



By: Krishnan Thiruvengadam

Securing IOT - Challenges

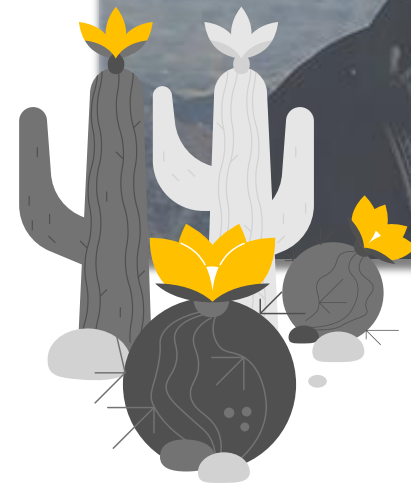


Connecting machines and people securely

About me



Home in Boston till 2015

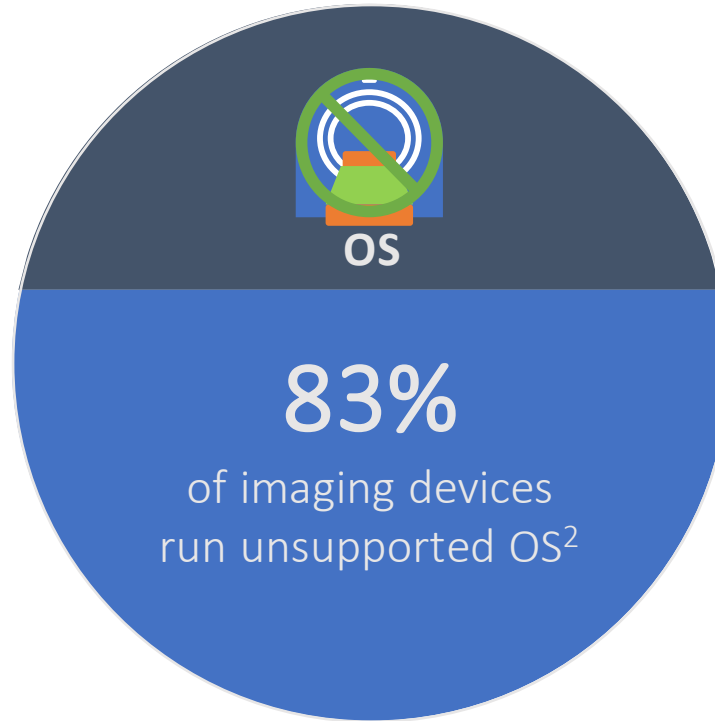


Warm California

Agenda

- Challenges in IOT
- Threats from Unsecured IOT
- IT and OT Convergence
- What do we need to do?
- Executive order highlights

Challenges in IOT



¹ [A-critical-look-at-gartners-top-10-iot-trends.html](#)

² [iot-threat-report-2020](#)

