



Consultation MAPA réf. 2025023PAS

Cahier des Clauses Techniques Particulières CyberSkills4All

Prestation de conception de formations continues et micro-certifications en mode distanciel sur plusieurs domaines de la cybersécurité (CMA CyberSkills4All, Université de Rennes)

I.	Généralités.....	1
1.	Contexte.....	1
2.	Objet et nature des prestations attendues.....	2
3.	Conduite et suivi des prestations (ou coordination et suivi).....	3
4.	Conditions de réalisation (communes à tous les lots).....	4
5.	Livraison du module.....	6
6.	Engagements post-réalisation de la formation.....	6
7.	Propriété intellectuelle.....	6
II.	Lot 1 : Réaliser une rétro-ingénierie réseau et système.....	7
III.	Lot 2 : Analyse après incident.....	8
IV.	Lot 3 : Analyser les flux réseaux.....	9
V.	Lot 4 : Analyser les journaux.....	11
VI.	Lot 5 : Définir une architecture de système d'information sécurisée.....	12
VII.	Lot 6 : Analyse de la menace.....	14
	Annexe 1 : Terminologie et définitions.....	15
	Annexe 2 : Cahier des charges des formations du CMA CyberSkills4All.....	17
	Annexe 3 : Charte graphique du CMA CyberSkills4All.....	17
	Annexe 4 : Trame de réponse à fournir.....	17

I. Généralités

1. Contexte

Le projet CyberSkills4All (CS4A) est un AMI CMA¹ France 2030 qui réunit dix acteurs majeurs de la formation et de la cybersécurité porté par l'Université de Rennes avec l'objectif de développer des parcours de sensibilisation et de formation, du Bac+1 au Bac+8 (<https://www.univ-rennes.fr/cyberskills4all>).

Ces acteurs sont : l'Université de Rennes, l'Université Bretagne Sud, Rennes School of Business, ENSTA, ENIB, le GIP de Formation de l'Académie de Rennes, le GIP France Université Numérique, le Pôle d'excellence Cyber, Orange et le Campus des métiers et des qualifications d'excellence numérique, photonique et cybersécurité. L'Université de Rennes a été désignée comme établissement en charge du portage administratif et financier de ce projet

La cybersécurité est un enjeu de tous les métiers, spécialistes et non spécialistes : le ROME de France Travail cite 3 métiers de la cybersécurité et introduit la cybersécurité dans 25 métiers non spécialistes. L'ANSSI² cartographie 28 métiers de la cybersécurité, l'ENISA³ 12 métiers et la NIST-NICE⁴ 52 métiers. Alors que les employeurs citent plus de 13.000 recrutements par an, la formation initiale insère 7 500 diplômés par an. Les enjeux majeurs du projet CyberSkills4All sont, d'une part, de sensibiliser à la cybersécurité une grande partie de la population scolaire (dispositif CyberCMQe) et universitaire (dispositif CyberNCU), et d'autre part de développer la formation continue *upskilling* et *reskilling* pour répondre aux besoins en compétences (dispositif CyberFUN). Les enseignants et expert de la cybersécurité trouveront dans le référentiel NICE⁵ ce qui permet de lier chacun des métiers (52) aux : Connaissances (630), Compétences (374), Capacités (176) et Activités (1006) qui « composent » ces métiers.

Afin de répondre à des besoins en compétences spécifiques en cybersécurité, le projet CyberSkills4All développe des micro-certifications en concluant des marchés de prestations de services avec des opérateurs économiques spécialisés dans ce domaine. Ces marchés d'élaboration de micro-certifications et formations continues en ligne sont mis en place et coordonnés par l'Université de Rennes, établissement porteur du CMA CS4A.

Le projet d'achat de prestation se fera en deux phases dont le calendrier est estimé ainsi :

- Phase 1 – 2025 : élaboration de six micro-certifications (objet de la présente consultation)
- Phase 2 – 2026 : élaboration d'une dizaine de micro-certifications (objet d'une seconde consultation qui sera publiée dans quelques mois))

Le présent cahier des clauses techniques particulières (CCTP) décrit les spécificités relatives aux différentes prestations de formation continue à distance que l'Université de Rennes souhaite diffuser sur la plateforme de France Université Numérique⁶, partenaire du projet. Ce CCTP s'appuie sur le cahier des charges des formations du CMA CS4A, disponible en Annexe 2.

¹ Appel à Manifestation d'Intérêt Compétences et Métiers d'Avenir

² <https://cyber.gouv.fr/publications/panorama-des-metiers-de-la-cybersecurite>

³ <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>

⁴ <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>

⁵ https://performatron.risk-redux.io/nice_categories

⁶ <https://niccs.cisa.gov/workforce-development/nice-framework/skill>

2. Objet et nature des prestations attendues

Les formations qui seront développées sont des micro-certifications. Elles s'adressent principalement à un public de spécialistes⁷ de la cybersécurité, conformément aux ambitions du projet de faire de la formation en cybersécurité à haut niveau d'expertise, par les experts et pour les experts. Les apprenants devront avoir des compétences dans la mise en place d'une station de travail.

