Parcours sécurité 5A

Compétences sécurité, liste de CyberEdu	Nb heures cours	Nb heures pratique	Niveau Entrée	Niveau Sortie
Fondamentaux	54	60	2	3
Électronique et architectures matérielles	0	0	2	2
Systèmes d'exploitation	0	20	2	2
Réseaux et protocoles	36	60	2	3
Cryptologie	14	30	2	3
Stéganographie et tatouage	4	20	1	2
Bases de données	3	20	2	2
Aspects systèmes et systèmes de systèmes	1	5	0	1
Normes, certifications, guides (organisationnel)	8	10	0	2
Certifications et évaluations de produits	1	0	0	1
Politique de cybersécurité et SMSI	2	5	0	1
Droit et réglementation	18	10	1	2
Développement logiciel et ingénierie logicielle	16	80	2	3
Gestion de projet	1	10	1	1
Cyberdéfense	4	10	0	2
Analyse post-mortem (Forensics)	18	30	0	2
Systèmes spécifiques, informatique industrielle	1	5	0	1
Aspects sociaux et sociétaux	6	30	1	2
Tests d'intrusion	6	20	0	2
Sécurité physique	18	10	0	2
Problématique SSI en contexte spécifique	1	0	0	1
Compétences sécurité en dehors de la liste de CyberEdu	Nb heures cours	Nb heures pratique	Niveau Entrée	Niveau Sortie
Rétro-ingénierie	4	10	0	1
Aspects économique de la sécurité	1	0	0	1
Compétences Sécurité autres	Nb heures cours	Nb heures pratique	Niveau Entrée	Niveau Sortie
Audit et contrôle (sécurité réseaux Locaux)	18	40	0	3

Les volumes horaires de la 2A à la 4A (justifiant le niveau d'entrée pour le parcours sécurité en 5A) sont donnés dans le tableau ci-dessous (format heures de cours/heures de pratique)

Compétences sécurité, liste de CyberEdu	Commentaires éventuels
Fondamentaux	Inclut les cours de théorie de l'information (appliquée à la sécurité, codes correcteurs d'erreur appliques a la sécurité), modèles mathématiques de la sécurité. Volume horaire de 2A à 4A : 36h/30h
Électronique et architectures matérielles	Mutualisé avec le bloc Electronique – Physique (1A a 4A) pas de cours en 5A. Volume horaire de 2A à 4A : 8h/10h
Systèmes d'exploitation	Linux – Windows (client et serveur) – Environnements mobiles (Android et iOS), microcontrôleurs (1A a 4A). Intervient en 5A sous forme de pratique en application des autres cours de

