# 從物聯網安全看基礎建設安全

是德科技 王欽洲
Joe.wang@keysight.com

# IoT Security for Critical Infrastructures

**Agenda**

- Governments and Critical Infrastructures
- Security Incidents and Cost of Breach
- IoT devices for Infrastructures
- Vulnerability, Exploit, and Attack
- Keysight can Help

## Across the World

**UK: additional £2.6B in cyber and legacy IT**

**Singapore:  additional $1B to uplift cyber security**

**Australia: additional $10B toward cyber security**

26.2B

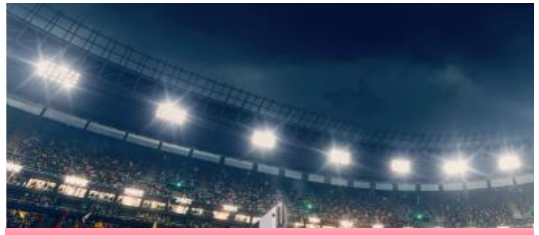
**US: >~~$22B~~ for federal cyber security budget**

**~~$175M for privately owned infrastructure~~**

**$245M for the cybersecurity and resilience of the energy sector**

# Critical Infrastructure Sectors

Chemical



Commercial Facilities

Communication

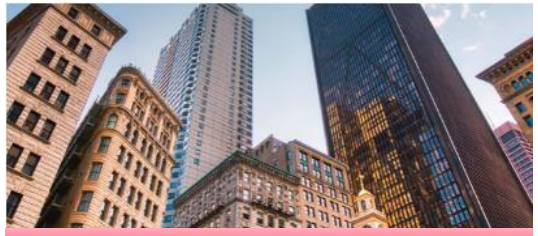
Critical Manufacturing

Dams

Defense Industry

Emergency Services

Energy



Financial Services

Food and Agriculture

Government Facilities

Healthcare/Public Health

Information Technology

Nuclear Reactor/Materials

Transportation System

Water and astewater

# Many recent security incidents in critical infrastructure

## JBS: Cyber-attack hits world's largest meat supplier

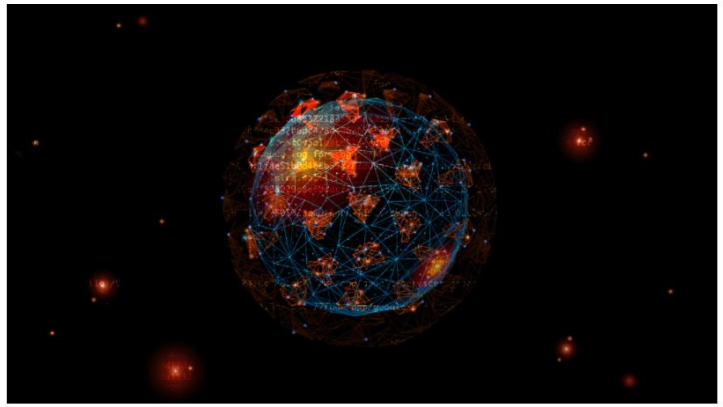
2 June


## European Medicines Agency cyber-attack: Coronavirus vaccine documents 'unlawfully accessed', claim Pfizer and BioNTech

Adam Bannister 10 December 2020 at 12:26 UTC

Healthcare | Coronavirus | Cyber-attacks

*EU healthcare body assures pharma giants that attack 'will have no impact' on vaccine authorization timeline*




Cybersecurity

## Hackers Breached Colonial Pipeline

## How a ransomware attack cost one firm £45m

By Joe Tidy
BBC Cyber-security reporter

25 June 2019


## Some operations at INA Group, Croatia's biggest oil company, and its largest petrol station chain were disrupted by a cyber attack.

A ransomware attack has disrupted operations at INA Group, Croatia's biggest oil company, and its largest petrol station chain.

