

Sicherheitsautomation mit KI: Mehr als nur Prompts

Prof. Dr. Jan Stehr
06.11.2025

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

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

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



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).

Informations- sicherheits- management- system

Sicherheitsleitlinie

Sicherheitspolitik / Security Policy

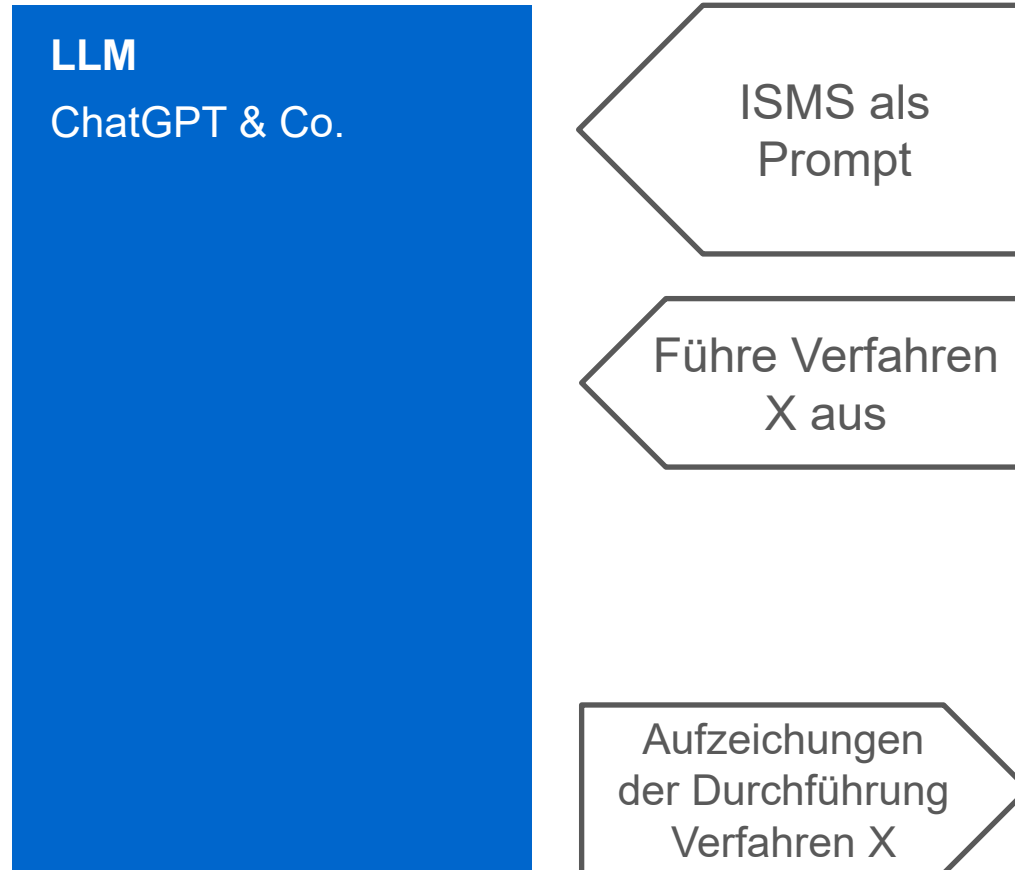
Sicherheitsrichtlinien

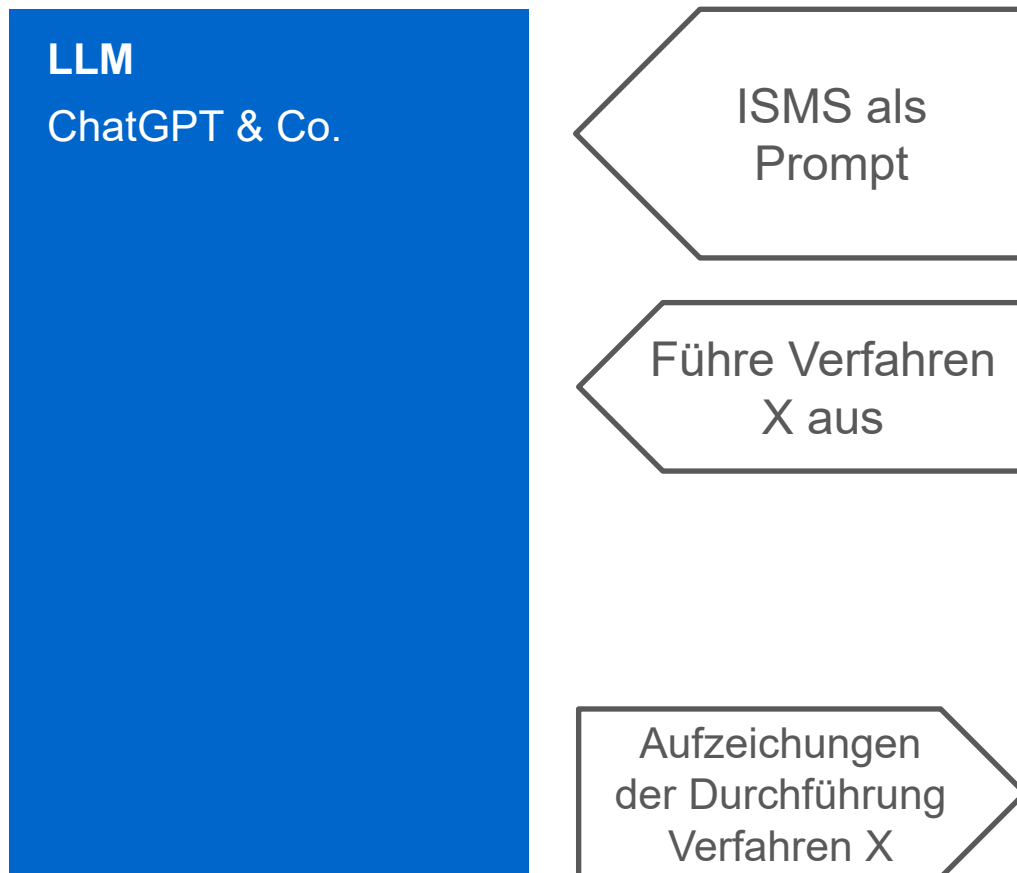
Umsetzung der
Sicherheitspolitik im
täglichen Betrieb

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!





Fremdes KI-System versus interne Betriebsdaten im ISMS.

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

← überspezifisches Dementi ☠

LLM

ChatGPT & Co.

Lokales SLM

evaluieren z. B. mit
`lmstudio.ai`

Aber: Reduzierte
Leistungsfähigkeit,
also...

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

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).

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/>

Menschliche Sicht

HTAG_ISMS_Sicherheitsleitlinie.md 35.09 KIB

Code Preview

HTAG_ISMS_Sicherheitsleitlinie.md

