# Référentiel d'activités, de compétences et d'évaluation

# Expert en gouvernance de la sécurité des réseaux et des systèmes (MS)

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)

« *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

Les étudiants en situation de handicap peuvent bénéficier d'un aménagement de leurs conditions de formation et d'examen.

**Les aménagements** dépendent de la situation de handicap (maladie chronique ou invalidante, déficience sensorielle, physique, psychique, cognitive ou mentale) et sont décidées par le Responsable de la formation Mastère Spécialisé® en accord avec le Référent handicap et la Direction.

Par exemple :

- Troubles « dys » : temps majoré, autorisation d'utiliser un ordinateur avec applications de correction pour les examens écrits
- Troubles « moteurs » ou « visuels » : facilitation de l'accès aux lieux d'examen et salles de TP, adaptation du poste avec utilisation de matériels plus appropriés (quand cela est possible)
- Maladies invalidantes : autorisation de sortie pendant l'épreuve, temps majoré

Pour plus d'information sur l'Inclusion du Handicap à Télécom SudParis : https://www.telecom-sudparis.eu/ecole/handicap/

**Bloc n°1 – Analyser et traiter les problématiques de cybersécurité spécifiques aux Opérateurs de Services Essentiels** [1]

| REFERENTIEL D'ACTIVITES | REFERENTIEL DE COMPETENCES | REFERENTIEL D'EVALUATION | |
|---|---|---|---|
| | | MODALITÉS D'ÉVALUATION | CRITÈRES D'ÉVALUATION |
| • Étude des métiers de la cybersécurité, en particulier au sein des Opérateurs de Services Essentiels<br>• Identification des problématiques juridiques propres à la pratique des métiers la cybersécurité<br>• Élaboration et mise en place de solutions techniques répondant aux besoins d'un Opérateur de Service Essentiel | • Analyser les besoins en cybersécurité des systèmes industriels et des Opérateurs de Services Essentiels dans le cadre de la loi du 26 février 2018 transposant la directive NIS [3] au droit français et dans le respect des obligations requises par l'ANSSI[2]<br>• Proposer et déployer une solution technique répondant aux besoins et aux contraintes d'un Opérateur de Service Essentiel, c'est-à-dire conforme aux 23 règles de sécurité à appliquer dans les 4 domaines que sont : la gouvernance de la sécurité des réseaux et systèmes d'information, la protection des réseaux et systèmes d'information, la défense des réseaux et systèmes d'information et la résilience des activités.<br>• Identifier les réglementations des cadres juridiques français et européen qui s'appliquent dans des situations concrètes liées à la cybersécurité, notamment au sein des Opérateurs de Services Essentiels | **Étude de cas** :<br>• portant sur une problématique technique spécifique aux Opérateurs de Services Essentiels<br>• avec comme objectif de mettre en œuvre des mécanismes de sécurité spécifiques au contexte des Opérateurs de Services Essentiels afin de prendre en compte des contraintes telles que la limitation de budget ou de puissance de calcul<br>• donnant lieu à l'élaboration et à la remise d'un rapport décrivant les solutions techniques proposées et argumentant sur leur choix<br>• à réaliser en binôme ou trinôme<br><br>**Étude de cas + soutenance**<br>• portant sur des problématiques techniques et juridiques rencontrées par des entreprises<br>• avec pour objectif de proposer une démarche d'analyse des textes réglementaires s'appliquant à des cas de litiges ou d'infractions dans le domaine de la sécurité des systèmes d'information<br>• avec rédaction d'un rapport et présentation orale de la démarche d'analyse des situations et de la recherche des règlementations à appliquer<br>• à réaliser en binôme ou trinôme | **Pour les études de cas :**<br>• Le contenu et la structure du rapport sont en adéquation avec la problématique<br>• La rédaction du rapport est organisée et un effort de synthèse est fait<br>• L'analyse des besoins en cybersécurité et des contraintes est menée avec méthode et rigueur<br>• Des réponses et des solutions pertinentes sont proposées pour répondre à la problématique<br>• Les règlementations à respecter pour chaque problématique sont identifiées<br>• Le temps et les responsabilités sont répartis avec efficience entre les membres du groupe<br>• La présentation est faite avec aisance<br>• Le groupe est réactif aux questions de l'auditoire et du jury de soutenance, le cas échéant<br>• Le rapport et la soutenance démontrent une compréhension de l'écosystème européen de la cybersécurité<br><br>**Pour le rapport :**<br>• Le rapport présente une cartographie de l'état de l'art et des pratiques opérationnelles de la cybersécurité des OSE, construite à partir des informations recueillies lors des visites d'entreprises et des conférences<br>• Les rôles et missions des différents acteurs de la cybersécurité sont identifiés et qualifiés, les types d'organisation sont caractérisés, le handicap pris en compte (ex : couleurs adaptées aux déficiences visuelles) |

| | | | |
|---|---|---|---|
| | • Déterminer le rôle et les missions des acteurs cybersécurité de l'entreprise pour organiser efficacement la gestion et la mise en œuvre de solutions, en tenant compte de personnel avec un handicap | **Rapport écrit**<br>• visant à cartographier les métiers et les pratiques de la cybersécurité au sein des opérateurs de services essentiels<br>• suite à des visites d'entreprises et au suivi d'un cycle de conférences<br>• à réaliser individuellement | |