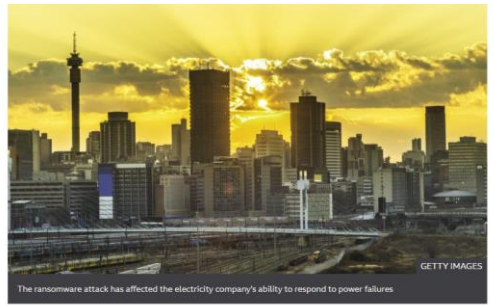
NEWS

Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health

Tech

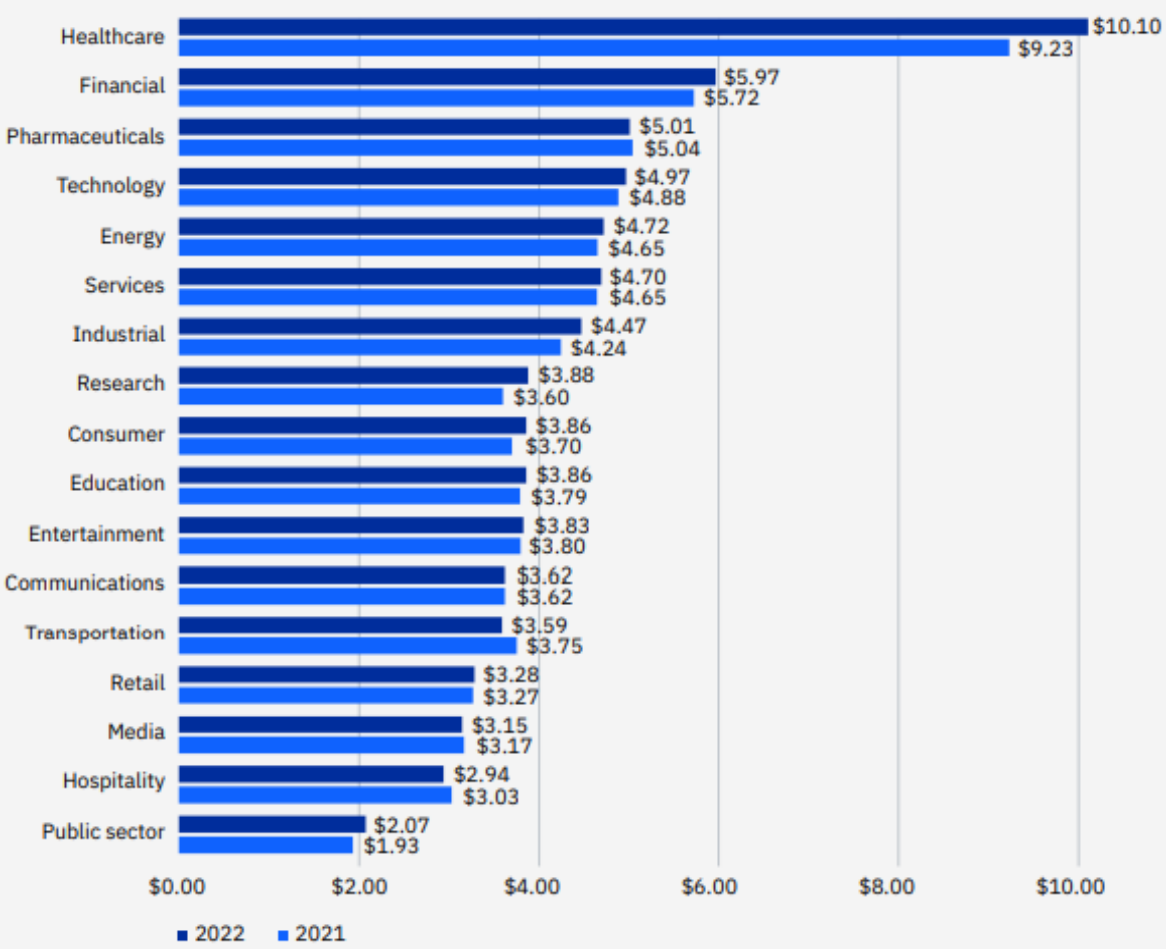
## Ransomware hits Johannesburg electricity supply

