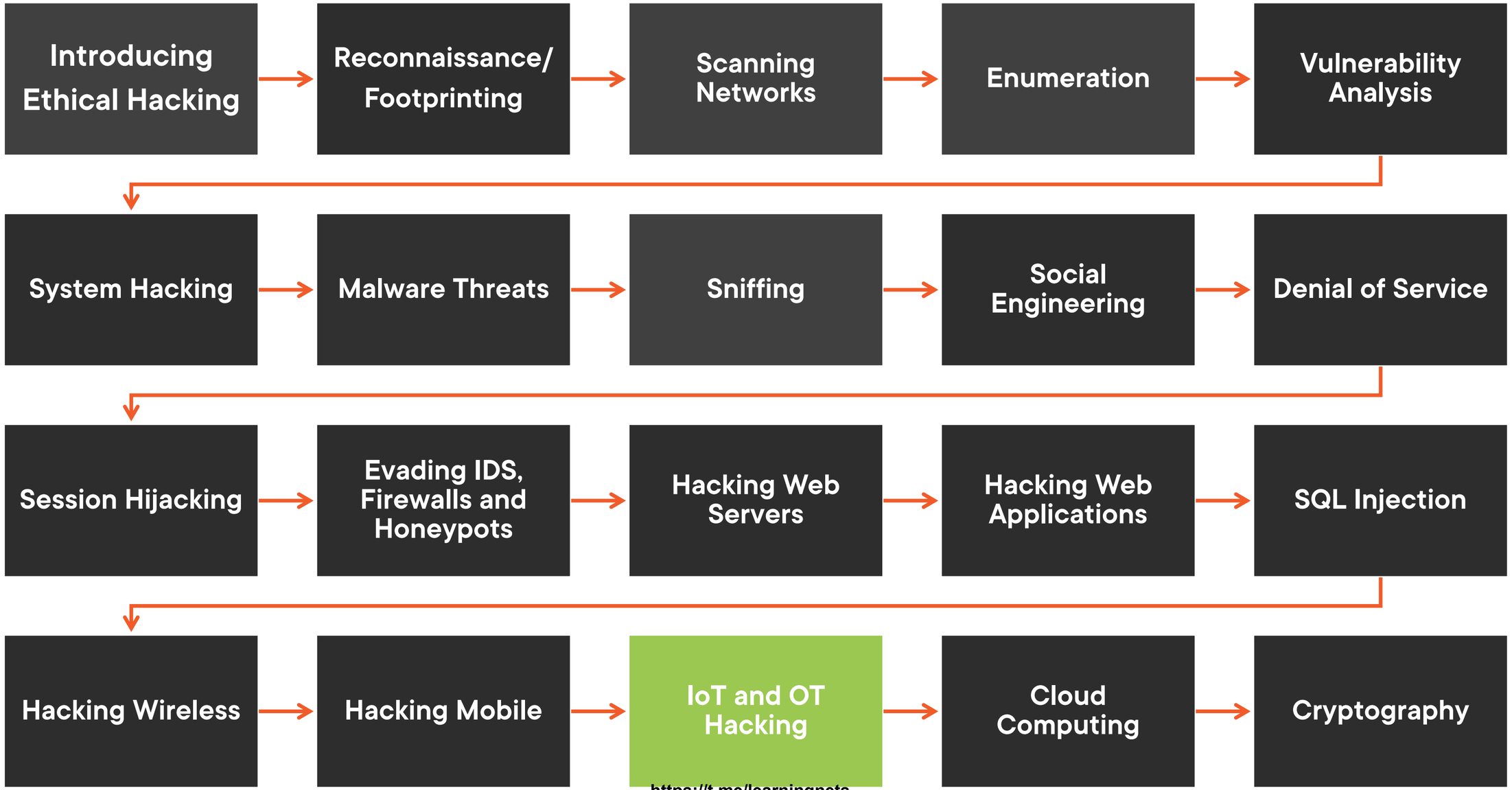
Ethical Hacking: Hacking IoT and OT

Investigating IoT and OT Concepts

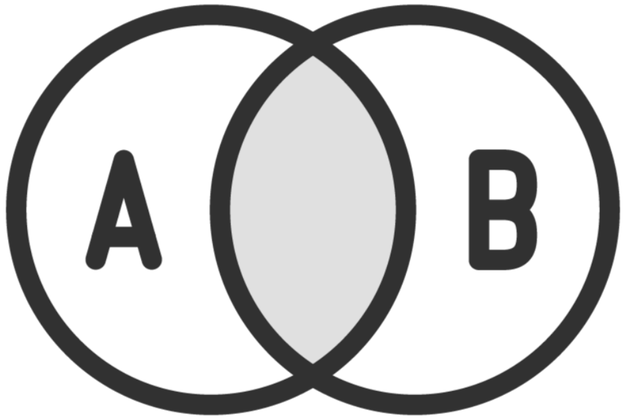
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

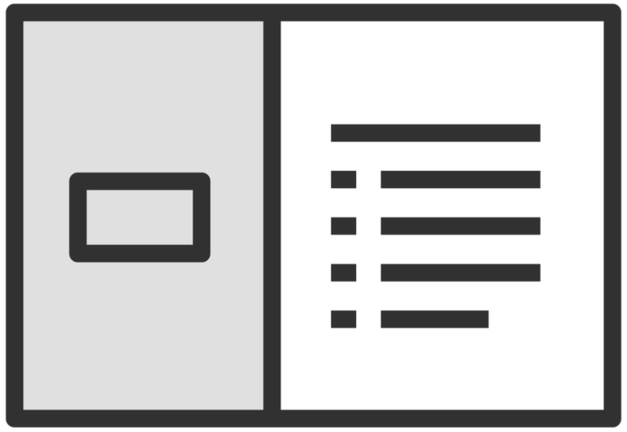
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Ethical Hacking Series

