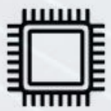
CyberWhiz

IoT Cyber Security Excellence

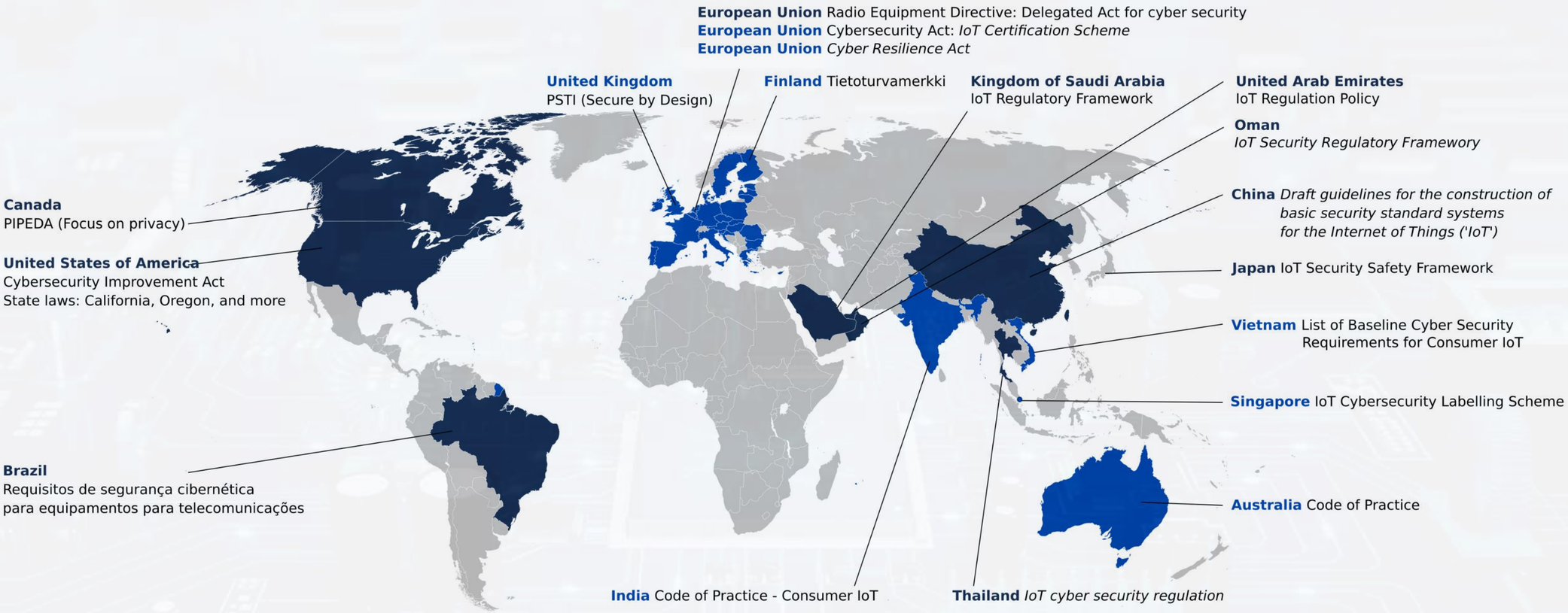
for

Edge · Mobile · Cloud



www.cyberwhiz.co.uk

IoT Cyber Security Regulations (Global Footprint)



UK is a subset of ETSI EN303645. UK's PSTI Legislation is active since **April 2024!**
Deadline for being %100 compatible to EN 18031 standard for all IoT device manufacturers for **EU** is **August 2025!**

There are 50+ Mandatory Provisions that every IoT manufacturer should comply.

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

Source: https://cetome.com/panorama

IoT Cyber Security Regulations

Active since April 29, 2024

EN303645 based

Only **3 of 33** mandatory provisions

Self Declaration

Active since August 1, 2025

EN18031 based

More than **50** provisions

Self Declaration/Notified Body

Mandatory after **September 11, 2026**

Product with digital elements

71 Articles + 8 Annexes

Self Declaration/Notified Body

CRA is much more difficult than others..

