Intitulé : Architecte cybersécurité et internet des objets (MS)

BLOC 1 : Concevoir et mettre en œuvre de Systèmes intelligents Sécurisés			
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**
Architecturation d'une solution IoT (Internet des Objets) pour un système intelligent sécurisé, du début à la fin : Définition et consignation l'état futur du système IoT pour l'organisation tout en garantissant que cette architecture répondra aux exigences métiers présentes et à venir. Conception d'une architecture sécurisée pour une solution IoT, couvrant une diversité de domaines technologiques, de la conception des objets (capteurs intelligents, actionneurs, etc.) aux réseaux de communication, en passant par les protocoles, la gestion des flux de données, la communication, ainsi que leur traitement, jusqu'à leur intégration harmonieuse avec	**Évaluer le contexte environnemental et conduire une analyse approfondie du système d'information** pour définir une architecture appropriée en se fondant sur le modèle fonctionnel et optimiser la mise en application. **Proposer des architectures techniques de référence conformes** pour répondre aux besoins du projet IoT et de cybersécurité. **Organiser et piloter des revues d'architectures et de conceptions** pour garantir la prise en compte des exigences initiales et des demandes d'évolutions du cahier des charges **Mettre en œuvre des processus de test robustes** en intégrer harmonieusement les composants IoT et de cybersécurité pour garantir la qualité de la solution répondre au cahier des charges	**Projet pratique - Conception de l'architecture d'une solution IoT :** A travers un projet pratique, les candidats conçoivent et mettent en œuvre une solution IoT sécurisée. Ils élaborent l'architecture complète d'un système intelligent intégrant des mécanismes de sécurité et tenant compte des pratiques et normes en vigueur. Enfin, ils rédigent le rapport de conception.	- Maîtrise des technologies clés de l'IoT : objets connectés, réseaux, protocoles de communication, API, flux de données, et traitement des données. - Analyse approfondie et élaboration d'une architecture technique en lien avec l'IoT basée sur un modèle fonctionnel. - Adaptabilité et originalité de la solution développée au regard du domaine d'activité et des exigences liées au contexte d'utilisation. - Intégration des principes et mécanismes de sécurité dès la conception : adoption de l'approche "Secure by Design". - Calibrage de l'architecture logicielle et matérielle développée en cohérence avec les exigences de volumétrie, de performance et de disponibilité.

le système d'information de l'organisation	**Intégrer les principes de sécurité dès la conception de la solution IoT** en adoptant l'approche "Secure by Design," et en respectant les meilleures pratiques et recommandations pour promouvoir la sécurité du système. **Analyser, calibrer et harmoniser l'architecture technique des solutions logicielles à connecter avec la plateforme IoT** en validant leurs interopérabilités afin de garantir la robustesse du système. **Assurer la conformité de la solution IoT et de cybersécurité développée aux normes et réglementations en vigueur** pour garantir la protection des données personnelles.		- Conformité avérée aux normes et réglementations relatives à la protection des données personnelles, comme le RGPD. - Interopérabilité démontrée des solutions logicielles à connecter avec la plateforme IoT. - Consolidation et structuration de flux de données issus de différentes solutions au sein de la plateforme IoT. - Qualité du rapport de conception incluant la clarté de la communication, la structuration du contenu et la pertinence des informations fournies.
Évaluation et renforcement de la sécurité technique d'une organisation, en prenant en compte les spécificités de la cybersécurité et de l'IoT	**Auditer les architectures réseau** en documentant les analyses conduites et les résultats des audits de sécurité IoT, pour identifier les points faibles dans l'écosystème IoT. **Planifier des tests d'intrusion éthiques sur les systèmes IoT** en utilisant les outils de Kali Linux pour évaluer la robustesse des défenses du système. **Simuler des attaques ciblant les objets connectés** à l'aide d'outils tels que nmap, metasploit ou armitage, pour identifier et analyser les vulnérabilités des systèmes IoT. **Analyser les configurations des équipements IoT et leurs mécanismes d'authentification** en utilisant des outils	**Mise en situation professionnelle - Rapport d'Audit IoT :** Les candidats rédigent un rapport d'audit de sécurité IoT détaillé, incluant l'application de jeux de rôle et de simulations d'attaques sur des systèmes IoT. Les tests d'intrusion peuvent être conduits à l'aide d'outils permettant d'identifier et d'analyser les vulnérabilités des systèmes IoT. Le rapport doit faire état, de façon structurée, des conclusions de l'audit mené.	- Maîtrise des normes de sécurité techniques spécifiques à la cybersécurité et à l'IoT (ISO 27001, NIST, CIS, etc.) et capacité à les interpréter et à appliquer dans le contexte des objets connectés. - Analyse documentée de la configuration des équipements IoT : mécanismes d'authentification, dispositifs de sécurité intégrés aux capteurs intelligents, aux actionneurs et aux microsystèmes IoT. - Planification et exécution réussies de tests d'intrusion éthiques sur les systèmes IoT, avec simulation d'attaques. - Utilisation efficace d'outils spécialisés (Kali Linux, nmap, metasploit, armitage) pour

