Objet

Ce document est le dossier qui accompagne la charte (cf. www.ssi.gouv.fr) pour une demande de labellisation SecNum*edu* par l'ANSSI des formations de l'enseignement supérieur en sécurité du numérique.

Modifications par rapport à la version 2.0 du dossier

C10 (titre délivré) : les certifications de niveau I ou II inscrites au RNCP ont été ajoutées. Cet ajout entraine des modifications ponctuelles sur d'autres critères.
C15 (ligne « Autres mises en pratique » : cette ligne a été ajoutée pour prendre en compte les heures de mises en pratique en sécurité (TP, projets…) qui ne peuvent pas être affectés à un thème technique défini pour l'ensemble d'une promotion.
C21 (intervenants) : seuls les personnes intervenant 6 heures ou plus doivent être citées (au lieu de 3h00 précédemment). Des informations supplémentaires sont demandées sur la formation ou l'expérience de l'intervenant dans le domaine d'intervention.

Modifications par rapport à la version 1.2 du dossier

La plupart des critères ont subi des modifications éditoriales afin de lever des ambiguïtés qui avaient été signalées ou constatées lors des premières labellisations. Ces modifications ne sont pas tracées.

Les principales autres modifications portent sur :

C10 (titre délivré) : les diplômes d'ingénieur de spécialisation reconnus par la CTI ont été ajoutés.
C12[1] (programme détaillé de la formation) : l'information minimum attendue est définie.
C15 (niveaux de compétence en sécurité) :

- il est possible de prendre en compte des programmes de formation qui se déroulent sur plusieurs années ;
- il est possible de mettre un commentaire publiable sous chaque thème de la sécurité. Par ailleurs, il est toujours possible de mettre un commentaire non publiable pour information ;
- sauf indication contraire, on ne peut prétendre aux niveaux 2 à 4 en sortie s'il n'y a pas de mise en pratique (sauf s'il n'y a pas d'augmentation par rapport au niveau d'entrée) ;
- L'intitulé de certains thèmes et leurs définitions ont été modifiés.

C17 (pratiques d'enseignement) :

[1] Les critères du dossier en version 1.2 étaient référencés par un numéro séquentiel <nn>. Dans la version 1.3, il s'agit désormais de familles de critères, référencées par C<nn> où <nn> est le numéro du critère de la version 1.2. Dans une famille, il peut y avoir un ou plusieurs critères. Lorsqu'il y en a plusieurs, C<nn> est suivi d'une lettre. Exemple :

C12 - Programme détaillé de la formation et modalités
C12a – lien sur le programme détaillé
…
C12b – lien sur une page donnant la tarification de la formation
…

- le fait qu'il y ait ou pas un cursus à l'étranger est traité à part. Ce critère peut avoir un impact sur le niveau de compétence en sortie dans C15.
- il est désormais possible d'indiquer la totalité des heures et mises en pratique portant sur la sécurité (pas seulement les heures de la dernière année).
- Pour qu'un diplômé puisse prétendre avoir suivi la formation labellisée, il doit avoir fait un stage ou une alternance et le thème de ce stage ou de cette alternance doit comporter une part « significative » d'activité dans le domaine de la sécurité.
- Le critère de volume de mise en pratique pour l'éligibilité à la labellisation a évolué. Les labellisations doivent proposer :

50% de mise en pratique dédiés à la sécurité (hors stage)
ou
200 heures de mise en pratique dédiées à la sécurité (hors stage)

C18 (volume de cours et TP dédiés à la sécurité) : le critère de volume pour l'éligibilité à la labellisation a évolué. Les formations doivent proposer :

70% de cours et mise en pratique (hors stage) dédiés à la sécurité
ou
400 heures de cours et mise en pratique (hors stage) dédiés à la sécurité

C16 (tableau compétence / métiers) : le tableau C16 a été supprimé.
C20 (liste des métiers) : la liste des métiers a été revue et fait l'objet d'un document séparé.
C23 (certifications professionnelles) : les informations demandées ont été revues pour prendre en compte les retours des établissements.

Conditions d'éligibilité à la labellisation

Pour être éligible à la labellisation SecNum*edu*, une formation doit répondre aux critères suivants :

- L'objet principal de la formation est la « sécurité du numérique » (sécurité des systèmes d'information, cyberdéfense, cybersécurité…).
- Le grade ou diplôme délivré à l'issue de la formation peut être :
  - un diplôme reconnu par l'État français conférant un grade de Licence ou de Master ;
  - un diplôme d'ingénieur reconnu par la Commission des titres d'ingénieur (CTI) ;
  - un Mastère spécialisé de la Conférence des grandes écoles (CGE) ;
  - une certification de niveau I ou II enregistrée au répertoire national de la certification professionnelle (RNCP) dont la durée de validité de l'enregistrement est supérieure ou égale à 3 ans.
- Les critères du présent document (cf. C15, C18…) sont respectés.
- L'établissement accepte de signer la charte des engagements disponible sur le site internet de l'ANSSI.
- L'établissement qui délivre la formation et qui demande la labellisation accepte la publication des informations signalées dans le présent document sur le site Internet de l'ANSSI.

Coordonnées où renvoyer le dossier

Il doit être envoyé en version électronique par courriel dans une version modifiable (.doc, .odt) à l'adresse suivante :

SecNum-edu[at]ssi.gouv.fr

Glossaire

CGE	Conférence des grandes écoles.
CTI	Commission des titres d'ingénieur.
CyberEdu	Programme visant à intégrer de la cybersécurité dans les formations en informatique non spécialisées en sécurité (www.cyberedu.fr).
SecNum*edu*	Programme de labellisation géré par l'ANSSI attestant de la conformité d'une formation de sécurité de l'enseignement supérieur à un ensemble d'exigences élaboré par l'ANSSI.
Formation	Formation pour laquelle la labellisation est demandée.
Etablissement	École d'ingénieur, université, IUT… qui dispense la formation pour laquelle la labellisation est demandée.
Référence ANSSI de la labellisation	Référence sous la forme ANSSI-SECNUMEDU-<année>-<N°> où année est l'année de délivrance de la labellisation et N°, un numéro d'ordre.

Légende

Le signalement des informations qui sont destinées à être publiées sur le site Web de l'ANSSI est écrit en **bleu**.

Certaines informations demandées dans ce dossier peuvent évoluer durant la période de validité de la labellisation. Ces évolutions doivent être signalées à l'ANSSI. Certaines évolutions sont qualifiées de « mineures », d'autres de « majeures » ce qui modifie leur traitement dans le processus de labellisation. Le signalement « mineur », « majeur » en relation avec les informations demandées est écrit en **rouge**. Lorsque rien n'est signalé, la modification n'a pas à être remontée à l'ANSSI.

Pour faciliter le remplissage du dossier, vous trouverez sur le site de l'ANSSI un exemple complet et réel correspondant à la formation ESSI de l'ANSSI (voir : ANSSI-SECNUMEDU-f-02_v2.0_dossier_ESSI_2017-07-12).

Objet du dossier

Le présent document

Date du dossier (jj/mm/aaaa)	12/07/2017

Le dossier concerne :

Objet du dossier	Cochez	Référence ANSSI de la labellisation
Une labellisation initiale (formation non labellisée)	X	
Le renouvellement de la labellisation d'une		

formation		
Une ou plusieurs modifications mineures en relations avec une formation déjà labellisée		
Une ou plusieurs modifications majeures en relations avec une formation déjà labellisée		

En cas de modifications mineures ou majeures, merci de bien vouloir résumer les modifications ci-après (en citant les numéros des points modifiés et en explicitant les raisons des modifications majeures).

Renseignements administratifs

C1 – Nom de l'établissement qui dispense la formation (Mineur)
Ce nom apparaitra sur le site Web de l'ANSSI.

Note : lorsque le titre délivré est une certification inscrite au RNCP (voir C10), l'établissement doit être dans la liste des lieux de préparation à la certification de la fiche RNCP décrivant la certification.

Centre de formation à la SSI de l'ANSSI

C2 – Liens internet concernant le référencement de l'établissement et de sa formation (Mineur)

C2a : adresse de la page d'accueil du site Web de l'établissement qui dispense la formation (**cette adresse sera publiée sur le site Web de l'ANSSI**)

https://www.ssi.gouv.fr

C2b : si disponible (obligatoire lorsque le titre délivré est une certification inscrite au RNCP), adresse de la page du RNCP où est inscrite la formation/certification (**cette adresse sera publiée sur le site Web de l'ANSSI**)

http://www.rncp.cncp.gouv.fr/grand-public/visualisationFiche?format=fr&fiche=4245

C2c : si disponible et pour information de l'ANSSI, adresse de la page du site de l'ENISA où est référencée la formation.

C3 – Statut de l'établissement (Majeur)

Fournir l'adresse internet d'une référence récente de la reconnaissance du titre délivré ou de l'autorisation à délivrer le titre par un organisme autorisé (CGE pour MS, CTI pour ingénieur, arrêté du Ministère de l'éducation nationale pour LP ou Master, inscription au RNCP…). Si l'information n'est pas accessible sur l'Internet, fournir une numérisation du document comportant l'information demandée avec le dossier.

http://www.rncp.cncp.gouv.fr/grand-public/visualisationFiche?format=fr&fiche=4245

C4 – Adresse postale de l'établissement qui dispense la formation (Mineur)

ANSSI/SDE/CFSSI 51 boulevard La Tour Maubourg 75700 Paris SP 07

C5 – Adresse du lieu où la formation est dispensée (Mineur)
Cette adresse apparaitra sur le site Web de l'ANSSI.

Notes :
- les formations doivent être localisées en France.
- Latitude et longitude : en degrés décimaux.
- Commentaire (facultatif) : texte libre qui sera publié s'il est présent.
- Dupliquez le tableau autant de fois qu'il y a de campus.

Nom du Campus	CFSSI		
Adresse du Campus	ANSSI Tour Mercure 31 quai de Grenelle 75015 Paris		
Latitude	48.8522949	**Longitude**	2.2861648
Commentaire (facultatif)			

C6 – Contact administratif pour la formation (civilité, prénom, nom, téléphone, courriel, adresse si différente de C4) (Mineur)
Notes :
- Dupliquez ce tableau autant de fois qu'il y a de contacts
- Accord pour être dans la liste de diffusion SecNum*edu* (Ou /Non) : l'ANSSI est susceptible d'envoyer des messages d'informations généraux, des invitations à des réunions, etc. Ces messages sont envoyés aux contacts ayant exprimé leur accord ci-après.

Civilité	M.
Prénom	Olivier
Nom	Levillain
Téléphone(s)	01 XX XX XX XX
Courriel	olivier.levillain@ssi.gouv.fr
Accord pour être dans la liste de diffusion SecNum*edu* (Oui/Non)	Oui
Accord pour que l'adresse courriel soit visible dans les courriels émis par SecNum*edu* (Oui/Non)	Oui
Adresse si différent de C4	

C7 – Contact technique et scientifique pour la formation (civilité, prénom, nom, téléphone, courriel, adresse si différente de C4) (Mineur)
Notes :
- Dupliquez ce tableau autant de fois qu'il y a de contacts
- Accord pour être dans la liste de diffusion SecNum*edu* (Ou /Non) : l'ANSSI est susceptible d'envoyer des messages d'informations généraux, des invitations à des réunions, etc. Ces messages sont envoyés aux contacts ayant exprimé leur accord ci-après.

-

Civilité	M.
Prénom	Olivier
Nom	Levillain
Téléphone(s)	01 XX XX XX XX
Courriel	olivier.levillain@ssi.gouv.fr
Accord pour être dans la liste de diffusion SecNum*edu* (Oui/Non)	Oui
Accord pour que l'adresse courriel soit visible dans les courriels émis par SecNum*edu* (Oui/Non)	Oui
Adresse si différent de C4	

-

C8 – Liste des formations dispensées par l'établissement déjà labellisées SecNum*edu*

Intitulé de la formation	Référence ANSSI de la labellisation

Renseignements sur la formation

C9 – Intitulé de la formation (Mineur)
Cet intitulé sera publié sur le site Web de l'ANSSI.

Expert en sécurité des systèmes d'information (ESSI)

C10 – Titre délivré (Majeur)
Ce titre sera publié sur le site Web de l'ANSSI.

Titre	Cochez
Licence, licence pro	
Master	
Ingénieur (CTI)	
Ingénieur de spécialisation (CTI)	
Mastère spécialisé (CGE)	
RNCP niveau I	X
RNCP niveau II	

Lorsque le titre délivré est une certification inscrite au RNCP, donnez ci-après le lien sur le dernier arrêté portant enregistrement au répertoire national des certifications professionnelles.

Lien vers arrêté	https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029181617

C11 - Nombre d'étudiants d'une promotion et nombre de promotions (Mineur, à actualiser annuellement)
Cette information apparaitra sur le site Web de l'ANSSI.

Notes :
- UE doit être comprise comme « union européenne hors France ».
- Nombre de promotions depuis la création : il s'agit du nombre de promotions formant au programme (par exemple, une majeure dans la formation) proposé à la labellisation[2].
- Commentaire (facultatif) : texte libre qui sera publié s'il est présent.

Nombre maximum d'étudiants dans une promotion	12			
Nombre d'étudiants de la dernière promotion (précisez l'année de la promotion)	**Total**	**Français**	**UE**	**Hors UE**
	10	10		
Nombre d'étudiants diplômés de la dernière promotion en pourcentage	100%			
Nombre de promotions sorties depuis la création	7			
Commentaire (facultatif)	Avant 2011, la formation existait dans un format différent (2 ans au lieu de 13 mois).			

C12 - Programme détaillé de la formation et modalités

C12a – lien sur le programme détaillé (Mineur)
(Ce lien sera publié sur le site Web de l'ANSSI)

Un programme détaillé de la formation doit être publiquement disponible. Le niveau de détail minimum attendu est disponible à cette adresse :

https://www.ssi.gouv.fr/uploads/2015/07/Presentation_scolarite_ESSI.pdf

L'ANSSI considère normal, voire indispensable, que le pro
conscient qu'au regard de certains critères de ce dossier, cer
cause la labellisation.

Un exemple de niveau de détail pour un module est présenté en annexe de ce document.

Lien sur un site Web présentant le programme détaillé	https://www.ssi.gouv.fr/uploads/2015/07/Presentation_scolarite_ESSI.pdf

C12b – lien sur une page donnant la tarification de la formation (Mineur)
(Ce lien sera publié sur le site Web de l'ANSSI)

La page peut être externe au site Web de l'établissement. En particulier, pour les universités, il est possible de pointer sur la page (à actualiser en fonction de l'année) :

http://www.enseignementsup-recherche.gouv.fr/cid20195/frais-d-inscription-pour-la-rentree-universitaire-2016.html

[2] Dans certains cas, la formation candidate à la labellisation est une « majeure » d'une formation délivrant un titre (par exemple, Ingénieur d'une certaine école). Le nombre de promotions à renseigner est celui correspondant à la majeure et pas au titre d'ingénieur.