(1) Un OSE est un opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société (cf. définition de l'ANSSI : https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/.

(2) l'ANSSI est l'Agence Nationale de la Sécurité des Systèmes d'Information, c'est l'autorité désignée pour la France pour accompagner les OSE dans la mise en œuvre de la réglementation, aux côtés des ministères concernés.

(3) la NIS est la directive Network and Information System Security adoptée par les institutions européennes le 6 juillet 2016 pour assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne

**Bloc n°2 –Conduire un projet de cybersécurité**

| REFERENTIEL D'ACTIVITES | REFERENTIEL DE COMPETENCES | REFERENTIEL D'EVALUATION | |
|---|---|---|---|
| | | MODALITÉS D'ÉVALUATION | CRITÈRES D'ÉVALUATION |
| • Conception et déploiement d'une solution répondant à un cahier des charges, portant sur un sujet de cybersécurité<br>• Rédaction d'un rapport synthétisant les choix et les réalisations<br>• Réalisation et déploiement d'un prototype de la solution retenue | • Établir et analyser l'état de l'art associé à une problématique de cybersécurité afin d'en déterminer les enjeux et de concevoir une contribution scientifique permettant d'y répondre<br>• Concevoir un prototype répondant à un cahier des charges et permettant de traiter la problématique identifiée en argumentant les choix réalisés<br>• Réaliser et déployer un prototype de la solution permettant d'évaluer sa faisabilité technique afin de s'assurer que la solution réponde fonctionnellement au cahier des charges | **Un projet est à mener sur un sujet de cybersécurité** choisi parmi des propositions d'industriels ou de chercheurs<br>Réalisation :<br>• en binôme<br>• tutoré par un enseignant-chercheur.<br>Objectifs :<br>• Identifier une problématique associée au sujet<br>• Établir et analyser l'état de l'art associé à cette problématique<br>• Élaborer une réponse à un cahier des charges<br>• Argumenter les choix réalisés<br>• Concevoir et réaliser un prototype répondant à cette problématique<br>Les attendus :<br>• un rapport écrit décrivant la problématique, l'état de l'art et la solution proposée<br>• une soutenance orale décrivant méthodiquement et synthétiquement la solution proposée suivie d'une séance de questions-réponses avec le jury | • Le rapport est structuré et clair<br>• La problématique associée au sujet au sujet est correctement identifiée<br>• L'analyse des pratiques en vigueur est réalisée<br>• La réponse au cahier de charges est élaborée et présentée, les choix sont argumentés<br>• La solution proposée est pertinente par rapport au cahier des charges<br>• La méthodologie et les techniques de conduite de projet sont correctement mises en œuvre<br>• Le prototype présenté répond au cahier des charges et à la problématique<br>• La présentation orale est claire<br>• Le binôme est réactif aux questions de l'auditoire et du jury<br>• Les réponses aux questions du jury sont de qualité |