HYPERTEGRITY Information Security Management System

Leitlinie zur Informationssicherheit HYPERTEGRITY AG

Einleitung

Orientierung und Navigation

BEHANDLUNG VON SICHERHEITSVÖ

Struktur und Prozess des ISMS

Anwendungsbereich des ISMS

Sicherheitsanforderungen

Relevante Bausteine des BSI-IT-Grunc

Sicherheitsziele und ihre Maßnahmen

Rollen und Verantwortlichkeiten

Das Team der Informationssicherheit

Regelmäßige Aufgaben und Abläufe

Normative Verweisungen

Richtlinien zur Informationssicherheit

Informationslenkung und -aktualisieru

Spezifischer Ansatz im ISMS der Da

Umsetzung

Änderungen an den Dokumenten de

Praxis der Informationssicherheit der

Aktualisierungs- und Änderungsmai

Asset Management

Audits und Managementbewertung

Behandlung von Sicherheitsvorfälle

Cloud-Management

Datenklassifikation

Datenschutz

Datensicherung und -wiederherstell

Identitäts- und Berechtigungsmanag

Kryptographie-Management

Multiplattformmanagement

Personenbezogene Maßnahmen

Physische Maßnahmen

Release Management

Risikoanalyse und -behandlung

Systemhärtung

Systemüberwachung

Glossar

Dieses Dokument repräsentiert den Au

HYPERTEGRITY AG mit dem Anwendun

von hier aus auffindbar.

