AYI NEDJIMI Consultants

DFIR : Réponse à Incident et Forensics | Guide Expert

Catégorie : Livres Blancs Lecture : 1 min Publié le : 11/03/2026 Auteur : Ayi NEDJIMI

Guide DFIR complet : methodologie PICERL, forensics Windows et Linux, analyse memoire Volatility, collecte de preuves et outils open source.

Découvrez nos outils open source développés pour les professionnels du DFIR :

Outil / Ressource	Description	Lien
AmcacheForensics	Analyse forensique de la ruche Amcache pour tracer les exécutions de programmes	Voir sur GitHub
BamDamForensics	Extraction et analyse des artefacts BAM/DAM du registre Windows	Voir sur GitHub
UserAssistDecoder	Décodeur d'entrées UserAssist encodées en ROT13	Voir sur GitHub
TaskSchedulerForensics	Analyse forensique des tâches planifiées Windows	Voir sur GitHub
SuperTimelineBuilder	Génération automatisée de super timelines forensiques	Voir sur GitHub
SysmonEventCorrelator	Corrélation d'événements Sysmon pour la détection de chaînes d'attaque	Voir sur GitHub
YaraMemoryScanner	Scan mémoire avec règles YARA pour la détection de malware	Voir sur GitHub
VSSIntegrityWatcher	Vérification de l'intégrité des Volume Shadow Copies	Voir sur GitHub
TokenPrivilegeForensics	Analyse forensique des privilèges de tokens Windows	Voir sur GitHub
Collection DFIR HuggingFace	Collection de modèles et datasets spécialisés en DFIR et réponse à incident	Voir sur HuggingFace

Tous ces outils sont disponibles en open source sur notre profil GitHub et nos modèles d'IA sur notre espace HuggingFace. N'hésitez pas à contribuer et à signaler les issues.

Pour approfondir, consultez les ressources de NIST Cybersecurity et de NVD (National Vulnerability Database).

Sources et références : ANSSI · CERT-FR

Articles connexes

- Red Team vs Blue Team : Méthodologies et Outils Expert
- Zero Trust : Architecture et Déploiement Entreprise
- Sécurité Microsoft 365 : Audit et Durcissement Complet
- Guide Complet du Pentest Cloud : AWS, Azure et GCP

Conclusion et Recommandations

La maîtrise du DFIR est devenue un impératif stratégique pour toute organisation. Face à des attaquants de plus en plus complexes, la capacité à détecter rapidement, investiguer méthodiquement et remédier efficacement fait la différence entre un incident contenu et une catastrophe. La méthodologie PICERL, les outils forensiques éprouvés et l'amélioration continue constituent les fondations d'une posture DFIR mature.

Les organisations qui investissent dans leurs capacités DFIR – formation des équipes, outillage adapté, playbooks testés, exercices réguliers – réduisent significativement l'impact des incidents et accélèrent leur rétablissement. N'attendez pas d'être victime d'une cyberattaque pour vous préparer.

Besoin d'un accompagnement DFIR ?
Nos experts certifiés DFIR vous accompagnent dans la mise en place de vos capacités de réponse à incident, l'investigation forensique de vos systèmes compromis et la formation de vos équipes SOC/CSIRT.

Demander un accompagnement DFIR

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr