



ChatZentDok

die Chat Abfrage in natürlicher Sprache
von Open Source Fachinformationen
für das BMLV

BMLV ZentDok/LVAk

April 2024

watsonx.ai

 Bundesministerium
Landesverteidigung + 

Agenda

| Ausgangssituation

| Was ist genAI? Beyond the Hype

| Projektablauf

| Anforderungen und Zielbeschreibung

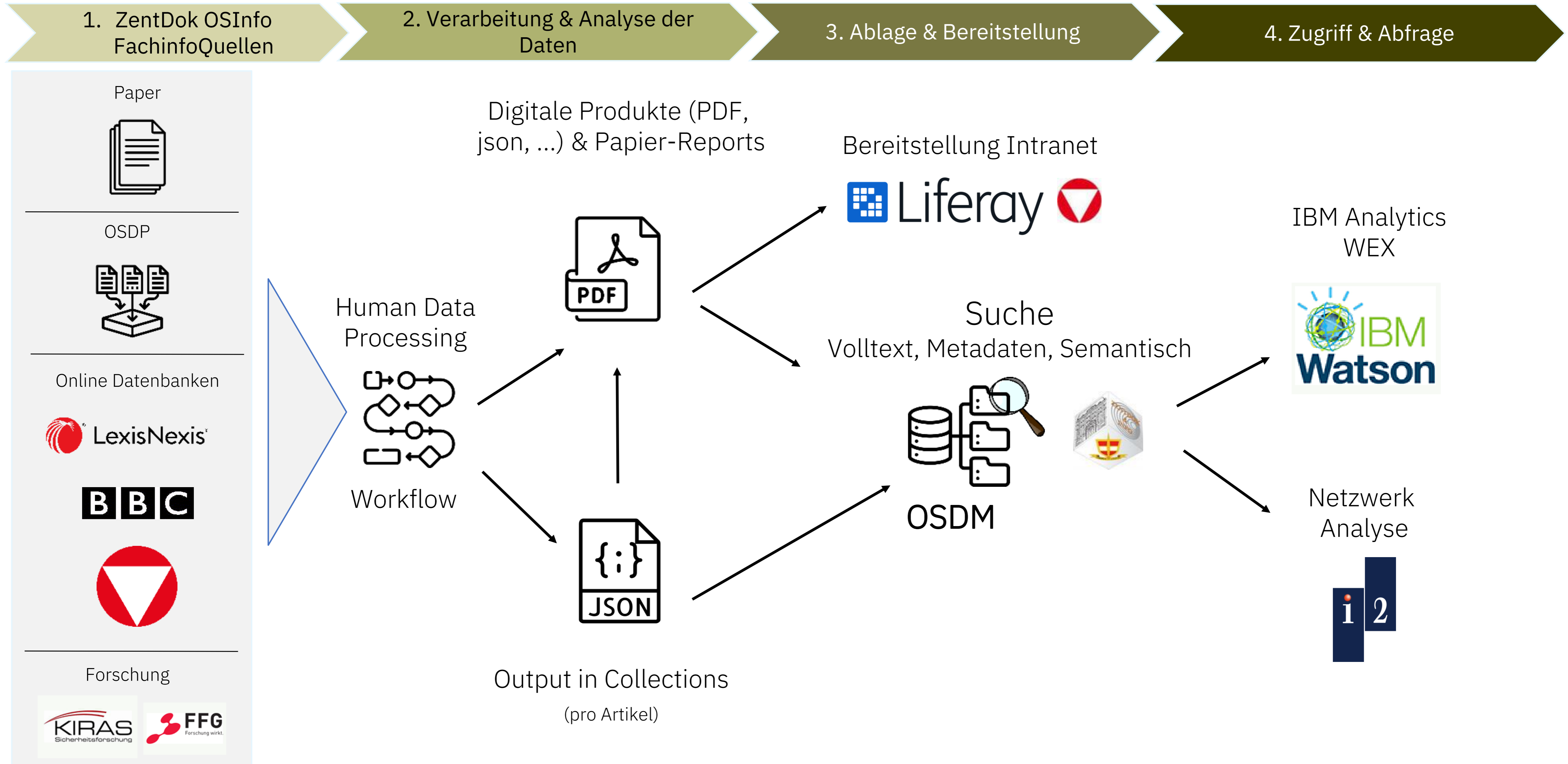
| Lösungsübersicht

| Ausblick