**Bloc n°3 – Analyser les menaces réseau et les mécanismes de sécurisation**

| REFERENTIEL D'ACTIVITES | REFERENTIEL DE COMPETENCES | REFERENTIEL D'EVALUATION | |
|---|---|---|---|
| | | MODALITÉS D'ÉVALUATION | CRITÈRES D'ÉVALUATION |
| • Identification des vulnérabilités et des mécanismes de sécurité réseaux<br>• Mise en place de mécanismes de filtrage dans le cadre d'une politique de sécurité | • Identifier les différents types d'attaques portant sur le réseau ainsi que les mécanismes de sécurité permettant de faire face à chacun de ces types d'attaques afin de mettre en œuvre les mécanismes de sécurité les plus efficaces face aux menaces identifiées<br>• Mettre en œuvre les règles de filtrage appropriées afin de bloquer des attaques réseau sans entraver le fonctionnement des applications<br>• Configurer et tester un pare-feu nouvelle génération (NGFW) afin de mettre en place une politique de sécurité qui vise à protéger un réseau interne tout en filtrant l'accès à certains services pour les utilisateurs de ce réseau interne | **Évaluations écrites**<br>• examens individuels en présentiel<br>• dont l'objectif est de vérifier l'acquisition des fondamentaux des réseaux, leur sécurisation et les mécanismes de filtrage<br><br>**Travaux pratiques**<br>Sur un poste informatique disposant d'interfaces réseau, le candidat doit :<br>• Identifier les modèles d'attaquants sur le réseau<br>• Mettre en œuvre des mécanismes de filtrage prenant en compte une politique de sécurité<br>Les travaux sont à réaliser individuellement sur un temps donné | **Pour les évaluations écrites**<br>• Les concepts et techniques de base des réseaux IP et de leur sécurisation sont acquis<br>• L'utilité respective des différents mécanismes de filtrage est acquise et leur fonctionnement assimilé<br><br>**Pour les travaux pratiques**<br>• Les réponses données sont précises et de qualité, les modèles d'attaquants bien identifiés<br>• Les techniques de filtrage sont correctement mises en application, les mécanismes de sécurisation proposés sont pertinents par rapport à la politique de sécurité retenue |

**Bloc n°4 –Analyser les vulnérabilités et sécuriser des applications informatiques**

| REFERENTIEL D'ACTIVITES | REFERENTIEL DE COMPETENCES | REFERENTIEL D'EVALUATION | |
|---|---|---|---|
| | | MODALITÉS D'ÉVALUATION | CRITÈRES D'ÉVALUATION |
| • Analyse des vulnérabilités d'applications informatiques<br>• Mise en œuvre de méthodologies de développement d'applications informatiques sécurisées | • Analyser les vulnérabilités classiques des systèmes d'exploitation et des applications informatiques, identifier les solutions permettant d'y remédier<br>• Mettre en œuvre des mécanismes de contrôle d'accès et d'isolation de fichiers sur un système Unix afin d'empêcher des attaques en confidentialité et en intégrité sur ces fichiers<br>• Analyser une vulnérabilité du noyau Linux pouvant conduire à une élévation de privilèges afin de déterminer les correctifs à apporter | **Évaluation écrite**<br>• examen individuel en présentiel<br>• dont l'objectif est de vérifier l'acquisition des fondamentaux des systèmes et de leur sécurisation<br><br>**Étude de cas**<br>• Examen écrit en présentiel<br>• portant sur l'analyse d'une vulnérabilité d'un système d'exploitation donné<br>• et donnant lieu à un compte rendu<br><br>**Travaux pratiques**<br>Sur un poste disposant d'un système d'exploitation Linux ou Windows, les candidats doivent :<br>• analyser les vulnérabilités des applications informatiques de l'entreprise<br>• mettre en œuvre de techniques de sécurisation des applications informatiques<br>• mettre en œuvre les mécanismes de sécurité des systèmes d'exploitation | **Pour l'évaluation écrite :**<br>• Les notions fondamentales en systèmes Linux et Windows sont acquises<br>• Les réponses proposées montrent une appropriation des notions de sécurité sur les systèmes d'exploitation<br><br>**Pour l'étude de cas :**<br>• L'analyse de vulnérabilité des applications informatiques est exhaustive et pertinente<br>• Le compte-rendu de l'étude de cas est organisé dans sa structure et clair dans sa rédaction<br><br>**Pour les travaux pratiques :**<br>• L'analyse de vulnérabilités des applications informatiques de l'entreprise est menée de façon pertinente<br>• Les techniques de sécurisation sont appliquées avec précision<br>• Les mécanismes de sécurisation mis en œuvre sont pertinents par rapport aux vulnérabilités des applications |

