RÉFÉRENTIEL D'ACTIVITÉS, COMPÉTENCES ET ÉVALUATION
EXPERT(E) EN SÉCURITÉ DES DÉVELOPPEMENTS INFORMATIQUES

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.* »

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Auditer la sécurité des applications d'un système d'information **A1.1 Analyse des risques informatiques** ● Définition d'un plan d'audit ● Choix de méthodologie d'audit ● Recherche de failles et non conformités ● Identification des risques et menaces ● Définition des objectifs de sécurité **A1.2. Définition et mise en oeuvre d'un plan d'action** ● Analyse des résultats de l'audit ● Proposition de mesures de sécurité pour renforcer des applications ● Définition d'un plan d'action	**C1.** Définir un plan d'audit adapté en termes de moyens, ressources, organisation et contraintes réglementaires, par l'application d'une méthodologie d'audit, afin de déterminer précisément les failles et non conformités des applications d'un système d'information. **C2.** Conduire une analyse de sécurité de l'information et des données des applications d'un système d'information, en s'appuyant sur un plan d'audit, afin d'identifier les risques et menaces et d'en dégager les causes. **C3.** Analyser les écarts au regard des procédures définis au plan d'audit en rédigeant un rapport d'audit, afin de déterminer le plan d'action permettant de renforcer la sécurité des applications et du SI.	**M1. Etude de cas faisant l'objet d'une présentation orale (C1 à C5)** L'étude de cas porte sur une organisation qui souhaite se préparer à la certification CSPN de l'ANSSI en s'appuyant sur une méthodologie d'analyse de risque afin de qualifier les enjeux, les menaces des applications du SI Le candidat a 4 heures pour préparer un compte rendu écrit présentant le résultat de ces analyses et ses propositions d'amélioration, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre :	C1. Un plan de test est présenté C2. Les preuves d'audit sont fournies et analysées C2. Une méthode d'analyse de risque est utilisée (méthode EBIOS RM,...) C2. Les contraintes d'ordre technique, organisationnel, juridique et réglementaire pouvant impacter la SSI sont recensées C3. Les mesures de sécurité des architectures logicielles et applicatives existantes sont analysées C4. La conformité de l'application avec les critères de sécurité est démontrée

● Suivi de la résolution des failles ● Mise en conformité par rapport aux certifications de l'ANSSI ● Formalisation de l'ensemble des preuves nécessaires à l'audit de certification	**C4.** Établir un plan d'action comportant les mesures de sécurité techniques et organisationnelles correctives et préventives, afin de corriger les non conformités et remédier aux failles de sécurité des applications et de leurs intéractions avec le système d'information. **C5.** Préparer l'entreprise à la certification en sécurité de l'information, par une démarche d'accréditation à partir d'une norme de certification, afin de rassurer les clients et les partenaires.	- l'identification des menaces vulnérabilité - l'analyse des risques en sécurité du système d'information comprenant l'évaluation des mesures de sécurité mises en place ; - le degré de conformité réglementaire et juridique de l'organisation au regard de la certification cible ; - l'évaluation des propositions de traitement des non conformités ; - un planning incluant la proposition de pistes d'amélioration pour renforcer la sécurité des applications en production.	C4. Un plan de mesure de traitement est rédigé et argumenté selon les meilleures pratiques de l'Open Web Application Security Project (OWASP) C5. Les preuves et documents nécessaires à l'auditeur sont produits
<u>Mettre en place une politique de sécurisation des applications</u> **A2.1. Elaboration d'une politique de sécurité des applications** ● Analyse des protocoles existants ● Entretiens avec les équipes techniques ● Définition des règles de conception, de codage et de tests par le Security By Design ● Analyse et sélection de logiciels d'automatisation des tests ● Création de tâches automatisées de sécurisation des données ● Mise en place de protocoles de sécurité	**C6.** Définir une politique de sécurité des applications du système d'information adaptée à l'activité de l'entreprise, à l'aide des différents acteurs et procédures existantes, afin de répondre à ses enjeux. **C7.** Mettre en place un référentiel "développeur sécurité" à destination des développeurs, en définissant des protocoles de développement et de tests issus du Security by Design, afin d'élaborer des bonnes pratiques par l'utilisation des outils (framework, composants…) les plus pertinents.	**M2. Etude de cas faisant l'objet d'une présentation orale (C6 à C11)** L'étude de cas porte sur une entreprise qui souhaite former ses développeurs à travers des ateliers de développements sécurisés et notamment sur le Security by Design. Il dispose des résultats d'une enquête pour connaître le niveau de chacun des collaborateurs, la cartographie des applications du SI et les résultats des audits de	C6. Les procédures définissent des routines de sécurité et des protocoles comme les tests réguliers. C6. Les préconisations sont en cohérence avec les contraintes de sécurité de l'organisation C7. Le référentiel respecte les règles du Security By design C8. Un outil de veille en sécurité personnalisé est accessible en ligne

