



EUROPEAN CENTRAL BANK

EUROSYSTEM

Von Compliance zu Cyberresilienz: Operative Umsetzung in einer verschärften Bedrohungslage



8. September 2026

Philipp Amann
Head of Digital Security Services
Division, ECB

Die Europäische Zentralbank (EZB)

Die Europäische Zentralbank und ihre spezielle Rolle

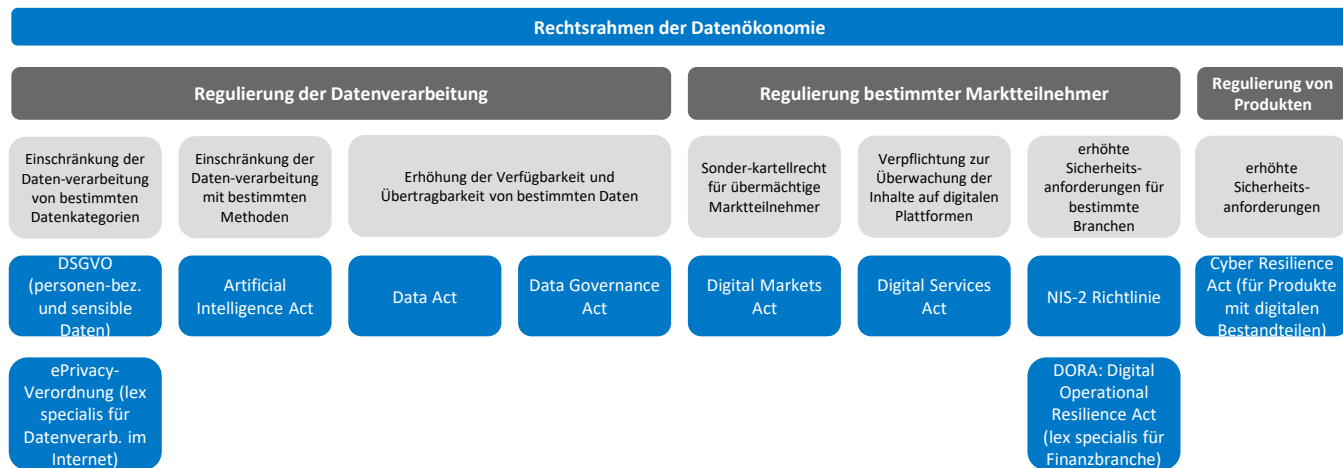
- Geldpolitik, Aufsicht, Zahlungsverkehr, Finanzmarktinfrastrukturen und Abwicklungsprozesse, und Krisenmanagement + Rolle im ESZB Rahmen
- Entscheidungen beruhen auf der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
- Operations hängt von vertrauenswürdigen digitalen Infrastrukturen und sicherer Kommunikation ab
- EZBs Glaubwürdigkeit hängt von der Fähigkeit ab, auch unter Belastung und in Krisen funktionsfähig zu bleiben



➡ Cybersicherheit schafft damit die Voraussetzungen für die Erfüllung des Mandats der EZB

Startpunkt Compliance

Ein Teil des regulatorischen Rahmens



Compliance ist notwendig, aber nicht ausreichend

- NIS2, DORA*, ISO 27001 und weitere Vorgaben schaffen Orientierung, Mindeststandards und Nachweisbarkeit
- Der Fehler beginnt dort, wo Compliance als reine Checkliste verstanden wird
- Eine erfüllte Kontrolle ist kein Selbstzweck; sie muss ein reales Risiko reduzieren, eine Fähigkeit stärken oder eine Entscheidung ermöglichen



➡ Compliance sollte nie zu einer „tick boxing exercise“ werden

* DORA ist nicht auf die EZB anwendbar sondern EU Verordnung 2023/2841 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

Gute Cyberhygiene macht Compliance (fast) zum Nebeneffekt

- Wer grundlegende Sicherheitsmaßnahmen konsequent umsetzt, erfüllt viele regulatorische Anforderungen fast automatisch
- Der Schwerpunkt sollte nicht auf dem Nachweis beginnen, sondern auf der Fähigkeit und Sicherheit im Betrieb



 Ein großer Teil des Nachweises kommt mit der operativen Sicherheit und Cyberhygiene

