How to get ready for a world of IoT cyber security regulations?

Dr. Cédric LEVY-BENCHETON

@CetomeLtd
cetome.com

Cetome: your IoT Cyber Security Consultancy

We make IoT Cyber Security work for you!

Accelerate project delivery with security-by-design

Keep your products secure after release

Upskill your staff with training and awareness

Consolidate market access in light of regulations

Summary

Why is IoT security still a joke in 2021?

Panorama of IoT Cyber Security Regulations

How to succeed in a world of IoT regulations?

Discussion on the future and conclusions

Why is IoT security still a joke in 2021?

Do you know…

#IoTSecurity

#RegulateVendors

What the S in IoT stands for?

Do you know…

#IoTSecurity

#RegulateVendors

What the S in IoT stands for?

It stands for:

Do you know…

#IoTSecurity

#RegulateVendors

What the S in IoT stands for?

It stands for:

"Stop making the same old joke, it's not funny anymore".

IoT SECURITY IS NOT A JOKE

#IoTSecurity

#RegulateVendors

Think of the children!

IoT SECURITY IS NOT A JOKE

#IoTSecurity

Think of our safety!

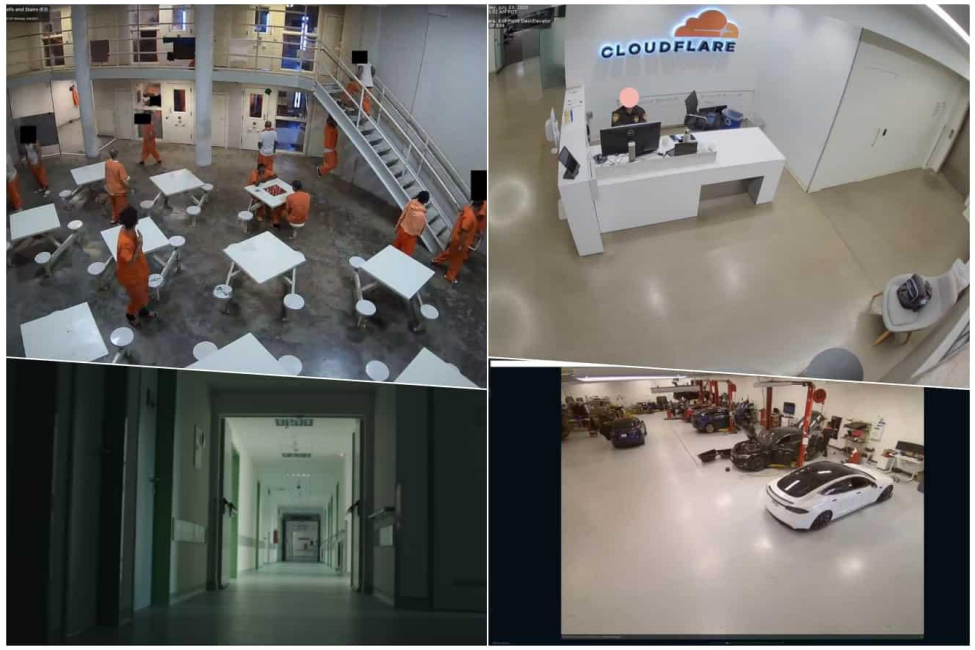
#RegulateVendors

IoT SECURITY IS NOT A JOKE

Think of our privacy!

#IoTSecurity

#RegulateVendors



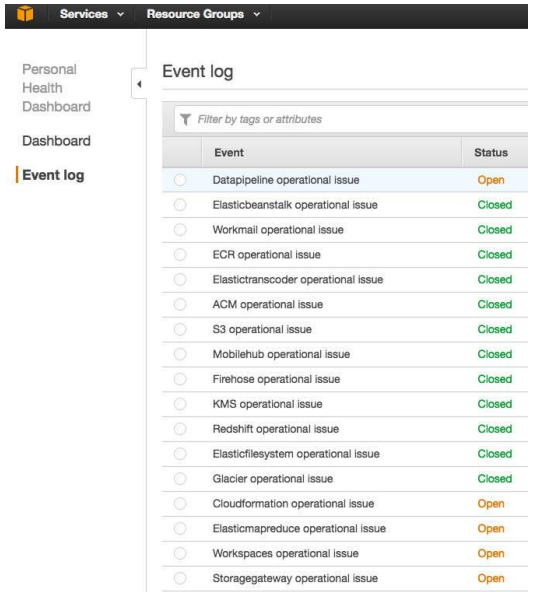
Cetome
Securing a Better Future

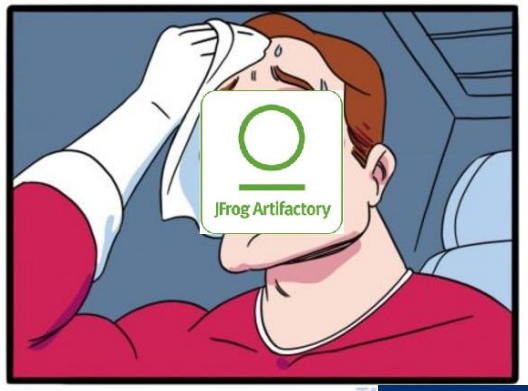
IoT SECURITY IS NOT A JOKE

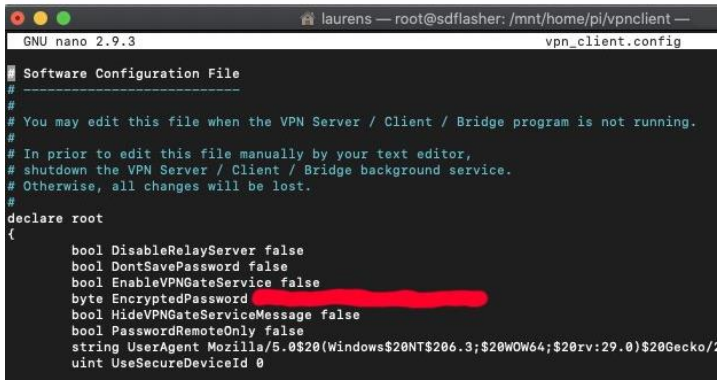
#IoTSecurity

Think of our developers and product manufacturers!

#RegulateVendors








```
function s3(tablename, tabledata, successCallback, errCallback) {
        var bucketName = "static-skypixel-dbeta-me";
            AWS.config.update({
                accessKeyId: 'AKIAIRKNYFZBHSS2COTA',
                secretAccessKey: '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',
                region: 'us-west-2',
                bucket: bucketName
            });
```

