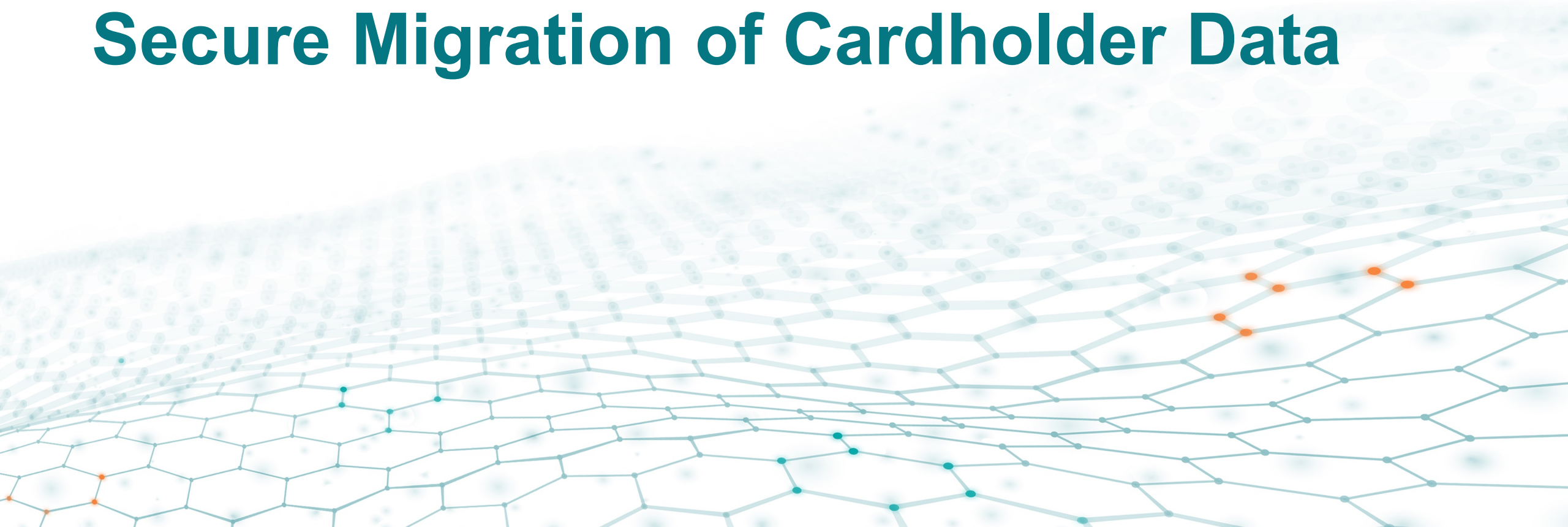
PCI Security Standards Council

Secure Migration of Cardholder Data



PCI Security Standards Council

Mika Rautio

Senior Security Architect
Nexi Group / Nexi Digital Finland

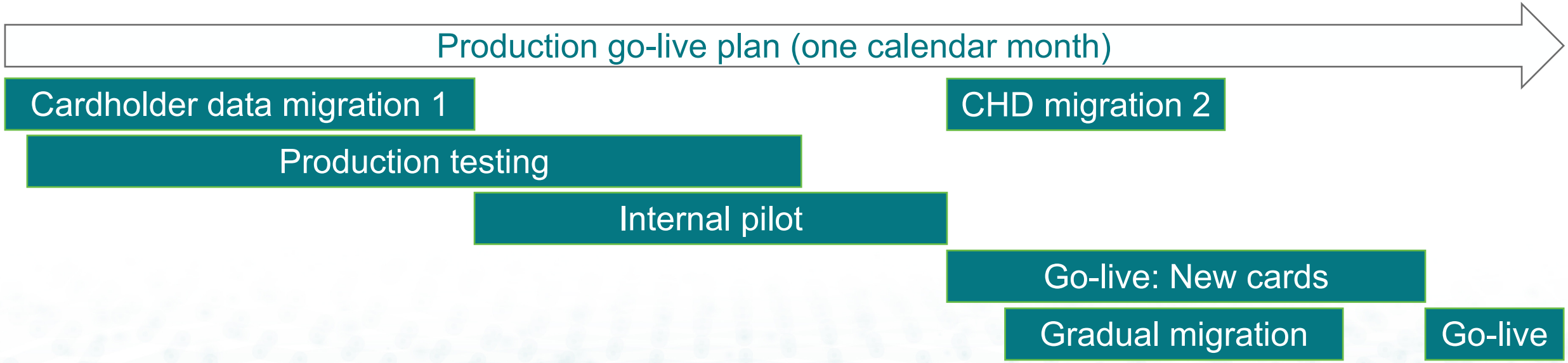
Agenda

- The Project – E-Commerce Migration
- The Cardholder Data Migration
  - Export Process
  - Protection of the Data