Der operative Kern: Priorisieren statt alles gleichzeitig wollen

- Regulatorische Anforderungen sind typischerweise breit, operative Ressourcen sind begrenzt
- Pragmatische Umsetzung bedeutet: kritische Services, kritische Daten und kritische Abhängigkeiten zuerst sowie eine belastbare Definition des Anwendungsbereiches haben
- Risikoentscheidungen dokumentieren, Lieferketten verstehen, Vorfälle melden können, kritische Prozesse wiederherstellen, Management-Verantwortung verankern
- Nicht jede Maßnahme hat denselben Resilienzwert und mitigierte dieselbe Risikostufe



 Cyberresilienz entsteht durch risikobasierte Priorisierung, nicht durch Vollständigkeitsrhetorik

Keine Organisation ist eine Insel

- Die operative Umsetzung gelingt nicht isoliert in einer Sicherheitsabteilung
- Konstruktiver Austausch mit Behörden, Prüfern, Industriepartnern, IT-Betrieb, Fachbereichen und Lieferanten hilft bei der Umsetzung und reduziert Unsicherheit
- Gute Aufsicht und gute Umsetzung brauchen dieselbe Sprache, idealerweise Risiko-basiert



➡ Cyberresilienz ist auch ein Koordinationsproblem, nicht nur ein Kontrollproblem

Derzeitige und künftige Herausforderungen

Angriffe und Verteidigung 'at the speed of AI'

Angriffe und Verteidigung 'at the speed of AI' (1/4)

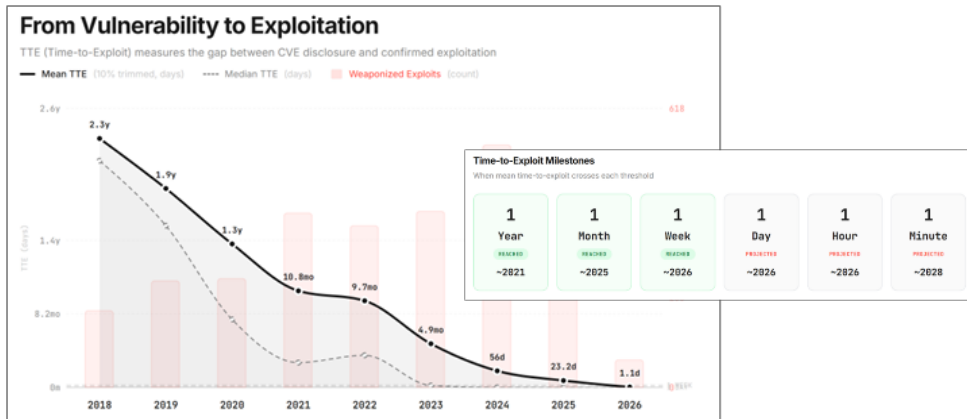
Künstliche Intelligenz beschleunigt sowohl Cyberangriffe als auch Cyberabwehr. Schnellere Priorisierung und stärkere Automatisierung sind erforderlich, um Exponierung zu reduzieren, Eindämmung zu verbessern, Abhängigkeiten von Dritten besser zu steuern und Schwachstellen zu beheben.

Fakten und Herausforderungen:

- Klare Signale, dass Frontier-KI-Modelle die Cybersicherheit wesentlich verändern
- KI-Modelle verkürzen die Zeit zwischen Entdeckung und Ausnutzung von Schwachstellen
- Die Lücke zwischen Schwachstellenidentifikation und Behebung muss deutlich verkleinert werden
- Grundlegende Sicherheitskontrollen müssen gestärkt werden, insbesondere wenn Patching nicht möglich ist
- Enge interne und externe Koordinierung bleibt unerlässlich

Schwerpunkte:

- Eindämmung und Priorisierung von Patching
- Abhängigkeiten zu Dritten und Open-Source Software
- Erhöhte Sichtbarkeit und Reduzierung der Angriffsfläche
- Einsatz künstlicher Intelligenz in Cyberabwehr und Softwareentwicklung



Zentrale Maßnahmen:

- Einführung kontextbasierter Priorisierung von Schwachstellen
- Festlegung klarer Kriterien für Behebung, einschließlich Eindämmung und Patching
- Verbessertes Management der Angriffsfläche und von externen Abhängigkeiten

Angriffe und Verteidigung 'at the speed of AI' (2/4)

Neue KI-Modelle verkürzen den Zeitraum zwischen Schwachstellenentdeckung und Ausnutzung und erhöhen operationelle Risiken sowie Lieferkettenrisiken, wenn Patching und Eindämmung nicht Schritt halten.

