

Summit

26 June 2024,
11:25-11:40 CST

Speaker

IoT Security Best Practices for Customer Trust

赢得客户信任的物联网安全最佳实践



James Lai,

Chairman
Malaysia IoT Association

James Lai, 马来西亚物联网协会主席

Hosted @ **MWC**
GSMA

Platinum sponsor:

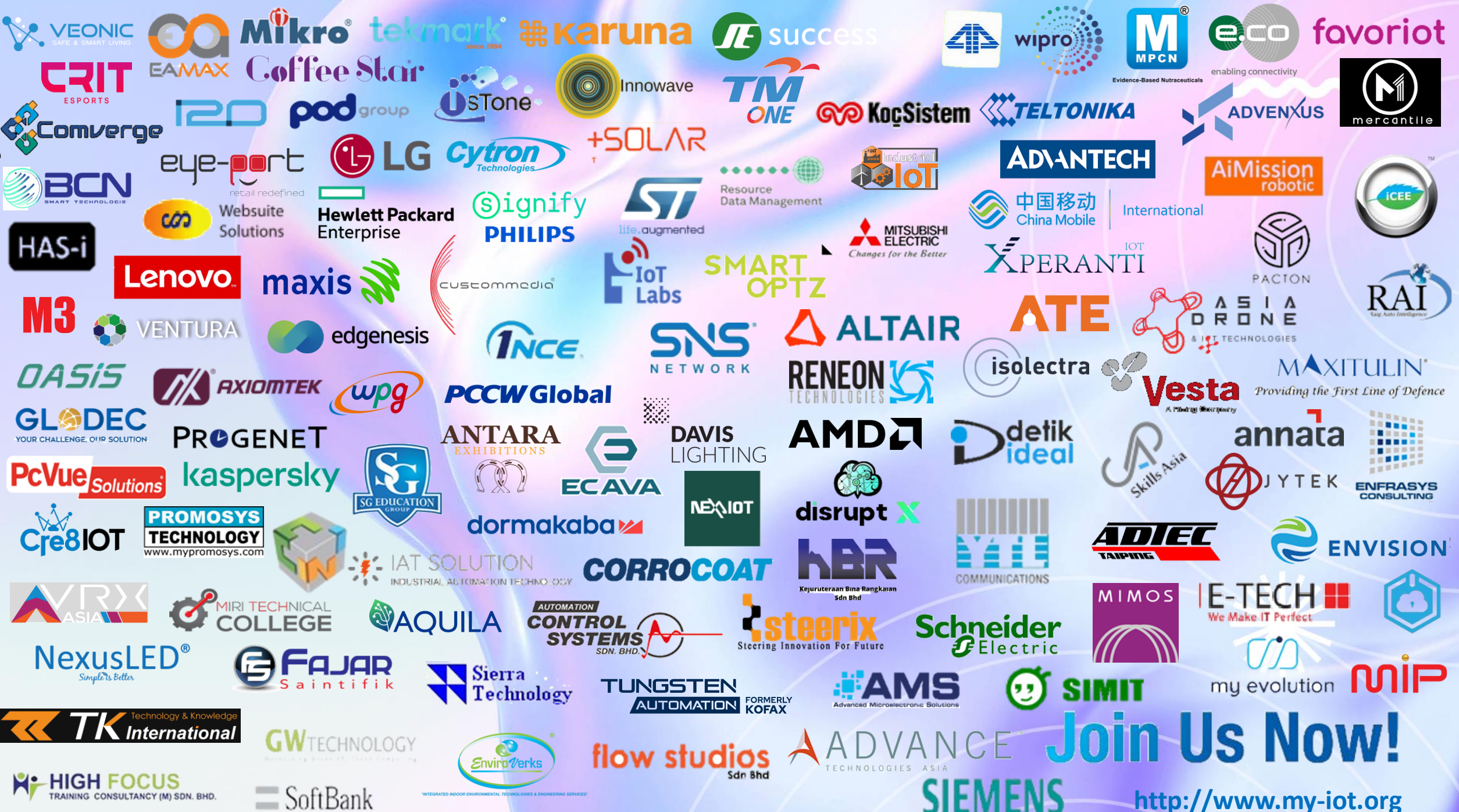




INTRODUCTION



Founded in 2016, Malaysia IoT Association or commonly know as MyIoT is the largest IoT & AI Eco-system & platform in Malaysia consisting of the entire IoT & AI value chain from semiconductors, sensors, 5G, connectivity, cloud, cybersecurity, software, hardware, research, funding & gov agency engagements. Find out more at www.my-iot.org

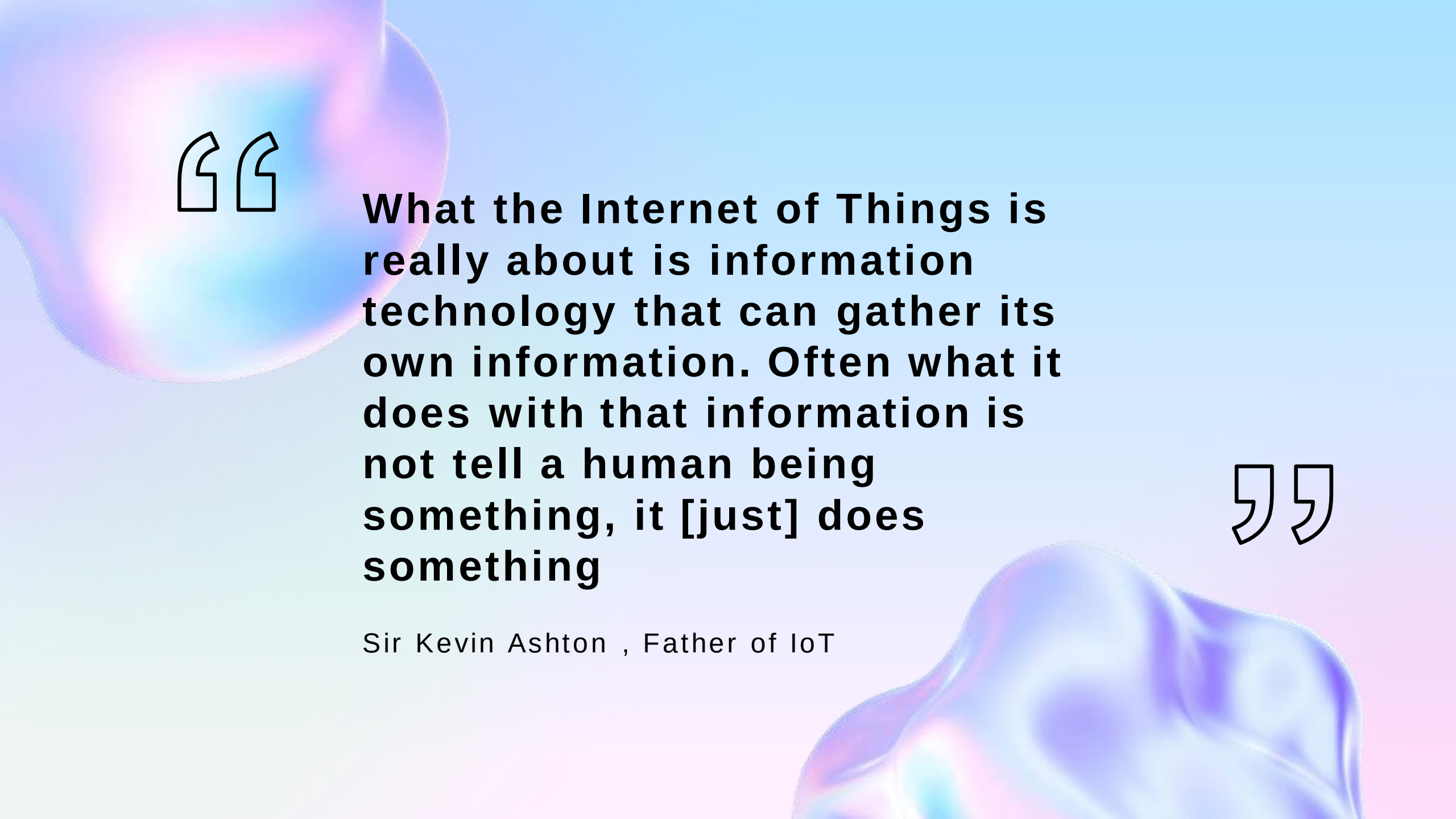


Join Us Now!

<http://www.my-iot.org>



**“DID YOU KNOW THAT BY 2025,
THERE WILL BE OVER 75
BILLION CONNECTED DEVICES
WORLDWIDE?”**



“

What the Internet of Things is really about is information technology that can gather its own information. Often what it does with that information is not tell a human being something, it [just] does something

”

Sir Kevin Ashton , Father of IoT

real-world examples of IoT security breaches

- Amazon-owned company Ring
 - **Incident:** User data was accidentally revealed to Facebook and Google. Cybercriminals hacked into families' connected doorbell and home monitoring systems
 - **How It Happened:** Hackers exploited weak, recycled, and default credentials to access live camera feeds and even communicate through integrated microphones and speakers. Some users reported verbal harassment.
 - **Lesson:** Always change admin credentials for new smart hardware and follow basic cybersecurity practices
-



vx-underground 
@vxunderground · Follow



Ring LLC, the home security and smart home company owned by Amazon, has been ransomed by ALPHV ransomware group.

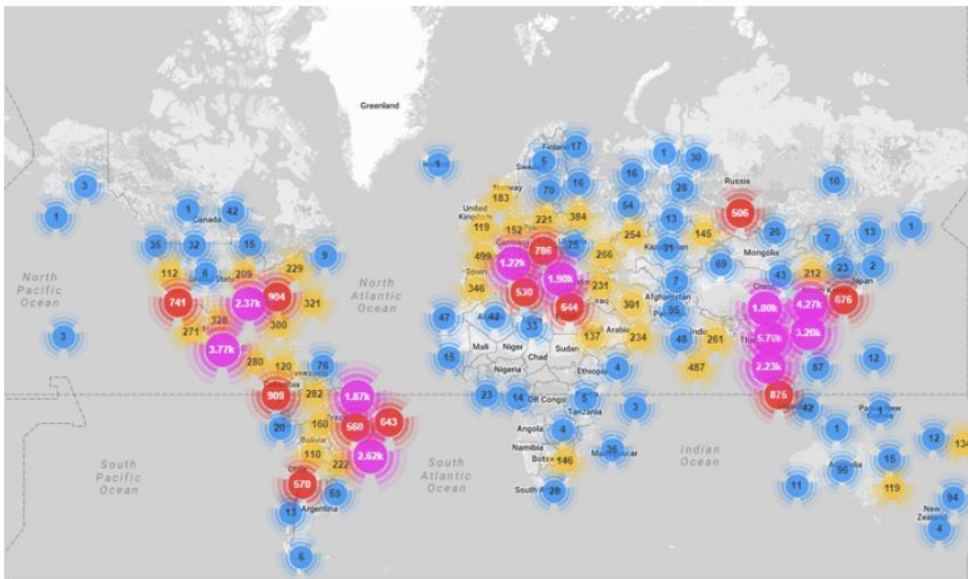
They left a simple message to Ring: "There's always the option to let us leak your data".

ALPHV

Ring: Security Systems
3/13/2023, 9:43:41 PM

There's always an option to let us leak your data





Report: Millions (and Millions) of Devices Vulnerable in latest Mirai Attacks

Attacks/Breaches | 1 MIN READ | QUICK HITS

IoTroop Botnet Hits Over a Million Organizations in Under 30 Days

The IoT botnet is expected to spread faster than Mirai.

A new IoT botnet dubbed IoTroop is expected to spread faster than Mirai because it has infected more than 1 million organizations since its discovery in late September, according to Check Point Software Technologies, which made the discovery.

<https://www.tutorialspoint.com/5-worst-examples-of-iot-hacking-and-vulnerabilities-in-recorded-history#>

Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system - which is normally cut off from the outside world - at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Iranian centrifuges for uranium enrichment

Date	In operation	Out of operation
Feb. 1, 2009	3,936	1,601
May 31	4,920	2,301
Aug. 12	4,592	3,716
Nov. 2	3,936	4,756
Jan. 29, 2010	3,772	4,838
May 24	3,936	4,592

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO

CYBERSECURITY

Hackers remotely kill Jeep's engine on highway

PUBLISHED TUE, JUL 21 2015-5:18 PM EDT | UPDATED WED, JUL 22 2015-8:41 AM EDT

Zack Guzman @ZGUZ

WATCH LIVE

SQUAWK BOX VIDEO 01:40 HACKERS HIJACK MOVING JEEP AUTOMAKER PUSHES FIX

CNN Business @CNNBusiness Follow

Recall Alert: Fiat Chrysler is recalling 1.4 million hackable vehicles. Check affected cars: cnnmon.ie/1OrrqGv

Hackers can cut the brakes, shut down the engine, drive it off the road, or make all the electronics go haywire.

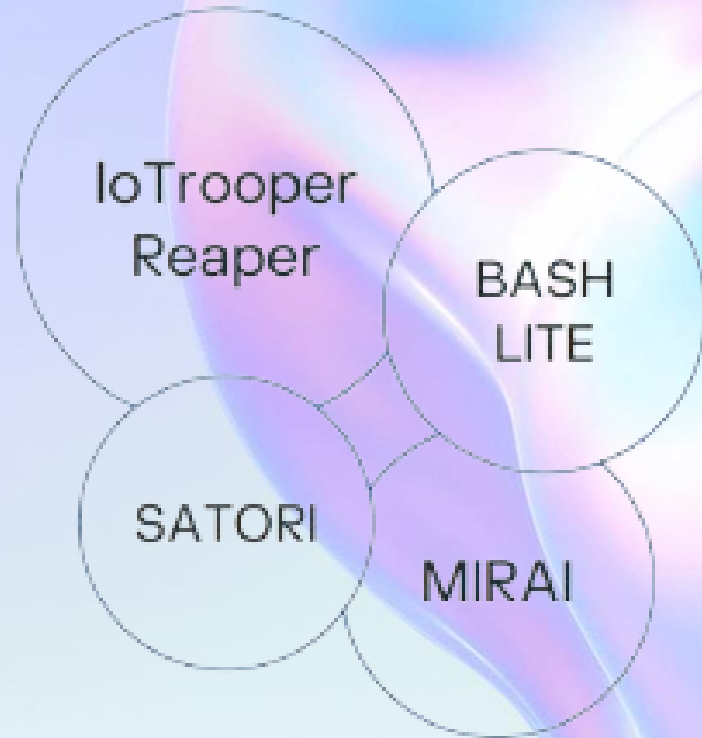
8:59 AM · Jul 25, 2015

18 Reply Share

Read more on Twitter

INCREASED IOT CYBERSECURITY THREATS

IoT threat statistics



Software
vulnerabilities

Vulnerabilities in
general-purpose OS

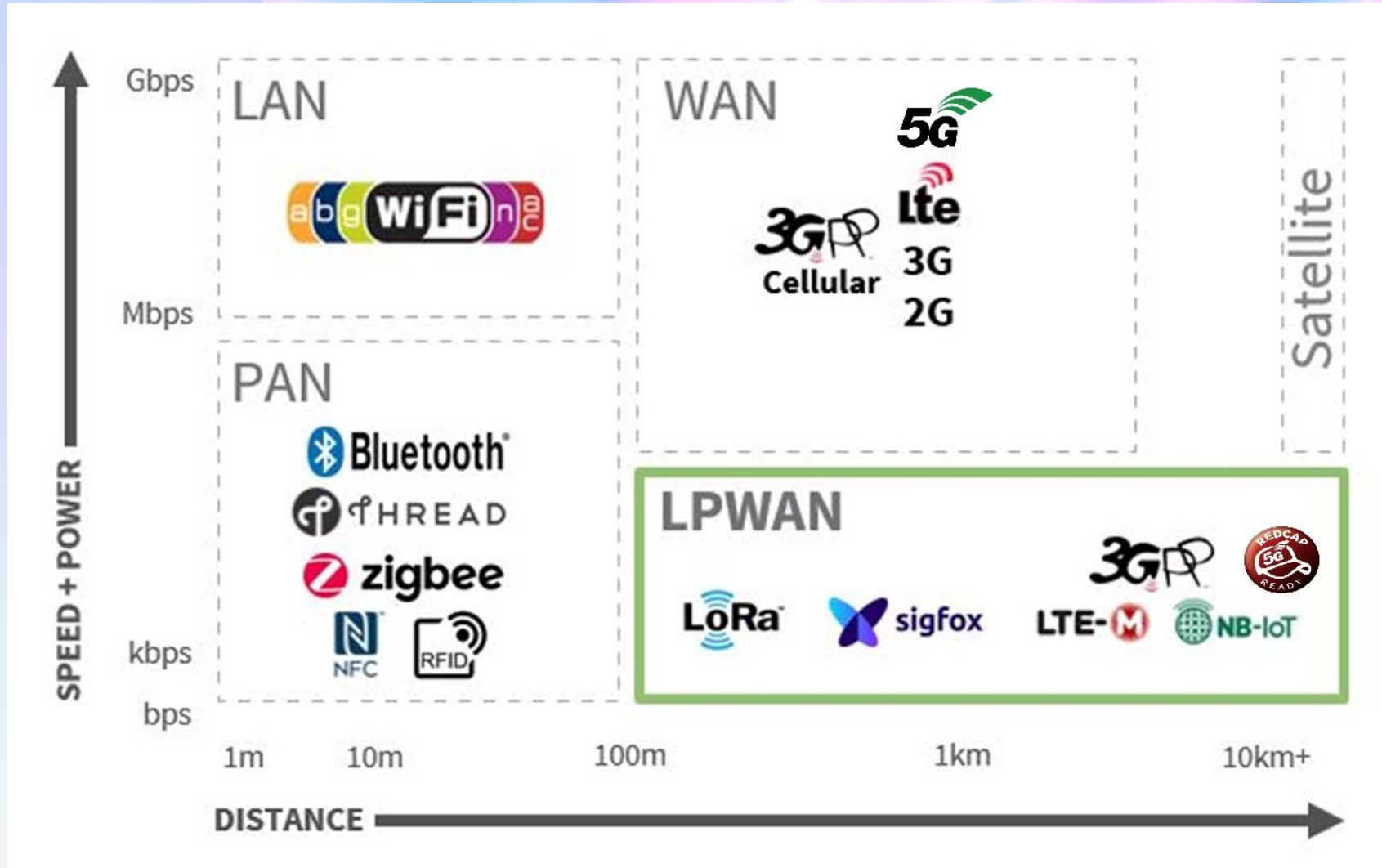
Undeveloped
security architecture

Growth of new IoT malware
over last 6 years:

more than
2000 times

+ 1,036,911
unique modifications

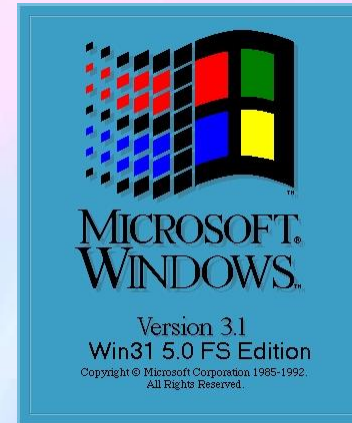
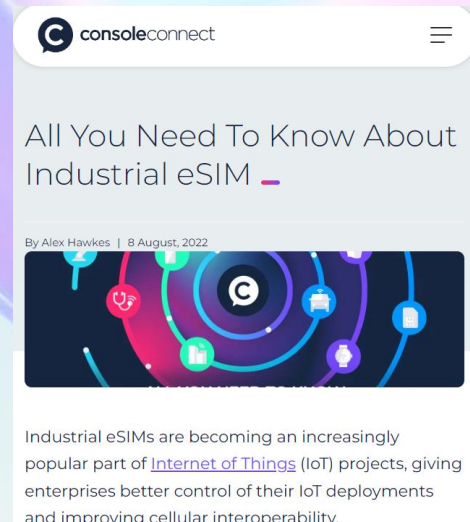
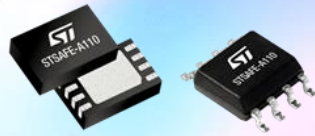
THE IOT VALUE CHAIN



