

The EU Cyber Resilience Act and PCI DSS

The Track Laid Bare

Daniel Thompson-Yvetot

CEO CrabNebula & Comply.Land

Founder Tauri

ETSI CYBER-EUSR Rapporteur Browsers, Password Managers
Author “Manufacturing European Software”



CYBER RESILIENCE ACT

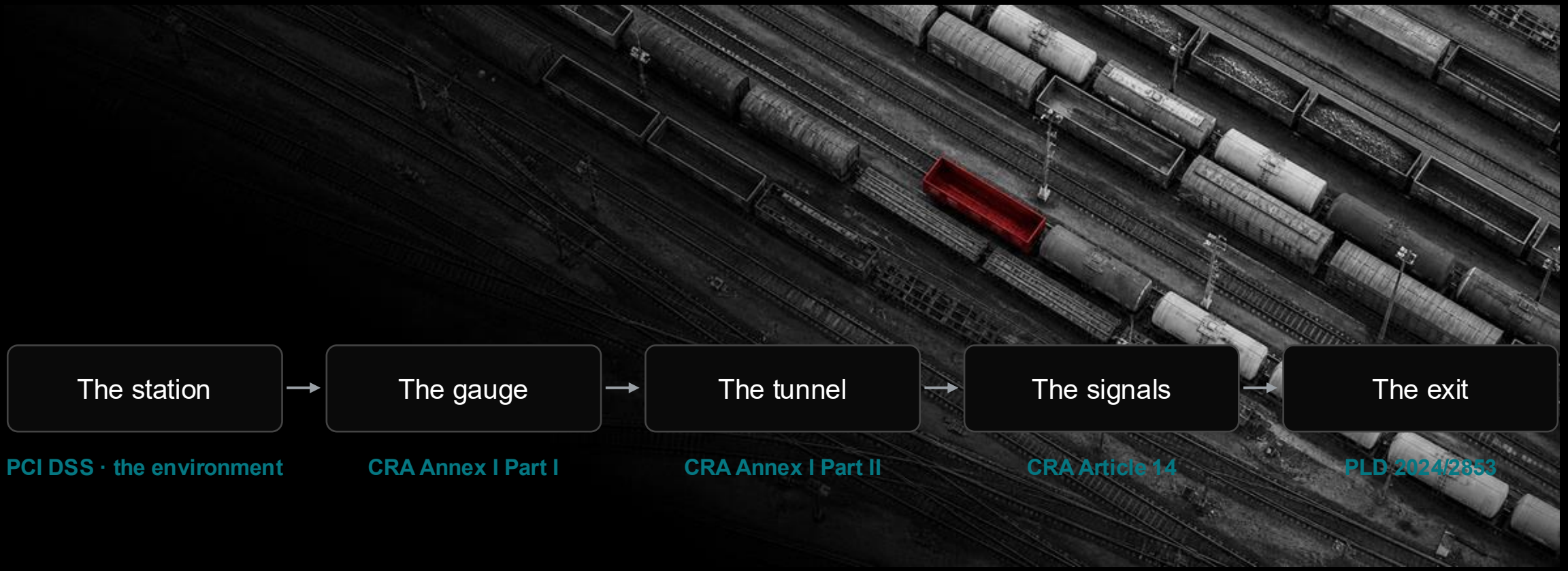
Essential cybersecurity requirements … for Data?

For the people who live and breathe PCI DSS.



The line moves forward

You already know the starting station of the journey, but where are we going?



DATA is an asset.

The station

PCI DSS secures the environment. The CRA regulates what rolls in.



The environment → The product

Article 2 · a product with digital elements

SSDLC + TARA + STRIDE

The gauge

Built to profile before it may enter. Secure by design, secure by default.



Designed → On the market

Annex I Part I · risk-based, Article 13(2)

It is not an excuse to be ignorant of your components.

You are in your supply chain.

Your code, the parts you source, the ground it runs on.



Sourced → Answered for

Article 13(5) due diligence · SBOM

If the terminal bricks when your service dies, that service is the tender.

Coupled, and in scope

The backend the train cannot run without travels with it.



