Fraunhofer SIT

Cyber Resilience Act

Changes and Challenges for Manufacturers

Crosscutting Regulation for Cybersecurity

Regulating Products with Digital Elements

Applies to all Products with Digital Elements

- Software
  - Software in a box
  - Apps
  - Software installed in products, e.g. firmware
- Hardware
  - Home and SoHo routers
  - Industrial production machines
- Remote processing solutions
  - Remote parts of products with digital elements

No exceptions for SME, tiny apps, etc!

Crosscutting Regulation for Cybersecurity

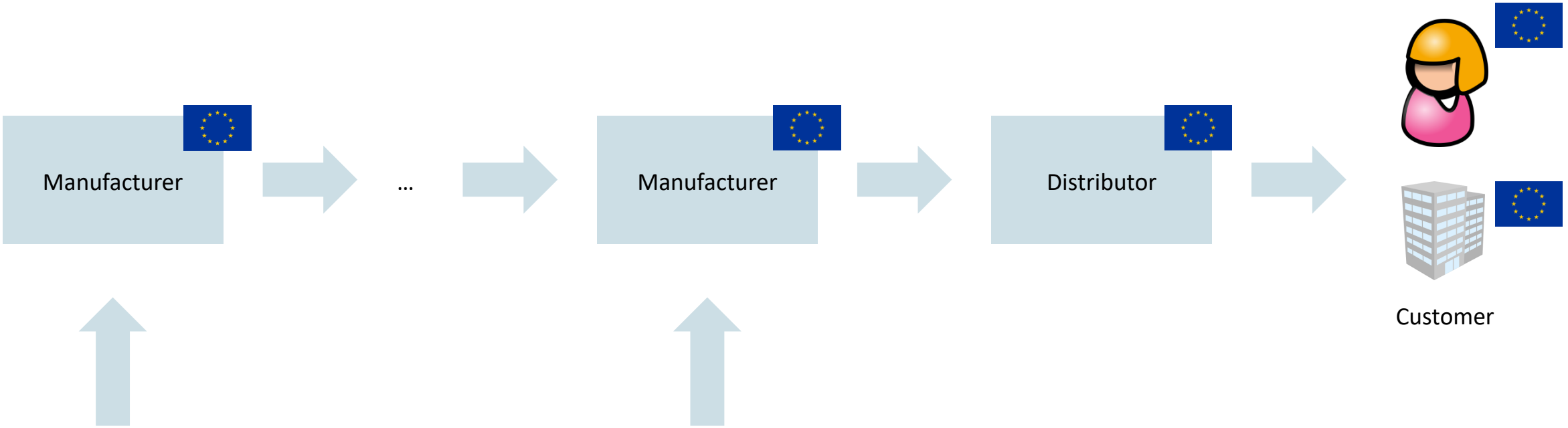
Regulating Products with Digital Elements

Exceptions

- Products under listed sector-specific regulations
  - Medical products
  - Civil aviation products
  - Car certification & road safety
  - National security and military products
  - …
- SaaS services not applicable
  - Pure cloud solutions without a product run by customer