Project Memoria

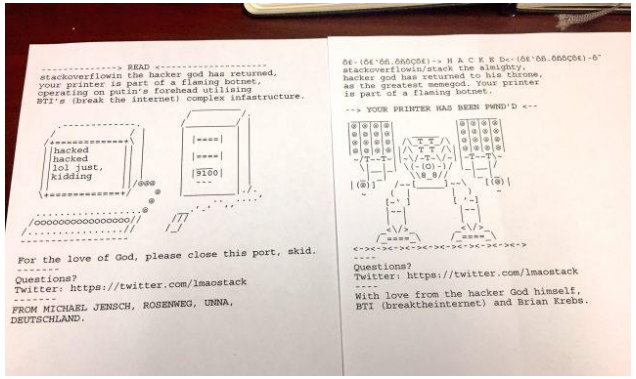
IoT SECURITY IS NOT A JOKE

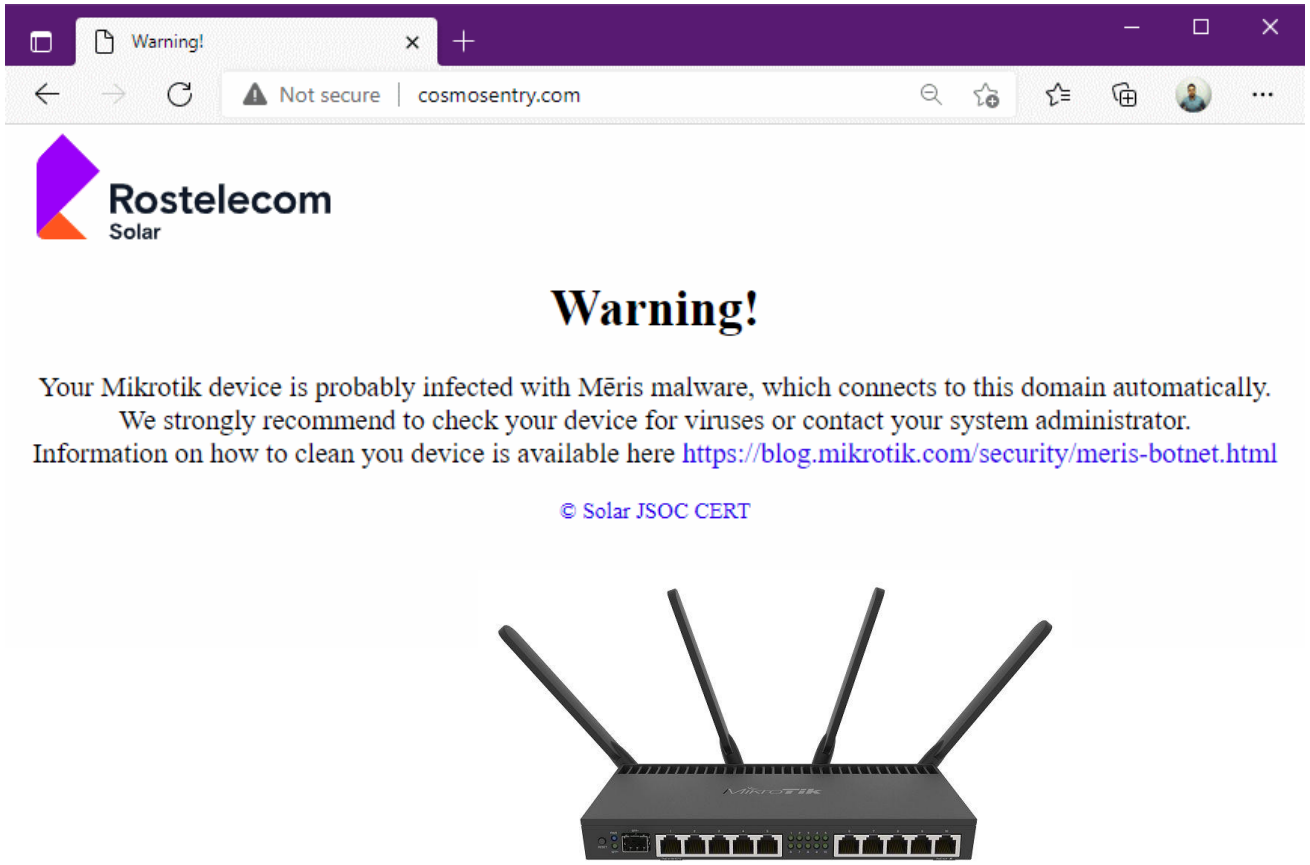
#IoTSecurity

Think of our digital economy!

#RegulateVendors

root:admin	admin:password
admin:admin	root:root
root:888888	root:12345
root:default	user:user
root:123456	root:pass
root:54321	admin:admin1234
support:support	root:1111
root:	admin:1111
admin:	root:666666





Cetome Securing a Better Future

Well Actually!

#IoTSecurity

#RegulateVendors

IoT Security is still a joke in 2021

And no one is laughing

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Patch your devices!

Change your password!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Patch your devices!

Change your password!

Use MFA!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Use MFA!

Get a VPN!

Patch your devices!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Patch your devices!

Use MFA!

Get a VPN!

Use a dedicated network!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Use MFA!

Get a VPN!

Patch your devices!

BLCOKHCAIN!11!

Use a dedicated network!

How do we secure IoT?

#IoTSecurity

#RegulateVendors

STOP

Don't buy IoT!

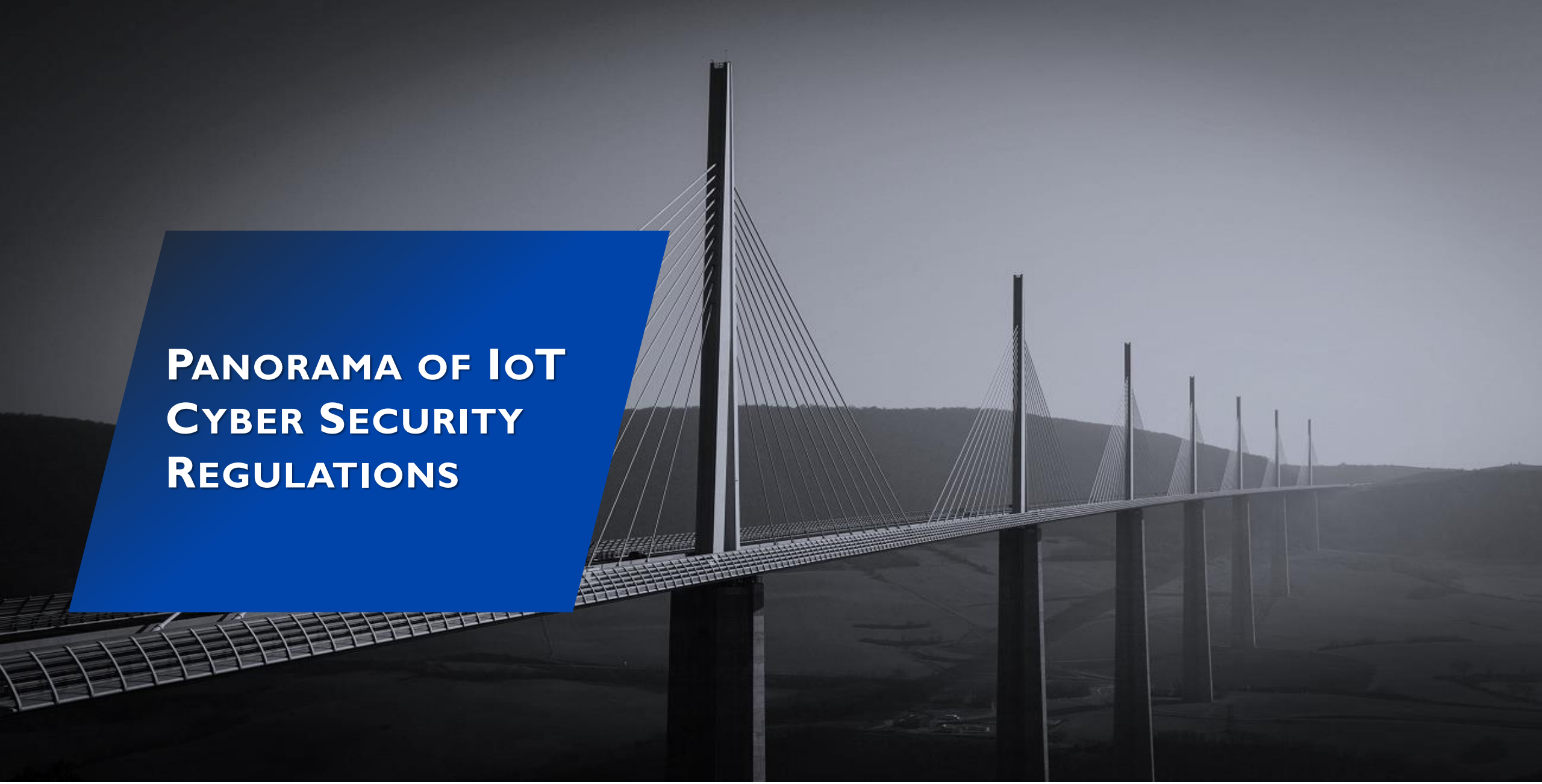
Change password!

Patch your devices!

Use MFA

Get a VPN

Use a dedicated network!



Panorama of IoT Cyber Security Regulations

Why do we need regulation?

#IoTRegulations

#RegulateVendors

Stop blaming end users!

Why do we need regulation?

#IoTRegulations

#RegulateVendors

Stop blaming end users!

Address the root causes of IoT insecurity

Why do we need regulation?