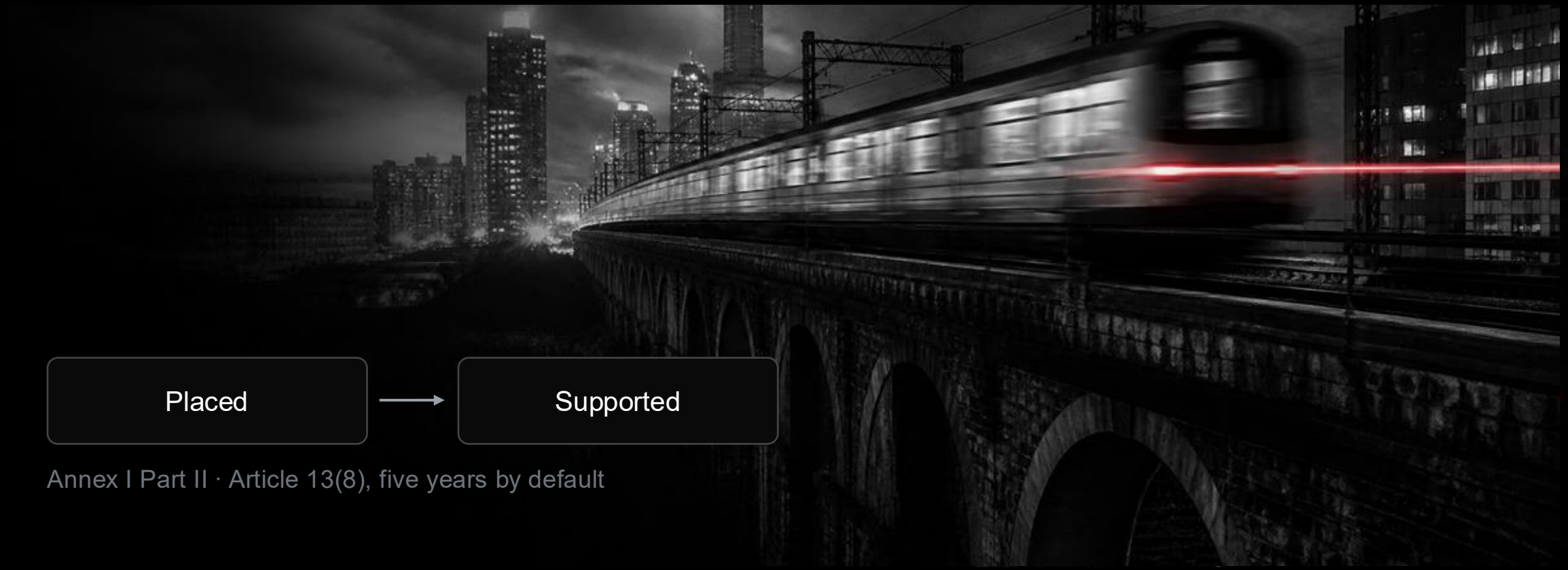
In the cloud → Part of the product

Article 3(2) · remote data processing

PSIRT, VEX, KEV, CWE

Maintained in motion

Vulnerability handling for the whole support period. No annual snapshot.



Annex I Part II · Article 13(8), five years by default

ENISA, MSA, SRP

24 h · 72 h · 14 d

Actively exploited vulnerabilities and severe incidents, to ENISA, from **11 September 2026**.



Early warning → Final report

Article 14 · single reporting platform

THE USERS

The passengers hold a claim

Strict liability. A missing update is a defect. Your file is evidence.



Nonconforming → Presumed defective

Directive (EU) 2024/2853 · Articles 9, 10, 11

THE TIMETABLE

The track ahead

PLD transposed 9 Dec 2026 · full CRA 11 Dec 2027



9 Dec 2026 → 11 Dec 2027

Regulation (EU) 2024/2847 · Directive (EU) 2024/2853

Attestation of Compliance is not a DoC

No EU regime treats an AoC as legal conformity



DEPARTURE

Build the train to fit, keep it running.

The tunnel is not optional. The gauge is published. The passengers have rights.

I will help you get and stay on track.



Daniel Thompson-Yvetot

ETSI CYBER-EUSR Rapporteur Browsers, Password Managers
CEO CrabNebula & Comply.Land, Founder Tauri
Author “Manufacturing European Software”