SECURING INDUSTRIAL INTERNET OF THINGS (IIOT) SYSTEMS

ISSUES

- Diverse Ecosystems
- Legacy Infrastructure
- Physical Vulnerabilities
- Scalability and Volume
- Interoperability
- Supply Chain Risks
- Lack of Security Awareness: Industrial operators may not fully grasp the security implications of IIoT adoption



RECOMMENDATIONS

- Harmonizing security
- Integrating modern security measures without disrupting existing operations
- Ensuring physical security and preventing unauthorized access
- Implementing scalable authentication, encryption, and monitoring mechanisms
- Establishing secure communication channels while maintaining compatibility
- Ensuring supply chain integrity and verifying device authenticity
- Raising awareness, providing training, and fostering a security-conscious culture

IOT CYBERSECURITY REGULATIONS

CONGRESS.GOV Sign In

Advanced Searches Browse Search Tools

Legislation Examples: hr5, sres9, "health care" MORE OPTIONS

Citation Subscribe Share/Save Site Feedback

H.R.1668 - IoT Cybersecurity Improvement Act of 2020

116th Congress (2019-2020)

LAW Hide Overview

Sponsor: [Rep. Kelly, Robin L. \[D-IL-2\]](#) (Introduced 03/11/2019)

Committees: House - Oversight and Reform; Science, Space, and Technology

Committee Meetings: [06/12/19 10:00AM](#)

Committee Reports: [H. Rept. 116-501](#)

Latest Action: 12/04/2020 Became [Public Law No. 116-207](#) (All Actions)

Tracker: 1

NIST Search NIST Menu

Information Technology Laboratory /Applied Cybersecurity Division

NIST CYBERSECURITY FOR IOT PROGRAM

The Cybersecurity for IoT Program's mission is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools.

About

FAQs

Events

IOT Advisory Board

Publications

Newsroom

Resources

Related Initiatives

Cybersecurity @ NIST

Information for Manufacturers

[NISTIR 8259 Series](#)

Read more about NIST's guidance for manufacturers

Information for Federal Agencies

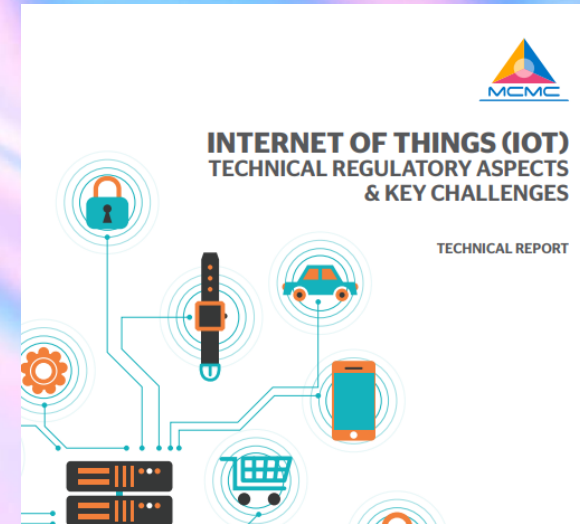
[SP 800-213 Series](#)

Read more about NIST guidance for Federal

Information Regarding Consumer IoT

[Consumer IoT Products](#)

Read more about the program's contributions to



Ministry of Communications and Multimedia Malaysia CyberSecurity MALAYSIA

First edition 2020-05-05

Guidelines for Secure Internet of Things (IoT)

Reference number: MyVAC-3-GUI-3-IOT-v1

MCMC MTSFB TC G013:2018

TECHNICAL CODE

INTERNET OF THINGS (IoT) - SECURITY MANAGEMENT

Developed by **MTSB** (Malaysian Technical Standards Forum Bhd) Registered by **MCMC**

Registered date: 15 October 2018

MCMC MTSFB TC GXXX:2023

TECHNICAL CODE

INTERNET OF THINGS - DEVICE SECURITY REQUIREMENTS

Developed by **MTSB** (Malaysian Technical Standards Forum Bhd) Registered by **MCMC**

Registered date: © Copyright 2023

<https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program>

PREVALENCE & RISK OF OPEN-SOURCED LIBRARIES & OS

GITHUB HAS FACED REAL-WORLD INCIDENTS WHERE MALICIOUS ACTORS EXPLOITED OPEN-SOURCE REPOSITORIES



The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally

By Check Point Research

Check Point Research flags a sharp increase in cyberattacks targeting IoT



DARK READING

NEWSLETTER SIGN-UP

CLOUD SECURITY

Patch Now: Massive RCE Campaign Wrangles Routers Into Botnet

Thousands of devices, including D-Link and Zyxel gear, remain vulnerable to takeover despite the availability of patches for the several bugs being exploited by IZ1H9 campaign.



Dark Reading Staff, Dark Reading
October 10, 2023

1 Min Read





CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

MALWARE & THREATS

Threat Actors Manipulate GitHub Search to Deliver Malware

Checkmarx warns of a new attack relying on GitHub search manipulation to deliver malicious code.



By Ionut Arghire
April 12, 2024

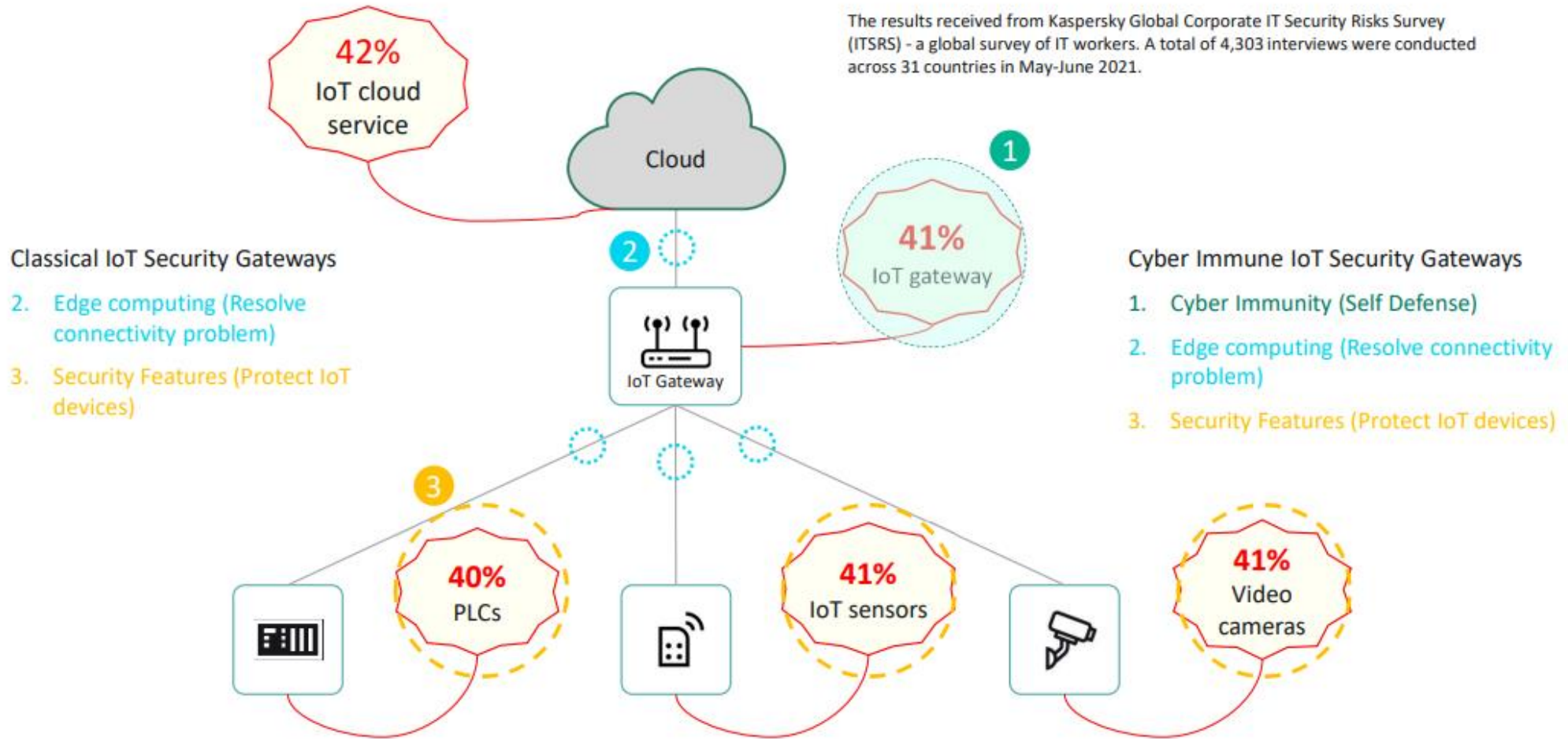


Threat actors have been observed manipulating GitHub search results to infect developers with persistent malware, application security firm Checkmarx warns.

WHERE ARE THE THREATS COMING FROM?