#IoTRegulations

#RegulateVendors

Stop blaming end users!

Address the root causes of IoT insecurity

Nudge corporate investments

Why do we need regulation?

#IoTRegulations

#RegulateVendors

Stop blaming end users!

Address the root causes of IoT insecurity

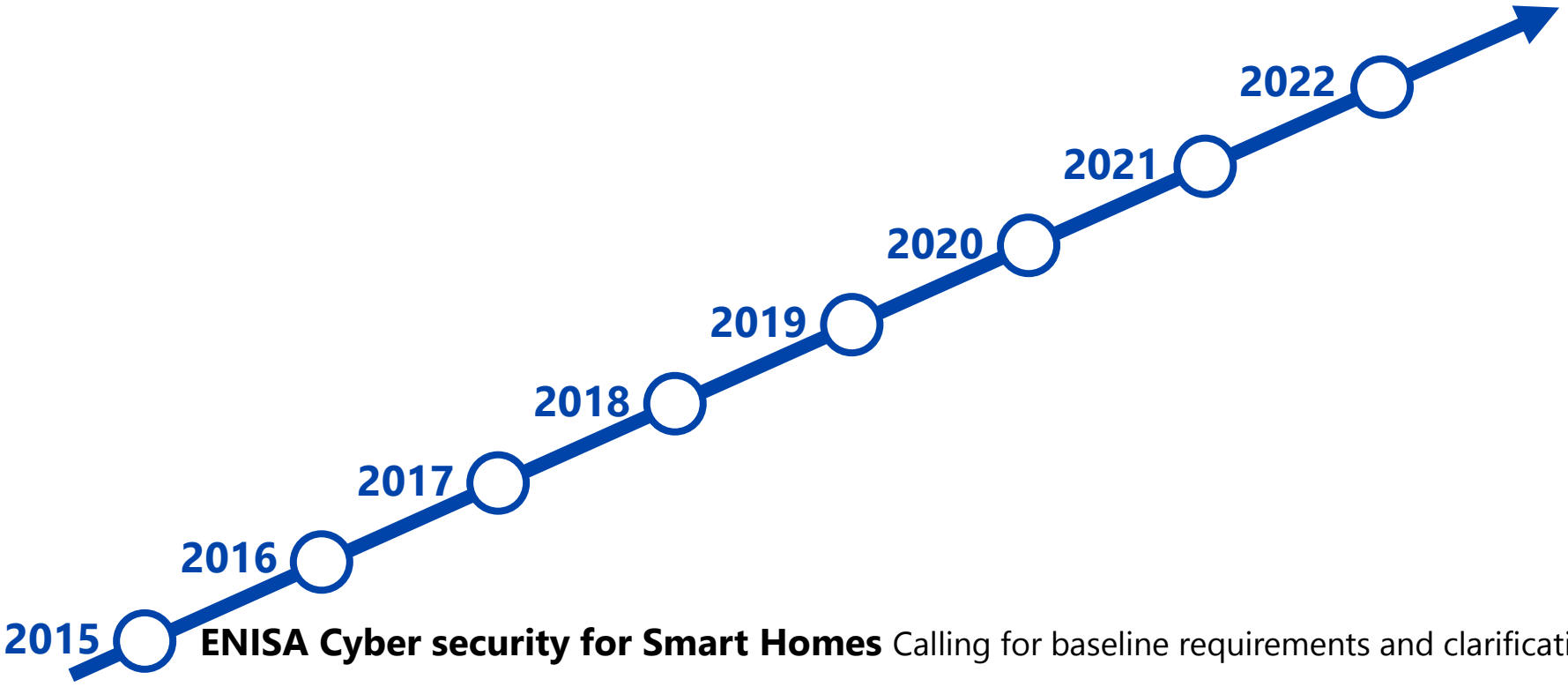
Nudge corporate investments

Clarify "best practices"

Why is regulation unavoidable?

#IoTRegulations

#RegulateVendors

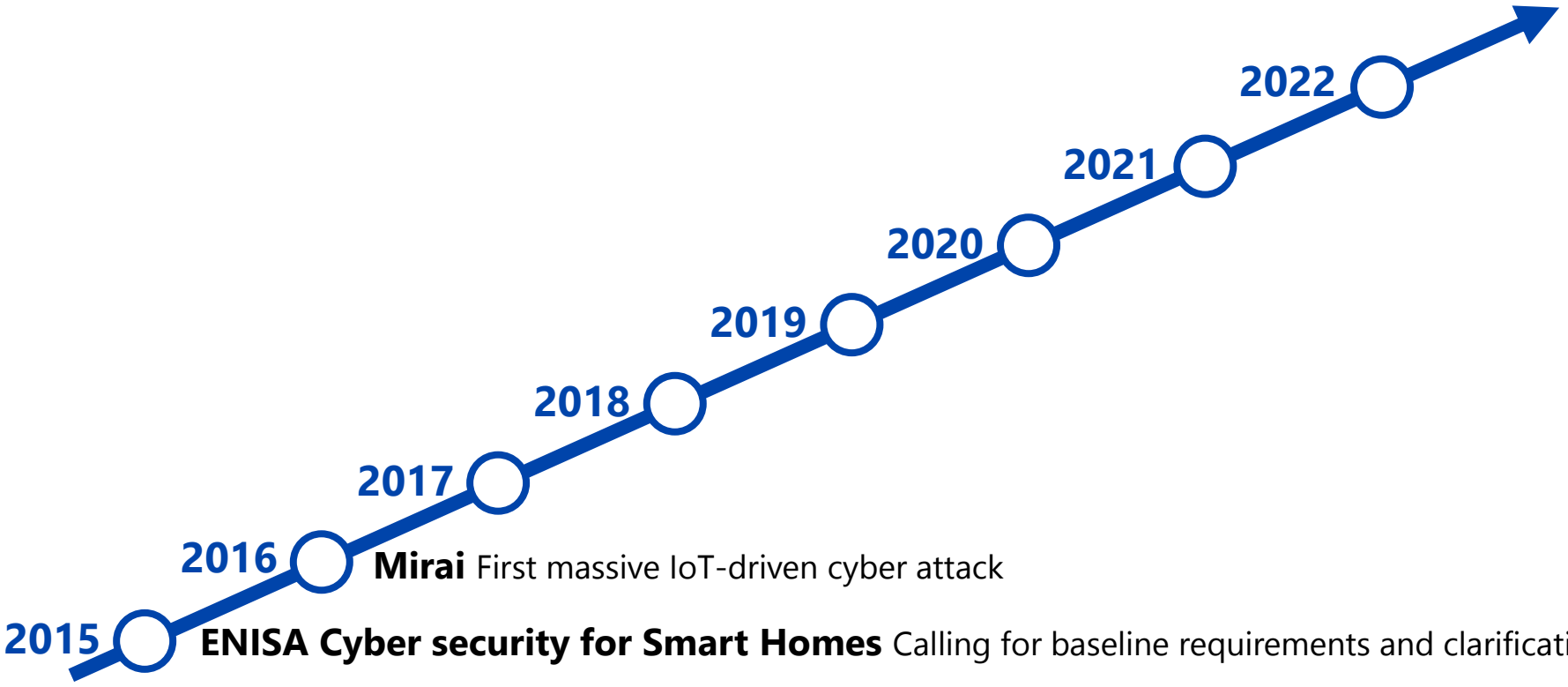


ENISA Cyber security for Smart Homes Calling for baseline requirements and clarification of corporate liabilities

Why is regulation unavoidable?