Risikoimplikationen

1 Schnellere Entdeckung

KI macht exponierte Dienste und verwundbare Abhängigkeiten für Angreifer schneller sichtbar

2 Verbessertes Social Engineering

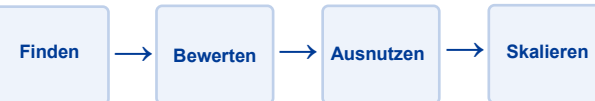
Phishing, Social Engineering und Deepfake-gestützter Betrug werden überzeugender und zielgerichteter

3 Schnellere Folgehandlungen

Nach initialem Zugriff kann KI schnellen Missbrauch von Zugangsdaten, laterale Bewegung, und Datenexfiltration unterstützen

4 Systemische Exponierung

Ein kompromittierter Lieferant, ein Update oder eine gemeinsam genutzte Komponente kann gleichzeitige Risiken für viele Institutionen schaffen



Angriffe und Verteidigung 'at the speed of AI' (3/4)

KI kann helfen, schneller zu triagieren, besser zu priorisieren, Behebung und Patching zu unterstützen und die Incident Response zu verbessern – bei klarer menschlicher Verantwortung.

Praktische Chancen in der Verteidigung

1 Triage und Priorisierung

Automatisierte Triage kann Alert Fatigue reduzieren und Analysten helfen, sich auf die relevantesten Schwachstellen und Vorfälle zu konzentrieren

2 Validierung und Patching

KI-gestützte Validierung, Code Review und Patch-Erstellung können Behebungsrückstände verkürzen und sichere Änderungen verbessern

3 Reaktion und Eindämmung

Bei Vorfällen kann KI Untersuchung, Anreicherung und schnellere Isolierung mutmaßlich kompromittierter Systeme oder Konten unterstützen

4 Höhere Resilienz im Zeitverlauf

Die Einbettung von KI in Patching, Abhängigkeitsmanagement und Code-Qualitätsprozesse sollte die Software-Resilienz insgesamt verbessern



KI kann schnellere Erkennung, schnelleres Patching und bessere Eindämmung unterstützen

Triage



Priorisieren



Patchen



Eindämmen

➡ ,It's not a scanner, folks!'

Angriffe und Verteidigung 'at the speed of AI' (4/4)

- KI und Frontier KI Modelle als möglicher Kipppunkt
- Das Risiko liegt nicht nur in KI-Modellen selbst, sondern in deren Integration in Prozesse, Datenflüsse und Entscheidungswege
- Organisationen brauchen KI-Governance und KI-gestützte Verteidigung, aber mit klaren Grenzen und menschlicher Verantwortung



➡ Wenn Angriffe mit KI-Geschwindigkeit erfolgen, kann Verteidigung nicht manuell bleiben

Post-Quanten-Kryptografie (PQC) Readiness

Q-Day vs. Y2K – nützliche Analogie mit Einschränkungen

Die Y2K-Analogie ist nützlich, aber Q-Day ist schwieriger: Die Frist ist ungewiss, was zu 'Trägheit' führen kann, und die Auswirkungen können anfangs unbemerkbar sein und rückwirkend eintreten

Dimension	Y2K	Q-Day
Ermittlung	Systematische Code-Analyse und Behebung	Systematische Erfassung und Migration kryptografischer Assets
Frist	Fest (01.01.2000)	Gleitend – aber enger werdend
Ausfallmodus	Systemstörung oder -ausfall – sichtbar	Unbemerkbare, rückwirkende Datenkompromittierung
Risikoträger	Primär interne Systeme und Abläufe	Gesamtes Ökosystem

Der oft falsch erinnerte Teil: Y2K verlief ruhig, weil die Umsetzung rechtzeitig abgeschlossen wurden.