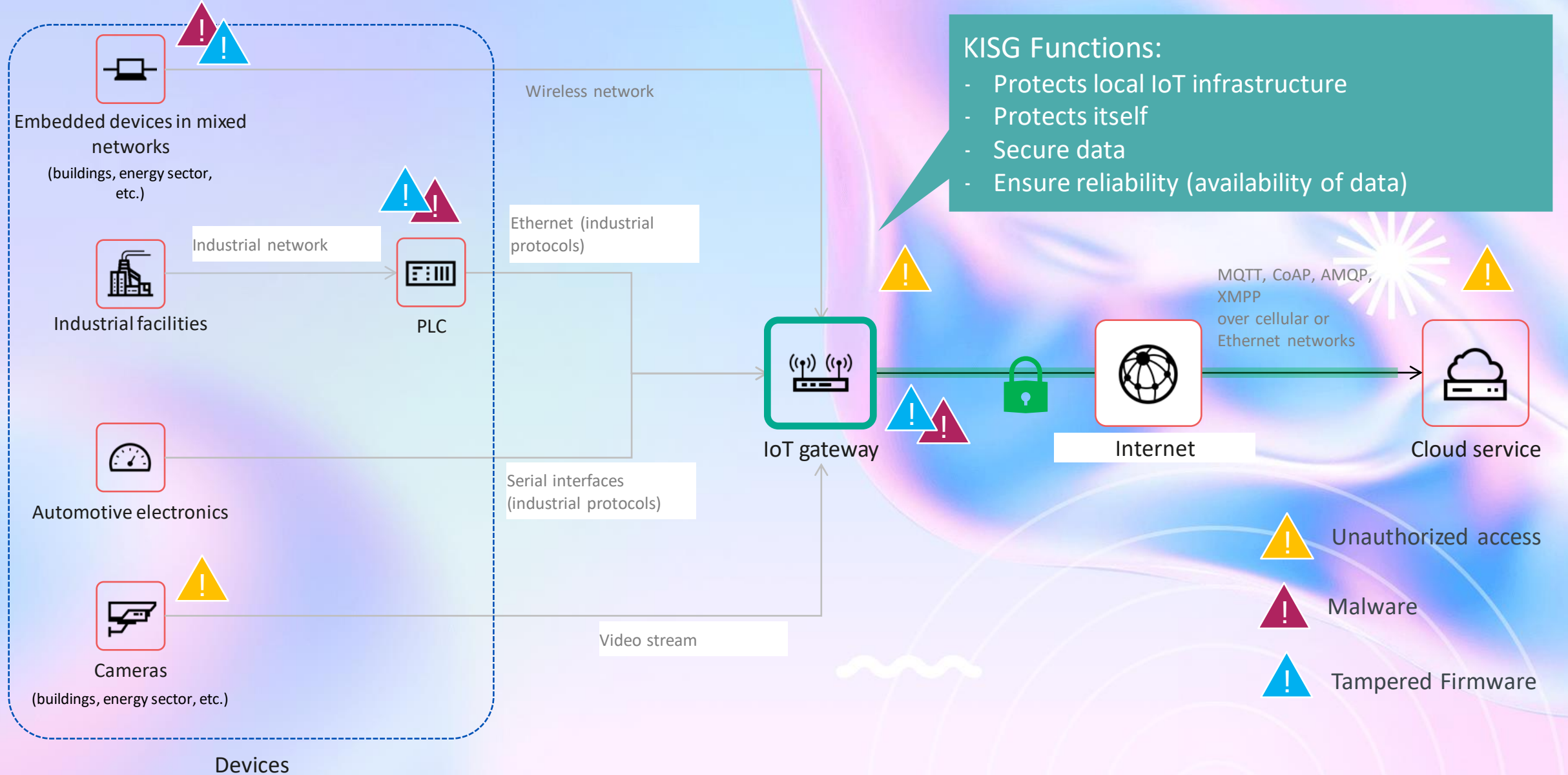
IoT/IIoT infrastructure threats

13



https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf

What is IoT Secure Gateway?



Microkernel vs Monolithic kernel

- Minimal possible code size allows to obtain a very high level of security
- Minimizing the probability of vulnerabilities in a key element of the information system
- Eliminates the risk of entire classes of cyberattacks
- Reliability and predictability of operation

≈ **35 millions**
of code lines in the **Linux** kernel

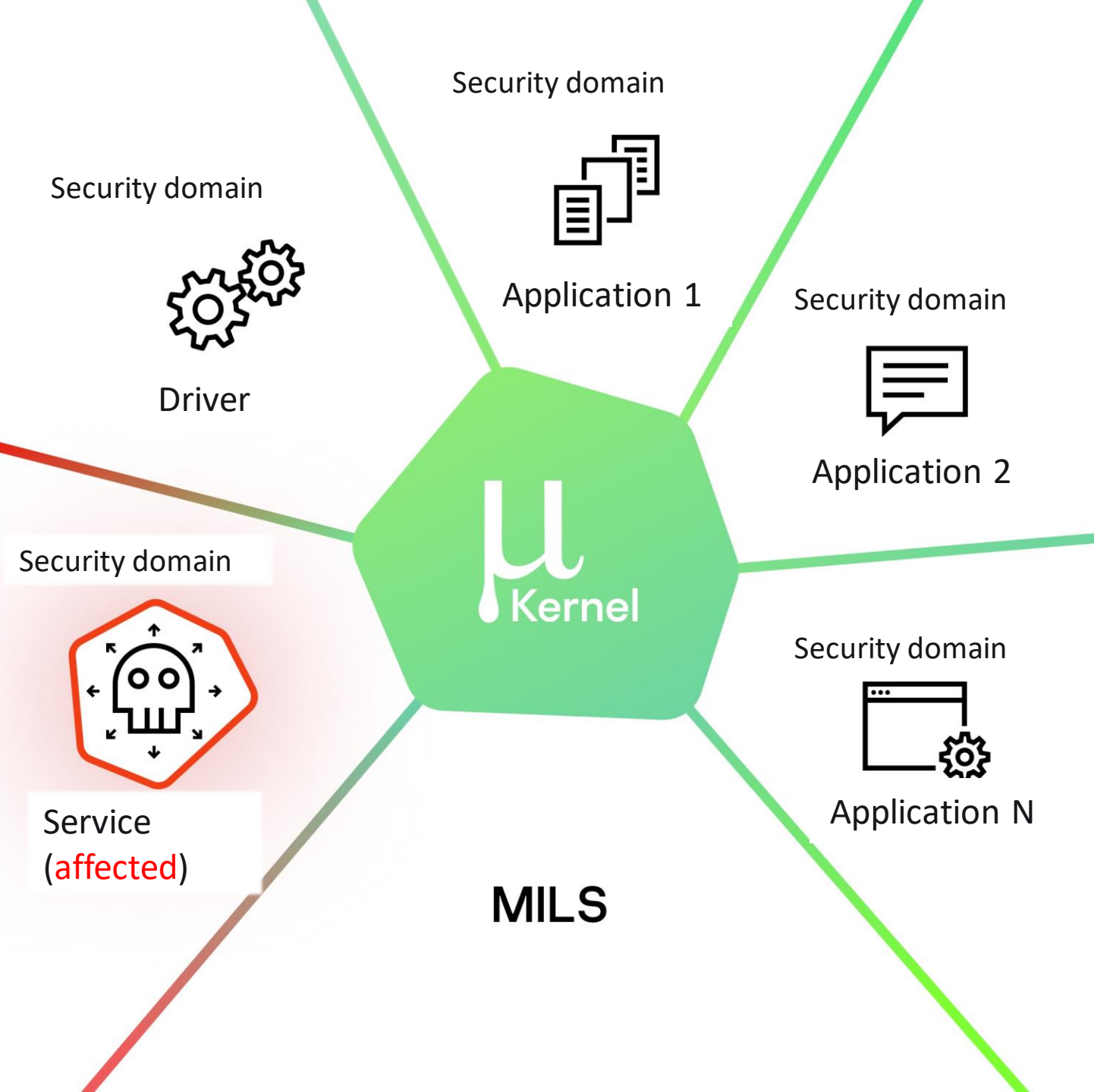
 ≈ **100 thousands**
of code lines in the
microkernel in **KasperskyOS**

