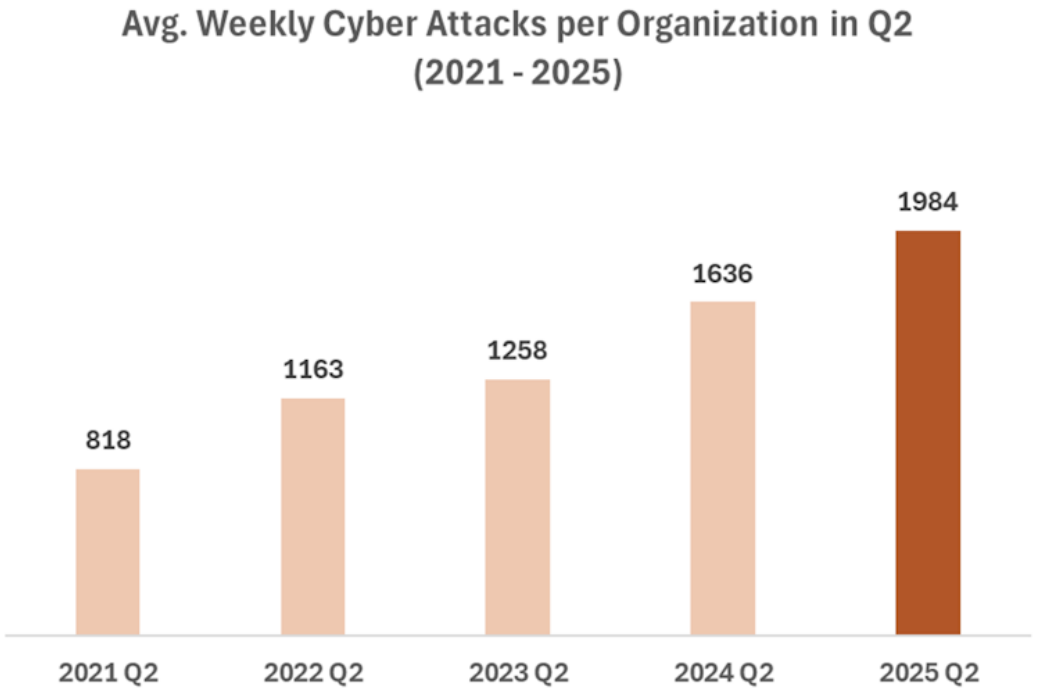

asvin
KI IN DER CYBER THREAT INTELLIGIENCE
Cybersecurity Region Stuttgart Meetup bei IHK Stuttgart
asvin.io

Dramatischer weltweiter Anstieg von Cyberangriffen um 21 % im zweiten Quartal 2025

Europa meldet das höchste Wachstum, Steigerung im Vergleich zum Vorjahr um 22 %



Source: https://cybersecurityasia.net/check-point-uncover-global-surge-cyberattack/

NIS2 Directive verpflichtet Unternehmen zur Implementierung risikobasierter Cybersicherheitsmaßnahmen und zur Reaktion auf Sicherheitsvorfälle für kritische Netzwerke und Systeme.

Herausforderungen der CTI-Berichterstattung

- KMU fehlt der klare Überblick über die Cybersicherheitslandschaft.
- Die Berichterstattung über Cyberbedrohungen (CTI) ist manuell und zeitaufwändig.
- Die Nutzung mehrerer CTI-Quellen birgt Herausforderungen:
  - Unstrukturierte und inkonsistente Informationen.
  - Stark schwankende Datenmengen.
  - Verschiedene Formate (PDF, JSON, XML).
  - Unterschiedliche Übermittlungskanäle (E-Mail, Newsletter, Abonnements).
- Der Kontext der Bedrohungsdaten fehlt oft.
- Die gewonnenen Erkenntnisse sind häufig nicht umsetzbar, was ihren praktischen Nutzen einschränkt.

asvin

CTI-Berichtsphasen

- **Datenerfassung**
  - Rohdaten aus verschiedenen Quellen
- **Normalisierung**
  - Datenbereinigung, -strukturierung und -anreicherung
- **Korrelation**
  - Datenverknüpfung, Mustererkennung, Bedrohungsanalyse
- **Berichterstattung**
  - Weitergabe von handlungsrelevanten Informationen an Stakeholder

asvin

Phase 1: Datenerfassung

- API-basierte Datenerfassung (REST, GraphQL, gRPC)
- Abonnement-Endpunkte/Feeds
- E-Mail-Erfassung
- Scrapping Open-Source Intelligence (OSINT)
- Kommerzielle Bedrohungsfeeds (STIX/TAXII, MISP)
- Darknet-/Underground-Quellen
- Bedrohungs-Sharing-Communities

