Sicherheitsautomation mit KI: Mehr als nur Prompts

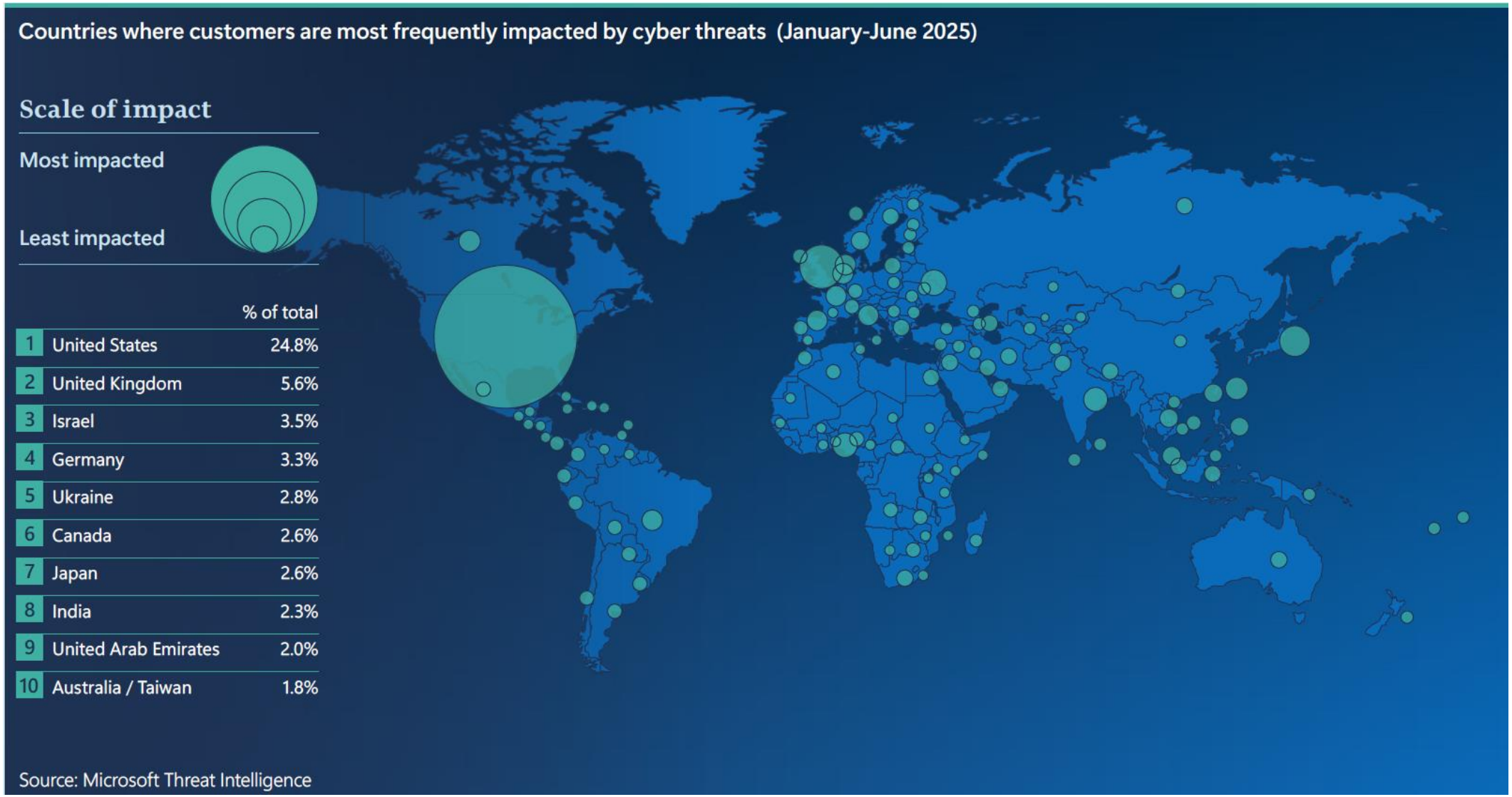
Prof. Dr. Jan Stehr
06.11.2025

Dozierende an der FHDW in Theorie und Praxis, z. B. ich

Dozent für Informatik-Kern- und Infrastrukturthemen, Cyber Security, KI an der FHDW.

