Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence «ANR-23-CMAS-0026».



DÉFINIR UNE ARCHITECTURE DE SYSTÈME D'INFORMATION SÉCURISÉE

« Explorer ce qui fait la robustesse, la cohérence et la sécurité d'un système d'information afin de concevoir et d'évaluer une architecture de SI où la sécurité est au cœur de chaque décision. »

SYLLABUS

Bienvenue dans la formation "Définir une architecture de système d'information sécurisée".

Ce syllabus a pour fonction de vous fournir un aperçu clair des étapes du parcours et des ressources mises à votre disposition en précisant notamment ses objectifs, son programme et ses méthodes pédagogiques. Il est pensé comme un guide pratique dans

lequel vous trouverez toutes les informations nécessaires pour suivre le fil conducteur de la formation et anticiper les prochaines étapes.

Nous vous invitons à le consulter régulièrement pour tirer pleinement parti de cette formation.

INFORMATIONS GÉNÉRALES

Titre du cours : Définir une architecture de système d'information sécurisée

Prix : 1 430 €

Dates : du 30 novembre 2026 au 6 février 2027

Durée en semaine : 7

Effort (h) : 26 heures

Rythme recommandé par semaine : 4 heures par semaine

Permanences virtuelles : 3 heures - 1 heure toutes les 2 semaines

Langues : Français

PRÉREQUIS

Prérequis de connaissances / compétences : La formation s'adresse à des professionnels disposant de connaissances fondamentales dans les domaines suivants :

- Le fonctionnement général d'un système d'information (réseaux, serveurs, applications, stockages, etc.) ;
- Les concepts de base de la cybersécurité (confidentialité, intégrité, disponibilité, authentification, contrôle d'accès, etc.).

ÉQUIPEMENT REQUIS

Un ordinateur avec une connexion internet.

INSCRIPTION AUPRÈS DE L'UNIVERSITÉ DE RENNES

En vous inscrivant, vous accéderez à la formation portée par l'Université de Rennes, qui va certifier la formation.

TEST DE POSITIONNEMENT POUR RÉUSSIR VOTRE MICRO-CERTIFICATION

Avant de vous inscrire, si vous souhaitez évaluer vos connaissances, vous pouvez accéder à un test de positionnement. Le lien est disponible sur le catalogue.

RESPONSABLE PÉDAGOGIQUE



Simon PRAUD : Spécialisé dans la gouvernance, la gestion des risques et la conformité (GRC), il occupe aujourd'hui le poste de référent cybersécurité gouvernance au sein de Wallack. En parallèle de ses missions de conseil, Simon est responsable de la gestion de l'organisme de formation. Il a développé et animé des parcours complets de sensibilisation à la cybersécurité ou d'introduction aux mesures de cybersécurité, adapté à la fois aux entreprises et aux établissements d'enseignement supérieur. Ce programme vise à rendre la cybersécurité accessible à tous, en vulgarisant les enjeux et les bonnes pratiques, que ce soit pour des profils techniques ou non techniques. Il intervient régulièrement en tant que formateur sur des thématiques comme la gestion des risques, la continuité d'activité (PCA/PRA) et la sensibilisation des utilisateurs à la cybersécurité.



Alexandre MATTHEY-DORET : Spécialisé dans la gouvernance de la sécurité, la gestion des risques et la conformité, il accompagne les organisations dans l'identification et la maîtrise de leurs risques cyber, la réalisation d'analyses de risques, la conduite d'audits de sécurité ainsi que la définition de mesures adaptées aux enjeux métiers et réglementaires. Au cours de sa carrière, il a évolué dans des environnements variés et conduit de nombreuses missions stratégiques, notamment l'homologation de sécurité de systèmes d'information sensibles (SI PVID, SI DR, SI bancaires, etc.), ainsi que la préparation, l'obtention et le renouvellement de certifications ISO 27001. En parallèle de ses activités de RSSI, Alexandre conçoit et anime des formations en cybersécurité auprès de différents publics. Il intervient notamment dans le cadre de formations destinées aux futurs RSSI ainsi qu'auprès d'étudiants spécialisés en cybersécurité à la cybersécurité



