Bloc de compétences	Année	Code ECTS	Module	Durée totale	Durée Théorie	Durée Pratique	Crédits ECTS	Objectif de la formation
Identifier les besoins en cybersécurité de l'entreprise et y répondre en analysant le risque cyber et en mettant en place une politique et une organisation adaptées.	4	4JURI	Juridique	18	16	2	2	Prendre en compte l'environnement juridique de la cyberdéfense
	4	4RISK	SMSI Analyse de risque EBIOS RM	35	20	15	4	Savoir appréhender la cybersécurité à travers les normes de management de la sécurité informatique et en s'appuyant sur des analyses de risque méthodiques.
	4	4GEOD	Enjeux, géopolitique Défense	21	16	5	2	Présenter les grands enjeux de la cyberdéfense
	4	4ECOI	Intelligence éconimique	21	14	7	2	Comprendre les enjeux d'intelligence économique en général et dans le monde numérique en particulier.
	5	5BECO	Intelligence éconimique	42	21	21	6	Progresser dans la comprehension des enjeux d'intelligence économique. Adopter un savoir-être adapté à chaque situation.
	4	4NDUS	Systèmes industriel et IOT	14	7	7	2	Connaître les spécificités de la sécurisation des systèmes d'information industriels et de l'Internet des objets
Prendre en compte la cybersécurité dans la conception et le déploiement d'un système d'information, au sein d'une équipe de développement, en appliquant les méthodes avancées de gestion de projet, de conception d'architectures sécurisées et en faisant appel au développement sécurisé.	4	4CRYP	Cryptologie	56	37	19	6	Donner à des futurs professionnels de la cybersécurité les bases nécessaires pour pouvoir utiliser de manière pertinente et en connaissance de cause les outils du chiffre.
	5	5CRYP	Cryptologie	28	7	21	5	Continuer la mise en pratique du module 4CRYP
	4	4ARCH	Architecture SSI	28	14	14	4	Comprendre les principes d'architecture SSI et les mettre en pratique.
	4	4OSEC	Sécurité système d'exploitation	63	28	35	6	Comprendre les vulnérabilités potentielles d'un système d'exploitation ainsi que les bonnes pratiques et les méthodes pour y faire face.
	4	4NETW	Sécurité réseau	63	28	35	6	Connaître les principaux risques cyber liés aux réseaux et savoir comment les traiter pour les supprimer ou les diminuer.
	4	4MATS	Matériel sécu (dont qualifications et agréments ANSSI)	7	7	0	1	Connaître les différents qualification, labellisations, agréments de produits et de service
	4	4DVSO	DEVSECOPS	28	21	7	2	Comprendre les enjeux sécurité du DEVOPS et des technos cloud et container
	4	4CONX	Connectivité (câble, sat, 5G, etc.)	7	7	0	1	Connaître les enjeux de cybersécurité lié aux infrastructures de connectivité
Estimer le niveau de sécurité d'un système d'information au sein d'une entreprise en effectuant des audits organisationnels et techniques et en assurant une veille technologique adaptée.	5	5IAAT	IA pour Attaque	21	7	14	2	Connaître les usage de l'IA dans le cadre de l'attaque
	5	5IAIA	IA contre IA	21	7	14	2	Acquérir une connaissance approfondie des vulnérabilités spécifiques aux systèmes d'IA. Acquérir une connaissance approfondie des vulnérabilités spécifiques aux systèmes d'IA. Comprendre comment une IA est adaptée pour attaquée une IA
	4	4TECH	Audit technique	84	21	63	6	Etre capable d'intégrer une équipe en charge de l'audit technique d'un système d'information.
	5	5TECH	Audit technique	81	10	71	6	Pratiquer les tests de pénétration
	4	4LNGS	Langage sécurisé, audit code source	21	7	14	2	Comprendre le risque cyber lié à la programmation et les normes et les méthodes pour maîtriser ce risque.
	4	4PROJ	Projet de développement d'une attaque sur un sujet donné	39	8	31	4	Prendre conscience des vulnérabilités d'un réseau en étant capable de l'attaquer
Gérer la sécurité d'un système d'information au sein de l'entreprise en utilisant les outils de supervision de la cybersécurité les mieux adaptés et en organisant une réponse adaptée en cas de crise.	4	4IATH	IA théorie	21	21	0	2	Posséder les bases en IA permettant d'aborder les modules IA suivants (4IADF, 5IAAT et 5IAIA)
	4	4IADF	IA pour défense	21	7	14	2	Connaître les usage de l'IA dans le cadre de la défense
	4	4CRIS	Gestion de crise	21	10	11	2	Appréhender la gestion de crise cyber avec méthode
	5	5CRIS	Gestion de crise	35	0	35	4	Mise en pratique des notions abordés dans le module 4CRIS
	5	5RECO	PCA PRA (commun IT)	42	28	14	4	Savoir établir un plan de continuité ou de reprise d'activité
	5	5SECU	Stormshield	48	13	35	4	Installer et gérer la solution Stormshield Endpoint Security (SES) Déployer des agents SES dans un pool de postes de travail et de serveurs nécessitant une protection Mettre en place une politique de protection Analyser une cyberattaque Configurer une politique de contrôle des appareils et du réseau Mettre en place une politique de configuration
	4	4SOC1	Security Operational Center	14	7	7	2	Comprendre l'organisation d'un SOC et connaître ses principaux outils
	5	5CERT	CERT	28	20	8	3	Comprendre la mission et l'organisation d'un centre de réponse à incident cyber
	5	5GMCS	Gestion du MCS	14	7	7	2	Assurer le maintien en condition de sécurité du SI de l'organisation en ayant conscience et en maîtrisant les risques sur la qualité de service.
	4	4FSIC	Forensic	35	10	25	2	Maîtriser les bases de l'analyse FORENSIC
	5	5SOC2	Security Operational Center	24	4	20	3	Donner une approche pratique du SOC
SOFT SKILLS	5	5MAST	Mémoire	21	7	14	15	
	4	4ENGL	Anglais	0	0	0	2	Être capable de soutenir une conversation professionnelle en langue anglaise.
	5	5ENGL	Anglais	0	0	0	2	Être capable de soutenir une conversation professionnelle en langue anglaise.
	4	4SPRT	Sport	32	0	32	2	Pas d'objectif ou de contenu pédagogique Cours relatif au bien-être de l'étudiant
	5	5SPRT	Sport	32	0	32	2	Pas d'objectif ou de contenu pédagogique Cours relatif au bien-être de l'étudiant
	4	4INTE	Stage pro	0	0	0	6	
	5	5XPRO	Stage pro	0	0	0	10	
			TOTAL	**1086**	**437**	**649**	**140**	