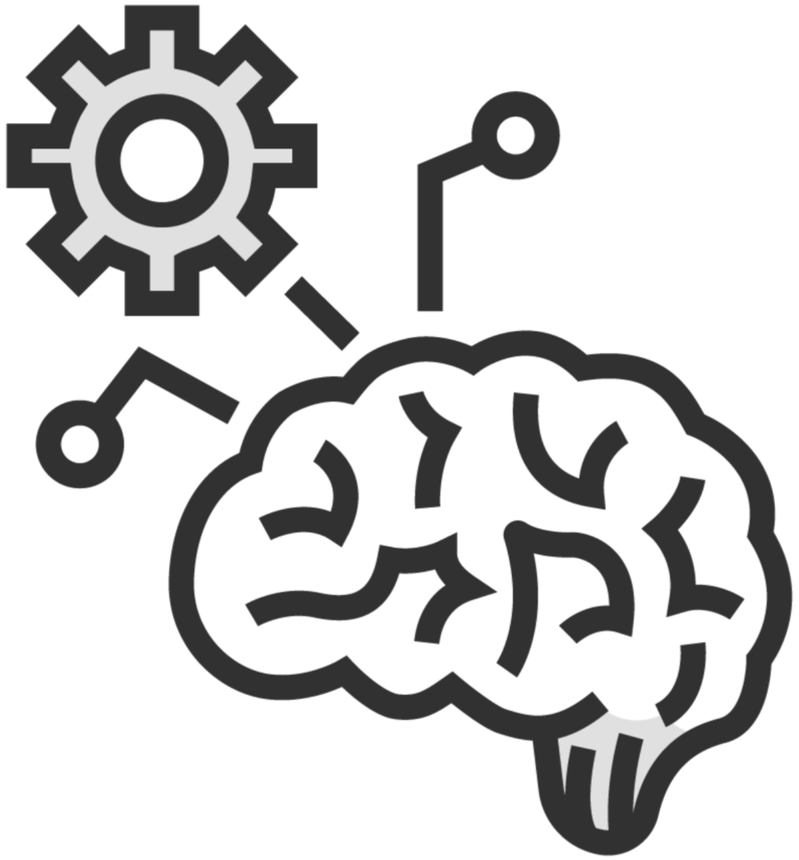


The Method behind My Madness





The Method behind My Madness

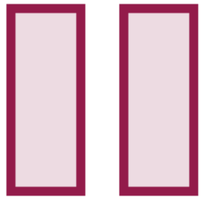


CEH Exam Study Tips

Dale's Study Tips

Study space

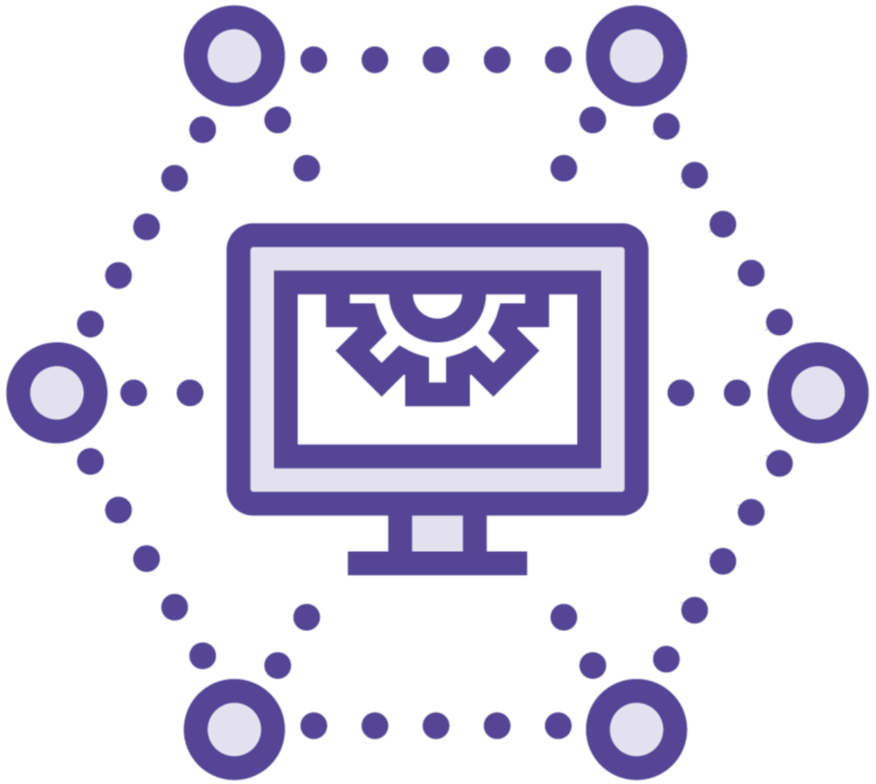
Take notes



Pause, think, repeat

Be kind and rewind

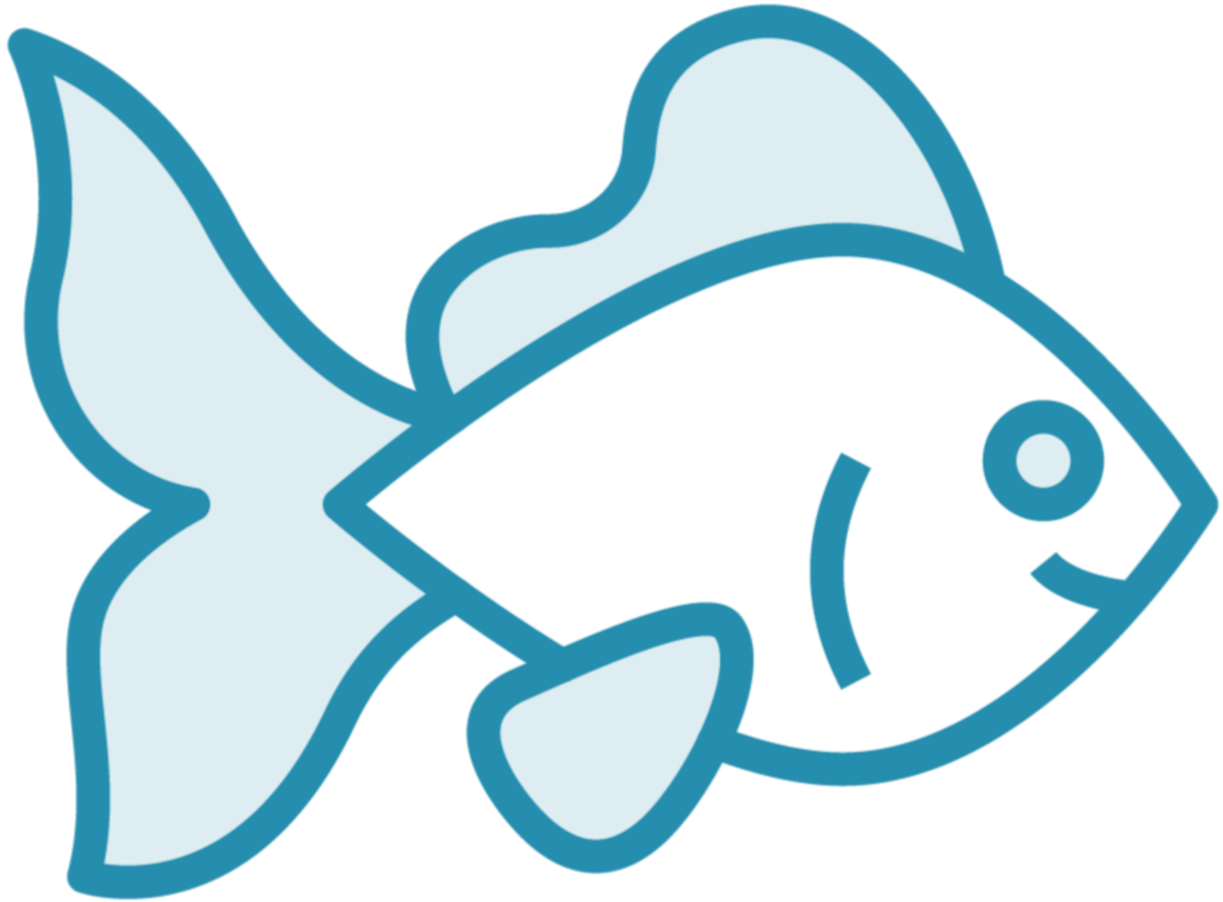
Dale's Study Tips



Understanding IoT and OT

“Despite continued security problems, IoT will spread, and people will become increasingly dependent on it. The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive.”

