Label
Smart & Secure IoT

Programme détaillé

Contact organisme de formation

Digital 113

Contacts formateurs

SCASSI
209 rue Jean BART
31670 Labège

Téléphone : 0561170854 Email : contact@scassi.com Site internet : https://www.scassi.com/	Sas créée le 01/03/2005 au capital de 40 000 € enregistrée à Toulouse Gérée par : M. Laurent PELUD Siret : 48120469100036

Présentation du formateur

Scassi est un groupe fondé en 2005, expert de la cybersécurité des systèmes critiques.
Le groupe est constitué de 3 filiales spécialisées.

SCASSI. be secure — Notre mission, sécuriser les systèmes critiques et embarqués

phosforea by SCASSI group — Nous engageons vos collaborateurs dans la cybersécurité de votre entreprise

june cybersec factory — Nous produisons des logiciels SSI uniques et des équipements Industriels IoT cybersécurisés

Présentation du label Smart & Secure IoT

La menace cybercriminelle persistante s'applique aujourd'hui aux objets connectés (IoT) tout comme à l'IT; il est donc nécessaire d'instaurer de la confiance entre les entreprises industrielles utilisatrices d'IoT et les entreprises productrices de matériels, de solutions et de services IoT.

Le label "Smart & Secure IoT" est un socle technique et organisationnel qui établit un standard essentiel en termes de cybersécurité pour toute entreprise concevant, fabriquant ou exploitant des équipements de l'Internet des Objets. Ce label a été développé par Scassi.

Le label "Smart & Secure IoT" sera délivré à travers des critères constitutifs du label. Les thématiques abordées :

- Gestion des risques et des processus
- Gestion des accès
- Gestion des mises à jour
- Traitement des évènements
- Chiffrement des données
- Gestion des configurations
- Gestion de la documentation
- Gestion des aspects juridiques

Le label "Smart & Secure IoT" est délivré par le comité d'attribution du label qui sera constitué et piloté par Digital 113.

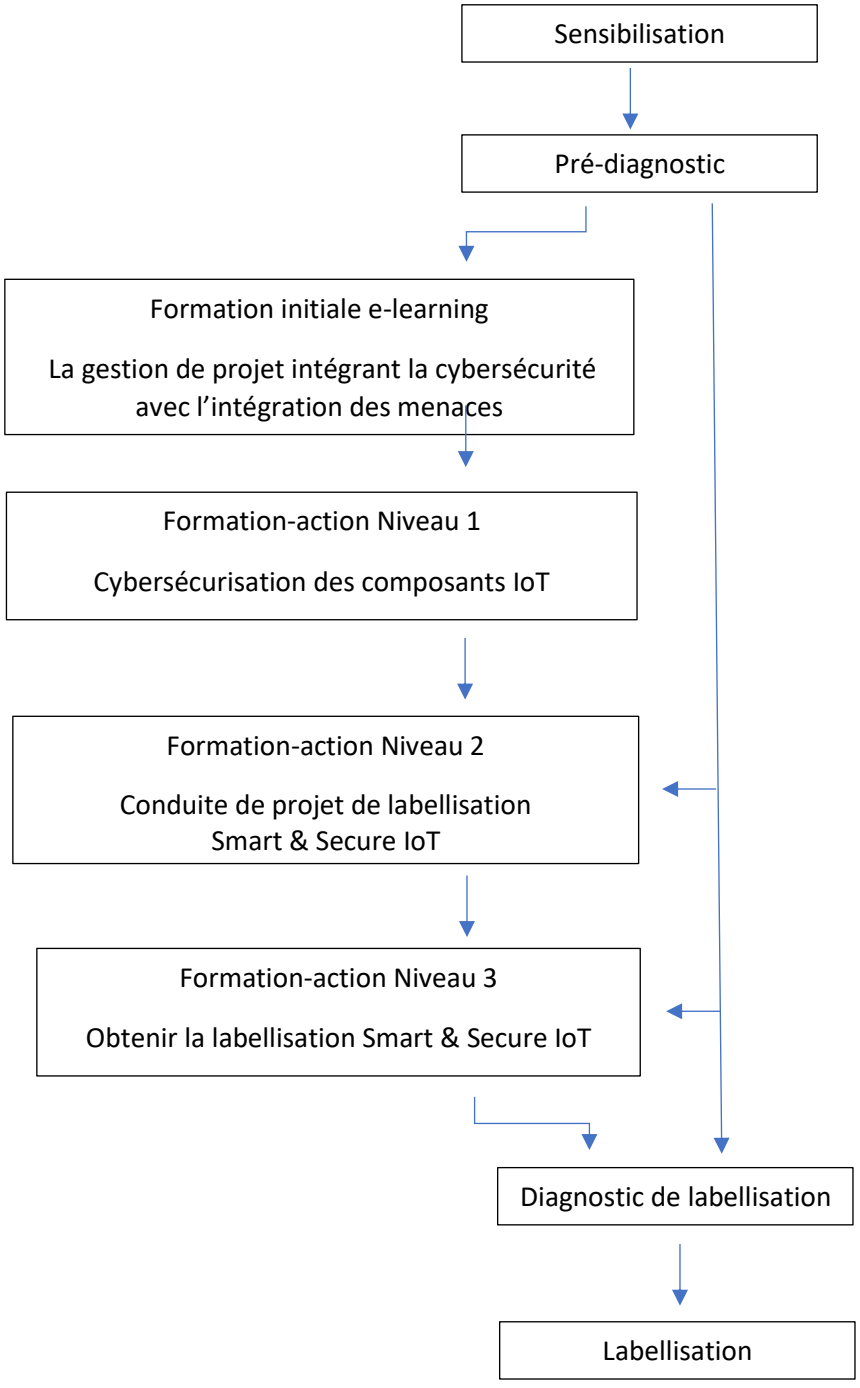
Le label est délivré 3 fois par an à l'issue des sessions du comité du label en novembre, février et juin.

