MEFF M3 Pro è uno scanner professionale per la sicurezza mobile, progettato per analizzare dispositivi Android e iOS e rilevare minacce, trojan governativi e spyware grazie all'intelligenza artificiale. Qui trovi tre schede tecniche funzionali in formato di sintesi, pronte per report PDF multilingua: italiano, inglese e francese. Ogni scheda riassume descrizione, funzionalità, architettura, casi d'uso e certificazioni, come richiesto .

ITALIANO

MEFF M3 Pro — Scheda Tecnica Funzionale

Descrizione Generale:
MEFF M3 Pro è uno scanner professionale di malware mobile per dispositivi Android e iOS, progettato per individuare minacce, spyware governativi e connessioni sospette tramite intelligenza artificiale.

Funzionalità Principali:

- Scanner Android via USB (WebADB), analisi real-time app e permessi critici, rilevamento trojan (Pegasus, Predator, ecc.), report PDF multilingua.
- Scanner iOS tramite analisi file Sysdiagnose, upload/trasferimento multiplo, rilevamento spyware certificato MVT, report dettagliato.
- Traffic Analyzer: cattura traffico e analisi connessioni live, verifica domini/IP sospetti, statistiche in tempo reale e report DNS.
- Licenze cloud con gestione centralizzata e validazione online.
- Report PDF multilingua con dati utente, minacce rilevate, analisi AI e certificazione MVT.
- Interfaccia e manuali multilingua (IT/EN/FR), cambio lingua istantaneo e accesso diretto ai manuali.

- Design futuristico con tema dark-neon, animazioni Matrix-style, effetti glow e responsive design per tablet Windows.
- Sistema di aggiornamento automatico via MongoDB/GitHub, notifiche e changelog multilingua.
- Tastiera virtuale ottimizzata per touchscreen e funzioni avanzate: storico, salvataggio sessioni, gestione report.

Architettura Sistema:

- Backend: Python FastAPI, MongoDB Atlas, Tshark, GPT-4o, ReportLab.
- Frontend: React.js, i18next, Tailwind CSS, WebADB.
- Deployment: Windows 10/11 nativo, installazione automatizzata, hotspot integrato.

Casi d'Uso:

- Cybersecurity: analisi forense dispositivi
- Aziende: verifica compliance dispositivi dipendenti
- Privati: controllo spyware/stalkerware
- Forze dell'ordine: analisi investigativa

Certificazioni:

- Certificazione MVT
- Database trojan governativi aggiornato
- Analisi AI con OpenAI GPT-4o
- Report conformi agli standard investigativi

ENGLISH

MEFF M3 Pro — Functional Technical Sheet

General Description:
MEFF M3 Pro is a professional mobile malware scanner for Android and iOS devices, designed to detect threats, government trojans, and spyware through artificial intelligence.

Key Features:

- Android scanner via USB (WebADB), real-time analysis of apps and critical permissions, detection of trojans (Pegasus, Predator, etc.), multilingual PDF report.
- iOS scanner: Sysdiagnose file analysis with multiple upload/transfer options, certified MVT spyware detection, detailed report.

- Traffic Analyzer: real-time traffic capture and connection monitoring, detection of dangerous domains/suspicious IPs, live stats, and DNS report.
- Cloud license management: centralized license validation and access control.
- Multilingual PDF reports featuring user/device data, threats list, AI analysis, and MVT certification.
- Multilingual interface and user manuals (IT/EN/FR), instant language switching, and direct manual access.
- Futuristic design: dark neon themes, Matrix-style animations, glow/shadow effects, responsive Windows tablet optimization.
- Automatic updates via MongoDB/GitHub, push notifications, multilingual changelogs.
- Virtual keyboard optimized for touchscreen with advanced functions: session history, report management, safe app shutdown.

System Architecture:

- Backend: Python FastAPI, MongoDB Atlas, Tshark, GPT-4o, ReportLab.
- Frontend: React.js, i18next, Tailwind CSS, WebADB.
- Deployment: Native Windows 10/11, automated installer, built-in hotspot.

Use Cases:

- Cybersecurity: forensic device analysis
- Companies: employee device compliance checks
- Private users: spyware/stalkerware detection
- Law enforcement: investigative device analysis

Certifications:

- MVT certification
- Updated government trojan database
- AI analysis via OpenAI GPT-4o
- Reports compliant with investigative standards

FRANÇAIS

MEFF M3 Pro — Fiche Technique Fonctionnelle

Description Générale :

MEFF M3 Pro est un scanner professionnel de malwares mobiles pour appareils Android et iOS, conçu pour détecter les menaces, les chevaux de Troie gouvernementaux et les spywares via l’intelligence artificielle.

Fonctionnalités Principales :

- Scanner Android via USB (WebADB), analyse en temps réel des applications et des permissions critiques, détection des trojans (Pegasus, Predator, etc.), rapport PDF multilingue.
- Scanner iOS par analyse du fichier Sysdiagnose, options multiples d'upload/transfert, détection spyware certifiée MVT, rapport détaillé.
- Analyseur de trafic : capture du trafic en temps réel, surveillance des connexions, détection de domaines/IP suspects, statistiques live et résolution DNS.
- Gestion des licences cloud : validation centralisée des clés d'activation et contrôle d'accès.
- Rapports PDF multilingues : données utilisateur/appareil, liste des menaces, analyse IA détaillée, certification MVT.
- Interface et manuels utilisateur multilingues (IT/EN/FR), changement de langue instantané, accès direct aux guides.
- Design futuriste : thème sombre néon, animations style Matrix, effets lumineux/ombres, design responsive pour tablettes Windows.
- Système de mises à jour automatiques via MongoDB/GitHub, notifications push, changelog multilingue.
- Clavier virtuel optimisé pour écran tactile et fonctions avancées : historique des scans, gestion des rapports, arrêt sécurisé de l'application.

Architecture du Système :

- Backend : Python FastAPI, MongoDB Atlas, Tshark, GPT-4o, ReportLab.
- Frontend : React.js, i18next, Tailwind CSS, WebADB.
- Déploiement : Windows 10/11 natif, installation automatisée, hotspot intégré.

Cas d'Utilisation :

- Cybersécurité : analyse forensique
- Entreprises : vérification des appareils des employés
- Particuliers : détection de spyware/stalkerware
- Forces de l'ordre : analyse d'appareils en enquête

Certifications :

- Certifié MVT
- Base de données trojans gouvernementaux à jour
- Analyse IA via OpenAI GPT-4o
- Rapports conformes aux standards d'enquête