Grade de Licence - Sciences et ingénierie - **Cybersécurité des Objets connectés**

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	MODALITÉS D'ÉVALUATION	
		MODALITÉS D'ÉVALUATION	CRITERES D'ÉVALUATION
Identification des risques de sécurité numérique pouvant atteindre les objets connectés dans leur environnement : - Développer une vision « Internet des objets » et cybersécurité permettant de fixer et de respecter les objectifs de l'entreprise en collaboration avec les principaux responsables informatiques. - Identifier l'objectif IoT de l'entreprise et s'assurer que l'architecture IoT répondra efficacement aux besoins actuels et à venir de l'entreprise. - Détecter les menaces de sécurité potentielles et répertorier les mesures à prendre pour protéger les systèmes IoT dans le respect des règlementations juridiques en vigueur. **Conception des solutions de sécurisation d'un réseau d'objets connectés en conformité avec la politique de sécurité de l'entreprise :** - Rechercher et/ou exploiter des documents techniques en français et en anglais pour proposer des solutions sécuritaires pertinentes. - Standardiser le processus de création de solutions IoT. - Concevoir une sécurité dynamique du réseau des IoT répondant aux normes en vigueur. - Mesurer les risques encourus par les IT par une veille active pour mesurer les points sensibles. - Participer et améliorer la veille sur la réglementation de la cybersécurité en utilisant les informations mises à dispositions **Implémentation de solutions de sécurité numérique dans le cadre du déploiement d'un parc d'objets connectés :** - Implémenter des solutions de sécurité dans le respect : des spécifications d'un cahier des charges en français et /ou anglais ; des standards de Sécurité en vigueur ; des procédures d'assurance qualité. - Collaborer avec les différentes équipes technologiques opérationnelles, au sein de l'entreprise afin que les solutions s'intègrent parfaitement aux opérations existantes. - Documenter les solutions mises en œuvre pour assurer les process de conception. - Déployer des éléments de sécurité **Elaboration et mise en place d'un plan de formation pour former les usagers à appliquer les principes de sécurité numérique d'un parc d'objets connectés :** - Analyser les écarts de compétences des collaborateurs en matière de sécurité. - Elaborer un plan de formation adapté aux situations professionnelles des collaborateurs. - S'assurer que les collaborateurs en situation de handicap auront accès à des aménagements adaptés afin de bien suivre la formation. - Sélectionner un organisme de formation répondant aux besoins. - Accompagner les utilisateurs à la détection de faille de cybersécurité sur un parc **Maintenance des outils de cybersécurité des objets connectés :** - Élaborer et planifier un programme de maintenance avec les parties prenantes. - Maintenir le niveau de sécurité à l'aide des tests réguliers et une surveillance soutenue. - Assurer le support client dans le cadre d'un service de maintenance. - Rédiger des rapports en conformité avec la réglementation. - Suivre les plans de maintenance curative et préventive. **Encadrement d'une équipe dans l'environnement professionnel de la cybersécurité des objets connectés :** - Définir et suivre les objectifs de projet (méthodes et outils) en prenant en compte l'environnement professionnel. - Planifier les activités et les ressources du projet en s'assurant que les collaborateurs en situation de handicap aient accès à des outils de travail adaptés afin de mener à bien leurs missions. - Veiller à la sécurité personnelle. - Organiser, coordonner et animer une équipe projet pour assurer le suivi des objectifs en tenant compte de sa diversité (culturelle, situation de handicap, etc) afin de mobiliser tous les membres.	- Identifier la nature de l'objet connecté en analysant l'environnement dans lequel il évolue afin de déterminer un mécanisme de sécurisation adapté. - Identifier les risques d'intrusions dans un système connecté en appliquant les méthodes d'analyse de risques afin de protéger l'environnement opérationnel et d'adapter les logiciels en conséquence- Détecter les alertes de sécurité en les analysant afin d'apporter la réponse aux incidents de sécurité. - Classifier les risques de sécurité en les analysant afin d'identifier les niveaux de vulnérabilité des objets connectés. - Caractériser les failles de sécurité en analysant les problèmes de cybersécurité des objets connectés mis en service afin de proposer des solutions en conformité avec les services informatiques internes et/ou externes à l'entreprise. - Répertorier les mesures à prendre pour protéger les systèmes des attaques potentielles en appliquant les méthodes de l'analyse de risque. - Effectuer une veille juridique afin d'être en capacité de respecter les réglementations en vigueur dans le but de répondre à toutes obligations légales. - Appliquer les différents standards relatifs à la sécurité des systèmes connectés afin de répondre aux obligations imposées en examinant les différents textes juridiques en vigueur. - Sécuriser un objet en sélectionnant des solutions existantes tant au niveau de leurs performances techniques (contraintes en termes de puissance de calcul, de mémoire, de disponibilité énergétique et d'occupation de la bande passante réseau, etc.) que de leur impact économique et social afin de répondre aux normes et standard en vigueur. - Concevoir une sécurité de manière dynamique en intégrant des mises à jour ou des changements de clés de chiffrement afin que ceux-ci puissent s'effectuer à distance (autoconfigurations automatiques et/ou reconfigurations de certains paramètres, configurations et clés de sécurité de manière dynamique au premier démarrage de l'appareil). - Appliquer une sécurité dynamique de l'objet connecté en s'appuyant sur des logiques permettant de changer les clés de sécurité de l'appareil si celles-ci ont été compromises et de révoquer un appareil si celui a été volé, etc. - Exploiter les documents techniques en version française et anglaise afin de proposer la solution la plus adaptée. - Implémenter les solutions, essentielles au déploiement d'objets connectés en adoptant des standards ouverts de Sécurité qui permettent d'assurer la sécurité des objets connectés notamment en termes d'authentification et de chiffrement des communications. - Analyser un cahier des charges en français et /ou anglais afin