q.beyond

vodafone business

solution factory

NIS 2 Compliance & Cyber Security:

Ihr Weg zu maximalem Schutz

Christian Manivong I q.beyond AG


vodafone
business
solution factory

Agenda

01 Einführung und Übersicht

02 Betroffenheit in Deutschland

03 Anforderungen und Maßnahmen

04 Sanktionen und Bußgelder

05 Beyond Cyber Security

01

Einführung und Übersicht

NIS-2 „Spielfeld und Spielregel “

Hintergrund und Zielsetzung für NIS-2

Hintergrund:

Die deutsche Wirtschaft ist auf funktionierende und resiliente Infrastruktur im physischen und als auch digitalen Bereich angewiesen.

Die IT-Sicherheitslage hat sich, gem. Einschätzung des BSI (Bericht aus 2023) insgesamt zugespitzt.

Bedeutung von NIS2:

- ✓ **EU-weite Sicherheitsanforderungen** für Netz- und Informationssysteme
- ✓ **Unternehmen und öffentliche Einrichtungen sind verpflichtet, angemessene Maßnahmen** zum Schutz ihrer Netzwerke und Daten zu ergreifen
- ✓ **Mindestniveau für Cybersicherheit innerhalb der EU erreichen**

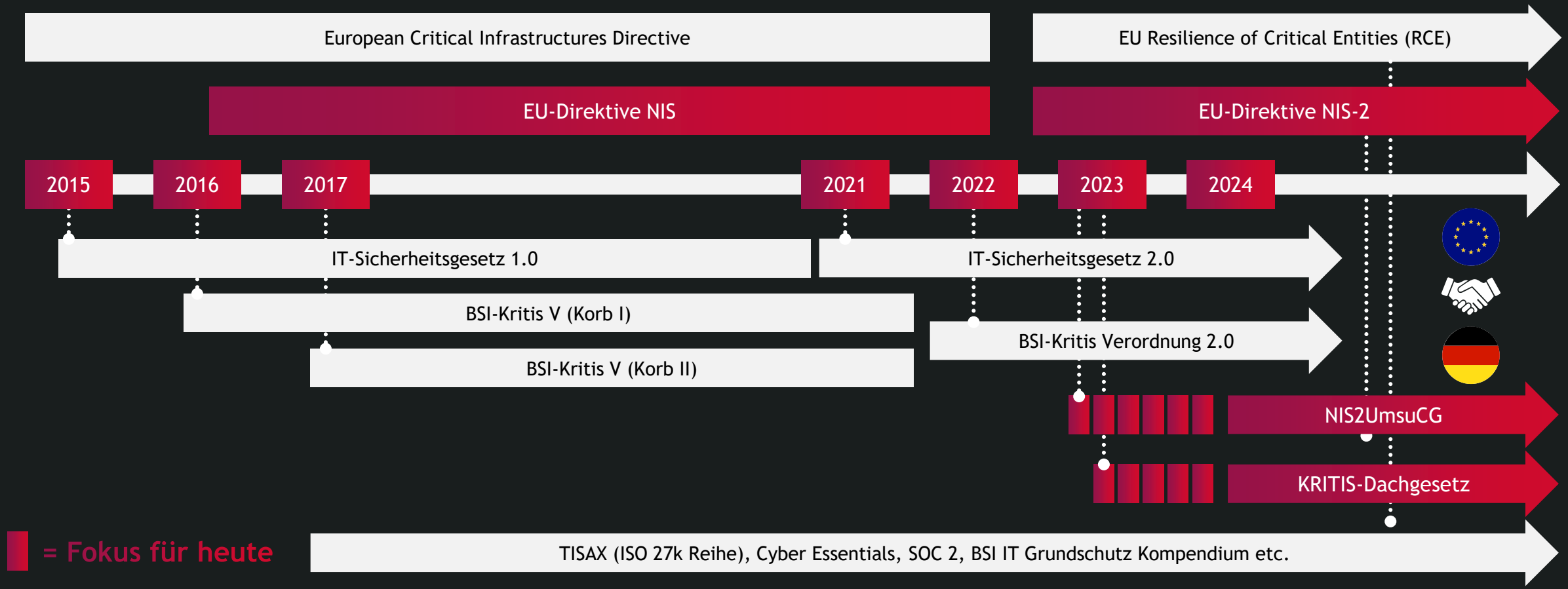
Hauptziele:

- ✓ **Erhöhung der Cybersicherheitsstandards:** Einführung verbindlicher Maßnahmen zur Verbesserung der Cybersicherheit
- ✓ **Schutz kritischer Infrastrukturen:** Sicherstellung der Kontinuität wichtiger Dienste durch stärkere Sicherheitsvorkehrungen
- ✓ **Stärkung der Verantwortlichkeit:** Geschäftsleitungen sind verpflichtet, Cybersicherheitsstrategien zu implementieren und zu überwachen