Lien sur un site Web présentant la tarification de la formation	https://www.ssi.gouv.fr/uploads/2015/07/Presentation_scolarite_ESSI.pdf (formation gratuite réservée à la fonction publique)

C13 - Dominante de la formation (Majeur)

Formation à dominante technique
La formation est considérée comme étant à dominante technique lorsque plus de 50% du volume horaire hors stage est consacré à des activités techniques pratiques dans le domaine de la sécurité (par exemple, des TP ou des projets techniques).

Les activités typiques entrant dans cette catégorie sont :
- le développement logiciel ;
- les travaux en lien avec les applications et les services sécurisés (mise en œuvre et configuration, analyse de la sécurité…) ;
- les travaux en lien avec les systèmes d'exploitation (mise en œuvre et configuration, audit de configuration, test de pénétration…) ;
- les travaux en lien avec les réseaux (mise en œuvre et configurations d'équipements sécurité, test de pénétration…) ;
- les travaux en liens avec du matériel (mesures de signaux compromettants, analyse logique, conception de produits matériels sécurisés…) :
- la rétro ingénierie (logicielle ou matérielle) ;
- la cryptographie (implémentation sûres…) ;
- l'analyse post-mortem (investigation numérique, forensique) ;
- et de manière générale, les activités à caractère technique ou scientifique.

Formation à dominante organisationnelle (managériale, méthodologique…)
La formation est à mettre dans cette catégorie lorsque les activités techniques pratiques font moins de 50% du volume horaire hors stage.

Les activités typiques entrant dans cette catégorie sont :
- les travaux méthodologiques ;
- les analyses de risques ;
- les audits organisationnels ;
- l'utilisation d'outils destinés à mettre en œuvre les activités d'analyse de risques, d'audit, de gestion de projet sécurité ;
- les travaux autour de la définition de politiques de sécurité ;
- les travaux visant à l'entraînement au management de la sécurité.

Le tableau ci-après sera publié sur le site Web de l'ANSSI.

Type de formation	Cochez
Formation à dominante technique	X
Formation à dominante organisationnelle	

C14 - Formation spécialisée (Majeur)
Cette information sera publiée sur le site Web de l'ANSSI.

La formation est dite spécialisée lorsqu'elle vise notamment à former à un domaine particulier de la sécurité. Par exemple, la cryptographie, la sécurité des circuits intégrés, la sécurité de la biométrie…

Le volume horaire dans ce domaine de spécialisation doit correspondre à au moins 50% du volume horaire hors stage (mise en pratique[3] et cours).

Le fait qu'une formation soit spécialisée peut autoriser que certains thèmes de la sécurité des technologies de l'information ne soient pas abordés et peut modifier l'appréciation de certains des autres critères de ce dossier.

Laissez « sans objet » dans le tableau ci-dessous si la formation candidate n'est pas une formation spécialisée.

Thème
Sans objet

C15 - Niveau de compétence en sécurité et heures de cours et de mise en pratique dédiés à la sécurité (Majeur)
Indiquez le niveau attendu **en sécurité** en entrée de la formation et le niveau visé à la sortie de la formation selon les codes suivants :

0 : Pas de compétence.

1 : SENSIBILISATION : comprendre les principaux enjeux et problèmes liés à la compétence.

2 : APPLICATION : réaliser des actes simples et certains actes complexes liés à la compétence.

3 : MAÎTRISE : réaliser des actes complexes ou tous les actes liés à la compétence.

4 : SPÉCIALISÉ : avoir reçu une formation dédiée à la compétence sur une durée longue permettant de justifier d'un niveau allant au-delà de la maitrise.

L'ANSSI s'attend à ce que pour l'ensemble des compétences, le **niveau en entrée** soit égal à 0. Si ce n'est pas le cas, un argumentaire dans la zone de commentaires publiables doit indiquer comment le niveau en entrée est vérifié par l'établissement.

L'ANSSI s'attend à ce que pour l'ensemble des compétences issues de CyberEdu, le niveau en sortie soit au moins de 1 (sensibilisé). Si ce n'est pas le cas, un argumentaire dans la zone de commentaire publiable justifiant la non-prise en compte des compétences concernées est attendu.

L'usage du niveau 4 devrait être exceptionnel, pour une formation initiale. Il concerne essentiellement certaines formations spécialisées dédiées à un domaine particulier.

Sauf indication contraire (voir l'annexe 1 où les thèmes sont définis), on ne peut prétendre aux niveaux 2 à 4 en sortie s'il n'y a pas de mise en pratique (sauf s'il n'y a pas d'augmentation par rapport au niveau d'entrée).

Les heures de conférences, lorsqu'elles sont obligatoires, peuvent être comptabilisées dans les heures de cours.

[3] Travaux pratiques, travaux dirigés, heures prévues dans l'emploi du temps pour les projets et autres mises en pratique, hors stage.

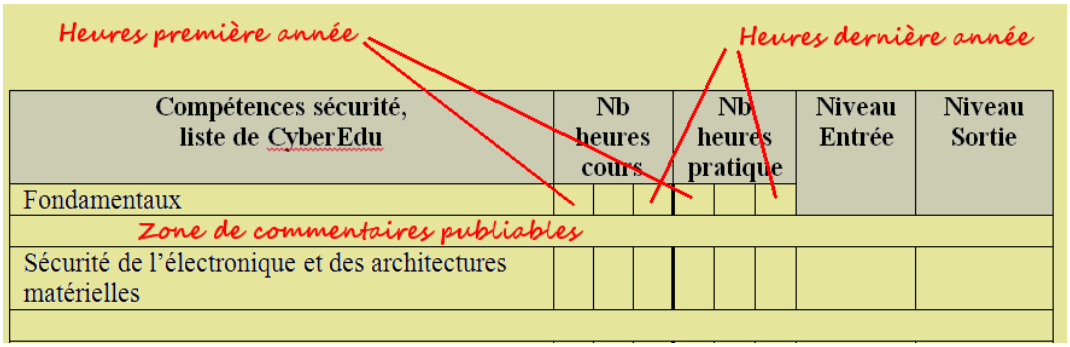
Pour des précisions sur les compétences provenant de la liste de CyberEdu[4], voir annexe 1, « Thèmes de la cybersécurité ». Si certaines compétences n'apparaissent pas dans le tableau ci-après, il est possible de les ajouter dans la rubrique « autres ».

Pour chaque thème de la sécurité, il est possible d'ajouter un commentaire en texte libre qui sera publié.

Les heures (cours et mise en pratique) peuvent être réparties sur plusieurs années. Si la formation se déroule sur une seule année, on ne remplira que la dernière colonne. Si elle se répartie sur 2 années, on remplira les deux dernières colonnes. Pour 3 années, on remplira les 3 colonnes.

Hors champs « commentaires », les informations saisies doivent être uniquement des nombres (entiers pour les niveaux, décimaux pour les heures).

Remarque sur la ligne « autres mise en pratique sécurité » : certaines formations réservent des heures pour des projets ou TP/TD dont les thèmes peuvent varier selon les groupes d'étudiants de la promotion.



Le tableau ci-dessous sera publié sur le site Web de l'ANSSI.