Présentation du dispositif

L'entrée dans le dispositif se fait par manifestation d'intérêt et rencontre lors des réunions de sensibilisation au label « Smart & Secure IoT » en région

Un pré-diagnostic permet d'évaluer la maturité du projet porté par l'entreprise et de structurer son programme de formation-action spécifique.

A l'issue de ce parcours adapté, l'entreprise disposera d'un diagnostic de maturité complet de son projet d'IoT. Il lui permettra de soumettre son projet au comité de labellisation « Smart & Secure IoT ».



Le financement

Afin de soutenir la mise en place du dispositif, **la DIRECCTE OCCITANIE finance 50% des coûts des PME participantes et de leurs salariés**, répondant aux critères de public cible, sous réserve d'étude du dossier. Les PME participantes doivent avoir moins de 250 salariés.

Le reste à charge des formations peut faire l'objet d'une demande de financement auprès de votre OPCO, sous réserve de l'éligibilité de l'entreprise et des critères en vigueur***. Il appartient à l'entreprise de vérifier ces éléments auprès de son OPCO.***

Modules	**Coût**	**Prise en charge possible à 50% par la Direccte**	***Financement possible par votre OPCO***	**Reste à charge**
Pré-diagnostic	1 100 € HT	550 € HT	-	550 € HT
Formation initiale e-learning	350 € HT	175 € HT	175 € HT	
Formation action initiale	900 € HT	450 € HT	450 € HT	
Formation action niveau 2	900 € HT	450 € HT	450 € HT	
Formation action niveau 3	900 € HT	450 € HT	450 € HT	
Labellisation	2 200 € HT	1 100 € HT	-	1 100 € HT

Sensibilisation au label Smart and Secure IoT

Intervenant : Consultant Scassi
Public cible : TPME de la filière numérique en Occitanie
Modalités pédagogiques : Rencontres publiques ouvertes aux porteurs de projets et dirigeants d'entreprises ayant un projet lié à l'IoT industriel.

Durée : 1 h
Lieu : en visioconférence ou en présentiel selon les conditions
Coût : gratuit

Objectifs
A la fin de cette réunion, les participants doivent être conscients des impacts de la démarche de labellisation « Smart and Secure IoT » et avoir compris le dispositif proposé par Digital 113.

A la fin de cette réunion, les participants reçoivent par email un document pdf d'information sur le dispositif, les interlocuteurs et des conseils méthodologiques pour se préparer au pré-diagnostic.