Les micro-certifications relèvent de la formation en ligne asynchrone et ont une durée variant de 7 à 30 heures de travail moyen estimé pour les apprenants. Celle-ci est fixée pour chaque lot et pourra faire l'objet d'un réajustement par l'Université de Rennes après évaluation des dossiers.

Ces micro-certifications permettent l'acquisition ou le développement de micro-compétences bien identifiées par un référentiel : NICE⁸.

Le prestataire pourra s'appuyer sur la matrice "métier-compétence" du campus Cyber⁹ pour :

- Présenter les différents niveaux des macro-compétences prérequis pour suivre la formation ;
- Préciser les différents niveaux des macro-compétences qui seront acquises après le suivi de la micro-certification.

Les micro-certifications développées dans le cadre du projet CS4A doivent permettre l'acquisition de compétences, notamment à des actifs en poste ou en mutation professionnelle. Les acquis de la formation devront ainsi être mobilisables immédiatement.

Les compétences identifiées seront également présentées dans le syllabus afin que les stagiaires en prennent connaissance.

Les micro-certifications donnent lieu à la délivrance d'un certificat numérique pour les candidats ayant réussi les évaluations. Sauf indication contraire, les micro-certifications ne sont pas des certifications professionnelles au sens de l'article L6113-1 du Code du Travail, elles relèvent d'une certification des compétences par l'Université habilitée à délivrer la micro-certification dans le cadre d'une formation qualifiante.

Les micro-certifications devront se conformer au cahier des charges des formations CS4A, à la charte graphique du CMA et respecter le rythme et le dynamisme des formations courtes à distance avec une approche par compétences. Les chapitres seront constitués de plusieurs séquences dynamiques de formats différents, alternant vidéos pédagogiques, travaux pratiques ou dirigés et autres activités.

Une évaluation des compétences sera faite. Cette évaluation pourra se faire de différentes manières : tout au long de la formation, par le biais d'un examen final ou encore par un mixte de ces deux modalités. Le prestataire proposera une évaluation des compétences développées dans ces chapitres selon un rythme qui lui semblera le plus adapté. Le candidat devra présenter avec son offre des modèles de livrables en matière de séquences, et une méthodologie d'évaluation.

Ces micro-certifications seront hébergées et exploitées sur la plateforme de France Université Numérique¹⁰.

⁷ https://wiki.campuscyber.fr/Matrice_des_comp%C3%A9tences_des_m%C3%A9tiers_techniques ; <https://campuscyber.fr/resources/referentiel-des-competences-des-metiers-connexes-de-la-cyber/>

⁸ <https://www.francecompetences.fr/faq-ext/index.php?q=FAQ---France-competences/01---Certification-professionnelle/12875517885e8628e7799052.57085463>

⁹ Le Du, S. (2023). Scénario pédagogique. Dans B.Doucey & C.Goï (dirs), Vocabulaire de l'ingénierie pédagogique (p.170-171). PUFR

¹⁰ Dans le CMA CyberSkills4All, un spécialiste en cybersécurité est une personne ayant une compétence technique dans un domaine de la cybersécurité d'un niveau supérieur ou égal à 2 selon la matrice des

3. Conduite et suivi des prestations (ou coordination et suivi)

Cadrage et itérations prévisionnelles des réunions :

Une réunion de démarrage au commencement de la prestation sera organisée, suivie de deux réunions de suivi en cours de création de contenus puis une dernière réunion au moment de la livraison de la formation.

Un accompagnement par les équipes technique de France Université Numérique sera organisé une fois par mois pour s'assurer de la compatibilité des outils utilisés pour la réalisation de la prestation et de la bonne intégration de la formation sur la plateforme FUN.

Ingénierie Pédagogique :

Conformément au cahier des charges des formations rédigé pour le projet CS4A, un accompagnement en ingénierie pédagogique par FUN'IP pourra être proposé. Le rythme de réunion d'un tel accompagnement sera déterminé au démarrage du projet, en concertation avec les équipes de FUN.

Suivant l'accompagnement en ingénierie pédagogique déterminé, la **prestation** réalisée pourra être :

- **Complète** : le Prestataire produit seul tous les livrables demandés dans le lot de l'appel d'offre. Il s'agit d'une sous-traitance dite "autonome" ;
- **Assistée** : Le Prestataire a besoin d'être accompagné par un expert pédagogique, dont l'intervention est plus particulièrement focalisée sur l'intégration des livrables et sur le cahier des charges des formations. Il s'agit de sous-traitance dite "accompagnée" ;
- **Partielle** : Le Prestataire ne répond qu'au cahier des charges des formations (cf. Annexe 2 et livrables "formation" indiqués en I.4.). Il s'agit de sous-traitance dite "partielle". Le projet CyberSkills4All produit les autres livrables.