#IoTRegulations

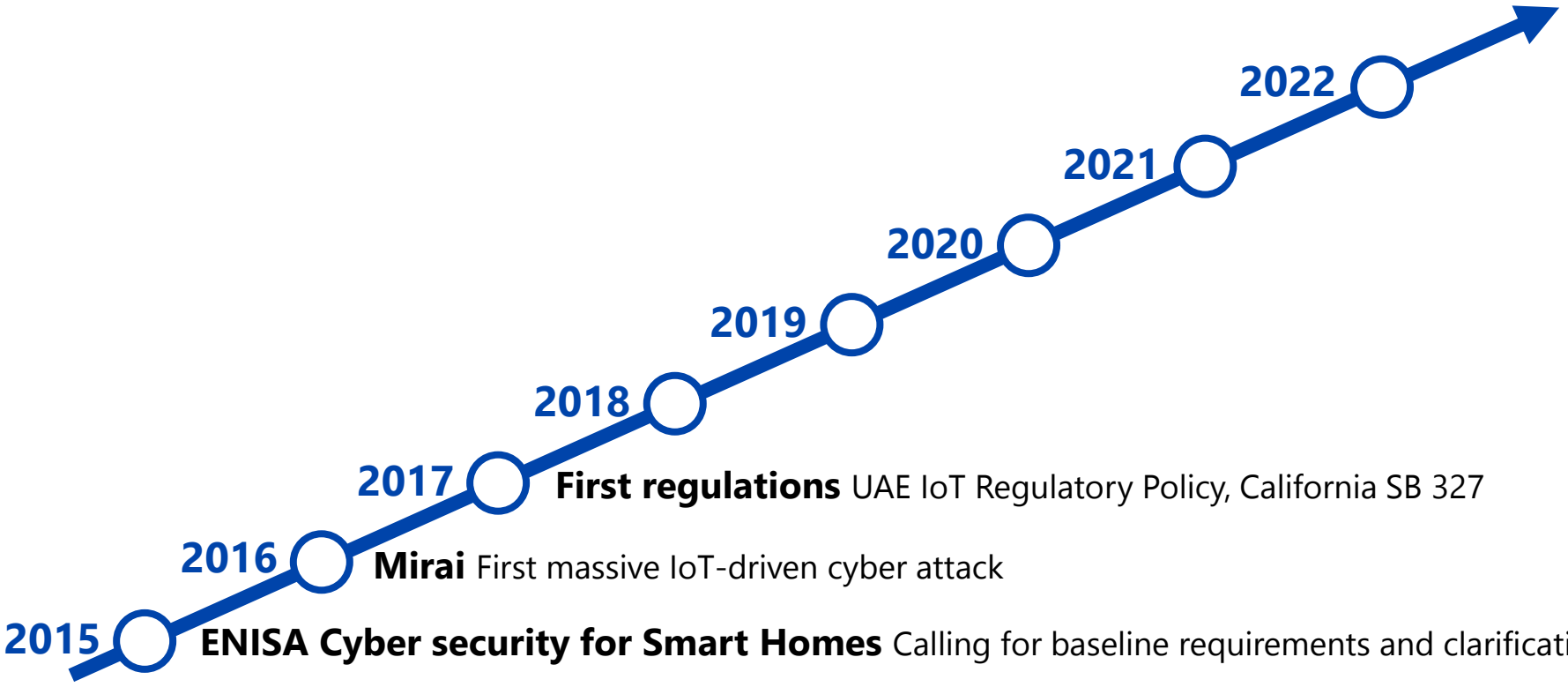
#RegulateVendors



Why is regulation unavoidable?

#IoTRegulations

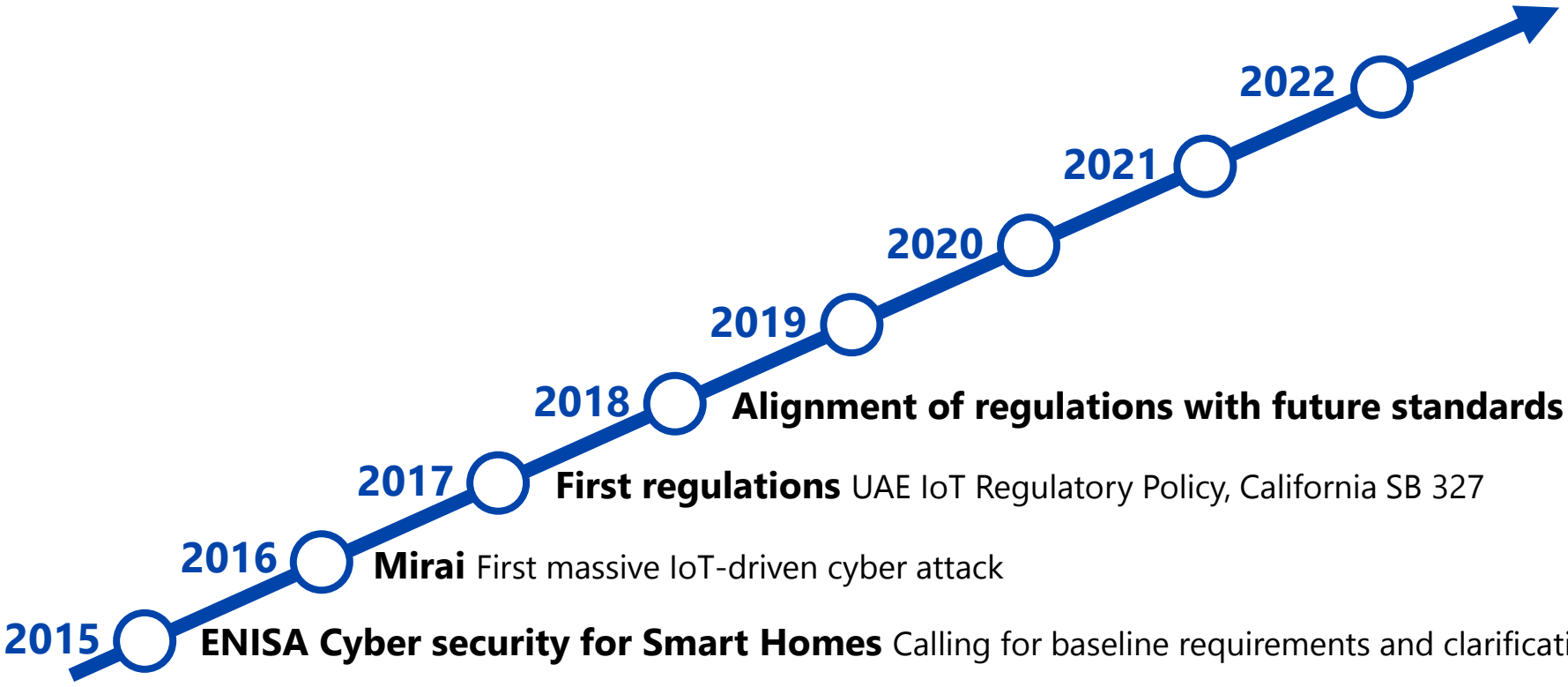
#RegulateVendors



Why is regulation unavoidable?

#IoTRegulations

#RegulateVendors



2018 **Alignment of regulations with future standards** UK Secure by Design draft

