OT Cyber Aggregation and Integration with IT Cyber, IOT and Physical Security

Tali Rosenwaks, COO

mPrest

CONNECTING THE DOTS

FROM **IRON DOME**

TO IOE…

From saving lives…

to quality of life

mPrest

CONNECTING THE DOTS

Israeli Cyber authority defines: The National Power Grid as a “Critical Infrastructure”

- Utilities’ infrastructures under more frequent and sophisticated attacks
- DDoS attacks to remove utilities’ ability to communicate with their grid (blackout)
- Difficult to spot attacks, even when happening

IT CYBER VS. OT CYBER GOALS

IT Systems Mainly Deal With Data

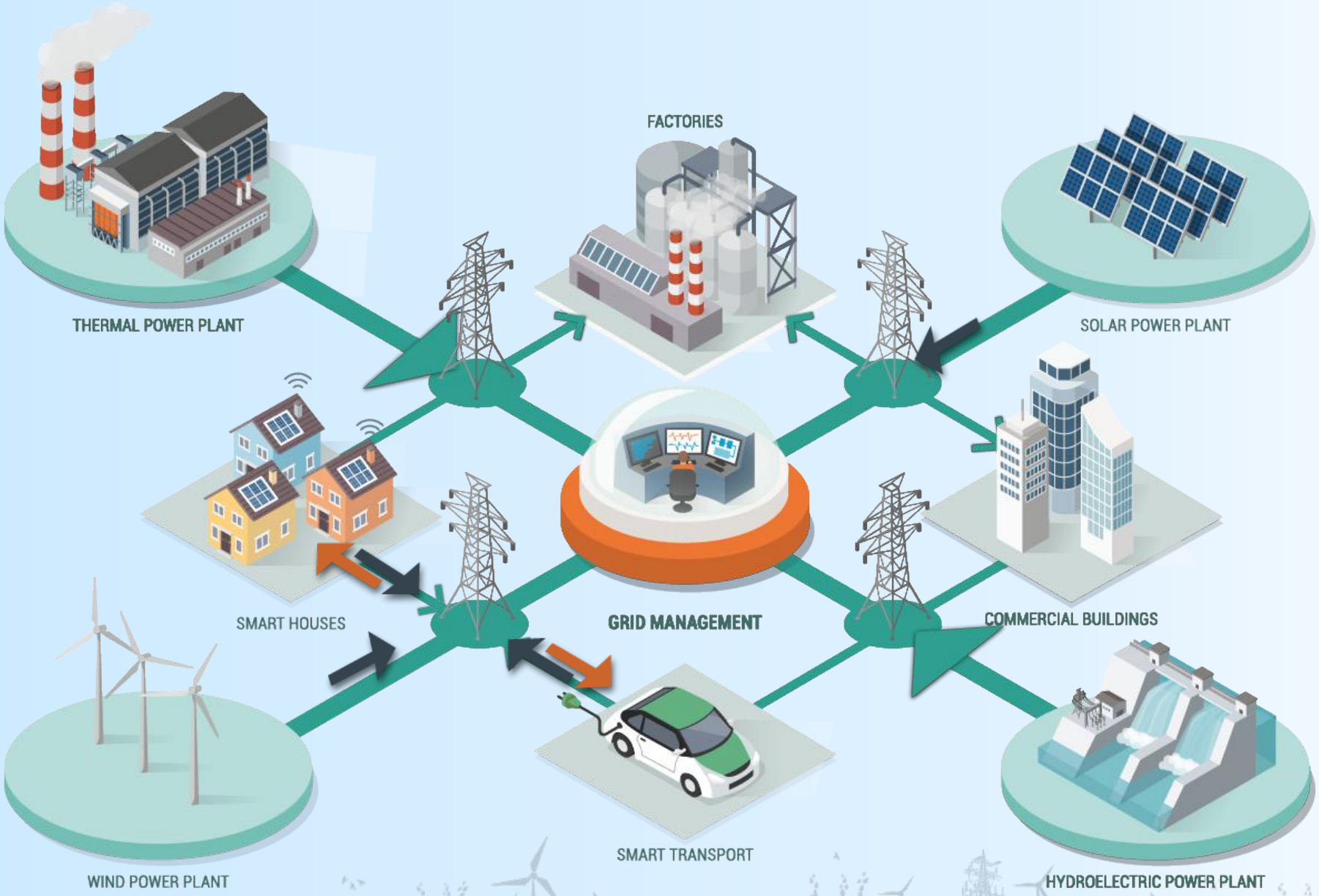
- Assure data confidentiality, integrity and availability

