HOW TO PREPARE FOR

THE EU's *CYBER RESILIENCE ACT*

JAN 2023

CYBERCRIME: THIRD LARGEST ECONOMY BY 2025

$10.5 Trillion

1. US Annual GDP $21.5 trillion
2. China Annual GDP $17.7 trillion
3. **Global Cybercrime $10.5 Trillion**
4. Japan Annual GDP $4.97 Trillion

WHAT IS THE NEW EU CYBER RESILIENCE ACT?

Rules to hold manufacturers responsible for product cybersecurity and updates that resolve vulnerabilities.

1. The first “Internet of Things” regulation in the world
2. Common cybersecurity rules for products in the EU
3. Applies to all “networkable” end products
4. Targets both hardware and software products

WHY IS IT BEING PUBLISHED NOW?

Billions of everyday objects getting Internet connected. EU estimates global annual cybercrime cost €5.5 Trillion

1. Attacks are growing in number & complexity
2. Society and Economies depend on digital tools and services
3. EU goal is technical and strategic sovereignty
4. Ensure consistent security across digital supply chains
5. Exploits can impact entire services, networks & economies

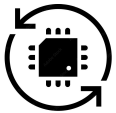
ATTACKS GROWING IN NUMBER & COMPLEXITY

1. **Colonial Pipeline**
   Halted all pipeline operations for several hours and paid $4.4M to Darkside group
2. **Solar Winds**
   Supply chain attack impacted hundreds of companies and government agencies.
3. **DoppelPaymer**
   Cyber-attack on hospital in Germany contributed patient death.
4. **Many more attacks are in the works**

ENISA Report Threat Landscape 2022

OBLIGATIONS OF MARKET PLAYERS

Assure Cybersecurity
During product design, development & manufacturing.



Lifetime Product Support
Provide security updates over stated product lifetime.

Cybersecurity Information
Report vulnerabilities and information over stated lifetime.

Conformity Assessment
Perform assessment before Applying CE mark to product.

Inform Distributors
Non-conforming products and product recalls.

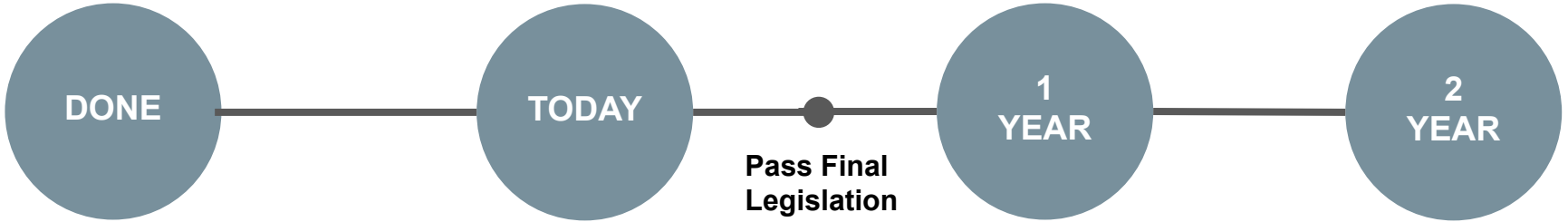
National Authorities
Provide proof of conformance upon request.

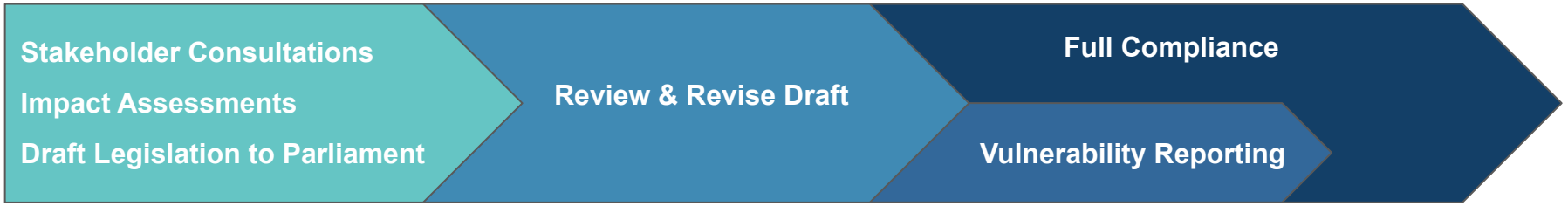
WHAT HAPPENS TO NON-COMPLIANT PRODUCTS?