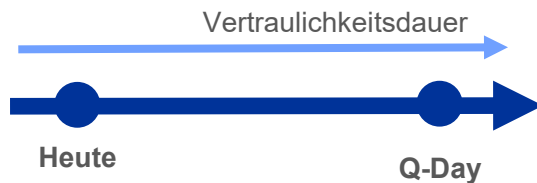
Der schwierigere Teil: Eine gleitende Frist begünstigt institutionelle Trägheit. Für langfristig vertrauliche Daten baut sich das Risiko bereits heute auf.

Harvest now, decrypt later – die Bedrohung hat bereits begonnen

Langlebige Geheimnisse können heute gesammelt und später kompromittiert werden, wenn der Schutz der Vertraulichkeit nicht frühzeitig auf PQC umgestellt wird.

Harvest now, decrypt later (HNDL)

Angreifer sammeln heute verschlüsselte langlebige Daten und entschlüsseln sie später, sobald verwundbare Public-Key-Kryptografie gebrochen werden kann.



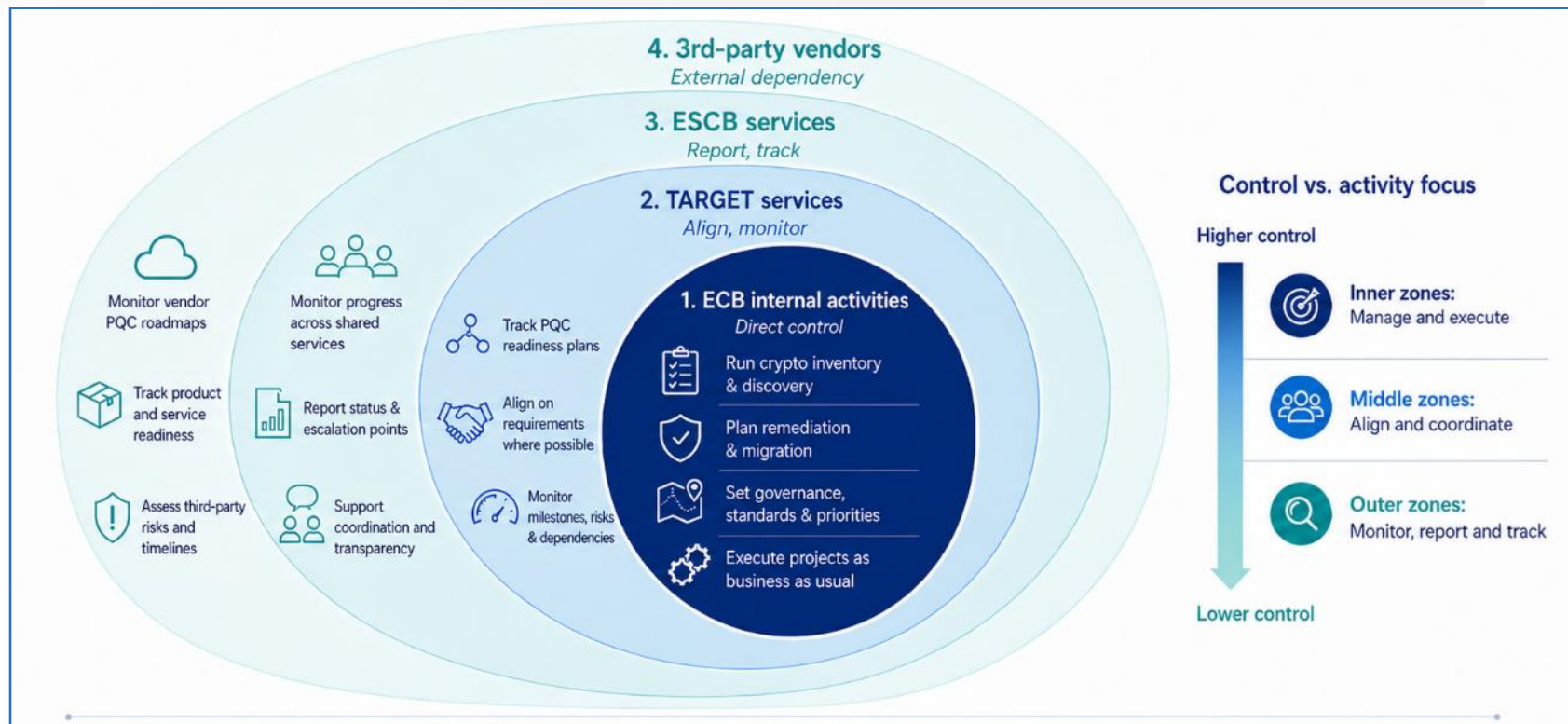
Diese Exponierung besteht strukturell – unabhängig vom genauen Q-Day-Datum