Risk Assessment & **DoC***

Secure by Design Principles

Regular **End-to-End** IoT Penetration Tests

Continuous Logging/Monitoring

5-year Security Support

SBOM** Management

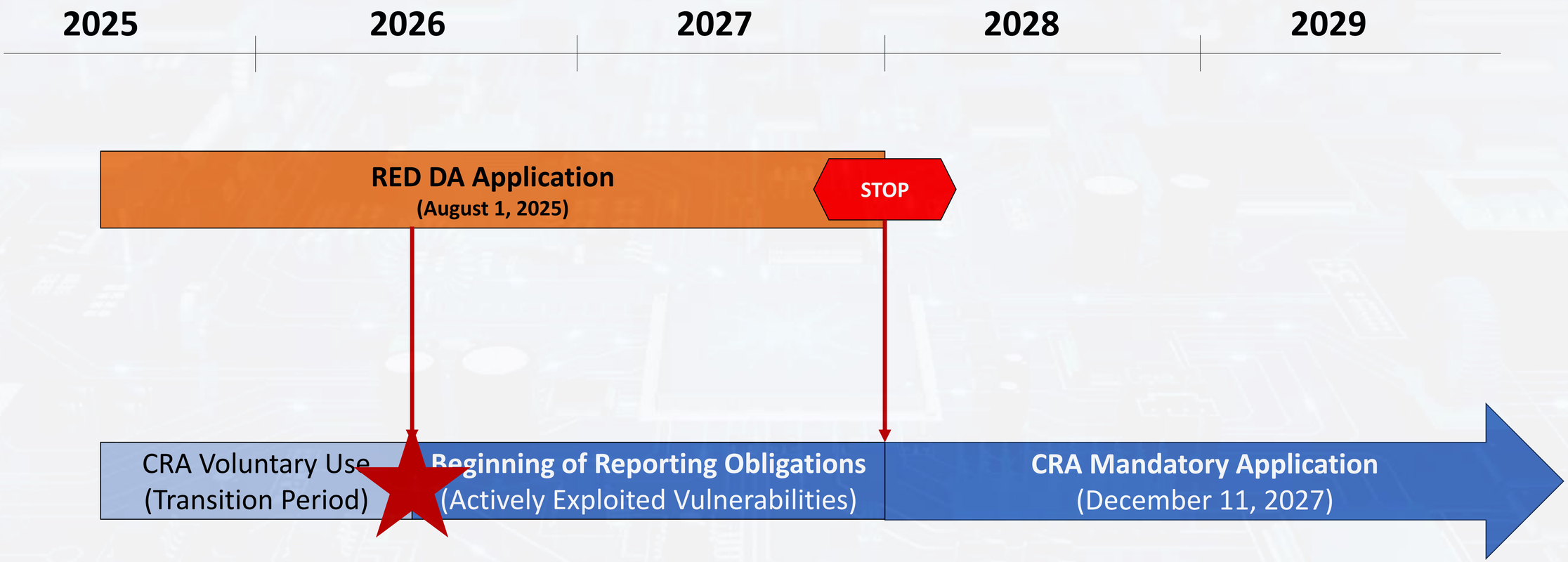
Vulnerability Handling in **1/3/14 days**

Vulnerability Disclosure Policy

OTA / SUMS***

* Declaration of Conformity
** Software Bill of Material
*** Software Update Management System

CRA Transition Period



What is Cyber Resilience Act(CRA)?

Official Journal
of the European Union

EN
L series

2024/2847

20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

81 pages

71 Articles + 8 Annexes

Definition of ‘Product with Digital Elements’

‘Product with digital elements’ is defined as

a **software or hardware** product and **its remote data processing solutions**,

including software or hardware components being placed on the market **separately**

What is the scope of ‘Product with Digital Elements’?

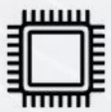
This is the most frequently asked question so far

(1st question over 71 FAQs)

- Various types of **hardware**, such as more foundational components (e.g. integrated circuits, motherboards; sensors); consumer devices (e.g. smartphones, laptops, smart fridges); complex devices (e.g. industrial IoT devices, machinery).

- Standalone software that can be downloaded and installed on a device, e.g. a **mobile app** that can be downloaded via an app store, or **a program** that can be downloaded via a website;