| Q&A

Ausgangssituation

Suche und Analyse



Generative KI... beyond the hype



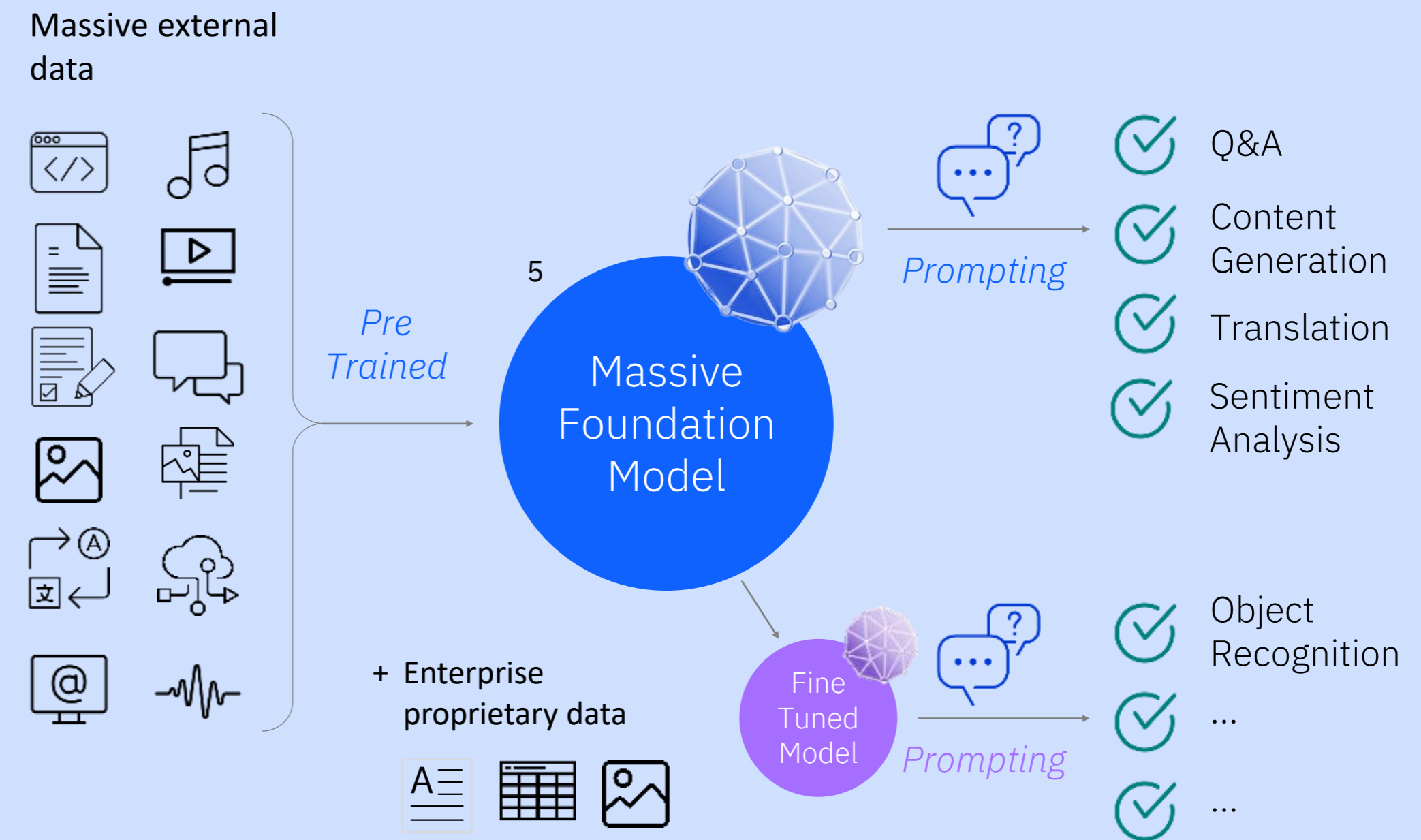
Large Language Models als Disruptives Ereignis in der Informationsbereitstellung

Traditionelle KI Modelle



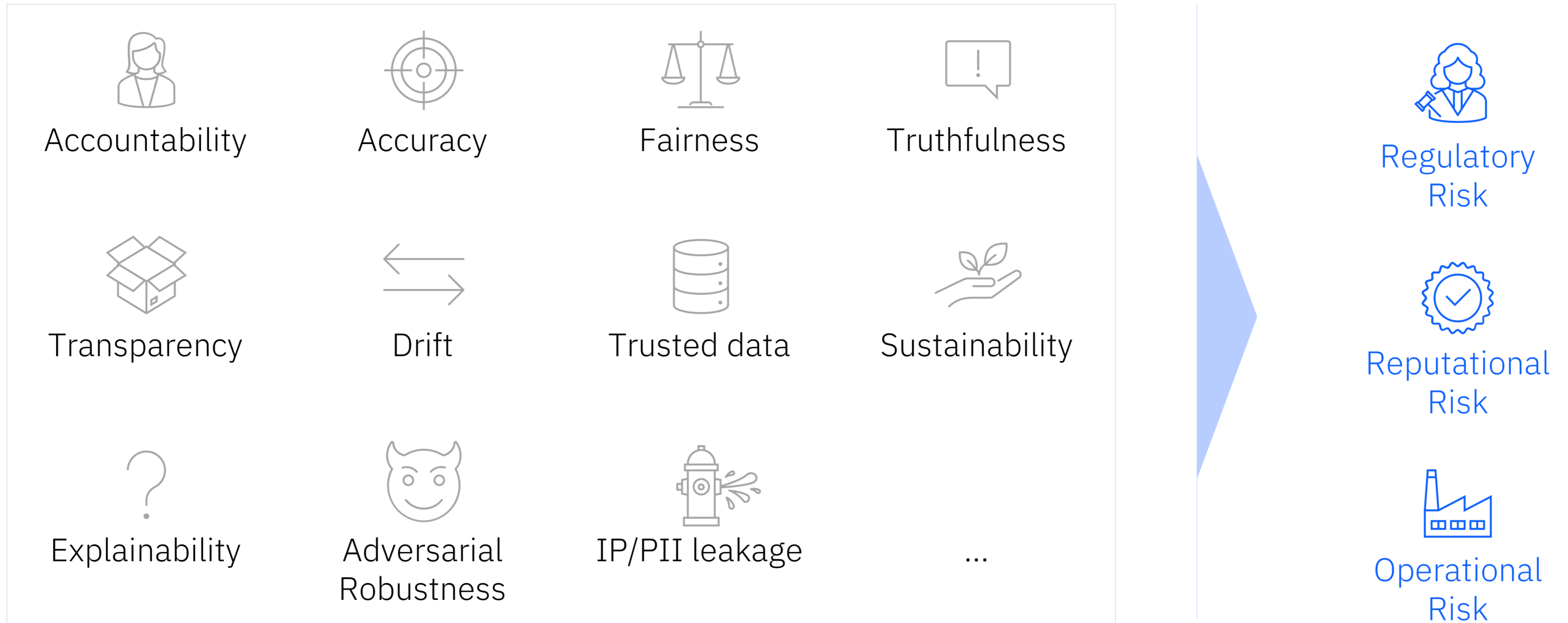
- Spezialisierte Modelle
- Aufgabenspezifisches Training
- Umfangreiches "human supervised training"