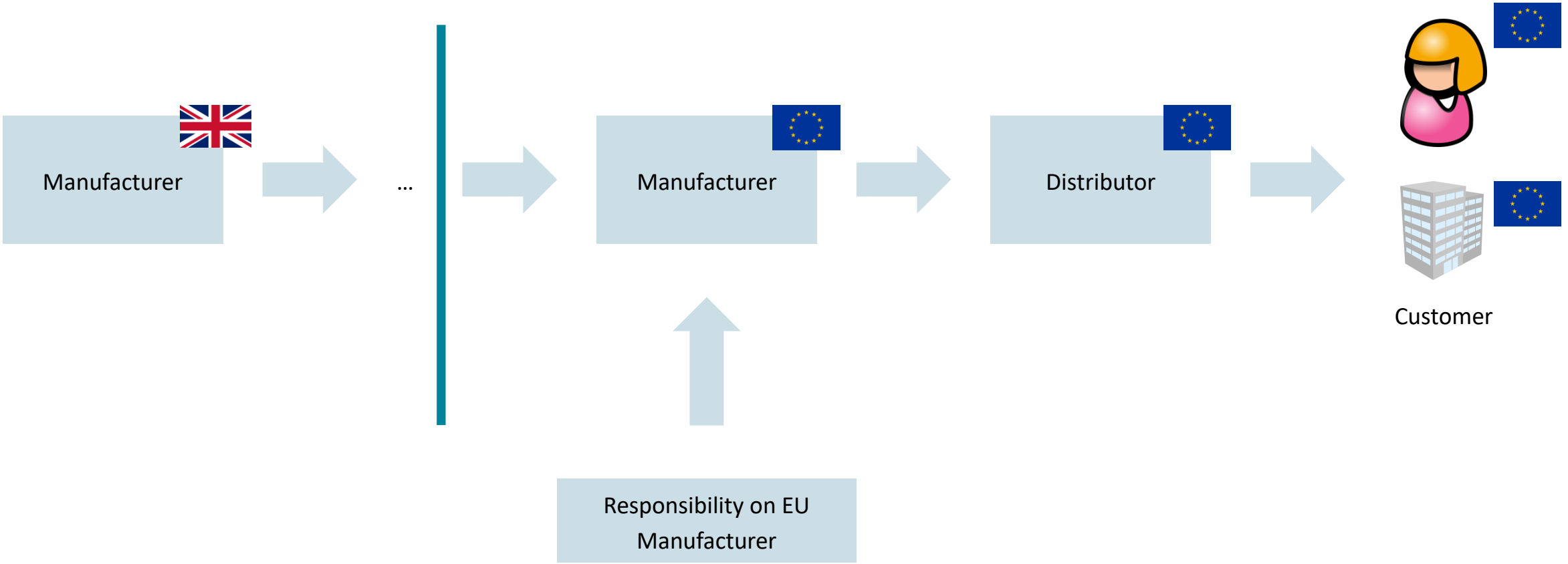
Composite and Imported Products

Who is Responsible?



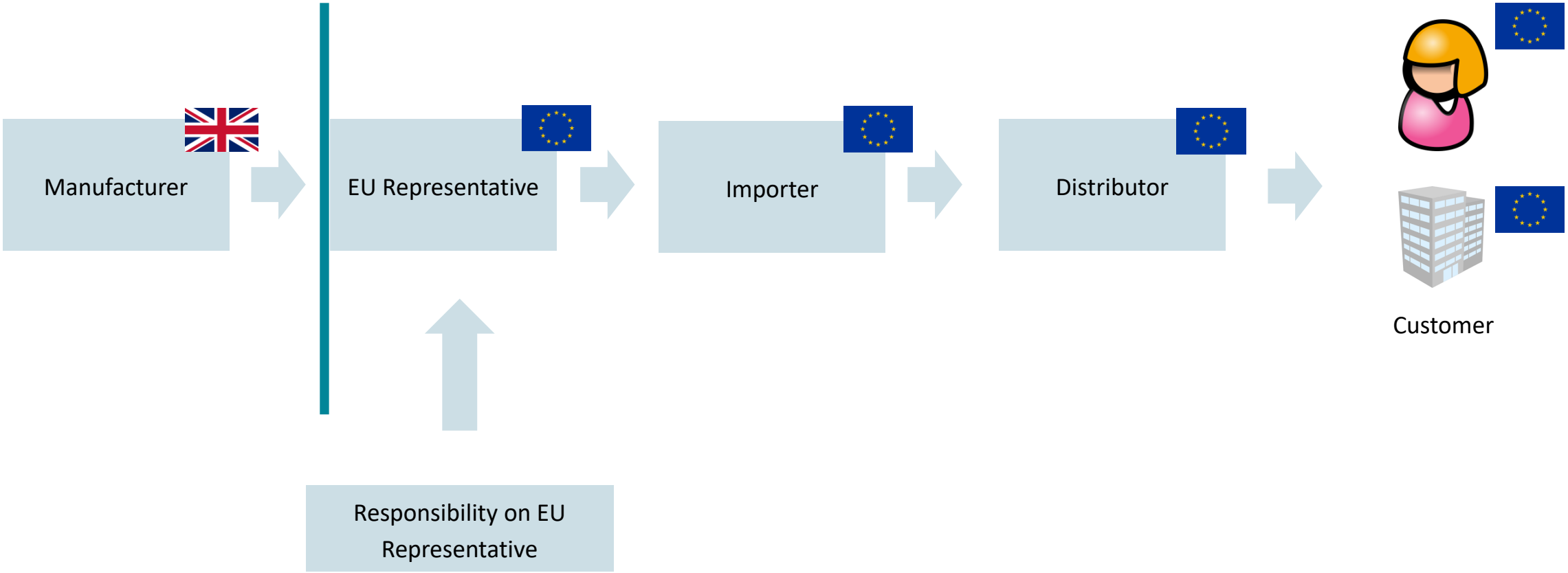
Composite and Imported Products

Who is Responsible?



Composite and Imported Products

Who is Responsible?



Core Pillars of the CRA

Security and Resilience Along the Product Lifecycle

Annex I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I ***Cybersecurity*** requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

Designed

Developed

Produced

Core Pillars of the CRA

Security and Resilience Along the Product Lifecycle

Designed

- Develop a risk model
- Design for essential cybersecurity requirements

Developed

- Develop without known vulnerabilities
- Implement with essential cybersecurity requirements in mind

Produced

- Secure default configurations
- Provision current version

(Operated)

- Allow for secure updates
- Handle incidents and vulnerability reports

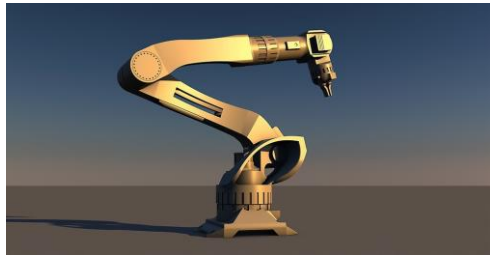
- Technical Documentation
- Conformity Assessment
- CE Marking

Spotlight: Risk Model

The Foundation for Designing and Implementing Measures

Smart TV

VS.



Industrial Production

User Authentication

- Physical access / short range remote control
- Internet services

Consequences of Unavailability

- Miss a football match

User Authentication

- Remote control
- Unauthorized staff in same machine shop?

Consequences of Unavailability

- Loss of production

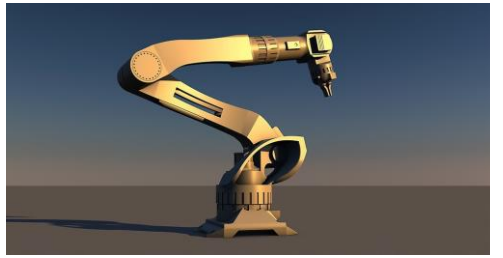
Spotlight: Risk Model

The Foundation for Designing and Implementing Measures

Smart TV

VS.