Plan d'intervention

- Accueil et présentation du contexte de l'action collective et des prestations de Digital 113
- Présentation des enjeux de la cybersécurité de l'IoT
- Retour d'expérience sur des cas d'IoT compromis et impact sur les entreprises et réseaux
- Présentation du label « Smart and Secure IoT »
- Création de valeur liée au label et ROI pour l'entreprise
- Présentation de la démarche de labellisation et du pré-diagnostic
- Présentation du programme spécifique de formation-action de Digital 113 pour le label
- Questions et échanges avec les participants

Méthode pédagogique
Présentation plénière interactive illustrée avec des études de cas permettant d'assimiler et de contextualiser la formation.

Pré-diagnostic

Intervenant : Consultant Scassi
Public cible : Chef de projet innovation, bureau d'études, R&D, Directeur, Directeur commercial, RSSI / CISO quand existant, Concepteurs, développeurs, Responsable qualité
Modalités pédagogiques : audit diagnostic
Lieu : selon projet, en entreprise ou à distance
Durée : 8h
Coût : 1100 €HT par entreprise

Objectifs
Etablir un pré-diagnostic de la maturité du projet de l'entreprise par rapport au référentiel « Smart & Secure IoT » et établir un programme de formation-action adapté.

La démarche
La conformité au label « Smart & Secure IoT » est évaluée au regard du label et en appliquant la démarche d'évaluation de Scassi.

Le contexte et les spécificités de l'entreprise et de son projet sont pris en compte par les experts Scassi. C'est au travers des documents fournis et d'entretiens avec le porteur du projet que l'auditeur, va mesurer la maturité du projet, proposer, le cas échéant, des axes d'amélioration et poser un diagnostic opérationnel.

Action enclenchée suite au pré-diagnostic
Le projet candidat est orienté, en fonction de sa maturité, vers :

- Un accompagnement par un programme formation-action adapté
- Une labellisation lors de la prochaine campagne de labellisation

Organisation
Ce diagnostic est réalisé pour chaque projet présenté. Il est confidentiel à l'entreprise.

Plan d'intervention

- Organisation et préparation du pré-diagnostic, signature de la convention de pré-diagnostic (clause de confidentialité, interlocuteurs, circuit de diffusion, etc.)
- Réunion de lancement et prise d'informations et échanges sur le projet (par vidéoconférence ou rendez-vous, selon le projet et les recommandations de l'auditeur Scassi)
- Etude du projet par les experts Scassi
- Etablissement et transmission du pré-diagnostic à l'entreprise
- Restitution et de clôture de l'audit (par vidéoconférence ou rendez-vous, choix de l'auditeur Scassi)
- Transmission du rapport de pré-diagnostic synthétique
- Proposition d'un programme de formation-action à Digital 113 et à l'entreprise

Livrable

- Rapport d'audit de pré-diagnostic détaillé pour l'entreprise
- Proposition de programme de formation-action

Formation initiale e-learning

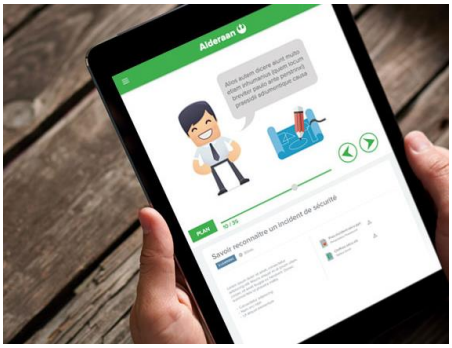
Référence : Module e-learning

Intitulé de la formation : La gestion de projet intégrant la cybersécurité, avec l'intégration des menaces.

Public cible : Chef de projet innovation, bureau d'études, R&D, Directeur, Directeur commercial, RSSI / CISO quand existant, Concepteurs, développeurs, Commercial, Responsable qualité, tout collaborateur
Prérequis : Quelques années d'expériences dans le domaine de l'IOT
Lieu : formation distancielle en ligne
Durée : 6 modules de e-learning de 30 minutes environ
Coût : 350 € HT par entreprise

Accessibilité **:** Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toute demandes spécifiques afin de l'on adapte au mieux nos modalités de formation (aménagement des horaires, des lieux, des supports…)

Objectifs
Accompagner un premier travail individuel en e-learning permettant d'acquérir ou revoir les notions du socle de base en cybersécurité



Contenu de la formation :

- La sécurité : un actif des projets
- Perception du risque
- Exigences de sécurité
- Tests de sécurité
- Dossier de sécurité et MCS
- Evaluation

Organisation
Cette étape du programme de formation est réalisée en autonomie par l'équipe de l'entreprise porteuse du projet.