Foundation Models & LLMs



- Große, multi-tasking-fähige Modelle
- Bereits ohne oder mit nur geringem Training nutzbar
- Grossteils "unsupervised learning" + RLHF

AI Risiken

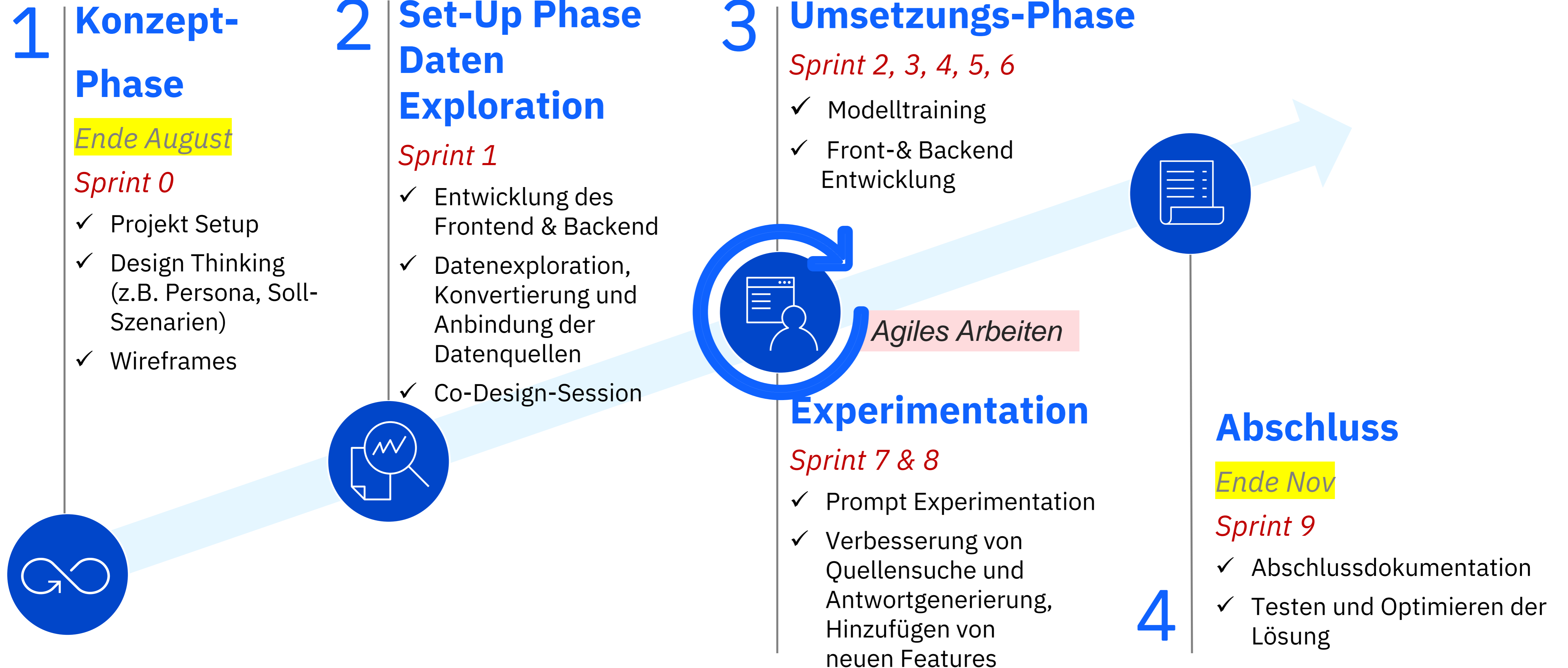


IBM adressiert viele dieser Herausforderungen mit [watsonx](#)

Projekttablauf



Projektverlauf & Agile Methodik



Zielbeschreibung der Lösung

”MVP Statement”

- Die Möglichkeit **Fragen in natürlicher Sprache zu stellen** bei Nutzung von Kontextoptionen wie z.B. Datums-Filter
- Die Antwort soll **faktenbasiert auf Basis der OSDP-Daten** und mit **Quellen** versehen sein
- Nutzer sollen **Feedback** auf Antworten geben können, die die Lösung generiert (+/- und Kommentar)

Es soll sichergestellt sein, dass:

- **große Dokumentenmengen effizient verarbeitet** werden können
- das **System leicht wartbar ist**