Richard Adler



Exploring

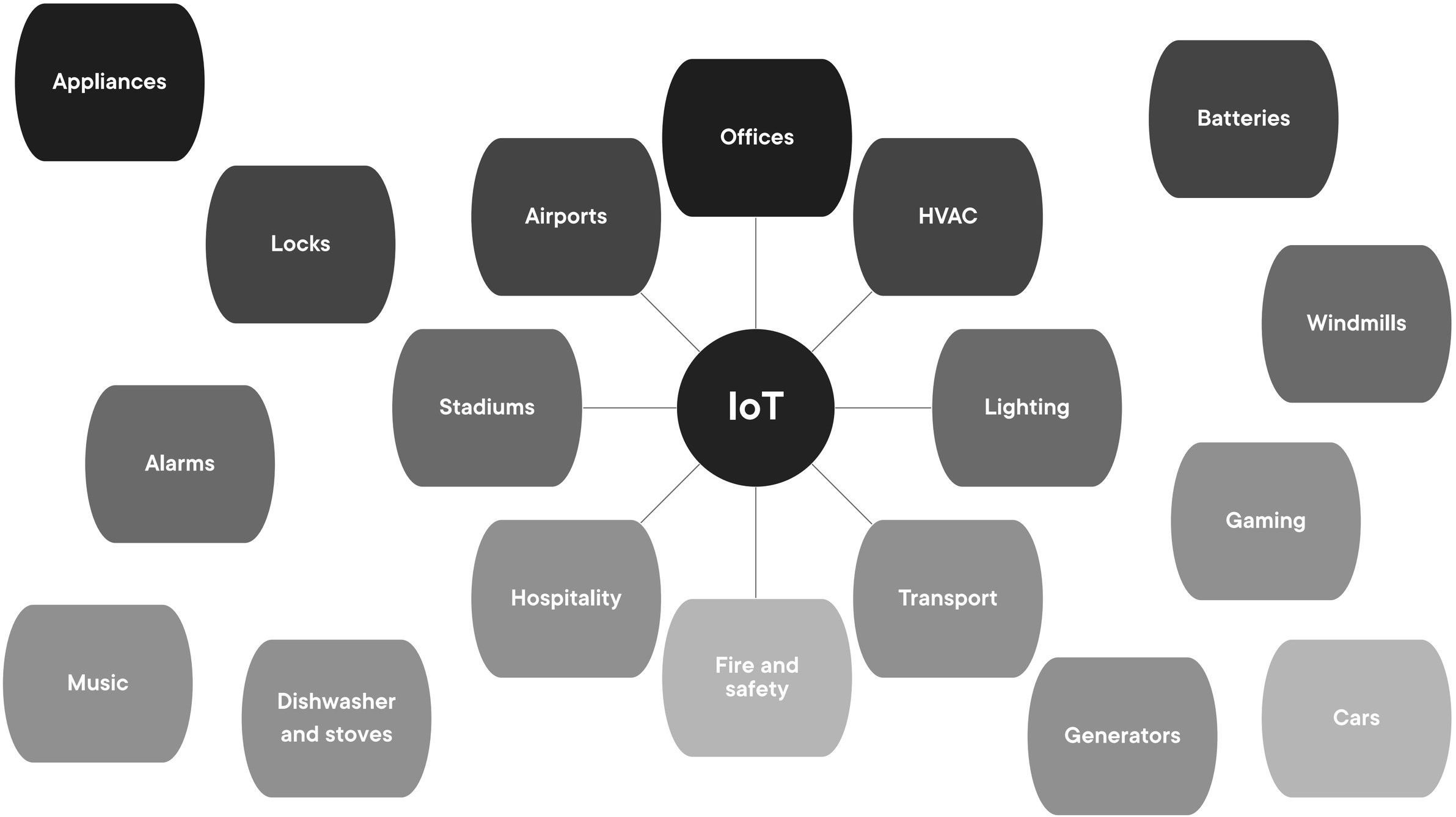
Understanding of IoT

IoT Hacking

IoT Methods

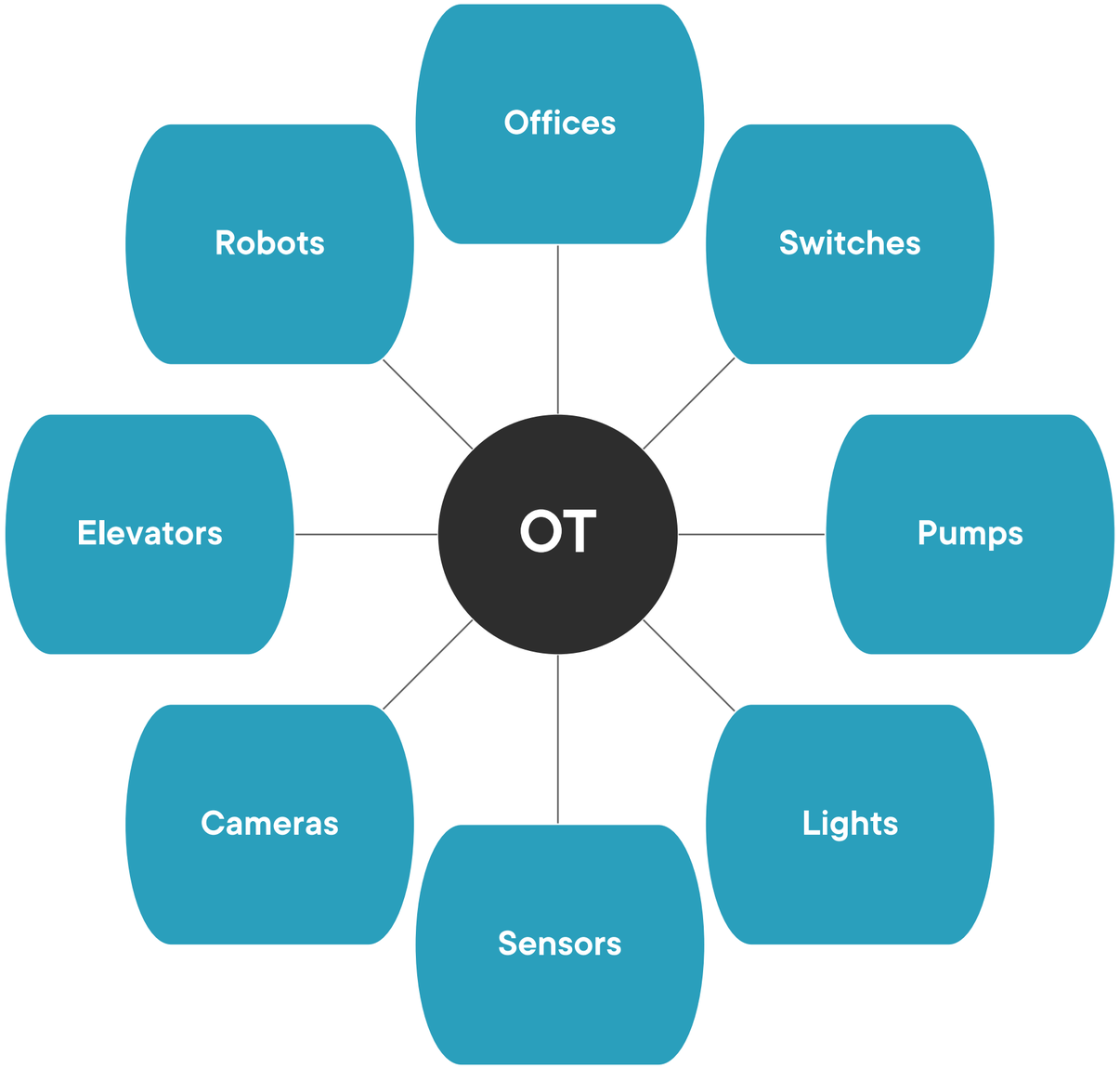
What is OT

OT Hacking

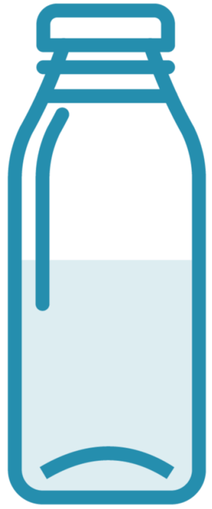


OT

Software and hardware designed to detect or cause changes in industrial operations through direct monitoring or controlling of industrial physical devices