CISO und Sicherheitsberater im Umfeld Smart Cities bei der HYPERTEGRITY AG.

Situation


Countries where customers are most frequently impacted by cyber threats (January-June 2025)
Scale of impact
Most impacted
Least impacted
% of total
1 United States 24.8%
2 United Kingdom 5.6%
3 Israel 3.5%
4 Germany 3.3%
5 Ukraine 2.8%
6 Canada 2.6%
7 Japan 2.6%
8 India 2.3%
9 United Arab Emirates 2.0%
10 Australia / Taiwan 1.8%
Source: Microsoft Threat Intelligence

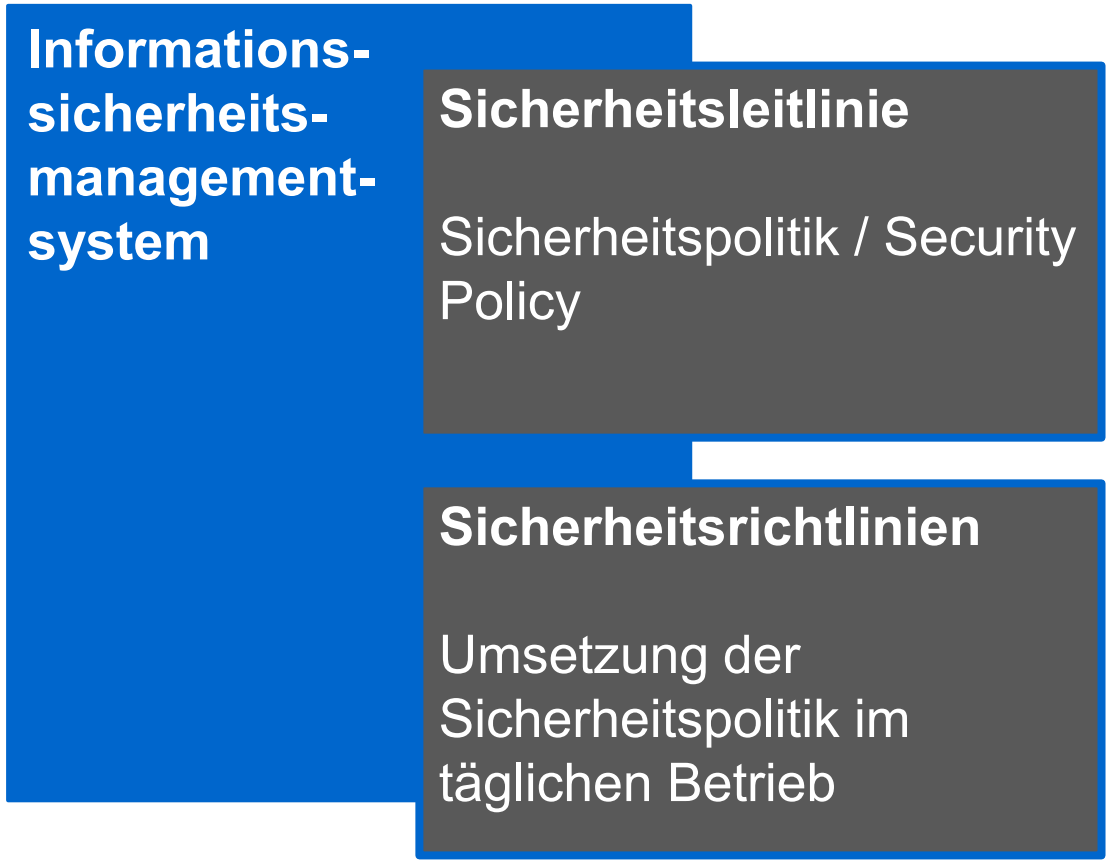
Situation

Die Sicherheitslage verschärft sich in Europa und Deutschland, die Sicherheitsanforderungen steigen.