Wir können den Erfolg unseres Systems daran messen, dass

- die bereitgestellten **Informationen korrekt und zuverlässig** sind.
- **das System intuitiv und einfach zu bedienen ist**, sodass Benutzer in der Lage sind, Fragen in natürlicher Sprache an die Datenbank zu stellen.
- Nutzer **qualitativ hochwertige Antworten** erhalten



ZentDok Anforderungen an die Lösung (MVP)



Eigene validierte Datenquellen

Eigenes & öffentliches Wissensspektrum
Die Lösung basiert auf Quellen, die vom BMLV geprüft wurden



Tagesaktuelle Daten

Die validierten Quellen werden täglich aktualisiert



Nutzer Vertrauen

Die Lösung muss anhand einer Ground Truth (Wahrheitsgetreu / Referenz) validiert werden.
Feedback-Funktion zur Optimierung der Lösung durch *"Human in the Loop"*



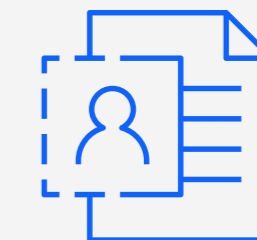
Personalisiertes Tool

Historisierung | Kopier- und Exportfunktionen
Einfache Nutzerverwaltung
Anwenderspezifische Einstellungen



Qualität

Hohe Qualität der Antworten
und der referenzierten Quellen
Performance des Tools



Transparenz

Welches Modell wird verwendet?
Welche Quellen werden genutzt?
Color Coding & Warnhinweise

ChatZentDok: MVP Scope

Print Media

OSDP

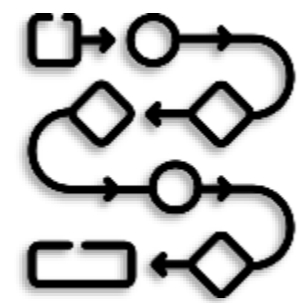
Online News Sources

- LexisNexis
- BBC

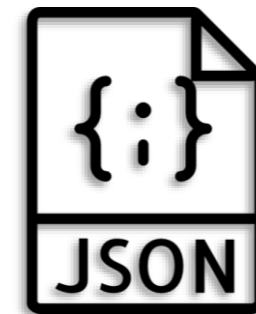
Research

- KIRAS
- FFG

Human Processing Workflow



Collections & Articles



Data Repository & Search
full text, metadata, semantic



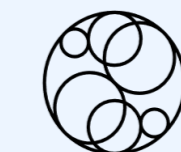
~115.000 Documents



ChatZentDok MVP

Retrieval Augmented Generation Pattern

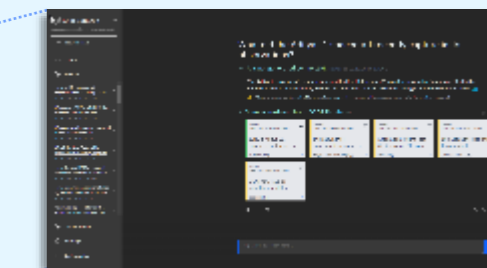
ChatZentDok



Watson.x

IBM Cloud

- ✓ watsonx.ai
- ✓ Milvus
- ✓ Watson Discovery
- ✓ Watson Studio
- ✓ Watson Pipelines
- ✓ COS
- ...