- Also includes its **remote data processing solutions**

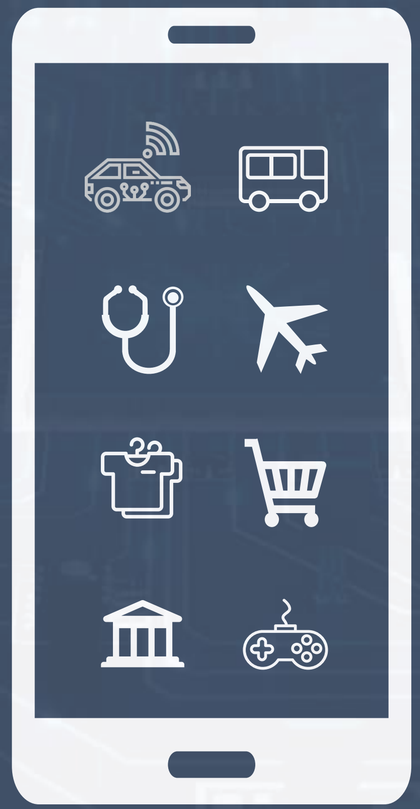


Source: https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

Scope of CRA

Edge Devices

Mobile Applications

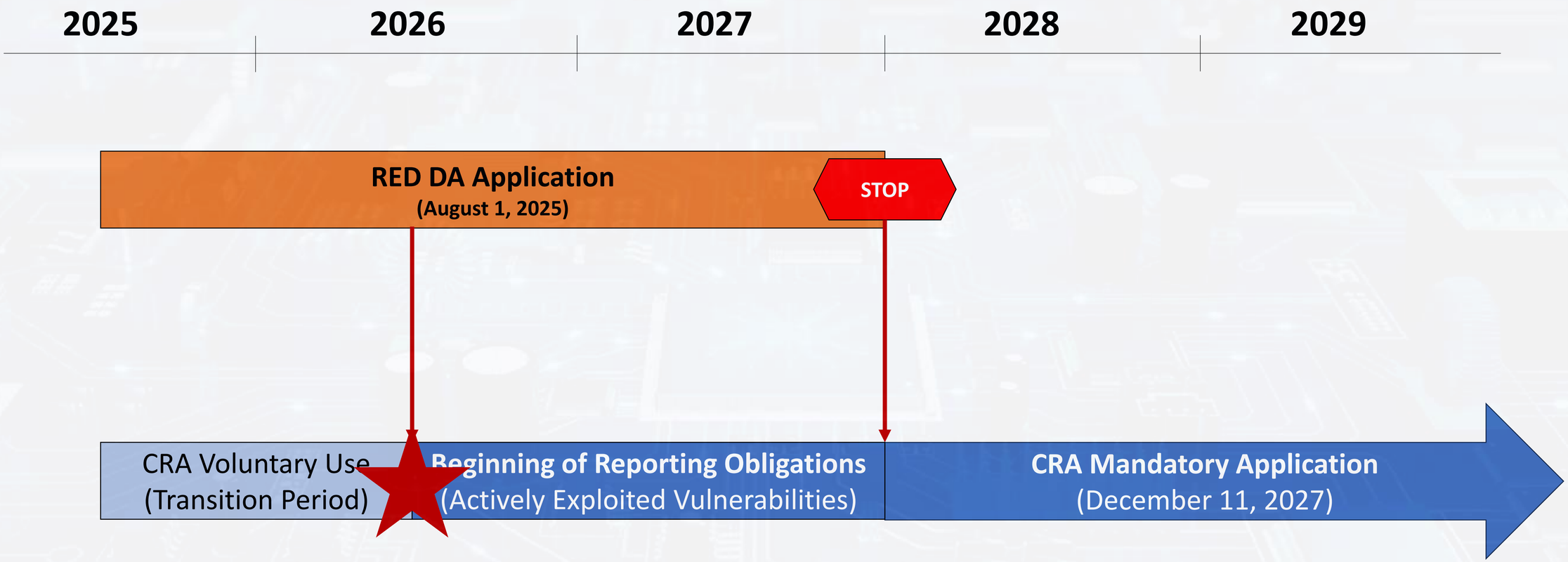


Cloud/Web Services

Product Categorisation

Default Category	Important Products Class-I	Important Products Class-II	Critical Products
Home Appliances	Smart Door Locks	Firewalls	HW Devices with Security Boxes
EV-Chargers	Home Alarm Systems	Intrusion Detection Systems	Smart Meter Gateways
Mobile Applications	Baby Monitoring	Tamper resistant microcontrollers	Smartcards
Telematic Control Units	Security Cameras	Tamper resistant microprocessors	
Computer Games	Connected Toys		
Memory Chips	Personal Wearables		
Smart Thermostats	Identity Management Systems		
	Embedded Browsers		
	Password Managers		
	Antivirus Softwares		
	VPNs, SIEMs, Boot Managers		
	PKI and Certificate Management Softwares		
	Routers and Modems		
	Secure MCU & MPU & FPGA & ASIC		
SELF DECLARATION	**NOTIFIED BODY**	**NOTIFIED BODY**	**NOTFIFIED BODY**

CRA Transition Period



CRA Annex 1 / Part 2 Vulnerability Handling Requirements

Manufacturers of products with digital elements shall:

1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a **software bill of materials** in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;
2) in relation to the risks posed to products with digital elements, address and **remediate vulnerabilities without delay**, including by providing **security updates**; where technically feasible, new security updates shall be provided separately from functionality updates;
3) apply **effective and regular tests and reviews** of the security of the product with digital elements;
4) once a security update has been made available, share and **publicly disclose information about fixed vulnerabilities**, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;
5) put in place and enforce a policy on **coordinated vulnerability disclosure**;
6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by **providing a contact address** for the reporting of the vulnerabilities discovered in the product with digital elements;
7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that **vulnerabilities are fixed or mitigated in a timely manner** and, where applicable for security updates, in an automatic manner;
8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, **free of charge**, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Placed on the Market Detail

Article 69

Transitional provisions

1. EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to Union harmonisation legislation other than this Regulation shall remain valid until 11 June 2028, unless they expire before that date, or unless otherwise specified in such other Union harmonisation legislation, in which case they shall remain valid as referred to in that legislation.

