Analyse et Rétroconception de Logiciels Malveillants

Lien : https://innov-maroc.com/formation/analyse-et-retroconception-de-logiciels-malveillants

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC305

CATÉGORIE
Analyse des Risques, Audit de Sécurité

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Savoir identifier, classifier et comprendre les mécanismes internes d’un logiciel malveillant
- Mettre en place un environnement sécurisé d’analyse et d’expérimentation
- Acquérir les bases techniques pour effectuer des analyses statiques et dynamiques avancées
- Maîtriser les outils de rétroingénierie et les approches d’unpacking
- Développer la capacité à extraire des indicateurs de compromission et à créer des signatures
- Comprendre les techniques d’évasion et de persistance utilisées par les malwares modernes

POUR QUI ?

- Analystes SOC / CERT / CSIRT
- Responsables ou ingénieurs sécurité
- Experts en réponse aux incidents
- Administrateurs sécurité ou systèmes expérimentés souhaitant approfondir l’analyse de menaces

Programme détaillé

1 / INTRODUCTION À LA RÉTROINGÉNIERIE

- Principes et finalités de l’analyse de logiciels malveillants
- Typologie des malwares et cycle de vie des menaces
- Processus de rétroingénierie et cadre légal

2 / CONSTRUCTION D’UN LABORATOIRE D’ANALYSE

- Configuration d’un environnement isolé et sécurisé
- Virtualisation, sandbox et simulation réseau
- Contournement de protections anti-VM et anti-détection
- Mise en place d’outils de capture et de monitoring

3 / BASES DE L’ASSEMBLEUR ET DE L’ARCHITECTURE x86

- Registres, instructions de base et structures de contrôle
- Conventions d’appels et gestion de la mémoire
- Compréhension du flux d’exécution

4 / ANALYSE STATIQUE

- Identification des métadonnées et chaînes de caractères
- Étude des sections PE et dépendances du binaire
- Introduction à IDA Pro et Ghidra
- Repérage des points d’entrée et des patterns suspects

5 / ANALYSE DYNAMIQUE ET COMPORTEMENTALE

- Utilisation de debuggers (x64dbg, WinDbg)
- Observation du comportement en exécution
- Analyse du réseau, du système de fichiers et du registre
- Corrélation entre traces dynamiques et code désassemblé

6 / ANALYSE MÉMOIRE ET FORENSICS

- Extraction et inspection de la mémoire vive
- Utilisation d'outils comme Volatility et Rekall
- Reconstruction de processus et détection d'injections

7 / MÉCANISMES DE PROTECTION ET D'ANTI-ANALYSE

- Obfuscation, chiffrement et polymorphisme
- Techniques anti-débogage et anti-désassemblage
- Méthodes d'évasion des sandbox et VMs

8 / MÉTHODES D'UNPACKING ET DE DÉSOBFUSCATION

- Identification de packers et techniques d'unpacking manuel
- Détection de l'OEP (Original Entry Point)
- Reconstruction de tables d'imports
- Introduction à Miasm2 et Unicorn Engine

9 / MALWARES CLASSIQUES

- Keyloggers, voleurs d'informations et sniffers
- Ransomwares : fonctionnement, chiffrement et persistance
- Bots et C2 : mécanismes de communication et de contrôle

10 / MALWARES SPÉCIFIQUES

- Rootkits (userland et kernel mode)
- Shellcodes et injections de code
- Étude de cas pratiques sur binaires réels anonymisés

11 / MALWARES MULTI-PLATEFORMES

- Analyse de malwares Android, scripts Web (JS/VBS)
- Étude de documents piégés (Office, PDF, RTF)
- Cas des applications .NET et Java obfusquées

12 / AUTOMATISATION DE L'ANALYSE

- Scripts Python pour automatiser les extractions et détections
- Interaction avec les outils IDA / Ghidra / Volatility via API
- Création de workflows d'analyse reproductibles

13 / INTÉGRATION DANS LA THREAT INTELLIGENCE

- Extraction d'IOCs et corrélation avec les bases de données MISP et Yeti
- Création de règles Yara et Sigma pour la détection
- Communication et documentation des résultats d'analyse

14 / ATELIER FINAL D'ANALYSE COMPLÈTE

- Étude d'un malware inconnu en conditions réelles
- Rédaction d'un rapport d'analyse
- Recommandations de remédiation et d'amélioration de la détection

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

06 au 10 Juil. 2026	Présentiel - Casablanca
31 Août au 04 Sep. 2026	Distanciel
26 au 30 Oct. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com