	adaptés pour tester la robustesse du système. **Identifier les risques potentiels pour la sécurité des systèmes IoT** en les classant selon leur criticité pour prioriser les actions correctives. **Détecter des activités anormales ou suspectes dans les environnements IoT** en interprétant les logs des dispositifs, des communications et des transactions en vue d'identifier des modèles de comportement et d'anticiper des incidents. **Renforcer la sécurité opérationnelle du système IoT** en veillant au respect des règles éthiques en matière de traitement des données sensibles pour limiter la survenance des risques d'intrusion.	**Mise en situation professionnelle - Analyse des Configurations IoT :** Les candidats analysent les configurations des équipements IoT existantes et proposent des améliorations pour renforcer la sécurité des configurations tenant compte des évolutions réglementaires, normatives et technologiques spécifiques à l'IoT et des nouvelles menaces identifiées.	identifier et analyser les vulnérabilités des systèmes IoT. - Documentation claire et précise des résultats des audits de sécurité IoT, y compris des captures d'écran des tests. - Classification des risques selon leur degré de criticité. - Détection des points faibles dans l'écosystème IoT en lien avec les risques potentiels identifiés. - Présentation claire de conclusions et de recommandations spécifiques à l'IoT aux parties prenantes de l'organisation. - Garantie du respect des règles éthiques liées à la sécurité, en tenant compte des données sensibles générées par les objets connectés. - Suivi de la mise en œuvre des recommandations spécifiques à l'IoT issues des audits.

Intitulé : Architecte cybersécurité et internet des objets (MS)

BLOC 2 : Elaborer un système d'intelligence artificielle et gérer des données, des identités et d'accès (IAM)			
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**
Conception et développement de solutions d'intelligence artificielle pour la sécurisation de l'IoT	**Créer des modèles prédictifs et de reconnaissance de motifs** en exploitant des algorithmes d'apprentissage automatique pour analyser et traiter les données issues des dispositifs IoT.	**Projet pratique et soutenance orale - Conception d'une solution intelligente** A travers un projet pratique, les candidats développent une solution de sécurisation de l'IoT en recourant et en exploitant les mécanismes de l'intelligence artificielle. Les candidats présentent leur projet au cours d'une soutenance orale.	- Maîtrise des algorithmes d'apprentissage automatique et de deep learning, développement sécurisé pour l'IoT, cryptographie et sécurité des réseaux. - Qualité et innovation des solutions développées. - Respect et mise en œuvre des principes de sécurité.
Analyse et gestion des données massives issues de l'IoT	**Collecter, nettoyer et analyser de grandes quantités de données** pour améliorer la prise de décision et la sécurité.	**Projet, rapport et soutenance orale - Analyse et gestion de données** A travers un projet pratique, les candidats analyse un système de gestion de données massives issues de l'IoT. Dans un rapport écrit, qu'ils présentent à l'oral, ils rendent compte du diagnostic réalisé et formulent des recommandations opérationnelles.	- Maîtrise des outils d'analyse de données (par exemple, Python, R), des bases de données (SQL, NoSQL), de l'analyse en temps réel. - Pertinence et exactitude de l'analyse des données réalisées quant aux objectifs de traitement définis. - Protection des données garantie.
Gestion des identités et des accès (Identity and Access Management)	**Configurer et administrer des solutions d'authentification robustes** basées sur les principes Zero trust et Least Privilege, d'authentification multifactorielle et/ou adaptative pour limiter les risques d'intrusion.	**Simulations pratiques – IAM** Les candidats sont confrontés à des scénarios réels. Ils ont pour mission d'assurer la sécurité des systèmes d'information par le déploiement et l'administration de solutions de gestion	- Sélection et mise en œuvre de solutions d'authentification basées sur les principes de Zero Trust et Least Privilege. - Configuration et administration de systèmes d'authentification multifactorielle (MFA).