Phase 2: Normalisierung

- Standardisierung von Datenformaten (STIX, TAXII, JSON, CSV)
- Entfernung von Duplikaten und redundanten Einträgen
- Validierung von Indikatoren für eine Kompromittierung (IOCs)
- Anreicherung von Daten mit Kontextinformationen (Geolokalisierung, Informationen zu Bedrohungsakteuren, Malware-Familien)
- Standardisierung von Zeitstempeln und Ereignisreihenfolge
- Kennzeichnung und Kategorisierung von Daten nach Typ, Schweregrad und Quelle

Phase 3: Korrelation

- Verknüpfung von Indikatoren aus verschiedenen Quellen
- Erkennen von Mustern und Trends bei Bedrohungen
- Zuordnung von Bedrohungen zu Angreifern oder Kampagnen
- Abgleich mit internen Protokollen und Warnmeldungen
- Priorisierung nach Schweregrad, Relevanz oder Auswirkung
- Kontextualisierung von Ereignissen mit historischen Daten

Phase 4: Berichterstattung

- Maßgeschneiderte Berichte für Führungskräfte (strategischer Überblick)
- Maßgeschneiderte Berichte für SOC/Analysten (taktische/umsetzbare Details)
- Maßgeschneiderte Berichte für IT-Teams (operative Anleitungen)
- Automatisierte Dashboards und Warnmeldungen
- Bedrohungsbewertung und -priorisierung in Berichten
- Inklusive empfohlener Maßnahmen und Gegenmaßnahmen
- Benutzerdefinierte Formate (PDF, HTML, JSON, E-Mail-Benachrichtigungen)

asvin

Cyber-Lagebericht –
Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026
Gültigkeit: 24 Stunden
Version: 1.0 | Herausgeber: asvin CTI

Aktuelle Cyber-Risikolage für Stadtwerke

Gesamteinschätzung

Bewertung der aktuellen Lage: **Erhöht**

Trend: **(unverändert gegenüber dem Vortag)**

Executive Summary

Die aktuelle Cyber-Risikolage für Stadtwerke im Energiesektor ist weiterhin als erhöht einzustufen.
Im Fokus stehen anhaltende Ransomware-Aktivitäten sowie gezielte Phishing-Kampagnen, die sich gegen Betreiber kritischer Infrastrukturen richten.

Im Vergleich zum Vortag wurden keine neuen Eskalationen beobachtet. Die Bedrohungslage bleibt jedoch auf einem erhöhten Niveau, insbesondere im Kontext von IT- und OT-nahen Systemen.
Für Stadtwerke ergibt sich daraus aktuell kein akuter Handlungsbedarf, jedoch weiterhin ein erhöhter Bedarf an Aufmerksamkeit und Lagebeobachtung.

Einordnung der aktuellen Lage

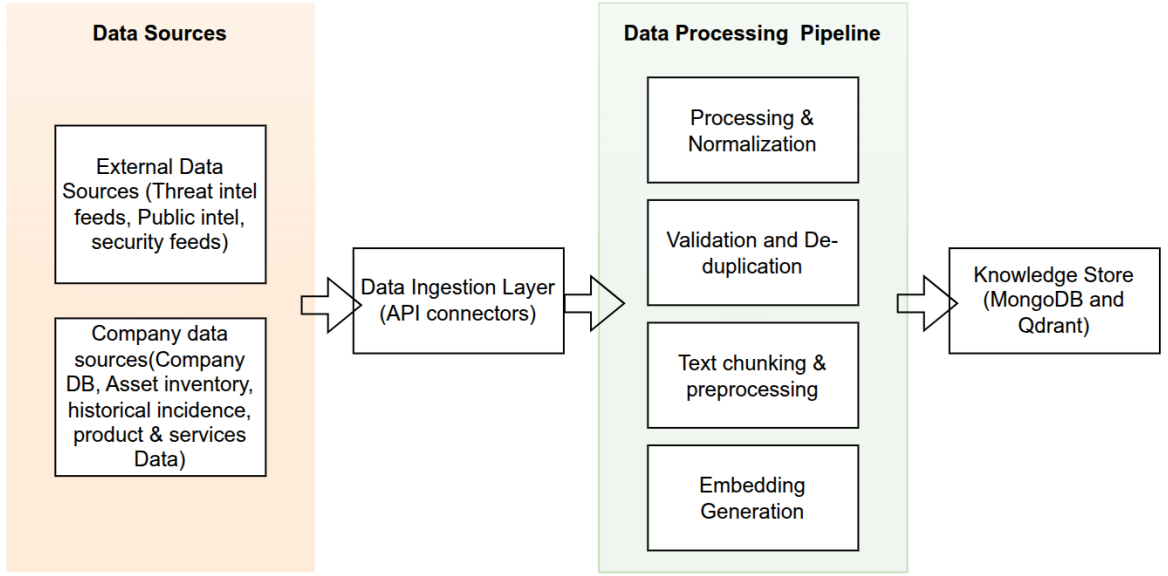
Was bedeutet das konkret für Stadtwerke?