A2.2. Veille sur la sécurisation des applications ● Définition des objectifs de veille ● Identification des sources d'information ● Collecte et organisation ● Analyse des informations et de leur impact sur la politique de sécurité	**C8.** Evaluer les dernières vulnérabilités connues et les opportunités technologiques, en organisant une veille axée juridique, réglementaire et technique, afin de répondre aux enjeux de sécurité de l'entreprise.	sécurité et des actions mises en place par l'entreprise. Le candidat a 4 heures pour préparer un support de formation sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre : - Le rappel des objectifs de sécurité de l'entreprise - Les principaux protocoles de développement du référentiel "développeur sécurité" - Les étapes de la démarche Security By Design appliquée à l'organisation - Les dernières failles connues et les résolutions - Les outils permettant d'automatiser les tests de sécurité à chaque étape d'un projet - Une proposition de planning détaillant les thématiques et objectifs des prochains ateliers à venir	C8. Les informations les plus pertinentes sont identifiées et priorisées
A2.3. Diffusion d'une culture de sécurité et de prévention ● Identification des services concernés ● Evaluation des niveaux de compétences des équipes en sécurité informatique ● Adaptation des messages aux cas de risque sécurité rencontrés et aux équipes formées ● Mise en place d'actions de sensibilisation aux risques et menaces ● Organisation d'ateliers sur les nouvelles procédures de sécurité ● Inclusion handicap	**C9.** Analyser les compétences des équipes en matière de sécurité des applications, au moyen de questionnaires et d'entretiens, afin de concevoir et mettre en place un plan de formation. **C10.** Sensibiliser et former les équipes, à un niveau approprié, aux meilleures pratiques de sécurité, risque et conformité à travers un plan de formation, afin d'améliorer leur niveau de compréhension des problématiques de sécurité informatique. **C11.** Utiliser le référentiel général d'amélioration de l'accessibilité (RGAA), afin d'adapter le formation interne de la sécurité aux personnes handicapées.		C9. L'analyse des enquêtes de niveau est synthétisée C10. Les recommandations des organismes de références (ANSSI, OWAST…) sont rappelées C10. Les notions d'identité numérique, certificats, HTTPS, SSL / TLS, typologie d'attaque, cryptographie, et la connaissance du risque et du cadre légal sont expliquées dans le powerpoint C11. Une proposition spécifique est formulée pour faciliter la prise en compte d'une personne en situation de handicap dans un contexte de crise

