LUNARIS
Digital Solutions

IN 10 SCHRITTEN ZUR CRA-KONFORMITÄT BIS 2028

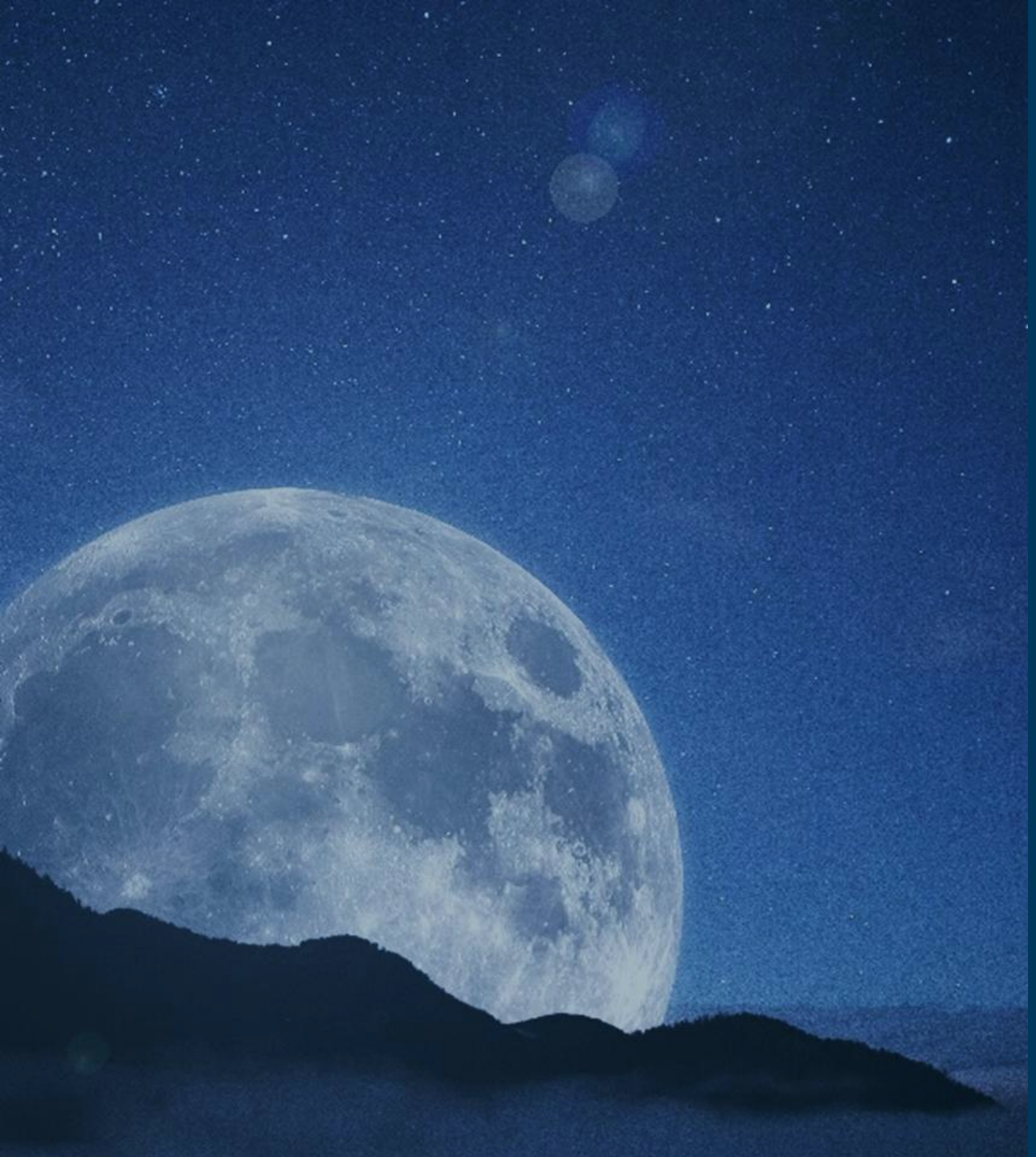
Lars Roith

AGENDA

01 INTRO

02 10 SCHRITTE

03 FAZIT



MIT WEM HABT IHR ES ZU TUN?