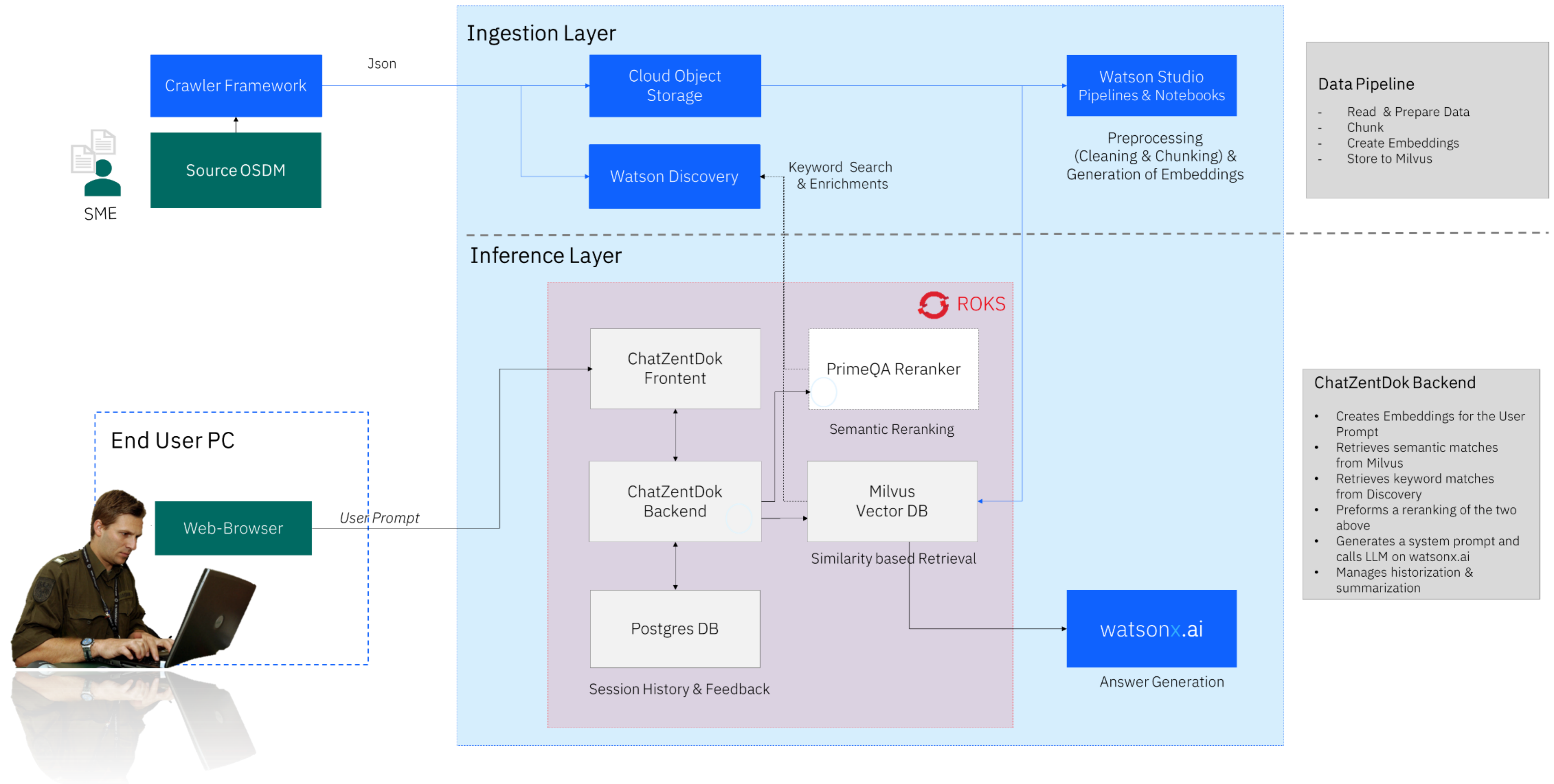


Natürlich-sprachliche Abfrage der Daten der ZentDok / LVAK

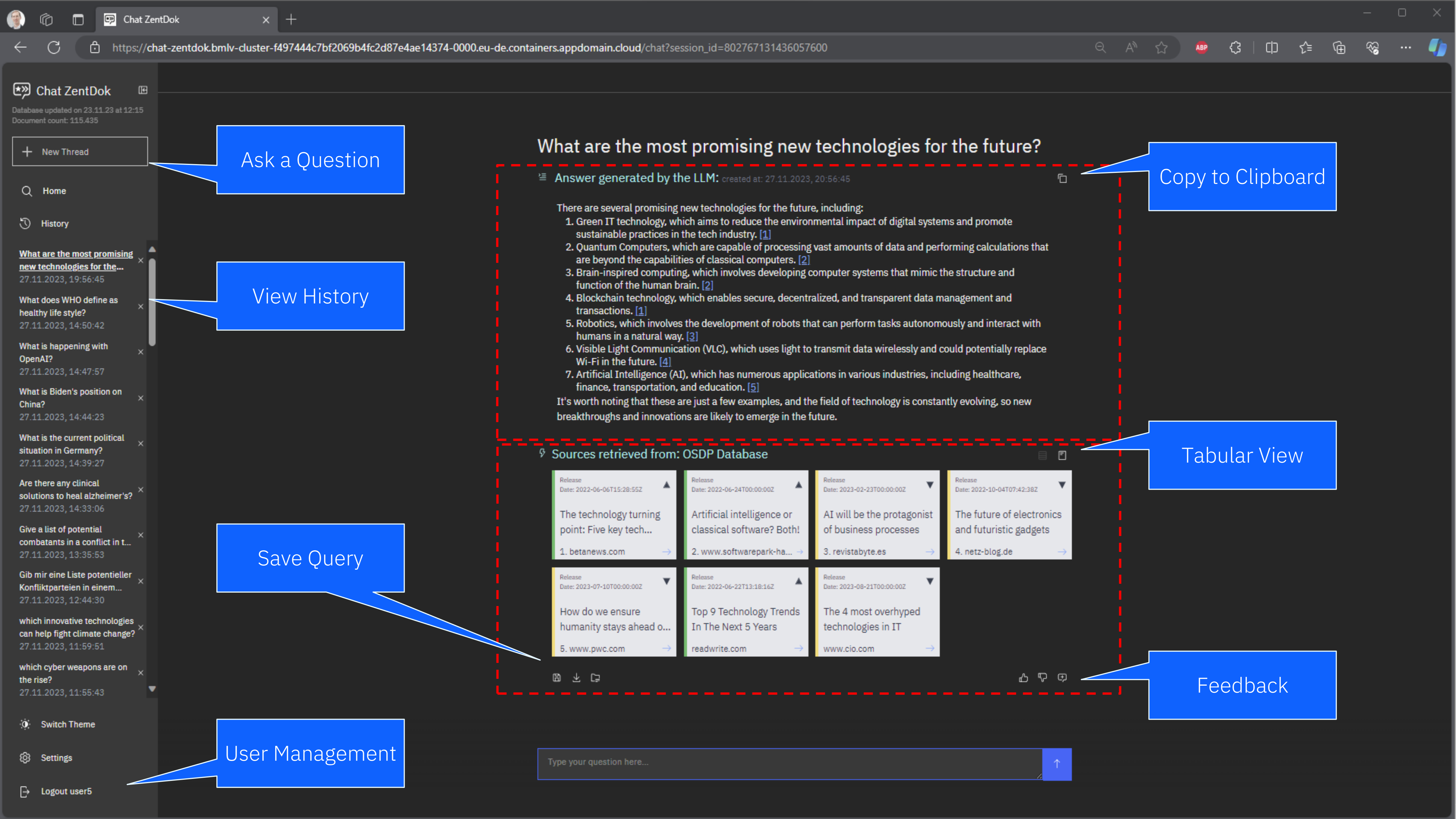
MVP Architektur und Lösungskomponenten



MVP Architektur



Willkommen zu ChatZentDok!