The Project

E-Commerce Migration

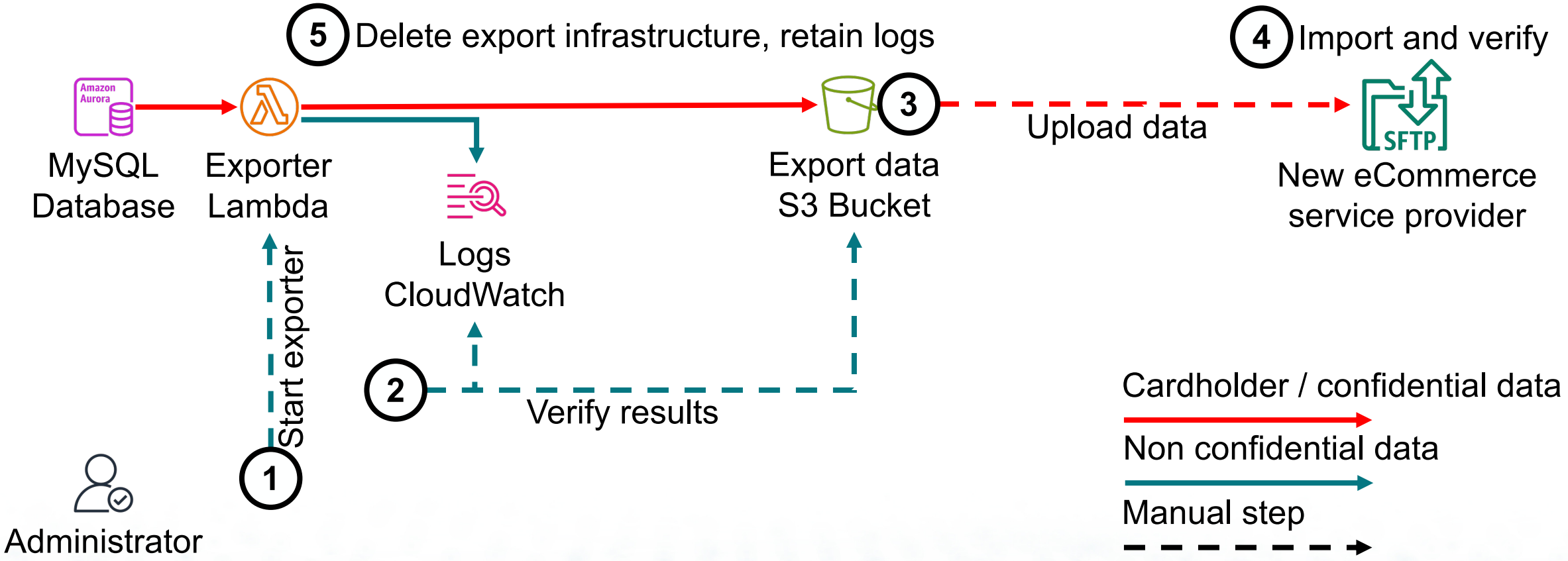
- Replace eCommerce service
- High availability, zero downtime
- Millions of cardholders and cards in scope



PCI Security Standards Council

The Cardholder Data Migration

Export Process



The Cardholder Data Migration

Protection of the Data

Primary controls

- Data minimization & short data retention
- Reduced network and access rights (“zero trust & least privilege”)
- Strong encryption & end-to-end-encryption

Cryptography

In-transit

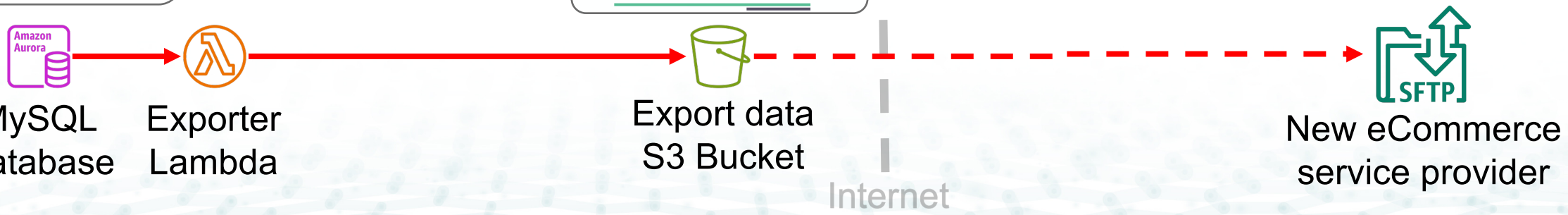
API & TLS 1.2
ECDHE-ECDSA-AES128-GCM-SHA256

SFTP & SSH-2
ECDH-SHA2-NISTP256, RSA-3072,
AES-128-CTR, HMAC-SHA2-256

OpenPGP (new service provider’s key), “end-to-end encryption”
RSA-3072, AES-256-CFB, SHA-1

At-rest

AWS KMS CMK
AES-256-GCM



PCI Security Standards Council

Takeaways

One ought to design PCI DSS CDE under the assumption that the threat actor will have full familiarity with the environment
– A take on Shannon's maxim

- Scope your migration
- Understand the lifetime of your data
- Move towards higher effective key strengths