L'accompagnement en ingénierie pédagogique pourra évoluer au fil de la prestation, sous réserve qu'un avenant soit signé avec les Parties.

4. Conditions de réalisation (communes à tous les lots)

Conditions du projet :

Les candidats devront se conformer aux prescriptions ci-dessous :

- ❖ Les candidats dont la langue d'enseignement est le français. Cependant, les formations pourront être conçues et réalisées en anglais si son usage est jugé opportun par l'Université de Rennes.
- ❖ Les candidats dont les structures relèvent de la cybersécurité souveraine, en adéquation avec la stratégie nationale France 2030 de développement de la souveraineté numérique dont dépend le projet CyberSkills4All. Les candidats devront expliciter dans leur offre tous les outils et toutes les mesures mises en œuvre pour se conformer avec cette problématique de cybersécurité souveraine, certifications et modes opératoires à l'appui.
- ❖ Les formations proposées en blended learning et asynchrones.

Durée de la mission : entre trois et six mois.

Calendrier prévisionnel : date de démarrage de la mission Été/rentrée 2025

Seront appréciées les formations qui pourront être finalisées et livrées avant le 15 novembre 2025, afin que l'Université de Rennes puisse en faire la promotion lors de l'European Cyber Week 2025.

Livrables :

Le candidat précisera dans sa réponse les livrables qu'il fournira pour chacun des lots de l'appel d'offre :

- ☐ Teaser de la micro-certification
- ☐ Scénario pédagogique
 - ☐ Intitulé de la formation
 - ☐ Présentation de(s) l'auteur(s)
 - ☐ Compétences visées
 - ☐ Apprentissages critiques (dans le cas de la micro-certification)
 - ☐ Modalités d'apprentissages et de situations authentiques d'évaluation
 - ☐ Ressources mobilisées
 - ☐ Paillasse numérique utilisée pour les enseignements
 - ☐ Médias mobilisés
 - ☐ Activités et leurs modalités
- ☐ Formation : pour chaque séquence pédagogique, volet « apprentissage » :
 - ☐ Powerpoint du cours
 - ☐ Powerpoint avec enregistrement vidéo (*Enregistrer le diaporama*)
 - ☐ Polycopié :
 - ☐ Powerpoint en PPT
 - ☐ Document Word modifiable
 - ☐ Autre : préciser)
 - ☐ Vidéo de la formation
- ☐ Formation : FeedBack de l'apprentissage :
 - ☐ QCM de positionnement pour chaque séquence pédagogique :
 - ☐ Tableau Excel « Compilable Moodle » renseigné ;
 - ☐ Autre module intégrable dans Moodle (Préciser) ;
- ☐ Formation : SAE situation authentique d'évaluation
 - ☐ Enoncé de la mise en situation
 - ☐ Document WORD ; ☐ Powerpoint ;
 - ☐ Autre document modifiable (Préciser)
 - ☐ Travail pratique
 - ☐ Paillasse numérique (☐ Cadre de l'apprenant ; ☐ Cadre de l'animateur pédagogique ; ☐ Autre (Préciser)
 - ☐ Evaluation de la SAE (pour chaque séquence pédagogique) :
 - ☐ QCM : Tableau Excel « Compilable Moodle » renseigné ;
 - ☐ Autre module intégrable dans Moodle (Préciser) ;
- ☐ Soutien à la formation : pour chaque séquence pédagogique :
 - ☐ Livret de l'animateur pédagogique ;
 - ☐ Autre modalité de soutien :
 - ☐ FORUM FAQ – pré-renseignée ; ☐ FORUM Evaluation entre pairs ;
 - ☐ Autre (Préciser) ;

Dans le cas où le candidat cocherait la case “paillasse numérique”, il devra faire apparaître, dans sa réponse, le coût estimé détaillé d’une paillasse numérique supplémentaire à l’utilisation d’un ordinateur portable. Ce coût envisagé sera alors éventuellement reporté sur le prix global de la formation qui sera commercialisée par l’Université de Rennes sur la plateforme de FUN.

Obligations des Parties :

Le Prestataire s’engage envers l’Université de Rennes à concevoir la formation avec le plus grand professionnalisme, à respecter les dispositions légales et réglementaires applicables et à se conformer aux procédures applicables.

Le Prestataire s’engage à mobiliser les moyens techniques nécessaires à la conception de la formation qu’il s’engage ainsi à fournir, étant convenu en tant que de besoin que le Prestataire sera seul maître de la définition des moyens affectés à la conception de la formation sans que l’Université de Rennes ne puisse interférer de quelque manière que ce soit dans ce choix.