Ask a Question

View History

Save Query

User Management

Copy to Clipboard

Tabular View

Feedback

What are the most promising new technologies for the future?

Answer generated by the LLM: created at: 27.11.2023, 20:56:45

There are several promising new technologies for the future, including:

1. Green IT technology, which aims to reduce the environmental impact of digital systems and promote sustainable practices in the tech industry. [1]
2. Quantum Computers, which are capable of processing vast amounts of data and performing calculations that are beyond the capabilities of classical computers. [2]
3. Brain-inspired computing, which involves developing computer systems that mimic the structure and function of the human brain. [2]
4. Blockchain technology, which enables secure, decentralized, and transparent data management and transactions. [1]
5. Robotics, which involves the development of robots that can perform tasks autonomously and interact with humans in a natural way. [3]
6. Visible Light Communication (VLC), which uses light to transmit data wirelessly and could potentially replace Wi-Fi in the future. [4]
7. Artificial Intelligence (AI), which has numerous applications in various industries, including healthcare, finance, transportation, and education. [5]

It's worth noting that these are just a few examples, and the field of technology is constantly evolving, so new breakthroughs and innovations are likely to emerge in the future.

Sources retrieved from: OSDP Database

<p>Release Date: 2022-06-06T15:28:55Z</p> <p>The technology turning point: Five key tech...</p> <p>1. betanews.com →</p>	<p>Release Date: 2022-06-24T00:00:00Z</p> <p>Artificial intelligence or classical software? Both!</p> <p>2. www.softwarepark-ha... →</p>	<p>Release Date: 2023-02-23T00:00:00Z</p> <p>AI will be the protagonist of business processes</p> <p>3. revistabyte.es →</p>	<p>Release Date: 2022-10-04T07:42:38Z</p> <p>The future of electronics and futuristic gadgets</p> <p>4. netz-blog.de →</p>
<p>Release Date: 2023-07-10T00:00:00Z</p> <p>How do we ensure humanity stays ahead o...</p> <p>5. www.pwc.com →</p>	<p>Release Date: 2022-06-22T13:18:16Z</p> <p>Top 9 Technology Trends In The Next 5 Years</p> <p>readwrite.com →</p>	<p>Release Date: 2023-08-21T00:00:00Z</p> <p>The 4 most overhyped technologies in IT</p> <p>www.cio.com →</p>	

Type your question here... ↑

Feature Umsetzung



Chat ZentDok

Database updated on 09.04.2024 at 03:05:23 PM, Document count: 148388
Database Source: osdp

+ New Thread

History

- What steps should be taken to secure a home Wi-Fi...
10.4.2024, 09:31:40 osdp
- What are the potential societal impacts of...
10.4.2024, 09:30:56 osdp
- What are the potential impacts of widespread...
10.4.2024, 09:22:25 osdp
- List gamechanging technologies in electronic...
7.4.2024, 20:05:17 osdp
- What are recent cyber related CVEs?
7.4.2024, 20:03:04 osdp
- Please provide me a list of drone manufacturers?
7.4.2024, 19:58:07 presse
- Provide me a list of drone manufacturers?
7.4.2024, 19:56:42 osdp
- Give me list of known hacker group names?
7.4.2024, 19:53:30 osdp

Admin Panel
Thread Logging
Settings
Logout klotzb

What steps should be taken to secure a home Wi-Fi network against unauthorized access?

Filtered by date: 01.01.2000 - 10.04.2024

Answer generated by the LLM: Wed Apr 10 2024 09:31:40 GMT+0200 (Central European Summer Time)

Here are some steps that can be taken to secure a home Wi-Fi network against unauthorized access:

1. Change the default username and password of the router to a strong, unique combination. This step helps protect against attackers who target default credentials. [1]
2. Enable WPA2 or WPA3 encryption on the Wi-Fi network to encrypt the data transmitted between devices and the router. Encryption adds an extra layer of security and makes it significantly more difficult for hackers to intercept sensitive information. [2]
3. Regularly update the router's firmware to ensure it has the latest security patches and features. This helps protect against known vulnerabilities and security threats. [1]
4. Use network segmentation to separate the home network into different segments, such as one for IoT devices, guests, and personal devices. This helps limit the spread of malware and unauthorized access to sensitive information. [1]
5. Use a firewall to block incoming and outgoing traffic that could pose a threat to the network. [2]
6. Consider using a personally owned routing device that connects to the ISP-provided modem/router, which can provide additional security features and controls. [1]
7. Limit administration to the internal network only, and use secure habits such as backing up data and disconnecting devices when not needed. [1]
8. Use a VPN or a secure communication channel such as HTTPS to protect against man-in-the-middle attacks. [3]
9. Keep software and firmware up to date, and use a robust antivirus software to detect and remove malware. [2]
10. Isolate devices that are not needed for the network, and use strict access control to manage Wi-Fi access rights at the device level. [4]

By following these steps, individuals can help protect their home Wi-Fi network from unauthorized access and potential security threats.