	sécurité. Volume horaire de 2A à 4A : 110h/40h
Réseaux et protocoles	Domaine transverse à la plupart des projets. Gros volume de TP. Volume horaire de 2A à 4A : 20h/10h
Cryptologie	Un gros cours de 40 heures avec TP en 2A. En 5A, pour la partie pratique, l'effort est mis sur l'implémentation efficace d'algorithmes et de protocoles (langage C), la programmation avec GMP (cryptographie asymétrique) et l'implémentation de cryptanalyses en conditions réelles (système de chiffrement par flot, à chiffré seul, détection et exploitation de clefs faibles, cryptanalyse appliquée par malware…). Volume horaire de 2A à 4A : 20h/20h
Stéganographie et tatouage	Bases théorique et implémentation d'un algorithme de sténographie usuel et de sa stéganalyse. Applications opérationnelles. Volume horaire de 2A à 4A : 4h/4h
Bases de données	Les aspects fondamentaux sont vus en 3A et 4A. En 5A, sécurisation des bases de données (SQL injection), utilisation des bases de données dans le domaine de la sécurité (en particulier utilisation de bases noSQL dans les problématiques de big data appliqué au renseignement). Volume horaire de 2A à 4A : 47h/10h
Aspects systèmes et systèmes de systèmes	Intervient essentiellement de manière transverse dans les projets et TP. Introduit lors des cours de mineures techniques
Normes, certifications, guides (organisationnel)	Cours *Risk analysis and security assessment*.
Certifications et évaluations de produits	Essentiellement dispositif CSPN
Politique de cybersécurité et SMSI	Introduit dans le cours Droit et Ethique (chaine fonctionnelle SSI française et organisation de la SSI en France). TP : analyse de documents légaux
Droit et réglementation	Ces aspects sont spécifiquement traites dans le cours Ethique et règlementation (IGI 900, IGI 910, IGI 920, IM 1300, SPC et II 300, IGI 901, Recommandation 600, CNIL, LPM, LR, CP Art.323, NIS, Wassenaar, CoCOM/ITAR…). De plus, lors de chaque enseignement technique, le point de droit affèrent est traité pour remettre les choses dans leur perspective légale. TP : analyse d'un texte de loi avec rapport critique commenté. Volume horaire de 2A à 4A : sensibilisation lors de la signature de la charte informatique et formation à l'esprit de défense par le réfèrent de défense et le CIRFA local, volume 2 heures
Développement logiciel et ingénierie logicielle	C, Java essentiellement + langages divers selon besoin. Les étudiants reçoivent une formation lourde en programmation de la 1A à la 4A (Volume horaire de 2A à 4A : 292h/200h). EN 5A, l'accent est mis sur la programmation sécurisée, l'analyse des vulnérabilités, l'analyse de code (statique et dynamique). Plusieurs projets (TP et surtout temps masqué) nécessitent l'implémentation systématique des principaux concepts et techniques vus en cours. Sur les 485 heures de TP et projets, le pourcentage impliquant du développement logiciel est *a minima* de 60 % (soit à peu près 300 heures). Les 80 heures de 5A mentionnes comme tels concernent des aspects implémentations

	spécifiques et dédiées (librairies crypto, réseau, programmation sécurisée…)
Gestion de projet	En 5A, l'effort porte sur la partie sécurité d'un projet (spécifications, conduite et sécurisation du projet, audit final des aspects sécurité du projet). Systématiquement évalué dans les TP et projets. Volume horaire de 2A à 4A : 9h/10h
Cyberdéfense	Transverse aux cours de mineures (et quelques heures en majeure)
Analyse post-mortem (Forensic)	Aspects légaux – Analyse statique et dynamique (mémoire). Analyse de malware
Systèmes spécifiques, informatique industrielle	Essentiellement objets connectés en liaison avec les cours réseaux. Problématique de la couche radio en entreprise.
Aspects sociaux et sociétaux	Aspects attaque : phishing, ingénierie sociale, exploitation des failles humaines, analyse informationnelle. Traité en particulier dans le cours OSINT Aspects défense : cartographie de la menace mondiale (acteurs, états, types de menaces), aspects citoyens et vie privée Volume horaire de 2A à 4A (sensibilisation) : 2h/0h
Tests d'intrusion	Présentation générale de la problématique (nature, aspects légaux, risques de mise en œuvre en entreprises, présentation des principaux outils). Traité essentiellement sous forme de TP et projets de manière transverse.
Sécurité physique	Cours optionnel en 2016. Obligatoire à partir de 2017. Analyse des contrôle d'accès (serrures physique et électroniques, coffres, systèmes alarmes…). Problématique du piégeage physique des systèmes d'information
Problématique SSI en contexte spécifique	Aspects légaux (zone de droit, contrat de service) et choix des prestataires de confiance uniquement
Compétences sécurité en dehors de la liste de CyberEdu	Commentaires éventuels
Rétro-ingénierie	Initiation en 2016. Un cours obligatoire de 18 heures est prévu à partir de 2017 (recrutement en thèse d'un spécialiste)
Aspects économique de la sécurité	Aspects sinistralité essentiellement
Compétences Sécurité autres	Commentaires éventuels
Audit et contrôle (sécurité réseaux Locaux)	Pratique et exercices directs avec entreprises volontaires. Audits réels d'entreprises. Les étudiants faisant leur stage dans ce domaine au laboratoire sortent réellement avec un niveau 4