Die beobachteten Aktivitäten zielen vor allem auf Organisationen ab, die eine hohe Betriebsverfügbarkeit sicherstellen müssen und bei denen Ausfälle unmittelbare Auswirkungen auf die Versorgungssicherheit hätten.

Für Stadtwerke bedeutet dies:
- **Cyberangriffe zielen weniger auf Datenabfluss, sondern auf Betriebsunterbrechung**
- **Angriffe erfolgen häufig indirekt über bekannte, alltägliche Angriffsvektoren**
- **Die Bedrohungslage ist nicht neu, aber anhaltend präsent**

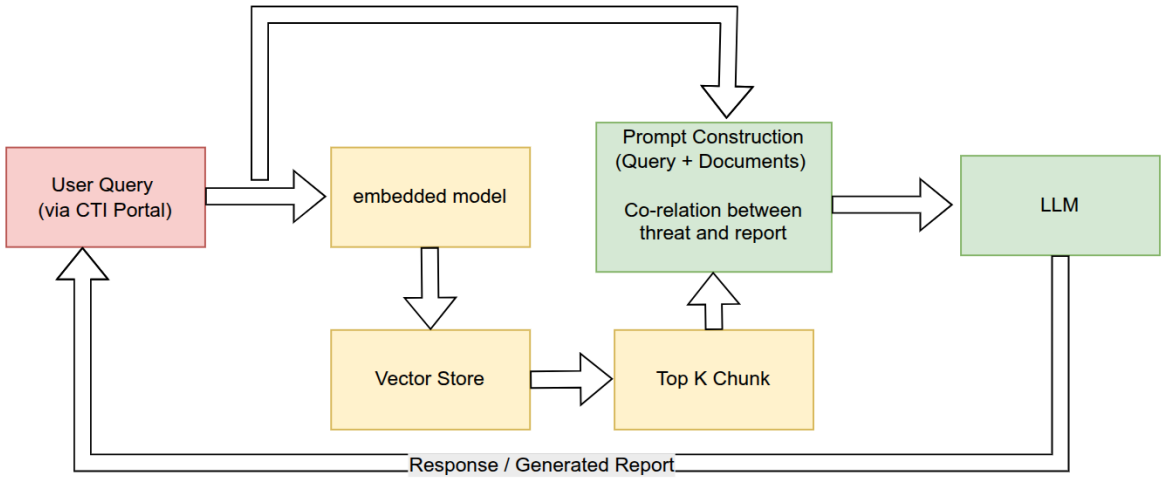
Eine kontinuierliche Einordnung der Lage bleibt daher notwendig, auch bei gleichbleibendem Risikoniveau.