OT Systems Deal With Safety & Reliability

- Prevent damaging of operational assets
- Prevent sabotaging of operational assets
- Prevent damaged operational assets from becoming a safety hazard
- Ensure seamless operation, supply quality, high productivity

CONNECTING THE DOTS

MODERNIZED GRID TRANSFORMATION OLD AND NEW GRID



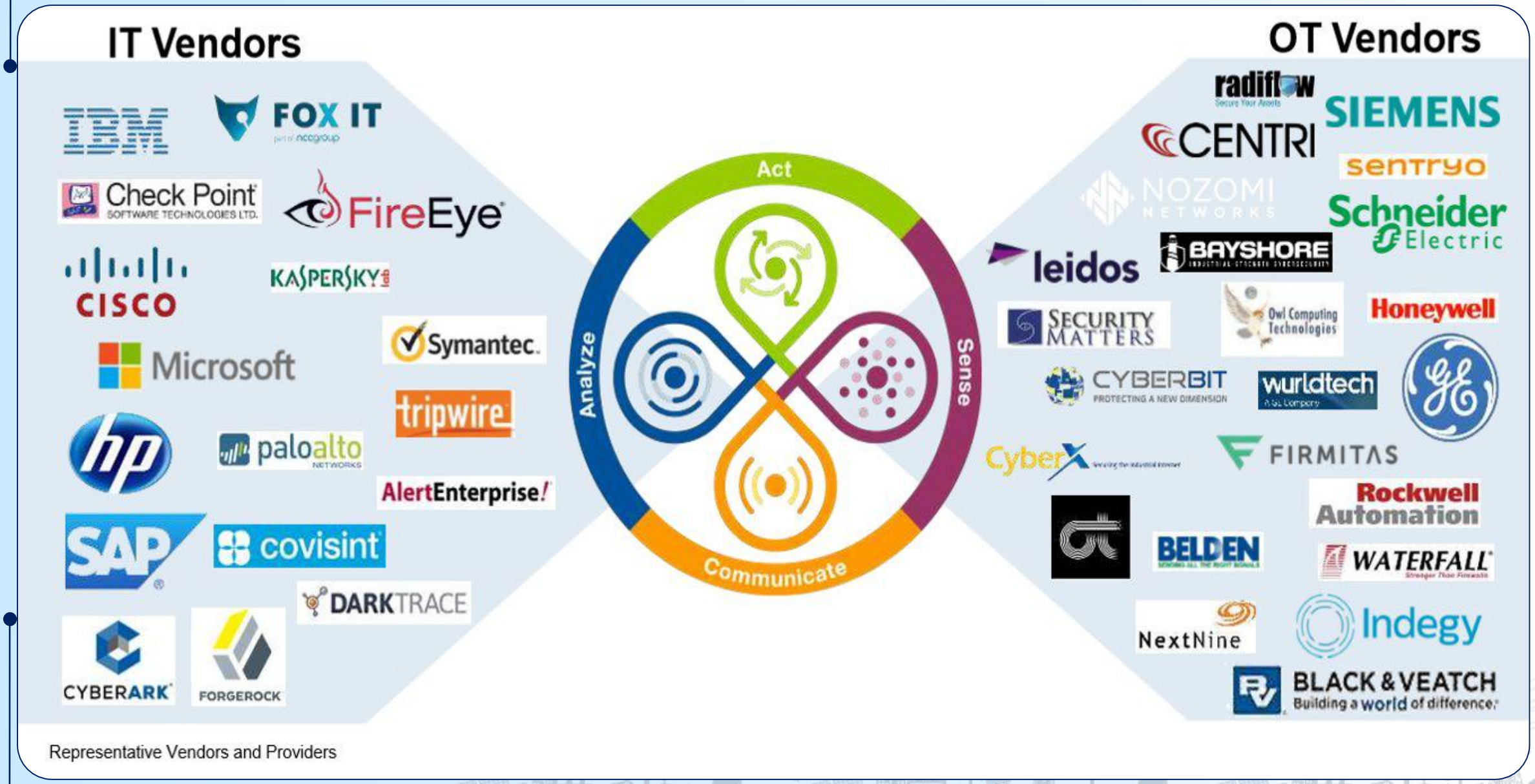
CONNECTING THE DOTS

Cyber Risks on Power Utility

1) Data network between DMS and the substations
2) Internal attack on substations – physical breach
3) Data Network between the substations and DERs
4) Attack on the DMS through the IT
5) Risks caused by remote access
6) Risks caused by Cloud based maintenance
7) Incorrect action by an authorized person
8) Cyber attack “look-a-like” due to fault