	Définir et déployer des politiques de gestion des accès et des privilèges liés à la gouvernance des identités (Identity and Access Governance) en conformité avec les normes de sécurité (Numeric Identity, Identity Lifecycle) en élaborant des matrices de rôles et d'accès limités par fonctions pour garantir une répartition des accès adaptée aux besoins métiers. **Intégrer des protocoles d'authentification et d'autorisation** tels que Kerberos, WS-Federation, SAML v2, OAuth2.0, OIDC pour protéger les ressources de l'organisation**.** **Garantir l'interopérabilité du système IAM** en s'appuyant sur le principe de fédération des identités (Identity Federation) pour assurer l'intégration fluide des systèmes et faciliter la navigation.	des identités et des accès, conformes aux principes de sécurité modernes.	- Mise en place de mécanismes d'authentification adaptative. - Respect des normes de sécurité (Numeric Identity, Identity Lifecycle). - Élaboration de matrices de rôles et déploiement de politique de gestion des accès privilégiés (PAM) en lien avec les besoins métiers identifiés - Création d'un annuaire central d'identités (protocoles Lightweight Directory Access Protocol ou Active Directory). - Utilisation des principes d'Identity Federation. - Définition d'une politique de gestion des concepts liés à la gouvernance des identités (IGA) : droits d'accès (entitlement, rôles métier), gestion des comptes orphelins et processus de certification. - Implémentation de protocoles tels que Kerberos, WS-Federation, SAML v2, OAuth2.0, Open ID Connect, Implicit Flow, Code Flow, PKCE... - Utilisation de Pentaho Data Integration.

Intitulé : Architecte cybersécurité et internet des objets (MS)

BLOC 3 : Gérer et piloter un projet de mise en œuvre d'une solution IoT sécurisée by design			
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**
Mise en œuvre d'une politique de sécurité	**Réaliser une veille permanente sur les évolutions technologiques liées à l'IoT et à la cybersécurité**, en anticipant et en accompagnant les changements organisationnels induits, afin d'intégrer les innovations pertinentes dans le projet et d'assurer l'adaptabilité du système. **Appliquer des normes de sécurité techniques spécifiques à la cybersécurité et à l'IoT (ISO 27001, NIST, CIS, etc.)** pour interpréter et appliquer les exigences de ces normes dans le contexte des objets connectés. **Garantir le respect des règles éthiques liées à la sécurité**, en tenant compte des données sensibles générées par les objets connectés et les informations sensibles découvertes lors des audits IoT pour garantir le respect de la réglementation en matière de traitement des données personnelles.	**Etudes de cas – Mise en place d'une politique de sécurité :** Le candidat met en place une politique de sécurité adaptée aux besoins d'une organisation, en intégrant des éléments réalistes ou simulés. Il veille au respect des règles et normes éthiques applicables en matière de sécurité.	- Identification et suivi des évolutions récentes, des risques et tendances émergents et des meilleures pratiques dans les domaines de la cybersécurité et des systèmes intelligents. - Prise en compte des enjeux de cybersécurité spécifiques à l'organisation. - Capacité à concevoir une politique adaptée. - Intégration des meilleures pratiques de sécurité dans la politique proposée. - Respect des normes de sécurité. - Protection des données personnelles et sensibles assurée.
Supervision de la collaboration avec des experts métiers de divers domaines (architectes experts en sécurité,	**Planifier de manière détaillée les différentes phases du projet IoT et de cybersécurité**, de la conception au	**Mise en simulation – Gestion de Projet IoT en Cybersécurité :** Le candidat gère les différentes phases d'un projet IoT en cybersécurité, en	- Planification et coordination efficaces des étapes du projet. - Gestion appropriée des ressources humaines et financières (budget) allouées.