Advantages of microkernel approach

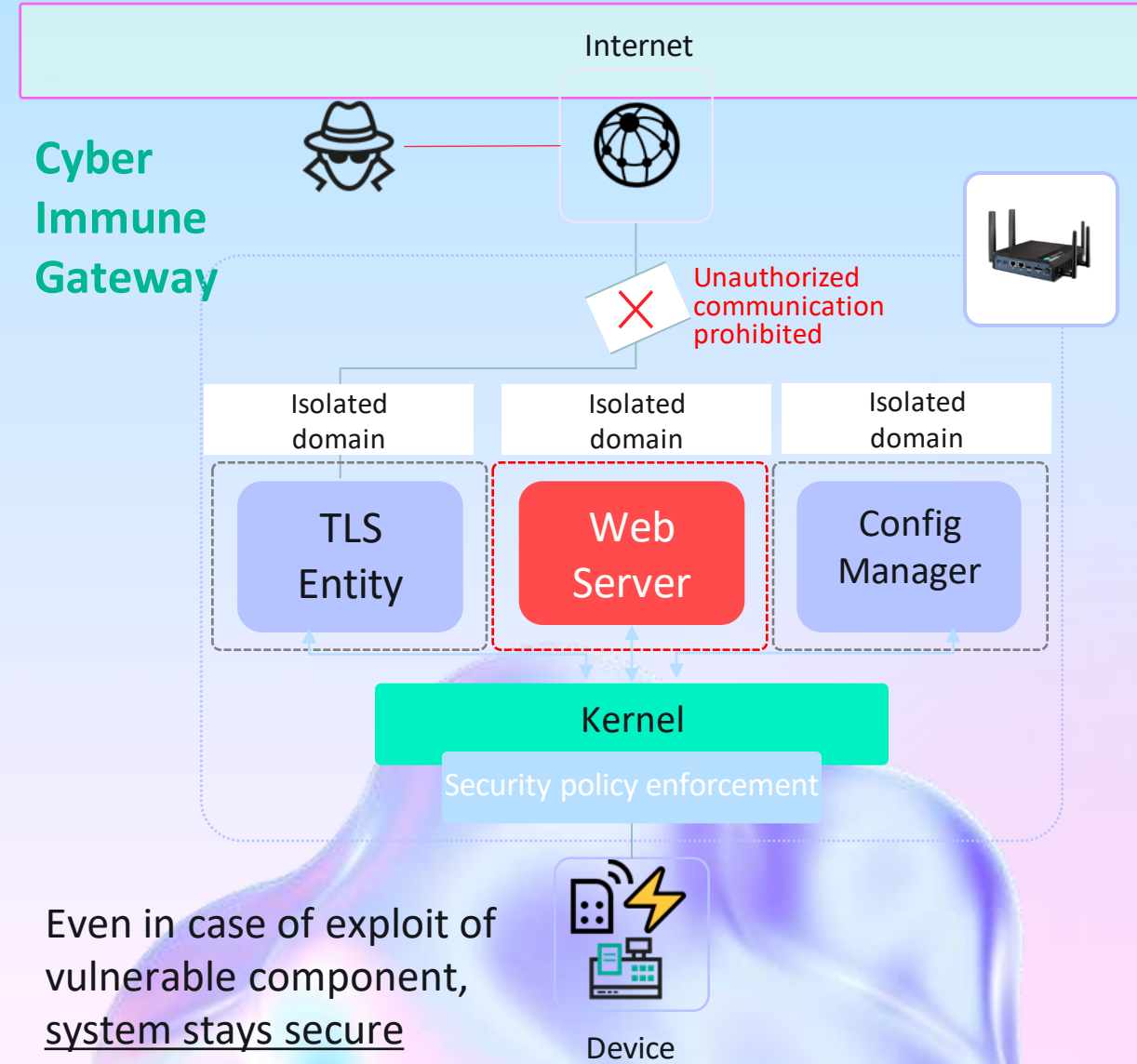
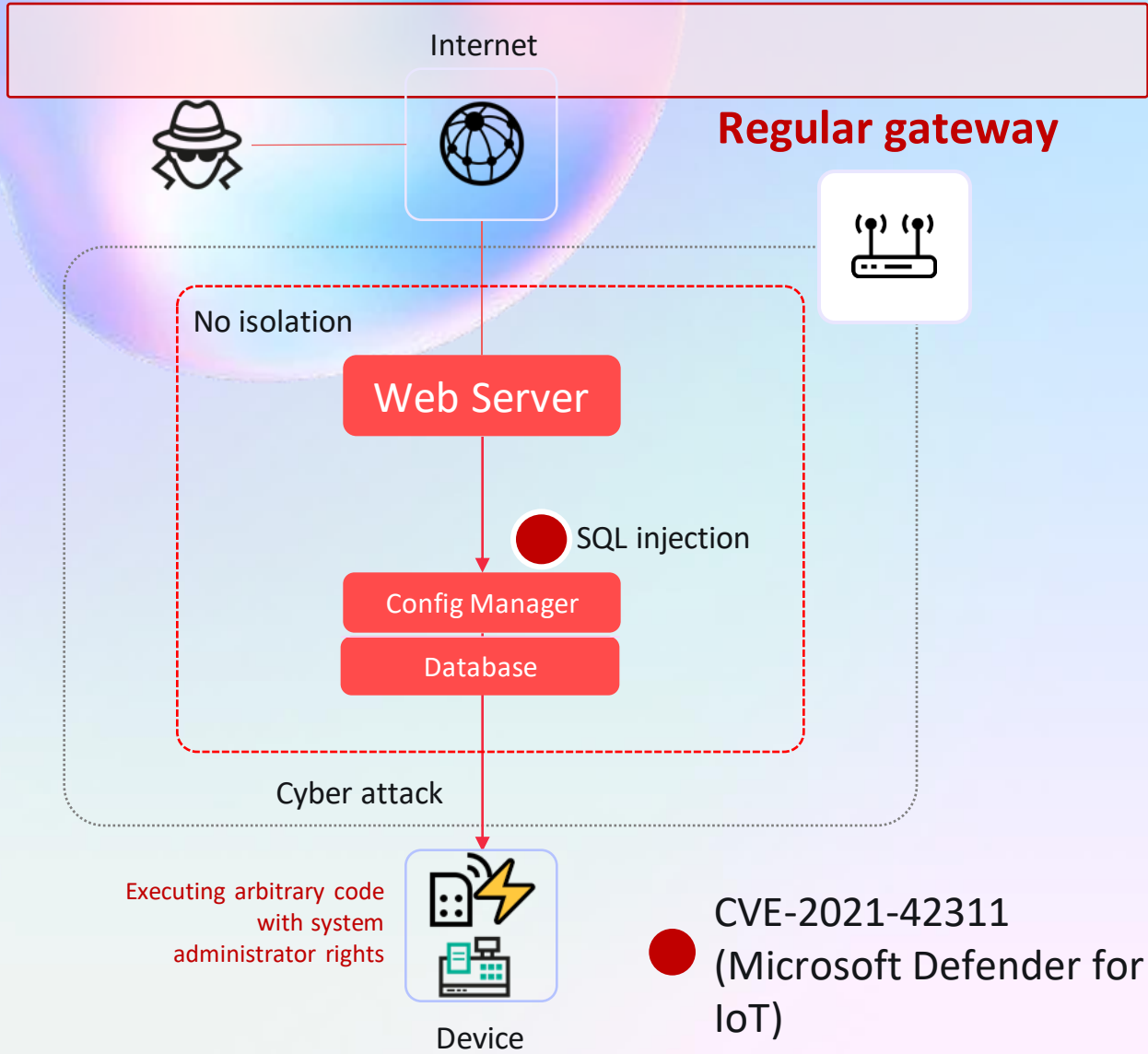
Component compromise does not compromise the kernel or the entire solution

This approach allows you to protect against even a compromised driver

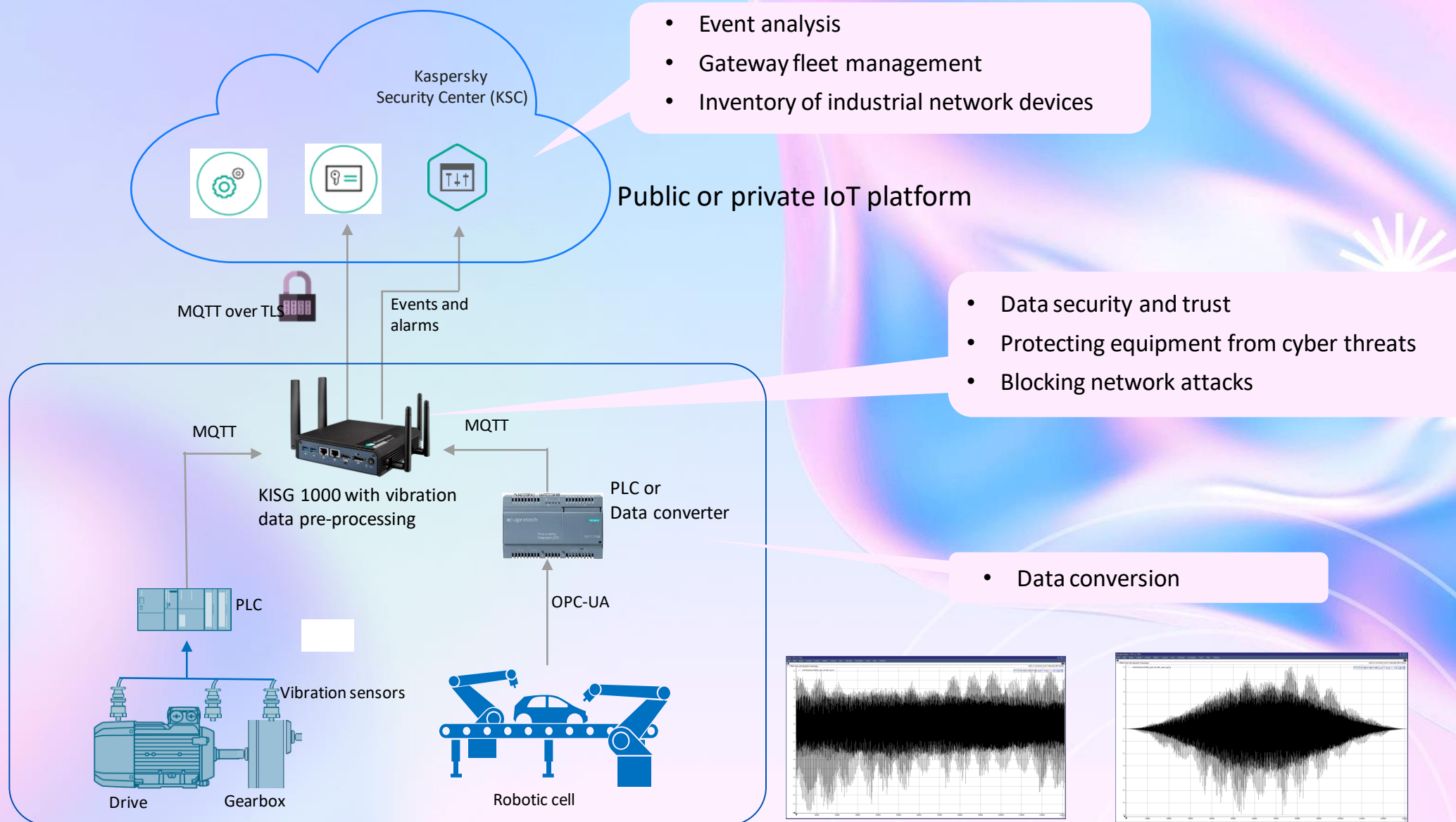
Attack spreading is complicated, and in some directions impossible