2. Products with digital elements that have been placed on the market before 11 December 2027 shall be subject to the requirements set out in this Regulation only if, from that date, those products are subject to a substantial modification.

3. By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027.

Article 14

Reporting obligations of manufacturers

1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.

How can CyberWhiz assist you with CRA compliance?

CyberWhiz supports you

holistically and **continuously**

to meet **all** CRA requirements

and avoid **€15,000,000** penalties.

CyberWhiz Location and Shareholder Details

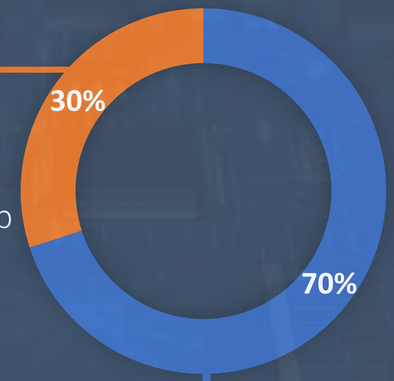
Location

HQ — UK, Cheltenham
(Center of UK's cyber security cluster)

R&D — Turkey, Kocaeli
(Science Park)

Strong Ownership Structure

Koç
Fortune 500 Company
The biggest group of Türkiye



All employees are shareholders

Spin-off from Beko

beko

EU's #1 home appliance manufacturer

We were Beko's, ex IoT Cyber Security team

Our vision is to be the global leader in providing **holistic** IoT Cyber Security solutions for **Edge·Mobile·Cloud**, securing at least one smart device and its mobile app in every home and street across the World.

Unique IoT Cyber Security Experience

2016

Hardware Security Module
integration into
IoT products

AUTHORIZED MICROCHIP DESIGN PARTNER

2018

IoT Security Foundation
Championship
Award

2019

The first Common Criteria
approval in EAL2 level
in the home appliance industry

Common Criteria

2021

The first company in UK
who got Silver Level certificate
from IASME product security assessment

IASME CYBER ASSURANCE

2022

Arm
Platform Security Architecture
Level-1 Certificate

psacertified™

2024

Koç VC Investment
%30

CyberWhiz

2025

Embedded World
3rd Best Start-Up

Leadership Team and Advisory Board

Çağatay Büyüktopçu
Founder CEO
20 years experience
Embedded Systems&Security

Beren Kuday Görün
Chief Security Architect
9 years experience
Offensive&Defensive Security

Anıl Doyran
Blue Team Manager
7 years experience
Embedded Security&Cryptology

Can Akçınar
Red Team Manager
7 years experience
Offensive Security

Ali Ergün
Automotive Cybersecurity Mng.
11 years experience
Embedded Systems&Security

Olcay Sevim
Purple Team Director
20 years experience
Governance

Nuri Dağdeviren
Microchip, VP of Security
30 years experience
Semiconductor Industry

Prof.Siraj Ahmed Shaikh
Swansea Uni.
30 years experience
Automotive Cybersecurity

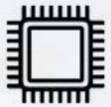
John Moor
IoTSF Director
30 years experience
Regulation&Legislations

Prof.Erkay Savaş
Sabancı Uni.
30 years experience
Post Quantum Cryptography

Trusted by Leading Brands

beko
VESTEL
karaca®
VitrA
BELBİM
DESi
gread elettronica
DUEPI group srl
finder®
monolitic
TRIOMOBIL
Litum
MYPV Empowering the Solar Future
BMC
ANADOLU ISUZU
Otokar
hera
wat
Tüpraş
QUANTUM DICE

End to End IoT Cyber Security includes Edge · Mobile · Cloud



Edge Security

Mobile Application Security

Cloud Security

But each domain requires different expertise

CyberWhiz IoT Cyber Security Solutions

Edge Security

We secure
any edge device
for any regulation

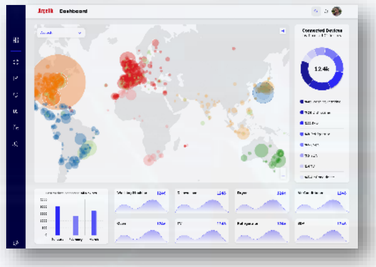
Our solution is
HW/SW/Industry
agnostic

Mobile Application Security

We secure
IoT
Mobile Applications.