<u>Concevoir et développer une application sécurisée</u> **A3.1. Conception de l'architecture d'une application sécurisée** ● Evaluation des besoins de sécurisation ● Modélisation d'une architecture logicielle ● Définition des outils de sécurisation des environnements cibles (Cloud,...) ● Définition des fonctionnalités matérielles et applicatives de sécurité (routeur,...) ● Automatisation du processus de sécurisation du code et intégration au sein du cycle de développement ● Mise en place d'un pare-feu applicatif ● Rédaction des spécifications techniques **A3.2. Développement des composants sécurisés** ● Développement des fonctionnalités de sécurité ● Implémentation des composants externes sécurisés	**C12.** Modéliser une architecture applicative et technique sécurisée, en s'appuyant sur une analyse des besoins et des spécificités du SI, afin de répondre aux exigences de sécurité durant tout le cycle de vie de l'application. **C13.** Structurer les choix technologiques et méthodologiques, en sélectionnant les solutions adaptées, afin de qualifier leur intégrations dans l'environnement de production et minimiser surface d'attaque à laquelle l'application va être exposée. **C14.** Définir l'automatisation des tests, par la mise en oeuvre des processus et outils adaptés aux tests techniques et fonctionnels automatisés, afin de garantir l'intégrité au niveau applicatif et des données. **C15.** Rédiger les spécifications techniques des attentes en matière d'architecture de solutions de sécurité, en vue de la rédaction du cahier des charges, afin de permettre la réalisation de l'application par les équipes de développement. **C16.** Coder des composants web, logiciel ou mobile conformes aux spécifications fonctionnelles et techniques, de sécurité et de performance, afin tester leur robustesse à travers des outils de tests. **C17.** Intégrer des composants technologiques externes, en appliquant des règles de conception des fonctionnalités définies, afin de	**M3. Etude de cas faisant l'objet d'une présentation orale (C12 à C17)** L'étude de cas porte sur la conception d'une nouvelle fonctionnalité sécurisée (web et mobile) au sein d'une application SAAS d'un éditeur de logiciel. Il est mis à disposition un cahier des charges et un environnement où le candidat peut programmer sur l'application et réaliser les tests. Le candidat a 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre : - Modélisation de l'application - Choix des composants utilisés et leurs justifications - La procédure de tests à mener - Les fichiers sources des développements front et back programmés - Le schéma de la base de données - Le lien vers le rendu fonctionnel de l'application	C12. Les problématiques à traiter dans un contexte de sécurité sont comprises C12. Les emplacements des pares-feux de type web application firewall (waf) les plus adaptés à la prévention des intrusions sont identifiés C13. Les choix techniques et technologiques des projets IT et métiers respectent les exigences de sécurité de l'organisation (accessibilité et performance) C13. Les exigences de sécurisation applicables aux différents constituants de son architecture ou aux outils permettant de la produire sont mises en œuvre (pare-feu,...) C14. Les hypothèses de sécurité relatives à l'environnement de son architecture sont énoncées et prises en compte dans sa conception. C15. Les procédures d'authentification et d'autorisation sont intégrées, afin de s'assurer que seuls les utilisateurs autorisés peuvent accéder à l'application C15. Les activités autorisées et interdites sont définies.

	mettre en œuvre une architecture applicative sécurisée.		C15. Une gestion sécurisée des données tout au long de leur cycle de vie est démontrée dans le respect des lois en vigueur C16. Des langages informatiques web et logiciel sont mobilisés (PHP, JS, Python, Java...) C16. Les standards de développement sont respectés C16. Les 4 critères de sécurité (disponibilité, confidentialité, intégrité et traçabilité) sont respectés C17. Les risques possibles sont identifiés (robustesse face à la résistance aux attaques identifiées) C17. Les composants externes sont connus, éprouvés et testés par un organisme ou une communauté (si open source)
<u>Piloter un projet d'application sécurisée</u> **A4.1. Pilotage d'un projet de sécurisation** ● Recueil des objectifs du projet ● Rédaction des cahiers des charges conformes aux besoins et aux orientations stratégiques définies ● Suivi du déroulement du projet à travers le framework Secure Software Development Life Cycle	**C18.** Concevoir un projet de développement sécurisé, par l'application d'une méthode de gestion de projet agile, afin de gérer les besoins de sécurité lors du développement d'une application, afin de minimiser les attaques et garantir la sécurité des programmes. **C19.** Planifier les différentes activités à réaliser à travers des outils collaboratifs nécessaires à la collaboration et au partage d'informations, afin	**M4. Etude de cas faisant l'objet d'une présentation orale (C18 à C24)** L'étude de cas porte sur les tests lors de la finalisation d'un projet d'évolution d'application (nouvelles fonctionnalités) avant son déploiement, sur la base de programmes informatiques développés.	C18. Les nouveaux développements n'impactent pas ceux qui ont déjà été faits. C18. Une méthode agile est mobilisée C19. Un plan de projet de développement sécurisé est présenté, intégrant les meilleures pratiques de Dev Sec Ops