Compétences sécurité, liste de CyberEdu	Nb heures cours			Nb heures pratique			Niveau Entrée	Niveau Sortie
Fondamentaux			6					
Sécurité de l'électronique et des architectures matérielles			3			0	0	1
Sécurité des systèmes d'exploitation			96			75	0	3
Le sujet de systèmes d'exploitation est traité en profondeur au travers de deux grands modules. D'une part le module « système » repose sur l'étude des systèmes Unix, avec une partie pratique importante (majoritairement sous la forme de TP en C sous Linux). D'autre part le module « Windows » traite des mécanismes internes aux systèmes Microsoft, avec là encore un certain nombre de travaux pratiques.								

[4] Certains thèmes de Cyberedu ainsi que leurs définitions ont été modifiés. Ces modifications font suites à de nombreuses demandes d'éclaircissement faites par les établissements d'enseignement labellisés sur la base du dossier en version 1.2.

Sécurité des réseaux et protocoles			60			30	0	3
Une première partie des cours réseaux consiste en une (re)découverte de la pile TCP/IP du point de vue de la sécurité ; cette première partie comporte de nombreuses manipulations. Une seconde partie explore les aspects opérateurs et gouvernance de l'internet. Une troisième partie présente les principaux protocoles réseau (IPv6, DNS, SMTP, HTTP, TLS, SSH) en insistant sur les aspects sécurité. Enfin une quatrième partie traite des aspects web, avec une part importante de pratique.								
Cryptologie			62			45	0	2
Les briques de base de la crypto sont abordées pendant la formation, tant du côté symétrique qu'asymétrique. Chaque cours fait l'objet d'une séance de travaux dirigés.								
Stéganographie et tatouage			1			0	0	1
Sécurité des bases de données			4.5			7.5	0	2
Contribution des architectures à la sécurité			6			0	0	1
Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité			15			0	0	2
Certifications et évaluations de produits			3			0	0	1
Politique de cybersécurité et SMSI			9			6	0	2
Droit et réglementation			13.5			0	0	1
Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité)			18			39	0	2
Un module est dédié au sujet du développement sécurisé (« SecuLog »). Il couvre à la fois les aspects écriture de code, mais également des aspects architecturaux. La mise en œuvre passe, entre autres, par un projet réalisé en binôme.								
Prise en compte de la sécurité dans les projets			15			9	0	2
Cyberdéfense			25.5			0	0	1
Analyse post-mortem (Forensic)			0			3	0	1
Sécurité des systèmes spécifiques et émergents			12			0	0	1
Aspects sociaux et sociétaux			0			0	0	1

Les étudiants ont une expérience professionnelle qui est évaluée lors de l'entretien.								
Tests d'intrusion			0			27	0	2
Les élèves suivent le stage catalogue 8b du CFSSI, qui traite des aspects techniques de l'audit en SSI.								
Sécurité physique			3			0	0	1
Sécurité des services externalisés			3			0	0	1
Compétences sécurité en dehors de la liste de CyberEdu	**Nb heures cours**			**Nb heures pratique**			**Niveau Entrée**	**Niveau Sortie**
Rétro-ingénierie								
Aspects économique de la sécurité								
Compétences Sécurité autres	**Nb heures cours**			**Nb heures pratique**			**Niveau Entrée**	**Niveau Sortie**
Autres mises en pratique sécurité (précisez)[5]						24		
Projet bibliographique sur des thèmes de la sécurité avec soutenance.								
Compétences Sécurité autres	Nb heures cours			Nb heures pratique			Niveau Entrée	Niveau Sortie

Pour être éligible à la labellisation, le nombre d'heures de la partie pratique de la formation sur les aspects sécurité **doit :**

- soit faire 200 heures ou plus (somme des heures indiquées dans la colonne « Nb heures pratique » du tableau précédent).
- soit correspondre à au moins **50%** du volume global de la formation sur la partie sécurité (la somme des heures indiquées dans la colonne « Nb heures pratiques » doit être supérieure ou égale à la somme des heures indiquées dans la colonne « Nb heures cours »).

Le tableau ci-dessous **ne sera pas publié** sur le site de l'ANSSI. Il permet d'associer, **si nécessaire**, un commentaire permettant de faciliter l'interprétation du tableau précédent par l'ANSSI.

Compétences sécurité, liste de CyberEdu	**Commentaires éventuels à l'attention de l'ANSSI**
Fondamentaux	
Sécurité de l'électronique et des architectures matérielles	
Sécurité des systèmes d'exploitation	
Sécurité des réseaux et protocoles	
Cryptologie	
Stéganographie et tatouage	
Sécurité des bases de données	
Contribution des architectures à la sécurité	

[5] Cette ligne permet de comptabiliser les heures de mise en pratique prévues à l'emploi du temps que l'on ne sait pas affecter à thème pour l'ensemble d'une promotion. Ce cas se rencontre lorsqu'une promotion est découpée en groupes et que chaque groupe travaille sur un sujet différent (ou du moins, tous les groupes ne travaillent pas sur le même sujet).

Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité	
Certifications et évaluations de produits	
Politique de cybersécurité et SMSI	
Droit et réglementation	
Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité)	
Prise en compte de la sécurité dans les projets	
Cyberdéfense	
Analyse post-mortem (Forensic)	
Sécurité des systèmes spécifiques et émergents	
Aspects sociaux et sociétaux	
Tests d'intrusion	
Sécurité physique	
Sécurité des services externalisés	
Compétences sécurité en dehors de la liste de CyberEdu	**Commentaires éventuels**
Rétro-ingénierie	
Aspects économique de la sécurité	
Compétences Sécurité autres	**Commentaires éventuels**

C16 – RESERVE A UN USAGE FUTUR

C17 - Répartition des pratiques d'enseignement et de leur évaluation dans l'obtention du diplôme (Majeur)

Il est possible de ne remplir qu'un tableau parmi les deux proposés (STAGE pour les formations proposant un stage et ALTERNANCE pour les formations en alternance). Il est aussi possible de remplir les deux tableaux lorsque la formation propose les deux modes.

C17a – pratiques d'enseignement

Ce ou ces tableaux apparaitront sur le site Web de l'ANSSI avec en plus la répartition en pourcentage.

Le tableau doit être rempli avec le nombre **total** d'heures de la formation pour chaque rubrique (donc, y compris les heures non dédiés à la sécurité).

La mise en pratique de la formation (TP, projets) **doit** se dérouler en présentiel pour au moins 50% de sa durée.

Afin d'illustrer les critères C15 et C17a sur un exemple concret, considérons une semaine de cours d'une formation d'ingénieur :

Lundi	Mardi	Mercredi	Jeudi	Vendredi
Cryptographie (cours) Réglementation SSI (cours)	Sécurité réseau (cours) Sécurité réseau (TP)	Projet de fin d'étude en sécurité	Langues et humanités Sport	Sécurité systèmes d'exploitation (cours) Sécurité systèmes d'exploitation (TP)

Dans le tableau C15, les cours du lundi, du mardi et du vendredi rentrent naturellement dans des catégories établies. Il faut ajouter les créneaux du jeudi via la case « Autres mises en pratique ». Pour cette semaine, le total du tableau C15 sera donc de 4 demi-journées de cours et 4 demi-journées de mise en pratique. Sur cet

échantillon, le critère de 50 % de mise en pratique est donc respecté.

Concernant les pratiques d'enseignement (C17a), il faut également prendre en compte les cours du jeudi matin. On obtient donc pour cette semaine 5 demi-journées de cours et 2 demi-journées de TP et 2 demi-journées de projet. En appliquant le critère sur la proportion de cours dédié à la sécurité à cette semaine, on obtient donc 8 demi-journées dédiées à la sécurité sur 9 demi-journées d'enseignement, soit 89 %.

Par ailleurs, les formations doivent proposer au moins un stage/alternance en entreprise dont le sujet a trait à la sécurité du numérique.