Lars Roith

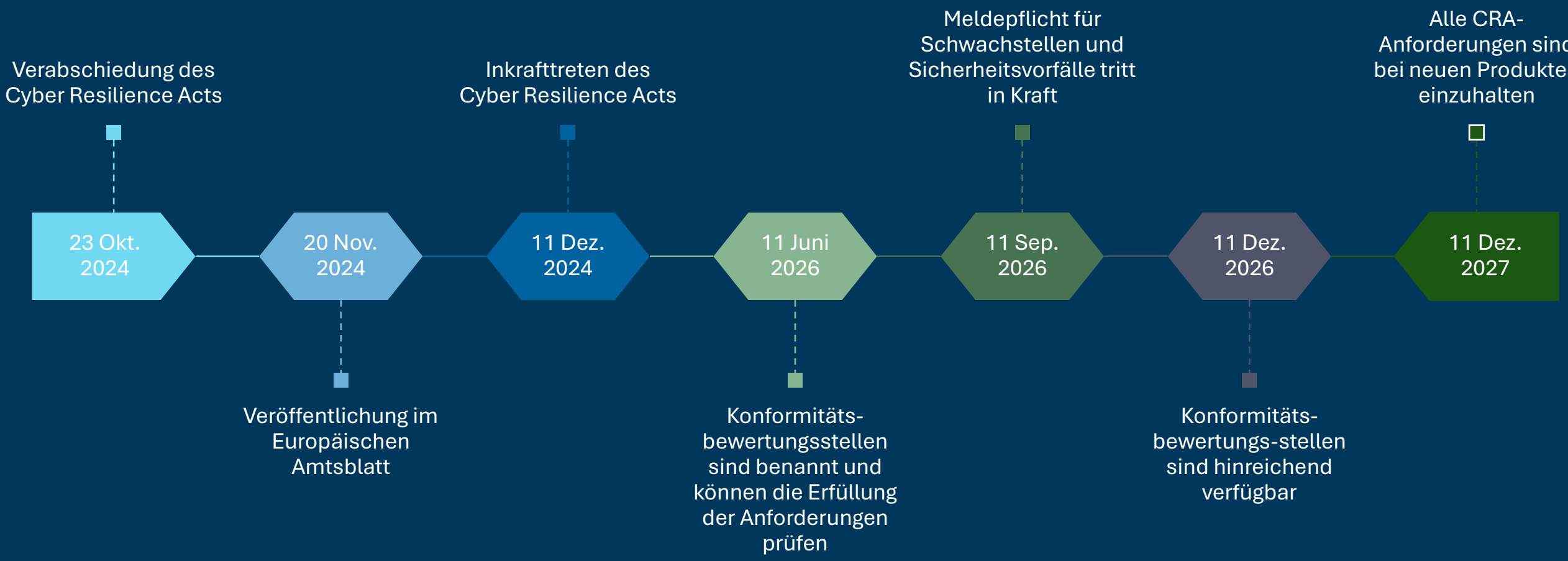
Solution Consultant | CEO

Lars.Roith@lunaris.digital

https://lunaris.digital

LUNARIS
Digital Solutions

DER ZEITPLAN DES CYBER RESILIENCE ACTS



LUNARIS
Digital Solutions

SCHRITT 1: PROJEKTSTRUKTUR AUFSETZEN UND VERANTWORTUNG KLÄREN

In 10 Schritten zu Konformität

Internen CRA-Kick-off initiieren

Projektteam aufstellen und Rollen definieren

RACI-Matrix erstellen

Budget und Zeitrahmen für das CRA-Projekt festlegen

C-Level über Scope, Zuständigkeiten und Risiken informieren

SCHRITT 2: PRODUKTE IDENTIFIZIEREN UND LEBENSZYKLUS FESTLEGEN

In 10 Schritten zu Konformität

Produkte mit digitalen Elementen identifizieren

Technische Gemeinsamkeiten und Plattformansätze erkennen

Zuordnung zu CRA-Kategorien

Unternehmensrollen klären

Lebensdauer und vorgesehener Supportzeitraum pro Produktfamilie definieren

Updatepolitik dokumentieren

Interne Prozesse und Ressourcen für langfristigen Support planen

Supportzeiträume und End-of-Support klar kommunizieren

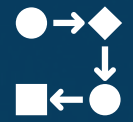
SCHRITT 3: SECURITY-BY-DESIGN IN DER PRODUKTENTWICKLUNG VERANKERN

In 10 Schritten zu Konformität

Sicherheitsanforderungen pro Produkt systematisch erfassen und dokumentieren

Risikoanalyse durchführen (z. B. mit STRIDE, DREAD, TARA oder ISO 27005)

Schutzmaßnahmen auf Architekturebene einplanen (z. B. Zugriffskontrollen, Logging, Verschlüsselung)



Umsetzung in den Entwicklungsprozess integrieren (Security-Reviews, sichere Coding-Guidelines etc.)

