifier le SI)<br>Reverse Engineering (trouver les failles)<br>Sécurité applicative (exploiter les failles)<br>Test d'intrusion (réseaux, WEB)<br>Malware (virologie, ...)              |
| SEC_DEF    | Sécurité défensive                         | 1          | S6    | LA<br>AM<br>MP<br>XC? | ASR_WIN<br>ASR_LIN                         | Cours généraliste qui introduira les sous-catégories suivantes:<br>Développement sécurisé (ou programmation défensive)<br>Audit et sécurisation des Systèmes réseaux<br>Réponse à des appels d'offres d'architecture sécurisée<br>Analyse de Threat Model<br>Sonde automatique et analyse de log   |
| SEC_INGSOC | Ingénierie Sociale                         | 2          | S7    | AH                    |  | Connaissance des comportements humains : biais cognitif, confiance, défiance de l'autorité, ...<br>Vu à travers les grandes expériences sociales, les techniques en cours...<br>Jeu de rôle, impersonation   |
| SEC_REASM  | Reverse engineering et assembleur exotique | 2          | S7    |                       | SEC_OFF                                    | Cours/Projets plus spécialisé que ce qui sera vu en SEC_OFF,<br>Intermediate Language,<br>IDA, Hydra, SAT Solver, decompiler<br>Etude d'autres ISA et architecture que intel: ARM, RISC, Motorola... (voir acteur du marché)<br>faire émerger des projets système/séc sur du matériel non-standard |

|          |   |   |    |     |                    |  |
|----------|---|---|----|-----|--------------------|--|
| SEC_ATK  | Sécurité applicative et technique d'attaque | 2 | S7 |     | SEC_OFF            | Fingerprinting, CVE, Poutrage (BO, ROP, Fuzzing), ... Réalisation de shellcodes  |
| SEC_NET  | Sécurité des réseaux                        | 1 | S9 | FB? | SEC_OFF            | MITM en LAN, sécurité switch/routeur, WIFI, analyse de paquet et rejeu (wireshark, scapy, nmap), ..., autres protocoles (réseau TCOM)<br>Surveillance de grand réseaux (Deep Packet Inspection), Veille, OSINT                   |
| SEC_WEB  | Sécurité web                                | 1 | S8 |     | SEC_OFF            | fiddler, selenium, sécurité d'API, d'encodage front, injections (détournement de javascript, sql, unicode)... E-payment et commerce électronique<br>OWASP  |
| SEC_FOR  | Forensic                                    | 2 | S8 | AM  | SEC_OFF<br>SEC_DEF | Analyse à froid et recherche de trace  |
| SEC_PROG | Programmation défensive                     | 2 | S8 |     | SEC_DEF            | Réduire le spectre d'attaque:<br>- utilisant les bonnes pratiques sur les langages critiques (C)<br>- utiliser les bons langages<br>- utiliser les outils d'analyse statique du code et notion de preuve (mise en pratique)      |
| SEC_ADM  | Administration défensive                    | 2 | S9 |     | SEC_DEF            | Administration moderne de bout en bout sécurisé<br>- firewall<br>- sécurisation wifi<br>- voip<br>- VPN<br>- Pax, Grsec, ...<br>- Honey-Pots<br>- CERT (Computer Emergency Response Team)<br>- SOC ( Security Operations center) |

|           |                            |   |     |     |                    |  |
|-----------|----------------------------|---|-----|-----|--------------------|--|
| SEC_MAL   | Virologie et Malware       | 2 | S9  | AM  | SEC_OFF            | Cours/Projets plus spécialisé que ce qui sera vue en SEC_OFF sur l'étude et l'écriture de code malveillant (vers, virus, trojans, rootkits, malwares),<br>Vecteur de contagion/réplication, code polymorphe, code polyglotte, ...  |
| SEC_INDUS | Cybersécurité industrielle | 1 | S10 |     | SEC_OFF<br>SEC_DEF | Etat de l'art des principaux standards et systèmes industriels.<br>Système de contrôle et d'acquisition de données (SCADA), leurs architectures et leurs vulnérabilités.<br>Protection des locaux et des infrastructures sensibles |
| SEC_BCH   | Blockchain                 | 1 | S10 |     | CRYPTO<br>SEC_PROG | Possible cours sur les blockchains et les smart-contracts et notamment les problématiques de sécurité lié.   |
| SEC_IOT   | Internet Of Thing          | 1 | S10 | FB? | SEC_ASM            | Cours sur les problèmes liées à l'internet des objets  |
| SEC_MOB   | Mobile                     | 1 | S10 |     | SEC_ASM            | Android/Ios, software et système, sécurité des paquets et plateformes.<br>Réseaux opérateurs (WiMax, 3G, 4G, 5G...)  |
| SEC_ID    | Gestion des identités      | 1 | S7  |     |                    | Sécurité de la gestion de l'identité:<br>- interconnexion de tous les protocoles<br>- token physique, biométrie<br>- pb de délégation dans N SI  |

### Groupe de cours scientifique et théorique

| Code Cours | Science dans la sécurité              | #Instances | Début    | Enseignant | Dépendances | Groupe de cours le plus scientifique et théorique  |
|------------|---------------------------------------|------------|----------|------------|-------------|--|
| STAT       | Probabilité et statistique            | 2          | S7       |            | FI_MATH     | Cours de math spécialisé sur les proba et les stats qui sont le fondement de la Data science et du machine learning  |
| CRYPTO     | Cryptologie appliquée                 | 4          | S7       |            | FI_MATH     | Cours de Crypto orienté sur : <ul style="list-style-type: none"> <li>- les enjeux globaux</li> <li>- les principaux algos</li> <li>- les failles et la cryptanalyse possible en CTF vs dans la vraie vie</li> <li>- Cryptographie symétrique et asymétrique (et principaux algos)</li> <li>- Signature numérique, authentification, identification</li> <li>- Infrastructure à clé publique (PKI)</li> <li>- Infrastructure décentralisée, consensus et blockchain</li> <li>- Fonctions de hashage et MAC</li> <li>- Protocoles d'échange de clés et d'échange de clés de groupe</li> <li>- Biométrie</li> <li>- Sécurité des mots de passe (UNIX/Windows) : faiblesses, cassages et contre-mesures</li> <li>- OpenSSL, OpenSSH, Polar SSL, PGP/GPG</li> <li>- Les cartes à puces : théorie et pratique</li> </ul> |
| DAML       | Data Science et Machine learning      | 2          | S9       |            | STAT        | Analyse de donnée Massive (Big data), algo et technologie<br>Classification, Régresseur, RN, Algo Gen  |
| COMP       | Compilation, automate logique, preuve | 3          | S5,S7,S8 | LA         | FI_*        | Etude des algos de compilation, du fonctionnement des compilateurs, du typage, et des mécanismes d'analyse statique en vue de détection/correction de faille   |