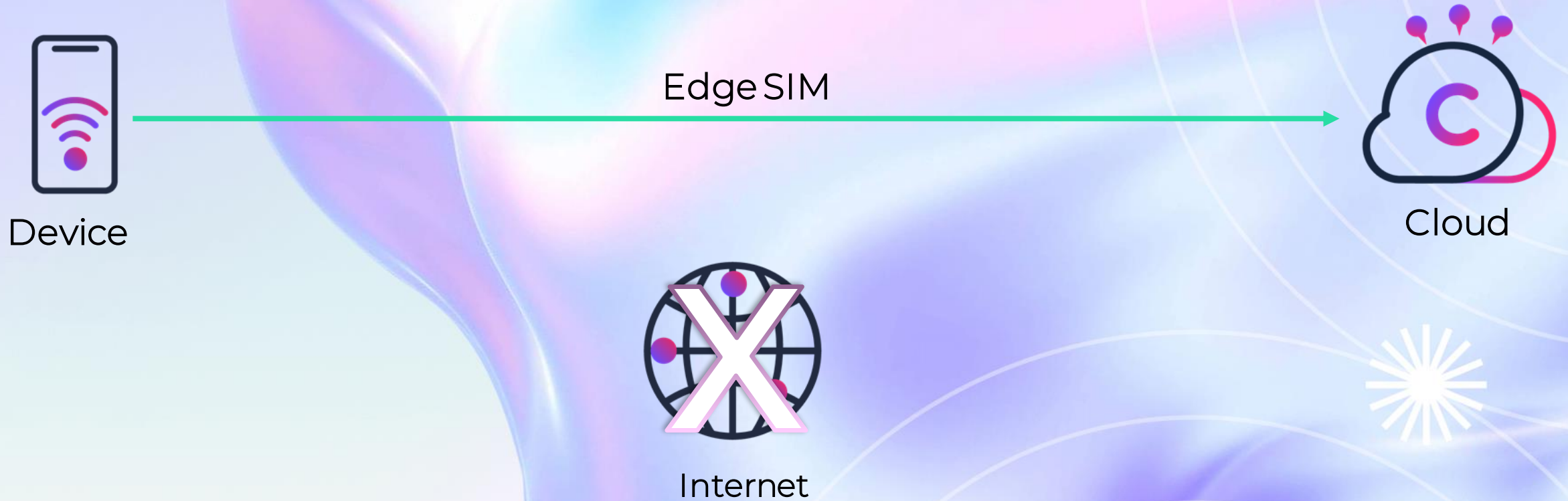
Regular gateway vs. Kaspersky Cyber Immune gateway under cyberattack (RCE as an example)



USE CASE: INDUSTRIAL IOT



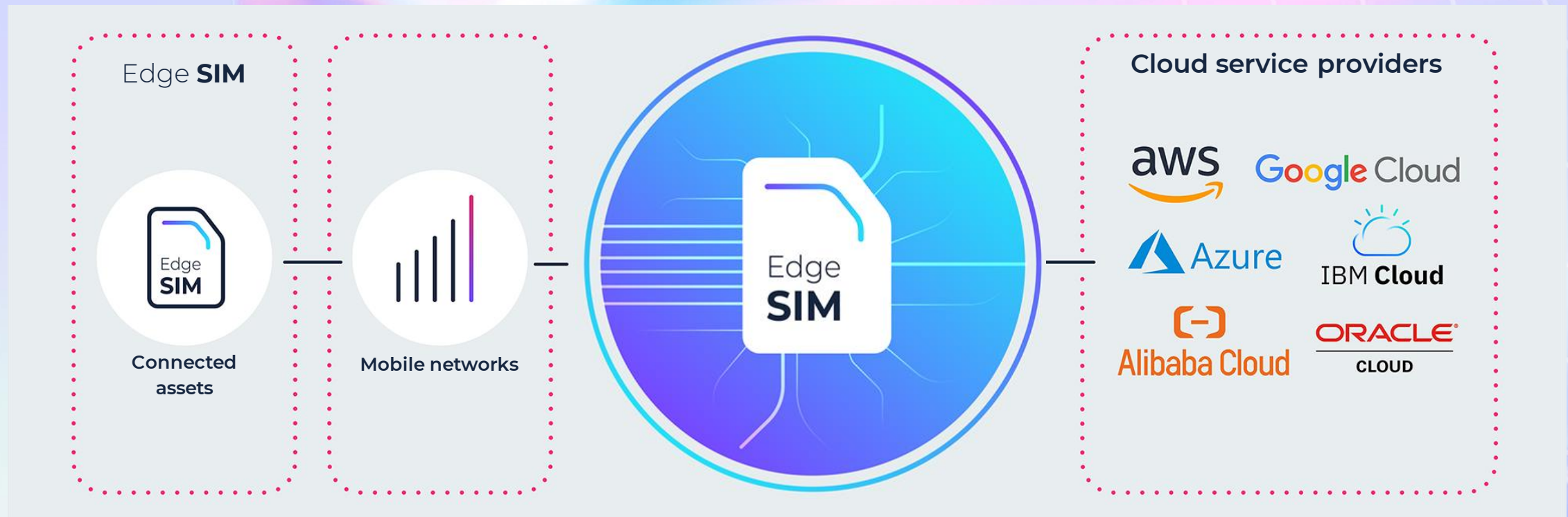
Edge SIM eliminate the risk





SECURELY CONNECT ANY DEVICE
TO ANYWHERE, WITHOUT
TOUCHING
THE PUBLIC INTERNET

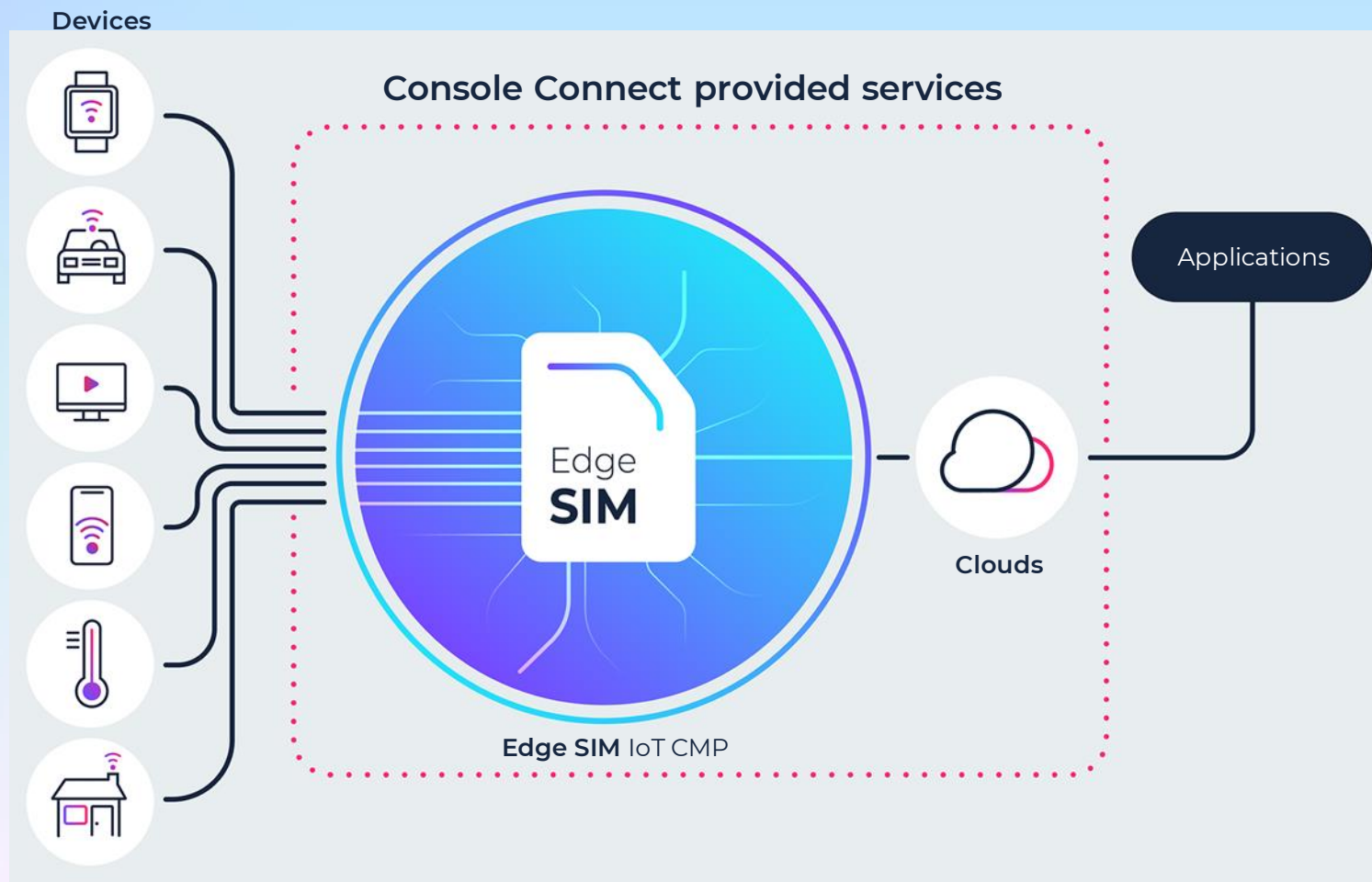
To **Simplified** Edge to cloud **network**