Auswirkung:

- ✓ **Anwendungsbereich:** Betrifft mehr Branchen, einschließlich kritischer Infrastrukturen und digitaler Dienstleister
- ✓ **Verstärkte Meldepflichten:** Unternehmen müssen Sicherheitsvorfälle frühzeitig und präzise melden
- ✓ **Erhöhte Sanktionen:** Bei Nichteinhaltung drohen erhebliche Geldbußen und persönliche Haftung der Geschäftsleitung

NIS2 basiert auf europäischen und nationalen Vorschriften sowie Standards und bewährten Verfahren



Das NIS2 Umsetzungsgesetz überführt die EU-weiten Mindest-standards für Cybersicherheit in die deutsche Regulierung

bis 10/2024

ab 10/2024*

EU-Direktive NIS2

Umsetzung durch

NIS2UmsuCG

Die EU-Direktive NIS2 stellt den neuen Rahmen für die Sicherheitsstrategie der Europäischen Union dar.

- Zweck: Europäische Richtlinie zur Erhöhung der Cybersicherheit.
- Ziel: Harmonisierung der Cybersicherheitsanforderungen und Erhöhung der Resilienz

Das NIS2-Umsetzungsgesetz ist die nationale Antwort auf die Anforderungen der EU NIS2-Richtlinie.

- Zweck: Nationales Gesetz zur Umsetzung der EU-Direktive NIS2 in deutsches Recht.
- Ziel: Anpassung der EU-Vorgaben an die nationalen Gegebenheiten.

* ursprüngicher Termin

02

Betroffenheit in Deutschland

NIS2 reguliert neben KRITIS-Betreibern noch weitere Unternehmen aus bestimmten Sektoren

Direkte Betroffenheit*
(ca. 30 Tsd. deutsche Unternehmen)

Besonders wichtige Einrichtungen nach Größe des Unternehmens in Sektoren Anlage 1

- Unternehmen ab 250 Mitarbeitern oder
- Unternehmen über 50 Mio. EUR Umsatz und Bilanz über 43 Mio. EUR

Wichtige Einrichtungen nach Größe des Unternehmens in Sektoren aus Anlage 1 und 2

- Unternehmen ab 50 Mitarbeitern oder
- Unternehmen über 10 Mio. EUR Umsatz und Bilanz über 10 Mio. EUR

Betreiber kritischer Anlagen (KRITIS-Betreiber) stellen weiterhin **mit KRITIS-Methodik die Betroffenheit einzelner Anlagen fest, auch im KRITIS-Dachgesetz**

- KRITIS-Anlage über Schwellenwert, in der Regel ≥ 500 Tsd. versorgte Personen

Indirekte Betroffenheit
(Anzahl unbestimmt)

Lieferkettenpflicht:

Viele Unternehmen werden indirekt über die Lieferkette betroffen sein, da §30, Absatz 2, Punkt 4 zur Lieferkettensicherheit verpflichtet und die NIS-2-Anforderungen wahrscheinlich über Verträge an einige Lieferanten weitergegeben wurden.

Die betroffenen Sektoren lassen sich zu unterschiedlichen Betreibergruppen zuordnen

03

Anforderungen und Maßnahmen

01

Hauptteil

Risikomanagement

Das Risikomanagement umfasst gemäß §30 und §31 Sicherheitsmaßnahmen, um Störungen der Informationssicherheit zu vermeiden. Es existieren diverse Ausschlüsse und Sonderregeln für das Risikomanagement.

02 **Meldepflichten**

Sicherheitsvorfälle müssen gemäß §32 frühzeitig (spätestens nach 24h und erneut nach 72h) und präzise (Bericht spätestens nach einem Monat) an die zuständigen Behörden gemeldet werden.

03 **Pflichten für die Geschäftsführung**

Die Geschäftsleitung trägt gemäß §38 die Hauptverantwortung für die Implementierung und Überwachung von Cybersicherheitsmaßnahmen.

04 **Unterrichtungs-pflichten**

Unternehmen müssen die Empfänger ihrer Dienste im Fall eines erheblichen Sicherheitsvorfalls, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte, unterrichten (§35).

05 **Nachweispflichten**

Unternehmen müssen regelmäßig durch Audits oder Zertifizierungen nachweisen, dass sie die Sicherheitsanforderungen erfüllen, gemäß §39.

06 **Registrierungspflichten**

Einrichtungen müssen sich gemäß §33 und §34 bei den zuständigen Behörden registrieren (Frist: 3 Monate).

