Architekturüberblick

Was diese Plattform leistet

Autonome Entwicklungs- und Betriebsplattform

Ausgangslage

Die Plattform verbindet eine bereits produktiv eingesetzte Website, lokale Entwicklerwerkzeuge, einen autorisierten Windows-Rechner und spezialisierte KI-Assistenten. Ziel ist eine kontrolliert fernbedienbare Arbeitsumgebung, die technische Aufgaben in derselben aktiven Arbeitssitzung vorbereitet, ausführt, prüft und nachvollziehbar dokumentiert.

Architekturziel

Nicht die maximale Anzahl autonomer Agenten steht im Mittelpunkt, sondern das wirksame Zusammenspiel bestehender Komponenten mit begrenzten Berechtigungen. Der Auftraggeber formuliert das fachliche Ziel und bleibt zuständig für Freigaben; ChatGPT strukturiert die Arbeit und orchestriert die verfügbaren Werkzeuge.

Wirkung

Aufgaben müssen nicht fortlaufend per Copy-and-Paste zwischen Chat, Windows, PowerShell, WordPress und Claude Code transportiert werden. Prüfberichte, SHA-Vergleiche, definierte Fehlerzustände und dauerhafte Haltepunkte dienen als überprüfbare Übergaben.

Berufliche Einordnung

Das Projekt ist eine eigene praxisbasierte Architektur- und Integrationsreferenz. Die Eigenleistung besteht vor allem in Zieldefinition, Gestaltung des Gesamtsystems, Werkzeugwahl, Sicherheits- und Kostenentscheidung, fachlicher Abnahme und unabhängiger Qualitätssicherung. Implementierung und Testautomatisierung erfolgten vielfach KI-gestützt.

> Dokumentierte Projektnachweise, keine pauschale Systemgarantie. Produktive Veröffentlichung nur nach gesonderter Schlussfreigabe.

Autonomie-Wächter

Begrenzte Werkzeugwahl statt blindem Agentenbetrieb

Autonome Entwicklungs- und Betriebsplattform

Auftragsverständnis

Der lokale Autonomie-Wächter A v1.3 untersucht bei passenden, klar abgegrenzten Aufträgen das Ziel und schlägt eine bewährte Route vor. Der Nutzer muss dafür keine Toolnamen, Skriptparameter oder technischen Formulare formulieren.

Aktueller tatsächlicher Ausführungsumfang

Die implementierte lokale Brücke kann eng erlaubte Sandbox-Textdateien erstellen und prüfen sowie eindeutig identifizierte Fenster in einer interaktiven Windows-Sitzung lesend untersuchen. Nicht erlaubte Schreibaufträge werden nicht in universelle Shell-Befehle übersetzt.

Beleg und Abgrenzung

Ein dokumentierter Integrationstest der zusammenwirkenden Werkzeuge bestand 10/10 sichere Fälle. Dazu gehörten kontrollierte Sandbox-Dateischritte, SHA-Rücklesen, ein lesender Windows-Fenstercheck und die sichere Weitergabe an vorhandene Werkbank-Einstiege. Kein autonomes WordPress-Publishing wurde dabei getestet.

Architekturentscheidung

Der Wächter bleibt ein bedarfsweises kleines Routing-Werkzeug. Weder ein neuer Dauerprozess noch ein zusätzlicher universeller Orchestrator wurde eingerichtet. Das hält die Angriffffläche, Tokenkosten und Pflegekosten begrenzt.

> Dokumentierte Projektnachweise, keine pauschale Systemgarantie. Produktive Veröffentlichung nur nach gesonderter Schlussfreigabe.

Ergebnisse und Transfer

Architekturkompetenz für einen professionellen Einsatz

Autonome Entwicklungs- und Betriebsplattform

Nachweisbare Einzelergebnisse

Die Kombination aus 10/10 isolierter Wächterintegration, 17/17 lesenden Statusprüfungen, echtem Windows-Voranmeldungsstart, kontrollierten WordPress-Vorschautests und unabhängiger KI-QA bildet ein belastbares Portfolio von Teilleistungen. Es ist kein einzelner End-to-End-Test aller Funktionen zugleich.

Was die Plattform im Alltag ermöglicht

Sichere lokale und entfernte Werkzeugbenutzung, Vorbereitung von Webseiten- und Kursänderungen, Code- und Testkoordination, Erkennen unerwünschter Änderungen, strukturiertes Rücklesen und Wiederaufnahme aus dokumentierten Projektständen.

Was bewusst nicht versprochen wird

Die Architektur veröffentlicht keine beliebigen Inhalte ohne Schlussfreigabe; sie ist weder selbstbewusst noch vollständig selbstständig. Der Funktionsumfang von Toolzugriff, GUI, Netzwerk und Modellen hängt von verfügbaren Werkzeugen und Berechtigungen ab.

Beruflicher Nutzen

Das Projekt demonstriert Solution Design, Systemintegration, Risikosteuerung, eine API-/MCP-orientierte Werkzeugarchitektur, Prüfdisziplin, Dokumentationsqualität und realistische Kostenentscheidungen. Die angestrebte Rolle lautet AI Solutions Architect; sie wird nicht als bereits ausgeübter Beruf ausgegeben.

> Dokumentierte Projektnachweise, keine pauschale Systemgarantie. Produktive Veröffentlichung nur nach gesonderter Schlussfreigabe.