Niveau :	MASTER					**année**
Domaine :	Sciences Technologies Santé					**M2**
Mention :	Informatique					
Parcours :	Cybersécurité					120 ECTS
Volume horaire étudiant :	90 h	148 h	167 h	h	h	**405 h**
	cours magistraux	travaux dirigés	travaux pratiques	cours intégrés	stage ou projet	total
Formation dispensée en :	☒ français		☐ anglais			

Contacts :

Responsable de formation	Scolarité – secrétariat pédagogique
Wahabou ABDOU Maître de conférences ☎ 03.80.39.36.05 wahabou.abdou@u-bourgogne.fr	Christine CASTELLA Responsable scolarité ☎ 03.80.39.60.09 christine.castella@u-bourgogne.fr
Composante(s) de rattachement : UFR sciences et techniques	

Objectifs de la formation et débouchés :

■ Objectifs :

Ce master vise à former des informaticiens ayant des compétences en :

- conception et mise en œuvre de politiques de sécurité des systèmes informatiques
- réalisation des audits de sécurité des systèmes d'information
- sécurisation des technologies émergentes
- sécurisation des données, des infrastructures et des échanges réseaux
- intégration de solutions de sécurité dans le contexte des données distribuées et/ou massives

■ Débouchés du diplôme (métiers ou poursuite d'études) :

- Responsable de la sécurité des systèmes informatiques
- Chef de projets en sécurité informatique
- Responsable du SOC
- Opérateur analyste SOC
- Gestionnaire de crise de cybersécurité
- Analyste de la menace cybersécurité
- Analyste réponse aux incidents de sécurité
- Risk manager
- Auditeur en sécurité des SI
- Administration des systèmes d'information
- Poursuite d'études en doctorat

■ Compétences acquises à l'issue de la formation :

1. Aptitude à mobiliser les ressources d'un champ scientifique et technique liées à une spécialité.
2. Mettre en place les procédures d'exploitation, d'utilisation et de sécurité des équipements informatiques
3. Maîtrise de la gestion et de l'administration des réseaux informatiques, de la sécurité des réseaux,
4. Connaissance des techniques de développement web et mobile, de l'intelligence artificielle, de la virtualisation et du cloud computing.
5. Pilotage de projets
6. Analyse des performances d'un système d'information
7. Conception de l'architecture d'un système d'information
8. Mise en œuvre d'une politique de gestion des risques des systèmes d'information
9. Conception et développement de programmes et applications informatiques
10. Esprit d'entreprise et aptitude à prendre en compte les enjeux économiques, le respect de la qualité, la compétitivité et la productivité, les exigences commerciales, l'intelligence économique.

Modalités d'accès à l'année de formation :

■ de plein droit :

Après validation du Master 1 de ce parcours.

■ sur sélection :

Les candidats sont sélectionnés sur examen de dossier (éventuellement complété par un entretien) pour les candidats titulaires d'un Master 1 en informatique, en télécommunications et réseaux, ou un autre diplôme ou niveau d'études équivalent.

La sélection est réalisée par une commission présidée par le Responsable de la formation et composée d'un ou plusieurs membres de l'équipe pédagogique.

■ par validation d'acquis ou équivalence de diplôme

- en formation initiale : s'adresser à la scolarité organisatrice de la formation
- en formation continue : s'adresser au service de formation continue de l'université (03.80.39.51.80)

Organisation et descriptif des études :

■ Schéma général des parcours possibles

■ tableau de répartition des enseignements et des contrôles de connaissances assortis

SEMESTRE 3

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Protocoles de sécurité et gestion des intrusions	Protocoles de sécurité des réseaux	8	8	14	30	4	Théorique/TP	Théorique ou projet	2,5	1,5	4
	Architecture et sécurité des réseaux sans fil	8	6	6	20	3	Théorique/TP	Théorique ou projet	2	1	3
	Gestion des intrusions et Pentesting	8	6	16	30	4	Théorique/TP	Théorique ou projet	2,5	1,5	4
TOTAL UE		24	20	36	80	11			7	4	11

(1) CC : contrôle continu - CT : contrôle terminal

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Analyse des procédures et normes de sécurité	Audit de sécurité	10	10	10	30	4	Théorique/TP	Théorique ou projet	2,5	1,5	4
	Normes internationales de la sécurité	10	10	-	20	3	Théorique/TP	Théorique ou projet	2	1	3
TOTAL UE		20	20	10	50	7			4,5	2,5	7