2017 **First regulations** UAE IoT Regulatory Policy, California SB 327

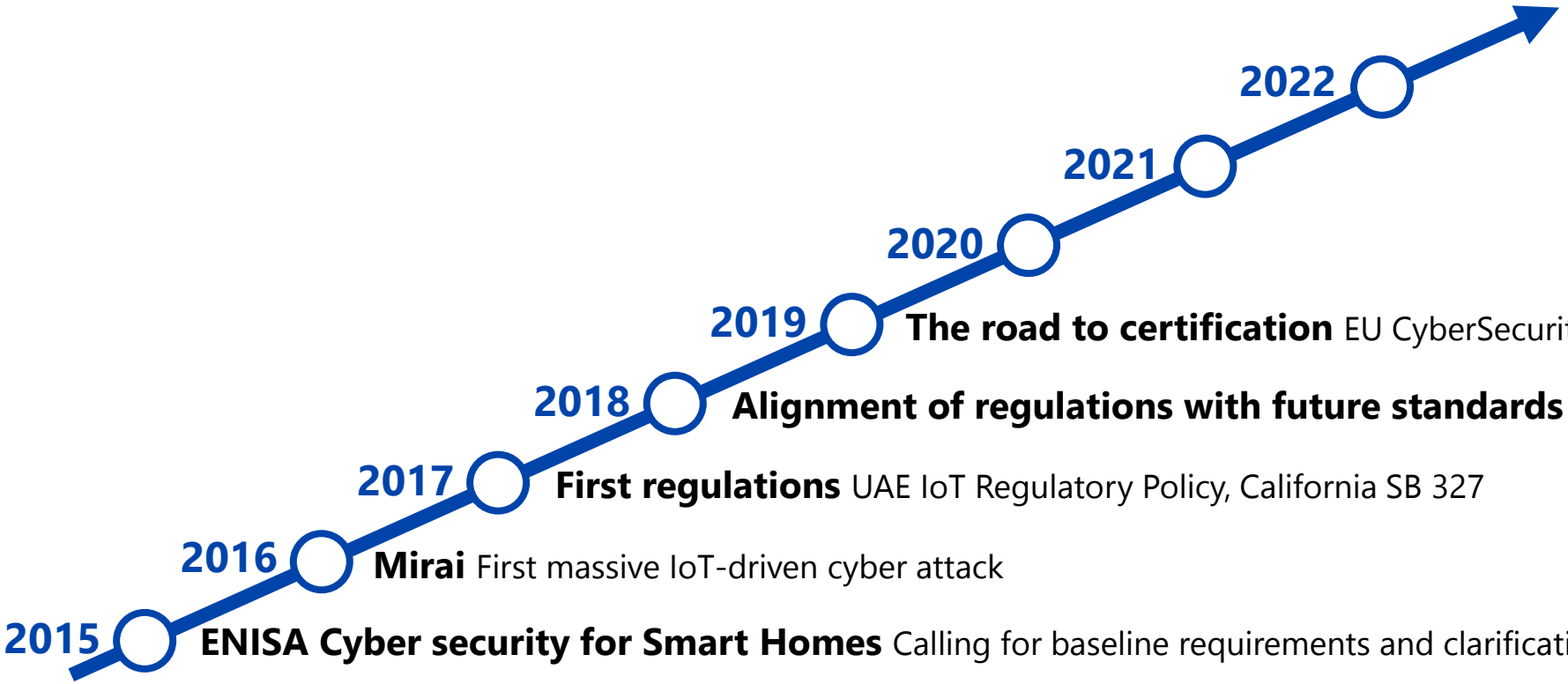
2016 **Mirai** First massive IoT-driven cyber attack

2015 **ENISA Cyber security for Smart Homes** Calling for baseline requirements and clarification of corporate liabilities

Why is regulation unavoidable?

#IoTRegulations

#RegulateVendors



2019 **The road to certification** EU CyberSecurity Act passed

2018 **Alignment of regulations with future standards** UK Secure by Design draft

2017 **First regulations** UAE IoT Regulatory Policy, California SB 327

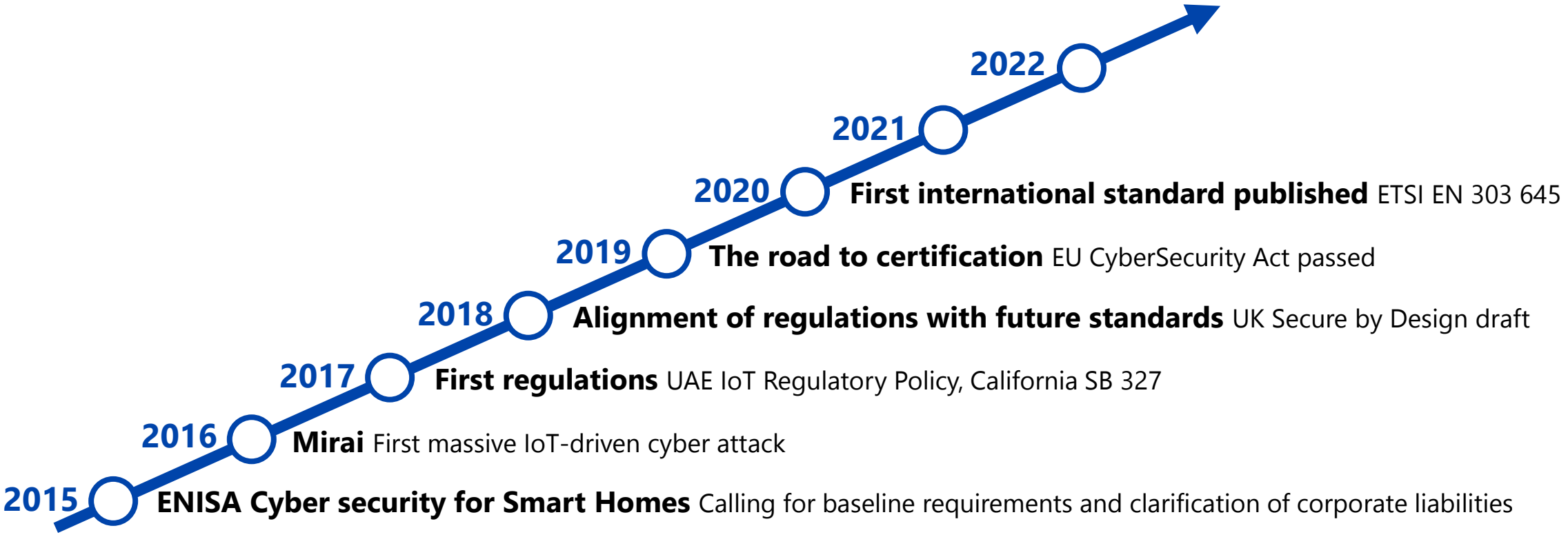
2016 **Mirai** First massive IoT-driven cyber attack

2015 **ENISA Cyber security for Smart Homes** Calling for baseline requirements and clarification of corporate liabilities

Why is regulation unavoidable?

#IoTRegulations

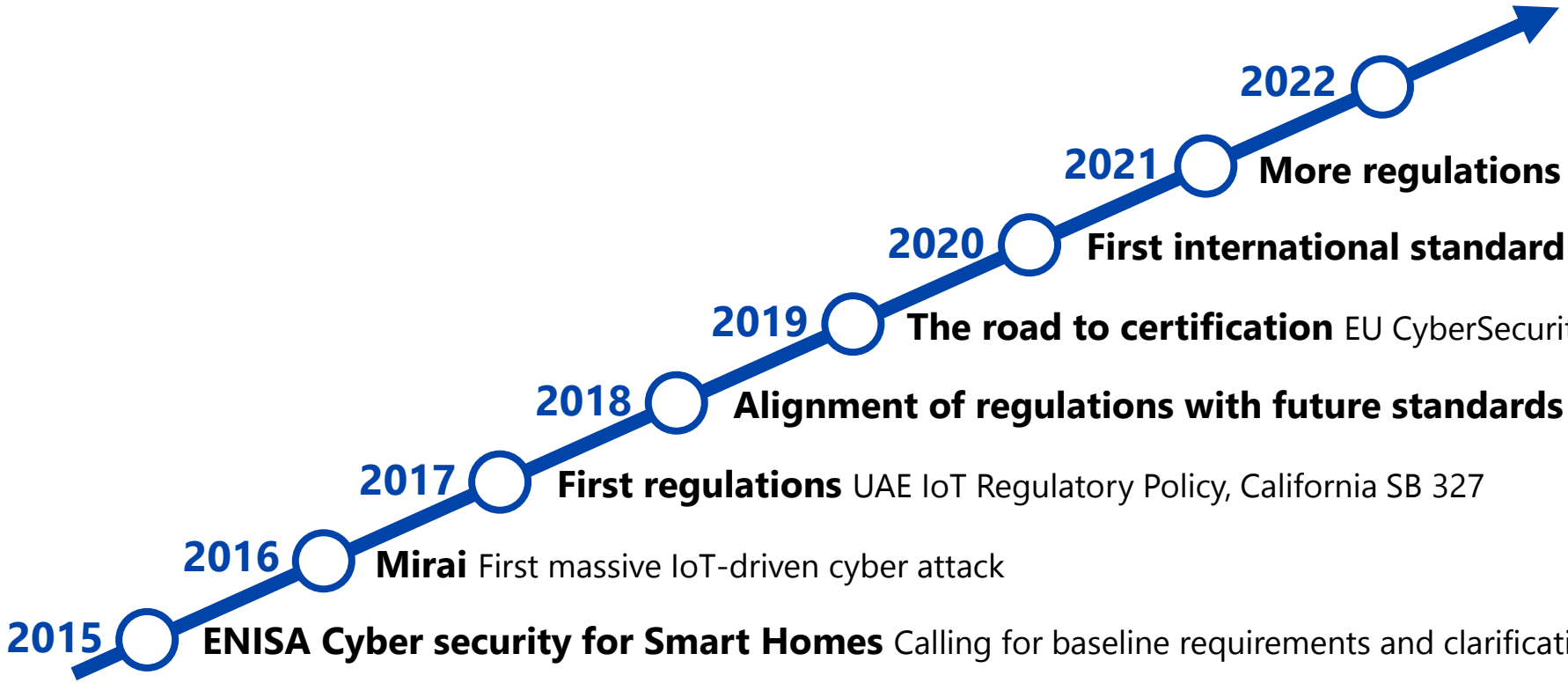
#RegulateVendors



Why is regulation unavoidable?

