exeon

Smart Cyber Security.

PostFinance – an ExeonTrace NDR Case Study

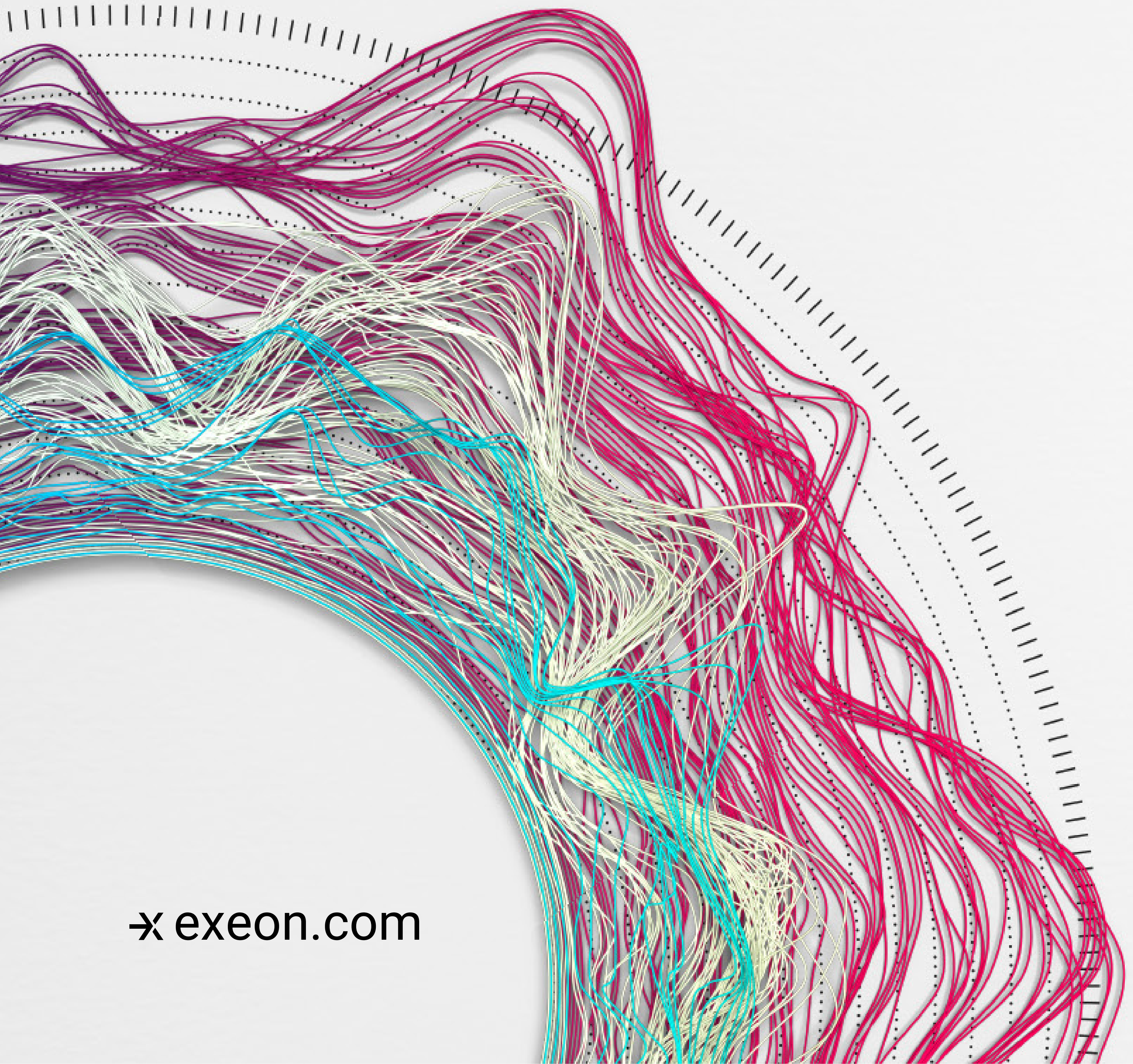
ExeonTrace secures

PostFinance core systems

PostFinance
PostFinance
PostFinance
Auszahlung
Auszahlung

Overview

Industry: Finance / Banking



Benefits provided by ExeonTrace:

- Deep integration of ExeonTrace in the multi-faceted protection of PostFinance core systems
- Complete visibility into the highly virtualized IT infrastructure
- Close and trustful collaboration of Exeon and PostFinance teams

