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

Mis à jour le 03/02/2026

S'inscrire

Formation Villager Framework

3 jours (21 heures)

Présentation

Villager est le premier framework de pentesting AI-native, conçu pour succéder aux outils de post-exploitation traditionnels comme Cobalt Strike. Cette approche repose sur des agents autonomes et le protocole MCP pour automatiser l'intégralité de la chaîne d'attaque.

Notre formation Villager vous permettra de maîtriser cette nouvelle génération d'outils d'audit de sécurité. Vous apprendrez à orchestrer des agents capables de générer des exploits dynamiques, de s'adapter aux défenses en temps réel et d'automatiser des tâches complexes via des conteneurs éphémères.

À l'issue de la formation, vous serez en mesure de déployer une infrastructure Villager, de piloter une flotte d'agents IA pour des audits de sécurité et d'industrialiser vos workflows Red Team pour des projets professionnels.

Objectifs

- Comprendre l'architecture des agents IA autonomes appliqués au pentesting.
- Installer et configurer le framework Villager et son infrastructure d'agents.
- Maîtriser le pilotage par langage naturel et le protocole MCP.
- Automatiser les phases de reconnaissance, d'exploitation et de mouvement latéral.
- Évaluer les capacités et les limites de l'IA face aux solutions de défense.

Public visé

- Pentesteurs et consultants en cybersécurité
- Ingénieurs Red Team
- Responsables SOC et analystes sécurité

Pré-requis

- Connaissances solides en Pentesting (réseaux, systèmes)
- Familiarité avec la ligne de commande Linux
- Notions de base sur les LLM et les API

Pré-requis logiciels

- 16 Go de RAM au minimum
- Linux (Ubuntu de préférence) ou Windows avec WSL2
- Docker et Docker-compose installés
- Un accès API (OpenAI, Anthropic ou DeepSeek) pour les exercices

Formation Villager : Pentesting & Agents IA

[Jour 1 - Matin]

Introduction à Villager et aux Agents Offensifs

- Panorama du pentesting IA : du script traditionnel à l’agent autonome
- Présentation de Villager : philosophie, architecture et comparaison avec Cobalt Strike
- Comprendre le rôle des LLM dans la prise de décision offensive
- Introduction au protocole MCP (Model Context Protocol)
- Atelier pratique : Installation de l’instance Villager et configuration des accès API LLM.

[Jour 1 - Après-midi]

Orchestration et Premier Scénario

- Interface de contrôle : piloter un agent en langage naturel
- Gestion des conteneurs éphémères pour l’exécution d’outils (Nmap, Metasploit)
- Décomposition d’objectifs (Task Planning) par l’IA
- Suivi des logs et monitoring des actions de l’agent
- Atelier pratique : Lancement d’une mission de reconnaissance automatisée sur un périmètre cible.

[Jour 2 - Matin]

Exploitation Dynamique et Adaptation

- Génération d’exploits "on-the-fly" par l’IA
- Contournement des premières lignes de défense (Firewalls, filtrage)
- Analyse des retours d’erreurs par l’agent et correction autonome du code d'attaque
- Utilisation des plugins et extensions Villager
- Atelier pratique : Scénario d’exploitation d’une vulnérabilité connue avec adaptation de l’agent.

[Jour 2 - Après-midi]

Post-Exploitation et Mouvement Latéral

- Persistance discrète via agents IA
- Mouvement latéral : pivotage et énumération de domaine automatisée
- Exfiltration de données sélective et intelligente
- Nettoyage des traces et rapports d'activité générés par l'IA
- Atelier pratique : Compromission d’un réseau Active Directory avec Villager.

[Jour 3 - Matin]

Sécurité, Éthique et Evasion Avancée

- Techniques d’évasion face aux EDR/XDR boostés à l’IA
- Obfuscation dynamique de payloads
- Limitations actuelles : hallucinations, coûts d’API et latence
- Cadre légal et éthique de l’usage de l’IA offensive
- Atelier pratique : Test de détection de Villager face à une solution de défense moderne.

[Jour 3 - Après-midi]

Industrialisation et Cas Pratiques

- Intégration de Villager dans une pipeline DevSecOps
- Personnalisation des "Prompts" système pour des missions spécifiques
- Études de cas réels (Rapports Cyberspike / Straiker)
- Workflow d’équipe Red Team et supervision
- Atelier pratique : Projet final - Simulation d’une attaque complète en autonomie supervisée.

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.