On peut admettre que la sécurité ne représente qu'une partie des activités d'un stage ou de l'alternance. Ainsi, un stage ou une alternance dans le domaine de l'administration des réseaux et système peut (devrait) comporter une part "significative" d'activité liée à la sécurité mais n'est pas à proprement parlé un stage dans le seul domaine de la sécurité.

Si le stage ou l'alternance ne comporte pas une part significative d'activité liée à la sécurité, le diplômé ne peut se prévaloir d'avoir suivi intégralement la formation labellisé et ne peut donc recevoir une éventuelle attestation démontrant qu'il a suivi cette formation.

Le fait que le sujet de stage/alternance comporte une part significative d'activité liée à la sécurité est laissé à l'appréciation de l'établissement

Heures première année

Heures dernière année

Répartition des pratiques d'enseignement (STAGE)					
Catégories		Nombre d'heures			Commentaires éventuels
Cours magistraux, conférences	Présentiel[5]				
	Distance[6]				
	MOOC[7]				
Travaux pratiques	Présentiel				
	Distance				
Projets[8]					

Répartition des pratiques d'enseignement (STAGE)					
Catégories		**Nombre d'heures**			**Commentaires éventuels**
Cours magistraux, conférences	**Présentiel**[6]			387	30 heures de cours de remise à niveau n'ont pas été prises en compte par à rapport à C15 (maths, programmation C, latex, git)
	Distance[7]				
	MOOC[8]				
Travaux pratiques	**Présentiel**			261	36 heures de cours de remise à niveau n'ont pas été prises en compte par à rapport à C15 (maths, programmation C)
	Distance				
Projets[9]				42	
Stages				840	6 mois de 4 semaines de 35 heures
Autres (précisez)	**Présentiel**				
	Distance				
Totaux				1530	

Répartition des pratiques d'enseignement (ALTERNANCE)					
Catégories		**Nombre d'heures**			**Commentaires éventuels**
Cours magistraux, conférences	**Présentiel**				
	Distance				
	MOOC				
Travaux pratiques	**Présentiel**				
	Distance				
Projets					
Alternance					
Autres (précisez)	**Présentiel**				
	Distance				
Totaux					

[6] Cours ayant lieu dans l'établissement d'enseignement.

[7] Cours suivi à distance à partir d'un cours intégralement retransmis.

[8] Indiquez le nombre d'heures en « heure-équivalent-présentiel » (cf. définition de la CTI).

[9] Un projet est défini comme un travail qui se déroule sur plusieurs semaines, en général en équipe (binôme, trinôme, voire, promotion complète), permettant de valider des compétences acquises durant la formation et mettant les étudiants dans une situation rappelant celle que l'on peut trouver en milieu professionnel (délais, réponse aux besoins, organisation et déroulement du projet, restitution…). L'établissement doit s'engager sur la disponibilité de moyens (salle, ressources informatiques) durant toute la durée du projet afin de permettre aux étudiants de travailler sur place en équipe selon les besoins.

C17b – pratiques d'évaluation

Ce ou ces tableaux apparaitront sur le site Web de l'ANSSI.

Répartition des pratiques d'évaluation (CLASSIQUE)		
Catégories	**Poids dans l'évaluation**	**Commentaires éventuels**
Examen sur table	30%	
Dossier seul	4%	Projet de programmation sécurisé
Oral seul (face à face…)	16%	Grand oral, épreuve de synthèse et projet bibliographique
Dossier+Oral	%	
Soutenance de stage[10]	50%	
Autres (précisez)	%	
Totaux	**100%**	

Répartition des pratiques d'évaluation (ALTERNANCE)		
Catégories	**Poids dans l'évaluation**	**Commentaires éventuels**
Examen sur table	%	
Dossier seul	%	
Oral seul (face à face…)	%	
Dossier + Oral	%	
Alternance[11]	%	
Autres (précisez)	%	
Totaux	**100%**	

C17c – Cursus à l'étranger

La formation propose-t-elle que tout ou partie de la formation se déroule dans un établissement de formation à l'étranger ?	~~OUI~~/NON

Si la réponse est « Non », la suite des informations demandées au titre de ce critère n'est pas à renseigner.

Pour les questions suivantes, il ne faut considérer que les cours et mise en pratique qui ont trait à la sécurité du numérique.

La formation impose-t-elle qu'une partie de la formation se déroule dans un établissement de formation à l'étranger ?	~~OUI~~/NON

Si la réponse est « Oui », veuillez contacter l'ANSSI. La suite des informations demandées au titre de ce critère n'est pas à renseigner.

A ce stade, on considère que la formation propose que certains cours et mise en pratique ayant trait à la sécurité se déroulent dans un établissement étranger.

[10] Doit être supérieur à 0% pour être éligible.

[11] Doit être supérieur à 0% pour être éligible.

Les étudiants qui suivent une partie de ce cursus dans un établissement étranger ne peuvent pas suivre les cours et mise en pratique ayant trait à la sécurité qui se déroulent en France durant leur absence. Dans le tableau ci-dessous, C<i>F/E…C<i>E, représentent des cours et mises en pratique ayant trait à la sécurité, <i> étant le numéro d'un cours.

Cours en France	**Cours à l'étranger**
…	
C1F	
C2F	
C3F	C1E
C4F	C5E
C5F	C8E
C6F	C9E
C7F	
…	

C1F, C2F, C5F, C7F pourront être pris en compte au titre de la labellisation secNum*edu*.
C3F, C4F, C6F, C8E, C9E ne pourront pas être pris en compte au titre de la labellisation SecNum*edu*.
Si C<i>F et C<i>E ne mènent pas au même niveau de compétence, alors, le niveau de compétence le plus faible doit être retenu au titre de SecNum*edu*.

L'objectif ici est de garantir que tout étudiant ayant suivi la formation labellisée, qu'il ait suivi une partie du cursus en France ou à l'étranger, a bien acquis les mêmes minimum de compétences sur les différents thèmes de la sécurité.

L'information qui sera publiée sur le site de l'ANSSI indiquera si la formation impose ou propose qu'une partie du cursus se déroule à l'étranger. **Le tableau (à compléter) suivant sera publié sur le site de l'ANSSI** :

Cursus à l'étranger	~~possible/obligatoire~~/non
Commentaires	

En commentaire, il est possible d'indiquer où se déroule le cursus à l'étranger (université, pays), une équivalence de diplôme éventuelle…

C18 - Volume de cours et TP dédiés à la sécurité (Majeur)
Les valeurs pertinentes ci-après seront publiées sur le site Web de l'ANSSI.

En s'appuyant sur le tableau précédent (cf. C17a), indiquez en pourcentage et en heures le volume de cours et mise en pratique dédiés à la sécurité (**hors stage**) par rapport aux autres cours et TP (mise à niveau, matières générales…).

Pour être éligibles à la labellisation, le volume de cours et mise en pratique dédiés à la sécurité doit :

- être supérieur ou égal à **70%** du volume de cours et mise en pratique de la formation). Cette valeur est calculée en prenant le total des heures de cours et pratiques du tableau C15 et le total des heures renseignées dans le tableau C17a, hors heures de stage/alternances ;
  ou
- être supérieur à **400h**[12]. Cette valeur est calculée en prenant le total des heures de cours et pratiques du tableau C15.

[12] Certaines formations peuvent être conformes aux deux critères mais en pratique, les formations sur un an rechercherons plutôt la conformité au critère « 70% » mais pas au critère « 400h » alors que les formations sur 3 ans rechercheront la conformité au critère « 400h » mais pas au critère « 70% ».

