Analyse des logiciels malveillants – niveau Perfectionnement

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Investigation, réponses à incidents

Rubrique : Logiciels malveillants

PRÉSENTATION

Objectifs & compétences

Analyse de codes malveillants Logiciels malveillants ayant des propriétés défensives Documents malveillants et analyses inforensiques de la mémoire

Public visé

Développeurs / Pentesters / Administrateurs / Analystes

Pré-requis

Connaissances généralistes en programmation et système / réseaux Avoir suivi le cours Ref ALM1

PROGRAMME

Programme détaillé

Section 1

Signatures YARA Création de règles Implémentation YARA Plateformes d'échanges

Section 2

Analyse de dumps mémoire Acquisition Volatility : Processus, DLLs, Ruches, Injections, Connections

Section 3

Introduction à l'assembleur (ia – 32)
Introduction Registres Flags Instructions La pile
Exemple de travaux pratiques
TP1 Etude de cas – Analyse d'une attaque et rédaction d'un rapport
TP2 Signer des malwares
TP3 Analyse de dumps mémoire
TP4 Premiers programmes (Hello World [Write] - Boucles – Execve [/bin/sh])
Modalité d'évaluation des acquis Auto-évaluation des acquis par la stagiaire via un questionnaire

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

Code de formation : ALM2

€ Tarifs

Prix public : 1400 €

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 : 14 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 15/09/2026

PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en 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 15/09/2026