RÉFÉRENTIEL DE COMPETENCES ET D'EVALUATION
« SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES RÉSEAUX »

Modalité M0 *: Tests d'évaluation des connaissances, ou QCM (questions à choix multiples)*

A la fin de chaque module de formation, tout au long de la période des enseignements théoriques, chaque participant est soumis à une épreuve de QCM. Il doit répondre à une série de questions portant sur le module dispensé. Ces tests permettent d'évaluer le niveau de compréhension, d'assimilation et de mémorisation des contenus. Chaque test comporte une vingtaine de questions. Il est élaboré par les enseignants à l'aide d'un modèle prédéfini. Les réponses sont alors évaluées par le responsable pédagogique.

Modalités M1 : *Ateliers de mise en œuvre et de simulation de cas pratiques*

Les travaux sont réalisés par binômes et consistent à suivre un énoncé qui détaille la configuration d'un équipement ou la prise en main d'un outil de sécurisation. L'évaluation des réponses aux questions posées est effectuée par un enseignant.

Modalité M1.1 : Elaboration et test d'une architecture de réseau privé virtuel
Modalité M1.2 : Recherche des flux non souhaités dans un modèle de contrôle d'accès
Modalité M1.3 : Mise en œuvre d'un cadre règlementaire et normatif, adapté à divers contextes

Modalités M2 : *Etudes de cas relatives à des problématiques de sécurité*

Les participants sont regroupés par équipes de 2 à 3. Ils doivent réaliser des études de cas en s'appuyant sur l'utilisation des outils pratiques. Un accompagnement est assuré par un enseignant qui oriente les équipes au fur et à mesure de leur avancement. L'enseignant évalue la qualité et la pertinence des livrables (rapport d'analyse, traces de simulation, tableaux de bord).

Les projets pédagogiques concernent les modalités d'évaluation suivantes :

Modalité M2.1 : Recensement et analyse des risques du SI de l'entreprise, étude des scénarios de menace
Modalité M2.2 : Analyse des protocoles cryptographiques illustrée par des applications de commerce électronique sécurisées
Modalité M2.3 : Mise en œuvre de recherche et de correction de vulnérabilités

Modalité M3 : *Rédaction d'une réponse à un appel d'offres, et restitution orale*

A l'issue de la période des enseignements théoriques et des ateliers, les participants sont regroupés en équipe de 3 ou 4 personnes. Chaque équipe doit simuler un projet de réponse à un besoin client présenté sous la forme d'un appel d'offres. Le travail sur le projet se déroule sur une durée de 2 mois. Il donne lieu à un document écrit, puis à une restitution orale devant un jury.

Le projet représente à la fois un moyen privilégié d'acquisition de compétences, et la possibilité d'appliquer les méthodes, les techniques, les outils et les approches étudiés lors des formations théoriques. Il offre l'opportunité de confronter la réflexion conceptuelle à l'expérience professionnelle. Les participants doivent alors proposer une solution globale intégrant les volets technique, organisationnel et financier.

Le sujet concerne deux modalités d'évaluation :

Modalité M3-1 : Rédaction de la réponse au besoin client
Modalité M3-2 : Restitution orale, simulée devant le client

REFERENTIEL DE COMPETENCES		REFERENTIEL D'EVALUATION	
COMPOSANTE DE CERTIFICATION	**COMPETENCE SPECIFIQUE**	**MODALITE D'EVALUATION**	**CRITERE D'EVALUATION**
SSR-CC1 Définir la gouvernance de la sécurité des systèmes d'information de l'entreprise	**CC1-C1** Répertorier les menaces courantes des systèmes d'information, et classer les occurrences d'attaques récentes, en consultant les sites d'alertes gouvernementaux, puis les supports d'information spécialisés.	Modalité M0 Modalité M1-3 Modalité M2-1	**A propos de CC1-C1** Les attaques informatiques récentes sont identifiées. Les principaux sites et organismes officiels en charge de la sécurité numérique en France sont répertoriés.
	CC1-C2 Analyser les vulnérabilités et failles du SI de l'entreprise, celles en rapport avec les attaques récentes et celles portant atteinte à la sécurité du système, dans l'objectif de développer une politique de sécurité.		**A propos de CC1-C2** Les différentes sources, comme les codes malveillants, les logs et l'organisation de l'entreprise sont analysées. Les vulnérabilités logicielles, réseaux et organisationnelles sont identifiées
	CC1-C3 Analyser la réglementation du droit numérique, dans l'objectif de définir les besoins internes de l'entreprise, puis vérifier la conformité des pratiques s'y rapportant.		**A propos de CC1-C3** Les références normatives telles que ISO/CEI 27000 et législatives (RGPD) sont mentionnées.