Volume de cours et mise en pratique dédiés à la sécurité (en pourcentage)[13]	Calculé automatiquement sur la base des tableaux C15 et C17a
Volume de cours et mise en pratique dédiés à la sécurité (en heures)	Calculé automatiquement sur la base du C1

90.87%

627h

C19 - Aspects juridiques dans la formation (Majeur)
Les aspects juridiques et légaux de la sécurité et de la protection des données person re abordés au niveau général et doivent être instanciés au niveau de chaque thème de l e justifie.

L'établissement s'engage à ce que ce thème soit abordé dans sa formation ou fasse partie des pré requis à l'entrée de la formation.

Explication en texte libre sur la façon dont ce thème est traité dans la formation	*Les aspects juridiques sont traités dans plusieurs cours :* *- réglementation nationale en matière de SSI* *- introduction au droit de la SSI* *- cybercriminalité* *- gouvernance internet* *- gestion des incidents*
Nombre d'heures	*10*

C20 – Après la formation (Mineur, à actualiser annuellement)

C20a – Activité la première année après le diplôme
Ce tableau sera publié sur le site de l'ANSSI.

Activité la première année après le diplôme	Pourcentage de la promotion
Diplômé en activité professionnelle	*100%*
Diplômé en recherche d'emploi	
Poursuite d'étude	
Autres cas (pas d'information, année sabatique…)	

C20b – Métiers visés en sortie et pratiquées, en sortie et 5 ans après la sortie
Ce tableau sera publié sur le site de l'ANSSI.

Légende du tableau ci-après :

- **Cat** : catégorie de métiers décrite en annexe et rappelée ici pour mémoire :
  - CAE : conseil, audit, expertise

[13] Pour un cours se déroulant sur une année, ce pourcentage est normalement directement issue du ratio entre le total des cours et mise en pratique du tableau C15 et le total des heures et de pratiques du tableau C17a. Pour un cours se déroulant sur plusieurs années, ce pourcentage n'a pas forcément de sens et peut être omis. Dans ce cas, l'ANSSI se base sur le volume de cours et mise en pratique en heures pour valider le critère.

  - MPC : management de projets et cycle de vie
  - OMCO : opération et maintien en condition opérationnelle
  - POG : pilotage, organisation et gestion des risques
  - SGI : support et gestion des incidents

- **Métiers** : nom possible du métier. Pour une liste plus importante, voir en annexe 2.
  Une rubrique **« Autre métier sécurité » est** disponible pour chaque catégorie et permet de prendre en compte des métiers qui ne sont pas dans la liste. Il n'est pas prévu la possibilité d'ajouter des nouvelles catégories.

- **En sortie** : permet d'indiquer les métiers visés et réellement pratiqués en sortie de formation.
  - **Visés** : métiers visés selon l'établissement :
    - « 1 » - métiers visés **principalement** selon l'établissement.
    - « 2 » - métiers visés **marginalement** selon l'établissement.
    - Non rempli : métiers non visés selon l'établissement.

  - **Pratiqués** : l'établissement dispose de statistiques concernant au moins 50% des diplômés ayant une activité professionnelle dans les 6 mois après la sortie de la formation. Le tableau est alors rempli avec des pourcentages de la population en choisissant une dominante pour les personnes ayant plusieurs métiers.
    Si l'établissement ne dispose pas de statistiques suffisamment consistantes, cette colonne **ne doit pas** être remplie.

- **Commentaire** : pour chaque métier, il est possible d'ajouter un commentaire qui sera publié.

- **5 ans après la sortie** : permet d'indiquer les métiers réellement pratiqués 5 ans après la sortie de la formation.
  - **Pratiqués** : l'établissement dispose de statistiques concernant au moins 50% des diplômés ayant une activité professionnelle 5 ans après la sortie de la formation. Le tableau est alors rempli avec des pourcentages de la population en choisissant une dominante pour les personnes ayant plusieurs métiers.
    Si l'établissement ne dispose pas de statistiques suffisamment consistantes, cette colonne **ne doit pas** être remplie.

Cat.	Métiers (Voir en annexe 1)	En sortie		5 ans après la sortie
		Visés 1 ou 2	Pratiqués %	Pratiqués %
CAE				
CAE	Conseiller juridique en sécurité			
CAE	Consultant sécurité « organisationnel »	2		
CAE	Consultant sécurité « technique »	1		
CAE	Cryptologue			
CAE	Délégué à la protection des données (DPD)			
CAE	Évaluateur sécurité			
CAE	Autre métier sécurité			
MPC				
MPC	Architecte de sécurité	2		
MPC	Chef de projet sécurité	2		
MPC	Développeur de sécurité			
MPC	Autre métier sécurité			
OMCO				
OMCO	Administrateur sécurité			
OMCO	Technicien sécurité			
OMCO	Autre métier sécurité			
POG				
POG	Correspondant sécurité	1		
POG	Responsable du plan de continuité d'activité			
POG	Responsable de la sécurité des systèmes d'information (RSSI)	1		
POG	Spécialiste en gestion de crise			
POG	Autre métier sécurité			
SGI				
SGI	Analyste SOC			

SGI	Expert réponse à incident (CERT)			
SGI	Autre métier sécurité			

C21 - Intervenants (Mineur)
Les noms et qualité des intervenants qui interviennent au moins 6h00 dans la formation accompagnés d'une courte biographie (une dizaine de lignes maximum).

Il est admis que certaines conférences ont pour objet la présentation d'un organisme par un intervenant désigné par cet organisme et qui peut changer d'une année sur l'autre. Dans ce cas, les noms, prénoms et biographie peuvent ne pas être renseignés.

Pour faciliter la manipulation du présent dossier, merci de bien vouloir **fournir ces informations dans un document à part**.

Nom	**Prénom**	**Organisme**
Domaine / nom de l'intervention		**Durée de l'intervention en heures**
Formations suivies par l'intervenant en lien avec l'intervention ou expérience professionnelle en lien avec l'intervention		
Biographie		

C22 - **Indiquez en pourcentage la part (en nombre) des intervenants provenant de milieux académiques des intervenants provenant du milieu professionnel (industrie, administration) (Mineur)**
Ce ratio sera publié sur le site Web de l'ANSSI.

Intervenants milieu académique	**Intervenants milieu professionnel**
20%	80%

Note : le total doit faire 100%

C23 - Certifications professionnelles passées dans le cadre de la formation (Mineur)
Cette liste sera publiée sur le site de l'ANSSI.

Le tableau suivant permet d'indiquer les certifications professionnelles préparées ou obtenues durant le cursus de formation.

- **Nom de la certification** : nom commercial ou nom tel qu'il est inscrit à l'Inventaire de la CNCP
- **Préparation** : indiquez si la préparation à la certification est optionnelle ou obligatoire dans le cadre du cursus.
- **Passage de la certification** : indiquez si le passage de la certification est obligatoire, optionnel ou « non passée ». Dans ce dernier cas, les lignes qui suivent ne doivent pas être remplies.
- **Organisme certificateur** : nom de l'organisme qui délivre le certificat.
- **Pourcentage des étudiants ayant passé la certification** : il s'agit d'un pourcentage d'étudiants sur l'effectif de la promotion qui suit l'enseignement labellisé. Doit être 100% si le passage de la certification est obligatoire.
- **Pourcentage des étudiants ayant obtenu la certification** : il s'agit d'un pourcentage d'étudiants sur l'effectif de la promotion qui suit l'enseignement labellisé. Cette information renseigne les étudiants sur leur chance d'obtenir la certification.