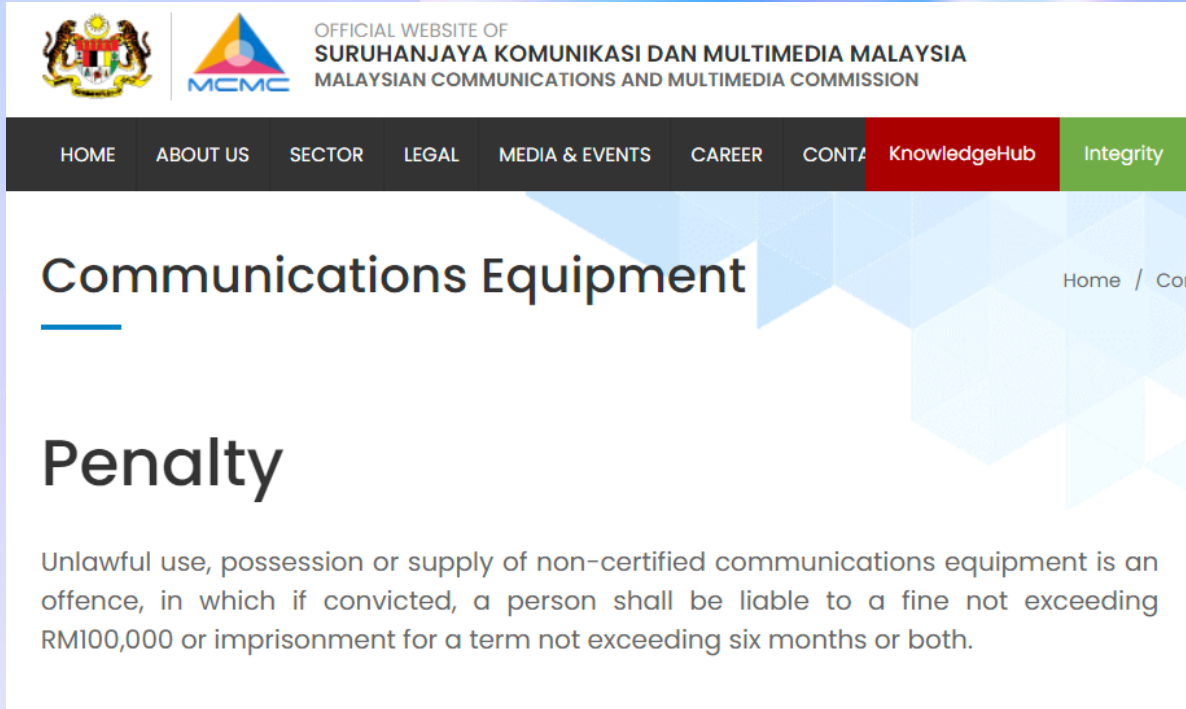
Edge SIM

- ☒ **Automated** provisioning
- ☒ **Scalability** build in
- ☒ **Secure** IoT data transfer over private network
- ☒ **Ubiquity** with full worldwide coverage in one SIM
- ☒ **Seamlessly** manage data and SIMs via the Console Connect portal

sales@consoleconnect.com



REGULATIONS & COMPLIANCE FOR WIRELESS DEVICES



The screenshot shows the official website of the Malaysian Communications and Multimedia Commission (MCMC). The header includes the MCMC logo and the text "OFFICIAL WEBSITE OF SURUHANJAYA KOMUNIKASI DAN MULTIMEDIA MALAYSIA" and "MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION". The navigation menu includes links for HOME, ABOUT US, SECTOR, LEGAL, MEDIA & EVENTS, CAREER, CONTACT, KnowledgeHub, and Integrity. The main content area features the heading "Communications Equipment" and a sub-heading "Penalty". Below this, a paragraph states: "Unlawful use, possession or supply of non-certified communications equipment is an offence, in which if convicted, a person shall be liable to a fine not exceeding RM100,000 or imprisonment for a term not exceeding six months or both."



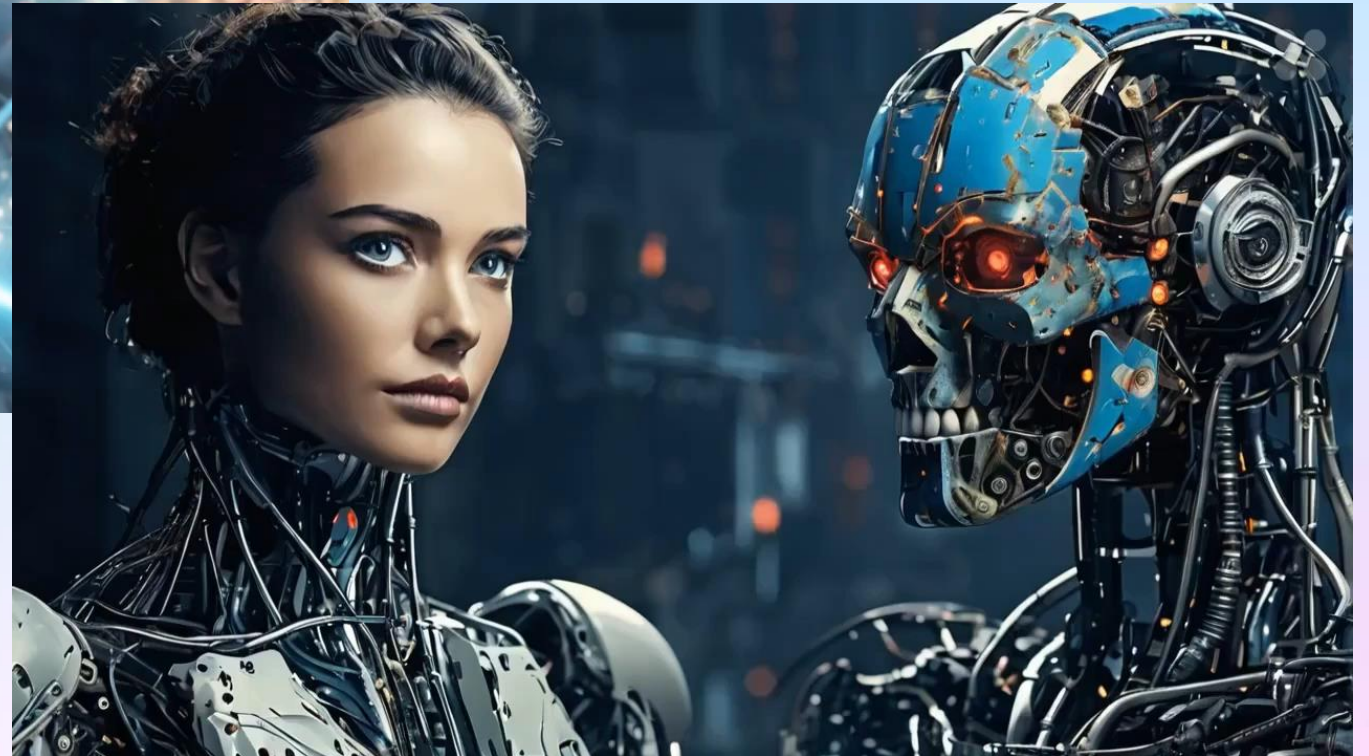
REGULATION 16

Use, offer for sale or sale of communications equipment which is contrary to standards, not certified or no longer complies with standards or does not bear a certification label. On conviction, fine not exceeding RM300,000 or imprisonment not exceeding three (3) years or both



<https://cyl.mcmc.gov.my/about#regulation>

AI TRENDS



SUPER HERO VS SUPER VILLAIN



thejapan times

JAPAN / CRIME & LEGAL

Kawasaki man arrested over malware made using generative AI



TheStar

Man in Japan arrested for creating virus using generative AI systems

Man in Japan arrested for creating virus using generative AI systems



AI

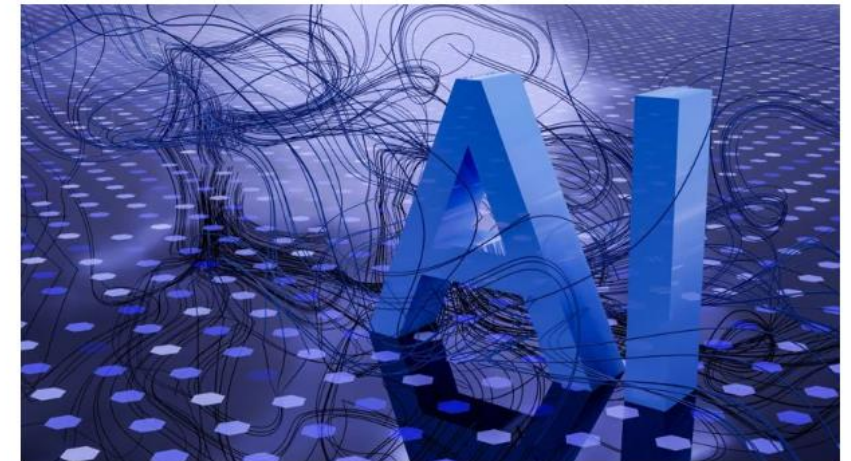
Tuesday, 28 May
2024

3:39 PM MYT

Related
News



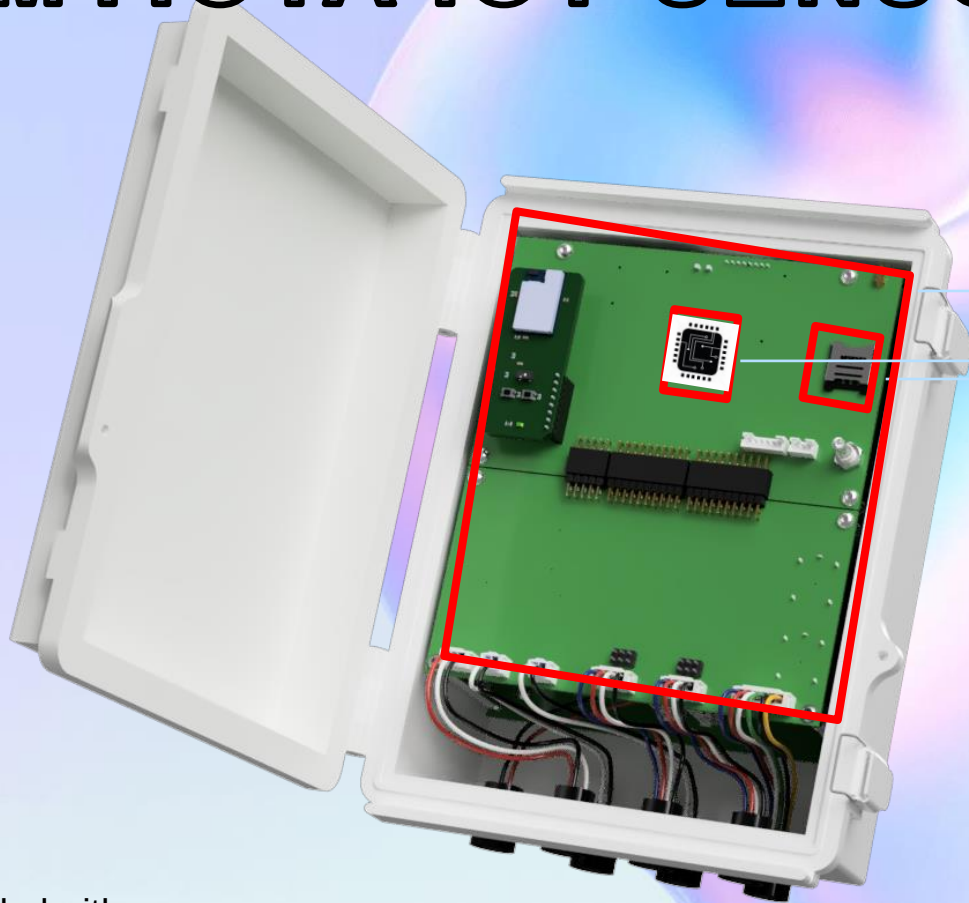
TECHNOLOGY 6h ago
Top EU data
regulator says tech