26 July 2019




KEYSI

# Avg. cost of breach by sector




KEYSIGHT

[1] Source: Cost of Data Breach Report, IBM and Ponemon Institute 2022

# Cost of a data breach report

**#1US**

Most expensive country
$9.44 million
average cost of
a breach

**$4.3m**

av. cost of a data-breach
across all (17) countries
and all (17) industries

**#1**

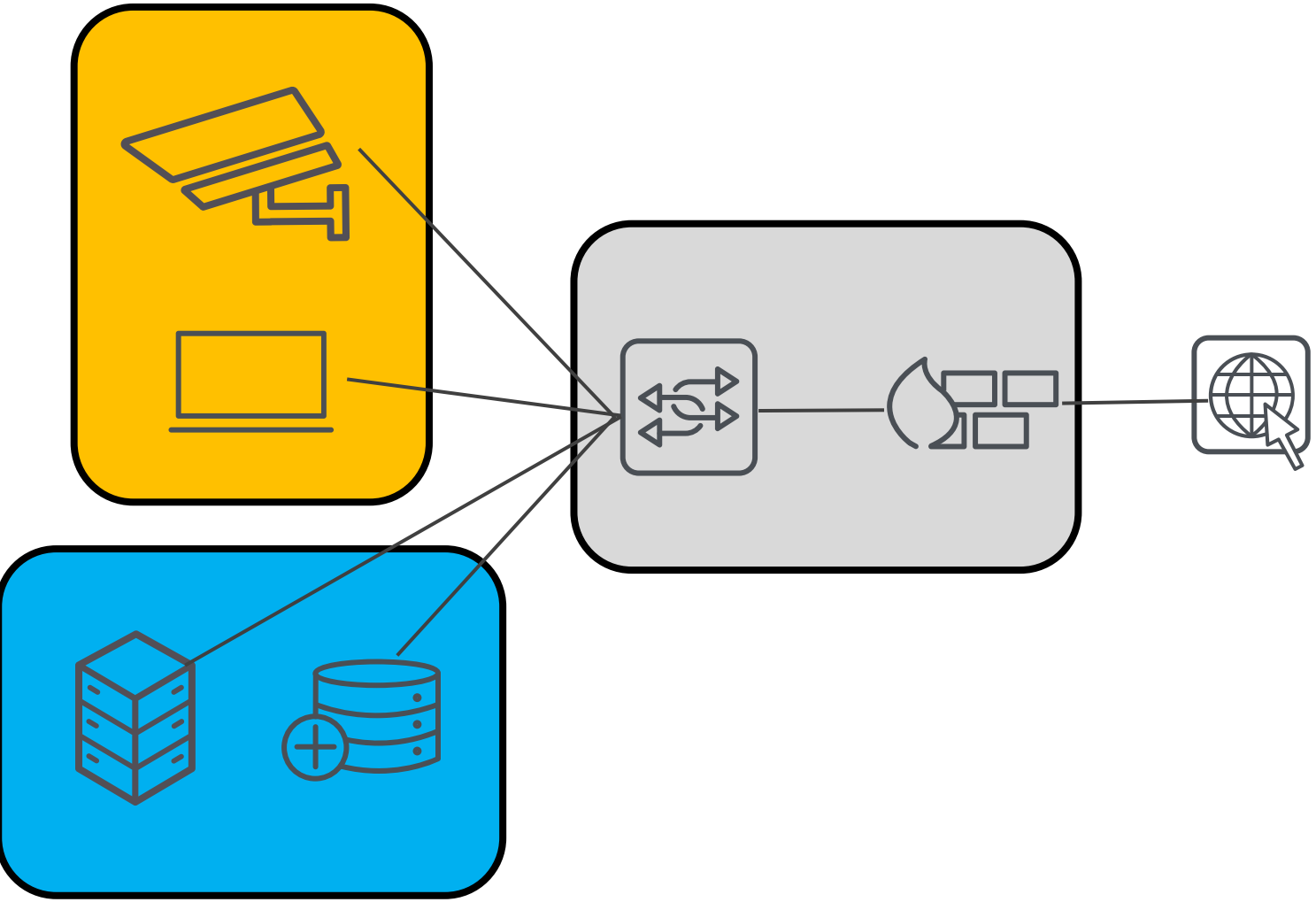
Healthcare was highest
cost industry with $10m+
av. cost of a breach