Ce tableau doit être dupliqué autant de fois qu'il y a de certifications professionnelles.

Nom de la certification	
Préparation à la certification	« Obligatoire » ou « optionnelle »
Passage de la certification	« Obligatoire », « optionnel » ou « non passée ».
Cas où la certification est passée	
Organisme certificateur	
Lien vers l'inventaire de la CNCP si disponible	
Pourcentage des étudiants de la promotion ayant passé la certification	
Pourcentage des étudiants de la promotion ayant obtenu la certification	
Commentaire éventuel en texte libre ci-après	

C24 - Formations labellisées par la CNIL (Mineur)
Cette liste sera publiée sur le site de l'ANSSI.

Indiquez dans le tableau ci-dessous les formations labellisées par la CNIL qui sont suivies par les étudiants.

Nom de la formation	Référence du label CNIL

C25 - Niveau d'anglais (Mineur)

Ce tableau sera publié sur le site de l'ANSSI.

De plus en plus d'employeurs imposent un niveau d'anglais dans les critères d'embauches. Les renseignements[14] qui suivent informent les étudiants et employeurs sur la façon dont la formation labellisée aborde ce sujet.

Niveau en entrée		
La formation impose-t-elle un niveau d'anglais minimum vérifié en entrée ?		Oui / ~~Non~~
Si oui, comment le niveau est-il vérifié (précisez) ?	**L'établissement**	Sans objet
	Une certification[15]	*Oui, TOEIC*
Si oui, niveau minimum demandé	**CECRL**[16]	Sans objet
	Autre	*TOEIC 750*

Niveau en sortie		
Niveau minimum visé par la formation en sortie	**CECRL**	Néant
	Autre	Néant
Comment le niveau est-il vérifié ?	**L'établissement**	Néant
	Une certification	Néant
L'atteinte du niveau est-il obligatoire pour l'obtention du diplôme ?		~~Oui / Non~~ / Sans objet
Si l'atteinte du niveau n'est pas obligatoire pour l'obtention du diplôme mais qu'il y a un examen ou une certification, indiquez le pourcentage de diplômés ayant atteint le niveau pour la dernière promotion connue (précisez l'année)		Sans objet

Points généraux

C26 - Points en texte libre que vous souhaitez porter à l'attention de l'ANSSI

C27 – Description de la formation (optionnel)

Cette description sera publiée sur le site de l'ANSSI sous réserve qu'elle soit acceptée.

[14] Modifiez les valeurs par défaut dans le tableau s'il y a lieu. Les valeurs par défaut correspondent à « pas de niveau minimum attendu en entrée » et « pas de niveau minimum imposé en sortie ».

[15] Pour les certifications ou les niveaux demandés ou obtenus, indiquez le référentiel d'évaluation (TOEFL, TOEIC, IELTS…).

[16] Cadre européen commun de référence pour les langues : http://www.coe.int/t/dg4/linguistic/Source/Framework_FR.pdf

L'objet de ce point est de décrire informellement la formation et de mettre en exergue les points qui vous paraissent importants.
L'ANSSI se réserve le droit d'en refuser la publication (description trop « commerciale », dénigrement d'autres formations, informations trompeuses…).

La description doit faire au maximum 1200 signes, espaces compris. Elle ne doit pas comporter d'enrichissements (gras, souligné, italique…).

La formation ESSI est un cursus dense qui propose une vision technique et large de la sécurité. Elle a pour principes la curiosité et la rigueur. L'objectif est de former des personnes crédibles auprès des équipes techniques et convaincantes auprès des décideurs.

Annexe 1 : thèmes de la cybersécurité

Tiré de CyberEdu (www.cyberedu.fr), Guide pédagogique pour l'intégration de la cybersécurité dans les formations en informatique.

Compétences	Description
Fondamentaux	Historique (de la cybersécurité, de la sécurité des systèmes d'information), vocabulaire et principes fondamentaux de la cybersécurité, objectifs et propriétés de la cybersécurité, objectifs et profils des attaquants, typologie des attaques, vulnérabilités, menaces et contre-mesures, *malwares*, type et évolution, principes de fonctionnement, protection contre les *malwares*, analyse et gestion de risques, acteurs de la cybersécurité, sûreté de fonctionnement.
Sécurité de l'électronique et des architectures matérielles	Attaques physiques, conception de composants sécurisés, architecture des ordinateurs, systèmes embarqués, cartes à puce / éléments sécurisés.
Sécurité des systèmes d'exploitation	Principes, Windows, Unix / Linux / MacOS…, systèmes d'exploitation embarqués, mobiles, hyperviseurs et virtualisation, logiciels malveillants, rétro ingénierie, équipements et produits de sécurité (anti-virus, pare-feu…).
Sécurité des réseaux et protocoles	Modèle d'interconnexion des systèmes ouverts (ISO), types de réseaux (réseaux privés, locaux, réseaux sans fil, réseaux étendus…), protocoles et services, équipements et produits de sécurité réseaux (pare-feu, sondes, passerelles, réseaux privés virtuels, concentrateurs, TLS, commutateurs…).
Cryptologie	Fondamentaux des principes (symétrique, asymétrique, hachage), fondamentaux des services (chiffrement, signature…), ingénierie de la cryptologie, infrastructures de gestion de clés (IGC), certificats, implantations matérielles et logicielles de la cryptographie, algorithmes, modes…
Stéganographie et tatouage	Définitions, principes, applications.
Sécurité des bases de données	Sécurité des bases de données, problématique *Big Data*, *Open Data*, vulnérabilités des applications.
Contribution des architectures à la sécurité	Architectures produits, architectures systèmes, architectures applicatives
Aspects systèmes et systèmes de systèmes	Architectures produits, architectures systèmes, architectures applicatives, notion de systèmes complexes…
Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité	ISO2700x, ISO22301, plan de continuité d'activité (PCA), plan de reprise d'activité (PRA), standards industriels et métiers (PCI-DSS, W3C, IEEE, IETF, UIT, UEFI…), management de la qualité… guides (ANSSI, ENISA, NIST, SANS, NSA/CSS…). **Note** : pour ce domaine, une mise en pratique n'est pas