- Industrial Control Systems (ICSs)
- Supervisory Control and Data Acquisition (SCADA)
- Remote Terminal Units (RTU)
- Programmable Logic Controllers (PLC)
- Distributed Control Systems (DCSs)



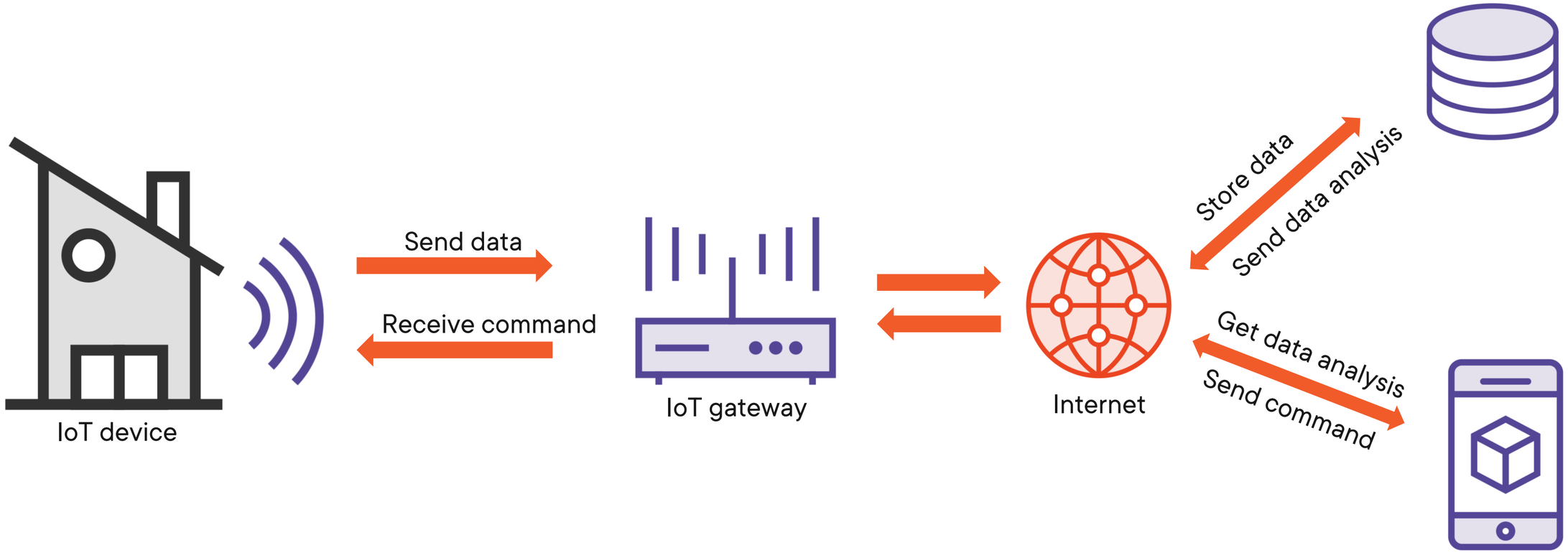
Changing Lives

Baby monitor
Smoke detector
Doorbell
Security alarms

and more...

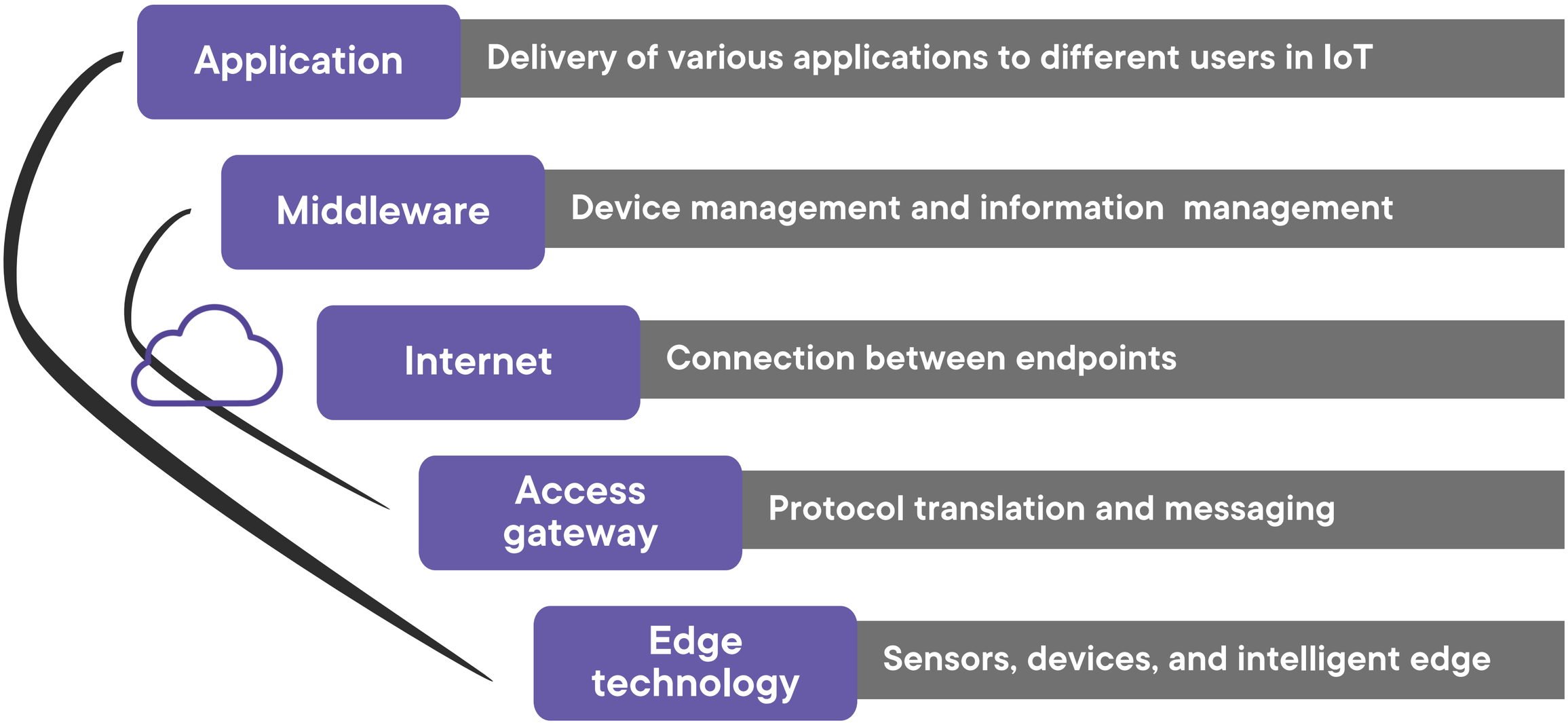
The Architecture of IoT

How Does It All Work?