Le formateur dispose via la plateforme de e-learning, d'éléments de suivi de chaque apprenant (suivi, évaluation, etc.).

Modalité d'évaluation :

- Test des acquis tout au long de la formation via différents exercices
- Questionnaire d'évaluation
- Evaluation à froid à 3 mois

Modalité de validation : Attestation de formation

Modalités pédagogiques :
Une journée en présentiel de présentation interactive et pratique des concepts théoriques présentés dans la partie distancielle.
Manipulations et mises en situations permettant d'assimiler les concepts et de contextualiser la formation.

Méthodes pédagogiques :

Expositives, Participatives, Interrogatives

Outils pédagogiques/support :

Support powerpoint, base documentaire, matrice de travail, cas pratiques…

INTERVENANTS :
Système de e-learning Phosforea, M. MONNIER, Mme REZE, M. LONGCHAMPS

INSCRIPTION :

Modalité : Groupe constitué en fonction de la demande

Délai : Inscription jusqu'à 48h avant l'entrée en formation

Contact : Mathilde Alarçon – formation@digital113.fr - 07 86 06 95 29

Formation-action niveau 1

Référence : Module 1

Intitulé de la formation : Cybersécurisation des composants IoT

Public cible : Chef de projet innovation, bureau d'études, R&D, Directeur, Directeur commercial, RSSI / CISO quand existant, Concepteurs, développeurs, Commercial, Responsable qualité, tout collaborateur
Prérequis : Quelques années d'expériences dans le domaine de l'IOT
Lieu : en région Occitanie (site Digital 113 de Toulouse et Montpellier)
Durée : 8 heures
Coût : 900 € HT par participant

Accessibilité **:** Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toute demandes spécifiques afin de l'on adapte au mieux nos modalités de formation (aménagement des horaires, des lieux, des supports…)

Objectifs

A l'issue de la formation, les porteurs de projets dans les entreprises devront être en capacité de monter en compétence sur la problématique de cybersécurisation des composants IoT.

Contenu de la formation :

- Comprendre l'ensemble des chapitres du label « Smart and Secure IoT »
- Présenter la démarche globale de labellisation « Smart and Secure IoT », son périmètre et ses exigences
- Impliquer l'ensemble des collaborateurs concernés dans un projet de labellisation
- Être en mesure de démontrer l'évolution des éléments en termes de cybersécurité IoT ainsi que les actions mises en place et leur suivi dans le temps
- Tracer l'ensemble de la démarche du projet de labellisation pour son entreprise

Modalité d'évaluation :

- Test des acquis tout au long de la formation via différents exercices
- Questionnaire d'évaluation
- Evaluation à froid à 3 mois

Modalité de validation : Attestation de formation

Modalités pédagogiques :

Une journée en présentiel de présentation interactive et pratique des concepts théoriques présentés dans la partie distancielle.
Manipulations et mises en situations permettant d'assimiler les concepts et de contextualiser la formation.

Méthodes pédagogiques :

Expositives, Participatives, Interrogatives

Outils pédagogiques/support :

Support powerpoint, base documentaire, matrice de travail, cas pratiques…

INTERVENANTS :
M. MONNIER, Mme REZE, M. LONGCHAMPS, M. CRASNIER

INSCRIPTION :

Modalité : Groupe constitué en fonction de la demande

Délai : Inscription jusqu'à 48h avant l'entrée en formation

Contact : Mathilde Alarçon – formation@digital113.fr - 07 86 06 95 29

Formation-action niveau 2

Référence : Module 2

Intitulé de la formation : Conduite de projet de labellisation Smart & Secure IoT

Public cible : Chef de projet innovation, bureau d'études, R&D, Directeur, Directeur commercial, RSSI / CISO quand existant, Concepteurs, développeurs, Commercial, Responsable qualité, tout collaborateur
Prérequis : Quelques années d'expériences dans le domaine de l'IOT
Lieu : Digital 113
Durée : 8 heures
Coût : 900 € HT par participant

Accessibilité **:** Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toute demandes spécifiques afin de l'on adapte au mieux nos modalités de formation (aménagement des horaires, des lieux, des supports…)

Objectifs

A l'issue de cette formation le participant dispose d'une capacité à mettre en place un plan d'action pour soumettre leur projet à labellisation et plus généralement un projet d'IoT cybersécurisé.