Standards may Apply



Industrial Production

Measures

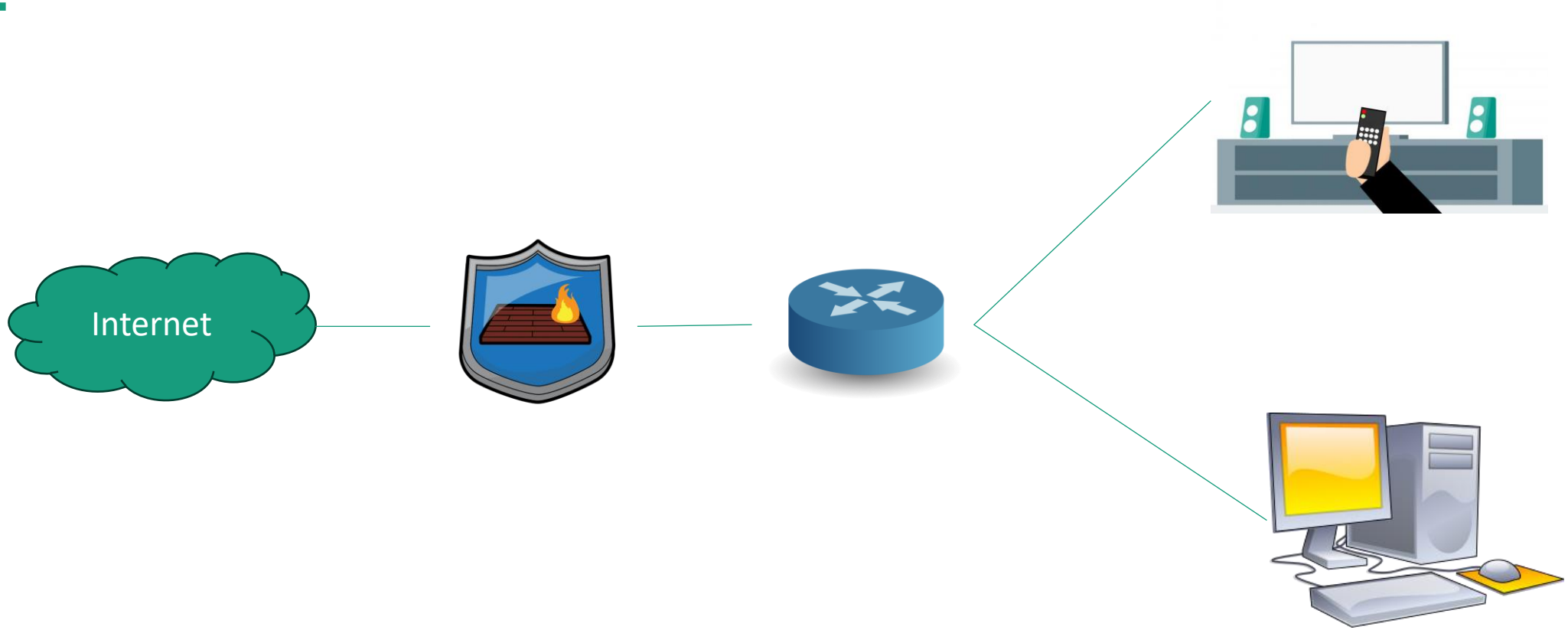
- No authentication for local users
- No access over the Internet

Measures

- Present badge (NFC) on site
- Username/password for remote access

Validate Against Intended Use

Make Clear What The Product is For

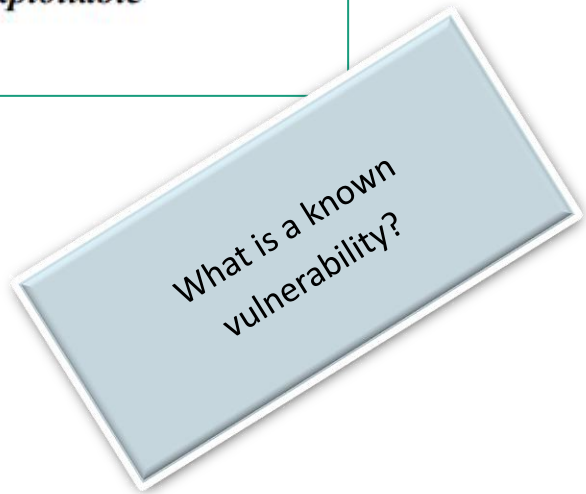


Spotlight: Without Known Vulnerabilities

Have Your Dependencies in Check

(2) On the basis of the ***cybersecurity*** risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;