d'exploiter les spécifications associées à sa réalisation dans une situation de bureau d'études. - Gérer à distance le dispositif en s'appuyant sur des standards édictés par des consortiums de standardisation internationaux afin de sécuriser les systèmes et objets connectés. - Appliquer les procédures d'assurance qualité en implémentant une sécurité aux objets connectés afin d'intégrer des fonctionnalités de gestion standardisées telles que le Bootstrap ou le provisioning de paramètres. - Rédiger la documentation fonctionnelle et technique en suivant les nouvelles directives afin de les appliquer et/ou de les faire appliquer. - Elaborer les process des solutions de sécurité implémentées afin de former les usagers aux nouveaux standards ou mises à jour déployées pour répondre aux différents niveaux de crise. - Analyser les écarts de compétences en observant l'application des procédures et des protocoles en matière de sécurité afin d'évaluer les besoins en formation du personnel et définir un plan de formation. - Définir un objectif pédagogique afin de sélectionner un organisme de formation pour adapter les compétences des usagers à leur poste de travail en prenant en compte les situations de handicap. - Planifier les mécanismes de mise à jour logicielle dans le but d'intégrer l'obsolescence des produits en appliquant des correctifs de sécurité. - Gérer des solutions logicielles correctives en adoptant des technologies adaptées aux objets connectés, afin d'assurer la pérennité et la viabilité économique du parc d'objets connectés. - Évaluer la progression et la nature des risques sur un réseau en exploitation en contrôlant le développement des endroits susceptibles d'être attaqués sur chaque parc d'appareils connectés à Internet afin de mettre en place une solution de sécurité (Pare-feu, etc). - Proposer un plan de maintenance en élaborant un projet tenant compte de l'obsolescence des équipements matériels et informatiques afin de répondre à la demande des parties prenantes. - Définir des objectifs en utilisant les méthodes et outils de l'environnement professionnel (Sécurité personnelle, poste de travail adapté aux situations de handicap) afin de garantir le bon déroulement du projet. -Apporter des corrections de trajectoire (durée, moyens matériels et humains) en fonction des résultats obtenus afin d'atteindre les objectifs du projet. - Travailler avec les équipes en prenant en compte leur diversité (culturelle, situation de handicap, etc) en mode collaboratif sur le choix de différents scénarios afin qu'ils s'approprient les solutions retenues. - Animer des réunions d'équipe en utilisant des outils de communication en langue française ou anglaise ainsi que des supports numériques adaptés (tableau de bord, illustrations graphiques, etc) afin de faciliter les échanges constructifs.	**Projet d'entreprise. Travail individuel.** Devant le jury de certification : - Soutenance individuelle d'un projet d'entreprise - Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise **Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :** - Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise **L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :** - Identifier l'environnement et les risques associés, - Classifier, répertorier les risques - S'appuyer sur des procédures de références et prendre en compte le cadre légal. - Analyser de textes juridiques - Concevoir et sélectionner des solutions de sécurité - Exploiter de documents techniques - Implémenter des solutions - Analyser le cahier des charges - Gérer à distance un dispositif avec son environnement sécurisé - Prendre en compte les nouvelles directives - Analyser les besoins des utilisateurs, avec la prise en compte et adaptation aux situations de handicap. - Définir un plan de formation. - Fournir un plan de maintenance tenant compte de l'obsolescence des différents matériels - Proposer des solutions d'ajustement pour garantir la sécurité - Comprendre les enjeux globaux d'un projet - Définir des objectifs de travail - Utiliser des outils de communication en anglais - Animer une réunion avec son groupe de travail en tenant compte des diversités de chacun (culturelle, situation de handicap, etc)	Démarche d'analyse des risques structurée : - L'analyse de l'environnement est clairement expliquée - Les risques et leurs menaces associées sont caractérisés - Les technologies de réseaux retenues (Wifi, Bluetooth, Sigfox, LoRa) sont justifiées - L'identification, et le classement des risques retenus sont clairement énoncés. - Les logiciels, documents et source d'information sont utilisés de façon fiable et sans erreur de compréhension en français et en anglais - Les normes et réglementations spécifiques aux environnements sont prises en compte et appliquées. - Les solutions proposées répondent aux scénarios de menaces retenues - Les choix techniques, économiques et environnementaux sont justifiés - Les différents standards répondent aux « obligations » tels que OpenFlow, OpenStack - Les solutions proposées sont conformes aux besoins et attentes des utilisateurs. - Les services fournis sont disponibles conformément au niveau de sécurité requis pour l'ensemble des utilisateurs et des équipements numériques concernés - Les règles de sécurité sont respectées, quel que soit le type d'équipement numérique accédant à l'infrastructure - L'ensemble du process de mise en œuvre est réalisé avec méthode - Les procédures sont testées et documentées - Les propositions de formations sont présentées de façon claires et structurées. - Les propositions de formation répondent au niveau de compétences des utilisateurs et prennent en compte des situations de handicap. - L'ensemble du process de maintenance est réalisé avec méthode - L'obsolescence des matériaux ou logiciels est prise en compte par des points de contrôle. - Clarté et concision du dossier professionnelle, remis au jury de certification. - Utilisation des outils de communication adaptés lors de la soutenance - Lors du temps de questions /réponses en anglais : vérification d'un niveau d'anglais B1 - Les règles de sécurité sont respectées dans le cadre du projet. - Lors de la présentation du projet : adaptation de la posture, la clarté du support, son adéquation avec le discours, la clarté du message et absence d'erreurs d'interprétation. - Des comptes rendus de réunions animés par le candidat dans le cadre de son projet professionnel sont présentés.