



q.beyond



vodafone  
business

solution factory



# NIS 2 Compliance & Cyber Security: Ihr Weg zu maximalem Schutz



# 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

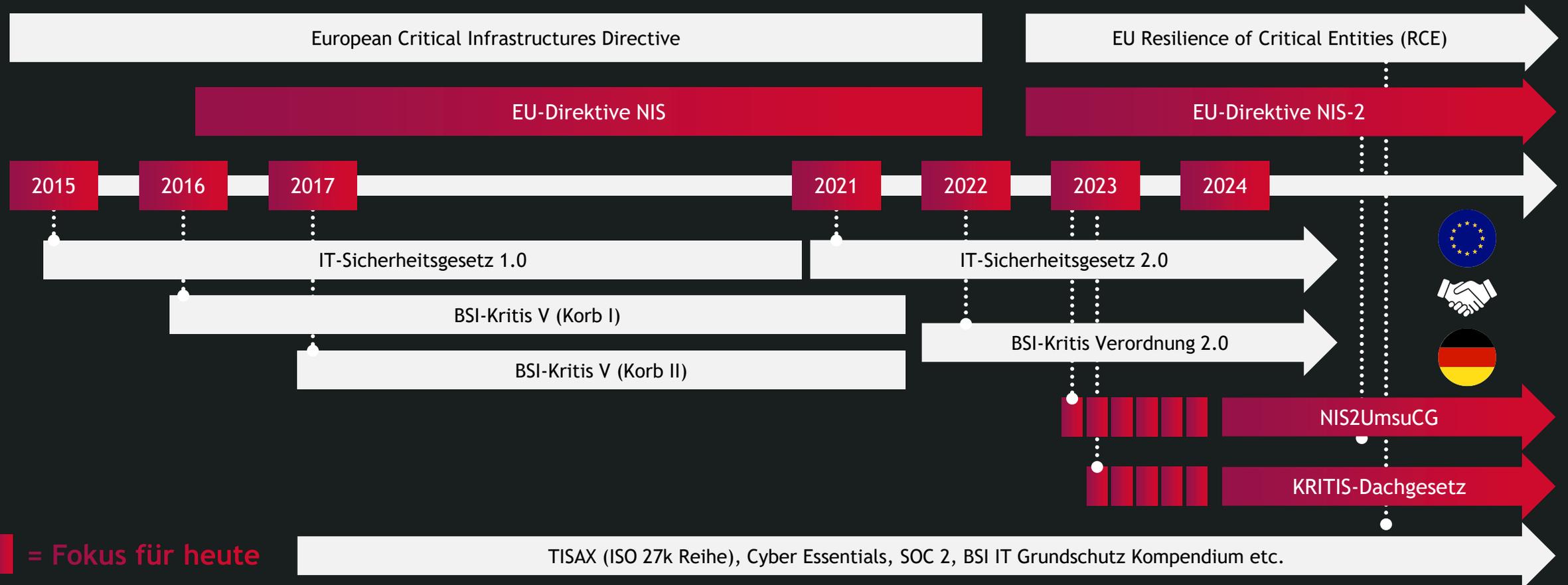
### Hauptziele:

- ✓ **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 Mindeststandards für Cybersicherheit in die deutsche Regulierung

bis 10/2024



EU-Direktive NIS2

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

ab 10/2024\*



NIS2UmsuCG

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.

Umsetzung  
durch

\* ursprünglicher 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  $\geq 500$  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

Betreiber kritischer Anlagen

2.000

KRITIS-Betreiber

Besonders wichtige Einrichtungen

6.250

Großunternehmen  
+ Sonderfälle

Wichtige Einrichtungen

21.600

Mittlere Unternehmen

Großunternehmen  
Mittlere Unternehmen

Energie

Transport und Verkehr

Finanz-, Versicherungswesen

Gesundheit

Wasser und Abwasser

IT und TK

Siedlungsabfallentsorgung

Weltraum

Ernährung

Zentralregierung

Post und Kurier

Chemische Stoffe

Verarbeitendes Gewerbe

Forschung

Anbieter Digitaler Dienste

Siedlungsabfallentsorgung

Ernährung

# 03

## Anforderungen und Maßnahmen

# Die betroffenen Sektoren lassen sich zu unterschiedlichen Betreibergruppen zuordnen

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

### Unterrichtspflichten

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



Audit



Incident Management



Schulung



Business Continuity Management



Verschlüsselung



Lieferantenmanagement



Access Management



Wartung und Betrieb



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 Fortschrittmeldung vorgelegt