Sources retrieved from: OSDP Database

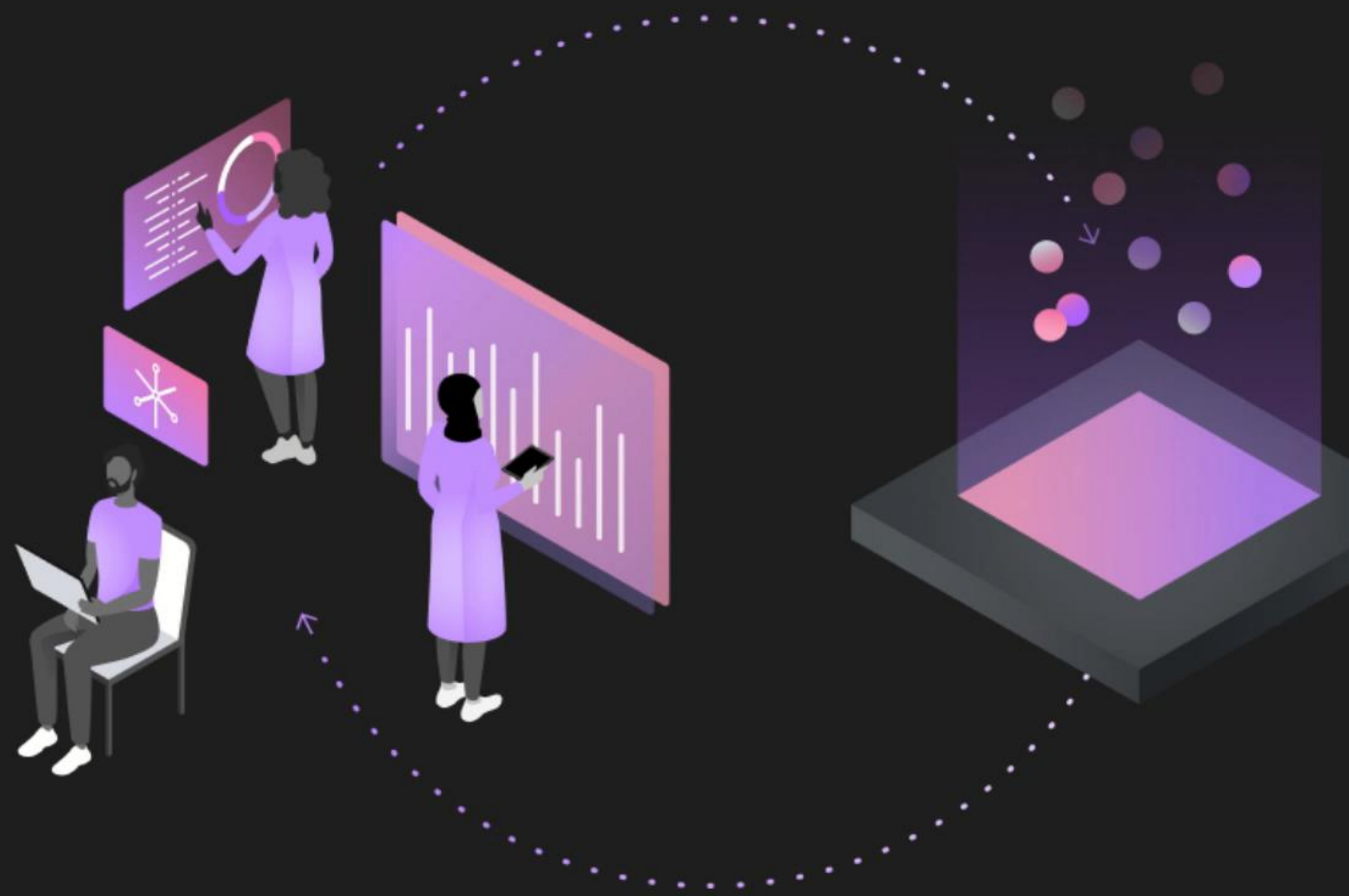
Release Date: 2023-02-23T14:21:18Z NSA Released Checklist To Secure Home Wi-Fi... 1. gbhackers.com	Release Date: 2023-07-22T00:00:00Z 10 Essential Cybersecurity Tips for... 2. www.hackread.com	Release Date: 2023-01-19T18:03:58Z Common Attacks on Wi-Fi and How to Prevent... 3. techlog360.com	Release Date: 2023-08-09T00:00:00Z Disposing of a gadget? Remember to wipe this
Release Date: 2023-03-01T00:00:00Z Wireless Security: WEP, WPA, WPA2 and WPA3... www.esecurityplanet.com	Release Date: 2022-07-18T20:03:00Z 7 ways to keep smart home devices safe from... cybersecuritynews.es	Release Date: 2024-01-15 15:11:42 Top 19 Network Security Threats + Defenses for... www.esecurityplanet.com	

Type your question here...