RAG Pipeline



- Wissensdatenbank aufbauen
- Abruf mittels Vektorsuche

Flow 1: Building the Knowledge Base

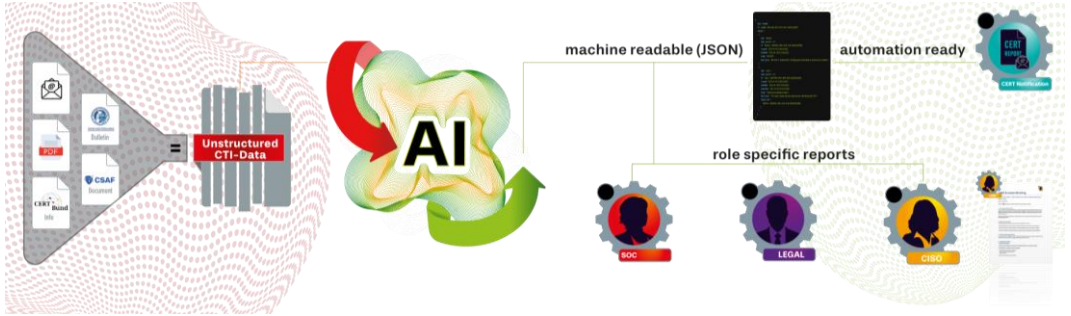


Flow 2: Retrieval from the Knowledge Base

Kontext optimiert Cyber Threat Intelligence (CTI)-Berichte

Die KI-gestützte CTI-Berichterstattung von asvin ermöglicht Automatisierung und Skalierbarkeit für die NIS 2-Konformität in kritischen Infrastrukturen:

- Bedrohungen für die Organisation: z. B. Ransomware- oder Phishing-Angriffe
- Bedrohungen der IT/OT-Infrastruktur durch Schwachstellen
- Bedrohungen durch Lieferanten in der Lieferkette, z. B. Datenlecks



asvin

Cyber-Lagebericht – Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026
Gültigkeit: 24 Stunden
Version: 1.0 | Herausgeber: asvin CTI

Aktuelle Cyber-Risikolage für Stadtwerke

Gesamteinschätzung

Bewertung der aktuellen Lage:

Erhöht

Trend:

(unverändert gegenüber dem Vortag)

Executive Summary

Die aktuelle Cyber-Risikolage für Stadtwerke im Energiesektor ist weiterhin als erhöht einzustufen.
Im Fokus stehen anhaltende Ransomware-Aktivitäten sowie gezielte Phishing-Kampagnen, die sich gegen Betreiber kritischer Infrastrukturen richten.

Im Vergleich zum Vortag wurden keine neuen Eskalationen beobachtet. Die Bedrohungslage bleibt jedoch auf einem erhöhten Niveau, insbesondere im Kontext von IT- und OT-nahen Systemen.
Für Stadtwerke ergibt sich daraus aktuell kein akuter Handlungsbedarf, jedoch weiterhin ein erhöhter Bedarf an Aufmerksamkeit und Lagebeobachtung.

Einordnung der aktuellen Lage

Was bedeutet das konkret für Stadtwerke?

Die beobachteten Aktivitäten zielen vor allem auf Organisationen ab, die eine hohe Betriebsverfügbarkeit sicherstellen müssen und bei denen Ausfälle unmittelbare Auswirkungen auf die Versorgungssicherheit hätten.

Für Stadtwerke bedeutet dies:

- **Cyberangriffe zielen weniger auf Datenabfluss, sondern auf Betriebsunterbrechung**
- **Angriffe erfolgen häufig indirekt über bekannte, alltägliche Angriffsvektoren**
- **Die Bedrohungslage ist nicht neu, aber anhaltend präsent**

Eine kontinuierliche Einordnung der Lage bleibt daher notwendig, auch bei gleichbleibendem Risikoniveau.

asvin

Cyber-Lagebericht – Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026
Gültigkeit: 24 Stunden
Version: 1.0 | Herausgeber: asvin CTI

Zentrale Einflussfaktoren der aktuellen Lage

IT-Systeme	OT / SCADA-nahe Systeme	Lieferketten & Dienstleister
Vermehrte Phishing- und Zugangskampagnen zielen auf Office-IT und VPN-Zugänge ab, um initiale Zugriffe zu erlangen	Keine Hinweise auf neue, gezielte Angriffe. Dennoch bleibt der Energiesektor im Fokus bekannter Akteure.	Abhängigkeiten von externen IT-Dienstleistern bleiben ein relevanter Risikofaktor, insbesondere bei Fernzugriffen.

Relevante Bedrohungsthemen

Bedrohungsthema	Relevanz für Stadtwerke	Betroffene Bereiche
Ransomware-Kampagnen	Hoch	IT / OT
Phishing-Aktivitäten	Mittel	Office-IT
Lieferkettenrisiken	Mittel	Externe Dienstleister

Kurz-Einordnung der Bedrohungsthemen

Ransomware-Kampagnen
Mehrere bekannte Akteursgruppen richten ihre Aktivitäten weiterhin auf den Energiesektor.
Ziel ist primär die Störung des Betriebs durch Verschlüsselung oder Systemblockaden.

Phishing-Aktivitäten
Aktuelle Kampagnen nutzen thematisch angepasste E-Mails, um Zugangsdaten zu erlangen.
Die Angriffe sind technisch wenig komplex, aber weiterhin effektiv.