KRITIS-DG, NIS2, DSGVO & Co. erfordern Dokumentation, Nachweise und Zertifizierungen.

Das erfordert
technische und **organisatorische (Sicherheits-) Maßnahmen (TOM)**.

TOM und ISMS

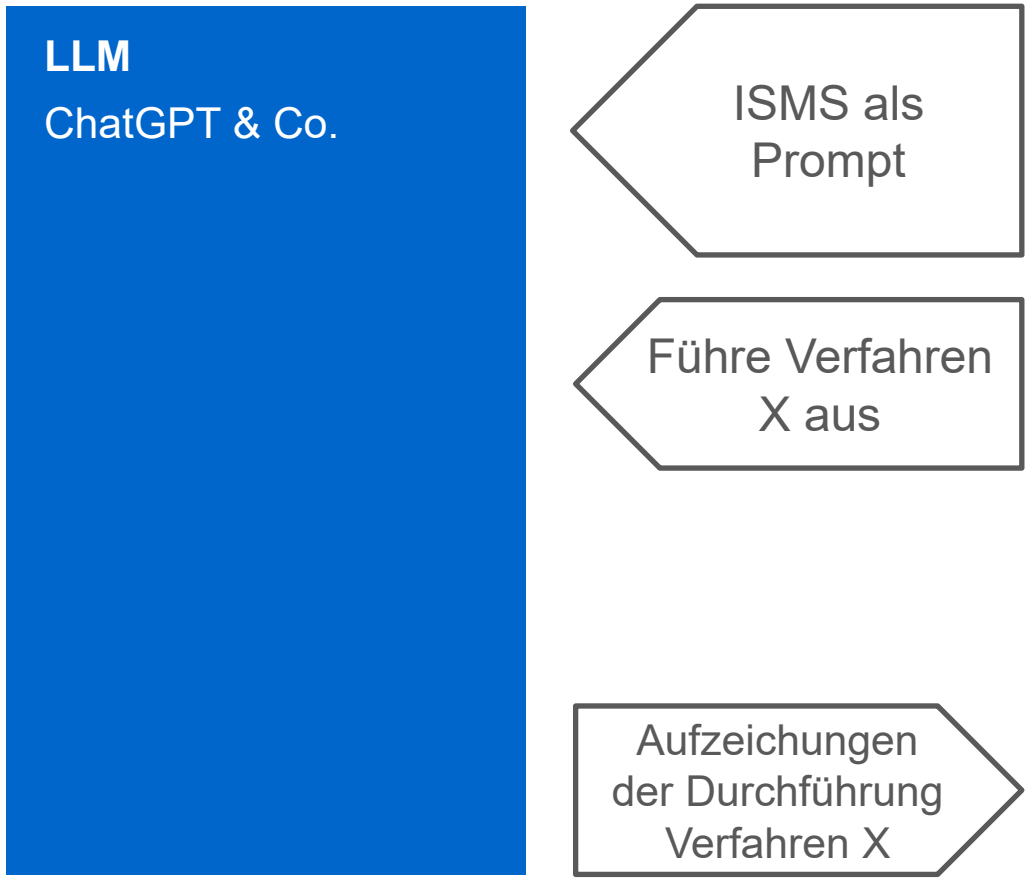


Angemessene TOM werden schnell so umfangreich und komplex, dass sie ein ISMS erfordern.