**277**

days, average time to
identify and contain
a data breach

# Security assessment guidelines for IoT-enabled field application

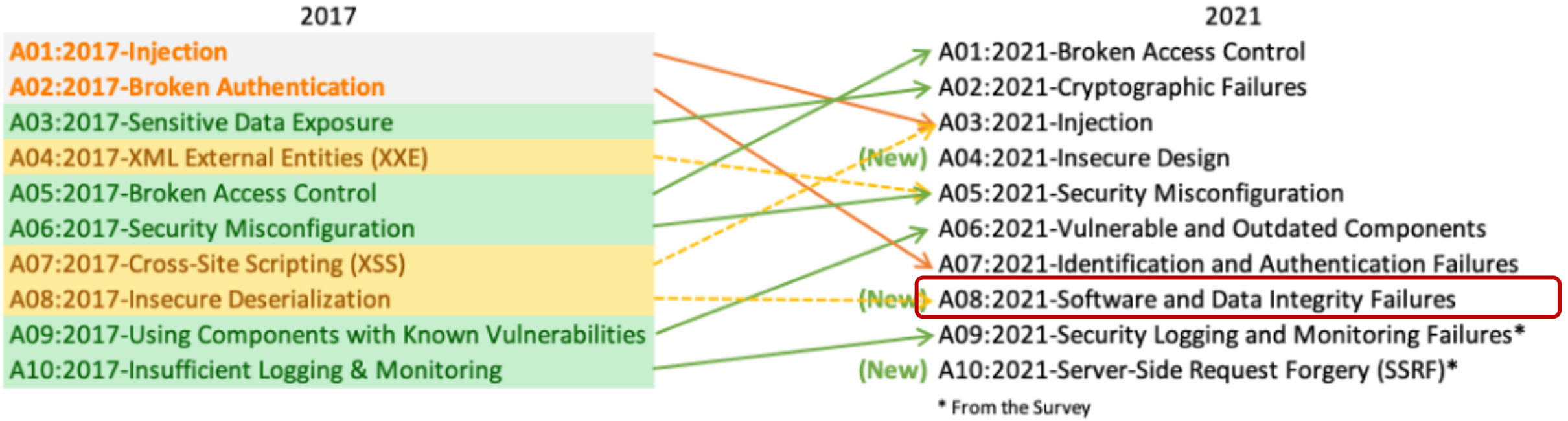
**STRIDE model**



- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

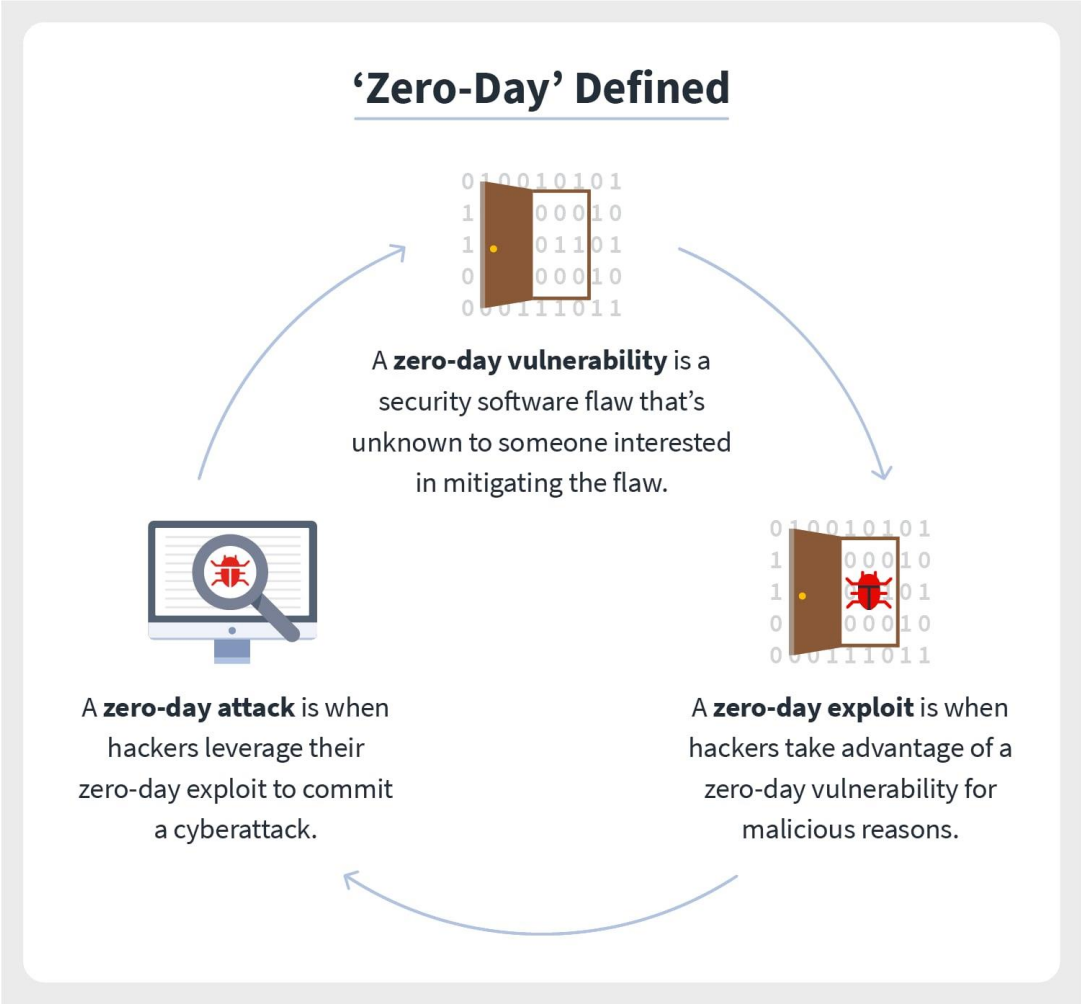
# Top Ten Web Security Risks (2017/2021)