10+ Jahre

Vertraulichkeitsbedarf:
Aufsichtsbewertungen, geldpolitische
Beratungen, bilaterale Kommunikation

Moscas Theorem: Wenn Vertraulichkeitsdauer + Migrationszeit > Zeit bis Q-Day, sind die Informationen bereits heute gefährdet

PQC Readiness – eine ganzheitliche Sicht



Überblick über PQC-Aktivitäten – europäische Organisationen und Regierungen

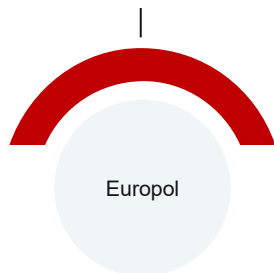
- Das BSI fordert eine beschleunigte Umstellung auf PQC mit Fokus auf „store now, decrypt later“-Angriffe und empfiehlt den Schutz sensibler Anwendungsfälle bis Ende 2030
- Fraunhofer AISEC bietet ein Kompetenzzentrum für PQC zur Unterstützung von Organisationen

SQPRIM-Projekt: Entwicklung neuer kryptografischer PQC-Primitive mit Fokus auf digitale Entsprechungen biometrischer Identifikatoren

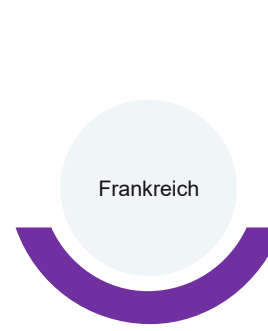
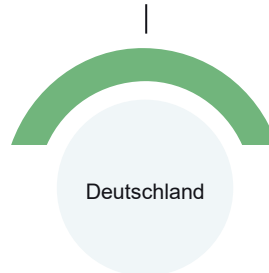
Quantum Safe Financial Forum (QSFF)



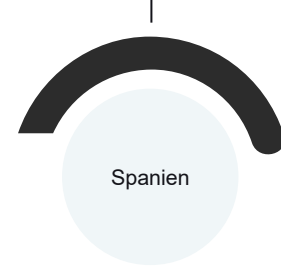
- Initiative European Quantum Communication Infrastructure (EuroQCI)
- Empfehlung vom April 2024 für einen harmonisierten Ansatz zu PQC mit Schwerpunkt auf dem Schutz digitaler Infrastrukturen und Dienste im Quantenzeitalter



EAGLE-1-Mission: Europas erstes weltraumgestütztes System für Quantum Key Distribution (QKD) mit dem Ziel, ein sicheres Quantenkommunikationsnetz in Europa aufzubauen



RESQUE-Konsortium: Zusammenarbeit von sechs französischen Cybereinrichtungen, darunter Thales und ANSSI, zur Entwicklung von PQC-Lösungen wie hybriden VPNs und leistungsfähigen Hardware-Sicherheitsmodulen



Roadmap zur PQC Readiness

HEUTE

2026

2030

Q-DAY



*Frist der Europäischen
Kommission für die
Planung der Umstellung*



*Frist der Europäischen
Kommission für die Umstellung
kritischer Infrastrukturen*

