



PARTAGEONS PLUS QUE L'ÉNERGIE



groupe e

In a Nutshell

2'500
employees

26'000
construction sites
per year
wide range of activities
strong expertise

12'900 km
electrical grid

The flagship energy company

bespoke solutions
proximity

3 TWh
electricity sold per year

277 GWh
heat delivered per year



groupe 

Une culture de pionniers

1873 Construction de la première usine hydroélectrique du canton de Fribourg (Maigrange)

1907 Création d'ENSA

1915 Création des EEF

1948 à 1964 Construction des grands barrages sur la Sarine

2001 Transformation des EEF en SA

2005 Fusion des EEF et d'ENSA





Energies

Electricity

New renewable
energies

Gas

Heat and cold

Hydrogen

Delivery

Electricity network

Smart Grid

Thermal network

Gaz network

Building technology, equipment & mobility

Electrical installations

Household appliances
& organisation

Information &
communication technologies

Refrigeration, air
conditioning &
ventilation

Electric mobility

Heating

Water & sanitary

Solutions & Services

Facility management

Energy efficiency /
engineering

General energy
company

Attacks on sensitive infrastructure

<https://en.wikipedia.org/wiki/Stuxnet>
[https://cyberlaw.ccdcoe.org/wiki/Steel_mill_in_Germany_\(2014\)](https://cyberlaw.ccdcoe.org/wiki/Steel_mill_in_Germany_(2014))
https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

Stuxnet (2010) - Iran

The most publicized example of a cyberattack against critical infrastructure is the Stuxnet computer virus. The worm, which targeted PLCs, disrupted Iran's nuclear program by damaging centrifuges used to separate nuclear materials.



Colonial Pipeline (2021) - USA

The company halted all pipeline operations to contain the ransomware attack. About 45% of all fuel consumed on the US East Coast arrives through the network of these pipelines.

Steel mill in Germany (2014)

The accumulation of individual SCADA industrial component failures prevented the furnace from shutting down, causing severe infrastructure damage.





groupe e

Recent attacks in Switzerland

The number of cyber attacks has significantly significantly in 2022.
More than 700 attacks are reported to NCSC every week.

MCH

Innovate
radicalement
la construction

Shifting
Building
Paradigms

**WIN
BIZ**

cremo+

Läderach
chocolatier suisse

MATISA



tpf
● ● ●

FINA | PORT

swissport 

LA LIBERTÉ



University of
Zurich^{UZH}

CarPostal 
La classe jaune.