- Globally recognized by developers as the first step towards more secure coding



# Zero-Day Vulnerability, Exploit and Attack

## Most Severe Security Threat




Fuzzing is the most effective mining tool for discover Zero-Day vulnerabilities

# Vulnerabilities detected using fuzzing

**Found vulnerabilities using fuzzing**

## 1. Exposure of Sensitive Information in Microsoft Windows

Reference: CVE-2015-0061

Risk: Medium

Fuzzing tool: American Fuzzy Loop (AFL)

The vulnerability was reported by Michal Zalewski, director of Inform Engineering at Google. Several Windows Servers

## 2. Out-Of-Bounds Read in Intrusion Detection System Suricata

Reference: CVE-2019-16411

Risk: Medium / High

Fuzzing tool: CI Fuzz

## 3. Exposure to Sensitive Information in OpenSSL

Reference: CVE-2017-3732

Risk: Medium

Fuzzing tool: OSS-Fuzz / libFuzzer

This issue was reported to OpenSSL by the Google OSS-Fuzz team. Carry propagation bugs mean that the developer failed to add every possible carry bit during a large integer addition or multiplication, which turns into an incorrect result. This vulnerability only appears in rare edge cases and therefore remains mostly unnoticed for a long time. A successful attack relying on this propagation bug can allow an attacker to recover encryption keys.

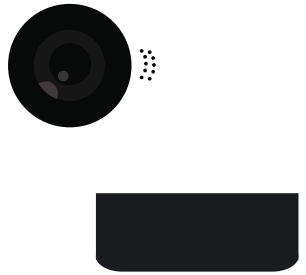
# What if you have below connected devices in your critical infrastructure