Im Risikomanagement wird die Implementierung von zehn organisatorischen und technischen Maßnahmen gefordert

- Informationssicherheit
- Incident Management
- Business Continuity Management
- Lieferantenmanagement
- Wartung und Betrieb
- Audit
- Schulung
- Verschlüsselung
- Access Management
- Identity Management

Im Risikomanagement wird die Implementierung von zehn organisatorischen und technischen Maßnahmen gefordert

Erheblicher Sicherheitsvorfall

Interne Meldestelle

< 24 Std.	▪ Verdacht rechtswidrige Handlungen ▪ Grenzüberschreitende Auswirkungen ▪ Zusatz für KRITS-Betreiber: Art der betroffenen Anlage, kritische DL, Auswirkungen auf kritische DL
72 Std.	▪ Bestätigung / Aktualisierung Erstmeldung ▪ Erste Bewertung mit Schweregrad, Auswirkungen, Kompromittierungsindikatoren
Zwischen-meldungen	▪ Auf Ersuchen des BSI ▪ Relevante Statusaktualisierungen
1 Monat	▪ Ausführliche Beschreibung mit Schweregrad, Auswirkungen ▪ Art der Bedrohung / Ursache ▪ Abhilfemaßnahmen ▪ Ggf. grenzüberschreitende Auswirkungen ▪ Dauert der Sicherheitsvorfall noch an, wird Fortschrittsmeldung vorgelegt

Bundesamt für Sicherheit in der Informationstechnik

Meldestelle vom BSI

04

Sanktionen und Bußgelder

Die Nicht-Einhaltung der Vorgaben aus dem NIS2-Umsetzungsgesetz kann zu hohen Sanktionen führen

	von	bis
KRITIS-Betreiber Besonders wichtige Einrichtungen	100.000 EUR	10 Mio. EUR oder 2% globaler Umsatz
Wichtige Einrichtungen	100.000 EUR	7 Mio. EUR oder 1,4% globaler Umsatz
Allgemeine Tatbestände	100.000 EUR	2 Mio. EUR

In bestimmten Fällen kann eine persönliche Haftung der Geschäftsführung in Betracht kommen, insbesondere bei Vorsatz oder grober Fahrlässigkeit

05

Beyond Cyber Security

Leistungsspektrum Cyber Security

Advise

Cyber Security Strategy, GRC

- Advisory
  - Strategy & Direction
- Analysis & Requirements
  - Compliance
  - Risk
  - Gov.