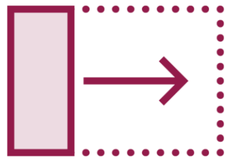
The Architecture of OT

IoT Architecture

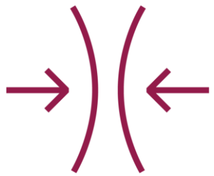


What is OT?

Technologies that work together as integrated or as a homogeneous system

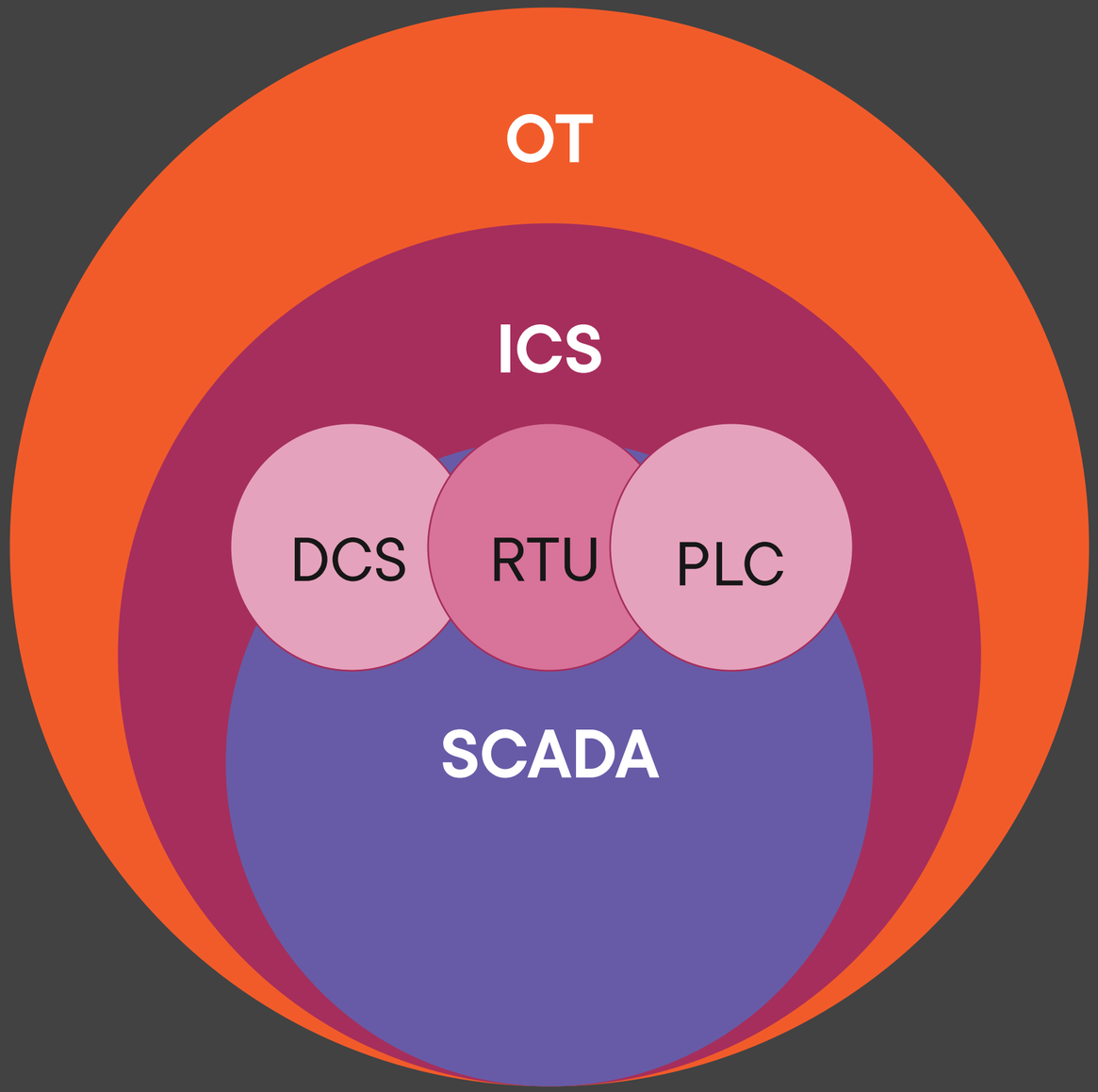


Telecommunications uses OT to move data from the electrical grid to the wheeling station



Financial transactions use OT between electrical consumers and producers

OT is used to monitor, manage and control industrial process assets



OT Components

- Assets
- Zones and conduits
- Industrial network
- Business network
- Industrial protocols
- Network perimeter
- Electronic security perimeter
- Critical infrastructure

Protocols and Technologies for IoT/OT

Short-range Communications

Z-Wave

ZigBee

Wi-Fi

Wi-Fi direct

Radio Frequency Identification (RFID)

Short-range Communications

Bluetooth smart or Bluetooth LE

Light fidelity (Li-Fi)

Near Field Communications (NFC)

Quick response (QR) codes

Mid-range Communications

HaLow

Transmits twice as far and doesn't require a true line of sight

LTE-Advanced

Stronger than standard LTE with a higher capacity to transmit data

Long-range Communications

Low-powered wide-area (LPWAN)

SigFox / Nuel

Very Small Aperture Terminal (VSAT)

Cellular

Ethernet

Multimedia over Coax Alliance (MoCA)

Power-Line Communication (PLC)

Operating Systems

IoT Operating Systems

ARM Mbed

Zephyr

Ubuntu Core

Apache Mynewt

RIOT

IoT Operating Systems

Brillo

Real-time Operating Systems (RTOS)

