WELT 12: INFRASTRUKTUR-NEBEL · MISSION 12.1

Log-Detektiv ohne Panik

Rund 900 Logzeilen, ein Gerücht («Wir werden gehackt!») und eine KI als Spürhund. Sie schwärzen, ermitteln und entlarven, was um 10:15 Uhr wirklich geschah.

Zur Mission

DAUER 55 Min. KOSTEN Gratis mit Konto WERKZEUGE OpenAI Codex, Claude Code, ChatGPT, LM Studio, Terminal DATENAMPEL Gelb – mit Vorsicht

Das Wichtigste

- Logzeile «combined»: Adresse – Benutzer – Zeit – Anfrage – Status – Grösse – Herkunft – Programm. Der Status verrät am meisten.
- Schwärzen mit gleichbleibenden Kürzeln ist Pseudonymisieren, nicht Anonymisieren. Zuordnungstabelle bleibt lokal; echte Logs trotzdem nur mit Freigabe auswerten.
- Agent an die Leine: Codex `--sandbox read-only`, Claude Code `--permission-mode plan`, nur der Übungsordner.
- Auftrag an die KI: Zeitfenster, Anzahl, Beispielzeile – und Beobachtung, Deutung, Vorschlag trennen.
- Gegenprobe mit `grep -c` (Windows: Select-String). Mindestens zwei Zahlen selbst bestätigen.
- Das Lauteste ist selten das Gefährlichste: der eine Erfolg zwischen vielen Fehlversuchen zählt.
- Analysieren ja, ändern nein: Massnahmen gehen als Empfehlung an die zuständige Stelle.
- Sensible echte Logs: lokal mit LM Studio oder in einer von der Schule zugelassenen Umgebung – nicht in Gratis-KIs.

Ihr Produkt

Eine ausgefüllte **Ermittlungsakte Logdatei** (Vorlage zum Wiederverwenden) mit belegter Ursache, dazu ein **geprüftes Verfahren zum Schwärzen** (Pseudonymisieren) und ein **Ermittlungs-Prompt**, den Sie für jede Logdatei wieder einsetzen können – auch als Fallarbeit für Lernende.

Abnahme: Ihre Ermittlungsakte nennt alle vier Spuren (darunter die Ursache der Langsamkeit und den kritischen Login-Fund) mit Zeitstempel und Anzahl, zwei Zahlen der KI sind mit einem eigenen Suchbefehl bestätigt, und die Kurzmeldung an die Schulleitung liegt vor.

So gehen Sie vor

1. Der erste Blick – ganz ohne KI
2. Erst schwärzen, dann ermitteln
3. Den Spürhund an die Leine nehmen
4. Gegenprobe: Trauen ist gut, grep ist besser
5. Urteil fällen – und die Panik beenden

Start-Prompt

Ich habe eine Logdatei mit einem Skript geschwärzt (pseudonymisiert). Hier sind 15 zufällige Zeilen daraus:
[15 ZEILEN AUS DER ANONYMISIERTEN DATEI, z. B. aus uebungslog-auth.anonym.log]
Prüfe sie wie eine Datenschutz-Verantwortliche: Findest du noch Angaben, mit denen man eine Person, ein Gerät oder eine Organisation erkennen könnte (IP-Adressen, Namen, Mailadressen, Rechnernamen, Pfade)? Liste jeden Fund mit Zeile auf und sage, was ein Skript zusätzlich ersetzen müsste.
Schweizer Rechtschreibung (immer «ss», kein Eszett).

Qualitätscheck

- Vor der Auswertung haben Sie eine **Kopie** angelegt und das Original nie geöffnet, um darin zu arbeiten.
- Falls Sie geschwärzt haben: Ihre Stichprobe in den `*.anonym.log` findet keine IP-Adresse und keinen Benutzernamen mehr – und Sie wissen, was das Skript nicht erkennt (IPv6, Mailadressen, freier Text).
- Der Agent lief nur lesend (read-only bzw. Plan-Modus) und nur im Übungsordner.
- Mindestens zwei Zahlen der KI sind mit einem eigenen Befehl bestätigt.
- Jede Spur in der Ermittlungsakte hat Zeitfenster, Anzahl und eine Beispielzeile; Deutung und Vorschlag sind getrennt.
- Veränderungen (Konto sperren, Konfiguration ändern) stehen nur als Empfehlung an die zuständige Stelle im Bericht.

Hängen Sie fest? Frag die KI

Ich bin Lehrperson an einer Schweizer Berufsfachschule und lerne gerade, Webserver-Logs zu lesen. Erkläre mir an dieser fiktiven Zeile Feld für Feld, was sie bedeutet: 192.0.2.53 - - [17/Nov/2026:09:30:04 +0100] "GET /api/stundenplan?klasse=INF2A HTTP/1.1" 200 3105 "https://www.schule.example.org/" "Mozilla/5.0 …". Erkläre danach die HTTP-Statuscodes 200, 401, 403, 404, 429 und 504 in je einem Satz. Nenne mir 2–3 Suchbegriffe für die offizielle Dokumentation (keine Links erfinden).

Klappt nicht? Ohne Installation: Die drei Übungslogs sind fiktiv – Sie können sie direkt in eine Gratis-KI im Browser hochladen (ChatGPT, Claude, Gemini, Copilot). Echte Logs gehören nicht in eine Gratis-KI, auch nicht pseudonymisiert: nur mit Freigabe der Schule in einer dafür zugelassenen Umgebung oder lokal mit LM Studio (gratis, offline). Codex läuft mit einem Gratis-ChatGPT-Konto (Desktop-App, CLI oder IDE, kleinere Limits); Claude Code braucht ein Abo ab Claude Pro.

Stand 19.11.2026 · CC BY 4.0 Alpasana GmbH · Werkzeuge ändern sich – prüfen Sie selbst.