Meldestelle vom BSI

# 04

## Sanktionen und Bußgelder

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

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

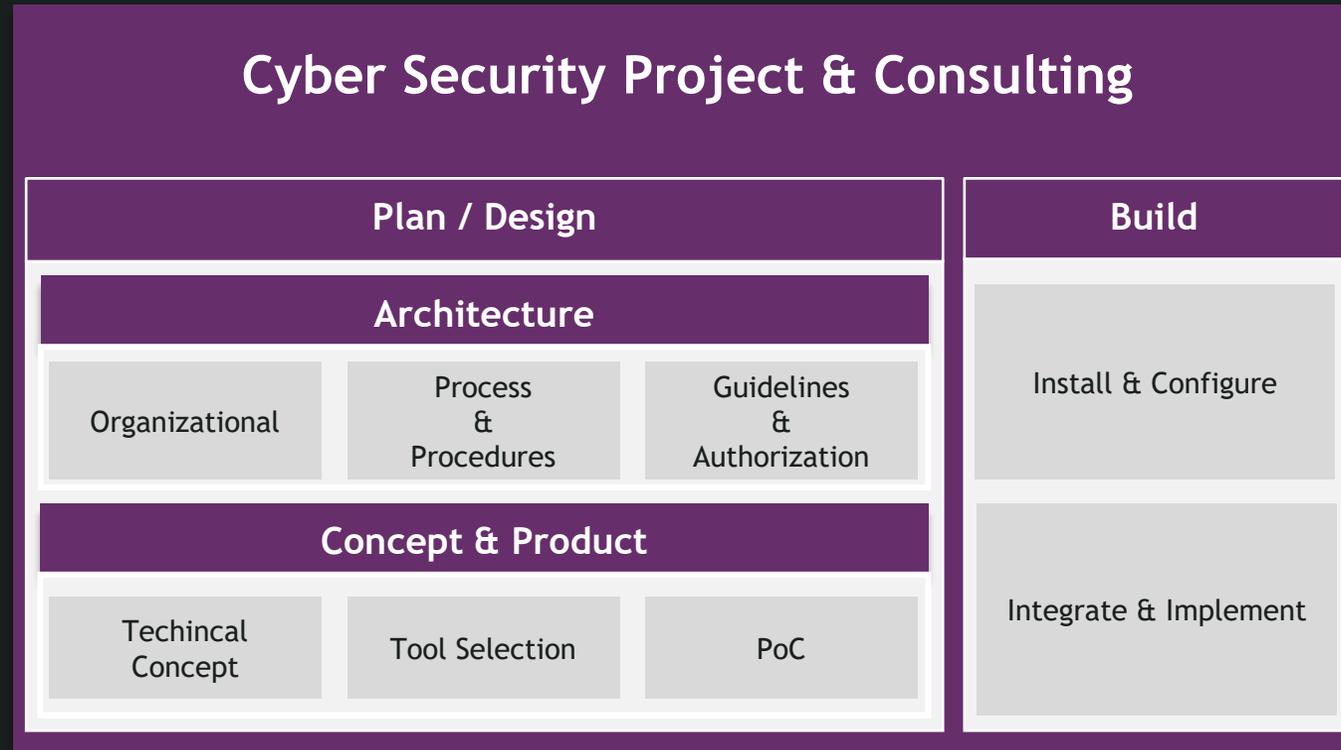
## Beyond Cyber Security

# Leistungsspektrum Cyber Security

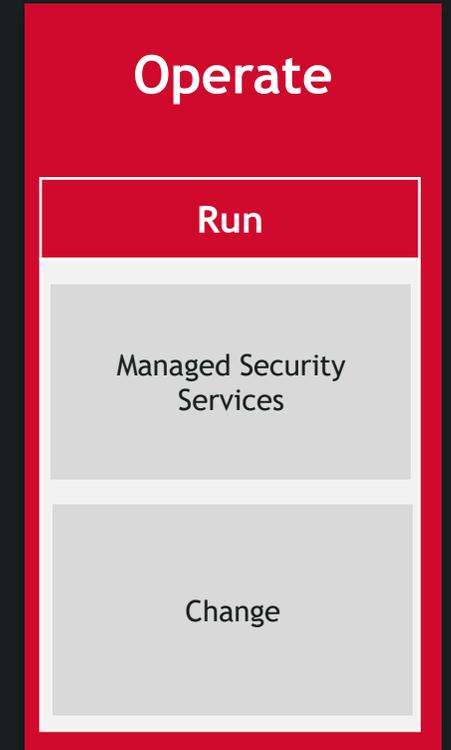
 Advise



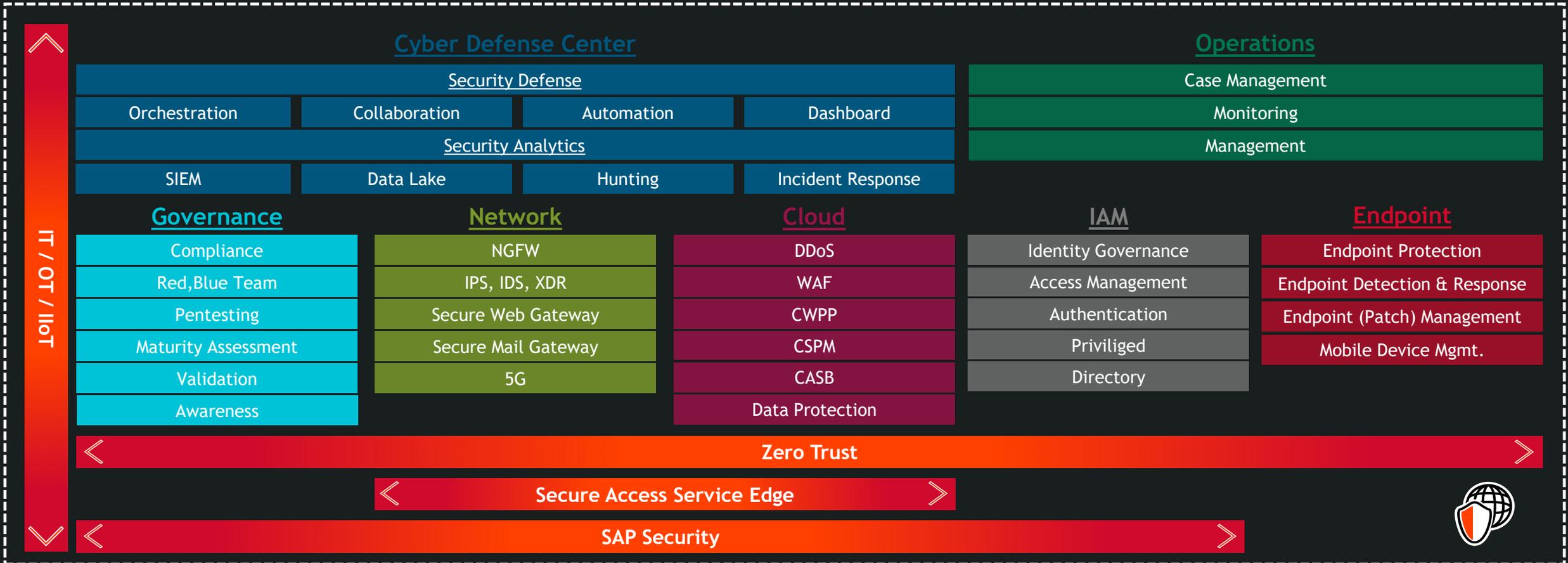
 Plan & Build



 Run

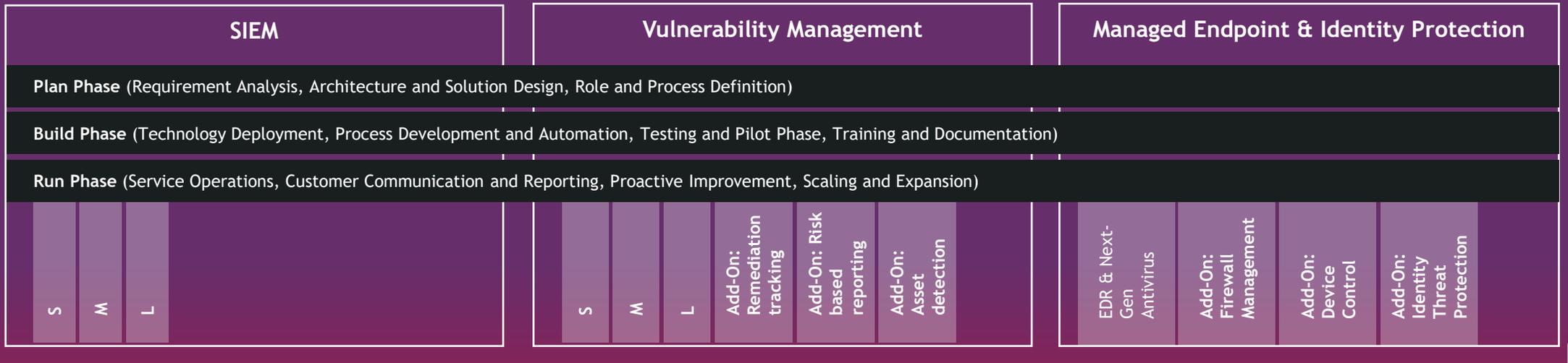


# Digital Shield: Die Building Blocks für maximale Cyber Sicherheit



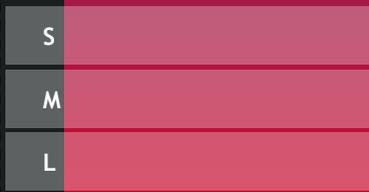
# one.secure customer packages

Basic