Check Dependencies Against CVEs

Need to Know Your Dependencies

Large Dependency Trees

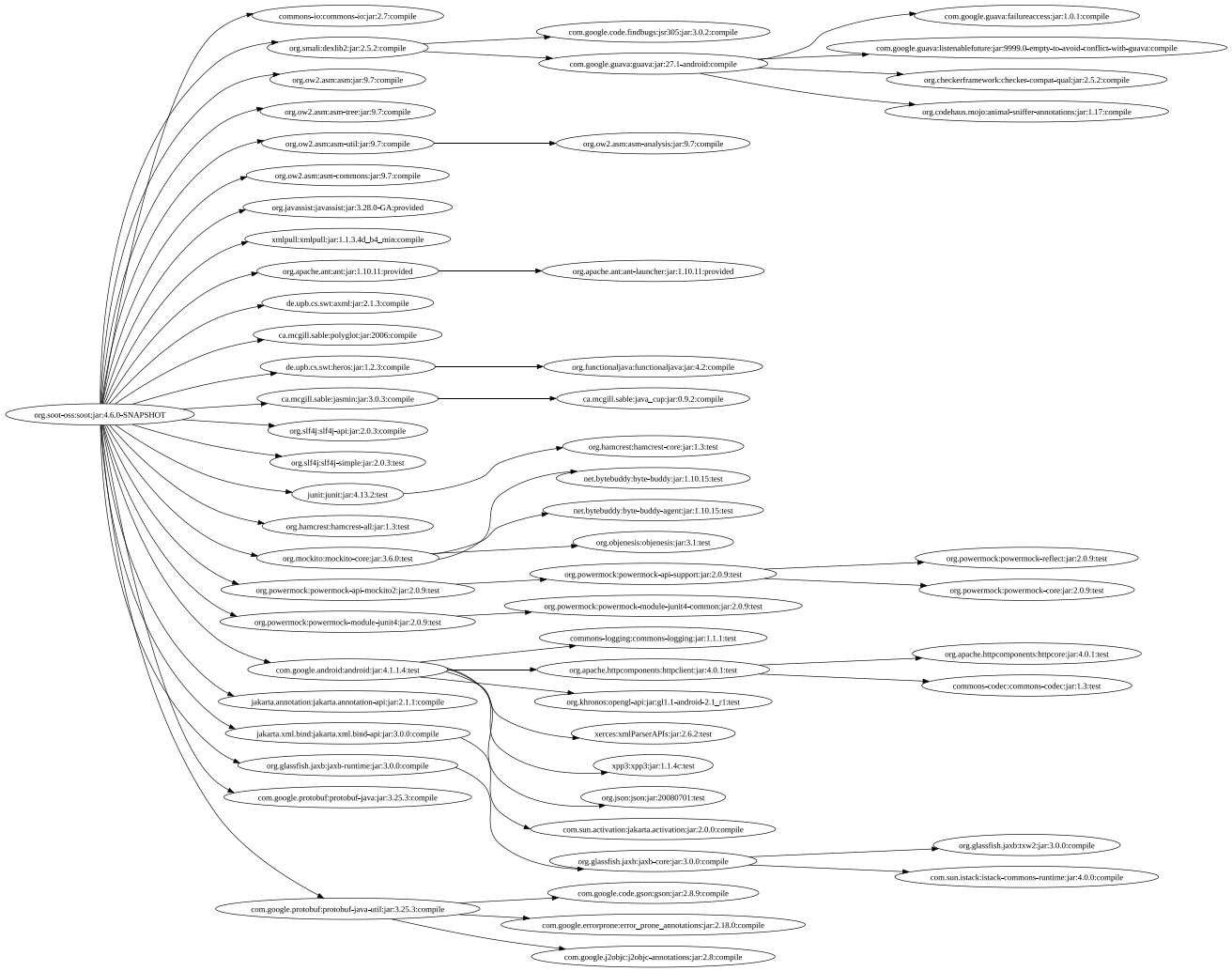
- Dependencies have other dependencies
- Even mid-size projects escalate quickly

Link to CRA

- Only first-level dependencies required in SBOM
- Each node may have vulnerabilities

Security Context

- Vulnerabilities
  - Known CVEs
  - End-of-life components
- Supply chain attacks: where to obtain software from?