L’Université de Rennes s’engage, à travers l’équipe de pilotage du CMA CyberSkills4All et les responsables du dispositif des micro-certifications (CyberFUN), à coopérer pleinement avec le Prestataire en vue de faciliter au mieux les conditions d’intervention du Prestataire et la bonne exécution des présentes et, à cet effet, notamment :

- ne rien faire ou laisser faire qui puisse être de nature à empêcher l’exécution par le Prestataire de la Mission ou à la rendre plus difficile ou onéreuse, sous réserve de la protection légitime par l’Université de Rennes de ses intérêts ;
- transmettre en temps utile au Prestataire l’ensemble des informations nécessaires à l’exécution par ce dernier de sa Mission dans les meilleures conditions ;
- informer en temps utile le Prestataire de toute décision, tout élément et toute précision susceptible d’avoir un impact sur la Mission.

Le Prestataire s’engagera à fournir la livraison de la formation objet du présent CCTP à la date convenue entre les Parties.

5. Livraison du module

Une réunion se tiendra entre les parties au moment de la livraison du module de formation. Elle actera que le module de formation respecte bien le cahier des charges des formations et les attendus.

6. Engagements post-réalisation de la formation

Le Prestataire s’engagera pour une durée qui sera déterminée par les Parties à compter de la création des formations à réaliser les ajustements et les mises à jour liés à l’usage pédagogique de ces formations qui lui auront été demandés par l’Université de Rennes.

L’Université de Rennes pourra demander des changements au Prestataire dans la limite d’un nombre d’heures de volume horaire maximum pour la mise à jour des contenus issus de la prestation. Ce nombre d’heures sera déterminé lors de la contractualisation.

Le candidat devra indiquer clairement dans son offre tarifaire et technique la limite maximale d’ajustements ou de mises à jour compris dans son offre de base sans surcoût, en renseignant

notamment celle-ci dans l'annexe 1 à l'Acte d'Engagement « Décomposition du Prix Global Forfaitaire » (DPGF).

7. Propriété intellectuelle

Le Prestataire accepte que la réalisation de la prestation donne lieu à la création de formations qui appartiennent à l'Université de Rennes dès leur création, conformément aux articles L. 111-1 et L. 131-3 du Code de la propriété intellectuelle afin de permettre la réalisation du projet Cyberskills4All.

Sur parfait paiement de toute somme due au Prestataire et sous réserve de ce qui sera prévu au Contrat, l'Université de Rennes deviendra propriétaire des droits d'auteur afférents aux œuvres finales créées dans le cadre des services exécutés par le Prestataire.

Nonobstant la généralité de ce qui précède, le Prestataire conservera, en tout temps des droits moraux sur les créations, une licence d'utilisation, gratuite et perpétuelle sur les œuvres créées. Le Prestataire pourra donc sans l'accord de l'Université de Rennes :

- Créer plus d'un projet en utilisant les œuvres,
- Utiliser les œuvres ou une portion des œuvres pour un mandat ou un projet non prévu à la présente,

A des fins de précision, le Prestataire conservera le droit d'utiliser les textes et de réutiliser les connaissances, techniques, procédés, savoir-faire, expertise, habiletés, idées, talents et autres éléments acquis avant ou pendant l'exécution du Contrat, et ce, sans avoir à verser quelque compensation que ce soit à l'Université de Rennes.

II. Lot 1 : Réaliser une rétro-ingénierie réseau et système

1. Public visé

Cette formation s'adresse à différents professionnels et à des niveaux différents en fonction des métiers :

- Cette compétence est maîtrisée au niveau expert pour les métiers : analyste en rétro ingénierie, chercheur en sécurité des systèmes d'informations.
- Le présent lot s'adresse aux professionnels exerçant en tant Analyste SOC, Analyste en investigation numérique, chercheur en sécurité des systèmes d'information ayant un niveau de maîtrise confirmée.
- Par ailleurs, elle s'adresse également à des personnels ayant à réaliser des actes simples liés à la compétence : RSSI, coordinateur sécurité, pilote technique de réponse à incident, chercheur en sécurité des systèmes d'informations.

2. Objectif de la formation

Les objectifs principaux sont :

- Découvrir et appliquer les techniques de rétro-ingénierie
- Mettre en pratique les sujets d'extraction et d'exploitation des indicateurs de compromission issus de cette rétro-ingénierie (IoC)
- Utiliser les signatures de détection dans un contexte d'investigation

3. Objectifs pédagogiques

Les connaissances développées porteront sur l'acquisition de connaissances dans les champs suivants :

- Principes et pratiques de rétro-ingénierie
- Outils et techniques d'analyse binaire
- Outils, techniques d'analyse des logiciels malveillants

Les compétences qui seront développées seront :

- Compétences en matière d'analyse statique et dynamique,
- Compétences en matière d'analyse statique et dynamique des logiciels malveillants
- Compétences en matière d'analyse de preuves numériques

4. Modules envisagés

Le volume d'heure envisagé en formation en ligne asynchrone est évalué à 20 – 27 heures.