Lieferkettenrisiken
Zugriffe über externe Dienstleister und Wartungszugänge stellen weiterhin ein strukturelles Risiko dar.

asvin

Cyber-Lagebericht – Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026
Gültigkeit: 24 Stunden
Version: 1.0 | Herausgeber: asvin CTI

Beitrag zur laufenden Risikoanalyse gemäß NIS2

Dieser Bericht unterstützt die laufende Cyber-Risikoanalyse gemäß den Anforderungen der EU-Richtlinie NIS2.

Erfüllte Maßnahmen:
- **Regelmäßige Analyse der Bedrohungslage**
- **Sektorbezogene Bewertung der Relevanz**
- **Dokumentation der Ergebnisse**
- **Nachvollziehbare Historisierung**

Status: Maßnahme laufend erfüllt | Aktualisierung: täglich

Methodik (Kurzfassung)

Die Bewertung basiert auf der Analyse kuratierter externer Cyber-Threat-Intelligence-Quellen mit Fokus auf den Energiesektor.

Die Einordnung erfolgt qualitativ unter Berücksichtigung von:
- **beobachteten Aktivitäten**
- **sektoraler Relevanz**
- **bekannten Angriffsmustern**

Nicht Bestandteil dieser Analyse sind:
- **interne Systemdaten**
- **individuelle Schwachstellenbewertungen**
- **operative Sicherheitsmaßnahmen**

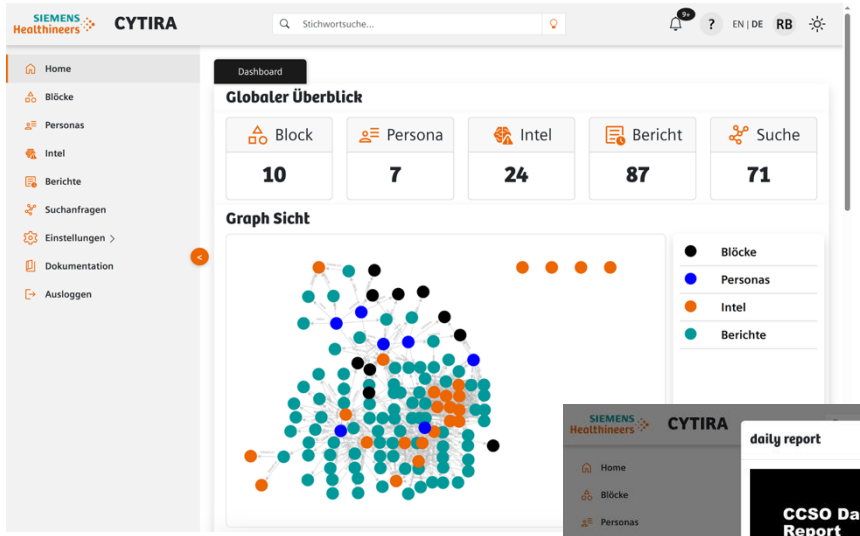
Transparenz & Zweck des Berichts

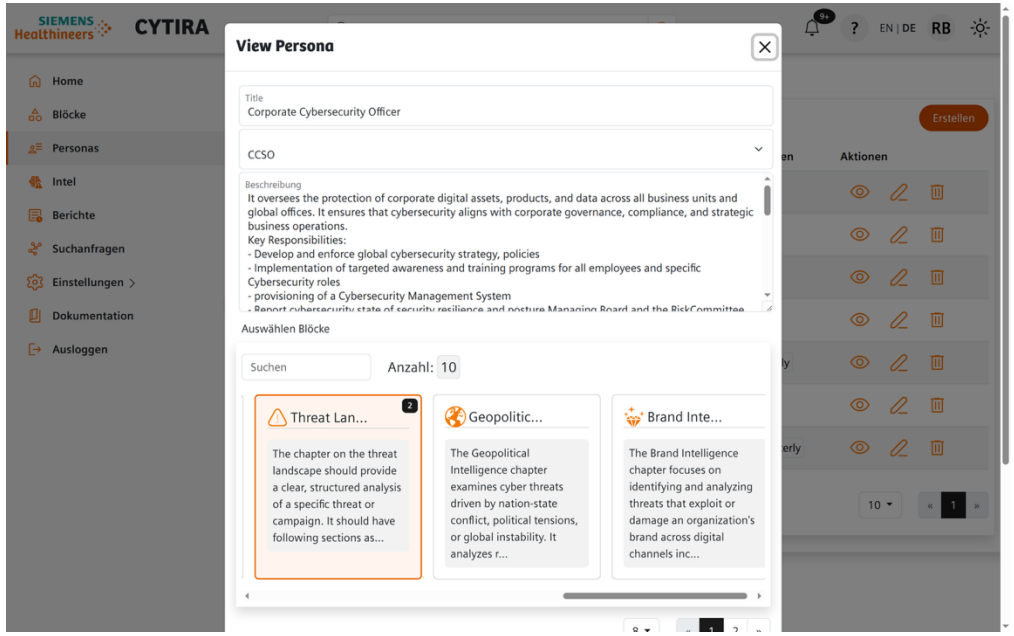
Dieser Bericht dient der regelmäßigen Information über die Cyber-Bedrohungslage im Energiesektor und der Unterstützung der organisatorischen Risikoanalyse.
Er ersetzt keine operativen Sicherheitsmaßnahmen und stellt keine Handlungsempfehlung im Einzelfall dar.