SBOM as Part of Vulnerability Handling

Not Only a Catalog

Part II 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;

Automatically Generate SBOM

Integrate into Development Process

```
<dependencies>
    <!-- https://mvnrepository.com/artifact/commons-io/commons-io -->
    <dependency>
        <groupId>commons-io</groupId>
        <artifactId>commons-io</artifactId>
        <version>2.7</version>
    </dependency>
    <dependency>
        <groupId>org.smali</groupI
        <artifactId>dexlib2</artif
        <version>2.5.2</version>
    </dependency>
    <dependency>
        <groupId>org.ow2.asm</grou
        <artifactId>asm</artifactI
        <version>${asm.version}</v
    </dependency>
    <dependency>
        <groupId>org.ow2.asm</grou
        <artifactId>asm-tree</art
        <version>${asm.version}</v
    </dependency>
```

```
[INFO] --- maven-dependency-plugin:2.8:tree (d
[INFO] org.soot-oss:soot:jar:4.6.0-SNAPSHOT
[INFO] +- commons-io:commons-io:jar:2.7:compil
[INFO] +- org.smali:dexlib2:jar:2.5.2:compile
[INFO] |  +- com.google.code.findbugs:jsr305:j
[INFO] |  \- com.google.guava:guava:jar:27.1-a
[INFO] |     +- com.google.guava:failureaccess
[INFO] |     +- com.google.guava:listenablefuture:jar:9999.0-empty-to-avoid-conflict-with-guava:compile
[INFO] |     +- org.checkerframework:checker-compat-qual:jar:2.5.2:compile
[INFO] |     \- org.codehaus.mojo:animal-sniffer-annotations:jar:1.17:compile
[INFO] +- org.ow2.asm:asm:jar:9.7:compile
[INFO] +- org.ow2.asm:asm-tree:jar:9.7:compile
[INFO] +- org.ow2.asm:asm-util:jar:9.7:compile
[INFO] |  \- org.ow2.asm:asm-analysis:jar:9.7:compile
[INFO] +- org.ow2.asm:asm-commons:jar:9.7:compile
[INFO] +- org.javassist:javassist:jar:3.28.0-GA:provided
[INFO] +- xmlpull:xmlpull:jar:1.1.3.4d_b4_min:compile
[INFO] +- org.apache.ant:ant:jar:1.10.11:provided
[INFO] |  \- org.apache.ant:ant-launcher:jar:1.10.11:provided
[INFO] +- de.upb.cs.swt:axml:jar:2.1.3:compile
```

```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "library",
      "name": "acme-library",
      "version": "1.0.0"
    }
  ]
}
```

Essential Cybersecurity Requirements

Concrete Measures Depend on Risk Analysis

Annex I

ESSENTIAL CYBERSECURITY REQUIREMENTS

(2) On the basis of the ***cybersecurity*** risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(b) be ***made available on the market*** with a secure by default configuration**,** ***unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements***, including the possibility to reset the product to its original state;

Essential Cybersecurity Requirements

Areas of Required Measures

Secure Standard Configuration

- Ability to restore settings to default

Authentication

- Controls against unauthorized access

Confidentiality

- All data, not only personal data (as in GDPR)
- Protection of data in storage, transit or being processed

Integrity

- All data, not only personal data (as in GDPR)
- Includes programs, commands, configuration

Data Reduction

- All data, not only personal data (as in GDPR)
- Reduce the data being processed to what is necessary