Alice GONTARD : Référente cybersécurité gouvernance au sein de Wallack, elle accompagne les organisations dans la mise en œuvre et l'amélioration de leur Système de Management de la Sécurité de l'Information (SMSI), la réalisation d'analyses de risques ainsi que la structuration de leurs démarches de conformité. Dans le cadre de ses missions, elle intervient sur la mise en conformité aux référentiels tels que l'ISO 27001 et l'ISO 22301, l'élaboration de politiques de sécurité, la réalisation d'audits ainsi que la définition de plans de continuité et de reprise d'activité (PCA/PRA). Son rôle consiste également à formuler des recommandations pragmatiques et à accompagner les équipes dans le déploiement de solutions adaptées à leurs contraintes métiers, techniques et réglementaires. En parallèle, Alice conçoit et anime des formations destinées aux professionnels, étudiants et cadres sur les thématiques de la gouvernance, de la gestion des risques, de la continuité d'activité et de la sensibilisation à la cybersécurité.



Emeric MARCHAND : Spécialisé dans les domaines de la gouvernance de la sécurité de l'information et de la sensibilisation à la cybersécurité, il accompagne les organisations dans le renforcement de leur posture de sécurité à travers des approches opérationnelles. Au sein de Wallack, il intervient sur des sujets liés à la gouvernance de la cybersécurité, notamment la mise en place et l'amélioration de Systèmes de Management de la Sécurité de l'Information (SMSI), la rédaction de Politiques de Sécurité des Systèmes d'Information (PSSI) ainsi que l'accompagnement des organisations dans leurs démarches de conformité. Il intervient notamment sur les exigences de la norme ISO 27001. En parallèle, Emeric anime des actions de sensibilisation à la cybersécurité destinées aux collaborateurs et aux équipes métiers. Ses interventions portent sur les principales menaces numériques, les bonnes pratiques de sécurité et les comportements à adopter pour réduire les risques liés au facteur humain.



Guillaume MOREL : Spécialisé dans les domaines techniques, il a notamment évolué au sein du CEA (Commissariat à l'Énergie Atomique et aux Énergies Alternatives), dans un environnement à très forts enjeux de sécurité, où il a participé à la mise en place d'une solution SIEM (Security Information and Event Management) dédiée à la centralisation des journaux, à la supervision des infrastructures et à la détection proactive des incidents de sécurité. Au sein de Wallack, il accompagne les organisations dans le déploiement de solutions de supervision et dans l'amélioration de leurs capacités de détection et de réaction face aux incidents de sécurité. Ses missions lui ont permis de développer une expertise concrète en supervision de la sécurité, détection d'anomalies, gestion des incidents et ingénierie des systèmes sécurisés. Parallèlement, Guillaume conçoit et anime des formations spécialisées dans les domaines de la supervision de la sécurité et de la supervision réseau.



Loris LIZE : Spécialisé en cybersécurité et formé à l'école Pôle Sup de La Salle, son activité professionnelle est centrée sur la conception d'architectures réseaux et systèmes sécurisées, intégrant les besoins métiers, les contraintes techniques, les exigences de sécurité ainsi que les enjeux de performance opérationnelle. Il accompagne les organisations dans la définition et la mise en œuvre d'infrastructures fiables et résilientes, en veillant à intégrer dès les premières phases de conception les principes de cloisonnement, de disponibilité et les bonnes pratiques de cybersécurité. Au cours de ses différentes missions, il a développé une solide expertise en architecture sécurisée lui permettant de proposer des solutions concrètes, efficaces et adaptées aux contextes spécifiques de chaque structure. En parallèle, Loris conçoit et anime des formations portant sur les réseaux, l'administration sécurisée des systèmes ainsi que les fondamentaux de la cybersécurité. Il intervient aussi bien auprès de professionnels que d'étudiants.



