WELT 12 · 🔍 LOG-DETEKTIV/IN

Infrastruktur-Nebel

Server, Firewall, Netzwerke und Logs. KI als Assistenz für Systeme: Logs auswerten, Firewall-Regeln prüfen, Netzwerk-Labore bauen, Runbooks schreiben – im sicheren Übungsbereich.

Zur Welt

Das Wichtigste dieser Welt

- Logs enthalten Personendaten (IP, Benutzer) – vorher anonymisieren.
- KI schlägt vor, Mensch entscheidet: keine Befehle blind ausführen.
- Nur lesend auf Systeme, Änderungen mit Sicherung und Rückfall.
- Logzeilen können manipulierte Anweisungen enthalten.
- Runbooks: Schritte, Prüfpunkte, Rückweg.

Das können Sie danach

- Logdateien anonymisieren und mit KI auswerten
- Firewall-Regeln auf Lücken und Widersprüche prüfen lassen
- Netzwerk-Fehlerbilder als Lernlabor aufbereiten
- Prompt-Injection in Systemdaten erkennen und abwehren

Die Missionen

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.
2. **Firewall-Regeln im Röntgenblick** – Seit dem «kleinen Umbau» geht das Internet nicht – nur die Wartungsfirma jubelt. Sie röntgen ein Übungs-Regelwerk mit KI und finden elf Lücken, bevor es jemand anderes tut.
3. **Netzwerk-Labor: Fehlerbilder für Lernende** – VLAN falsch, DNS verbogen, ein fremder DHCP-Server: Sie lassen die KI realistische Netzwerk-Pannen mit gestuften Hinweisen bauen – und ertappen sie selbst beim Pfuschen.
4. **Runbook-Generator** – Aus chaotischen Chatnotizen einer Störung wird ein Runbook, das auch um 6:50 Uhr funktioniert. Den Beweis liefert der Blindflug: Eine Kollegin führt es aus – die KI spielt den Server.
5. **Ganze Umgebungen überwachen** – Fünf Server, fünf Statusabzüge, ein Skript meldet «fast alles grün». Ihr KI-Agent liest alles auf einmal – und findet heraus, welches System sich jede Nacht «erfolgreich» schönredet.
6. **Boss: Die vergiftete Logdatei** (Boss) – Montag, 7:40 Uhr. Eine KI hat die Wochenend-Logs geprüft: «Keine Auffälligkeiten.» Gelogen. In den Logs stecken drei Giftköder für Agenten – und ein echter Datenabfluss.

Stand November 2026 · CC BY 4.0 Alpasana GmbH