**Kryptografie-Inventar
aufbauen**

**Daten und Systeme
priorisieren und
Migrationsstrategie sowie
Roadmap festlegen**

**Anforderungen in
Sicherheitsstandards und
Beschaffung aktualisieren**

**Kompetenzen konsolidieren
und ausbauen, um Analyse
und Unterstützung zu
ermöglichen**

Kritische Dienste migrieren

**Abhängigkeiten von
Dritten**

Upgrades oder
Ersatz planen

**Eigenentwickelte
Anwendungen**

Kryptoagile
Architekturen
umsetzen

Altsysteme

Außer Betrieb
nehmen oder
refaktorisieren

Zielpunkt - Digitale Souveränität und Resilienz

Digitale Souveränität ohne digitale Isolation

- Souveränität bedeutet die Fähigkeit, ausreichend Kontrolle und Handlungsfähigkeit zu behalten
- Sie bedeutet nicht, globale Technologie abzulehnen oder Innovation zu verlangsamen
- Sie bedeutet ua offene Standards, starke Governance und glaubwürdige Ausstiegsoptionen zu nutzen
- Sie bedeutet, europäische Fähigkeiten dort zu stärken, wo sie am wichtigsten sind



Zentrale Fähigkeiten für Cyberresilienz (1/2)

- Abhängigkeiten verstehen: kritische Dienste, Datenflüsse, Lieferanten und Konzentrationsrisiken erfassen
- Vermeidbare Abhängigkeiten reduzieren: Wahlmöglichkeiten, Portabilität und Austauschbarkeit erhalten
- Für eingeschränkten Betrieb auslegen: Fallbacks, Isolation, Wiederherstellung und Krisenmodi vorbereiten
- Resilienz des Ökosystems stärken: mit Organisationen, Infrastrukturen und EU-Partnern koordinieren
- Auf strategische Unsicherheit vorbereiten: Szenarien üben, in denen zentrale Annahmen nicht mehr gelten



Zentrale Fähigkeiten für Cyberresilienz (2/2)

- Eine Organisation ist nicht resilient, weil sie ein Framework besitzt, sondern weil sie auch unter Druck handlungsfähig bleibt
- Messgrößen sollten operative Fähigkeiten abbilden
- Tabletop-Übungen, Krisenentscheidungen, technische Tests und Lessons Learned als Beweis der Wirksamkeit



➡ Was nicht gemessen, getestet und geübt wird, ist im Ernstfall nur eine Annahme

Herausforderung

- Geopolitisches Risiko und Konzentrationsrisiken

PRESS RELEASE | Apr 17, 2026 | Brussels | 2 min read

Commission awards €180 million tender for sovereign cloud to four European providers

PAGE CONTENTS

Top

Related media

Related topics

Print friendly pdf

Contacts for media

The European Commission is strengthening the European Union's digital sovereignty by awarding a tender that allows EU institutions, bodies, offices and agencies (Union entities) to procure sovereign cloud services for up to €180 million over 6 years.

The four awarded providers are European companies: **Post Telecom** with its partners **CleverCloud** and **OVHcloud**, **STACKIT**, **Scaleway**, and finally **Proximus**, which partners with **S3NS** (a joint venture of **Thales** and **Google Cloud**), **Clarence** and **Mistral**.

This tender supports the Commission's broader efforts to enhance its own sovereignty, reinforcing strategic control across key technologies and infrastructure.

The awarded providers were selected based on their alignment with the Commission's [Cloud Sovereignty Framework](#), which measures sovereignty across eight objectives.

- Geopolitische Risiken und Konzentrationsrisiken reduzieren
- Resilienterer und unabhängiger IT-Betrieb
- Beitrag zur europäischen Agenda für digitale Souveränität

Lieferketten-



Von Compliance zu Cyberresilienz

Cybersicherheit bedeutet nicht mehr nur, Systeme zu verteidigen, sie bedeutet, Vertrauen zu schützen, Unabhängigkeit zu bewahren und zum Aufbau einer resilienten europäischen digitalen Grundlage beizutragen.

- Im digitalen Zeitalter hängt Vertrauen von Resilienz ab
- In einer fragmentierten Welt werden ungesteuerte Abhängigkeiten zu einer strategischen Verwundbarkeit
- Compliance gibt den Rahmen, Cyberhygiene schafft die Basis, Priorisierung macht Umsetzung realistisch
- Messung und Übungen machen Resilienz glaubwürdig, Zusammenarbeit macht sie skalierbar



➡ Das Ziel ist nicht, eine Prüfung zu bestehen. Das Ziel ist, im Ernstfall (gemeinsam) weiter handlungsfähig zu bleiben

Cybersecurity team
worried about losing jobs to AI

AI solution



Cybersecurity team
worried about losing jobs to AI

AI solution



Vielen Dank!