Solène PAULIN : Spécialisée dans la gouvernance de la sécurité, la gestion des risques et la continuité d'activité, elle accompagne les organisations dans la structuration de leur démarche de cybersécurité et dans le renforcement de leur résilience. Dans le cadre de ses missions, elle intervient sur des problématiques liées à la continuité et à la reprise d'activité, en accompagnant les structures dans la définition, la formalisation et le test de leurs dispositifs de PCA/PRA. Elle participe également à la formalisation de politiques de sécurité, à l'amélioration continue des dispositifs de gouvernance et à l'intégration des bonnes pratiques de cybersécurité au sein des organisations. En parallèle, Solène anime des actions de sensibilisation et des formations dédiées à la cybersécurité, avec une expertise particulière sur les thématiques de continuité d'activité et de résilience organisationnelle.

ÉTABLISSEMENTS

Wallack

Université de Rennes

DESCRIPTION

La formation est proposée entièrement en distanciel asynchrone, afin de s'adapter aux contraintes professionnelles et organisationnelles des apprenants. Elle repose sur un parcours structuré, rythmé et accompagné, combinant différents formats pédagogiques pour favoriser la montée en compétences. Elle comprend :

- Des ressources pédagogiques accessibles en ligne à tout moment, sous forme de vidéos explicatives, de fiches mémo, de supports PDF détaillés et de schémas interactifs, permettant aux apprenants de progresser à leur rythme.
- Des quiz de validation à la fin de chaque module, conçus pour permettre aux apprenants de vérifier la bonne assimilation des concepts clés et de renforcer leur compréhension ;
- Des travaux pratiques, destinés à mettre en application les connaissances acquises et à développer des compétences opérationnelles sur des cas concrets.

L'objectif pédagogique est de garantir un équilibre entre autonomie, interaction et accompagnement, favorisant une appropriation efficace et durable des compétences

OBJECTIFS

Sur le plan de l'offre de formation existante, ce module se positionne comme un complément stratégique aux formations généralistes en cybersécurité. Là où nombre de parcours se concentrent principalement sur la gestion des risques, la gouvernance ou la conformité, cette formation apporte une approche centrée sur la sécurisation des systèmes d'information dès la phase d'architecture. Elle répond à un besoin clairement identifié sur le marché : le manque de profils capables de concevoir, d'évaluer ou d'améliorer des architectures sécurisées, adaptées aux environnements complexes et critiques, en tenant compte à la fois des contraintes métiers, des exigences techniques et des référentiels normatifs (tels que les familles de normes ISO 27000, ou les standards propres aux systèmes industriels et critiques).

À la fin de cette formation, les participants seront en mesure de :

1. Définir une architecture de système d'information sécurisée

> Le positionnement de cette formation est résolument tourné vers le développement de compétences immédiatement mobilisables. Elle est conçue pour répondre aux attentes de plusieurs catégories de métiers de la cybersécurité. Elle s'adresse en priorité aux architectes sécurité, pour qui la compétence de définir une architecture de système d'information sécurisée constitue un socle indispensable.

2. Evaluer, auditer, comprendre les architectures sécurisées

> Elle est également parfaitement adaptée aux RSSI, aux auditeurs de sécurité technique, aux pilotes techniques de réponse à incident, ainsi qu'aux analystes en investigation numérique, pour lesquels la compréhension approfondie des architectures sécurisées et la capacité à les évaluer, les auditer ou les challenger est une compétence clé.

3. Analyser les risques cyber propres à un système d'information donné

> Cette formation est pertinente pour des professionnels occupant des fonctions connexes à l'architecture ou à la gouvernance de la cybersécurité, tels que les directeurs cybersécurité, coordinateurs sécurité, responsables SOC, administrateurs ou intégrateurs de solutions de sécurité, développeurs de solutions sécurisées, auditeurs organisationnels, ou encore gestionnaires de crise.

4. Définir les mesures de sécurités en cohérence avec l'analyse de risques réalisée

> La formation permettra à l'apprenant d'être plus pertinent dans ses prises de décision, ses recommandations et ses actions opérationnelles.