systèmes, réseaux, logiciels, big data, etc.)	déploiement afin d'assurer la réalisation du projet dans les temps impartis **Gérer les ressources, le budget et les délais** du projet pour assurer la réalisation efficace des objectifs fixés. **Participer aux instances de pilotage (comité de pilotage) et définir des indicateurs de suivi de projet (KPIs) et des tableaux de bord** pour assurer la coordination des tâches et une gestion efficace du projet. **Coordonner et communiquer de manière efficace et transparente avec les parties prenantes et experts de divers domaines** tels que la sécurité, les systèmes, les réseaux, les logiciels, le big data, le cloud… etc afin de comprendre les besoins spécifiques de chaque spécialiste et promouvoir le suivi du projet.	tenant compte des enjeux de sécurité. Il en définit les étapes, coordonne et gère les ressources humaines et financières.	- Respect des échéances et des délais fixés. - Définition et suivi d'indicateurs de performance adaptés. - Elaboration de tableaux de bord de pilotage.
Pilotage de l'exécution du projet et animation des équipes intervenantes à chaque étape, de la conception au déploiement, en passant par le développement, les tests et l'intégration.	**Diriger et motiver les équipes dans une démarche inclusive tout au long du projet** pour stimuler leur créativité et leur implication. **Encourager la collaboration, la créativité et l'innovation au sein des équipes de conception, de développement, de tests, d'intégration et de déploiement** pour améliorer la cohésion d'équipe.	**Jeu de rôle – Animation d'équipe et gestion des conflits** A travers une mise en situation, le candidat est amené à prendre en charge la gestion d'une équipe projet, lorsqu'une situation de conflit survient.	- Déploiement d'un management agile, collaboratif et inclusif, anticipant les besoins spécifiques liés à une personne en situation de handicap. - Leadership et capacité à motiver les membres de l'équipe. - Pertinence des solutions proposées pour résoudre les conflits survenus.
Déploiement et suivi de la solution IoT	**Recueillir les retours d'expérience utilisateurs et intégrer les remarques dans les demandes d'évolution des solutions IoT et de cybersécurité** afin de	**Etude de cas – Suivi de projet :** Dans le cadre du suivi de la mise en œuvre d'une politique de sécurité IoT, le	- Analyse et prise en compte des retours utilisateurs, et notamment de ceux émanant des personnes en situation de handicap.

	perfectionner le système IoT et de garantir son accessibilité à tous les publics. **Identifier rapidement et les problèmes potentiels et mettre en place des processus de maintenance corrective et évolutive** pour assurer la pérennité des solutions IoT et de cybersécurité. **Développer des actions de sensibilisation et de formation à la cybersécurité à destination des personnels de l'organisation** pour prévenir la survenance du risque cyber.	candidat analyse les retours d'expérience utilisateurs et propose le déploiement d'ajustements et correctifs tenant compte des observations formulées. En parallèle, il élabore un plan de sensibilisation du personnel visant à informer et à former aux enjeux de cybersécurité. **Etude de cas – Plan de communication de crise** Dans un contexte de gestion de crise cyber, le candidat élabore un plan de communication comprenant une proposition spécifique pour faciliter la prise en compte d'une personne en situation de handicap.	- Définition de procédures de maintenance périodique de la solution IoT. - Réactivité quant aux problèmes identifiés. - Pertinence des processus de résolution déployés eu égard aux problématiques identifiées (nature, criticité). - Clarté et portée du plan de sensibilisation de crise élaborés : sensibilité à l'inclusivité et à la prise en compte des besoins spécifiques démontrée. - Elaboration d'un plan de communication de crise adapté et efficient. - Créativité dans les approches pédagogiques pour assurer une compréhension maximale.