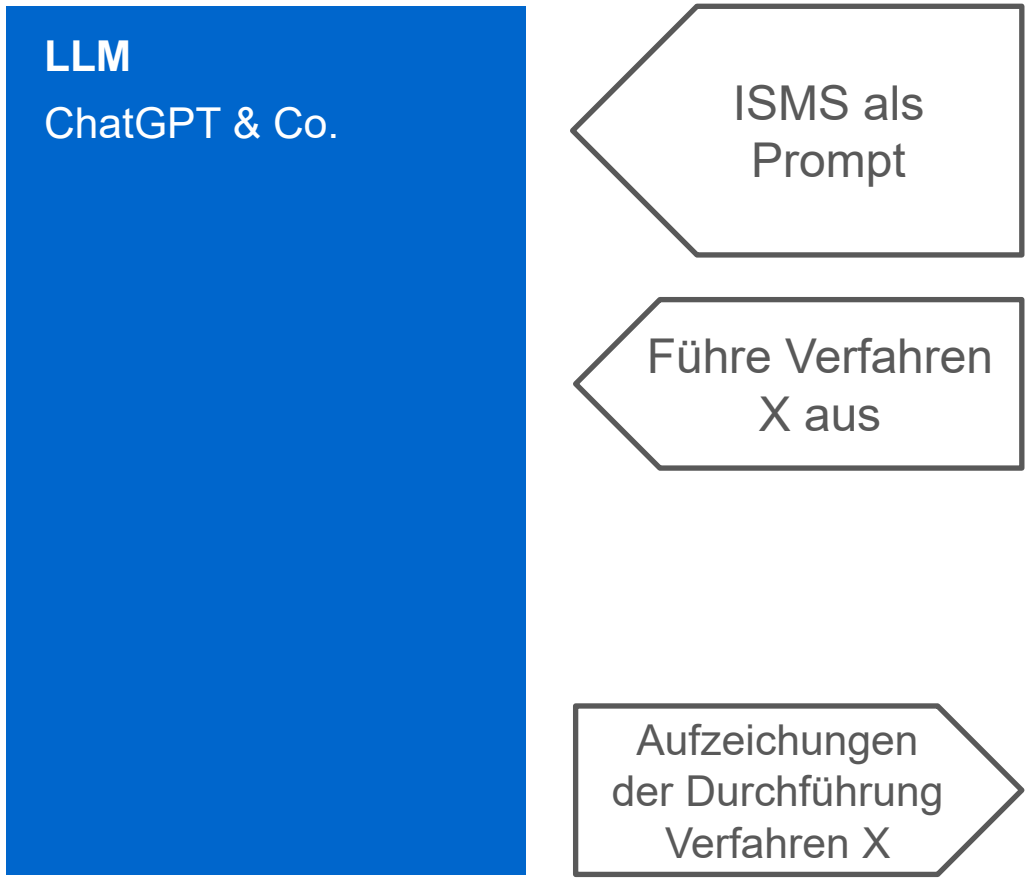
Der mit dem – jederzeit „audit ready“ – Betrieb eines ISMS verbundene Zeit- und Personalaufwand ist von Kommunen und vom Mittelstand wirtschaftlich schwer leistbar.

Machen wir das doch einfach mit KI!

Naiver Ansatz



Naiver Ansatz: Probleme



Fremdes KI-System versus interne Betriebsdaten im ISMS.

„OpenAI verwendet keine Daten aus dem Arbeitsbereich [Ihrer Organisation] zum Trainieren seiner Modelle.“
← überspezifisches Dementi ☠

Besserer Ansatz

LLM

ChatGPT & Co.

Lokales SLM

evaluieren z. B. mit `lmstudio.ai`

Aber: Reduzierte Leistungsfähigkeit, also...

Besserer Ansatz

LLM

ChatGPT & Co.