	obligatoire pour atteindre un niveau 2.
Normes, certifications, guides (organisationnel)	ISO2700x, ISO22301, plan de continuité d'activité (PCA), plan de reprise d'activité (PRA), standards industriels et métiers (PCI-DSS, W3C, IEEE, IETF, UIT, UEFI…), management de la qualité… guides (ANSSI, ENISA, NIST, SANS, NSA/CSS…).
Certifications et évaluations de produits	Schémas d'évaluation et de certification (Critères Communs (CC), Certification sécurité de premier niveau (CSPN), EMVCo, PCI…).
Politique de cybersécurité et SMSI	Organisation de la cybersécurité en France et à l'étranger, démarche d'analyse de risque, conception et mise en place d'une politique de sécurité des systèmes d'information (PSSI), supervision, contrôle audit, *Computer Emergency Response Team* (CERT), *Security Operating Center* (SOC), traitement des incidents de sécurité.
Droit et réglementation	Droit et réglementation en France, cas des opérateurs d'infrastructures vitales (OIV), droit et réglementation au niveau international.
Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité)	Compilation / interprétation et exécution, développement sécurisé, durcissement de code, analyse formelle, architecture logicielle, relecture, analyse statique de code, tests, environnement de développement.
Prise en compte de la sécurité dans les projets.	Méthodes de prise en compte de la sécurité dans les projets (documentation, cycle de vie, tests spécifiques, sécurité de l'environnement de développement, etc.), démarche d'homologation.
Cyberdéfense	Doctrine d'emploi, détection, agrégation, normalisation, corrélation, *reporting*, stockage, gestion de crise, communication, préservation de la preuve, réponse juridique, réaction, traitement, *Computer Security Incident Response Team* (CISRT), coordination, plan de continuité d'activité (PCA), plan de reprise d'activité (PRA), cyber résilience.
Analyse post-mortem (Forensic)	Analyse post-mortem, sûreté des logs.
Sécurité des systèmes spécifiques et émergents	SCADA, objets connectés, informatique industrielle, informatique embarquée… (préciser les thèmes en commentaire)
Systèmes spécifiques, informatique industrielle	SCADA, objets connectés...
Aspects sociaux et sociétaux	Ingénierie sociale, *phishing*, contournement de la politique de sécurité, ergonomie de la sécurité, hygiène informatique, géopolitique et intelligence économique.
Tests d'intrusion	Principes, droits, outils.
Sécurité physique	Contrôle d'accès, sécurité physique des systèmes d'information.
Sécurité des services externalisés	Sécurité dans l'informatique nébuleuse, l'infogérance, l'externalisation de services, etc. Prise en compte de la sécurité dans les contrats.
Problématique SSI en contexte spécifique	Informatique nébuleuse, mobilité, multi-niveaux, infogérance, externalisation.
Aspects économiques de la sécurité	Connaissance des éléments de coûts de la sécurité, par exemple : - ordres de grandeur du coût des

	interventions/prestations (experts, consultants, SOC…) selon la durée ; - ordres de grandeur du coût de la mise en conformité vis-à-vis de certains référentiels (27000, PCI-DSS…) ; - ordres de grandeur du coût de l'évaluation sécurité des produits de sécurité ; - ordres de grandeur du coût des produits de sécurité (investissements / fonctionnement). - impacts sociaux-économiques suite à une attaque réussie ; - impacts économiques suite à la divulgation de données personnelles ; - …

Annexe 2 : métiers de la sécurité

La liste des métiers utilisée est disponible sur www.ssi.gouv.fr (rubrique SecNum*edu*, document « 2017-06-20 Document-travail liste métiers SSI V3.pdf »). Elle est issue de travaux menés en 2017 avec des professionnels du domaine du numérique et de la sécurité du numérique. A la date de publication du présent dossier, cette liste est encore version préliminaire.

Annexe 3 : exemple de description d'un module

Le tableau ci-après présente un exemple du niveau de description qui devrait être publié dans la rubrique présentant le programme de formation labellisé.
Au minimum, il est attendu une description des objectifs du module, les thèmes abordés avec le volume de cours et de mise en pratique correspondants.

MODULE SYSTÈME UNIX/LINUX

Objectifs pédagogiques

À la fin du module, les étudiants doivent comprendre le fonctionnement des éléments constitutifs de base des systèmes d'exploitation (fichiers, processus, etc.), et être capable de saisir les enjeux de sécurité liés. En particulier, ils doivent pouvoir comprendre et analyser un avis de sécurité concernant une vulnérabilité système.

Description

Le module système a pour objectif de faire comprendre les principes de base d'un système d'exploitation, et d'expliquer les enjeux de sécurité liés à chacune des notions abordées.

La majorité des exemples pris en cours et les TP concerne les systèmes Unix et Linux en particulier. Un module séparé traite des spécificités du système d'exploitation Windows.

L'approche retenue est de partir des notions les plus abordables et concrètes (shell, fichiers) pour arriver vers les sujets plus complexes et plus bas niveau en fin de module (assembleur, format des exécutables).

Les cours et TP sont entrelacés sur une période de 7 mois, allant de début septembre à fin mars.

L'évaluation se fait sur la base des éléments suivants :

- un partiel en décembre (coefficient 1) qui porte sur les premiers modules (shell, fichiers et processus) et dont l'objectif est de vérifier l'assimilation de ces notions.
- un examen en mars (coefficient 1) qui porte sur l'ensemble du programme et vise en général à tester, au-delà des connaissances des notions décrites dans le module, les capacités de raisonnement des étudiants. Cela passe par exemple par l'analyse concrète d'un avis de sécurité récent.
- le grand oral (coefficient 2) évalue en partie le module système, soit au travers du sujet tiré au hasard (car les sujets à traiter par les étudiants peuvent relever du module système), soit dans la partie questions qui suit (puisqu'un enseignant du module système est présent au jury).

Pour information, une colle (un oral blanc) qui ne compte pas dans la note finale, est proposée aux étudiants début décembre.

Cours et pratique (TP, projets, études de cas…)	Cours	Pratique
Le *shell*, qui permet de dresser un aperçu d'un large ensemble de notions, tout en permettant à chacun d'apprivoiser cet outil, essentiel pour le reste du cours.	6h	6h
Les fichiers sont un vaste sujet qui va du fonctionnement d'un système de fichiers sous Unix aux problématiques de synchronisation (accès à une ressource partagée) en passant par l'étude des interfaces disponibles en C (les appels système d'une part et les fonctions de plus haut niveau d'autre part).	12h	12h
Les processus sont un concept essentiel dans la compréhension d'un système d'exploitation. Cette partie du cours traite de la représentation d'un processus au sein du noyau, d'ordonnancement, et présente là encore les interfaces disponibles en C pour gérer les processus.	6h	3h
La mémoire est traitée dans un cours long qui présente les mécanismes de gestion sur les architectures classiques (segmentation, pagination).	9h	6h
Les *threads* sont brièvement abordés, notamment pour mettre en avant les problèmes de synchronisation et pour insister sur la notion d'action atomique présenter les problématiques de *race conditions*.	3h	3h

Les *sockets* sont présentées suffisamment tard dans l'année pour que les étudiants aient vu les concepts TCP/IP dans le cours réseau. Ce cours leur permet d'aborder les mêmes concepts, du point de vue du système.	6h	3h
Les signaux (2 créneaux) sont un cours permettant d'illustrer une notion courante, mais complexe, des systèmes d'exploitation. Le caractère asynchrone des signaux les rend délicats à prendre en compte proprement.	6h	3h
L'assembleur est abordé pour présenter en quoi consistent concrètement les binaires exécutés sur un système. Les exemples reposent sur l'architecture x86, le système Linux et les compilateurs C classiques.	6h	
Les exécutables sont enfin présentés en fin de module. Le format ELF est disséqué pour présenter le fonctionnement concret du système, et en particulièrement la manière dont les mesures de sécurité peuvent être appliquées lors de la projection mémoire et de l'édition dynamique de liens.	6h	
OpenBSD : compilation du noyau, étude des appels systèmes et écriture d'un module noyau.		9h
Étude de cas : analyse d'une faille noyau.		3h
Écriture d'un serveur multi-clients.		3h
Totaux	**60h**	**51h**
Bibliographie		

Aucune lecture n'est nécessaire préalablement à ce module, mais voici quelques liens utiles pour les étudiants intéressés.

- Les systèmes d'exploitation par Andrew Tanenbaum est un ouvrage de référence. Les premiers chapitres présentent clairement les missions des systèmes d'exploitation, et proposent un historique des architectures et systèmes existants.
- oss-security (http://www.openwall.com/lists/oss-security/) est une liste de diffusion sur laquelle sont publiées des vulnérabilités et des correctifs de sécurité concernant des logiciels libres.
- Smashing Stack For Fun and Profit, l'article historique décrivant l'exploitation d'un dépassement de tampon (http://insecure.org/stf/smashstack.html).