**Bloc n°5 – Auditer un système d'information**

| REFERENTIEL D'ACTIVITES | REFERENTIEL DE COMPETENCES | REFERENTIEL D'EVALUATION | |
|---|---|---|---|
| | | MODALITÉS D'ÉVALUATION | CRITÈRES D'ÉVALUATION |
| • Analyse des risques d'un système d'information<br>• Réalisation d'attaques sur une application Web<br>• Identification de vulnérabilités Web<br>• Détection d'intrusion | • Identifier les risques, découvrir les vulnérabilités afin d'évaluer la sécurité du système d'information<br>• Appliquer la démarche d'analyse de risque EBIOS et employer les outils d'audit d'un réseau afin de professionnaliser la démarche d'audit d'un SI<br>• Concevoir des règles pour la détection d'intrusion dans le contexte d'un centre de sécurité opérationnelle (SOC) afin de réduire le niveau d'exposition des SI aux risques externes comme internes<br>• Élaborer une méthodologie de réponse à incident pour faire face à des intrusions réelles afin de plus rapidement et efficacement réagir en cas d'attaques<br>• Auditer une application Web et rédiger un rapport d'audit afin d'identifier les vulnérabilités web | **Évaluation écrite** :<br>• examen individuel en présentiel<br>• dont l'objectif et de vérifier l'acquisition des techniques d'audit et d'identification de vulnérabilités d'un système d'information<br><br>**Étude de cas** :<br>• à rendre sous la forme d'un compte-rendu<br>• portant sur l'analyse forensique d'une intrusion sur un système informatique ou industriel simple mais réaliste<br><br>**Mise en situation pratique** :<br>En salle informatique, sur une application Web réaliste (de type Wiki), le candidat doit :<br>• réaliser des attaques sur l'application Web<br>• proposer des solutions pour renforcer la sécurité de l'application web<br>• rédiger un compte-rendu | **Pour l'évaluations écrite :**<br>• Les techniques d'audit d'un système d'information sont acquises<br><br>**Pour l'étude de cas :**<br>• L'analyse forensique de l'intrusion est exhaustive et pertinente<br>• Le compte-rendu de l'analyse forensique est bien organisé dans sa structure et clair dans son contenu<br><br>**Pour la mise en situation pratique :**<br>• Les attaques applicatives réalisées sont présentées dans le compte rendu de façon claire et professionnelle<br>• Les solutions proposées pour renforcer la sécurité de l'application web sont techniquement précises<br>• Le compte-rendu est clair et bien organisé |

**Bloc n°6 – Déployer des services d'authentification, de chiffrement et de protection de la vie privée dans un système d'information**

| REFERENTIEL D'ACTIVITES | REFERENTIEL DE COMPETENCES | REFERENTIEL D'EVALUATION | |
|---|---|---|---|
| | | MODALITÉS D'ÉVALUATION | CRITÈRES D'ÉVALUATION |
| • Analyse et mise en œuvre de plusieurs mécanismes de chiffrement<br>• Analyse et déploiement de protocoles d'authentification<br>• Déploiement de VPN (réseau privé virtuel) | • Établir les besoins en chiffrement et en authentification dans l'architecture d'un système d'information afin de garantir la confidentialité des données sensibles et de certifier l'identité des utilisateurs de manière robuste<br>• Générer des certificats numériques X.509 et déployer une infrastructure à clés publiques (PKI) afin de mettre en œuvre des connexions sécurisées en HTTPS<br>• Configurer et déployer un réseau privé virtuel (VPN) IPsec entre deux sites distants afin de déterminer les options adéquates à utiliser pour répondre aux différents besoins, notamment en confidentialité et en authentification<br>• Mettre en œuvre des mécanismes d'anonymisation des bases de données afin d'assurer la conformité avec le RGPD | **Évaluation écrite** :<br>• Examen individuel en présentiel<br>• Dont l'objectif et de vérifier la maîtrise des techniques cryptographiques et d'anonymisation des bases de données<br><br>**Travaux pratiques** :<br>En salle informatique équipée notamment de boîtiers Stormshield, librairies OpenSSL et de VPNs, le candidat doit :<br>• mettre en œuvre des mécanismes de sécurisation répondant à un cahier des charges<br>• rédiger des comptes rendus | **Pour l'évaluation écrite :**<br>• Les mécanismes mathématiques et les algorithmes de cryptographie, leurs protocoles et applications ainsi que les techniques d'anonymisation des bases de données sont correctement mis en œuvre<br><br>**Pour les travaux pratiques :**<br>• Les mécanismes de sécurisation mis en œuvre au regard du cahier des charges sont pertinents<br>• La mise en œuvre des mécanismes proposés est techniquement précise et efficace<br>• Les comptes rendus des travaux réalisés sont bien organisés et clairs dans leur rédaction |

**Modalités de certification :**

L’accès à la certification professionnelle est possible soit par la formation, soit par la VAE.

Pour obtenir la certification, les candidats issus de la formation initiale ou continue doivent capitaliser la totalité des blocs de compétences et valider la thèse professionnelle. Sans validation de la thèse professionnelle, les candidats n'obtiennent pas la certification.

La validation de la thèse professionnelle s’obtient par :

- la réalisation d’une mission de cybersécurité en entreprise (de 5 mois équivalents temps plein réalisée après la formation) ;
- la rédaction et la soutenance orale de la thèse basée sur la mission de cybersécurité réalisée

Pour obtenir la certification, les candidats de la voie VAE doivent valider la totalité des blocs de compétences et fournir un rapport d’activité de développement sur plusieurs mois d’une solution technique en entreprise, attestant de leur capacité à concevoir une solution répondant à un cahier des charges spécifique à l’entreprise et à en réaliser un prototype.