Threat from unsecured IOT

Reconnaissance



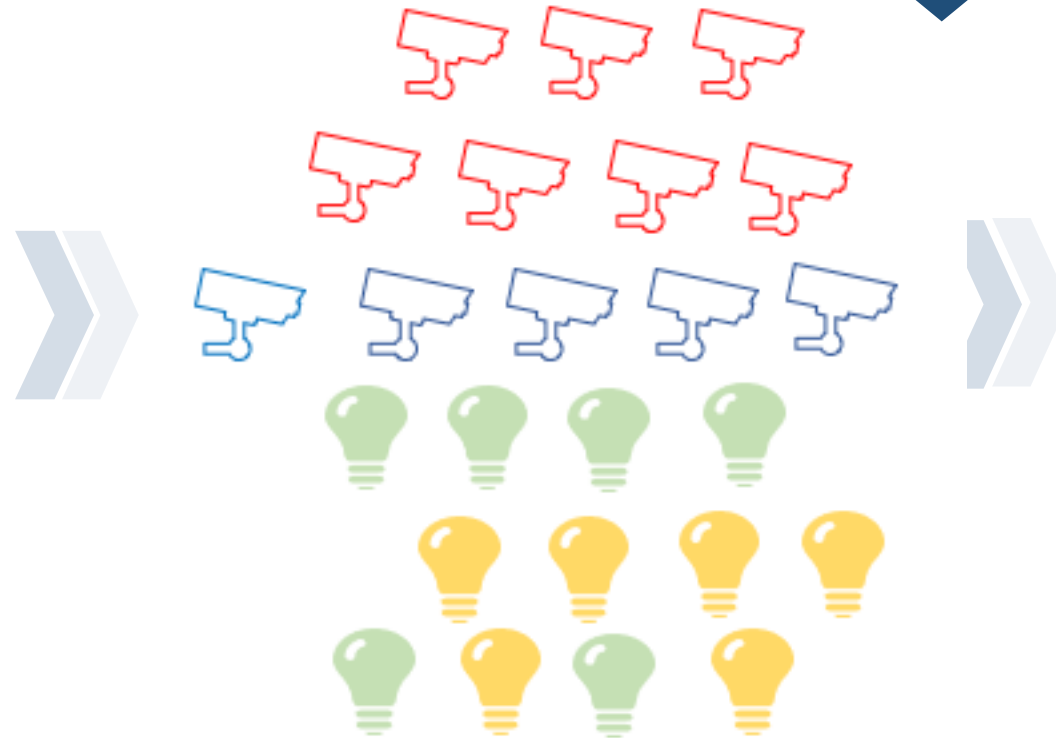
Targeting



Breach



Examples:
MIRAI
WannaCry
Peekaboo



Data Theft

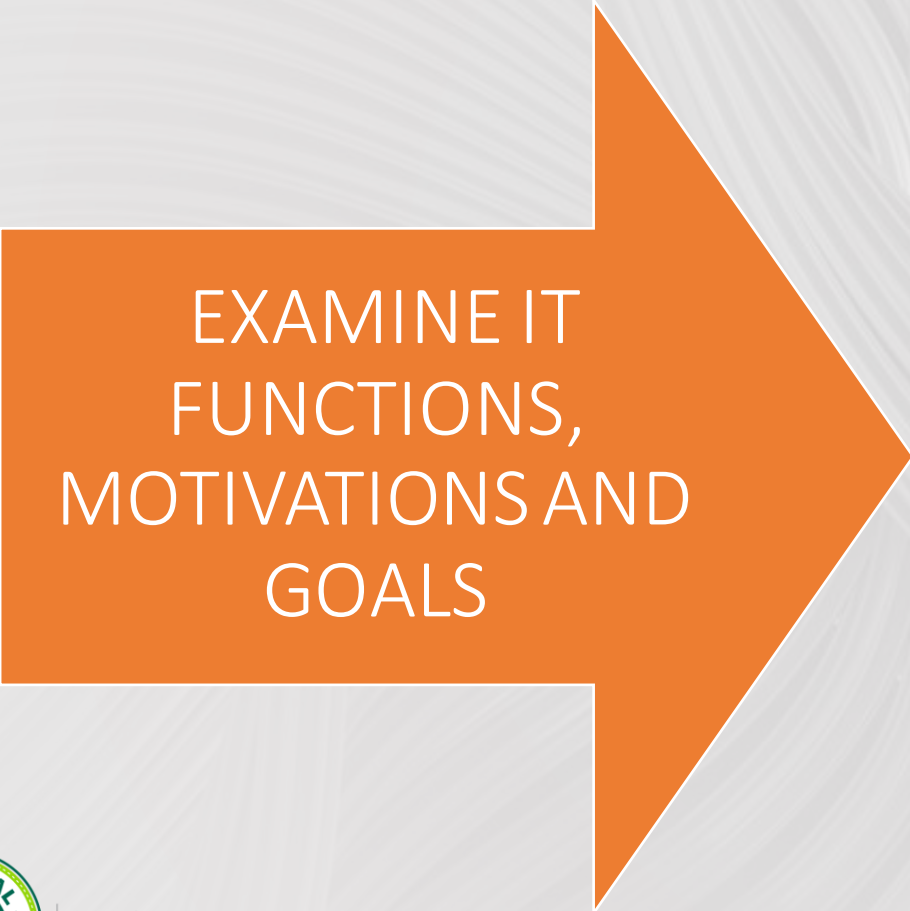
Data Tampering

Ransomware

Denial of Service

Unsecured IoT can be the attack target as well as the route to expanded network attacks

IT and OT convergence



EXAMINE IT
FUNCTIONS,
MOTIVATIONS AND
GOALS



UNDERSTAND THE
OT ENVIRONMENT
AND HOW IT
CHANGES



EAST BAY

IT and OT Convergence

IT

Function: Manages networking, compute, storage, security of data

Objective: Logical security (human error, cyberattack, natural disaster risk management)

Main priority: Data Security (confidentiality)

Access: Connected to outside world

Frequency of change: Constantly changing (people and devices)

Interface: Web browser, keyboard, device

Life Cycle: Short (3-5 years)