mPrest

IT'S A DIVERSE AND FRAGMENTED OT SECURITY MARKET

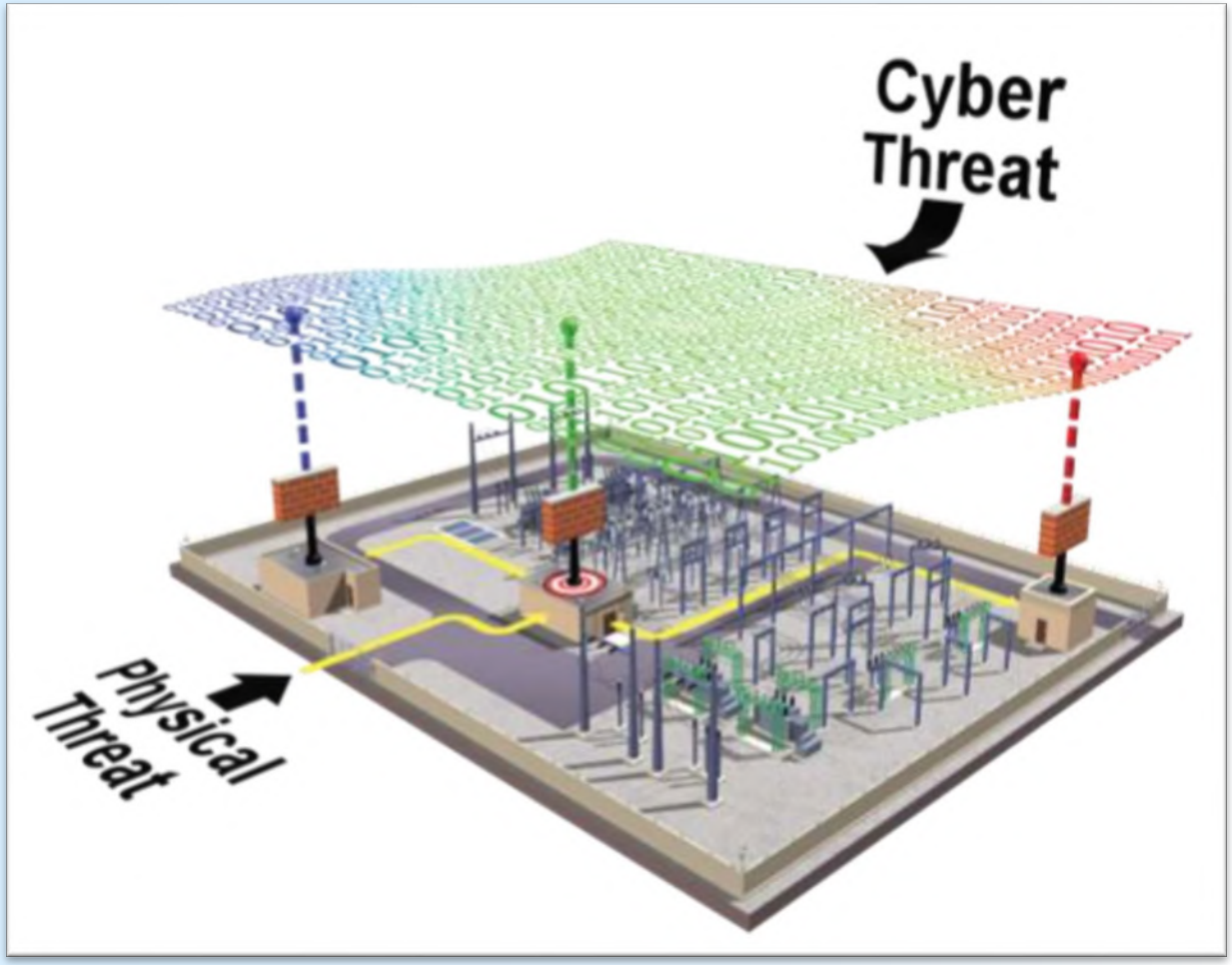


Representative Vendors and Providers

CONNECTING THE DOTS

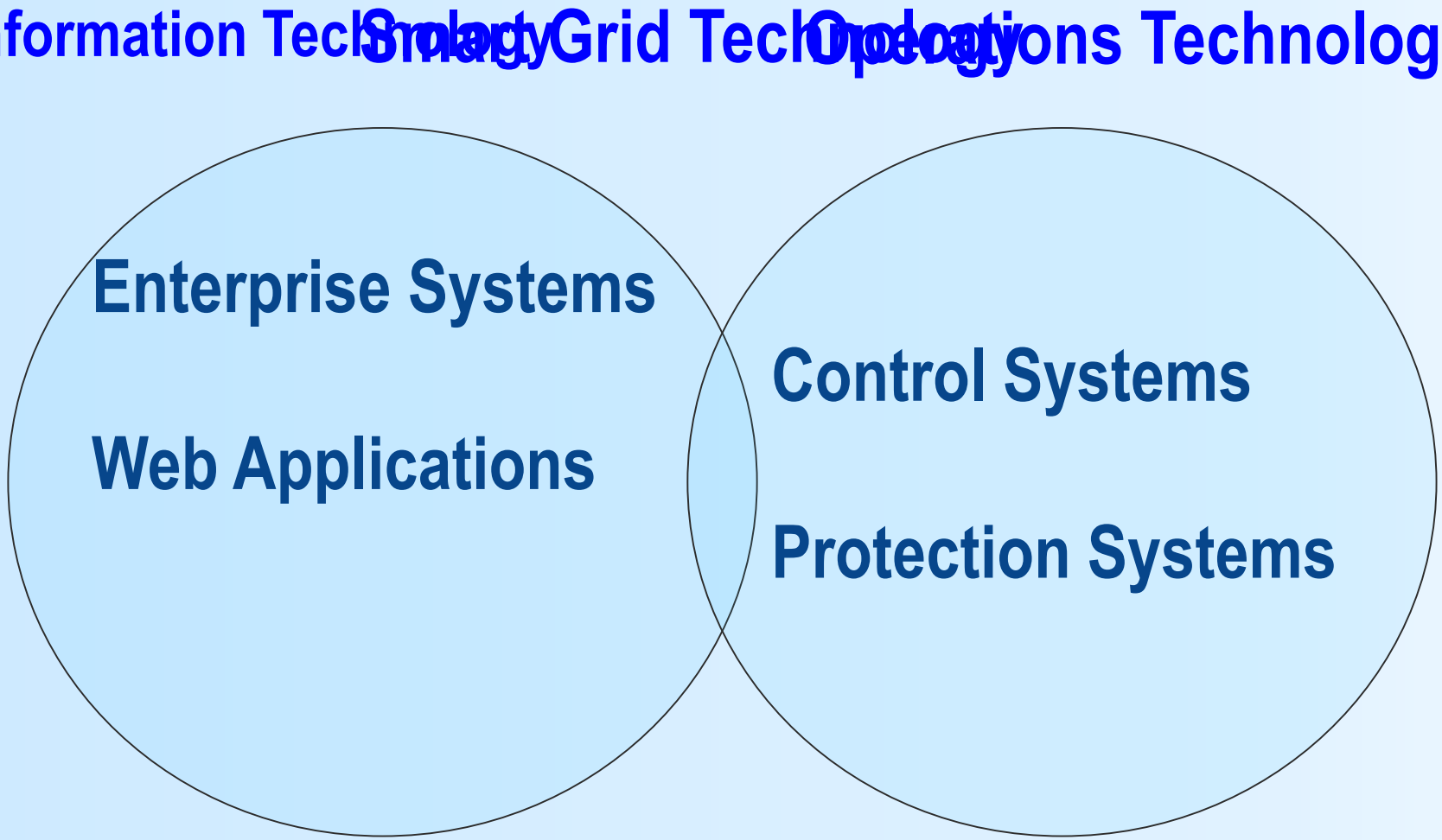
TRENDS OF OT SECURITY IN 2018

- Cyber-Physical convergence is accelerating
- OT and IT security share similar pains
- IT/OT security organizations are converging



CONNECTING THE DOTS

THE SMART GRID IS BRINGING IT AND OT CLOSER TOGETHER



Concerns of Cyber Security

CONNECTING THE DOTS

A Cyber Attack Is Typically Coming With A Physical Attack

A physical attack is a clue

Attack on a California Transformer Could Have Been Dress Rehearsal for Terror Attack on Power Grid

SHARE TWEET EMAIL

BY: Washington Free Beacon Staff
February 5, 2014 10:07 am

An attack on California electrical transformers in April is believed by some to be a practice round for a terrorist attack on the U.S. power grid.