#IoTRegulations

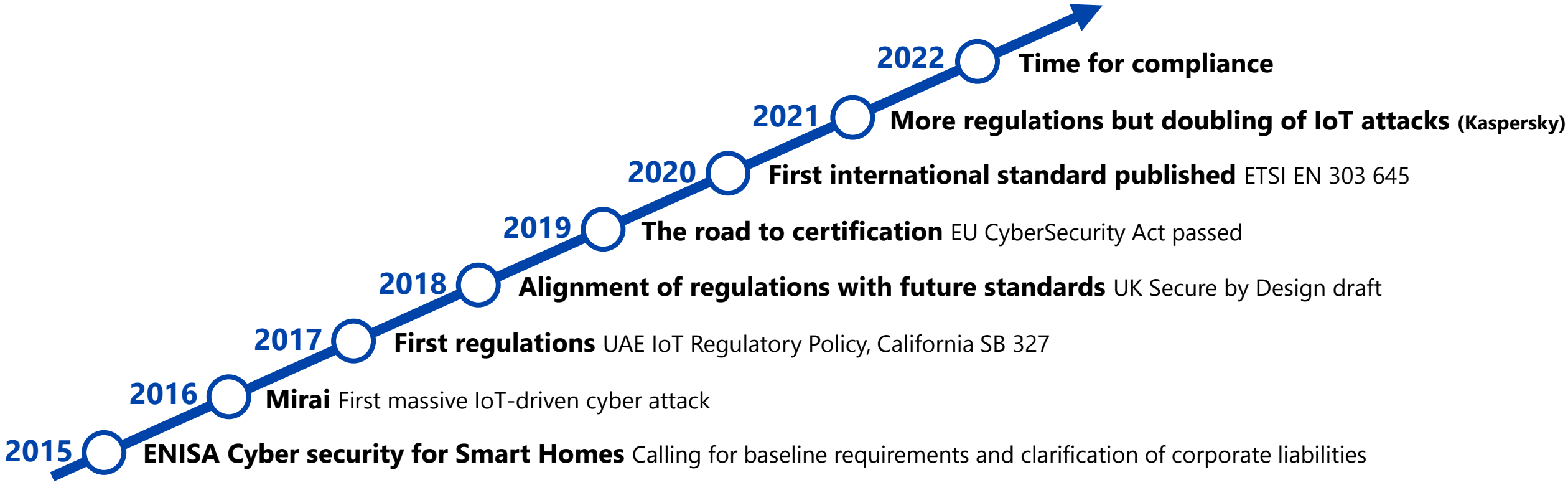
#RegulateVendors



Why is regulation unavoidable?

#IoTRegulations

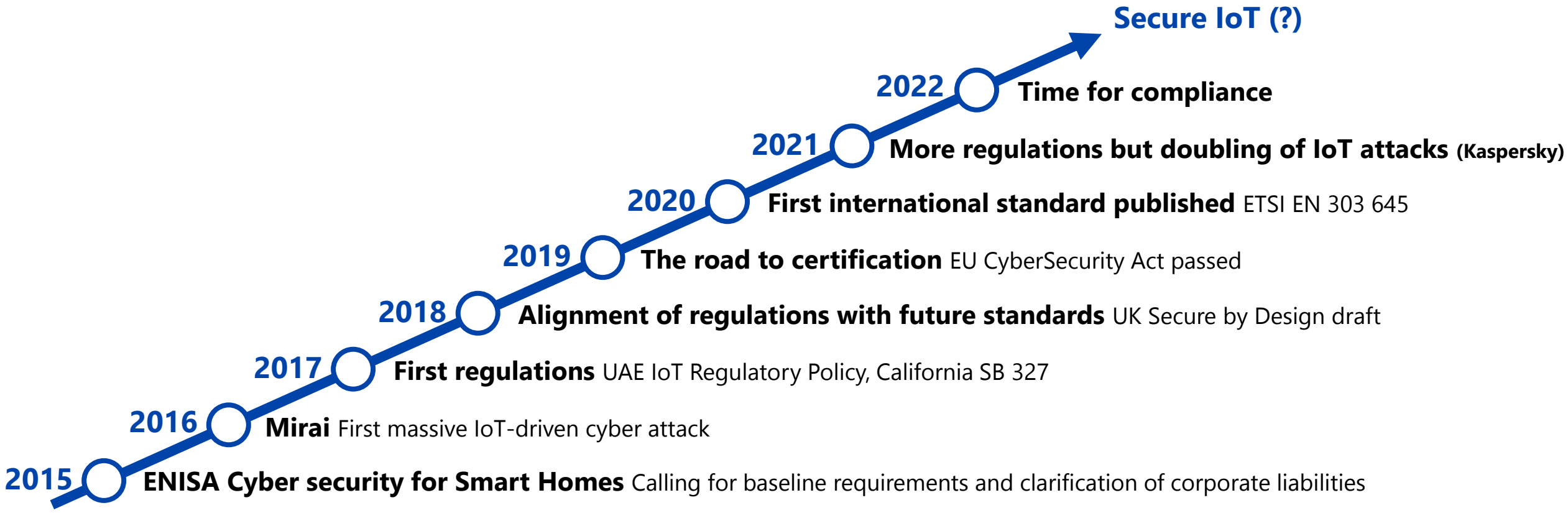
#RegulateVendors



Why is regulation unavoidable?