Ce module est imaginé avec une approche par compétences, ce qui signifie que des Travaux pratiques ou dirigés devront être proposés.

Le mode d'évaluation des compétences sera proposé, soit tout au long de la formation, soit par le biais d'un examen final, soit par un mixte de ces deux propositions.

5. Accompagnement en ingénierie pédagogique

Autonomie : pour ce lot de l'appel d'offre, le Prestataire produit seul tous les livrables demandés, allant du teaser à la formation en passant la scénarisation pédagogique du contenu. Il s'agit d'une prestation dite "autonome".

III. Lot 2 : Analyse après incident

1. Public visé

Cette formation s'adresse à différents professionnels et à des niveaux différents en fonction des métiers :

- Cette compétence est maîtrisée au niveau « Expert » pour les métiers d'Analyste en investigation numérique
- Cette compétence est maîtrisée au niveau « Confirmée » pour les métiers de RSSIO ; Coordinateur sécurité ; Opérateur analyste SOC ; Pilote technique de réponse à incident
- Cette formation s'adresse également à des personnels ayant à réaliser des actes simples liés à la compétence pour les métiers de Directeur cybersécurité ; Responsable du CSIRT ; Analyste en rétro ingénierie

A noter : Prérequis : Compétences dans la mise en place d'une station de travail d'investigation numérique.

2. Objectif de la formation

Cette formation vise à former des personnels qui auront les capacités d'agir conformément au processus de réponse à incident en utilisant efficacement les outils de forensique.

3. Objectifs pédagogiques

Les compétences développées porteront sur l'acquisition de connaissances dans les champs suivants :

- L'organisation de la cybersécurité et le processus de réponse à incident.
- Les outils et techniques de Forensique.
- Les outils de détection et en identifier les cas d'usage.
- Les données d'intérêt pour l'investigation dans un système d'exploitation
- L'analyse de malware

Les compétences qui seront développées seront :

- Agir conformément au processus de réponse à incident.
- Connaître et utiliser les outils d'investigation forensique.
- Utiliser des outils de détection d'incidents.
- Identifier et extraire les données d'intérêt pour l'investigation sur différents supports (forensique)
- Réaliser des analyses forensiques dans un système d'exploitation (windows et Linux).
- Analyser de manière approfondie les codes malveillants capturés (par exemple, forensic de malwares).

4. Modules envisagés

Le volume d'heure envisagé en formation en ligne asynchrone est évalué à 20 - 30 heures.

Ce module est imaginé avec une approche par compétences, ce qui signifie que des Travaux pratiques ou dirigés devront être proposés.

Le mode d'évaluation des compétences sera proposé, soit tout au long de la formation, soit par le biais d'un examen final, soit par un mixte de ces deux propositions.

5. Accompagnement en ingénierie pédagogie

Autonomie : pour ce lot de l'appel d'offre, le Prestataire produit seul tous les livrables demandés, allant du teaser à la formation en passant la scénarisation pédagogique du contenu. Il s'agit d'une prestation dite "autonome".

IV. Lot 3 : Analyser les flux réseaux

1. Public visé

Cette formation s'adresse à différents professionnels et à des niveaux différents en fonction des métiers :

- Cette compétence est maîtrisée au niveau « Expert » pour les métiers d'analystes SOC de niveau 3 ou analystes en investigation numérique.
- Cette compétence est maîtrisée au niveau « Confirmée » pour les métiers d'administrateurs réseau ou analystes SOC niveau 1 et 2.
- Cette formation s'adresse également à des personnels ayant à réaliser des actes simples liés à la compétence pour les métiers de RSSI, architectes sécurité, ou intégrateurs.

A noter qu'il sera fortement recommandé que les apprenants aient des acquis préalables dans les domaines des réseaux informatiques et des systèmes d'exploitation (linux, windows).

2. Objectif de la formation

Cette formation vise à former des personnels qui auront les capacités d'analyser le trafic circulant sur un réseau pour identifier des anomalies et ainsi détecter des menaces. Ils auront également la capacité de réaliser les analyses forensiques nécessaires pour planifier la mise en place des actions de remédiation et de sécurisation.

3. Objectifs pédagogiques

Les compétences développées porteront sur l'acquisition de connaissances dans les champs suivants :

- La compréhension du comportement normal d'un réseau et l'identification d'anomalies.
- L'identification d'attaques (DDOS, scan de ports, malwares, connexions suspectes, ...)
- La pratique de l'analyse de forensique

Les compétences qui seront développées seront :

- Surveiller les réseaux
- Détecter des menaces et des intrusions
- Réaliser des analyses forensiques

4. Modules envisagés

Le volume d'heure envisagé en formation en ligne asynchrone est évalué à 20h à 24h.