**You have some security holes**

**ICSA-22-172-03**
Could allow an attacker to **execute malicious code** on the device.

**ICSA-20-063-01**
Could grant **access control to a thief** by means of remote execution.

**CVE-2021-39238**
Enables **remote code execution**, can **spread** across network.

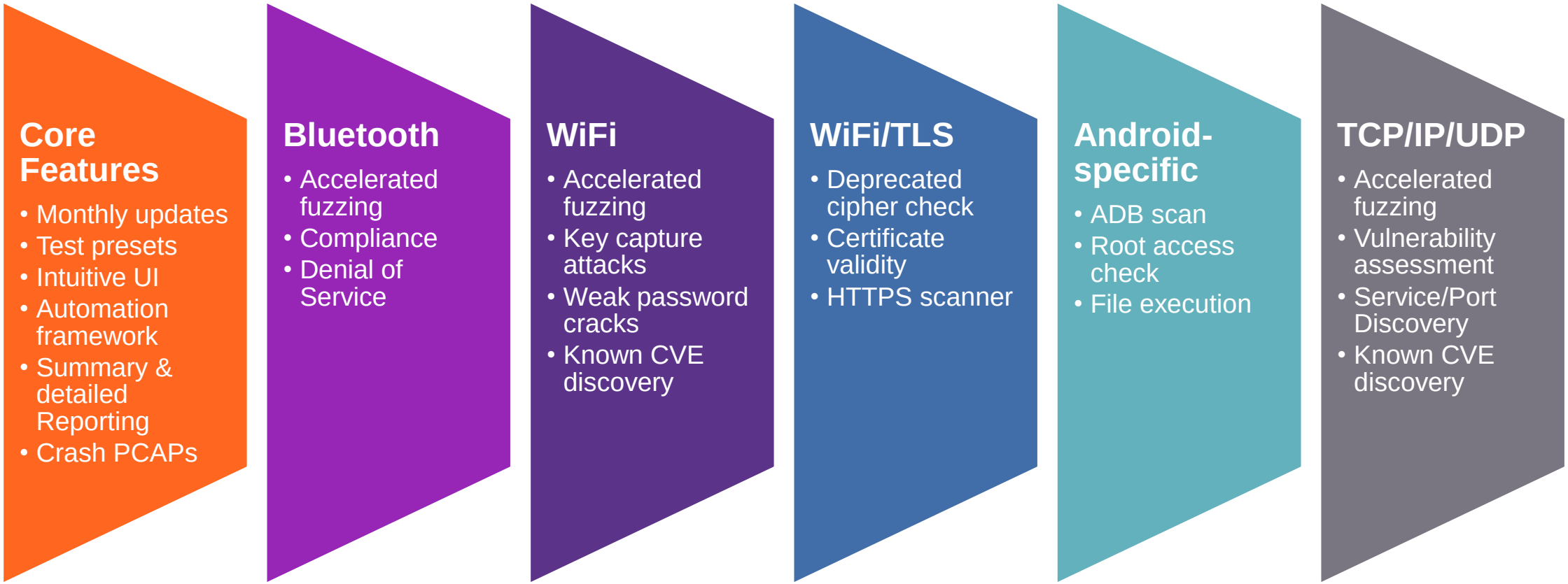


**CVE-2021-28372**
Allows hackers to **watch and listen** to live feeds.


**CVE-2021-33883**
Allows **altered doses of medication** to be delivered to patients without any checks.

# Keysight Security Testing Capabilities

## Protocol and Application Layer



# Keysight IoT Security Testing is proven.

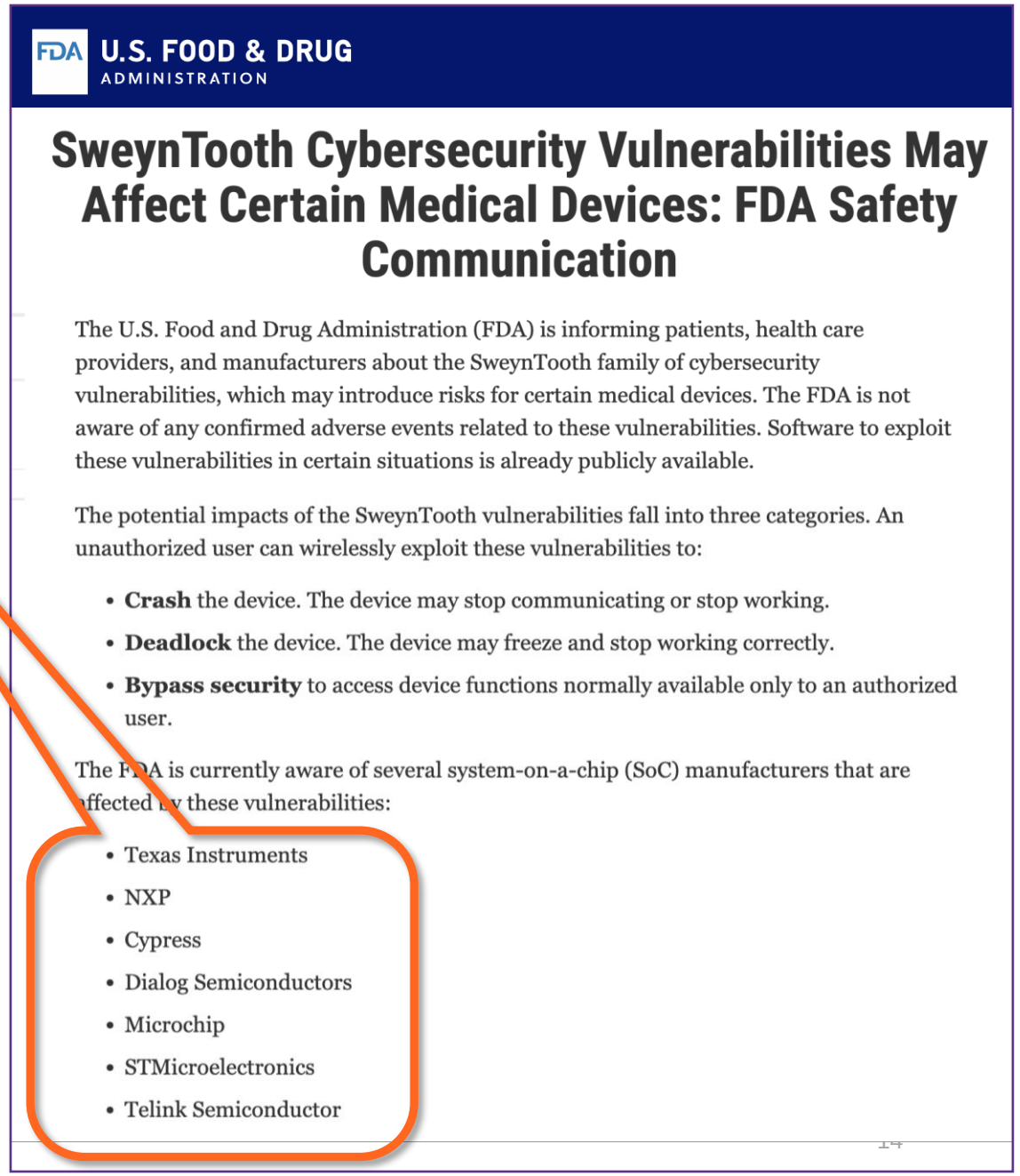
- Covers 9/10 of **OWASP IOT Top 10** (all but physical security)
- Used in discovery & validation of significant vulnerability classes:
  - **Sweyntooth** – causes crash/reboots in healthcare, industrial, and consumer devices
  - **Braktooth** – impacts over 1 billion deployed IOT devices
- Finds both **known** (vulnerability scanning) and **unknown** (protocol fuzzing) **security flaws**