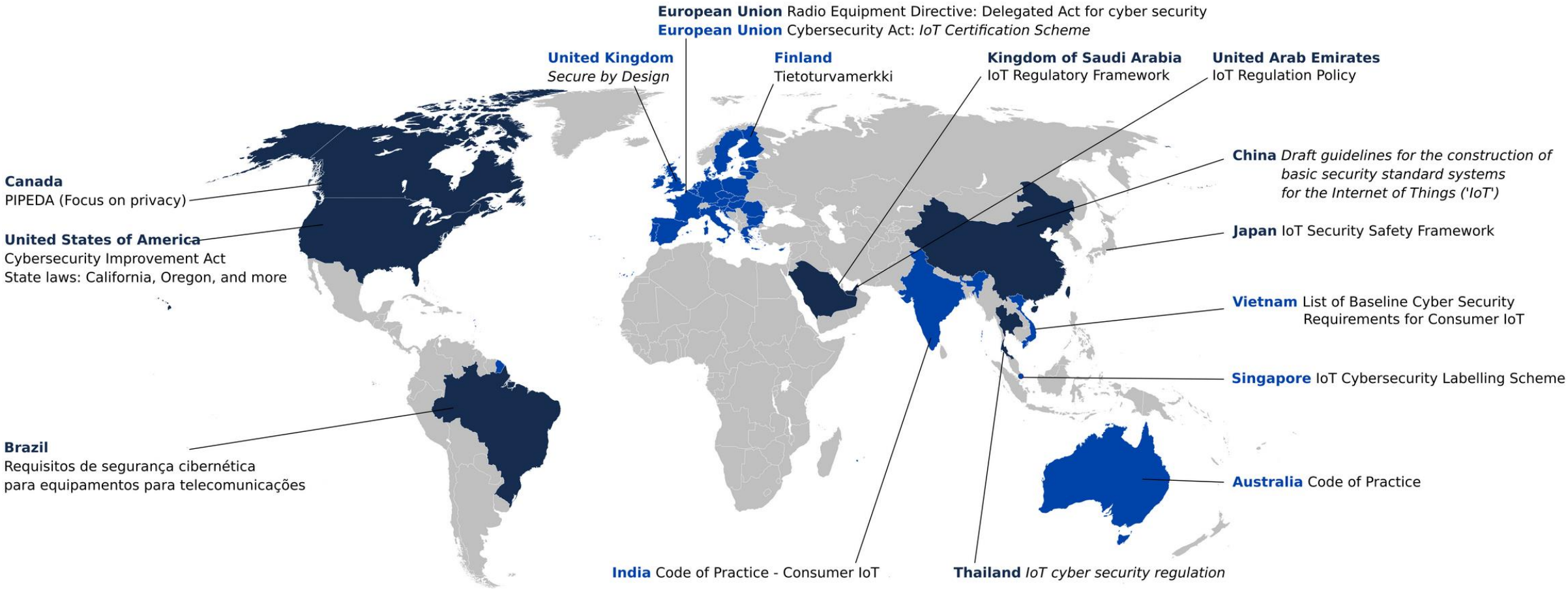
#IoTRegulations

#RegulateVendors



Panorama of IoT Cyber Security Regulations #IoTPanorama

cetome.com/panorama #IoTRegulations



- **Regulation based on ETSI EN 303 645**
- **Possible compliance by following ETSI EN 303 645**
  On-going work

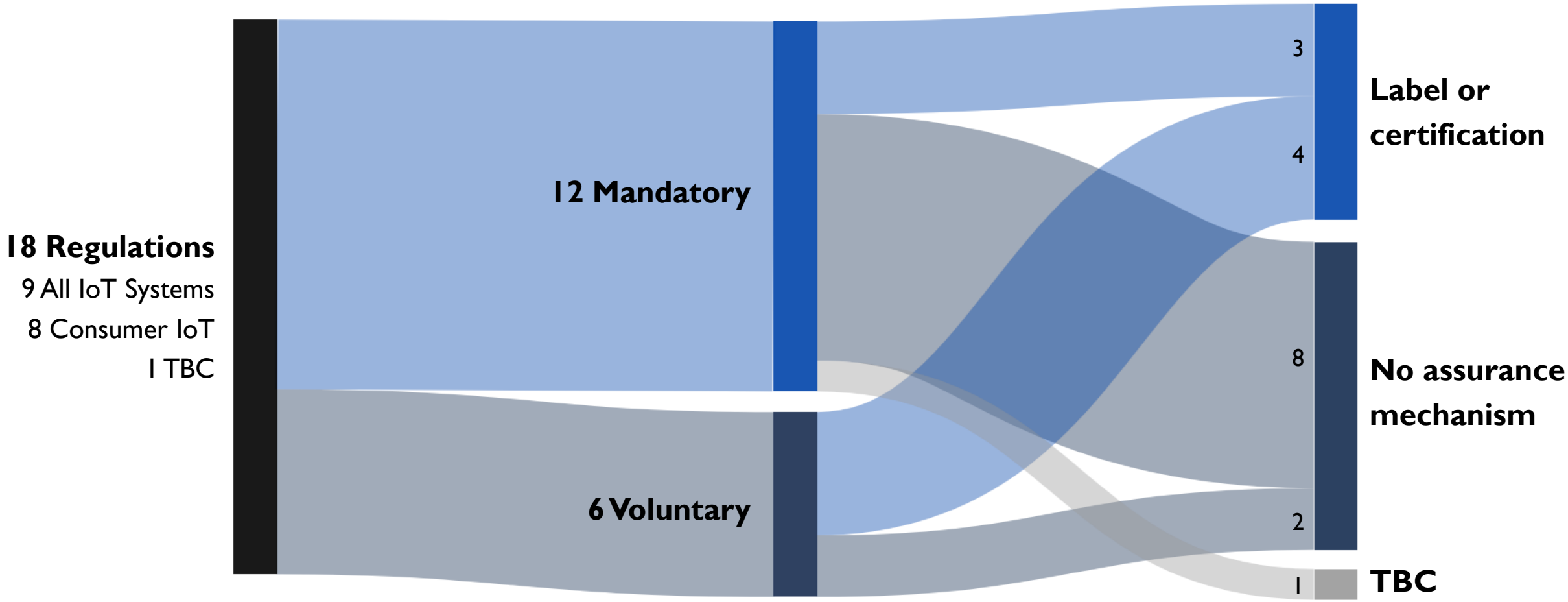
A world of IoT cyber security regulations

Cetome Securing a Better Future

Overview of IoT Cyber Security Regulations

#IoTPanorama

#IoTRegulations



Cetome Securing a Better Future

Do your own research they say. Here are the results

#IoTPanorama

#IoTRegulations

Ensure regulation is fit for purpose

Baseline requirements (17/18)

Alignment with standards (all)

#RegulateVendors (17/18)

#RegulateEndUsers (2/18)

Some will #RegaluateRetailers (2/18) and #RegulateServiceProviders (3/18)

Ensure regulation is followed

Enforcement is key (12/18)

Assurance mechanisms to inform customers, especially for voluntary regulations (4/6)

Self-assessment vs third-party certification

How to succeed in a world of IoT regulations?

How to succeed in a world of IoT Regulations?

Policy Makers

Future-proof your policy requirements

Have **clear requirements** that do not leave place to interpretation

Rely on **international standards** for implementation and verification

Support regulated entities to achieve compliance

Have the means for **strong and fast enforcement**

Manufacturers and Regulated Entities

Have a **security governance for IoT** to drive compliance

Have **technical means** to meet baseline requirements

Must do:

- **Training** on requirements and standards
- **Threat modelling** and **risk assessment**
- Secure **implementation and verification**
- **Post-release security activities** (vulnerability management, secure patching)
- **Documentation** (in-house and for end users)

IoT Security ProTips

Learn about ETSI EN 303 645 to achieve compliance with new regulations

Duration: ½ day
Audience: Project managers, programme managers, future IoT security experts, software developers, non-IoT security consultants, senior management

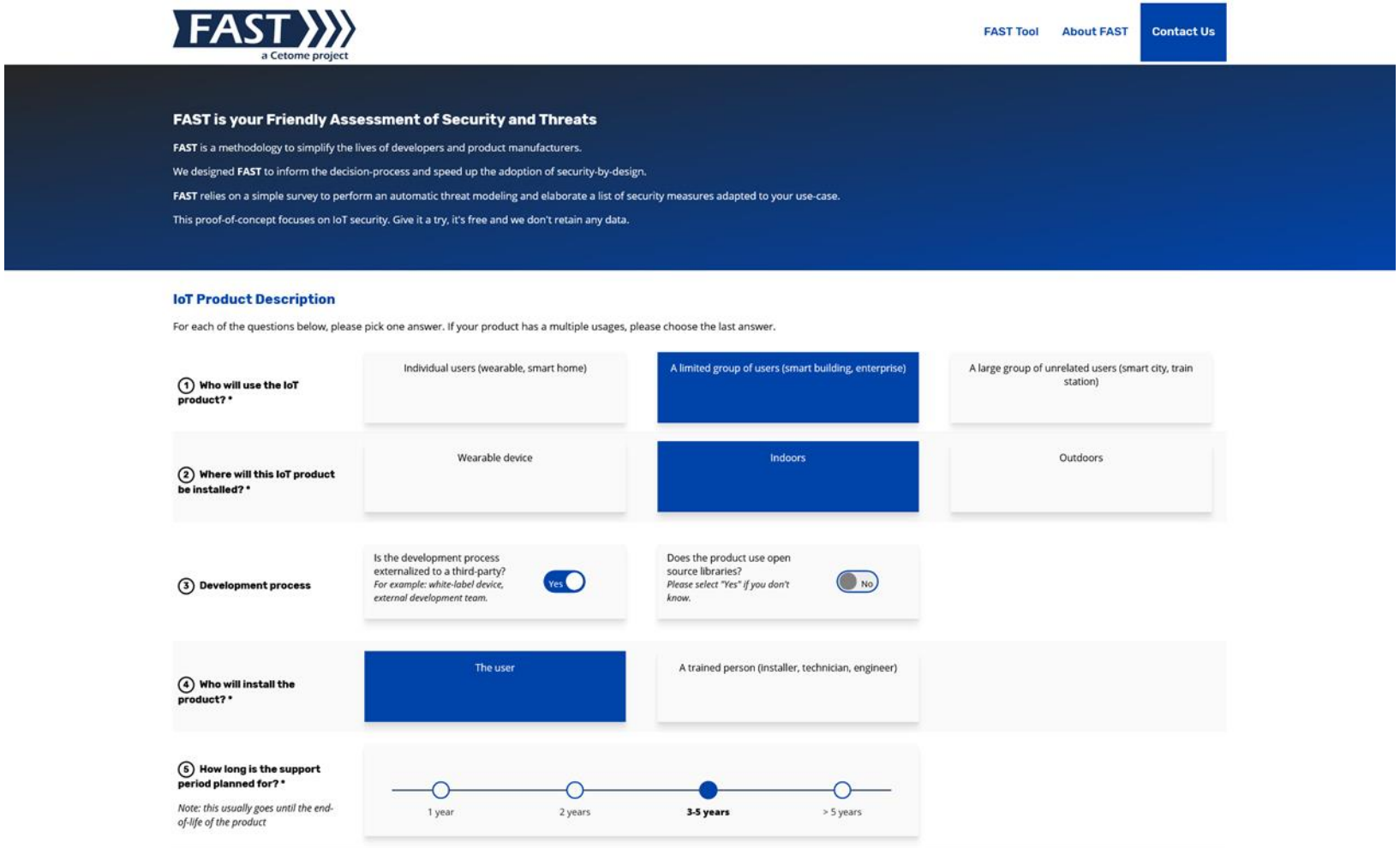
Objectives: **discover ETSI EN 303 645** and understand how you can **drive IoT cyber security in projects**