Lokales SLM

evaluieren z. B. mit `lmstudio.ai`

ITSec Ontology

ISMS RAG Storage

Unterstützung der KI durch aufbereitete Datenbasis

Vokabular + Regeln

Unternehmensspezifische Sicherheitsinformationen als Wissensgraph

Strukturierte Informationsbasis für KIs: Die Ontologie

Ontologie für Informationssicherheit (IS)

Das semantische Fundament unserer IS-Daten und -Prozesse. Die Ontologie macht Begriffe, Beziehungen und Regeln eindeutig, damit Menschen und Maschinen verlässlich und konsistent damit arbeiten können.

- Gemeinsame Sprache und Interoperabilität zwischen SIEM, CTI, Compliance etc.
- Datenintegration und Normalisierung heterogener Telemetrie und TI.
- Abfragen und Schlussfolgern (z. B. „welche S-Maßnahmen mitigieren welche Bedrohungen unserer kritischen Assets?“).
- Automatisierung in Analyse und Reaktion (Playbooks, Detektion und Folge, Risiko-Priorisierung).

Ontologie praktisch

Keine akademisch-theoretische Spinnerei!

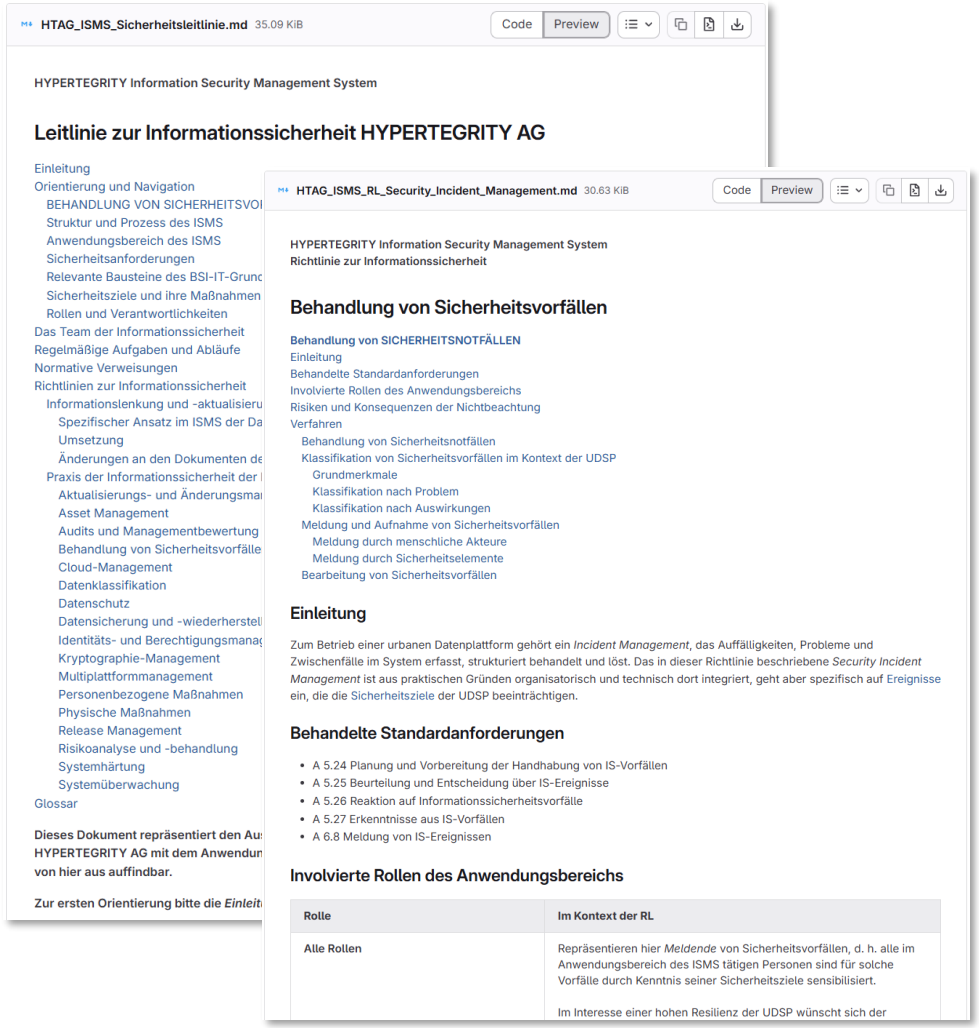
Bei **Palantir** Verbindung digitaler Assets und der realen Welt, für den digitalen Zwilling:
`https://www.palantir.com/docs/foundry/ontology/overview`