Availability

- Preserve availability of essential features even under DoS attack

Reduce Negative Impact

- Reduce effect on other devices on the network
- Reduce exploitability

Reduce Attack Surface

Provide Logging

Allow Security Updates

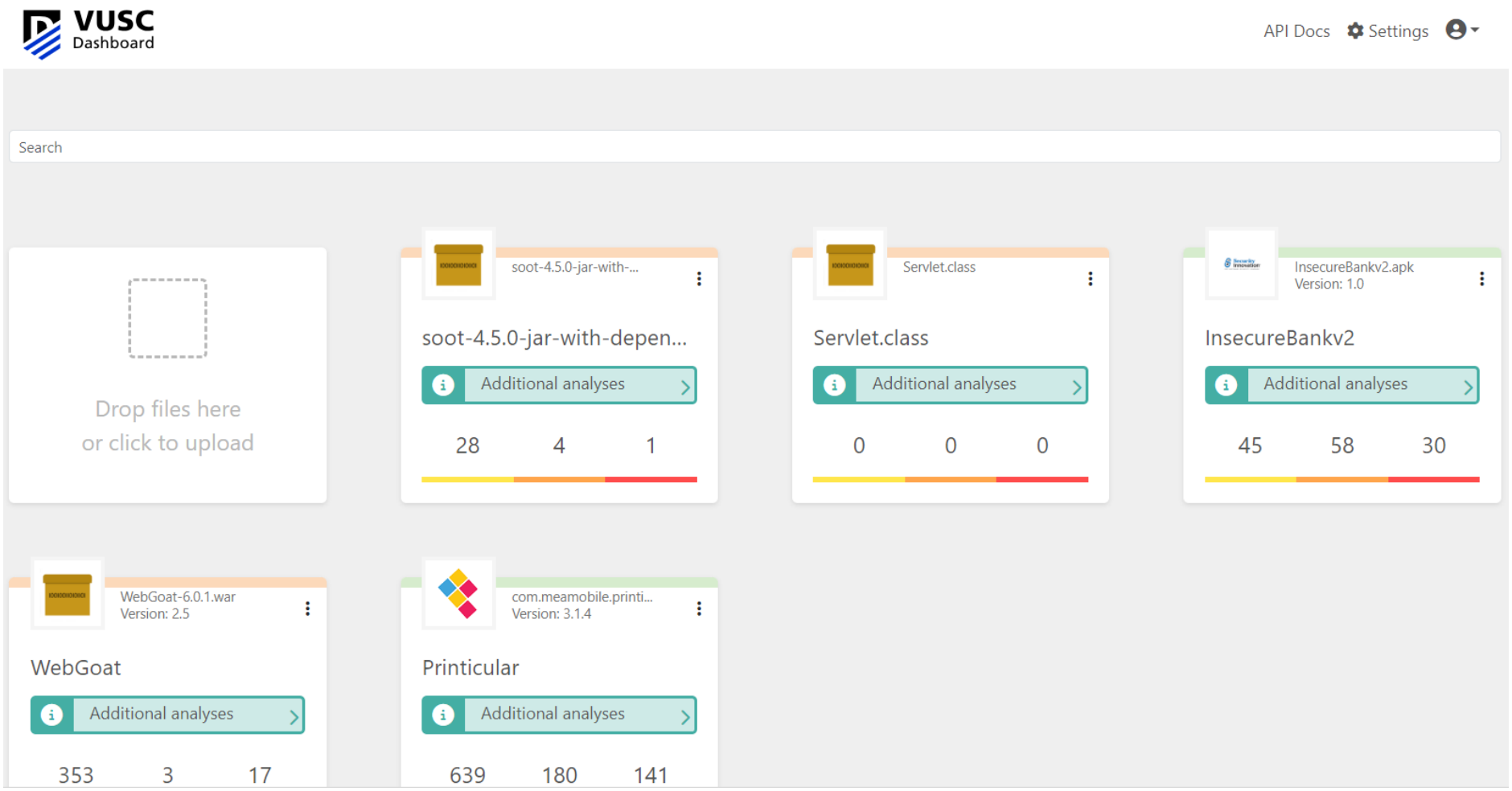
Checking The Own Code

Avoiding Vulnerabilities During Development

During Development	Peer Reviews	Coding Guidelines	Code Scanning
During Testing	Code Reviews	Penetration Testing	