| Used to find/validate 40+ CVEs such as: | |
|---|---|
| CVE-2021-28139 | CVE-2019-12586 |
| CVE-2021-34144 | CVE-2019-12587 |
| CVE-2021-28136 | CVE-2019-12588 |
| CVE-2021-28135 | CVE-2019-16336 |
| CVE-2021-28155 | CVE-2019-17519 |
| CVE-2021-31609 | CVE-2019-17517 |
| CVE-2021-31612 | CVE-2019-17518 |
| CVE-2021-34150 | CVE-2019-17520 |
| CVE-2021-31613 | CVE-2019-19195 |
| CVE-2021-31611 | CVE-2019-19196 |
| CVE-2021-31785 | CVE-2019-17061 |
| CVE-2021-31786 | CVE-2019-17060 |
| CVE-2021-31610 | CVE-2019-19192 |
| CVE-2021-34149 | CVE-2019-19193 |
| CVE-2021-34146 | CVE-2019-19194 |

# Supply Chain Impacts Device Security

**Critical Flaws Found in Medical Devices**

- Most manufacturers use off-the-shelf communication chipsets from **established vendors**
- Those chipsets **may not be fully tested** or have latest firmware
- When critical vulnerabilities are discovered, device **manufacturers must scramble** to address flaws and rush updates
- Brand damage, **expensive recalls**, compliance risk
- Result of **inadequate full-stack testing**



FDA U.S. FOOD & DRUG ADMINISTRATION

## SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. Software to exploit these vulnerabilities in certain situations is already publicly available.

The potential impacts of the SweynTooth vulnerabilities fall into three categories. An unauthorized user can wirelessly exploit these vulnerabilities to:

- **Crash** the device. The device may stop communicating or stop working.
- **Deadlock** the device. The device may freeze and stop working correctly.
- **Bypass security** to access device functions normally available only to an authorized user.

The FDA is currently aware of several system-on-a-chip (SoC) manufacturers that are affected by these vulnerabilities:

- Texas Instruments
- NXP
- Cypress
- Dialog Semiconductors
- Microchip
- STMicroelectronics
- Telink Semiconductor


U.S. CYBER TRUST MARK
U.S. CYBER TRUST MARK
PROGRAM


KEYSIGHT
START