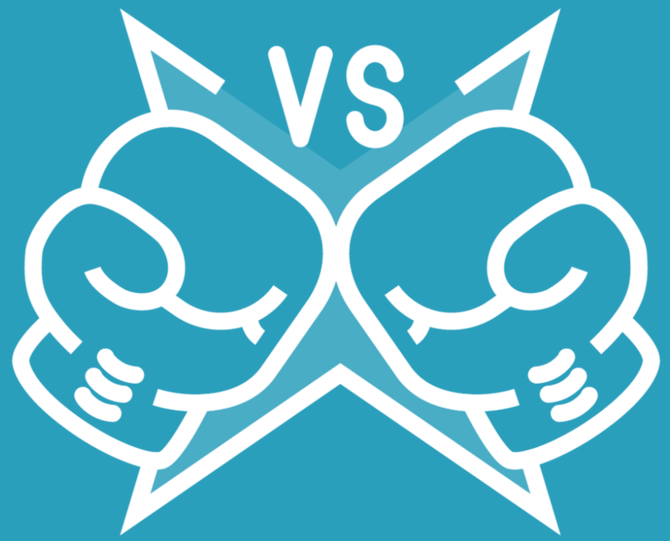
Zephyr

Windows 10/11 IoT

Amazon Free RTOS

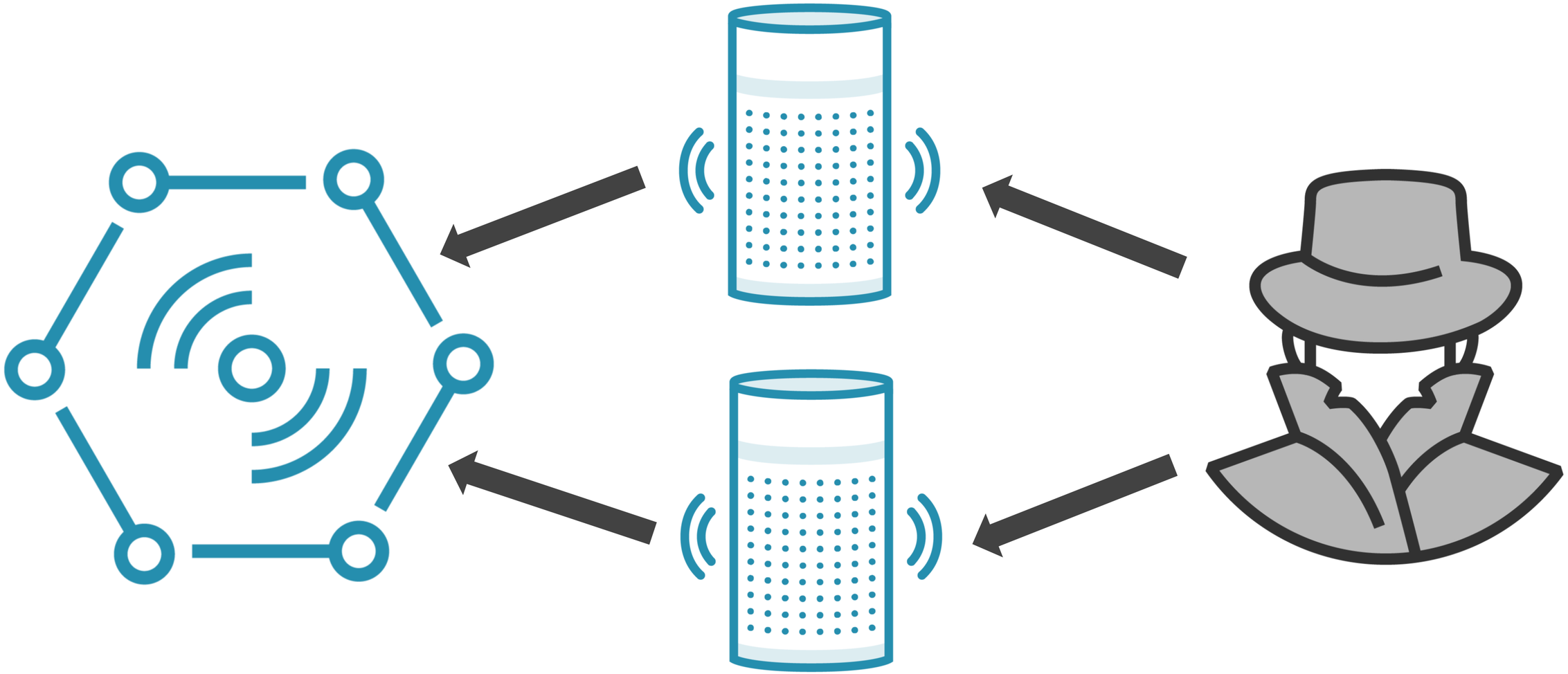
Challenges of IoT/OT

Challenges

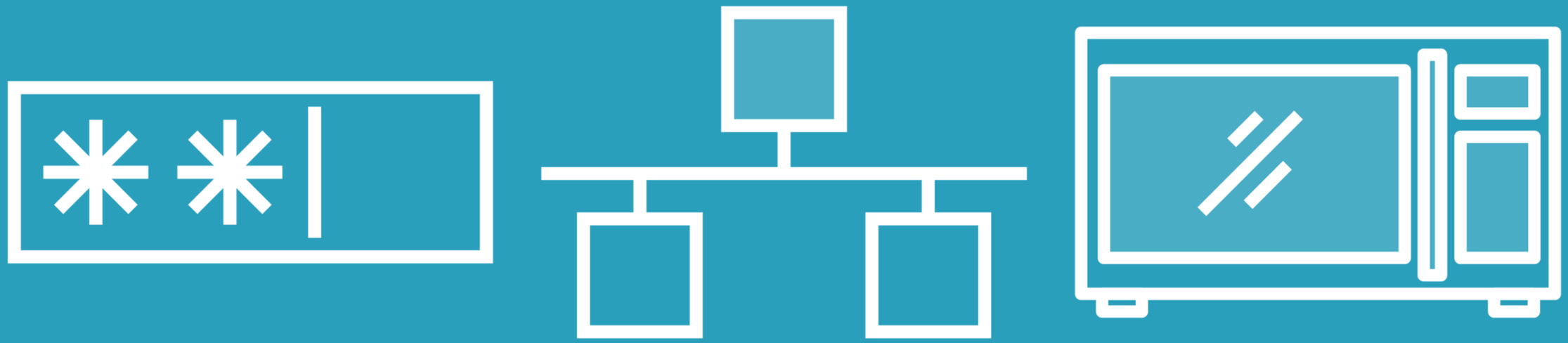


Non-interoperability between systems

Fails to test how the device integrates with other devices



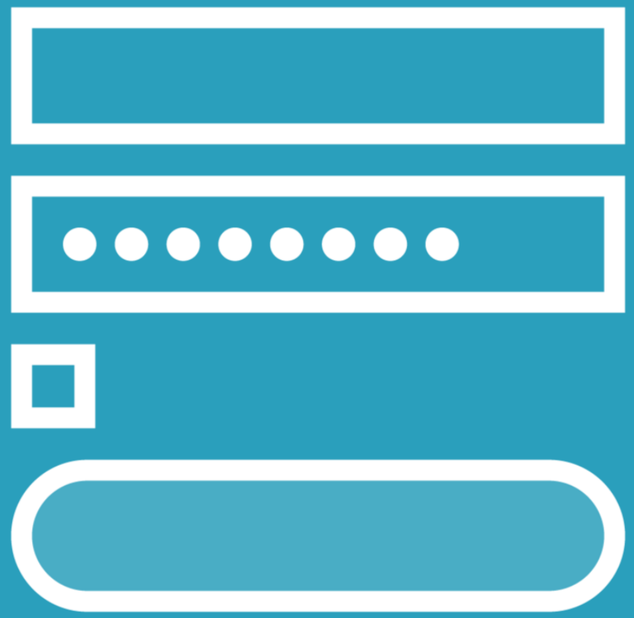
Security and Privacy Challenges



System Update Support