The coordinated attack began outside of Silicon Valley where attackers cut telephone wires at 1 a.m. on April 16, according to the *Wall Street Journal*.

About half an hour later snipers shot at an electrical substation for about 19 minutes, destroying 17 transformers in the process. The attackers escaped before police arrived and remain at large.

It took 27 days to repair the substation and crews had to reroute power around the site using Silicon Valley power plants.

17 Power Transformers were shot, the fiber lines were cut. The snippers cut teleco cables in an underground vault & outsmarted security cameras and motion sensors at the power substation in a remote corner of Santa Clara County.

Snipers Coordinated an Attack on the Power Grid, but Why?

A story seemingly stolen from the pages of a crime thriller, but far less comprehensible.

ALEXIS C. MADRIGAL | FEB 5, 2014 | TECHNOLOGY

mPrest

ASSET HEALTH ALARM MAY BE A CYBER ALERT

- **Standard operation** error notifications
- **Temperature** from sensors (sudden large gaps may indicate attack…)
- **Load** (going up) **temperature** (going down)
- **Invalid data points** (specifics, too many…)
- Extreme abnormalities, **Health Index turns red**

CONNECTING THE DOTS

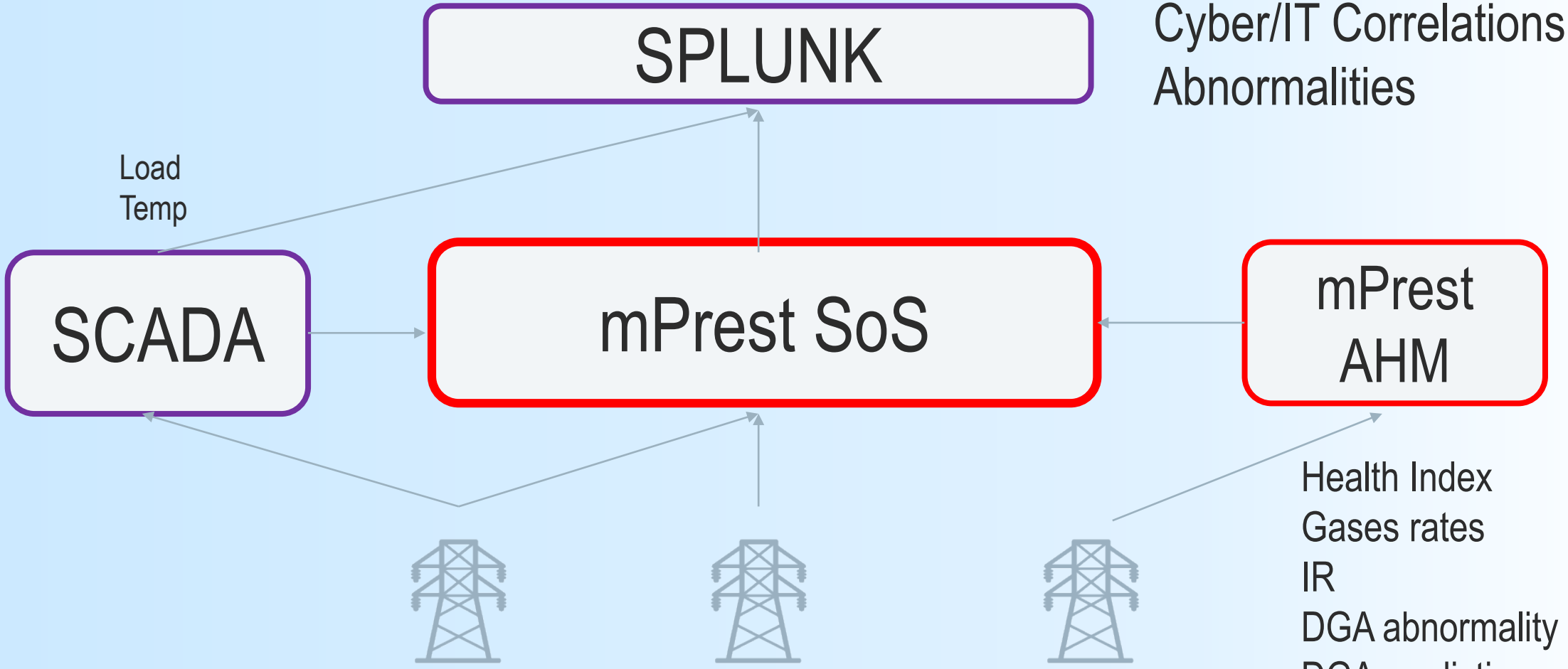
AND MORE ASSET HEALTH ALARM MAY BE A CYBER ALERT