The crafted virus was designed to do things such as encrypt data on targeted systems and demand cryptocurrency as ransom. — Photo by Steve Johnson on Unsplash

TOKYO: A 25-year-old unemployed man from Kawasaki has been arrested for allegedly creating a computer virus by using interactive

MYIOTA IOT SENSORHUB: MAKING IOT EASY



Powered-by STMicroelectronics

STM32L475VG, Cortex-M4 MCU 80 MHz with 1 Mbyte of Flash memory, 128 KB SRAM
1GB FLASH Onboard memory (20,000 sampling log, 100,000 activity log)



PCB-Designed by Cre8IoT

Malaysian embedded design house



consoleconnect

Global roaming data SIM

6-month plan from PCCW Global



IoT Middleware Dashboarding & Training

Favoriot



MATRIXINVENT

Real-Time Historian & MQTT server

Matrix Invent MSC



ALTAIR

AI/ML Prototyping & Development tools

Altair Engineering



Firmware Development Training on Customization

IoT Labs 3-day embedded C-programming & prototyping for IoT SensorHub

Bundled with:-

IoT sensors, Edge Computing, Hybrid cloud services, HMI/SCADA, IoT Middleware, AI/ML Tools, Wireless, Industrial Rating, Reference Applications, Multi-vendor support/components & eco-system etc. Target for SME's & Start-ups deploying IoT solutions out-of-the box



MYIOTA SENSORHUB REFERENCE ARCHITECTURES

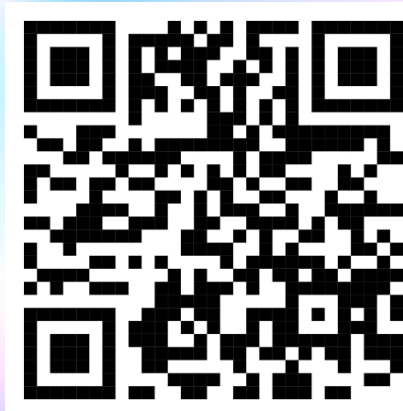


MYIOTA SENSORHUB FOR SMART CITY

Smart Street Light



MikroE board with
Lora, Wifi, GNSS



Smart rubbish bin



Smart Parking



MYIOTA SENSORHUB ARCHITECTURE

Application Areas



Smart Agriculture



Smart Building



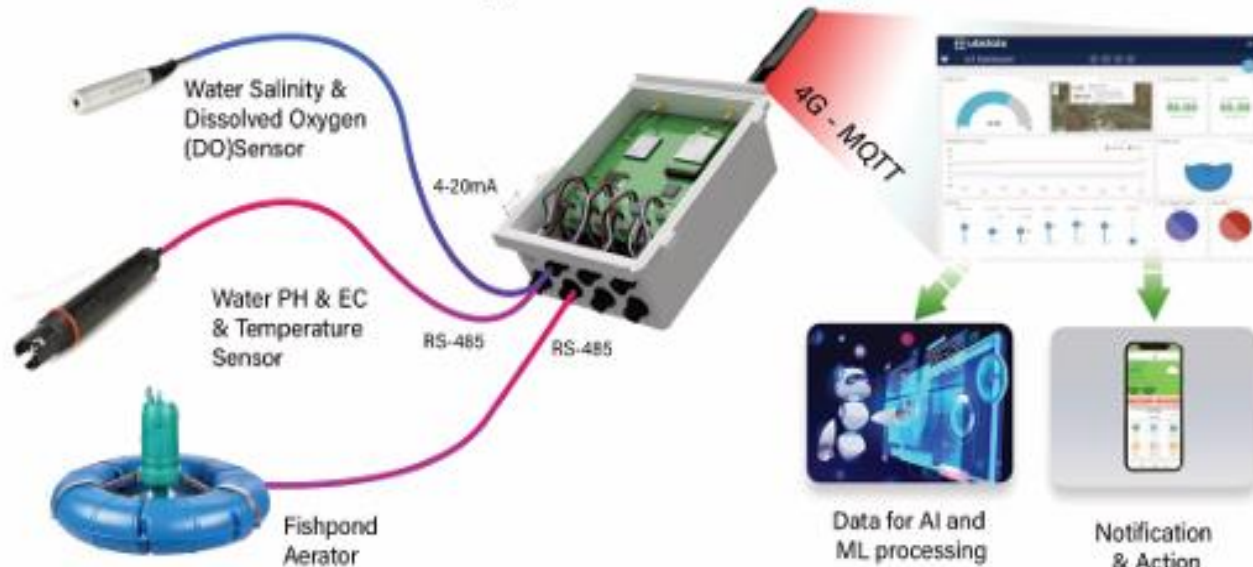
Smart Manufacturing



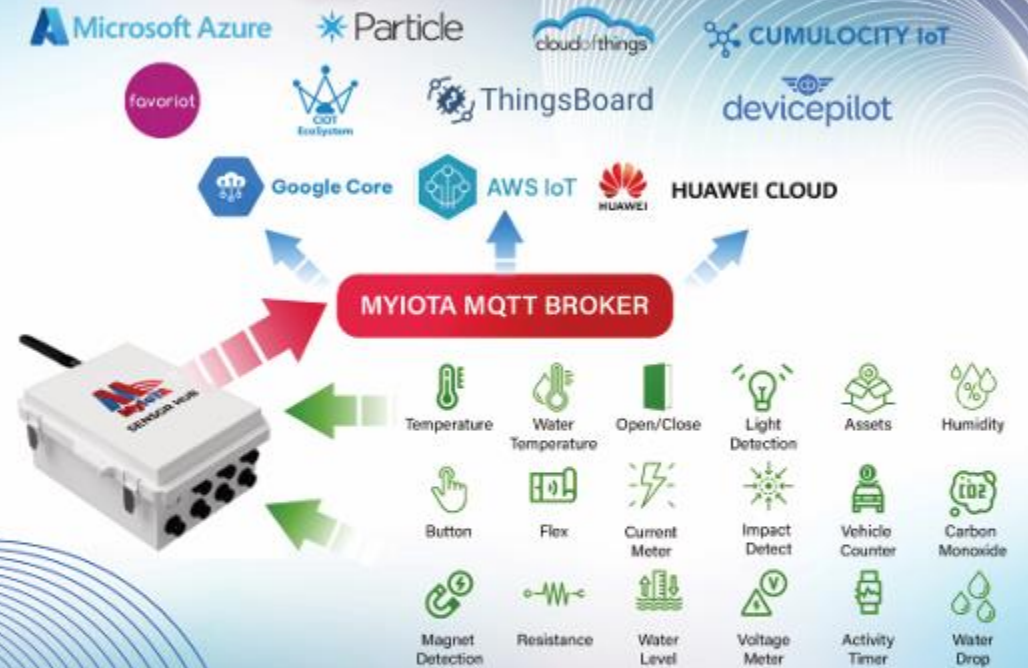
Smart City

Smart Agriculture Example

Shrimp, Prawn and Fish Farming



Application Diagram



Specification

Power Source	Direct Solar Panel or 10-36VDC
Solar Charger Controller	Built-In
Battery Capacity	4000mAh
GSM	4G CAT-1 OR 4G CAT-1bis
4G Band	B1, B3, B7, B5, B38, B40
Expansion	MIKROE module
Size	160mm x 210mm x 100mm
IP Rating / Weight	IP64 / 118 kg

Specification IO Card

Rs-485	2 channels, MODBUS-RTU with Selectable Sensor Power 5V, 12V, 24V @ 150mA
Analog In	24V sensor power loop (max. 25mA per channel) or single ended with 20-ohm impedance.
Digital Input	2 channels opt-isolated, can be configured as contact input or pulse input. - Contact input either dry contact or wet input. - Pulse input either rising or falling edge counter with 1KHz speed.
Digital Output	2 channels, Relay 5A, NC/C/NO.

Join us at HoT 2024



HYPERNET OF THINGS

EXHIBITION & CONFERENCE

Asia's Premier Exhibition & Conference
for IoT, AI & Digital Technologists

27 - 28 NOVEMBER 2024

WORLD TRADE CENTRE

KUALA LUMPUR

www.hypernetofthings.net

CONNECTING THE FUTURE

SUMMARY

Securing IIoT demands a holistic approach—combining technical solutions, policy frameworks, and collaboration across various industries & its value chain

SECURING THE IOT ISN'T AN
OPTION—IT'S AN
IMPERATIVE. LET'S WORK
TOGETHER TO BUILD A
SAFER, SMARTER
CONNECTED WORLD

Ts. James Lai

James.lai@my-iot.org

www.my-iot.org