Zur ersten Orientierung bitte die Einleit

HTAG_ISMS_RL_Security_Incident_Management.md 30.63 KIB

Code Preview

HTAG_ISMS_RL_Security_Incident_Management.md

HYPERTEGRITY Information Security Management System

Richtlinie zur Informationssicherheit

Behandlung von Sicherheitsvorfällen

Behandlung von SICHERHEITSNOTFÄLLEN

Einleitung

Behandelte Standardanforderungen

Involvierte Rollen des Anwendungsbereichs

Verfahren

Behandlung von Sicherheitsnotfällen

Klassifikation von Sicherheitsvorfällen im Kontext der UDSP

Grundmerkmale

Klassifikation nach Problem

Klassifikation nach Auswirkungen

Meldung und Aufnahme von Sicherheitsvorfällen

Meldung durch menschliche Akteure

Meldung durch Sicherheitselemente

Bearbeitung von Sicherheitsvorfällen

Einleitung

Zum Betrieb einer urbanen Datenplattform gehört ein Incident Management, das Auffälligkeiten, Probleme und Zwischenfälle im System erfasst, strukturiert behandelt und löst. Das in dieser Richtlinie beschriebene Security Incident Management ist aus praktischen Gründen organisatorisch und technisch dort integriert, geht aber spezifisch auf Ereignisse ein, die die Sicherheitsziele der UDSP beeinträchtigen.

Behandelte Standardanforderungen

- A 5.24 Planung und Vorbereitung der Handhabung von IS-Vorfällen
- A 5.25 Beurteilung und Entscheidung über IS-Ereignisse
- A 5.26 Reaktion auf Informationssicherheitsvorfälle
- A 5.27 Erkenntnisse aus IS-Vorfällen
- A 6.8 Meldung von IS-Ereignissen

Involvierte Rollen des Anwendungsbereichs

Rolle	Im Kontext der RL
Alle Rollen	Repräsentieren hier Meldende von Sicherheitsvorfällen, d. h. alle im Anwendungsbereich des ISMS tätigen Personen sind für solche Vorfälle durch Kenntnis seiner Sicherheitsziele sensibilisiert.
	Im Interesse einer hohen Resilienz der UDSP wünscht sich der

Maschinelle Sicht

isms_responsibilities.json

isms_role_responsibilities.json

isms_responsibilities.json

```

1  {
2    "precondition": "Es gab eine Änderung von Komponenten in einem produktiv
3    eingesetzten Branch im Repository einer Datenplattform.",
4    "process": "Erstellung SBOM auf Basis des Repository",
5    "guideline": "Asset Management"
6  },
7  {
8    "precondition": "Der Scan über ein Pr
9    Intervalls *täglich*",
10   "process": "Erstellung SBOM der Kompo
11   "guideline": "Asset Management"
12 },
13 {
14   "precondition": "- Laut Auditprogramm
15   größere Änderungen am ISMS, oder eine
16   unregelmäßiges Audit erforderlich.",
17   "process": "Durchführung eines intern
18   "guideline": "Interne Audits und Mana
19 },
20 {
21   "precondition": "Der Zeitpunkt für di
22   "process": "Messung der Erfüllung der
23   "guideline": "Interne Audits und Mana
24 },
25 {
26   "precondition": "Der Zeitpunkt für di
27   liegt ein interner Auditbericht vor.",
28   "process": "Bewertung des ISMS durch
29   "guideline": "Interne Audits und Mana
30 },
31 {
32   "precondition": "- Es liegt ein neuer
33   mit neuen Daten oder neuen Arten von
34   es gab Änderungen in den sicherheitsr
35   ",
36   "process": "Klassifikation von Daten"
37   "guideline": "Datenklassifikation"
38 },
39 {
40   "precondition": "Keine der bisher in
41   entspricht dem Schutzbedarf der neu k
42   "process": "Neue Sicherheitsmaßnahme
43   "guideline": "Datenklassifikation"
44 },
45 {
46   "precondition": "Eine bestehende Sich
47   Schutzbedarf der neu klassifizierten
48   "process": "Passende Sicherheitsmaßna
49   "guideline": "Datenklassifikation"
50 },
51 {
52   "precondition": "- Strukturanalyse" un
53   "Datenklassifikation" von für die ide
54   Anwendungsfalls. Maßnahmen zu Schutz
55   auf/n/ni. die **Kontrolle der Zugriff
56   erfolgte Datenklassifikation liefert
57   angemessener Vertraulichkeit die Grun
58   Strukturanalyse und Schutzbedarfsfest
59   "process": "Schutz der Vertraulichkei
60   "guideline": "Datenschutz"
61 }
62
63