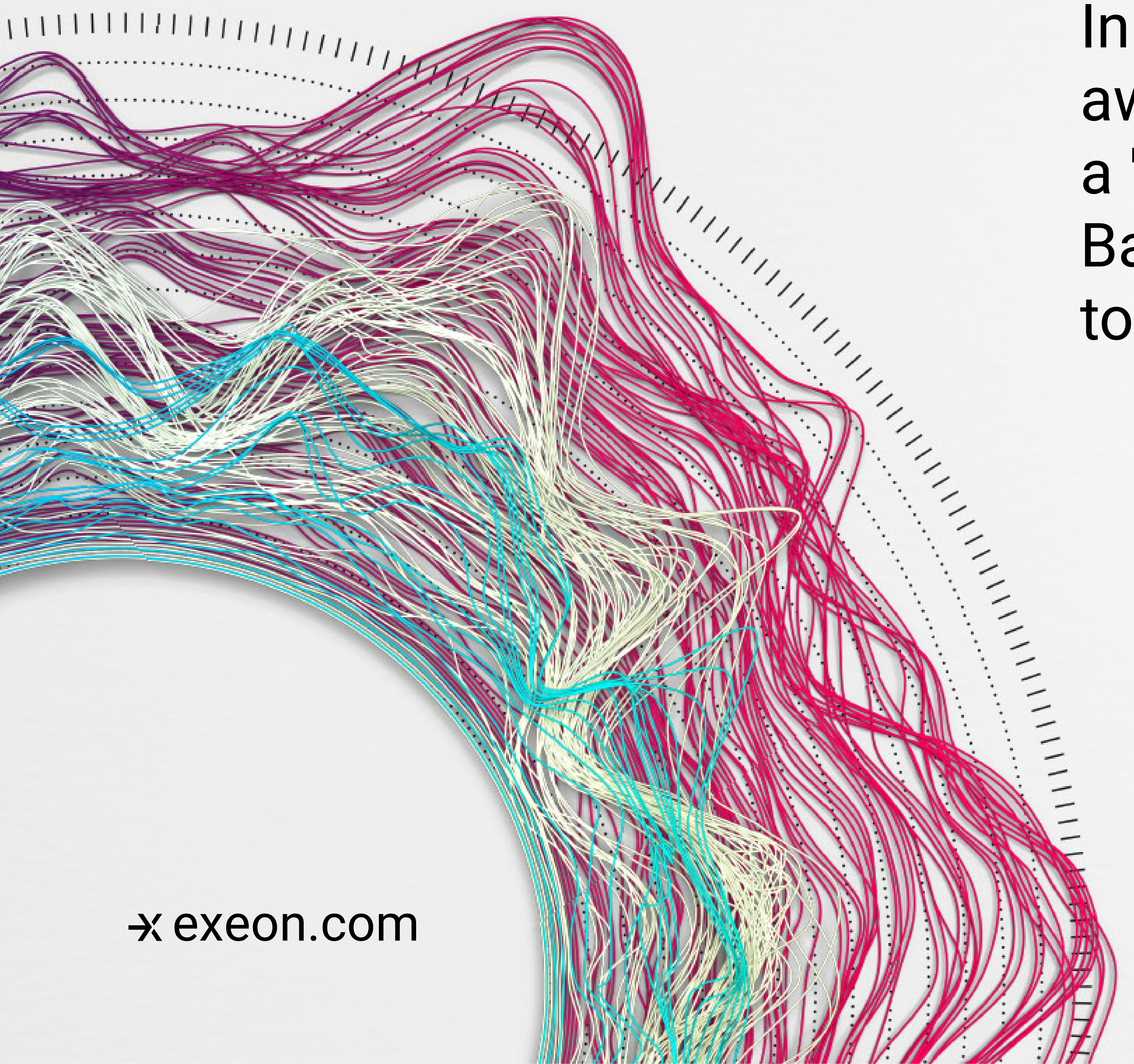
Challenges faced by ExeonTrace:

- Far-reaching requirements of the Swiss Financial Market Supervisory Authority (FINMA)
- Best-of-breed approach with various interfaces to surrounding systems
- Mirroring the whole network traffic was not an option
- Broad evaluation of leading suppliers

PostFinance Business Background

PostFinance is the financial services unit of Swiss Post which was founded in 1906. It is one of Switzerland's leading retail financial institutions. In its role as market leader and with more than a billion payment transactions a year, it ensures a seamless flow of liquidity on a daily basis.

In 2013, the Swiss Financial Market Supervisory Authority (FINMA) awarded PostFinance a bank licence. In 2015, PostFinance was declared a "systematically important" financial institution by the Swiss National Bank, which means the bank must follow special regulations with regards to liquidity and equity - but also with regards to data security.