Operating System: Standard OS

OT

Function: Control of process, tool and function of the IOT

Objective: Protect environment, people, infrastructure

Main priority: Uptime, availability and integrity

Access: Restricted access with special privileges

Frequency of change: Less to no change

Interface: No interface, limited browser access

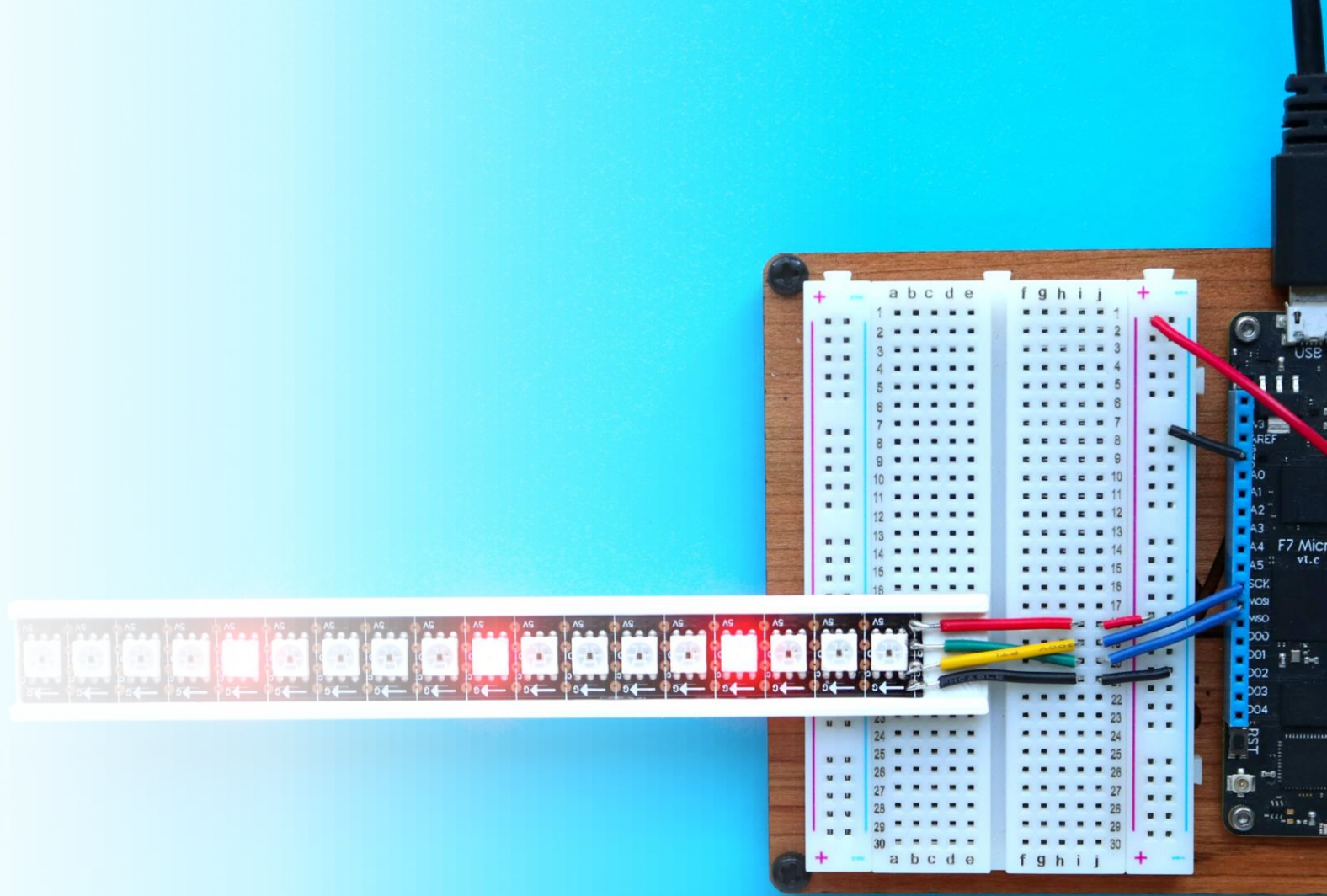
Life Cycle: Long, 15 to 20 years

Operating system: Custom OS

What do we need to do?




KNOW your
endpoints and
understand
their behavior





DO the right
access control





TRUST nothing
until
understood



REMEDiate as
needed





Secure the data and data path



Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

SCOPE

IT and OT

Prevention, detection, assessment, remediation
of cyber incidents

Key aspects of executive order

01

Modernizing Federal Government Cybersecurity.

- **Zero Trust**, XaaS, Data Analytics to manage Cybersecurity risks

02

Improving Detection of Cybersecurity Vulnerabilities and Incidents

- Early detection using EDR for active cyber hunting, containment and remediation

Thank You.