Unified Cyber Ontology (UCO) als Beispiel für IT-Sicherheit:
`https://unifiedcyberontology.org/`

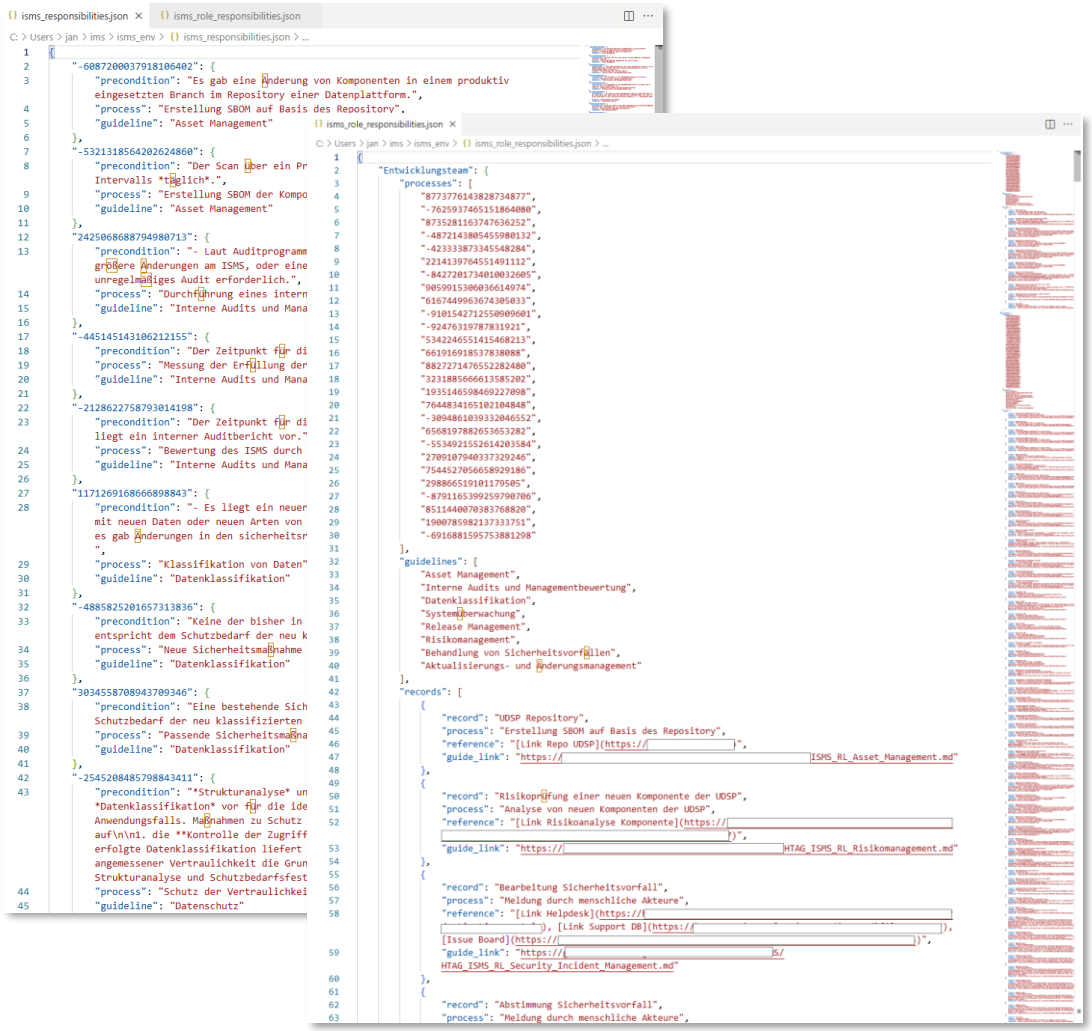
Spezifikation der **Web Ontology Language** (OWL kein Tippfehler):
`https://www.w3.org/OWL/`