- Any **loss of SCADA or IR communication** (two losses may indicate attack….)
- **Failure** in (multiple) **assets** (in the same time)
- **IR camera detects abnormality** in the temperatures gaps
- **Login / Fail**ed login detected (unauthorized?)
- **Any significant user / accounts activity** (reinstallation, configuration change, password change, user account creation etc…)

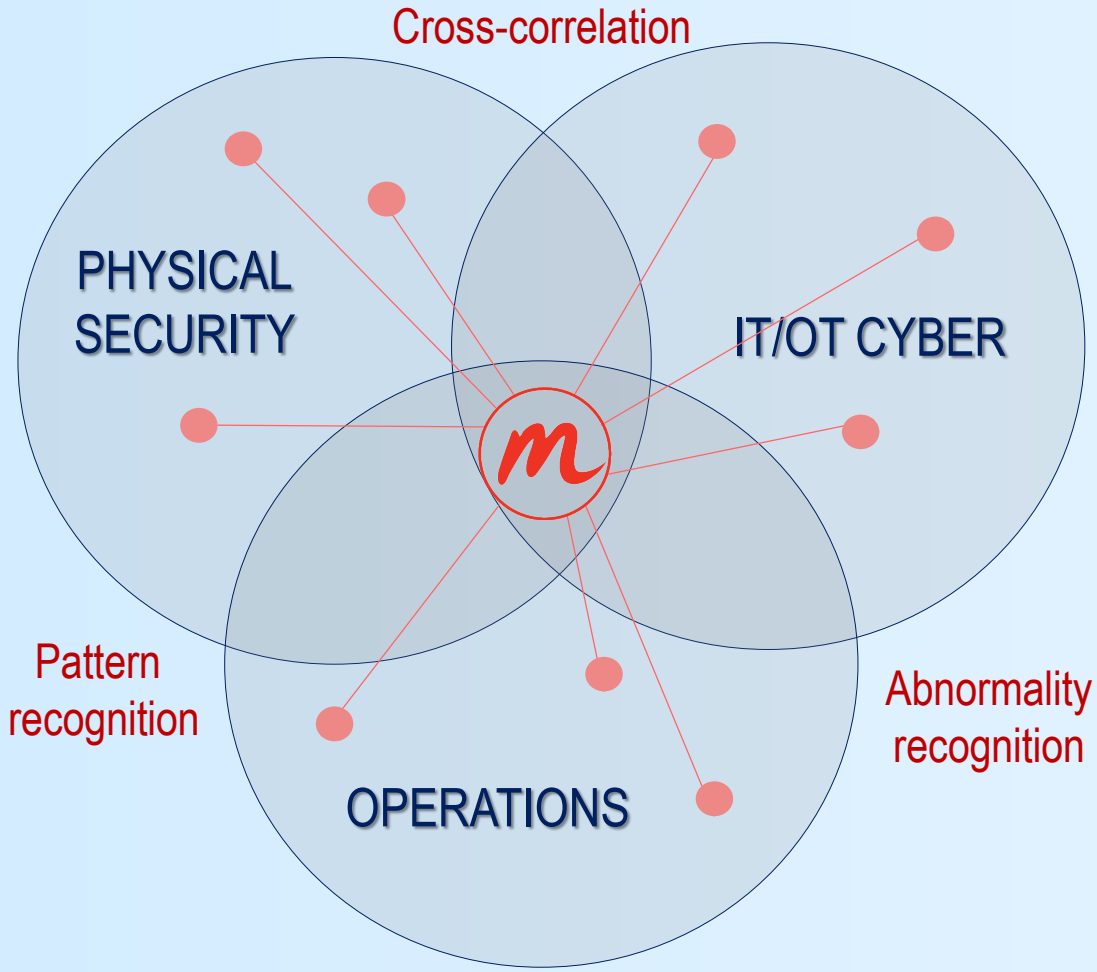
mPrest

CONNECTING THE DOTS

mPrest SoS and SPLUNK Integration Concept



CONNECTING THE DOTS



CONNECTING THE DOTS

mPREST SECURITY PLATFORM

SYSTEM OF SYSTEMS

OT Cyber Security
- Detection Engines
- Asset Discovery
- Analytics
- User Behavior
- Other