Ce module est imaginé avec une approche par compétences, ce qui signifie que des Travaux pratiques ou dirigés devront être proposés.

Le mode d'évaluation des compétences sera proposé, soit tout au long de la formation, soit par le biais d'un examen final, soit par un mixte de ces deux propositions.

5. Accompagnement en ingénierie pédagogie

Autonomie : pour ce lot de l'appel d'offre, le Prestataire produit seul tous les livrables demandés, allant du teaser à la formation en passant la scénarisation pédagogique du contenu. Il s'agit d'une prestation dite "autonome".

V. Lot 4 : Analyser les journaux

Cette formation peut être vue comme l'approfondissement d'une autre micro-certification développée actuellement par l'Université de Rennes. Si un candidat est intéressé par ce lot, et sous réserve qu'il signe une attestation sur l'honneur de non-divulgateur du contenu qui lui sera transmis, il sera possible de lui fournir le syllabus de la micro-certification en cours de développement à l'Université de Rennes. Cela permettra au candidat de construire sa réponse en ayant connaissance du périmètre et du niveau de la micro-certification en cours de développement à l'Université de Rennes.

1. Public visé

Cette formation s'adresse à différents professionnels et à des niveaux différents en fonction des métiers :

- Cette compétence est maîtrisée au niveau « Expert » pour les métiers d'analystes SOC de niveau 3 ou analystes en investigation numérique. Cela inclut une maîtrise avancée de l'analyse des journaux (chaînes d'attaque complexe), la corrélation multi sources pour reconstituer des incidents de sécurité avancés.
- Cette compétence est maîtrisée au niveau « Confirmée » pour les métiers d'administrateurs réseau ou analystes SOC niveau 1 et 2. Cela inclut l'utilisation d'outil de type SIEM, SOAR, l'analyse et la corrélation des journaux dans le cadre de la détection d'incidents de sécurité, et l'enrichissement des journaux à l'aide de sources externes.
- Cette formation s'adresse également à des personnels ayant à réaliser des actes simples liés à la compétence pour les métiers de RSSI, coordinateurs sécurité, ou responsables de projet sécurité. Seront couverts les bases telle la compréhension du rôle des journaux dans la cybersécurité, la collecte et l'organisation des logs, et l'identification d'anomalies simples dans les journaux.

A noter qu'il sera fortement recommandé que les apprenants aient des acquis préalables solides dans le domaine des systèmes & réseaux.

2. Objectif de la formation

Cette formation vise à former des personnels qui auront la capacité de détecter des comportements suspects au sein d'un système d'information à partir de l'examen des fichiers de journaux générés par les équipements (serveurs, pare-feu, sondes, routeurs, ...).

Ils pourront enquêter sur les incidents, en assurant la conformité avec la réglementation.

3. Objectifs pédagogiques

Les compétences développées porteront sur l'acquisition de connaissances dans les champs suivants :

- La source des données de journaux
- Le traitement des données de logs
- La compréhension des logs et l'identification d'évènements critiques
- L'automatisation de l'analyse des logs

Les compétences qui seront développées seront :

- Récupérer et mettre en forme les données de journaux générées par les équipements du SI.
- Analyser, corréler et interpréter les données de journaux
- Détecter des anomalies
- Automatiser l'analyse des logs
- Analyser des logs sur Linux et Microsoft

4. Modules envisagés

Le volume d'heure envisagé en formation en ligne asynchrone est évalué à 15 - 20 heures.

Ce module est imaginé avec une approche par compétences, ce qui signifie que des Travaux pratiques ou dirigés devront être proposés.

Le mode d'évaluation des compétences sera proposé, soit tout au long de la formation, soit par le biais d'un examen final, soit par un mixte de ces deux propositions.

5. Accompagnement en ingénierie pédagogie

Autonomie : pour ce lot de l'appel d'offre, le Prestataire produit seul tous les livrables demandés, allant du teaser à la formation en passant la scénarisation pédagogique du contenu. Il s'agit d'une prestation dite "autonome".

VI. Lot 5 : Définir une architecture de système d'information sécurisée

1. Public visé

Cette formation s'adresse à différents professionnels et à des niveaux différents en fonction des métiers :

- Cette compétence est maîtrisée au niveau « Expert » pour les métiers d'**Architecte sécurité**.
- Cette compétence est maîtrisée au niveau « Confirmée » pour les métiers de RSSI ; Auditeur de sécurité technique ; Pilote technique de réponse à incident ; Analyste en investigation numérique.
- Cette formation s'adresse également à des personnels ayant à réaliser des actes simples liés à la compétence pour les métiers de Directeur cybersécurité ; Coordinateur sécurité ; Spécialiste sécurité (dans un domaine) ; Responsable du SOC ; Administrateur de solution de sécurité ;

Auditeur de sécurité organisationnelle ; Gestionnaire de crise de cybersécurité ; Évaluateur de la sécurité des technologies de l'information ; Développeur de solutions de sécurité ; Intégrateur de solutions de sécurité.

