+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 16/09/2026

S'inscrire

Formation Ghidra

3 jours (21 heures)

Présentation

Ghidra est une plateforme de reverse engineering conçue pour analyser des binaires, comprendre leur logique et accélérer l'investigation de codes malveillants. Grâce au désassemblage, à la décompilation, aux graphes et aux scripts, elle aide les analystes à produire des diagnostics fiables sur des exécutables complexes.

Notre formation Ghidra vous permettra de maîtriser les méthodes essentielles d'analyse statique pour examiner des exécutables suspects dans un environnement maîtrisé. Vous apprendrez à importer des binaires, configurer les analyses automatiques et naviguer efficacement entre les vues de code, de mémoire et de références.

Vous étudierez les principes de lecture de l assembleur, l'interprétation du pseudo code produit par le décompilateur et l'enrichissement progressif des fonctions avec des noms, commentaires, structures et signatures adaptés.

La formation aborde également les techniques d'identification des comportements utiles à l'analyse de malwares, comme les mécanismes de persistance, les appels système, les chaînes significatives, les communications réseau et les fonctions de chiffrement.

À l'issue de la formation, vous serez en mesure de conduire une analyse structurée avec Ghidra, de documenter vos constats, de comparer des versions de binaires et d'automatiser certaines tâches répétitives avec des scripts Python.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Prendre en main l'environnement Ghidra pour analyser des binaires compilés
- Interpréter le désassemblage, le pseudo code et les graphes de contrôle
- Reconstruire la logique d'un programme avec les fonctions, types, structures et références
- Identifier des comportements caractéristiques lors d'une analyse statique de malware
- Documenter les résultats et automatiser des analyses répétitives avec des scripts

Public visé

- Analyste cybersécurité
- Analyste SOC
- Analyste malware
- Ingénieur réponse à incident
- Consultant en sécurité offensive

Pré-requis

- Connaissances des fondamentaux de la cybersécurité
- Pratique de la ligne de commande sous Windows ou Linux
- Bases de programmation en C ou Python
- Notions d'architecture processeur et d'assembleur x86 ou x64

Pré-requis techniques

- Poste sous Windows 10 ou 11, Linux ou macOS compatible 64 bits
- Installation d'une version récente de Ghidra avec JDK 25 64 bits
- Ordinateur disposant d'au moins 8 Go de RAM et de 2 Go d'espace disque disponible
- Machine virtuelle isolée pour manipuler les échantillons fournis
- Connexion Internet stable pour préparer l'environnement et installer les dépendances

Programme de notre formation Ghidra

[Jour 1 - Matin]

Fondamentaux du reverse engineering avec Ghidra

- Rôle de Ghidra dans le reverse engineering et l analyse statique de malwares
- Panorama des formats exécutables, architectures processeur et informations disponibles dans un binaire
- Installation, configuration de l espace de travail et organisation des projets Ghidra
- Importation d un exécutable, choix du langage processeur et paramètres d analyse automatique
- Découverte du CodeBrowser, des vues Listing, Symbol Tree, Program Trees et Memory Map

[Jour 1 - Après-midi]

Lire et qualifier le code désassemblé

- Principes de lecture de l assembleur x86 et x64, registres, pile et conventions d appel
- Différences entre code, données, chaînes, imports, exports et ressources
- Navigation par références croisées, recherches de chaînes et identification des fonctions importantes
- Utilisation des bookmarks, labels, commentaires et regroupements pour tracer l analyse
- Atelier pratique : importer un exécutable pédagogique, repérer son point d entrée, ses imports et ses chaînes significatives.

[Jour 2 - Matin]

Décompiler et reconstruire la logique applicative

- Fonctionnement et limites du décompilateur, relation entre pseudo code et assembleur
- Identification des paramètres, variables locales, valeurs de retour et appels de fonctions
- Renommage des symboles et fonctions pour construire une nomenclature compréhensible
- Application de types, structures, énumérations et signatures pour améliorer le pseudo code
- Analyse des graphes de flux de contrôle, embranchements, boucles et chemins d exécution

[Jour 2 - Après-midi]

Analyser les comportements suspects

- Méthode de triage statique pour prioriser les zones pertinentes d un échantillon
- Repérage des mécanismes de persistance, exécution de processus et manipulation de fichiers
- Identification des indicateurs liés aux communications réseau, à la configuration et au chiffrement
- Analyse des techniques d obfuscation simples, des chaînes encodées et du code non atteignable
- Atelier pratique : reconstituer le comportement d un binaire d entraînement et produire une première note d analyse.

[Jour 3 - Matin]

Approfondir et fiabiliser les investigations

- Correction manuelle du désassemblage et redéfinition des zones de code ou de données
- Création et réutilisation de types de données pour clarifier les fonctions complexes
- Utilisation des arbres d appels, des références croisées et des fonctions similaires
- Comparaison de programmes et suivi des évolutions entre deux versions d un binaire
- Bonnes pratiques de traçabilité, hypothèses, niveaux de confiance et restitution technique

[Jour 3 - Après-midi]

Automatiser les analyses avec les scripts

- Présentation du gestionnaire de scripts et des possibilités d automatisation dans Ghidra
- Principes de l API, parcours des programmes, fonctions, symboles et références
- Création de scripts Python pour extraire des informations et enrichir une analyse
- Introduction au mode headless pour traiter plusieurs binaires de manière reproductible
- Atelier pratique : créer un script Python d inventaire des fonctions et chaînes, puis préparer un rapport synthétique sur un échantillon.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.