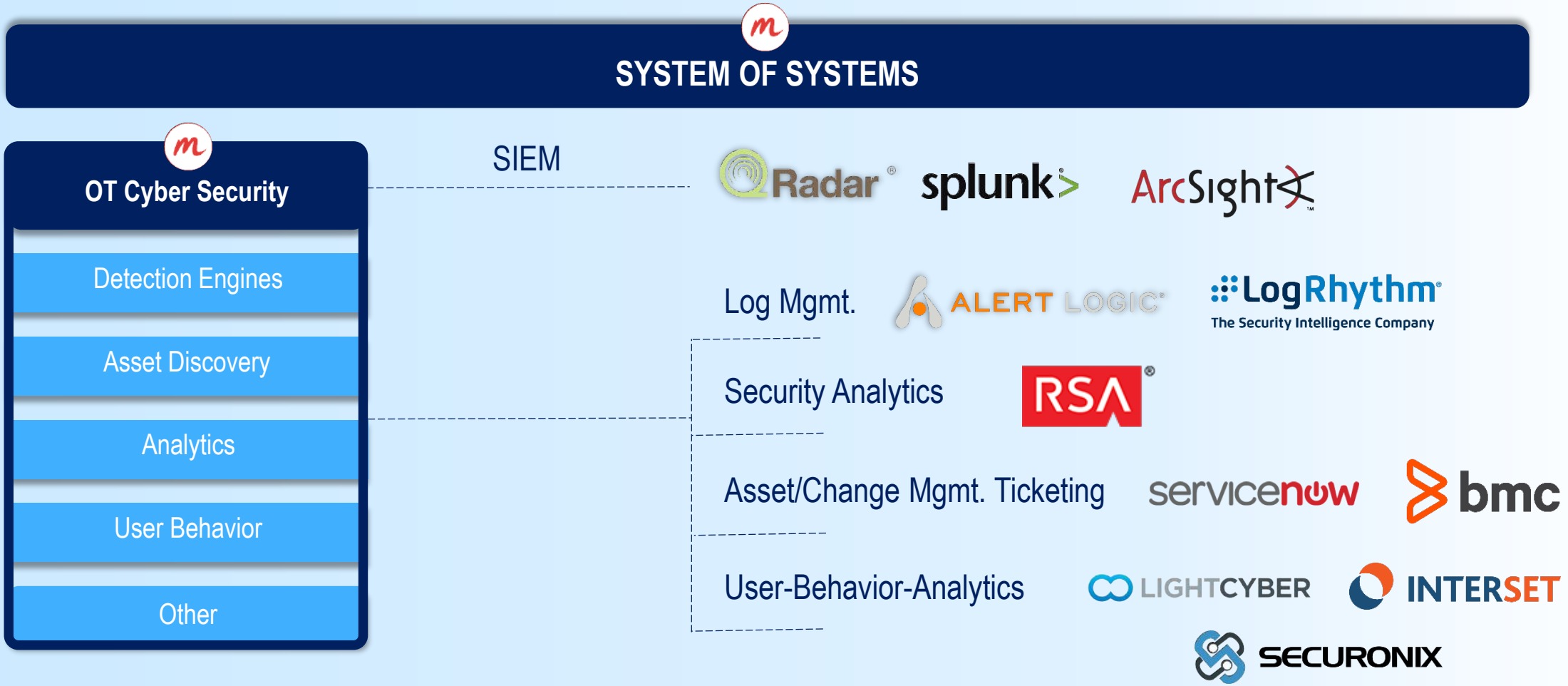
IT Cyber Security
- Intrusion Detection
- Forensics
- Cloud Protection
- End point Protection

IOT
- Device Protection
- Asset Management
- Access Management
- Asset Health Management
- DERMS