	CC1-C4 Définir les critères de l'analyse de risque afin d'exprimer les besoins de sécurité de l'entreprise, puis mettre en place le référentiel de sécurité (la politique de sécurité)		**A propos de CC1-C4** Les étapes de l'analyse de risque sont maîtrisées. Un outil de gestion de risques (EBIOS) est proposé pour être mis en œuvre Les tableaux de bord et les graphiques sont interprétés, et les éléments pertinents qui permettent de contribuer à l'élaboration de la politique de sécurité sont extraits.
SSR-CC2 Mettre en place des mécanismes de sécurité	**CC2-C1** Analyser les mécanismes de protection des SI, telles que le chiffrement, la signature numérique, l'authentification, ceci afin de mettre en œuvre les services de sécurité visés.	Modalité M0 Modalité M2-2	**A propos de CC2-C1** Les algorithmes cryptographiques doivent être assimilés et mis en œuvre pour répondre aux services de sécurité requis.
	CC2-C2 Mettre en œuvre une infrastructure de gestion de clé publique afin d'assurer l'authenticité des clés publiques et éviter les attaques par usurpation d'identité.		**A propos de CC2-C2** Les processus de génération et de gestion de certificats doivent être décrits. Les certificats numériques doivent être analysés et les composants cryptographiques doivent être identifiés.

SSR-CC3 Concevoir ~~de~~ la sécurité des systèmes informatiques	**CC3-C1** Vérifier que les procédures de plans de secours et de sauvegarde des SI, celles mises en place ou à venir, permettent de remédier aux sinistres et de poursuivre l'activité.	Modalité M0 Modalité M1-1	**A propos de CC3-C1** Une procédure de sauvegarde et de secours est proposée. Les ressources sensibles du SI à protéger sont placées dans des zones précisément identifiées.
	CC3-C2 Vérifier que la politique de sécurité mise en œuvre pour l'audit de sécurité et la détection d'intrusion est conforme aux normes de sécurité		**A propos de CC3-C2** Les règles sont adaptées aux normes et exigences de sécurité, leur efficacité et leur cohérence sont vérifiées.
	CC3-C3 Analyser et mettre en place les mécanismes de sécurité des systèmes informatiques, tels que les droits d'accès ou les filtrages de trafic dans les équipements.		**A propos de CC3-C3** Les règles des droits d'accès sont définies et implémentées Les équipements de filtrage tels que les routeurs/pare-feu sont configurés.

SSR-CC4 Concevoir ~~de~~ la sécurité des réseaux de télécommunication	**CC4-C1** Sélectionner les protocoles de mise en œuvre de la sécurité entre les sites de l'entreprise, en s'assurant de l'opportunité des services de sécurité requis (comme la mise en place de VPN – réseaux privés virtuels).	Modalité M0 Modalité M1-1 Modalité M2-3	**A propos de CC4-C1** Une architecture sécurisée est décrite en établissant des VPN.
	CC4-C2 Segmenter le réseau afin de cloisonner les trafics des départements de l'entreprise, puis superviser les échanges de flux avec précision		**A propos de CC4-C2** Une politique de sécurité est déployée en configurant des pare-feu.
	CC4-C3 Analyser et mettre en œuvre les techniques de détection des intrusions et de correction des vulnérabilités.		**A propos de CC4-C3** Les failles de sécurité doivent être identifiées et des solutions doivent être proposées. Un outil de pentesting (Metasploit) est mis en œuvre pour détecter des vulnérabilités.

SSR–global Projet ou mise en situation professionnelle mettant en œuvre l'ensemble des composantes de la certification globale SSR		Modalité M3-1 Modalité M3-2	**A propos de SSR–global** Un projet type de déploiement d'une architecture sécurisée est détaillé, avec les contraintes de coût, délai et qualité, et une projection à 5 ans de la montée en débit des trafics, et des protections à mettre en place. Les différentes parties sécurisées du réseau et du SI sont distinguées, décrites fonctionnellement et structurellement. Des exemples d'intrusions physiques, logicielles et télécoms sont mentionnés, avec les parades pour s'en prémunir. La soutenance orale est réalisée de façon dynamique, synthétique, organisée, dans le temps imparti. Les réponses aux questions sont claires et convaincantes.