Intitulé : **Architecte cybersécurité et internet des objets (MS)**

BLOC 4 : Réaliser une analyse forensique			
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**
Réalisation d'une investigation approfondie dans le domaine de la cybersécurité et de l'IoT	**Identifier, extraire et analyser les traces numériques laissées dans les systèmes, les réseaux et les dispositifs IoT et interpréter les données** pour reconstruire des scénarios d'incident. **Considérer la volumétrie des données, le temps disponible, le matériel de copie et d'autres contraintes externes** pour définir une stratégie de protection de données efficace. **Rédiger le document de traçabilité des actions effectuées** pour assurer le suivi et la mise en application des actions identifiées.	**Mise en situation - Simulation d'Investigation Forensique** Les candidats participent à une simulation d'investigation forensique destinée à évaluer leur maîtrise des outils forensiques, de la collecte des preuves, de l'analyse des artefacts numériques, et de la stratégie de préservation des données. **Rapport d'Analyse Forensique** Les candidats rédigent un rapport détaillé sur les résultats de leur analyse forensique, intégrant la traçabilité des actions effectuées. Ils formulent des recommandations sur la base de leurs observations.	- Maîtrise des outils forensiques (finalité et fonctionnalité) : Expertise avec EnCase, FTK, Autopsy, Wireshark, etc. Compréhension approfondie des fonctionnalités. - Reconstitution des scénarios d'incident à partir de l'analyse des traces numériques et l'interprétation des données. - Intégrité et admissibilité en justice assurées des preuves collectées. - Suivi des actions menées formalisé à travers le document de traçabilité. - Evaluation de l'impact des incidents à travers l'analyse des Logs et Artefacts Système. - Détection et analyse des malwares et intrusions favorisant une intervention rapide. - Identification précise des indicateurs de compromission (IoC) et des méthodes d'intrusion. - Détection des activités suspectes à partir de l'examen du trafic réseau .
Analyse et exploitation des preuves numériques pour établir une chronologie détaillée des incidents de sécurité et identifier les failles exploitées.	**Collecter des preuves de manière sécurisée**, en préservant leur intégrité et en garantissant leur fiabilité pour assurer leur admissibilité devant un tribunal. **Interpréter les logs système, les journaux d'événements et les artefacts** pour retracer les activités malveillantes et mesurer l'étendue des incidents. **Détecter, isoler et analyser des malwares dans les systèmes et les dispositifs IoT** pour intervenir sur les incidents détectés. **Identifier les indicateurs de compromission (IoC) et les méthodes**	**Mise en situation Simulation de Témoignage Expert** A travers une mise en situation reconstituée, les candidats témoignent en tant qu'experts devant un tribunal, répondant à des interrogatoires croisés.	

	d'intrusion pour optimiser l'analyse de risque. **Extraire et analyser la mémoire volatile** et examiner le trafic réseau pour identifier les processus en cours, les connexions réseau et les artefacts liés à des incidents. **Analyser les protocoles spécifiques à l'IoT** pour comprendre les communications entre les objets connectés. **Rédiger des rapports techniques et légaux détaillés sur les résultats de l'analyse forensique et présenter clairement les conclusions, les découvertes et les recommandations** pour garantir une traçabilité des données transmises. **Collaborer de manière interdisciplinaire, y compris avec des experts en sécurité, des juristes et des forces de l'ordre et assurer une coordination efficace** pour une investigation complète.	**Examen - Éthique et Confidentialité :** Les candidats sont évalués sur leur respect strict des principes éthiques lors de la collecte et de l'analyse des preuves, ainsi que sur la garantie de l'intégrité et de la confidentialité des données manipulées.	- Respect des dispositions légales et réglementaires en matière de collecte et de traitement des preuves. - Clarté et pertinence des conclusions, découvertes et recommandations formulées au sein des rapports techniques et légaux rédigés au regard des preuves collectées.