Duration: 2 days
Audience: Software developers, product managers, IoT manufacturers, security consultants, security experts, auditors

Objectives: become proficient at ETSI EN 303 645 to **comply with IoT security regulations and achieve certification worldwide**

IoT Security ProTips

Simplify threat modelling and compliance with #FAST (fast.cetome.com)



Cetome Securing a Better Future

IoT Security ProTips

Simplify threat modelling and compliance with #FAST (fast.cetome.com)

71 Security Measures applicable

Do you need help for the next steps? Do you want to customize FAST? Contact us! We will be happy to help you.

Export to CSV

id	IoT security measures	Descriptions	Threats mitigated	ETSI provisions fulfilled	Decision
[IoT-001]	Require password change at first boot	The easiest way to implement Security-by-Default.	[T-002] Broken authentication	[5.1-1]	Todo
[IoT-002]	Implement password rules to avoid basic default passwords	The default password must not be guessable nor follow a pattern: *password*, *password1*, *manufacturer123*, *admin*	[T-033] Legal threat [T-046] Backdoor	[5.1-1]	Counter-measure
[IoT-003]	Generate secure individual passwords for each device.	When each device or service has its own randomly generated password, it becomes virtually impossible to guess.	[T-001] Lack of unique identity [T-002] Broken authentication [T-003] Unauthorized access	[5.1-3]	Will not be done
[IoT-004]	Do not use public information to generate passwords.	It is easy for an attacker to guess the password for all devices when using public information (e.g. MAC address, Serial Number)	[T-001] Lack of unique identity [T-019] Reverse engineering	[5.1-3]	N/A
[IoT-007]	Remove passwords for authentication	When communicating with Cloud systems, it is preferable to use tokens to protect authentication information. When using mobile applications, it is possible to rely on biometrics to authenticate a human user.	[T-001] Lack of unique identity [T-019] Reverse engineering	[5.1-3]	Todo
[IoT-008]	Authenticate machine-to-machine communications with certificates	Certificates can be generated in factory or at first boot.	No threat computed but mandatory requirement from the standard	[5.1-3]	Todo

Top threats (occurrence)

31 threats computed

- [T-017] Information Leakage (9)
- [T-033] Legal threat (9)
- [T-021] Issue related to security requirements (8)
- [T-008] Insecure dependency (8)
- [T-032] Lack of Privacy Considerations (8)
- [T-040] Denial of Service (8)
- [T-044] Insecure protocols (8)
- [T-003] Unauthorized access (7)
- [T-034] Malicious Code (7)
- [T-023] Remote Code Execution (6)
- [T-035] Use of asset in cyberattacks (6)
- [T-016] Insecure encryption (6)
- [T-046] Backdoor (6)
- [T-006] Escalation of privileges (6)
- [T-037] Physical tampering (5)

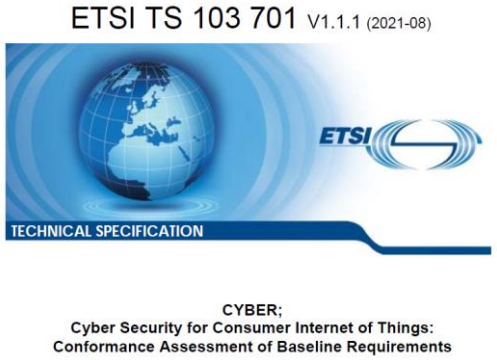
Discussion on the future and conclusions

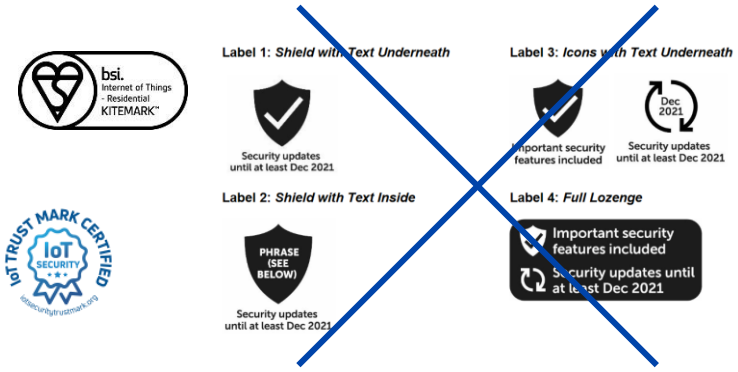
The future of IoT Regulations

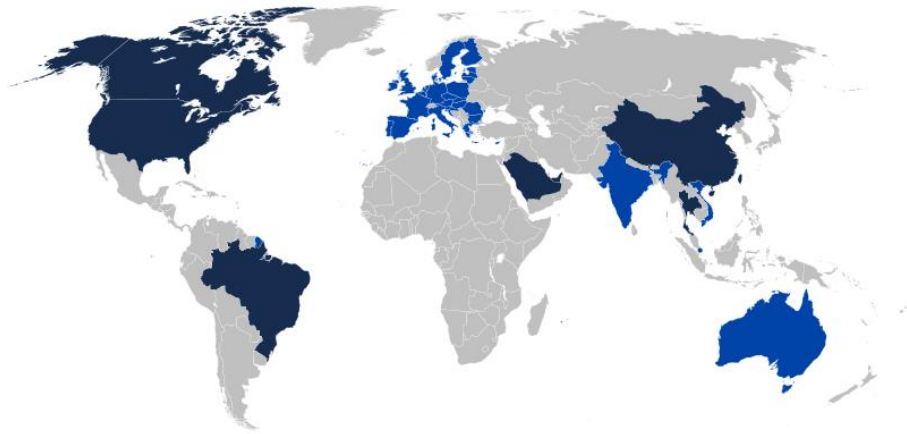
#IoTSecurity

Verification, certifications, labels, more regulations, globalisation

#RegulateVendors







A world of IoT cyber security regulations

Cetome
Securing a Better Future

Conclusion

IoT Cyber Security Regulation is here

- Finally a way to secure IoT systems?
- Regulations must align with standards
- Support to manufacturers is key to success

Still a new domain

- Awareness remains an important topic
- Need for robust enforcement mechanisms
- Lack of harmonization globally

The “S” in IoT Security is a “R”

Thank you!

cetome.com

Cetome
Securing a Better Future