Plan d'intervention

Il s'agit d'un dispositif de type mentorat dispensé pour les porteurs de projets. En outre, l'organisation par groupe de 4 à 10 personnes permettra de bénéficier des échanges et des interactions stimulées par le formateur.

Contenu de la formation :

Le contenu de la formation est adapté en fonction des sujets identifiés par le formateur à l'issue de la session de formation présentée dans le module 1 et du pré diagnostic.

Les thématiques abordées pourront en particulier porter sur :

- Mesurer l'impact des failles de sécurité au travers d'exemples pris dans les dossiers des participants ou de l'actualité
- Constat et analyse factuelle d'une situation en lien avec un incident
- Analyse critique sur les vulnérabilités identifiées et échange sur la méthode et les niveaux de criticité
- Présentation interactive et pratique adaptée aux situations identifiées avec les participants, échanges et travaux par binômes.

Livrables
A l'issue de cette formation, chaque porteur de projet disposera d'une feuille de route des travaux à réaliser dans l'objectif de soumettre un dossier à la labellisation « Smart & Secure IoT ».

Modalité d'évaluation :

- Test des acquis tout au long de la formation via différents exercices
- Questionnaire d'évaluation
- Evaluation à froid à 3 mois

Modalité de validation : Attestation de formation

Modalités pédagogiques :
Une journée en présentiel de présentation interactive et pratique des concepts théoriques présentés dans la partie distancielle.
Manipulations et mises en situations permettant d'assimiler les concepts et de contextualiser la formation.

Méthodes pédagogiques :

Expositives, Participatives, Interrogatives

Outils pédagogiques/support :

Support powerpoint, base documentaire, matrice de travail, cas pratiques…

INTERVENANTS :

M. MONNIER, Mme REZE, M. LONGCHAMPS, M. CRASNIER

INSCRIPTION :

Modalité : Groupe constitué en fonction de la demande

Délai : Inscription jusqu'à 48h avant l'entrée en formation

Contact : Mathilde Alarçon – formation@digital113.fr - 07 86 06 95 29

Formation-action niveau 3

Référence : Module 3

Intitulé de la formation : Obtenir la labellisation Smart & Secure IoT

Public cible : Chef de projet innovation, bureau d'études, R&D, Directeur, Directeur commercial, RSSI / CISO quand existant, Concepteurs, développeurs, Commercial, Responsable qualité, tout collaborateur
Prérequis : Quelques années d'expériences dans le domaine de l'IOT
Lieu : Digital 113
Durée : 8 heures
Coût : 900 € HT par participant

Accessibilité **:** Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toute demandes spécifiques afin de l'on adapte au mieux nos modalités de formation (aménagement des horaires, des lieux, des supports…)

Objectifs

A l'issue de cette formation le participant dispose d'une capacité à mettre en place un plan d'action et des processus pour soumettre un projet à labellisation « Smart & &Secure IoT ».

Le participant est également en mesure de structurer en amont la démarche dans son entreprise et d'accompagner plus généralement un projet d'IoT cybersécurisé dans le processus de son entreprise.

Plan d'intervention

Il s'agit d'un dispositif de type mentorat dispensé pour les porteurs de projets. En outre, l'organisation par groupe de 4 à 10 personnes permettra de bénéficier des échanges et des interactions stimulées par le formateur.

Contenu de la formation :

Le contenu de la formation est adapté en fonction des sujets identifiés par le formateur à l'issue de la session de formation présentée dans le module 2 et du pré diagnostic.