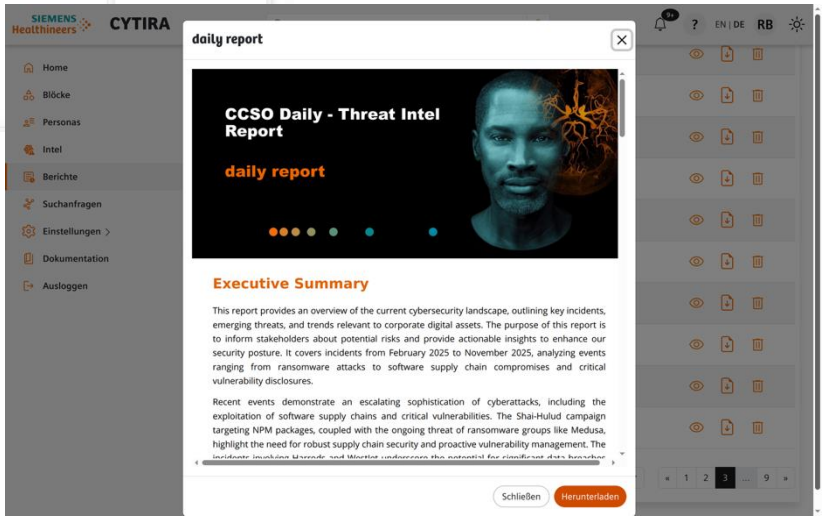
Referenz-ID: ASV-CTI-ENERGY-2026-01-14
Vertraulichkeit: Intern

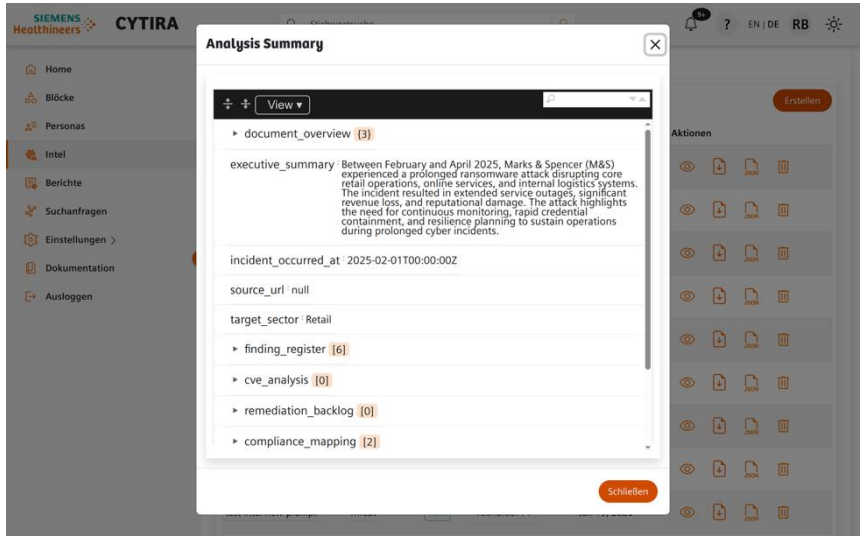
asvin

SHS Case Study









asvin

THANK YOU FOR YOUR TIME

Rohit Bohara
CTO
r.bohara@asvin.io

asvin GmbH
Stuttgart, Germany
www.asvin.io
contact@asvin.io