Plan & Build

Cyber Security Project & Consulting

Plan / Design

Architecture

- Organizational
- Process & Procedures
- Guidelines & Authorization

Concept & Product

- Techincal Concept
- Tool Selection
- PoC

Build

- Install & Configure
- Integrate & Implement

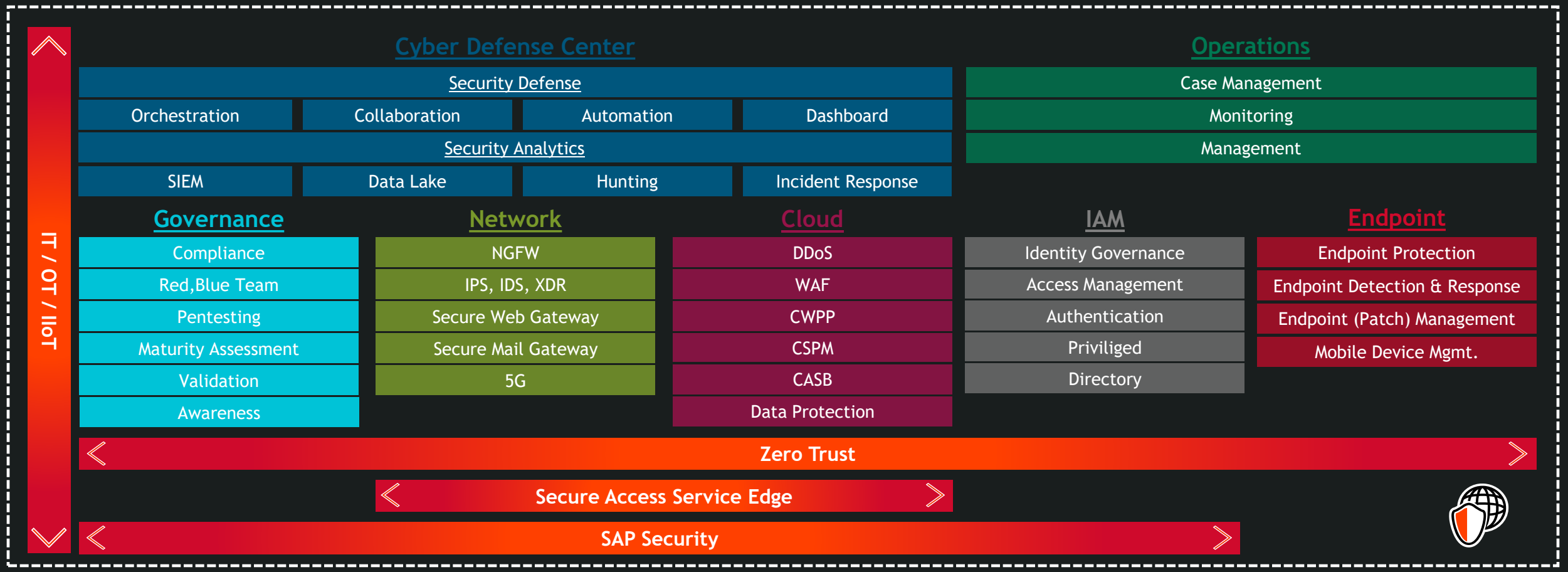
Run

Operate

Run

- Managed Security Services
- Change

Digital Shield: Die Buliding Blocks für maximale Cyber Sicherheit



one.secure customer packages

Basic

SIEM	Vulnerability Management	Managed Endpoint & Identity Protection
Plan Phase (Requirement Analysis, Architecture and Solution Design, Role and Process Definition)		
Build Phase (Technology Deployment, Process Development and Automation, Testing and Pilot Phase, Training and Documentation)		
Run Phase (Service Operations, Customer Communication and Reporting, Proactive Improvement, Scaling and Expansion)		
S M L	S M L Add-On: Remediation tracking Add-On: Risk based reporting Add-On: Asset detection	EDR & Next-Gen Antivirus Add-On: Firewall Management Add-On: Device Control Add-On: Identity Threat Protection

XaaS / Managed Security Services

CDC

S
M
L

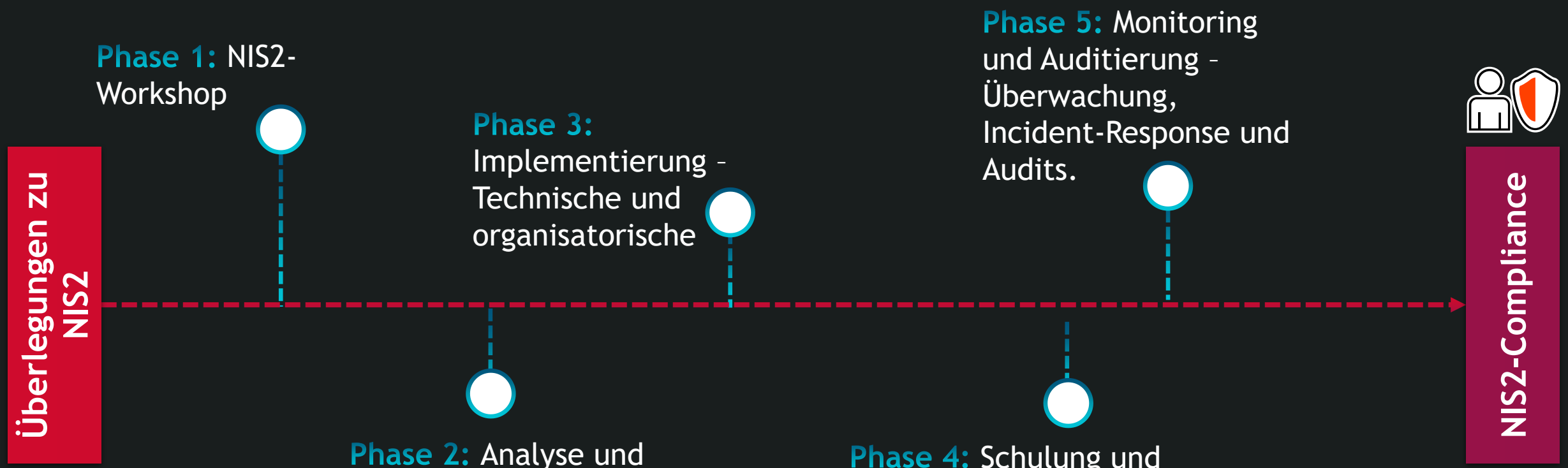
Cyber Defense Center:

Monitoring, Detection, Response, Proactive Prevention, Threat Intelligence Integration, Incident Forensics and Analysis, Patch Management, Threat Hunting

splunk> a CISCO company · Microsoft Sentinel · RAPID7 · Microsoft Defender · CROWDSTRIKE

Möglicher Weg zur NIS2-Compliance

Wir holen unsere Kunden individuell dort ab, wo sie stehen - ganz gleich, ob sie gerade erst beginnen oder bereits erste Schritte unternommen haben.



vodafone business

solution factory

Excellence in all we do.

Zeit für Feedback oder Fragen!

q.beyond