We secure
wireless communications
between edge &mobile

Cloud Security



24/7 live edge and mobile security
monitoring with
CyberWhiz Defence Center

We detect
any cyber risks
instantly

We cover all three domains holistically, including the RF communications between them.

CyberWhiz IoT Cyber Security Services

RED TEAM

Offensive security

Embedded Penetration Tests

Mobile App Reverse Engineering

End to End Vulnerability Analysis

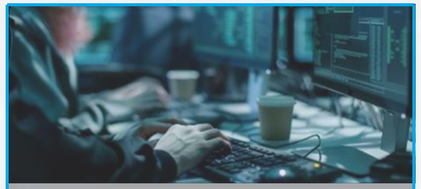
PURPLE TEAM

Standards&Regulations

IoT Security Monitoring

Consultancy for compliance

RED DA & CRA & 155&156



BLUE TEAM

Defensive security

Embedded Security Design

Mobile Application Security

Cloud Security Design

Some End-to-End Secure IoT Project Deployments So Far

Eczacıbaşı Vitra

CyberWhiz Embedded
Hardware and Software Security Integration

CyberWhiz Mobile Integration
for iOS&Android Mobile Application

CyberWhiz Defence Center
usage for **RED DA** and **CRA** compliance

Continuous **SBOM** management
for Edge · Mobile · Cloud

AWS IoT Cloud Services design
from scratch

Otokar All-in-One-Diagnostic

Key Management software
for **R155&R156** compliance

TARA analysis, training
and workshops

CyberWhiz Defence Center
usage for **R155 & R156** compliance

Continuous **SBOM** management
for Edge · Cloud

Telematic Control Unit
edge software

Hera EV-Charger

OCPP Server design and
implementation from scratch

CyberWhiz Mobile Integration
for iOS&Android Mobile Application

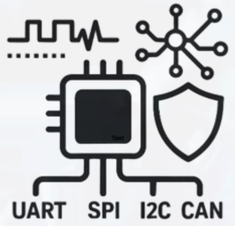
CyberWhiz Defence Center
usage for **RED DA** and **CRA** compliance

Continuous **SBOM** management
for Edge · Mobile · Cloud

AWS IoT Cloud Services design
from scratch

CyberWhiz Embedded Software Security Solutions

Dynamic Threat Monitoring



Host Intrusion Detection System
(HIDS) algorithms for embedded systems

Detection of **wired** (UART, SPI, I²C, CAN-bus) and **wireless** (Wi-Fi, Bluetooth) **anomalies** in real time

Runs **silently in the background**
ensuring no impact
on device performance or connectivity

Security Anomaly Detection

Detects abnormal activities including
port scans, and **suspicious network behaviour**.

Transmits collected security data to the cloud via
mTLS-encrypted MQTT for centralized monitoring.

Monitors critical system metrics such as
kernel logs, system **uptime**, **memory** and **flash usage**,
and core crash events.

HW&SW Agnostic with AI

Runs in **any mcu/mpu** or
for **Free RTOS**, **Emb. Linux/Android**, **Bare Metal**

Implementation lasts
only a few days

Embedded AI-driven learning models
recognize protocol behaviour
enabling **continuous lifecycle monitoring**

What can be done for the Sustainability of Mobile Application?

OWASP Mobile Top10

A mobile application must be at least compatible to **OWASP Mobile Top 10** Cyber Security feature lists

Periodic Penetration Tests

Mobile application and its related APIs must be analysed **periodically**

Secure By Design

Any new feature added into mobile application can create **new attack surfaces**. In such case, it should be analysed **by security experts from scratch**

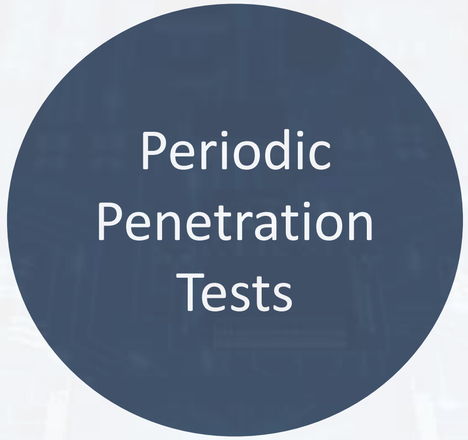
How CyberWhiz Mobile Can Help..