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Investigation numérique et intelligence artificielle	Analyse forensique	8	6	14	28	3	Théorique/TP	Théorique ou projet	2	1	3
	Rétro-ingénierie	8	6	12	26	3	Théorique/TP	Théorique ou projet	2	1	3
	Intelligence artificielle	8	6	12	26	3	Théorique/TP	Théorique ou projet	2	1	3
TOTAL UE		24	18	38	80	9			6	3	9

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Entreprise 3	Séjour en entreprise 3	-	-	-	-	3	Pratique	Projet	3	-	3
TOTAL UE		-	-	-	-	3			3	-	3

TOTAL S3	**68**	**58**	**84**	**210**	**30**			**20,5**	**9,5**	**30**

SEMESTRE 4

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Sécurité et disponibilité des ressources	Sécurité des bases des données	8	8	14	30	4	Théorique/TP	Théorique ou projet	2,5	1,5	4
	Systèmes de haute disponibilité	8	6	10	24	4	Théorique/TP	Théorique ou projet	2,5	1,5	4
TOTAL UE		16	14	24	54	8			5	3	8

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Cyberdéfense et hacking	Cyberdéfense	6	6	8	20	3	Théorique/TP	Théorique ou projet	2	1	3
	Ethical hacking	-	-	51	51	7	Pratique	Projet	7	-	7
TOTAL UE		6	6	59	71	10			9	1	10

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Management humain, économique et social / langue	Droit du travail et droit informatique	-	30	-	30	3	Théorique/TP	Théorique ou projet	2	1	3
	Intelligence économique et aspects juridique de la cybersécurité	-	20	-	20	3	Théorique/TP	Théorique ou projet	2	1	3
	Anglais	-	20	-	20	3	Théorique/TP	Théorique ou projet	2	1	3
TOTAL UE		-	70	-	70	9			6	3	9

UE	Discipline	CM	TD	TP	Total	ECTS	Type éval (1) Session 1	Type éval (1) Session 2	Coeff CT	Coeff CC	Total coeff
Entreprise 4	Séjour en entreprise 4	-	-	-	-	3	-	Projet	3	-	3
TOTAL UE		-	-	-	-	3			3	-	3

TOTAL S4	**22**	**90**	**83**	**195**	**30**			**23**	**7**	**30**

■ Modalités de contrôle des connaissances :

Les règles applicables aux études LMD sont précisées dans le Référentiel commun des études mis en ligne sur le site internet de l'Université

http://www.u-bourgogne-formation.fr/IMG/pdf/referentiel_etudes_lmd.pdf

● *Sessions d'examen*

1ère session

Une session d'examens est organisée à la fin de chaque semestre. Toutes les épreuves (contrôle continu, examen) sont obligatoires. Toute absence à une épreuve doit être justifiée ; en cas d'absence injustifiée, le candidat sera déclaré défaillant à l'épreuve et donc à la session concernée. A chaque élément constitutif d'UE est attribuée une note sur 20 qui est la moyenne pondérée des notes obtenues à l'écrit et au contrôle continu.

Les séjours en entreprise font l'objet d'une évaluation par l'encadrant en entreprise (ou laboratoire) et/ou l'enseignant référent chargé du suivi de l'étudiant durant son alternance.

La validation de l'année est subordonnée à l'obtention de la moyenne générale compensatoire calculée à partir des notes de toutes les UE, y compris les séjours en entreprise.

2ème session

La deuxième session se déroulera sous forme d'épreuves écrites, orales ou de projets selon les UE. Elle portera sur l'ensemble des UE suivies par l'étudiant non validées en première session. La note d'examen de deuxième session remplace la note d'examen de la première session, la note de contrôle continu, le cas échéant, étant conservée. Pour les UE de séjour en entreprise ainsi que le module *Ethical hacking*, la note de deuxième session remplace la note de la première session.

● *Règles de validation et de capitalisation :*

Principes généraux :

COMPENSATION : Une compensation s'effectue au niveau de chaque semestre. La note semestrielle est calculée à partir de la moyenne des notes des unités d'enseignements du semestre affectées des coefficients. Le semestre est validé si la moyenne générale des notes des UE pondérées par les coefficients est supérieure ou égale à 10 sur 20.

CAPITALISATION : Chaque unité d'enseignement est affectée d'une valeur en crédits européens (ECTS). Une UE est validée et capitalisable, c'est-à-dire définitivement acquise lorsque l'étudiant a obtenu une moyenne pondérée supérieure ou égale à 10 sur 20 par compensation entre chaque matière de l'UE. Chaque UE validée permet à l'étudiant d'acquérir les crédits européens correspondants. Si les éléments (matières) constitutifs des UE non validées ont une valeur en crédits européens, ils sont également capitalisables lorsque les notes obtenues à ces éléments sont supérieures ou égales à 10 sur 20.