A noter qu'il sera fortement recommandé que les apprenants aient des acquis préalables dans le domaine de l'architecture des systèmes d'information.

2. Objectif de la formation

Cette formation vise à former des personnels intervenant au sein des domaines maritime et/ou de l'aéronautique qui auront les capacités de définir des architectures de systèmes d'information sécurisées prenant en compte les contraintes spécifiques liées à ces secteurs d'activités.

3. Objectifs pédagogiques

Les compétences développées porteront sur l'acquisition de connaissances dans les champs suivants :

- architecture des systèmes d'informations
- système de management de la sécurité de l'information
- mesures de sécurité de l'information
- analyse de risques
- famille des normes ISO 27 000

Les compétences qui seront développées seront :

- Définir une architecture de système d'information
- Analyser les risques cyber propres à un système d'information donné
- Définir les mesures de sécurité en cohérence avec une analyse de risques

4. Modules envisagés

Le volume d'heure envisagé en formation en ligne asynchrone est évalué à 20 - 30 heures.

Ce module est imaginé avec une approche par compétences, ce qui signifie que des Travaux pratiques ou dirigés devront être proposés.

Le mode d'évaluation des compétences sera proposé, soit tout au long de la formation, soit par le biais d'un examen final, soit par un mixte de ces deux propositions.

5. Accompagnement en ingénierie pédagogie

Prestation partielle : pour ce lot de l'appel d'offre, le Prestataire ne répond qu'au cahier des charges des formations (cf. Annexe 2 et livrables "formation" indiqués en I.4.). Il s'agit de sous-traitance dite "partielle". L'Université de Rennes et le GIP FUN accompagnent le Prestataire pour la production des autres livrables (teaser de la formation et scénarisation pédagogique du contenu).

VII. Lot 6 : Analyse de la menace

1. Public visé

Cette formation s'adresse à différents professionnels et à des niveaux différents en fonction des métiers :

- Cette compétence est maîtrisée au niveau « Expert » pour les métiers d'Analyste de la menace cyber.
- Cette compétence est maîtrisée au niveau « Confirmée » pour les métiers de RSSI ; Auditeur de sécurité technique ; Pilote technique de réponse à incident ; Analyste en investigation numérique.
- Cette formation peut s'adresser également à des personnels ayant à réaliser des actes simples liés à la compétence pour les métiers de Directeur cybersécurité ; Coordinateur sécurité ; Spécialiste sécurité (dans un domaine) ; Responsable du SOC ; Administrateur de solution de sécurité ; Auditeur de sécurité organisationnelle ; Gestionnaire de crise de cybersécurité ; Évaluateur de la sécurité des technologies de l'information.

A noter qu'il sera fortement recommandé que les apprenants aient des acquis préalables dans le domaine des principes fondamentaux de l'analyse des menaces cyber et la capacité à analyser des intrusions au sein d'un système d'information.

2. Objectif de la formation

Cette formation vise à former des personnels qui auront la capacité à analyser la menaces cyber en prenant en compte tous ses paramètres tels que les écosystèmes criminels, la complexité des systèmes. Il aura la capacité de se confronter à des situations stratégiques, opérationnelles et techniques et sauront analyser la menace afin de reprendre l'initiative à l'attaquant

Les aspects liés à la criminologie, la planification, la géopolitique ou l'économie seront abordés.

3. Objectifs pédagogiques

Les connaissances développées porteront sur l'acquisition de connaissances dans les champs suivants :

- la criminologie et les écosystèmes criminels
- l'organisation de la cybersécurité
- la menace cyber et les outils d'analyse
- les vulnérabilités, l'analyse de risques cyber

Les compétences qui seront développées seront :

- comprendre les écosystèmes criminels, les cybermenaces et leurs contraintes
- utiliser les outils d'analyse de la menace
- analyser la menace cyber
- restituer les analyses et communiquer

4. Modules envisagés

Le volume d'heure envisagé en formation en ligne asynchrone est évalué à 20 -30 heures.

Ce module est imaginé avec une approche par compétences, ce qui signifie que des Travaux pratiques ou dirigés devront être proposés.

Le mode d'évaluation des compétences sera proposé, soit tout au long de la formation, soit par le biais d'un examen final, soit par un mixte de ces deux propositions.

5. Accompagnement en ingénierie pédagogie

Autonomie : pour ce lot de l'appel d'offre, le Prestataire produit seul tous les livrables demandés, allant du teaser à la formation en passant la scénarisation pédagogique du contenu. Il s'agit d'une prestation dite "autonome".