CyberWhiz Mobile Application

Cyber Security Libraries

%100 guarantee

OWASP Mobile Top 10 compatibility



CyberWhiz Red Team

will perform end to end

vulnerability analysis

at least once a year

CyberWhiz Blue Team

will perform

design consultancy

whenever a new feature is planned

CyberWhiz Mobile Feature Set


Root/Jailbroke Detection


Anti-Debugging


Remote Control


Remote File Deleting


Simulator/Emulator Detection


Unsecure Network Detection


VPN Implementation


Proxy Detection


Integrity Check


Obfuscate


SOC Implementation


MITM Detection

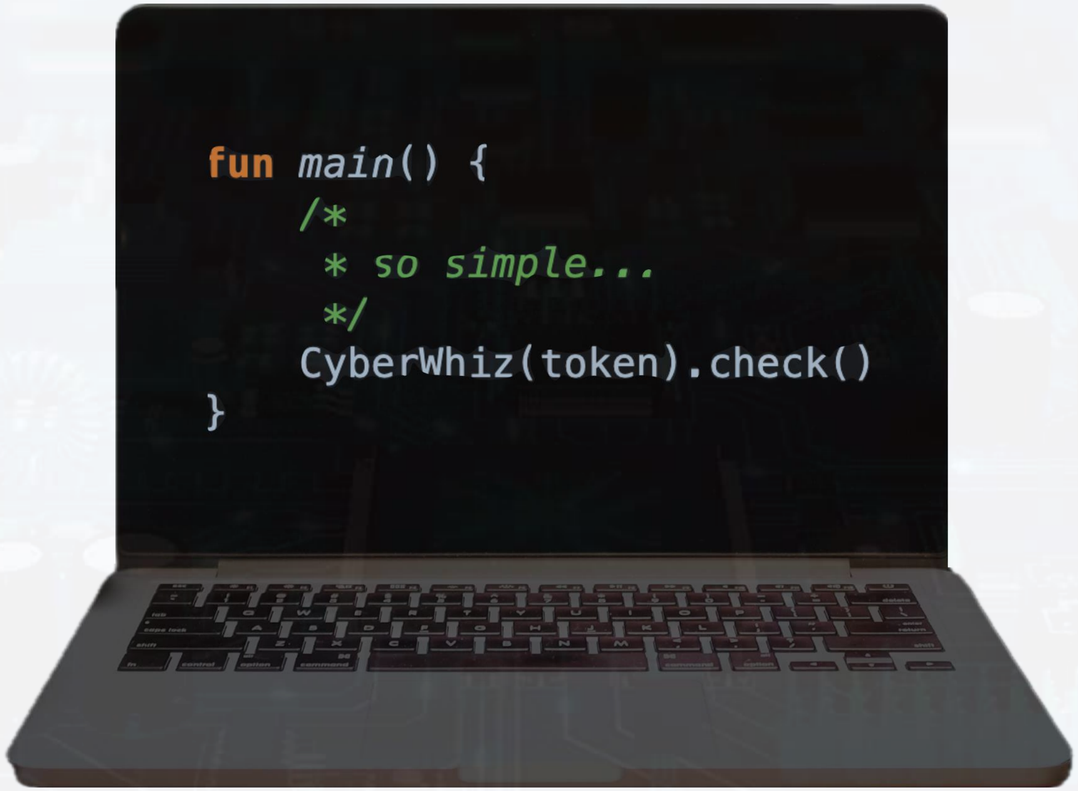

Hooking Detection


Easy To Implement


HITS Algorithm Implementation


And More...

One line of code..



CyberWhiz Mobile can be integrated into **any** mobile application

with just one line of code in less than 1 minute

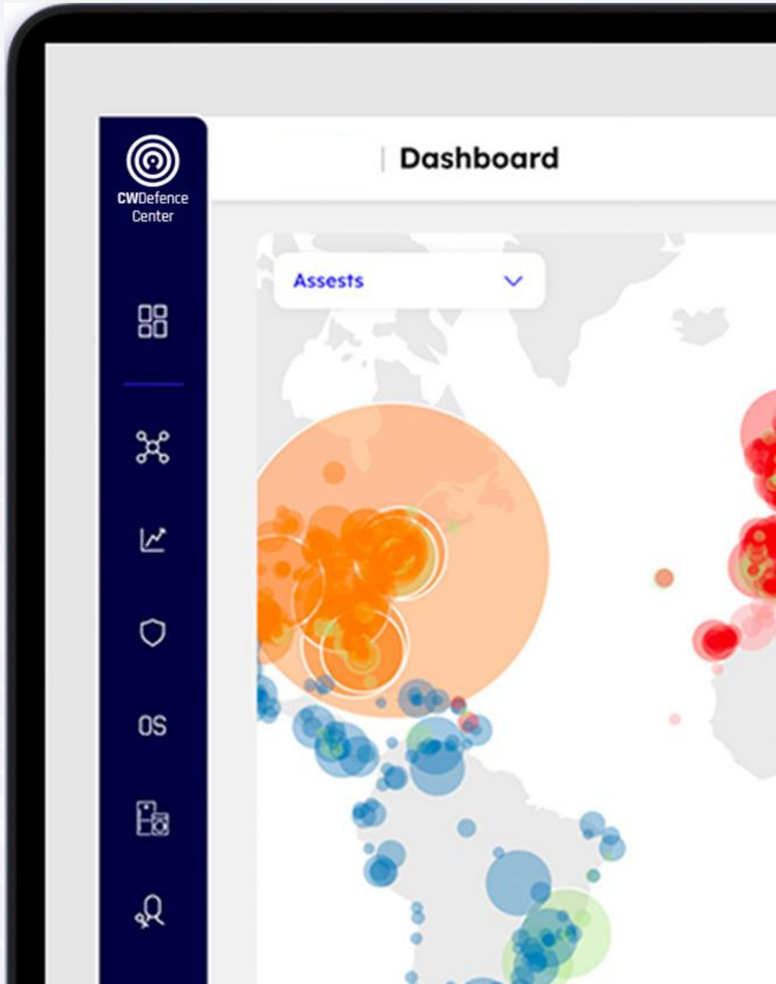
CyberWhiz Defence Center Continuous Incident Management

