Comprendre les malwares : détection, prévention et réponse

Date et durée

Code formation : SSR001FR
Durée : 2 jours
Nombre d'heures : 14 heures

Description

Les **malwares ou logiciels malveillants** constituent une menace informatique majeure et en constante évolution, rendant leur compréhension indispensable pour toute entité. Cette formation vous offrira une analyse détaillée des malwares : leur fonctionnement, leurs diverses classifications (**virus, ransomwares, chevaux de Troie, etc.**) et leurs méthodes d'infiltration. Vous développerez une perspective claire sur les défis actuels en matière de sécurité informatique liés à ces menaces persistantes.
D'une durée de 2 jours, ce programme vous guidera à travers la typologie des malwares, des virus classiques aux ransomwares et malwares IoT. Vous analyserez leurs vecteurs d'infection, de **l'ingénierie sociale** à l'exploitation de vulnérabilités. Les cours mettront l'accent sur les **stratégies de détection et d'analyse**, avec l'étude d'outils comme les antivirus, EDR, et les plateformes d'analyse en ligne. Des ateliers pratiques vous permettront d'analyser des malwares simples et de simuler des incidents pour une meilleure compréhension opérationnelle.
À l'issue de ces cours, vous serez capable de mettre en œuvre des mesures efficaces de prévention et de détection des malwares. Vous maîtriserez les **bonnes pratiques de sécurisation des systèmes** et de sensibilisation des utilisateurs. Plus important encore, vous saurez réagir efficacement en cas d'incident, depuis le confinement jusqu'à l'éradication et la restauration des systèmes, en passant par la **rédaction de rapports d'incident**.

Objectifs

À l'issue de cette formation sur les malwares, vous atteindrez les objectifs suivants :

- identifier les différentes familles de malwares et leurs caractéristiques spécifiques ;
- appréhender les vecteurs d'infection et les techniques d'évasion utilisées par les logiciels malveillants ;
- analyser les impacts potentiels d'une attaque par malware sur les systèmes et les données ;
- mettre en œuvre des mesures efficaces de prévention et de détection contre les menaces ;
- réagir de manière efficace en cas d'incident de sécurité lié à un malware.

Points forts

- **Analyse approfondie des menaces** : plongez au cœur du fonctionnement des logiciels malveillants, explorez leurs diverses typologies (virus, ransomwares, chevaux de Troie) et identifiez leurs méthodes d'infiltration.
- **Approche pratique et concrète** : développez des compétences directement applicables sur le terrain grâce à des démonstrations interactives, des études de cas réels et des ateliers pratiques dédiés à la détection, la prévention et la réponse aux incidents.
- **Maîtrise des stratégies de défense** : acquérir une expertise pour identifier les différentes familles de malwares, comprendre leurs techniques d'évasion, analyser leurs impacts et mettre en œuvre des mesures

efficaces de prévention et de détection.

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Connaissances en informatique et sécurité des systèmes** : une compréhension des bases de l'informatique et des concepts fondamentaux de la sécurité des systèmes est requise.
- **Aisance avec les environnements Windows ou Linux** : une familiarité avec l'utilisation et la navigation dans l'un de ces systèmes d'exploitation est nécessaire.

Public

Cette formation s'adresse aux publics suivants :

- Les **techniciens et administrateurs sysèmes** qui souhaitent renforcer leurs compétences en matière de sécurité contre les logiciels malveillants.
- Les **analystes SOC ou cybersécurité** qui veulent approfondir leurs connaissances sur le fonctionnement, la détection et la réponse aux malwares.
- Les **étudiants en sécurité informatique** qui cherchent à acquérir une compréhension approfondie des menaces malveillantes et de leurs mécanismes.
- Les **responsables IT ou RSSI débutants** qui veulent comprendre les enjeux des malwares pour mieux protéger leur infrastructure.
- Les **recruteurs IT** qui souhaitent mieux cerner les profils en cybersécurité et les compétences liées à la gestion des malwares.

Programme

Module 1 : comprendre l'introduction aux malwares

- La définition et l'historique des logiciels malveillants.
- Les objectifs des cyberattaquants (espionnage, sabotage, demande de rançon et vol de données.
- Le panorama des menaces actuelles en matière de malwares.

Module 2 : identifier la typologie des malwares

- Les différentes typologies de malwares (virus, vers et chevaux de Troie).
- Le fonctionnement, les techniques de chiffrement et le processus de rançon des ransomwares.
- Les spywares, adwares et keyloggers.
- Les rootkits et bootkits.
- Les malwares spécifiquement conçus pour les plateformes mobiles et l'IoT.

Module 3 : analyser les vecteurs d'infection

- Le phishing et l'ingénierie sociale comme vecteurs d'infection.
- L'exploitation des vulnérabilités (exploits, zero-day).
- Les points d'entrée physiques et numériques : clés USB, téléchargements malveillants, sites web piégés.

Travaux pratiques :

- Analyser un fichier suspect pour en détecter la nature malveillante.
- Mener une analyse comportementale en utilisant un bac à sable (sandbox).
- Identifier les indicateurs de compromission (IoC).

Module 4 : détecter et analyser les malwares

- Les outils de détection avancés (antivirus, antimalwares et EDR (Endpoint Detection and Response).
- La distinction entre l'analyse statique et l'analyse dynamique des malwares.
- L'utilisation d'outils en ligne spécialisés pour l'analyse, tels que VirusTotal, Any.Run et Hybrid Analysis.

Module 5 : mettre en œuvre la prévention et les bonnes pratiques

- La mise à jour régulière des systèmes et l'application des correctifs de sécurité.
- La sécurisation des accès et la gestion des privilèges des utilisateurs.
- La sensibilisation des utilisateurs aux risques et aux bonnes pratiques de sécurité informatique.

Module 6 : gérer la réponse à incident malware

- Les étapes de containment (isolement du poste infecté) lors d'un incident.
- Les procédures d'éradication du malware et de restauration des systèmes affectés.
- La communication post-incident et le processus de retour d'expérience pour l'amélioration continue.

Travaux pratiques :

- Simuler la détection d'un ransomware en situation réelle.
- Élaborer un plan d'action de réponse à incident.
- Rédiger un rapport d'incident complet.