IS-Ontologie praktisch

Menschliche Sicht

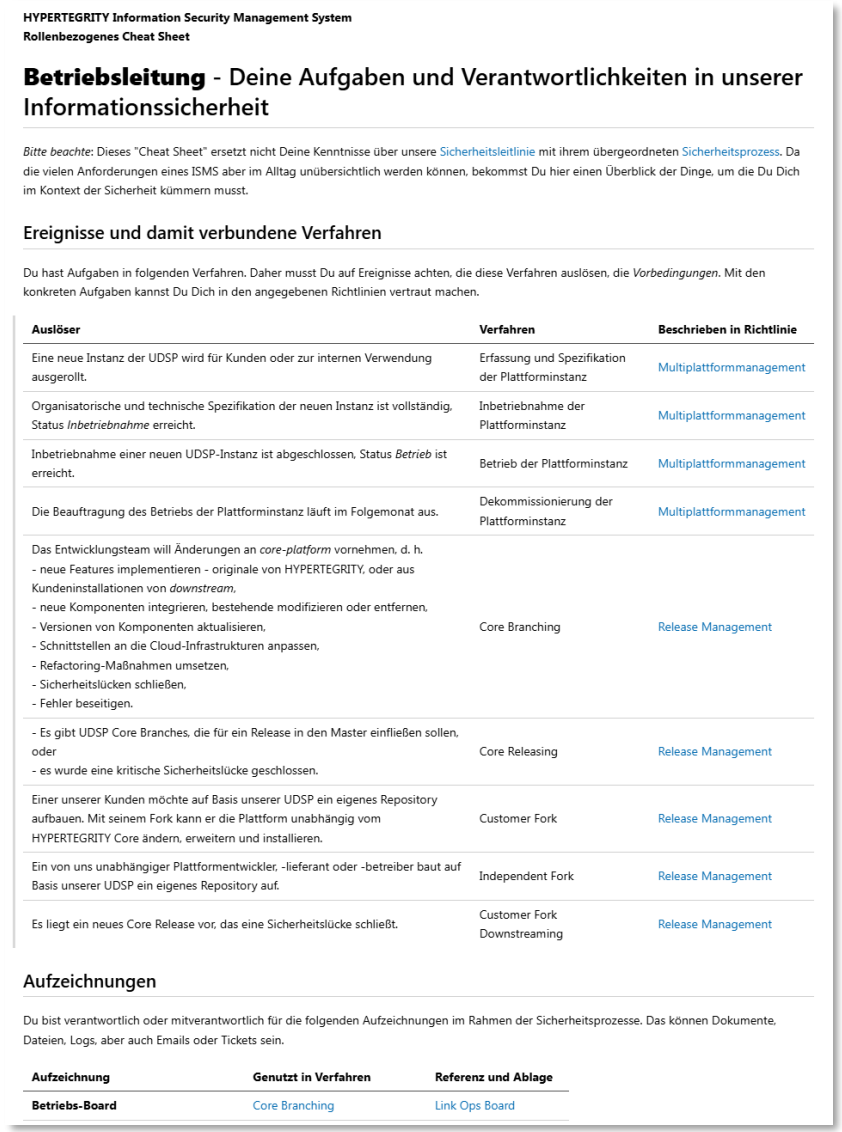


Maschinelle Sicht



IS-Ontologie praktisch

Einfacher Anwendungsfall:
Welche **Aufgaben** und **Verantwortlichkeiten** hat die menschliche **Betriebsleitung** im komplexen IS-Management?



