Management du DevSecOps

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Pilotage de la sécurité organisationnelle

Rubrique : Certifications ISO

Code de formation : MDSOPS

PRÉSENTATION

Objectifs & compétences

Cette formation présente les concepts du management en DevSecOps. L'objectif pour l'apprenant est d'acquérir une méthode ESD, des outils afin de pouvoir créer un cycle de développement sécurisé.

Public visé

manager en sécurité de l'information.

Pré-requis

connaissances généralistes en sécurité de l'information, gestion des risques, conformité SSI.

PROGRAMME

Programme détaillé

Jour 1 matin

Section 1

Les enjeux du DevSecOps pour les organisations
Qu'est-ce que le DevOps ?
Pourquoi séparer le Dev et les Ops ?
DevOps versus modèle classique Le DevOps pour qui ?
Philosophie de l'agile Et le DevSecOps ?

Section 2

Problèmes de compréhension du DevSecOps par les managers de la SSI Château fort et défense en profondeur
DevSecOps, quel modèle de sécurité?
Intégrer le DevSecOps dans un SMSI

Section 3

Problèmes de compréhension du DevSecOps par les techniciens de la SSI
Sécurité de l'information est une contrainte
Donner un sens à la SSI

Jour 1 après-midi

Section 4

Intégrer le DevSecOps dans la gouvernance d'une organisation
Les principales missions d'un manager en sécurité de l'information
Mission 1 – l'approche par les risques
Mission 2 – la conformité avec le socle normatif
Mission 3 – la mise en condition de sécurité (MCS)

€ Tarifs

Prix public : 2889 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 21 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 2/11/2026

Section 5

Quel modèle, référentiel choisir pour le DevSecOps Microsoft SDL OWASP SAMM BSIMM OWASP ASVS

Jour 2 matin

Section 6

Phase 1, préparer un SDLC adapté
Activité 1.1 – budgétiser un SDLC
Activité 1.2 – Identifier un équipe pour le SDLC

Section 7

Phase 2, former l'équipe au DevSecOps
Activité 2.1 – créer une formation "tous les profils"
Activité 2.2 – créer une formation "technique"

Jour 2 après-midi

Section 8

Phase 3, analyser les risques Fonctionnement d'une analyse de risque
Activité 3.1 – obtenir les besoins de sécurité et les scénarios graves STRIDE et DIC(T) Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege Adapter les méthodes d'analyses de risques classiques au DevSecOps avec le Bugs bar
Activité 3.2 – modéliser les menaces Qu'est-ce que la modélisation des menaces (Threat modeling) Créer un diagramme Identifier les menaces Utilisation de Microsoft Threat modeling tools Obtenir la vraisemblance des risques avec la modélisation des menaces Construire la matrice des risques via les objectifs de sécurité et la vraisemblance des menaces
Activité 3.3 – calcul des risques
Activité 3.4 – choisir une option de traitement
Activité 3.5 – créer un plan de traitement des risques Ne pas oublier les données à caractère personnel

Jour 3 matin

Section 9

Phase 4, mise en conformité & intégration d'outils Aller plus loin avec l'implémentation d'un référentiel de conformité adapté au DevSecOps
Activité 4.1 – Identifier les référentiels, normes, lois
Activité 4.2 – appliquer l'analyse des écarts L'OWASP AVSV
Activité 4.3 – intégration d'un SAST Activité 4.4 – intégration d'un DAST

Jour 3 après-midi

Section 10

Phase 5, auditer et améliorer la sécurité
Activité 5.1 – planifier un test d'intrusion
Activité 5.2 – adapter le système de suivi des bugs du SDLC à STRIDE
Activité 5.3 – préparer un tableau de bord
Activité 5.4 – préparer un plan de réponse à incident
Activité 5.5 – aller plus loin avec un modèle de maturité Activité 5.6 – veille SSI

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en

Informations non contractuelles - PDF généré le 2/11/2026

sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 2/11/2026