Analyse des logiciels malveillants – niveau expert

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

Code de formation : ALM3

PRÉSENTATION

Objectifs & compétences

Analyse approfondie de codes malveillants Rétro ingénierie Cas concrets

Public visé

Développeurs / Pentesters / Administrateurs / Analystes

Pré-requis

Connaissances généralistes en programmation et système / réseaux Avoir suivi le cours ALM2

PROGRAMME

Programme détaillé

Shellcoding Introduction à GDB Commandes utiles Shellcode méthode stack Shellcode méthode Jmp-Call- Pop
Les encoders Les stagers Où trouver des shellcodes Encoder des shellcodes existants (Metasploit)
Exemple de travaux pratiques
TP1 Création d'un encodeur XOR TP4 Création d'un stager
TP2 Reverse d'une charge
Modalité d'évaluation des acquis Auto-évaluation des acquis par la stagiaire via un questionnaire Examen pour l'obtention d'un badge Analyse de malware ESD Academy (prévoir un supplément de 495 €/examen/ stagiaire)

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 sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.

€ 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.

Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.