Intitulé : Architecte cybersécurité et internet des objets (MS)

BLOC 5 : Détecter et traiter les incidents techniques

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**
Gestion, détection et analyse des incidents de sécurité	**Détecter les incidents techniques de sécurité** en utilisant des algorithmes d'IA (apprentissages automatique et profond) pour identifier des schémas inhabituels et des activités suspectes. **Interpréter les alertes générées par les modèles d'IA et analyser les événements de sécurité** pour retracer la chronologie des cyberattaques.	**Mise en situation réelle – Gestion des Incidents de Sécurité avec l'Intelligence Artificielle** L'évaluation repose sur une approche immersive, plaçant le candidat dans un environnement simulé qui reproduit fidèlement les conditions d'un incident de sécurité au sein d'une organisation. Cette mise en situation authentique vise à évaluer la capacité du candidat à réagir de manière réaliste et efficace face à des scénarios complexes. L'évaluation est conçue pour s'étendre sur une période de 72 heures. Ce laps de temps a été déterminé pour refléter une fenêtre réaliste au cours de laquelle un professionnel de la cybersécurité devrait être en mesure de détecter, analyser et traiter des incidents variés, y compris une fuite de données. **Scénarios Variés :** Les incidents proposés couvrent une gamme diversifiée, allant des attaques techniques aux fuites de données, imitant ainsi la complexité du paysage de la cybersécurité moderne.	- Identification efficace et exacte des incidents techniques et de la fuite de données à partir des algorithmes d'IA mobilisés (algorithmes d'apprentissage automatique - Machine Learning - et d'apprentissage profond - Deep Learning). - Interprétation précise des alertes détectées et reconstitution de la chronologie des événements permettant l'identification des vecteurs d'attaques. - Déploiement de méthodes et d'outils d'analyse de données de sécurité (Splunk) et d'intrusion (Kill chain, Diamond Model, Mitre Att&ck) adaptés aux activités malveillantes détectées. - Catégorisation effective des incidents. - Réactivité et adaptabilité démontrées face aux incidents et à la fuite de données : réduction des délais entre détection et remédiation. - Efficacité des mesures préventives déployées au regard des risques identifiés. - Qualité de la documentation produite pendant le processus de gestion de
Mise en place de mécanismes de réponse aux incidents et de remédiation pour limiter l'impact des attaques et restaurer la sécurité des systèmes.	**Développer des stratégies automatisées de réponse aux incidents** en produisant des correctifs avec des outils tels que Kali Linux et en intégrant des normes telles que ISO 27035 pour remédier aux incidents. **Superviser les infrastructures de l'organisation et les événements de sécurité** en utilisant un système de gestion des informations et des événements de sécurité (SIEM) pour détecter les menaces avant qu'elles ne perturbent ses activités. **Mettre en place des systèmes de détection en temps réel** pour identifier les sources d'incidents et accroître la réactivité de traitement.		

	Bloquer proactivement les accès au système informatique pour prévenir les menaces. **Effectuer une analyse statique et/ou dynamique du code malveillant** en déployant des méthodes telles que Kill Chain, Diamond Model, et la matrice MITRE ATT&CK pour qualification et catégorisation de l'incident. **Mettre en place un système de veille recensant l'OSINT, SOCMINT, HUMINT, et les informations du Deep et Dark web** pour anticiper les évolutions des menaces et limiter l'exposition de l'entreprise et réduire la surface d'attaque.	**Données Réalistes :** Les données et les paramètres de l'évaluation sont conçus pour refléter de manière précise les défis rencontrés dans un contexte professionnel, garantissant ainsi que les compétences évaluées sont directement applicables dans un environnement opérationnel. **Interactions Dynamiques :** L'évaluation inclut des interactions dynamiques avec divers éléments de l'environnement simulé, simulant les réponses en temps réel aux mesures prises par le candidat. Cela assure une évaluation holistique des compétences en gestion d'incidents.	l'incident, y compris des rapports détaillés sur les incidents identifiés et les actions entreprises. - Structuration d'un dispositif de veille et de renseignement permettant d'anticiper les évolutions des menaces et de réduire la surface d'attaque.