- ✓ **Quellenangabe:** Das Tool gibt an, welche Quellen zur Formulierung der Antwort verwendet wurden
- ✓ **Historie der Queries:** Speichert und zeigt die Historie der durchgeführten Suchanfragen des Nutzers an
- ✓ **Feedback-Funktion** für die Antwort: Ermöglicht es dem Nutzer, Feedback zur Qualität und Relevanz der erhaltenen Antworten zu geben
- ✓ **Filtern nach Datum:** Der Nutzer kann seine Suche auf einen bestimmten Zeitraum eingrenzen, indem er nach Datum filtert
- ✓ **Warnhinweise:** ChatZentDok warnt den Nutzer, falls die Inhalte von der Frage abweichen oder nicht auf fakten basieren
- ✓ **Quellen mit Release-Datum:** Zeigt das Veröffentlichungsdatum der verwendeten Quellen an
- ✓ **Sicht Switch (Tabelle/Kacheln):** Bietet die Möglichkeit, zwischen verschiedenen Ansichtsmodi (wie Tabelle oder Kacheln) zu wechseln
- ✓ **Light/dark Theme,** um den visuellen Komfort zu erhöhen

Version 1.0

[Sign In](#) →



+ New Thread

History

List gamechanging technologies in electronic...
7.4.2024, 20:05:17 osdp

What are recent cyber related CVEs?
7.4.2024, 20:03:04 osdp

Please provide me a list of drone manufacturers?
7.4.2024, 19:58:07 presse

Provide me a list of drone manufacturers?
7.4.2024, 19:56:42 osdp

Give me list of known hacker group names?
7.4.2024, 19:53:30 osdp

Admin Panel

Thread Logging

Settings

Logout klotzb

Looking for answers? Ask me anything

Ask anything... [Microphone icon] [Send icon]

Refine search 1.1.2000 - 7.4.2024 osdp [Dropdown arrow]

Try some example questions

- Crisis, military & security policy**
How did Russian forces target a Ukrainian ammunition depot in the Donetsk People's Republic, and what was the outcome of this action?
Make me a list of all the means and methods used by HAMAS terrorists to cross the border into Israel on 7 October 2023.
- Cyber**
What are the concerns and challenges identified in the use of AI-powered search engines like Microsoft's Bing and Google's Bard?
Describe per country Israel, UAE, Bahrain, Morocco, Oman and Kuwait the recent developments in cybersecurity cooperation following the Abraham Accords.
- Innovation & technology**
How is IBM preparing organizations for the potential threat posed by quantum computers?
Describe the key innovation of the fabric-based wearable device developed by scientists at Rice University for navigation.

+ New Thread

History

- Provide military trends in AI? 7.4.2024, 21:08:45 osdp
- List gamechanging technologies in electronic... 7.4.2024, 20:05:17 osdp
- What are recent cyber related CVEs? 7.4.2024, 20:03:04 osdp
- Please provide me a list of drone manufacturers? 7.4.2024, 19:58:07 presse
- Provide me a list of drone manufacturers? 7.4.2024, 19:56:42 osdp
- Give me list of known hacker group names?

- Admin Panel
- Thread Logging
- Settings
- Logout klotzb

Provide military trends in AI?

Filtered by date: 01.01.2000 - 07.04.2024

Answer generated by the LLM: Sun Apr 07 2024 21:08:45 GMT+0200 (Central European Summer Time)

Sure! Here are some military trends in AI:

1. Increased use of AI in combat simulations to improve operational efficiency, reduce reliance on human input, reduce loss of life, and save money and time. [1]
2. Integration of AI into war planning, including the use of AI to help generals decide battlefield movements. [2]
3. Use of AI for targeting, sorting through intel functions, and pattern recognition. [3]
4. Development of autonomous drones for surveillance, attacks, and delivery of supplies. [4]
5. Investment in AI research and development to improve military capabilities, including the establishment of an AI lab. [5]
6. Focus on developing AI systems that can make good decisions, not just for commanders. [5]
7. Exploration of the potential of AI to support warfighters in their missions. [6]
8. Efforts to address concerns about the ethical implications of using AI in warfare. [2]

These are some of the military trends in AI that can be inferred from the provided documents.

Sources retrieved from: OSDP Database

<p>Release Date: 2023-02-17T00:00:00Z ▲</p> <p>The AI war that is responsible for the mor...</p> <p>1.www.rti.org.tw →</p>	<p>Release Date: 2023-03-27T00:00:00Z ▲</p> <p>Will the generals of the future be artificial?</p> <p>2.cybernews.com →</p>	<p>Release Date: 2023-06-22T18:24:41Z ▲</p> <p>Kendall: Air Force studying 'military...</p> <p>3.breakingdefense.com →</p>	<p>Release Date: 2022-07-07 07:15:22 ▲</p> <p>Why business is booming for military AI startups</p> <p>4.www.technologyreview.com →</p>
<p>Release Date: 2022-11-29T14:08:14Z ▲</p> <p>How Israel is preparing the next generation of...</p> <p>5.www.defensenews.com →</p>	<p>Release Date: 2022-05-17T08:00:19Z ▲</p> <p>AI for Military Uses – Unexpected News</p> <p>6.i-hls.com →</p>	<p>Release Date: 2023-03-27 02:00:00 ▲</p> <p>Will the generals of the future be artificial?</p> <p>cybernews.com →</p>	<p>Release Date: 2024-03-06 06:00:17 ▲</p> <p>US Army Is Looking Into AI's Potential for Battle...</p> <p>www.techtimes.com →</p>

Type your question here... [Microphone icon] [Send icon]

Ausblick & Nächste Schritte

- Horizon Scanning KI
- On Premise Infrastruktur
- Vergleich von LLMs
- ...



Fragen?



Vielen Dank!

The background is a low-poly, abstract pattern of irregular polygons. The colors transition from a light, yellowish-green on the left side to a dark, almost black brown on the right side. The overall effect is a textured, geometric gradient.