HYPERTEGRITY Information Security Management System
Rollenbezogenes Cheat Sheet

Betriebsleitung - Deine Aufgaben und Verantwortlichkeiten in unserer Informationssicherheit

Bitte beachte: Dieses "Cheat Sheet" ersetzt nicht Deine Kenntnisse über unsere Sicherheitsleitlinie mit ihrem übergeordneten Sicherheitsprozess. Da die vielen Anforderungen eines ISMS aber im Alltag unübersichtlich werden können, bekommst Du hier einen Überblick der Dinge, um die Du Dich im Kontext der Sicherheit kümmern musst.

Ereignisse und damit verbundene Verfahren

Du hast Aufgaben in folgenden Verfahren. Daher musst Du auf Ereignisse achten, die diese Verfahren auslösen, die *Vorbedingungen*. Mit den konkreten Aufgaben kannst Du Dich in den angegebenen Richtlinien vertraut machen.

Auslöser	Verfahren	Beschrieben in Richtlinie
Eine neue Instanz der UDSP wird für Kunden oder zur internen Verwendung ausgerollt.	Erfassung und Spezifikation der Plattforminstanz	Multiplattformmanagement
Organisatorische und technische Spezifikation der neuen Instanz ist vollständig, Status *Inbetriebnahme* erreicht.	Inbetriebnahme der Plattforminstanz	Multiplattformmanagement
Inbetriebnahme einer neuen UDSP-Instanz ist abgeschlossen, Status *Betrieb* ist erreicht.	Betrieb der Plattforminstanz	Multiplattformmanagement
Die Beauftragung des Betriebs der Plattforminstanz läuft im Folgemonat aus.	Dekommissionierung der Plattforminstanz	Multiplattformmanagement
Das Entwicklungsteam will Änderungen an *core-platform* vornehmen, d. h. - neue Features implementieren - originale von HYPERTEGRITY, oder aus Kundeninstallationen von *downstream*, - neue Komponenten integrieren, bestehende modifizieren oder entfernen, - Versionen von Komponenten aktualisieren, - Schnittstellen an die Cloud-Infrastrukturen anpassen, - Refactoring-Maßnahmen umsetzen, - Sicherheitslücken schließen, - Fehler beseitigen.	Core Branching	Release Management
- Es gibt UDSP Core Branches, die für ein Release in den Master einfließen sollen, oder - es wurde eine kritische Sicherheitslücke geschlossen.	Core Releasing	Release Management
Einer unserer Kunden möchte auf Basis unserer UDSP ein eigenes Repository aufbauen. Mit seinem Fork kann er die Plattform unabhängig vom HYPERTEGRITY Core ändern, erweitern und installieren.	Customer Fork	Release Management
Ein von uns unabhängiger Plattformentwickler, -lieferant oder -betreiber baut auf Basis unserer UDSP ein eigenes Repository auf.	Independent Fork	Release Management
Es liegt ein neues Core Release vor, das eine Sicherheitslücke schließt.	Customer Fork Downstreaming	Release Management

Aufzeichnungen

Du bist verantwortlich oder mitverantwortlich für die folgenden Aufzeichnungen im Rahmen der Sicherheitsprozesse. Das können Dokumente, Dateien, Logs, aber auch Emails oder Tickets sein.

Aufzeichnung	Genutzt in Verfahren	Referenz und Ablage
Betriebs-Board	Core Branching	Link Ops Board

Maschinelle Sicht dahinter als Grundlage für **Agenten**...

Und das war er auch schon,
ein kleiner Impuls zu
Ontologien in der IT-Sicherheit.

Für genauere Einblicke steht Ihnen
das Team der FHDW zur Verfügung!

U. a. jan.stehr@fhdw.de