Ergebnisse und Maßnahmen in der technischen Dokumentation erfassen

SCHRITT 4: SCHWACHSTELLENMANAGEMENT AUFBAUEN

In 10 Schritten zu Konformität

Verfahren zur Schwachstellenbehandlung definieren (inkl. Bewertung, Priorisierung, Behebung)

Für jedes betroffene Produkt eine SBOM erstellen und pflegen

Automatisierte Tools für CVE-Scanning und Dependency-Checks einsetzen

Zuständigkeiten für Schwachstellen-management organisatorisch verankern

Offenlegungs- und Meldeprozesse (z. B. Coordinated Vulnerability Disclosure) aufsetzen

Ergebnisse und Prozesse in der technischen Dokumentation abbilden und dokumentieren

SCHRITT 5: LIEFERKETTE UND OPEN SOURCE PRÜFEN

In 10 Schritten zu Konformität

Automatisierte Tools zur Erkennung von Schwachstellen in Drittsoftware einsetzen

Prozesse zur Prüfung und Freigabe von Komponenten (insbesondere Open Source) etablieren

Vertragliche Anforderungen an Lieferanten anpassen, um Sicherheits- und Updatepflichten abzusichern

Externe Lieferanten auditieren

SCHRITT 6: TECHNISCHE DOKUMENTATION UND KONFORMITÄT VORBEREITEN

In 10 Schritten zu Konformität

Struktur und Inhalte der technischen Dokumentation gemäß CRA-Anforderungen definieren

Bestehende Informationen (z. B. aus ISO 27001, MDR, Maschinenrichtlinie) integrieren und konsolidieren

Verantwortlichkeiten und Ablagestrukturen intern festlegen

Kontakt zu benannten Stellen aufnehmen, wenn eine externe Konformitätsbewertung erforderlich ist

SCHRITT 7: SICHERHEITSVORFÄLLE ERKENNEN UND MELDEN

In 10 Schritten zu Konformität

Prozesse zur Erkennung und Behandlung von Sicherheitsvorfällen aufsetzen

Interne Meldeketten definieren (z. B. IT → CISO → Management)

Verbindung zur ENISA-Meldeplattform vorbereiten (inkl. Fristen und Format)

Support-, Service- und Vertriebsmitarbeitende sensibilisieren und schulen

Dokumentation aller Sicherheitsvorfälle und Reaktionen im Rahmen der technischen Unterlagen sicherstellen

SCHRITT 8: UPDATE-STRATEGIE ANPASSEN

In 10 Schritten zu Konformität

Bestehende Update-Strategie analysieren und anpassen

Trennung von Funktions- und Sicherheitsupdates technisch und organisatorisch umsetzen

Automatische Sicherheitsupdates inkl Opt-Out ermöglichen (wenn technisch vertretbar)

Release- und Testprozesse auf neue Anforderungen ausrichten

DevOps-Pipeline um Security-Gates erweitern

Änderungen in technischer Dokumentation und Kundenkommunikation festhalten

SCHRITT 9: MITARBEITENDE SCHULEN – UND NICHT NUR DIE ENTWICKLER

In 10 Schritten zu Konformität

Zielgruppenspezifische Schulungen konzipieren und durchführen

Schulungsnachweise dokumentieren und regelmäßig auffrischen

Schulungsformate wählen, die in den Arbeitsalltag passen (z. B. kurze Online-Module, Onboarding-Elemente, Lunch & Learn)

SCHRITT 10: PRODUKTSTRATEGIE ANPASSEN UND PORTFOLIO STEUERN

In 10 Schritten zu Konformität

Bestehende Produktlinien und Roadmaps im Hinblick auf CRA-Fitness analysieren

Entscheidungen treffen: Nachrüsten, abkündigen oder ersetzen?

Neue Produkte ab 2025/26 mit CRA-Anforderungen planen und entwickeln

Interne Freigabeprozesse um ein CRA-Konformitätskriterium erweitern

FAZIT

In 10 Schritten zu Konformität

CRA ist kein (ausschließliches) IT-Thema

Bestehende Standards sind kein Selbstläufer

Dokumentation wird zum Zulassungskriterium

Frühzeitige Analyse spart teure Umwege


LUNARIS
Digital Solutions