24/7 Monitoring

All **edge** and **mobile application logs** are monitored **continuously**

Incident Response Service

CyberWhiz Purple Team inform stakeholders in 24 hours in case of a cyber risk



SBOM Creation for Edge·Mobile·Cloud and Vulnerability Management

Automize

Automates SBOM-based **vulnerability tracking**

CVE mapping for known vulnerabilities

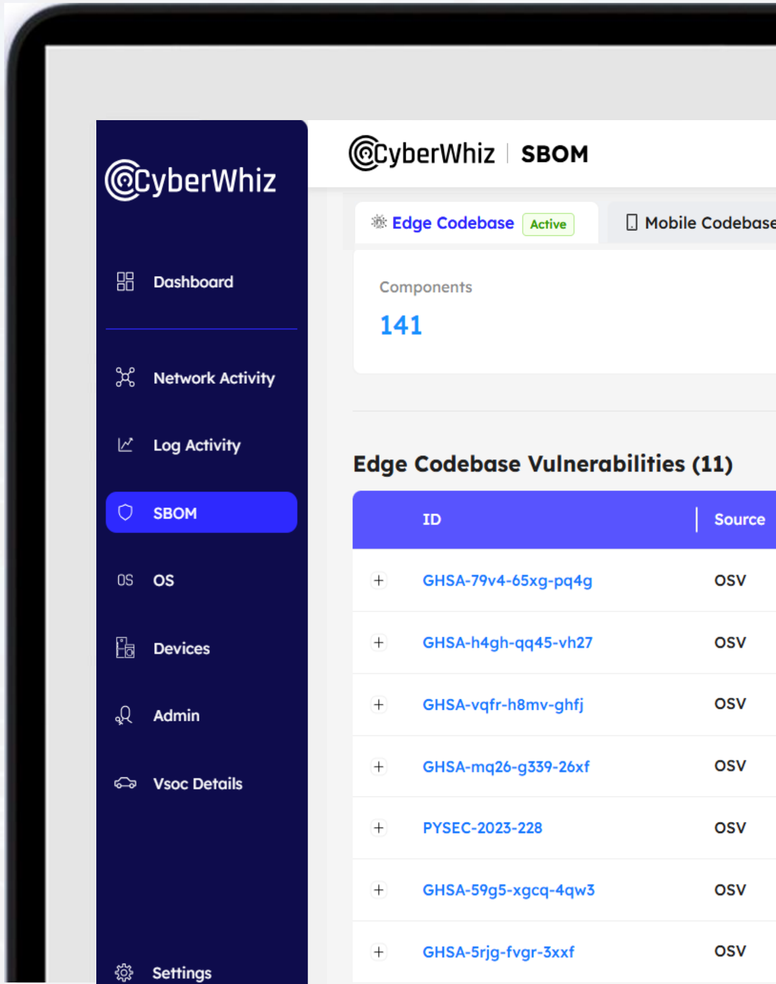
Reduces manual effort and human error

Continuous

Continuously monitors **new releases** and vulnerabilities

Supports project import **directly from repository**

Provides clear dashboards for **quick insights**



Red Team: End-to-End IoT Penetration Tests for Edge · Mobile · Cloud

Signal Tests

RF spectrum analysis using SDR tools
(HackRF, RTL-SDR, etc.)

Reverse engineering of proprietary **RF protocols**
(Bluetooth, Wi-Fi, LoraWan, ZigBee, GSM, UWB, etc.)