Face fees up to €15 M, or 2.5% of worldwide revenue (whichever higher)

1. Prohibit or restrict product availability on the market
2. Require that product be brought into compliance
3. Face an order to withdraw or recall product
4. Mounting fines for additional breaches

REGULATORY TIMELINES





EU DECLARATION OF CONFORMITY

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 20, shall contain all of the following information:

1. Name and type and any additional information enabling the unique identification of the product with digital elements;
2. Name and address of the manufacturer or his authorised representative;
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;
4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);
5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;
6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;
8. Additional information:

Signed for and on behalf of: ……

(place and date of issue):

(name, function) (signature):

CONSIDERATIONS FOR TRUSTED FIRMWARE

VULNERABILITY REPORTING PROCESS

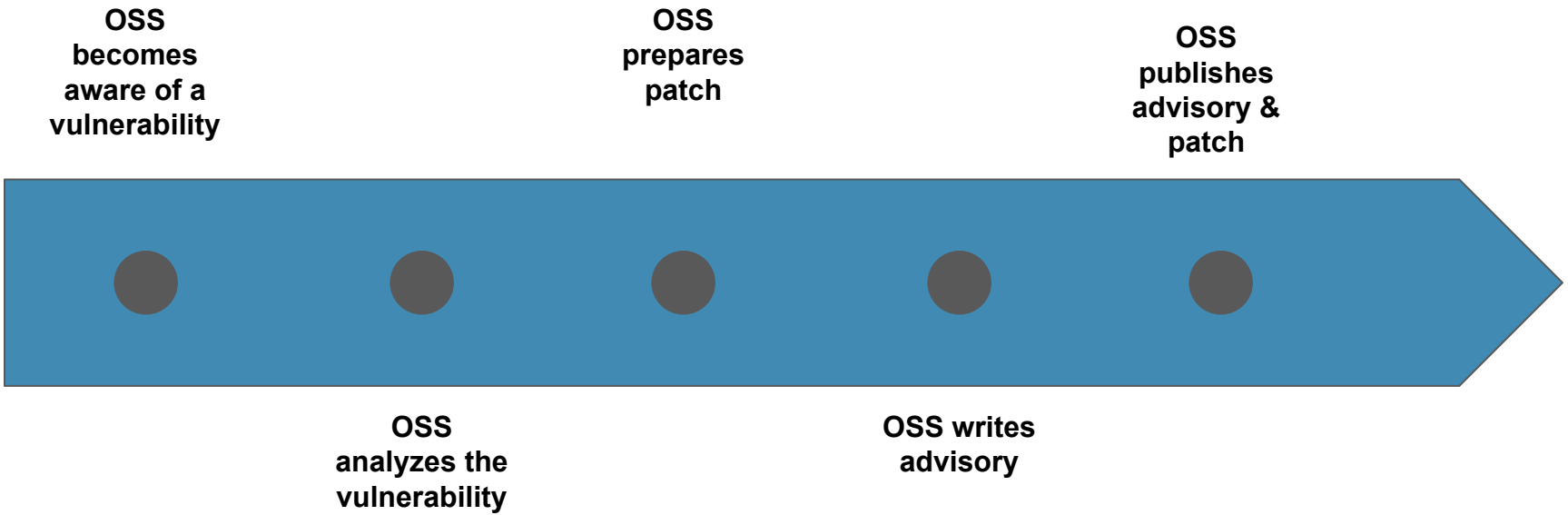
“In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of material.”

“Manufacturers […] should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities […] to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public”

“ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products. Manufacturers should also consider disclosing fixed vulnerabilities to the EU vulnerability database […] managed by ENISA or under any other publicly accessible vulnerability database.”