Challenges

“To comply with the Finma regulations and to address future threats, PostFinance wanted to strengthen its data security.”

Architectural decision towards a best-of-breed solution in the different security-relevant segments (Threat Detection, Threat Hunting, Vulnerability Management and others)

Therefore, high integration requirements of the Network Detection & Response solution to the surrounding security solutions

Mirroring the whole network traffic was not an option

Broad evaluation of the leading Network Detection & Response providers

Solutions

- ✓ ExeonTrace was the most successful solution in detecting the tested use cases in the Red Team Proof of Concept

- ✓ In addition to the multi-year Software licensing, Exeon also supports the PostFinance team in integrating ExeonTrace in the wider cybersecurity architecture

- ✓ Multiple PostFinance locations that are covered through one holistic view on their network

- ✓ Use cases that were tested, i.a.:
  - Lateral movements
  - Domain-Generation Algorithms
  - Hidden DNS Channel
  - Command & Control Channels
  - Various Threat Hunting use cases

- ✓ Consequently, deep integration of ExeonTrace in the core systems

Benefits

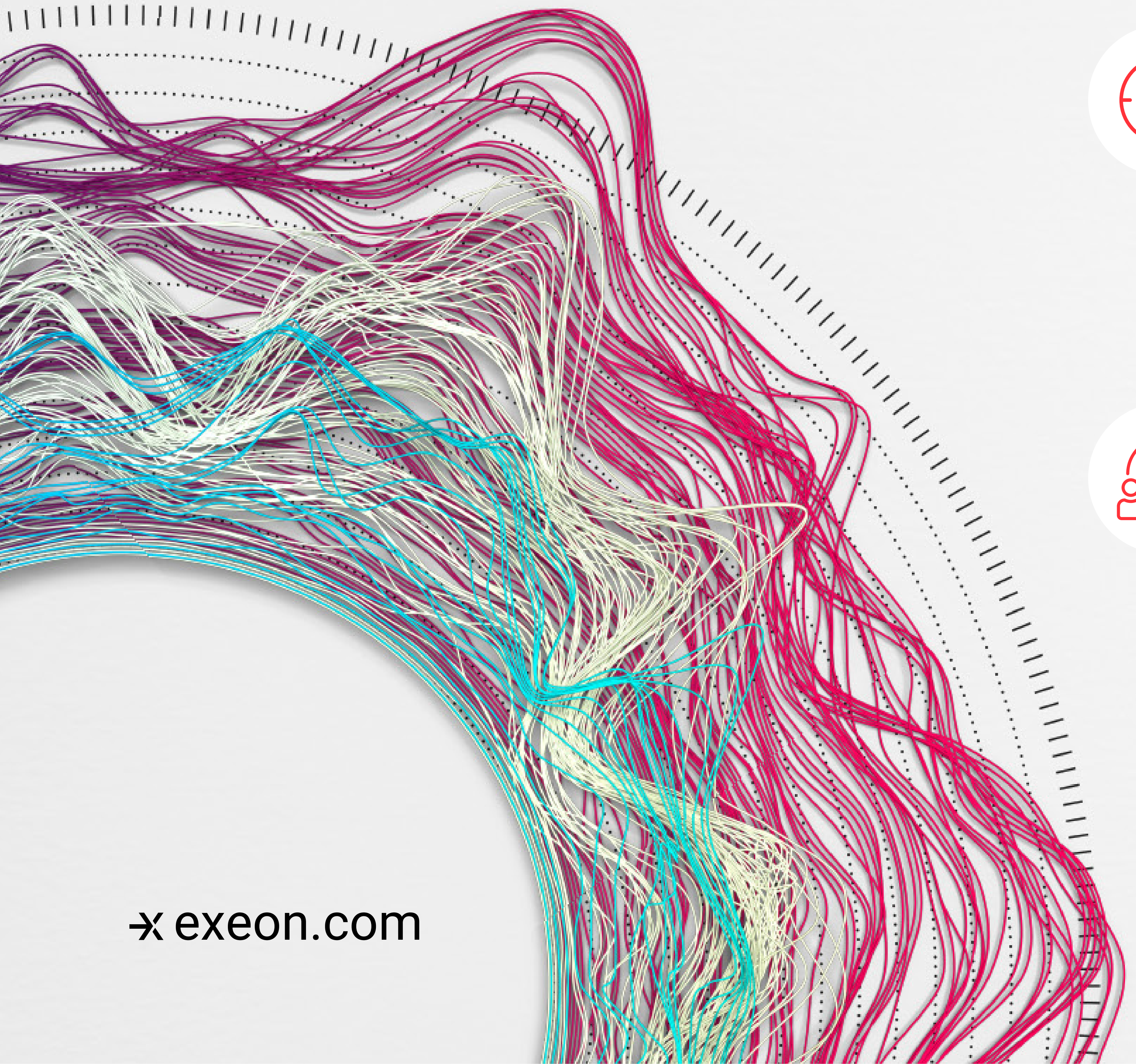
Highly integrated Network Detection & Response supporting the multi-faceted protection of PostFinance core systems