Interception and **decoding** of unencrypted data
(433 MHz, 868 MHz systems)

Testing of **replay**, **jamming**,
spoofing attacks

Frequency scanning,
modulation analysis

Wireless Network Tests

Security testing of 802.11 a/b/g/n/ac
Wi-Fi networks (WPA2/WPA3)

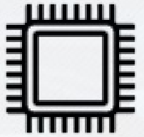
Attacks against **EAP protocols**,
captive portal bypass, **rogue AP** setups

Exploitation of known vulnerabilities
(KRACK and PMKID hash Collection)

Discovery of hidden SSIDs,
MAC spoofing, and client isolation bypass

Bluetooth/BLE scanning,
pairing process testing, **MITM attacks**

Embedded Systems



Hardware-level analysis
(UART, JTAG, SPI, NAND flash access)

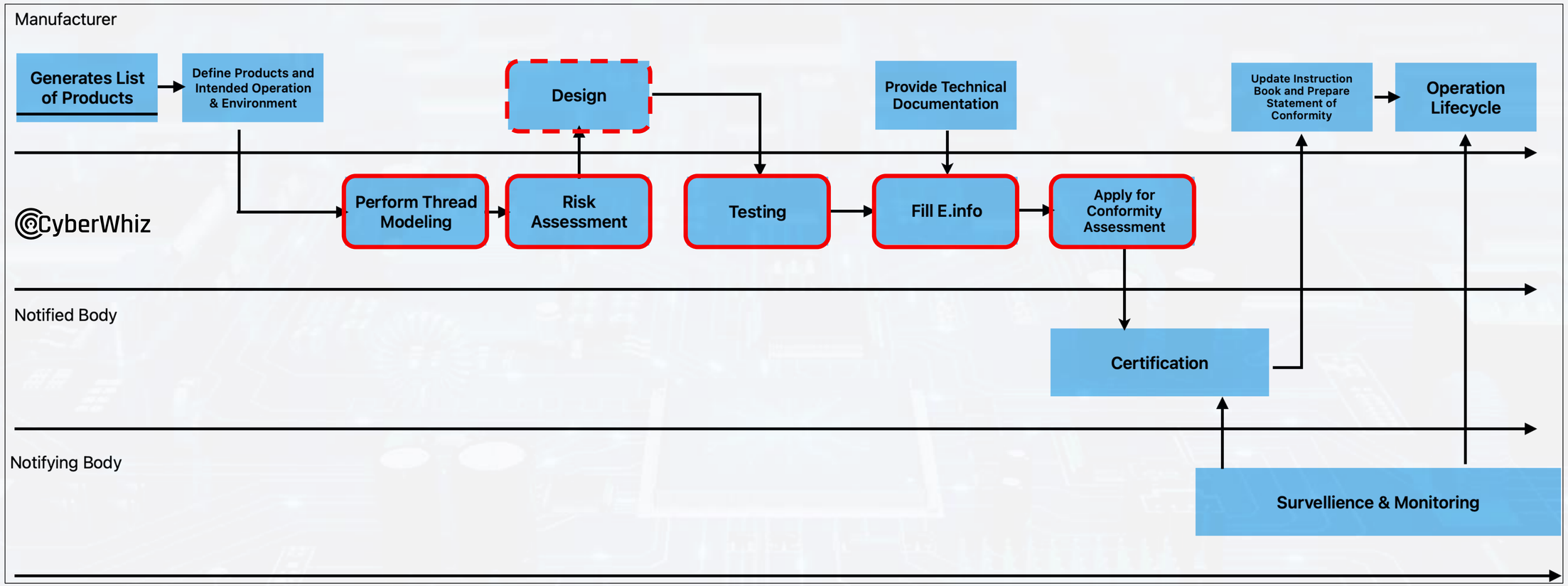
Software Access, Firmware analysis,
credential extraction, binary hardening review

Device misconfiguration,
default credentials detection

Security evaluation of OTA
(Over-the-Air update mechanisms)

API, mobile app and cloud communication
End-to-end security validation

Purple Team: Regulation Consultancy for IoT Cyber Security Regulations



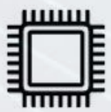
- Performing risk assessments aligned with **RED DA** and/or **CRA** requirements and tailored to IoT specific threats.
- Analysing your device architecture, firmware, and connectivity models to identify regulatory security gaps.
- Preparing **E.Info** and Declaration of Conformity (DoC) documents to meet CRA submission standards.
- Working closely with your technical teams to ensure all documentation is accurate, complete, and audit-ready.

CyberWhiz

IoT Cyber Security Excellence

for

Edge · Mobile · Cloud



info@cyberwhiz.co.uk