PROGRAMME / DEROULÉ

1. **Introduction à l'architecture sécurisée d'un SI (2h)**
   - Introduction à la formation
   - Introduction à l'architecture sécurisée théorique
   - Quiz
2. **TP architecture sécurisée d'un SI (4h30)**
   - Réalisation du TP en individuel (cartographie, identification des zones critiques et rédaction d'un rapport)
   - Correction du TP et explications
3. **Le SMSI (4h)**
   - Le SMSI
   - Les normes ISO/IEC 27000
   - Quiz
   - Mesures de sécurité de l'information
   - Quiz
4. **Analyse de risque EBIOS RM partie 1/3 (6h)**
   - Objectifs, concepts et méthodes
   - Quiz
   - TP valeur métier, évènement redoutés, sources de risques et objectifs visés
   - Corrections
5. **Analyse de risque EBIOS RM partie 2/3 (4h40)**
   - TP parties prenantes, scénarios stratégiques et opérationnels (4h)
   - Corrections (40 minutes)
6. **Analyse de risque EBIOS RM partie 3/3 et conclusion (4h50)**
   - TP traitement des risques et mesures de sécurité (3h50)
   - Correction (30 minutes)
   - Clôture de la formation (30 minutes)

COMPÉTENCES VISÉES

- S0023 : Capacité à concevoir des mesures de sécurité fondées sur les concepts et les principes de la cybersécurité.
- S0034 : Capacité à discerner les besoins de protection (c'est-à-dire les mesures de sécurité) des systèmes d'information et des réseaux.

RESSOURCES PÉDAGOGIQUES ET ATTENDUS

Le parcours combine différentes modalités pour favoriser l'acquisition des compétences :

- Vidéos pédagogiques : des capsules thématiques (segmentation réseau, passerelle d'internet sécurisé, SMSI, famille de normes 27 000, etc.) ;
- Supports théoriques : des fiches techniques, présentations PowerPoint enrichies, guides méthodologiques, etc. ;
- Travail personnel : questionnaires à choix multiples (QCM) ou quiz de validation des connaissances ;
- Travaux pratiques (TP) :

- Modélisation d'une architecture sécurisée d'un Système d'Information : à partir d'un cas d'usage ;
- Réalisation d'une analyse de risque sur un système d'information fourni. Cette analyse est découpée en plusieurs étapes progressives, permettant aux participants de maîtriser chaque phase de la méthode.

À chaque étape clé, un modèle ou un canevas sera fourni, garantissant que tous les stagiaires partent avec les mêmes bases et les mêmes chances de réussite. Cela permet de se concentrer pleinement sur la compréhension de la méthode et des mécanismes d'évaluation des risques, sans être pénalisé par des écarts de forme ou de présentation.

Les TP sont conçus comme des situations professionnelles réalistes, permettant de mobiliser les connaissances acquises et de les traduire en compétences opérationnelles

La formation est réalisée en autonomie avec des temps d'accompagnement destinés à favoriser la progression des apprenants tout au long du parcours. Vous y trouverez des ressources variées telles que des vidéos, des documents de référence, des fiches pratiques et des Travaux Pratiques pour mettre en application les contenus théoriques. Ces ressources sont complétées par des quiz permettant de vérifier progressivement votre progression.

Vous serez également invités à participer aux échanges au travers des forums, afin de partager votre expérience, vos représentations, et enrichir votre réflexion.

Vous bénéficiez de **3 heures de permanence virtuelle**, à raison d'1 heure toutes les 2 semaines.

Nous vous recommandons de consulter régulièrement les ressources pédagogiques, de réaliser les activités et les évaluations proposées, et de participer aux échanges dans les forums afin de tirer pleinement profit de la formation.

ASSIDUITÉ ET VALIDATION DE LA FORMATION

Certaines activités sont obligatoires pour témoigner de votre assiduité et pour l'obtention de votre micro-certifications. Elles vous seront précisées dans l'espace de formation.

La validation de la formation est conditionnée par l'achèvement d'activités qui jalonnent le parcours et attesteront de son suivi.

Ces activités sont :

- Les modules asynchrones ;
- Les tests et quiz ;
- Les TP réalisés et corrigés.

ÉVALUATION ET CERTIFICATION

L'évaluation repose sur un modèle par compétences, avec deux types de validations.