ENISA = European Union Agency for Cyber Security

SECURITY VULNERABILITY REPORTING PROCESS



NXM

VULNERABILITY REPORTING TODAY

Currently a very manual process

GHSA Repo: https://github.com/github/advisory-database

Github Security Advisory(GHSA): https://github.com/advisories

Component advisory for NanoPb:
https://github.com/nanopb/nanopb/security/advisories

Component advisory for MbedTLS
https://github.com/Mbed-TLS/mbedtls/security/advisories

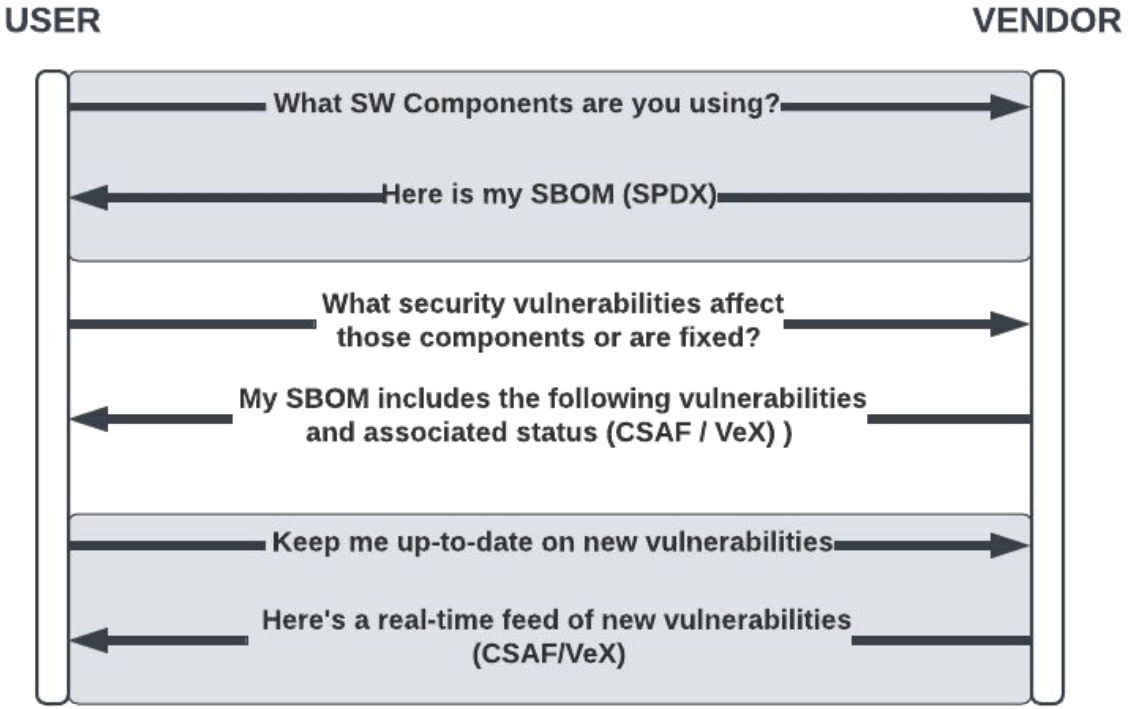
VULNERABILITY REPORTING => TOWARDS AUTOMATION

Standard	Description
Software Identification Tag (SWID)	Transparent way for organizations to track the software installed on their devices
Software Package Data Exchange (SPDX) or CycloneDX	Software Bill of Material standards
Common Security Advisory Framework (CSAF)	Machine-readable format for security advisories (JSON)
Resource-Oriented Lightweight Information Exchange (ROLIE)	Content syndication protocol to discover, syndicate & exchange security advisories
Vulnerability Exploitability eXchange (VEX)	Vendor attestation as to whether their software is vulnerable to an exploit

Further information: https://www.youtube.com/watch?v=z6Psfopy55E

NXM

VULNERABILITY REPORTING: AUTOMATION FLOW



Source: https://www.youtube.com/watch?v=z6Psfopy55E

QUESTIONS