## XaaS / Managed Security Services

CDC



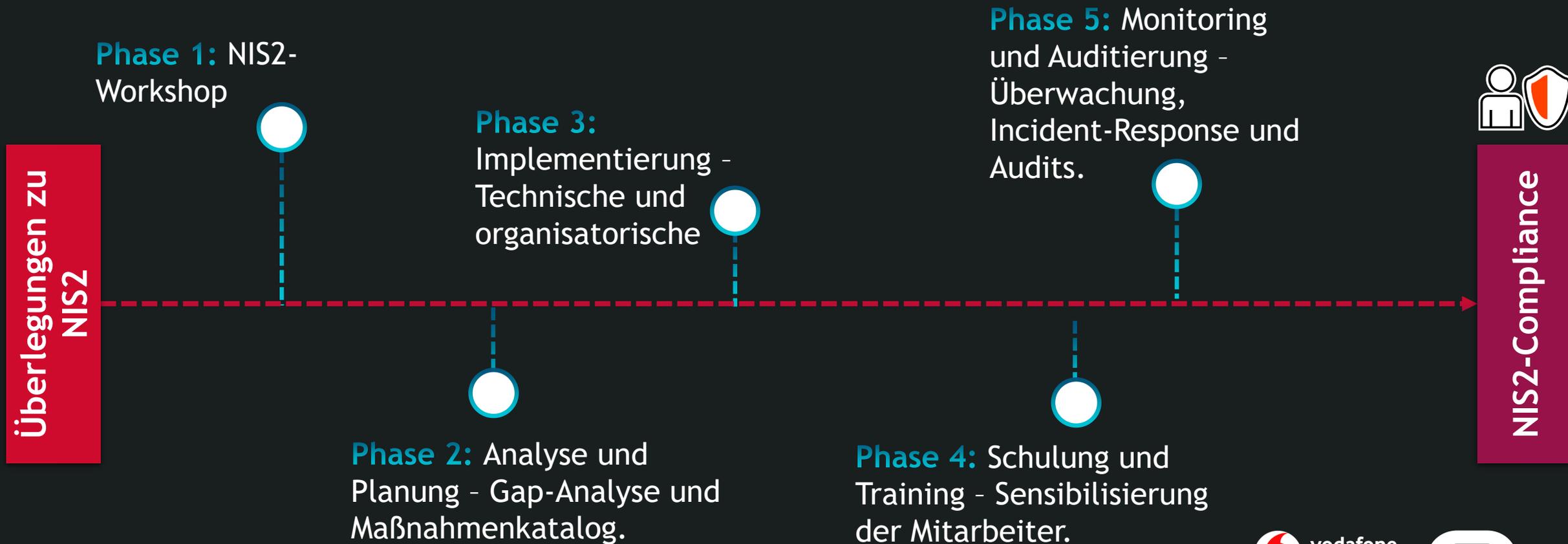
### Cyber Defense Center:

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



# 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.*



**Excellence in all we do.**

**Zeit für Feedback oder Fragen!**