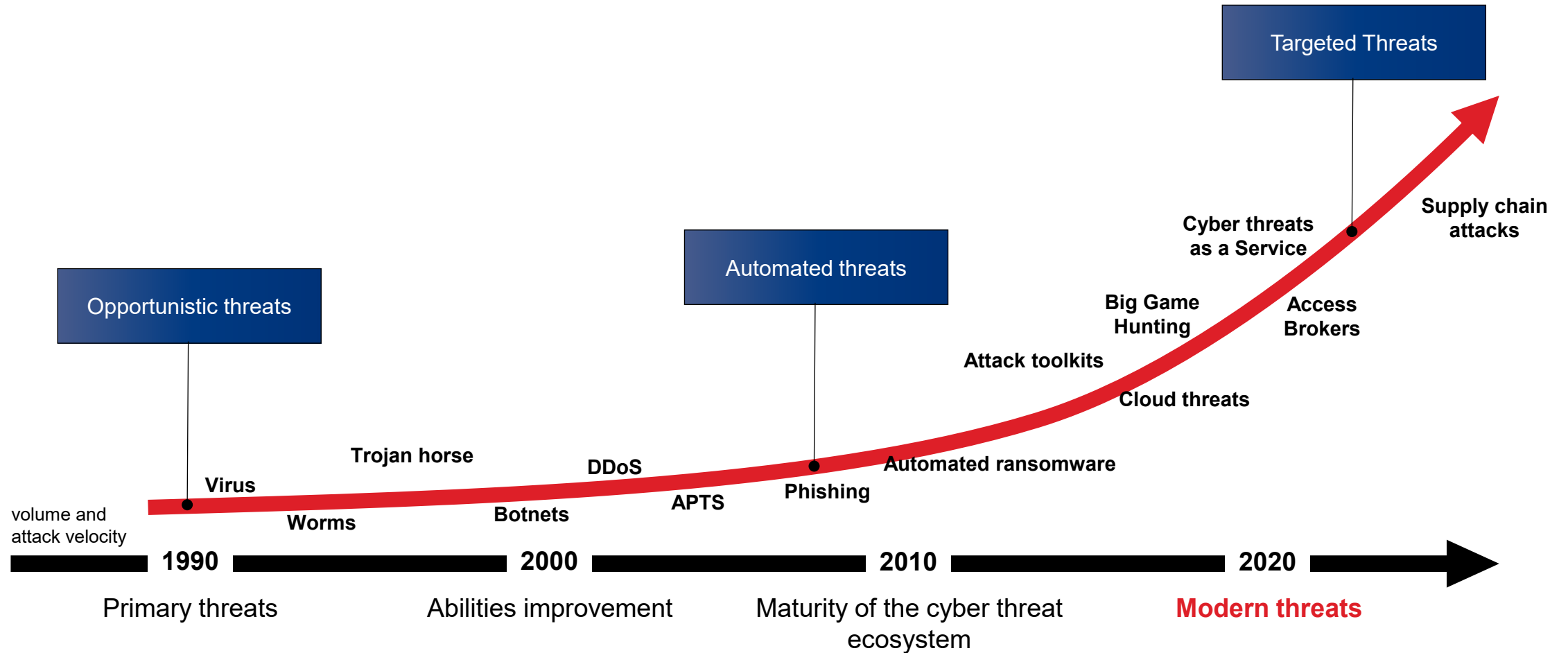


CICR



groupe e

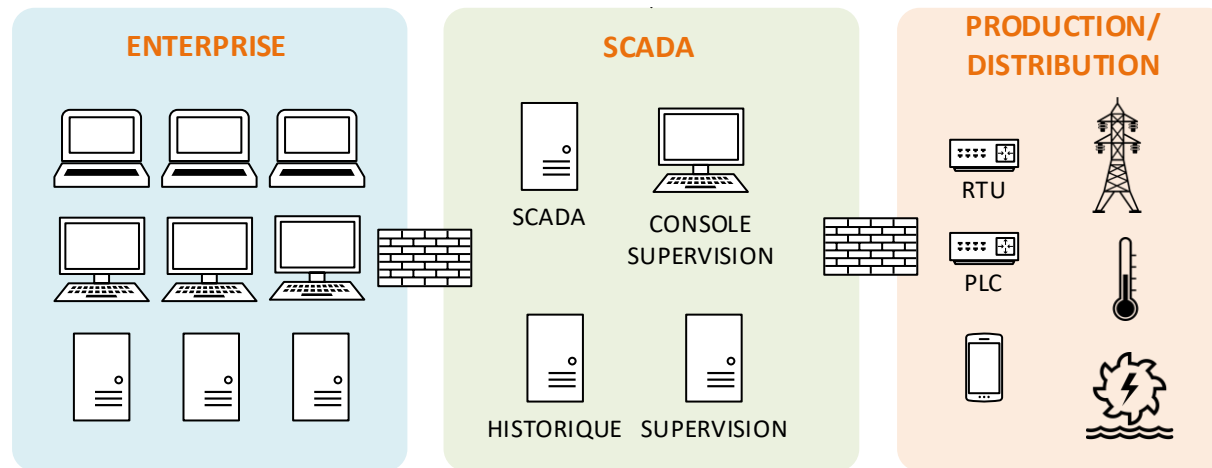
Cyber threats evolution





groupe

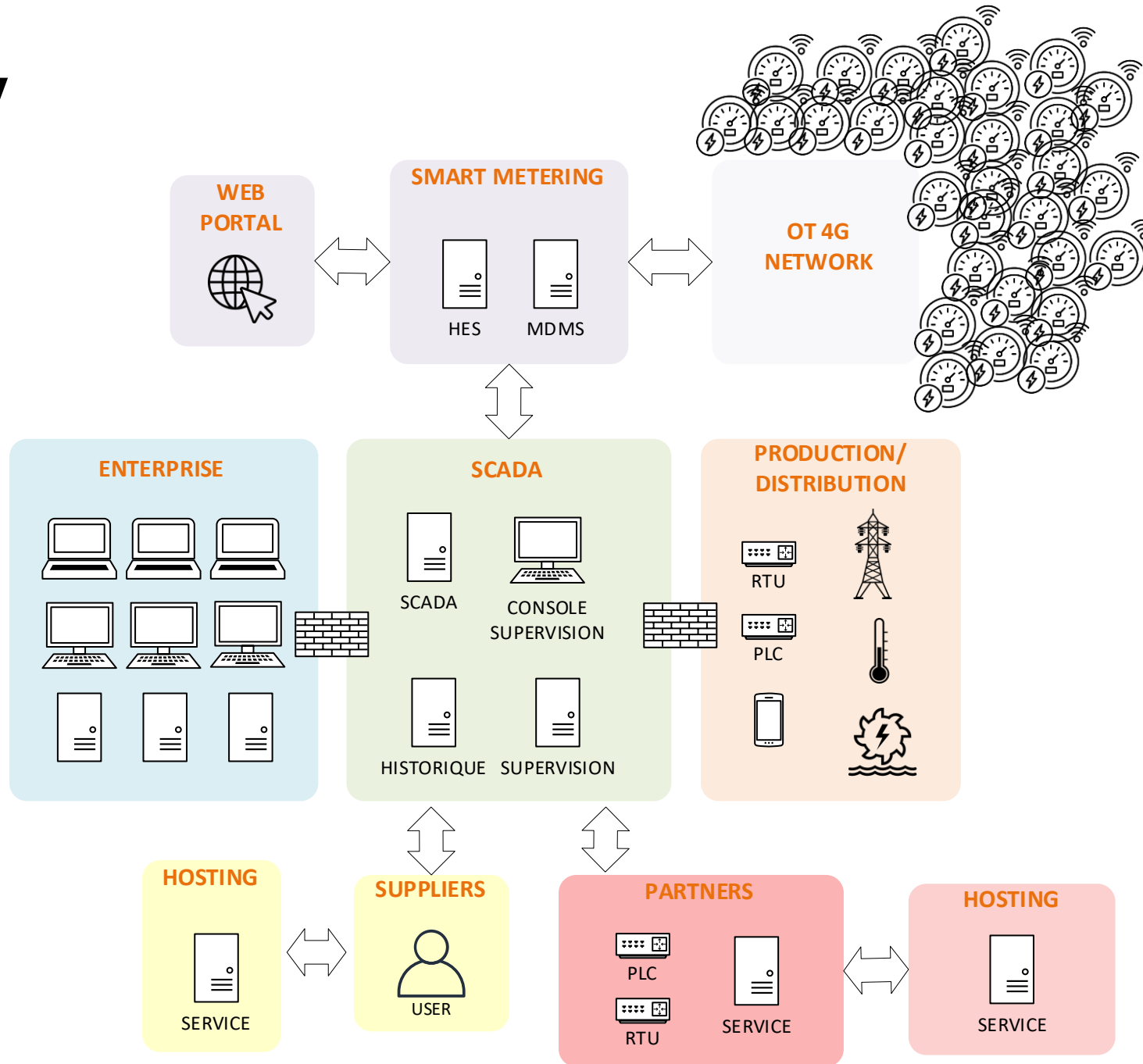
Historical



Historical – focus on the peripheral protection



Today





Today – holistic approach of Cyber Security





Smart Metering



Key element to make the electricity supply system fit for the energy transition and for the client's better control of their consumption.

Deadline 80% for 2027 (OApEI Art. 31^e alinea 1).

300'000 Smart Meters to deploy.