Easy navigation through the historic log data for complete visibility directly in the ExeonTrace interface – achieved through a graph database that reduces the required storage

Close and trustful collaboration of the Exeon and PostFinance teams

ExeonTrace provides complete visibility into the highly virtualized IT infrastructure of PostFinance

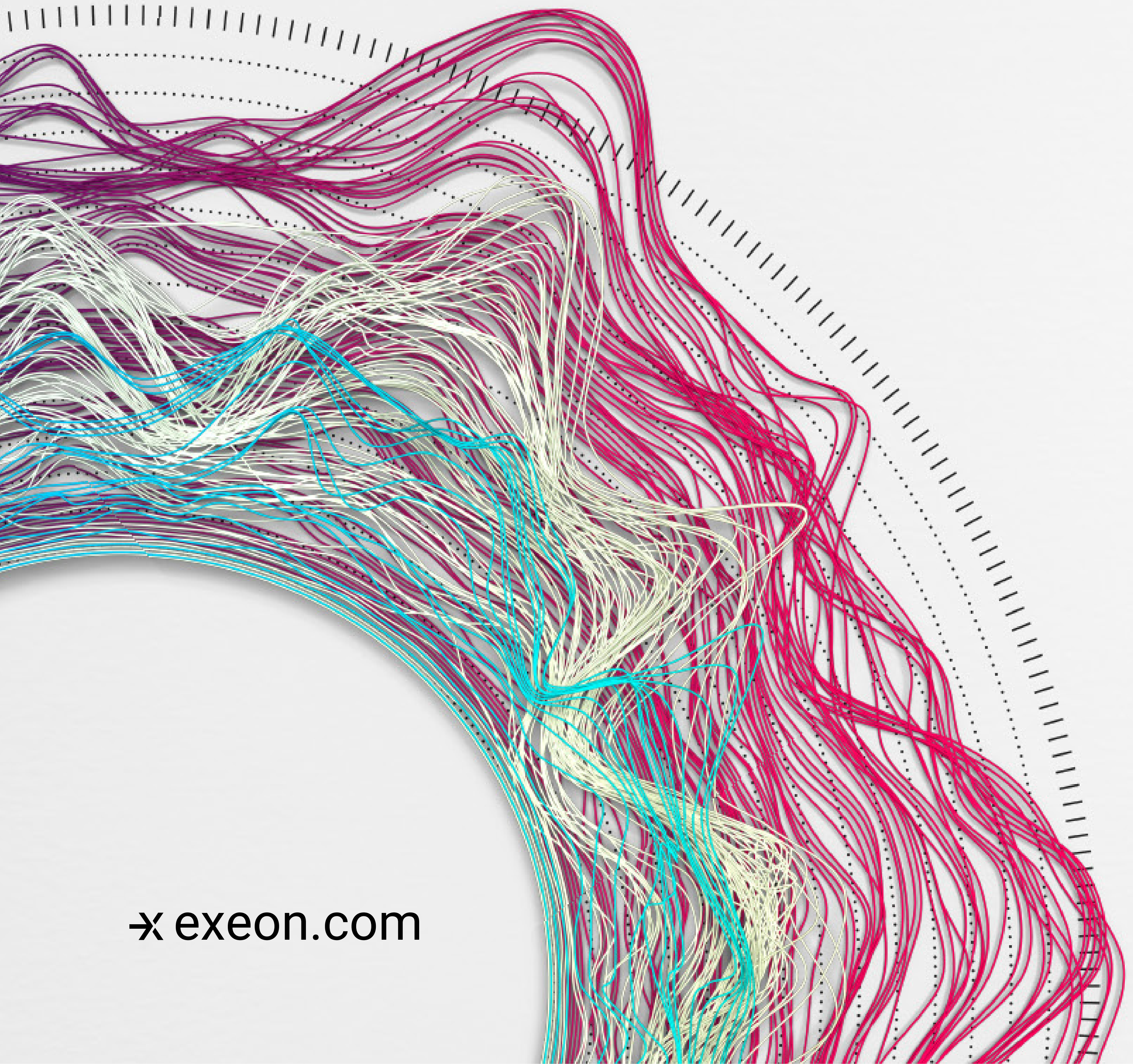
ExeonTrace also supports the monitoring of industry-specific assets, such as ATMs



> “PostFinance has chosen ExeonTrace because of its open and future-proof architecture. Not needing any hardware sensors and being able to control data flows, we didn't have to make any significant changes to our existing infrastructure. We are also convinced by the cooperation with the competent and technically outstanding Exeon team.”