PSIM
- Access Control
- Cameras & Video Analytics
- Perimeter Protection
- Biometric Scanners

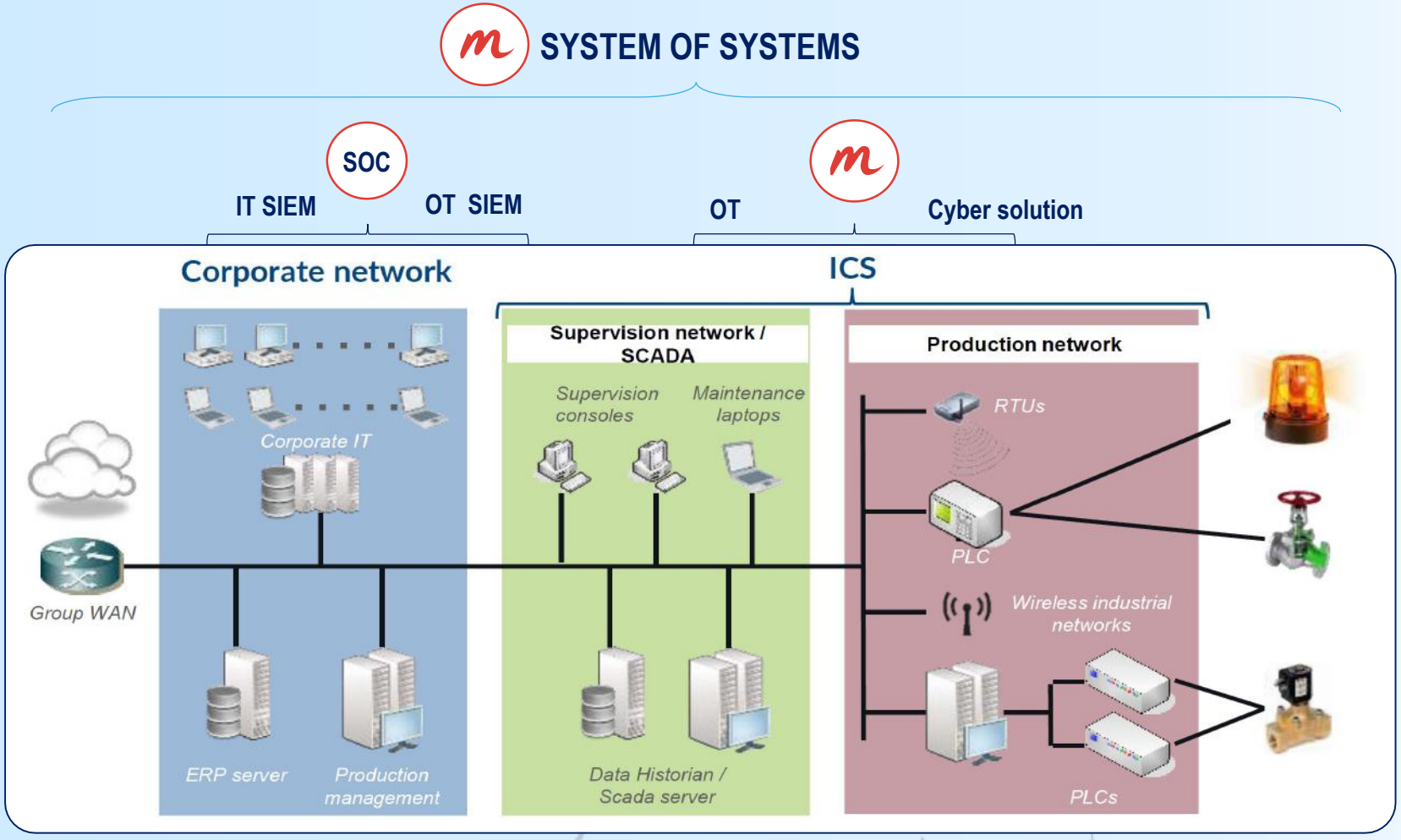
CONNECTING THE DOTS

mPREST SECURITY PLATFORM



CYBER SECURITY POWER PLANT CONFIGURATION

What is Industrial Control System?



SUMMARY

- Utilities will be investing significantly more in Cyber Security
- The only true holistic cyber solution would be one which fully integrates between Physical Security, IT Cyber Security, OT Cyber Security and Online Operational Asset Condition

mPrest

Thank you