Intitulé : Architecte cybersécurité et internet des objets (MS)

BLOC 6 : Sécuriser les réseaux et les communications

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**
Conception et déploiement d'architectures sécurisées	**Développer des stratégies de sécurité réseau et concevoir des architectures sécurisées pour les réseaux et les communications** afin d'implémenter des protocoles et des mécanismes de sécurité. **Assurer la conformité aux normes de sécurité en vigueur et suivre les évolutions des réglementations liées à la sécurité des réseaux** pour garantir une sécurité des pratiques. **Chiffrer les communications sensibles et mettre en place des réseaux privés virtuels (VPN) sécurisés** afin de garantir l'intégrité et la confidentialité des données transitant à travers les communications.	**Mise en Situation Professionnelle :** **Analyse de la Sécurité d'un Système et Réseau d'Entreprise :** Mise en situation professionnelle consistant en l'analyse de la sécurité d'un système et d'un réseau d'entreprise. Cette approche permet de mesurer la capacité du candidat à appliquer ses connaissances théoriques à des contextes réels et à démontrer des compétences concrètes en matière de sécurité des réseaux. **Durée de l'Évaluation** La mise en situation professionnelle est conçue pour être réalisée dans un délai déterminé, reflétant les contraintes temporelles réalistes auxquelles un professionnel de la sécurité pourrait être confronté dans un environnement opérationnel.	- Elaboration d'une stratégie de sécurité réseau adaptée aux besoins identifiés (analyse des risques, conformité aux normes). - Intégration des mécanismes de sécurité pertinents (chiffrement, segmentation, firewalls) aux architectures conçues. - Respect des exigences réglementaires (RGPD, ISO, etc.) - Intégrité et confidentialité des données garanties via les solutions VPN. - Respect des pratiques de sécurité (TLS, IPsec) dans les choix technologiques et protocoles. - Configuration et opérationnalité des outils de surveillance (IDS/IPS). - Analyse des journaux d'événements réseau : identification rapide d'activités anormales. - Déploiement de mesures adaptées et efficaces face aux menaces détectées. - Intégration et mise à jour des technologies de détection des menaces.
Surveillance des activités réseau et détection des menaces	**Mettre en place des outils de surveillance des flux de données et configurer des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS)** pour assurer une surveillance continue des activités réseau. **Interpréter les journaux et les données de surveillance** pour repérer les anomalies et mettre en œuvre des technologies de détection des menaces et réagir rapidement à des activités suspectes ou malveillantes.		

Analyse des vulnérabilités et gestion des incidents de sécurité	**Effectuer des analyses de vulnérabilité sur les infrastructures réseau et mettre en place des correctifs de sécurité** en appliquant des pratiques de gestion des risques pour remédier aux vulnérabilités identifiées et sécuriser le système. **Élaborer des plans d'intervention et coordonner les actions collaboratives nécessaires lors de la détection d'une activité malveillante** pour une résolution efficace.		- Pertinence des recommandations formulées quant aux vulnérabilités identifiées. - Elaboration de plans d'intervention clairs et opérationnels permettant une résolution efficace des incidents. - Rédaction de rapports d'incidents sont précis, détaillés et exploitables pour des améliorations futures. - Complétude, accessibilité et tenue à jour de la documentation des configurations et politiques de sécurité. - Clarté et adaptation au public cible des messages diffusés sur les enjeux de sécurité. - Adhésion renforcée des parties prenantes aux politiques de sécurité. -
Sensibilisation aux enjeux de sécurité	**Documenter les configurations de sécurité mises en place** en rédigeant des rapports d'incidents et d'analyses de sécurité et maintenir une documentation à jour sur les politiques de sécurité réseau pour garantir une traçabilité efficace. **Communiquer efficacement sur les enjeux de sécurité aux parties prenantes et sensibiliser les utilisateurs aux bonnes pratiques de sécurité des réseaux** afin de minimiser les risques.		

L'obtention de la certification est conditionnée à la validation conjointe de tous les blocs de compétences et d'une thèse professionnelle, modalité globale et transversale, s'appuyant sur la réalisation d'une mission en entreprise de 4 mois minimum.