```

isms_role_responsibilities.json

```

1  {
2    "Entwicklungsteam": {
3      "processes": [
4        {
5          "id": "873776143828734877",
6          "description": "- 7625937465151864888",
7          "reference": "- 8735281163747636252",
8          "guideline": "- 487214380455980132",
9          "reference": "- 423333873345548284",
10         "reference": "- 2214139764551491112",
11         "reference": "- 8427201734810832685",
12         "reference": "- 9859915380836614974",
13         "reference": "- 6167449963674305833",
14         "reference": "- 9101542712550899081",
15         "reference": "- 9247633578781921",
16         "reference": "- 5342246551415468213",
17         "reference": "- 661916918537838088",
18         "reference": "- 8827271476552282488",
19         "reference": "- 3231885666613585282",
20         "reference": "- 1935145588469227088",
21         "reference": "- 7644834165102104848",
22         "reference": "- 38048618393328046552",
23         "reference": "- 6568197882653653282",
24         "reference": "- 5534921552614203584",
25         "reference": "- 2789187948317329246",
26         "reference": "- 7544527866658929186",
27         "reference": "- 298866519101179505",
28         "reference": "- 8791165399259790786",
29         "reference": "- 851448078383768820",
30         "reference": "- 190678598213733751",
31         "reference": "- 6916881595753881298"
32       ],
33       "guidelines": [
34         "Asset Management",
35         "Interne Audits und Managementbewertung",
36         "Datenklassifikation",
37         "Systemüberwachung",
38         "Release Management",
39         "Risikomanagement",
40         "Behandlung von Sicherheitsvorfällen",
41         "Aktualisierungs- und Änderungsmanagement"
42       ],
43       "records": [
44         {
45           "record": "UDSP Repository",
46           "process": "Erstellung SBOM auf Basis des Repository",
47           "reference": "[Link Repo UDSP](https://[ ])",
48           "guideline_link": "https://[ ] ISMS_RL_Asset_Management.md"
49         },
50         {
51           "record": "Risikoprüfung einer neuen Komponente der UDSP",
52           "process": "Analyse von neuen Komponenten der UDSP",
53           "reference": "[Link Risikoanalyse Komponente](https://[ ])",
54           "guideline_link": "https://[ ] HTAG_ISMS_RL_Risikomanagement.md"
55         },
56         {
57           "record": "Bearbeitung Sicherheitsvorfall",
58           "process": "Meldung durch menschliche Akteure",
59           "reference": "[Link Helpdesk](https://[ ])",
60           "reference": "[Link Support DB](https://[ ])",
61           "reference": "[Issue Board](https://[ ])",
62           "guideline_link": "https://[ ] IS/ HTAG_ISMS_RL_Security_Incident_Management.md"
63         },
64         {
65           "record": "Abstimmung Sicherheitsvorfall",
66           "process": "Meldung durch menschliche Akteure",
67           "reference": "[Link Support DB](https://[ ])",
68           "reference": "[Issue Board](https://[ ])",
69           "guideline_link": "https://[ ] IS/ HTAG_ISMS_RL_Security_Incident_Management.md"
70         }
71       ]
72     }
73   }
74 }

```

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 <i>Inbetriebnahme</i> erreicht.	Inbetriebnahme der Plattforminstanz	Multiplattformmanagement
Inbetriebnahme einer neuen UDSP-Instanz ist abgeschlossen, Status <i>Betrieb</i> 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 <i>core-platform</i> vornehmen, d. h. - neue Features implementieren - originale von HYPERTEGRITY, oder aus Kundeninstallationen von <i>downstream</i> , - 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