Analyse des logiciels malveillants – niveau Initiation

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Investigation, réponses à incidents

Rubrique : Logiciels malveillants

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Les fondamentaux de l'analyse de logiciels malveillants Les démarches complémentaires d'analyse de logiciels malveillants

Public visé

Développeurs / Pentesters / Administrateurs / Analystes

Pré-requis

Connaissances généralistes en programmation et système / réseaux

PROGRAMME

Programme détaillé

Section 1

Etat de l'art Introduction
Historique Vecteurs d'infection
Compromission Impacts Business Défenses classiques

Section 2

Bases système Séquence de boot Dissection d'un processus
Dissection d'un exécutable Gestion de la mémoire
Techniques communes Obfuscation, packers, encoders (évasion)

Section 3

Environnement Infrastructure
Bonnes pratiques et création d'un lab

Section 4

Outils d'analyse
Présentation des outils d'analyse
Analyse statique
Analyse dynamique
Introduction à la suite Flare Mandiant Sandbox (virus total, Cuckoo, AnyRun
Exemple de travaux pratiques TD1 Découverte de la suite Sysinternals (Procmon, Procexp)
TD2 Analyse d'un PDF TD3 Analyse Meterpreter / Unicorn / Macros

Modalité d'évaluation des acquis Auto-évaluation des acquis par la stagiaire via un questionnaire

Code de formation : ALM1

€ Tarifs

Prix public : 700 €

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 : 7 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.

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