Analyse des malwares : reverse engineering statique et dynamique

Lien : https://innov-systems.com/formation/analyse-des-malwares-reverse-engineering-statique-et-dynamique

DURÉE
5 jours (35h)

RÉFÉRENCE
SI93

CATÉGORIE
Sécurité Wifi/IOT et Malware

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les fondamentaux du reverse engineering de malwares
- Mettre en place un environnement d’analyse sécurisé
- Réaliser des analyses statiques et dynamiques de malwares
- Identifier les techniques d’obfuscation et d’évasion
- Analyser les communications C2 des malwares
- Extraire des indicateurs de compromission (IoCs)
- Développer des signatures de détection efficaces
- Améliorer les capacités de threat hunting
- Produire des rapports d’analyse professionnels
- Renforcer la détection et la réponse aux incidents
- Maîtriser les outils d’analyse de sécurité avancés
- Étudier des cas réels de menaces avancées

POUR QUI ?

- Analystes cybersécurité
- Threat hunters
- SOC analysts
- Reverse engineers
- Malware analysts
- Pentesters / Red Teamers
- Ingénieurs sécurité
- Consultants cybersécurité
- Forensic analysts
- DevSecOps engineers
- Architectes sécurité
- Toute personne impliquée dans l’analyse des menaces et la cybersécurité offensive/défensive

Innov Systems

Programme détaillé

1 / Introduction à l’analyse des malwares

- Typologie des malwares (virus, trojans, ransomware, rootkits)
- Objectifs du reverse engineering en cybersécurité
- Cycle de vie d’une analyse de malware

2 / Environnement d’analyse sécurisé (Lab)

- Mise en place d’un sandbox isolé
- Virtualisation et machines d’analyse
- Bonnes pratiques de sécurité en laboratoire malware

3 / Analyse statique des malwares

- Inspection de fichiers sans exécution
- Analyse de chaînes, métadonnées et structures PE/ELF
- Utilisation d’outils (Ghidra, IDA, strings, PE-bear)

4 / Désassemblage et décompilation

- Lecture de code assembleur
- Décompilation et reconstruction logique
- Compréhension des fonctions malveillantes

5 / Analyse dynamique des malwares

- Exécution contrôlée en sandbox
- Observation des comportements système (processus, registre, réseau)
- Monitoring avec outils (Procmon, Wireshark, API Monitor)

Innov Systems

6 / Techniques d’obfuscation et d’évasion

- Packers et crypters
- Anti-debugging et anti-VM
- Techniques de camouflage avancées

7 / Reverse engineering avancé

- Analyse de malware polymorphique et metamorphique
- Analyse mémoire (dumping et forensic RAM)
- Extraction de configurations et C2

8 / Analyse réseau et communication C2

- Identification des serveurs de commande et contrôle
- Analyse des protocoles malveillants
- Traçage des flux réseau suspects

9 / Détection et réponse aux menaces

- Création de signatures de détection (YARA, Sigma)
- Intégration SIEM et threat hunting
- Stratégies de mitigation et containment

10 / Cas pratiques d’analyse de malwares

- Analyse complète d’un ransomware
- Reverse engineering d’un trojan avancé
- Rapport d’analyse et recommandations

Innov Systems

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

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 2027	Présentiel - Casablanca

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

Réservation & Renseignements

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

Innov Systems — Tous droits réservés