Les thématiques abordées pourront en particulier porter sur :

- Intégrer la sécurité dans le cycle de développement
- Etude de cas sur un programme à développer avec proposition de mesures de sécurité à intégrer en amont en aval selon la criticité du programme et de ses vulnérabilités
- Identification des acteurs et des guides pratiques
- Analyse critique sur les vulnérabilités identifiées et échange sur la méthode et les niveaux de criticité
- Analyser la qualité d'un développement
- Maintenir la sécurité en lien avec la dimension de maîtrise des processus dans le label « Smart & Secure IoT »

- Mise en place d'un processus de revue de code sur un cas d'étude
- Analyser un incident
- Méthode pédagogique
- Présentation interactive et pratique adaptée aux situations identifiées avec les participants, échanges et travaux par binômes.

Livrables

A l'issue de cette formation, chaque porteur de projet disposera d'une feuille de route des travaux à réaliser dans l'objectif de soumettre un dossier à la labellisation « Smart & Secure IoT ».

Modalité d'évaluation :

- Test des acquis tout au long de la formation via différents exercices
- Questionnaire d'évaluation
- Evaluation à froid à 3 mois

Modalité de validation : Attestation de formation

Modalités pédagogiques :
Une journée en présentiel de présentation interactive et pratique des concepts théoriques présentés dans la partie distancielle.
Manipulations et mises en situations permettant d'assimiler les concepts et de contextualiser la formation.

Méthodes pédagogiques :

Expositives, Participatives, Interrogatives

Outils pédagogiques/support :

Support powerpoint, base documentaire, matrice de travail, cas pratiques…

INTERVENANT :

M. MONNIER, Mme REZE, M. LONGCHAMPS, M. CRASNIER

INSCRIPTION :

Modalité : Groupe constitué en fonction de la demande

Délai : Inscription jusqu'à 48h avant l'entrée en formation

Contact : Mathilde Alarçon – formation@digital113.fr - 07 86 06 95 29

Diagnostic de Labellisation

Intervenant : Consultant Scassi
Public cible : Chef de projet innovation, bureau d'études, R&D, Directeur, Directeur commercial, RSSI / CISO quand existant, Concepteurs, développeurs, Responsable qualité
Prérequis : Quelques années d'expériences dans le domaine de l'IOT
Modalités pédagogiques : audit diagnostic
Lieu : selon projet, en entreprise ou à distance
Durée : 16 heures
Coût : 2200 € HT par entreprise

Objectifs
Ce diagnostic permet de valider la maturité du projet au regard du label « Smart & Secure IoT ».
A l'issue de cette étape le participant sera en mesure de connaître les derniers ajustements pour satisfaire les exigences du label.
Il lui sera alors possible de soumettre son dossier au comité de labellisation.

La démarche
La conformité au label « Smart & Secure IoT » est évaluée au regard du label et en appliquant la démarche d'évaluation de Scassi.

Le contexte et les spécificités de l'entreprise et de son projet sont pris en compte par les experts Scassi. C'est au travers des documents fournis et d'entretiens avec le porteur du projet que l'auditeur, va mesurer la maturité du projet, proposer, le cas échéant, des axes d'amélioration et poser un diagnostic opérationnel.

Organisation
Cette action fait suite à un pré-diagnostic et à un programme de formation-action (voir précédemment).

Ce diagnostic est réalisé pour chaque projet présenté. Il est confidentiel à l'entreprise.

Plan d'intervention
- Organisation et préparation de l'audit du dossier, signature de la convention d'audit (accord de confidentialité, liste des interlocuteurs, circuit de diffusion, etc.)
- Réunion de lancement, revue du dossier et échanges sur le projet (par vidéoconférence ou rendez-vous, selon le projet et les recommandations de l'auditeur Scassi)
- Etude du dossier par les experts Scassi
- Etablissement et transmission du diagnostic à l'entreprise
- Accompagnement à la finalisation du dossier après diagnostic (par vidéoconférence ou rendez-vous, choix de l'auditeur Scassi)
- Revue des actions correctrices et préparation du rapport d'audit
- Restitution et clôture de l'audit (par vidéoconférence ou rendez-vous, selon recommandations de l'auditeur Scassi)
- Transmission de la conclusion de l'audit au comité de labellisation

Livrable
- Rapport d'audit détaillé pour l'entreprise
- Conclusions de l'audit qui seront transmises au comité de labellisation