Core change for Groupe E:

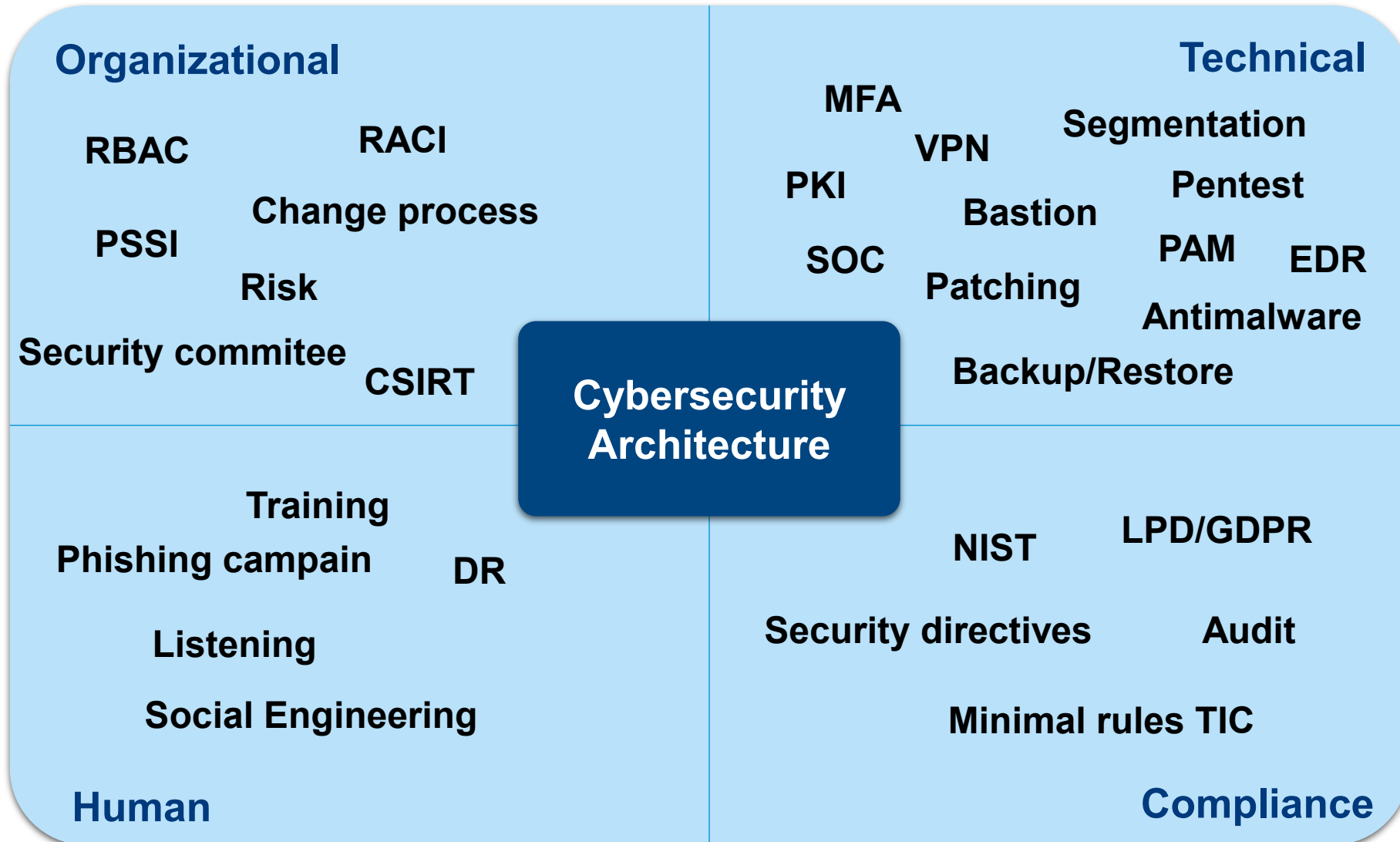
- Digitalisation of the metering process: no more need of employee to read once a year the consumption
- New interaction with the customers: application to see the live consumption, dynamic pricing, invoicing based on effective consumption, ...
- Enhanced security mindset



Smart Metering – Security challenges

- Open the network to 300K points.
- Limited security maturity of the suppliers.
- Groupe E security not fully adapted to accommodate a Smart Metering infrastructure.
- Many external actors involved. (Smart Meter supplier, TELCO, datacenters, numerous applications integration, cybersécurité experts, ...)
- Future integration with the SCADA infrastructure which is the Groupe E most critical infrastructure.
- Provide an easy access for the customers to their consumption data.

Approach to securing critical infrastructure





groupe e