Annexe 1 : Terminologie et définitions

- **Micro-certification** : Relevé des acquis d'apprentissage obtenus par un apprenant à la suite d'un petit volume d'apprentissage. Ces acquis d'apprentissage auront été évalués au regard de critères transparents clairement définis. Les expériences d'apprentissage menant à des micro-certifications sont conçues pour doter l'apprenant de connaissances, aptitudes et compétences spécifiques qui répondent à des besoins sociétaux, personnels, culturels ou du marché du travail. Les micro-certifications sont détenues par l'apprenant, peuvent être partagées et sont transférables. Elles peuvent être autonomes ou être combinées pour former des certifications plus étendues. Elles sont étayées par une assurance qualité suivant des normes convenues dans le secteur ou le domaine d'activité concerné.
- **Compétences** : « La compétence peut être envisagée comme la mobilisation de manière pertinente de ses ressources (par exemple : savoirs, savoir-faire techniques, savoir-faire relationnel) et de celles de son environnement dans des situations diverses pour exercer une activité en fonction d'objectifs à finalité professionnelle à atteindre. Le résultat de sa mise en œuvre est évaluable dans un contexte donné (compte tenu de l'autonomie, des ressources à dispositions, de la situation) mais la compétence doit pouvoir être transférable d'un contexte à un autre.

Autrement dit, la compétence - combinaison de « savoirs » en action, mobilisés en vue de réaliser une activité professionnelle - s'apprécie, en tant qu'acquis de l'apprentissage selon des modalités adaptées permettant d'en certifier la possession et au regard de l'atteinte d'un résultat pour un niveau d'exigence prédéterminé.

Enfin, la compétence contribuant à la réalisation d'une activité, il convient de retenir que la cohérence du référentiel d'activités constitue les fondations du référentiel de compétences.¹¹»

- **Formation** : Ensemble cohérent de ressources, avec leur évaluation, qui amène à la maîtrise d'une connaissance et d'une compétence que l'on définit sous le nom d'une micro-certification (7 à 30 heures) ou d'un bloc d'apprentissage (pas d'approche compétence obligatoire, 15 heures).

Dans la proposition CyberSkills4All, une formation est nommée “ressources de formation”.

Les ressources et formations ciblées dans le projet CyberSkills4All sont prioritairement développées pour la formation distancielle et asynchrone.

- **FUN'IP** : service d'ingénierie pédagogique de France Université Numérique.
- **Œuvre** : Toute création qui répond à la définition du code de la propriété intellectuelle. L'auteur d'une formation doit s'assurer de son droit d'exploiter une œuvre dans la création de sa ressource et il peut sous certaines conditions bénéficier des droits sur celle-ci. Attention à privilégier de courts extraits de textes, l'utilisation de média en *creative common* (CC-Zero, -BY -BY-SA -BY-ND et -BY-NC pour les blocs d'apprentissage).
- **Parcours** : ensemble de micro-certifications assemblées dans une logique d'apprentissage plus long. Le parcours de formation est mis en œuvre par l'entité qui exploite une ou plusieurs formations.

¹¹ <https://www.fun-mooc.fr/fr/categories/types/formation-professionnelle/micro-certification/>

- **Référentiels de compétences, de formation et de certification** : Description en compétences d'une micro-certification, modalités et critères d'évaluation : voir les publications de [France](#) Compétence.
- **Ressources** : élément atomique constitutif d'une formation.
Il peut s'agir d'un document textuel, d'une illustration, d'une vidéo, d'une activité interactive, etc. Les ressources sont potentiellement remobilisables dans différents contextes de formation.
- **Séquence d'apprentissage** : ensemble de ressources scénarisées en un ensemble d'une durée de 1h à 1h30 formant un chapitre de la formation.
- **Scénario pédagogique** : « (...) outil de conception pédagogique. Il prend la forme d'un document écrit formalisant l'organisation et le déroulement d'un cours, d'une séquence ou d'un projet d'enseignement et de formation. Il est initié par un enseignant et/ou une équipe pédagogique et s'inscrit dans une échelle de temps définie et un contexte et un environnement donnés.¹²»
- **Syllabus** : « (...) présentation générale d'un cours. Il implique une synthèse globale d'éléments structurant un enseignement (intitulé du cours, objectifs et sous objectifs d'apprentissages ou compétences visés, volume horaire, séances, activités pédagogiques, modalités d'évaluation, bibliographie, etc.).³»

Annexe 2 : Cahier des charges des formations du CMA CyberSkills4All

Annexe 3 : Charte graphique du CMA CyberSkills4All

Annexe 4 : Trame de réponse à fournir

¹² <https://www.fun-mooc.fr/fr/>