Évaluations formatives :

Quiz de validation des connaissances à l'issue de chaque séquence théorique, permettant aux apprenants de vérifier leur compréhension des notions abordées avant de poursuivre.

Évaluation certificative (SAE) :

Les travaux pratiques réalisés tout au long de la formation font l'objet d'une évaluation, visant à valider l'acquisition des compétences suivantes :

- *Définir une architecture de système d'information sécurisée ;*

- *Analyser les risques cyber propres à un système d'information donné ;*
- *Définir les mesures de sécurité adaptées et cohérentes avec une analyse de risques.*

Chaque TP fera l'objet d'une évaluation en cohérence avec la grille de notation créée pour la micro-certification.

→ *Pour accompagner les apprenants tout au long de leur progression, des vidéos d'aide intermédiaires seront mises à leur disposition. Ces vidéos sont conçues pour débloquer des situations spécifiques dans le cadre des travaux pratiques, en apportant des explications ou des démonstrations ciblées.*

Toutefois, afin de valoriser l'autonomie et de préserver la dimension évaluative des travaux pratiques, le recours à ces vidéos entraîne une pénalité sur la note du TP concerné. Cette règle vise à encourager les apprenants à mobiliser en priorité leurs compétences et les ressources fournies avant de solliciter cette aide supplémentaire.

Néanmoins, l'objectif reste de favoriser la réussite et la continuité des apprentissages : un apprenant en difficulté pourra ainsi choisir de visionner la vidéo pour se débloquer et poursuivre son travail, tout en acceptant la minoration partielle de sa note.

Par ailleurs, un accompagnement pédagogique sera proposé avec un forum de réponses aux questions des apprenants et l'animation par l'expert pédagogique de la formation d'une classe virtuelle hebdomadaire.

Les apprenants en situation de handicap sont invités à se rapprocher de leur gestionnaire administratif (coordonnées dans le contrat de formation) pour une adaptation des modalités d'évaluation.

ACCESSIBILITÉ

Nos formations sont ouvertes à toutes et à tous. Si vous présentez un handicap (moteur, visuel, auditif, cognitif, trouble dys ou maladie invalidante), un aménagement spécifique est peut-être possible.

Avant de vous inscrire ou dès votre convocation, contactez notre référent handicap pour étudier ensemble vos besoins et adapter l'accueil, les supports pédagogiques ou les rythmes de la session, contact : pve@univ-rennes.fr.

Cette formation a été conçue pour être accessible au plus grand nombre. Les équipes de conception ont veillé à respecter autant que possible les recommandations du Référentiel Général d'Amélioration de l'Accessibilité (RGAA), publié par la Direction Interministérielle du Numérique. En particulier, toutes les vidéos incluent un sous-titrage et une transcription téléchargeable.

Vous pouvez également signaler à tout moment un problème d'accessibilité au responsable pédagogique ou à un tuteur afin que des solutions adaptées soient rapidement mises en place.

AIDE ET CONTACTS

Pour toute question sur le fonctionnement de la plateforme ou de votre compte FUN : formapro@fun-mooc.fr

Pour tout renseignement sur le contenu de la formation ou toute question d'ordre pédagogique, écrivez à cette adresse.

COMMUNICATION

En amont de la formation

Pour toute question sur le fonctionnement de la plateforme ou de votre compte FUN vous pouvez nous contacter via l'espace suivant : https://www.fun-mooc.help/hc/fr

Pendant la formation

Pour communiquer avec le responsable pédagogique, un forum dédié est à votre disposition. Vous pouvez y poser des questions générales sur la formation, des questions spécifiques sur le contenu des ressources proposées, ou préparer vos interventions pour les deux sessions synchrones. Les messages sont consultés quotidiennement, avec un délai de réponse maximal de trois jours.

Un espace dédié est prévu pour les questions techniques liées à la plateforme. Cet espace vous permet de signaler des problèmes et de contacter directement l'assistance techno-pédagogique.

Nous vous encourageons à maintenir un climat respectueux et collaboratif dans tous vos échanges – qu'ils soient avec l'enseignant, l'ingénieur pédagogique, les tuteurs ou vos pairs.