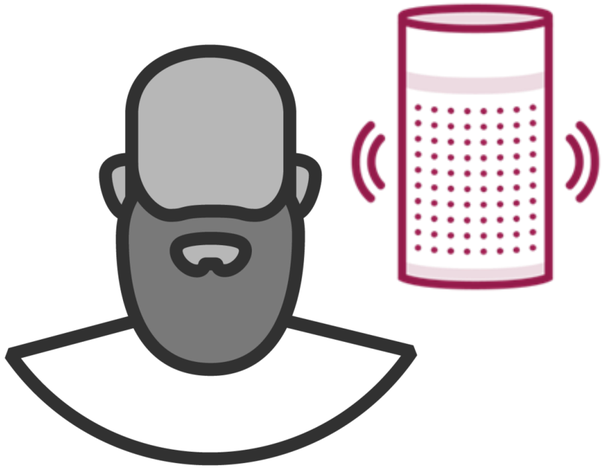
Legacy Technology Challenges

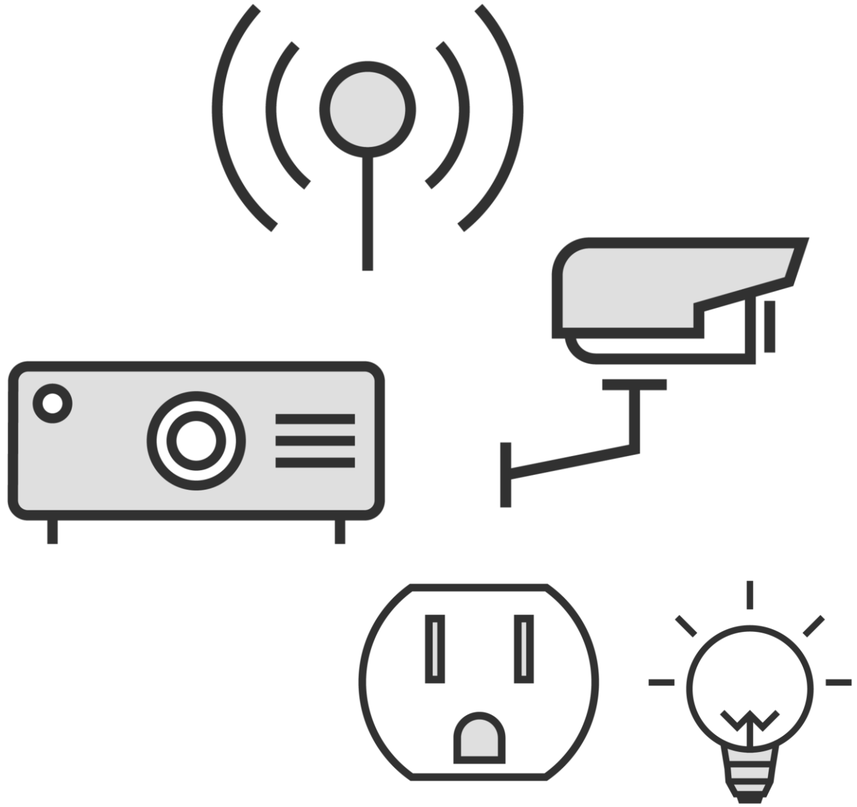
Storage Challenges



Vulnerabilities

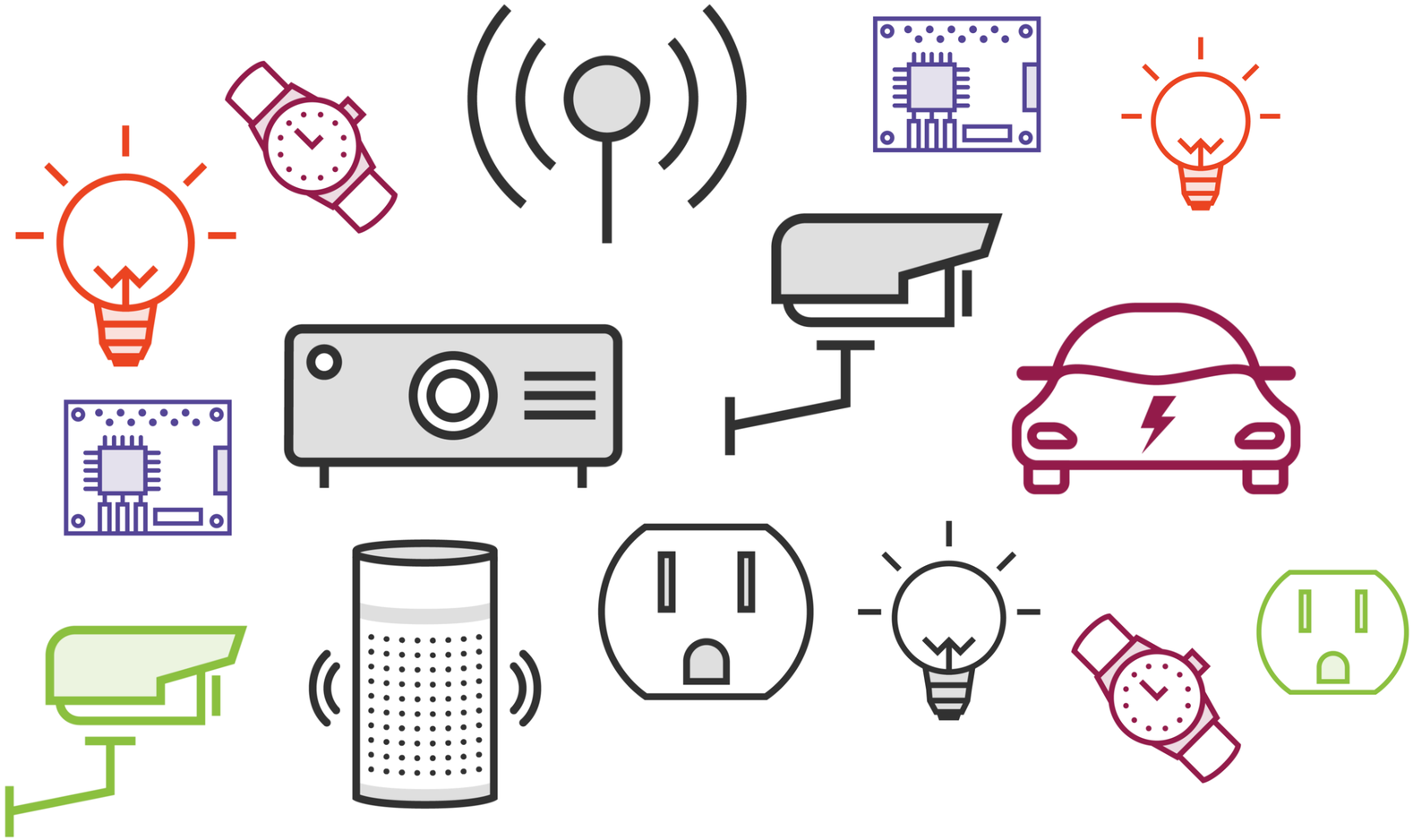
Physical Attack





Insecure Web interfaces

Development Insecurities



Vendor Support

Regulatory and Rights

Securing OT

Securing OT



Built to monitor and control not to protect

Limited access to information

Industrial Control System (ICS)