● Sécurisation du code dès la conception à travers les pratiques DevSecOps **A4.2. Management d'une équipe projet** ● Accompagnement des équipes de développement vers l'appropriation des nouvelles procédures de sécurité et bonnes pratiques de développement ● Contrôle des composants implémentés et des librairies utilisées ● Aménagement spécifique du projet pour les collaborateurs en situation de handicap **A4.3. Encadrement et contrôle des tests de sécurité** ● Sélection des outils ● Mener des tests fonctionnels et techniques ● Réalisation d'une analyse statique ● Lancement des tests automatisés ● Protection cross-site scripting ● Réalisation d'un pentest ● Analyse des résultats des tests et du scoring	d'assurer la bonne diffusion des informations liées à la sécurité auprès de l'ensemble des équipes de développement. **C20.** Coordonner et motiver les équipes pour implémenter de manière appropriée les fonctionnalités spécifiées, afin de contrôler que les règles de codage préalablement définie sont appliquées dans le cycle de vie du projet de manière pertinente. **C21.** Mettre à disposition des outils et des infrastructures de développement pour optimiser et industrialiser les travaux des équipes de développement, afin d'atteindre les objectifs du projet. **C22.** Accompagner une personne en situation de handicap afin de faciliter son intégration dans l'équipe et dans son environnement de travail. **C23.** Mener une analyse statique (analyse de code et de dépendance) et dynamique (pentest) des développements réalisés à travers des outils sélectionnés et automatisés, afin de tester la sécurité de l'application. **C24.** Analyser les ambiguïtés non détectées lors des tests et corriger les failles détectées, afin de remédier aux attaques avant le déploiement de l'application.	Les candidats travaillent en groupe et ont 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). Au sein d'une équipe projet, les candidats doivent : - Présenter la répartition des tâches au sein de l'équipe - Présenter le fonctionnement agile de l'équipe - Faire une revue de code mutuelle et présenter les résultats - Déployer l'application sur un environnement de tests - Mener les tests automatiques de vulnérabilités par l'utilisation de l'outils de scan (SonarQube) - Mener les résultats des tests statique et dynamique, limites et hors limites (injection, pentest) - Analyser les rapport des tests automatisés générés par ces outils (résistance aux attaques identifiée - Présenter la synthèse des failles et leur scoring - Reformuler les spécifications fonctionnelles et techniques des composants testés - Présenter un planning agile à jour présentant les correctifs à mettre en œuvre avant déploiement.	C20. Des techniques de management sont appliquées C21. L'application est disponible sur l'environnement de développement C22. Une proposition spécifique est formulée pour faciliter la prise en compte d'une personne en situation de handicap dans un contexte de crise C23. une revue de code est présentée, corrigeant les vulnérabilités d'un logiciel liée à une programmation non sécurisée C23. Les tests sur la qualité du code sont automatisés C23. Une revue de sécurité est présentée (droits honorés,...) C23.Un test à données aléatoires est mené C24. Les failles de sécurité connues (issues du standard OWAST) sont analysées (score) et rapprochées (CVE) C24. Les réponses de l'application sur les valeurs ou entrées inattendues sont relevées C24. La qualité du code permet d'assurer la pérennité de la vitesse de développement des fonctionnalités et la non-régression du produit au fur et à mesure des mises en production

		Chaque candidat se verra attribuer une note individuelle, s'appuyant sur la présentation qu'il fera du travail collectif pendant cette présentation orale.	