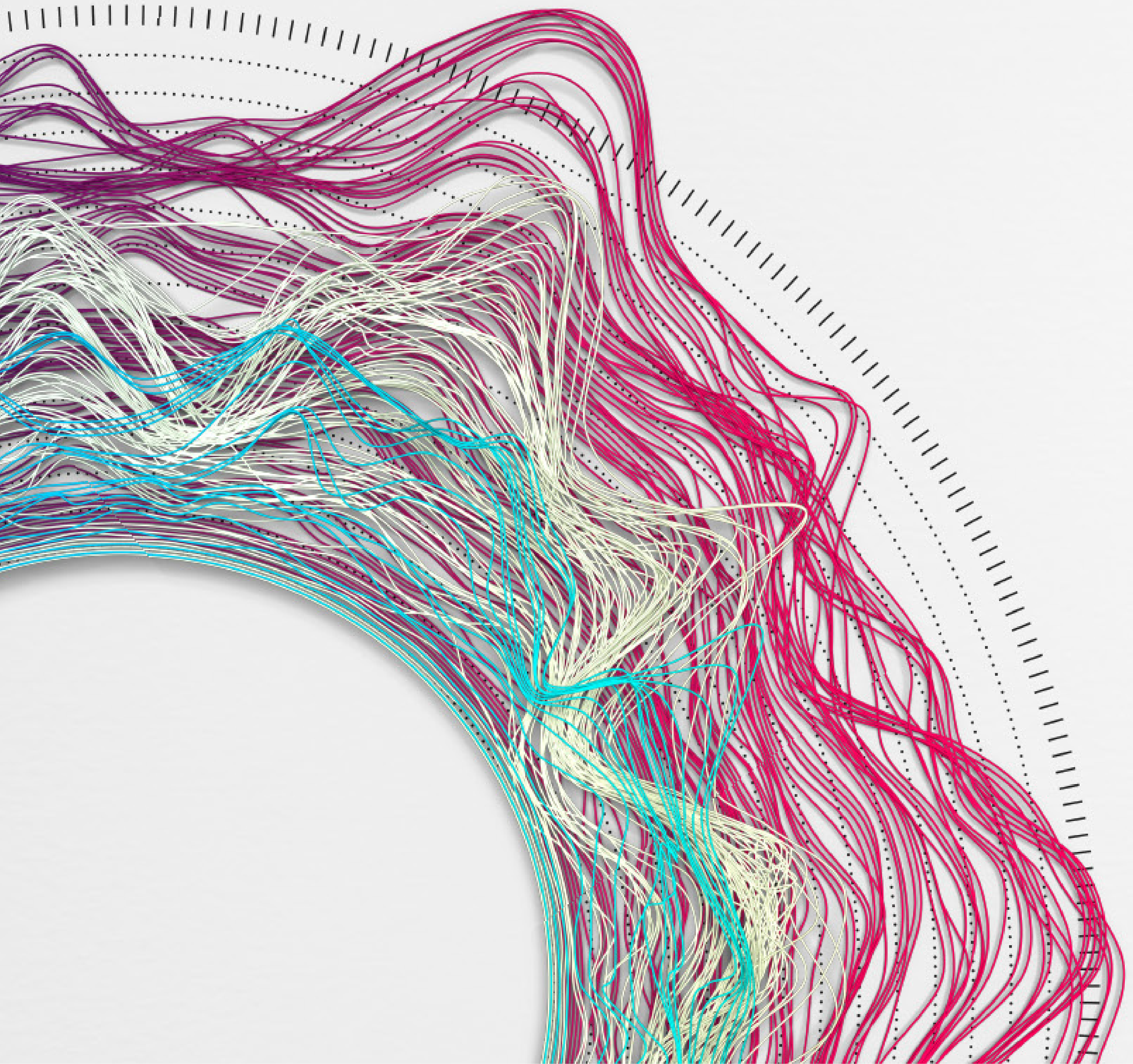
Head IT Security

PostFinance



Get in touch with us

exeon
Smart Cyber Security.



Gregor Erismann
CCO
+41 78 797 05 09
gregor.erismann@exeon.com

Exeon Analytics AG
Grubenstrasse 12
8045 Zurich
Switzerland
contact@exeon.com
exeon.com