SCADA

DCS

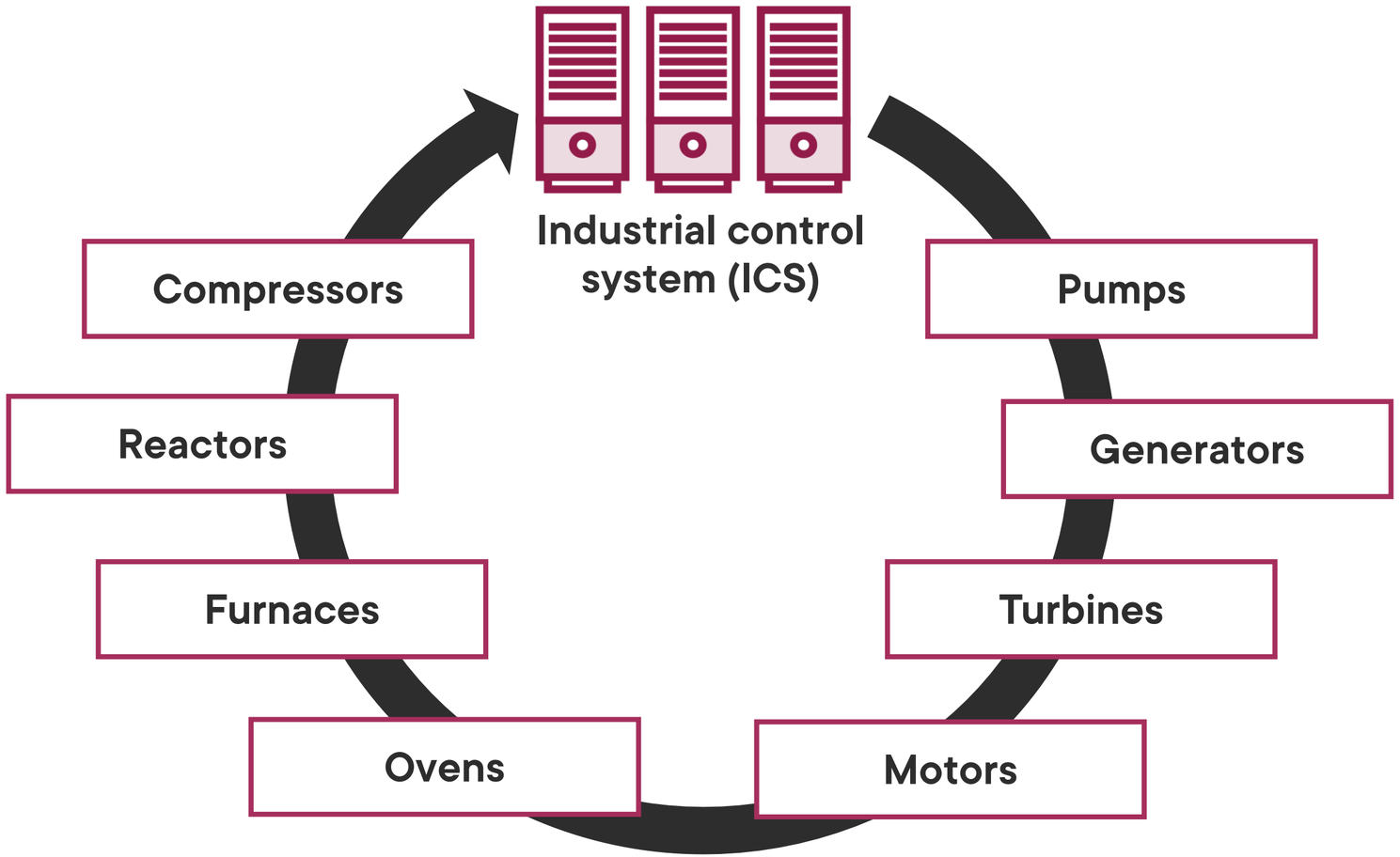
PLC

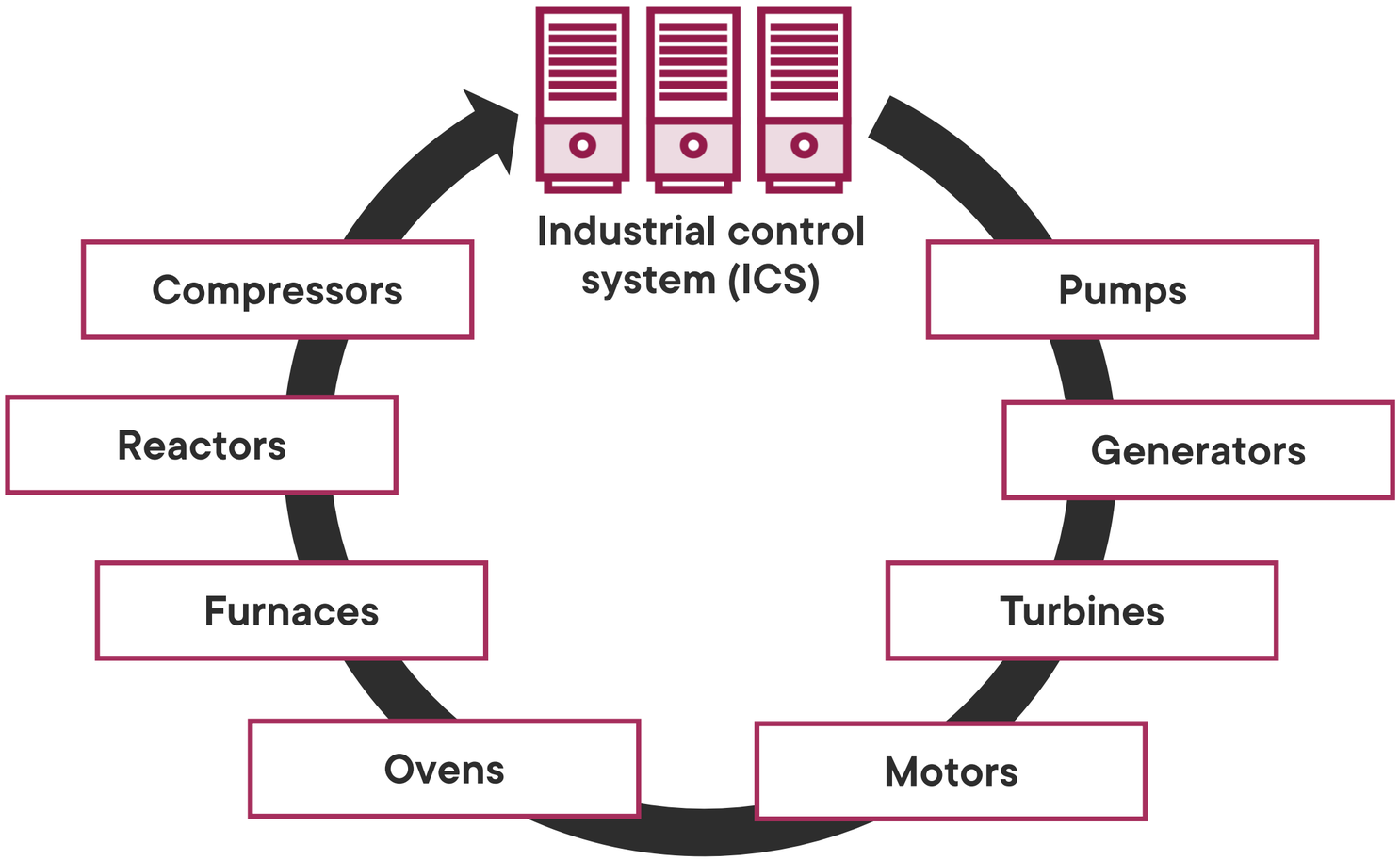
HMI

BPCS

SIS

IED





ICS Operation Modes

Open-loop

Closed-loop

Manual-loop

Learning Check

Learning Check

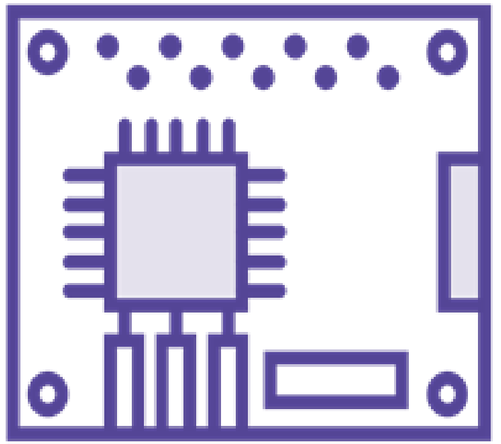
IoT Gateway

Internet Layer

Edge Technology Layer

Z-Wave or ZigBee

RTOS



Up Next:
Reviewing IoT and OT Attacks