<u>Déployer et maintenir la sécurisation des applications d'un SI</u> **A5.1. Pilotage du déploiement d'une application dans un environnement sécurisé** ● Création d'environnement de tests, pré-production et production virtualisées, conteneurisées ● Déploiement des chaînes de développement et de leur paramétrage ● Management de services Cloud managés ● Déploiement de l'application sur l'environnement cible ● Réalisation des tests de bout en bout ● Mise en place des pare-feux **A5.2. Contrôle et protection des applications** ● Suivi en continu des mesures de sécurité via des outils de monitoring applicatifs, système et réseaux ● Industrialisation et automatisation des tests de sécurité des applications	**C25**. Déployer une architecture technique sécurisée, en appliquant les méthodes et outils définis par la politique de sécurité de l'entreprise, afin de garantir le niveau de sécurité et fonctionnement opérationnel des applications. **C26**. Superviser la sécurité des applications en mettant œuvre des solutions techniques de protection automatisées, afin de protéger les données sensibles de l'application. **C27.** Déployer des solutions de monitoring pour être alerté de l'apparition des anomalies de sécurité dans le système, afin d'établir une surveillance la plus complète des évènements et limiter l'impact d'un incident de sécurité.	**M5. Etude de cas faisant l'objet d'une présentation orale (C25 à C32)** L'étude de cas porte sur l'analyse d'un incident sur une application en production dans le cloud, remontée par une équipe Ops. Le candidat a 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre : - Le rapport de scan de vulnérabilités - Identifier le mode opératoire des hackers - Analyser les logs et outils de monitoring (requêtes web) - Vérification des versions des composants	C25. Des outils et plateformes CI/CD (Kubernetes, Terraform) sont mis en place C25. Le déploiement de l'application sur différents environnements (Dev, QA technique) est réalisé C26. Le cycle de vie des certificats est géré C26. Un pare-feu d'applications est appliqué C27. Les paquets de données considérés comme dangereux sont bloqués C27. Des tests de charge sont réalisés pour vérifier que la charge peut être absorbée

● Accompagnement de l'intégration de nouvelles stacks applicatives dans la chaîne DevSecOps **A5.3. Remédiation des incidents** ● Anticipation des comportements d'attaques ● Réaction aux attaques de sécurité en suivant les procédures établies ● Gestion des incidents et suivi de leurs traitements avec toutes les parties prenantes ● Analyse des incidents de sécurité ● Identification des plans d'action et encadrement du suivi ● Mise à jour des politiques de sécurité	**C28.** Assurer la continuité d'activité des applications en concevant un plan de reprise d'activité, en s'appuyant sur la norme ISO, afin d'automatiser le traitement des incidents. **C29.** Suivre l'obsolescence et maintenir à jour les composants et de stacks logiciels devenus vulnérables, en installant les patchs correctifs, afin de corriger les menaces et failles de sécurité et maintenir l'intégrité des applications. **C30.** Définir un plan de remédiation permettant de réagir aux incidents de sécurité , en s'appuyant sur des mesures de contournements et des solutions techniques précédemment identifiées, afin de pallier à de nouveaux incidents de sécurité et en réduire les impacts. **C31.** Mener une investigation technico légale , en s'appuyant sur les outils adéquats afin d'identifier la cause des incidents de sécurité et d'y apporter des solutions. **C32**. Évaluer la performance des mesures de sécurité en place, à travers la définition, la mise en œuvre et le pilotage des indicateurs clés de sécurité, afin d'assurer l'amélioration continue des dispositifs de sécurité et mettre à jour les procédures.	- Vérification des droits et accès utilisateurs ont uniquement accès aux données - Définir un plan pour remédier aux failles (montée de version…) - Définir la répartition des tâches à exécuter par l'équipe Ops - Contrôler que l'application intègre toujours la dimension sécurité face aux menaces et vulnérabilités communes - Les actions de redéploiement à mener - Le plan d'action pour protéger l'application des failles identifiées à destination des équipes de développement et ops.	C28. Les failles d'authentification, autorisation, chiffrement, journalisation des applications sont testées C27. Le trafic transitant entre l'utilisateur et le cloud est chiffré (chiffrement symétrique et asymétrique, anonymisation, pseudonymisation…) C29. Les services tiers (Middleware, serveur, cookies, certificats) sont à jour C30. La réglementation et les bonnes pratiques dans la gestion des incidents est appliquée C31. Les logs de connexion sont analysés pour avoir un contexte et des informations C31. Les utilisateurs ayant eu accès aux données concernées sont identifiés C31. Les éléments auxquels les utilisateurs ont accédé sont identifiés. C32. Les mesures de protection adéquates sont appliquées (gestion des sources, gestion de configuration, gestion des faits)