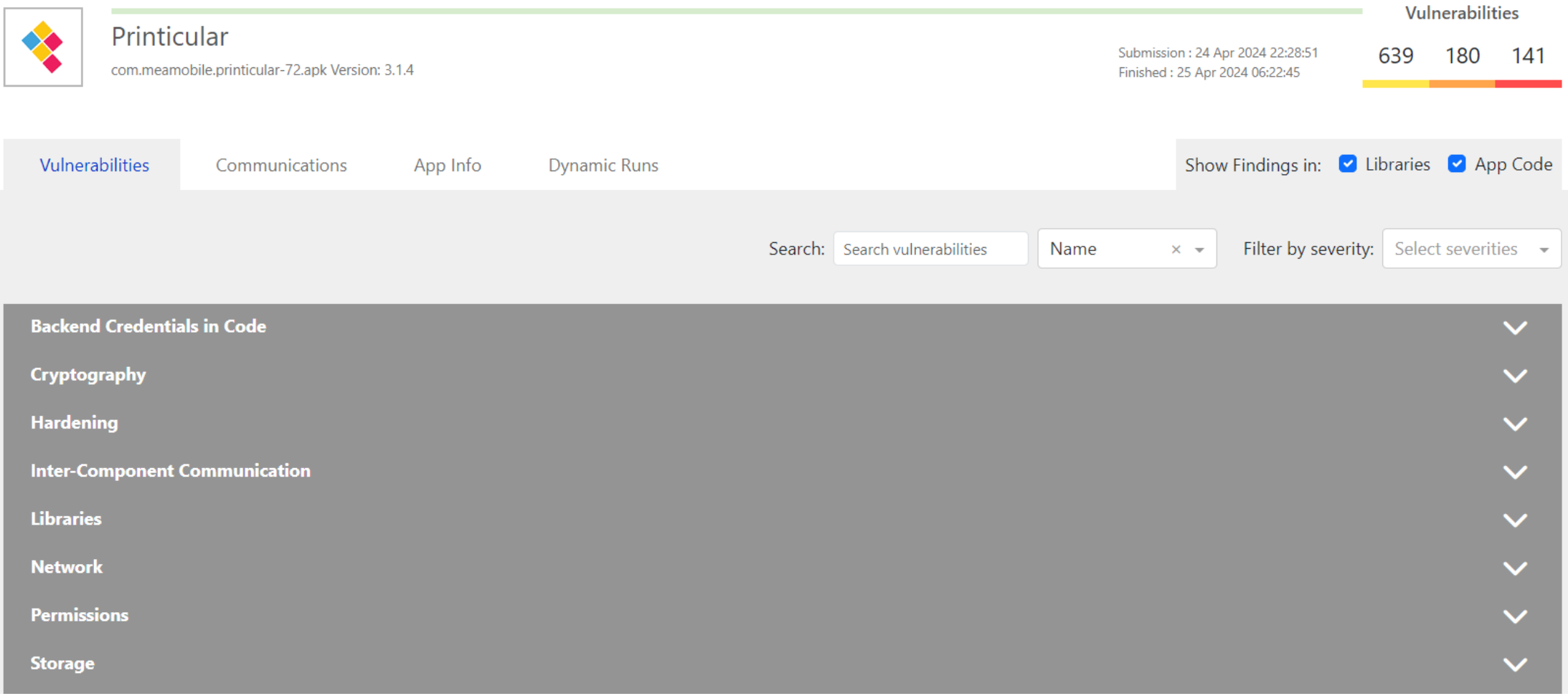
Spotlight: Code Scanning

Possible During Development Process



Spotlight: Code Scanning

Vulnerability Categories on Example



Spotlight: Code Scanning

Vulnerability Details on Example

Backend Credentials in Code

Hard-Coded Backend Credentials for AWS

Description

The app connects to a Amazon Web Service (AWS) database backend using hard-coded credentials.

Mitigation

Never place backend credentials into the app. Use a trusted middleware to connect to the database instead. Ensure that this middleware applies proper authentication and authorization.

References:

The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption. Mobile Application Security Verification Standard as defined by OWASP (Open Web Application Security Project) 3.1

Guide on how to test the key management

Location:

Verify | Jump to Code

Vulnerability was found
in class **com.meamobile.photoserviceandroidapi.photocreate.api.ImagesAPI$S3Connector**

in method **java.lang.String doInBackground(java.lang.String[])**

in statement **specialinvoke $BasicAWSCredentials5.<com.amazonaws.auth.BasicAWSCredentials: void <init>(java.lang.String,java.lang.String)>($String8, $String9)**

Additional data:

Access Key:	AKIAIENI6Q6VG33W4GNA
Secret Key:	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

Models and Code

Integrating Vulnerability Scanning and Risk Model

Analyze Effect of Vulnerabilities

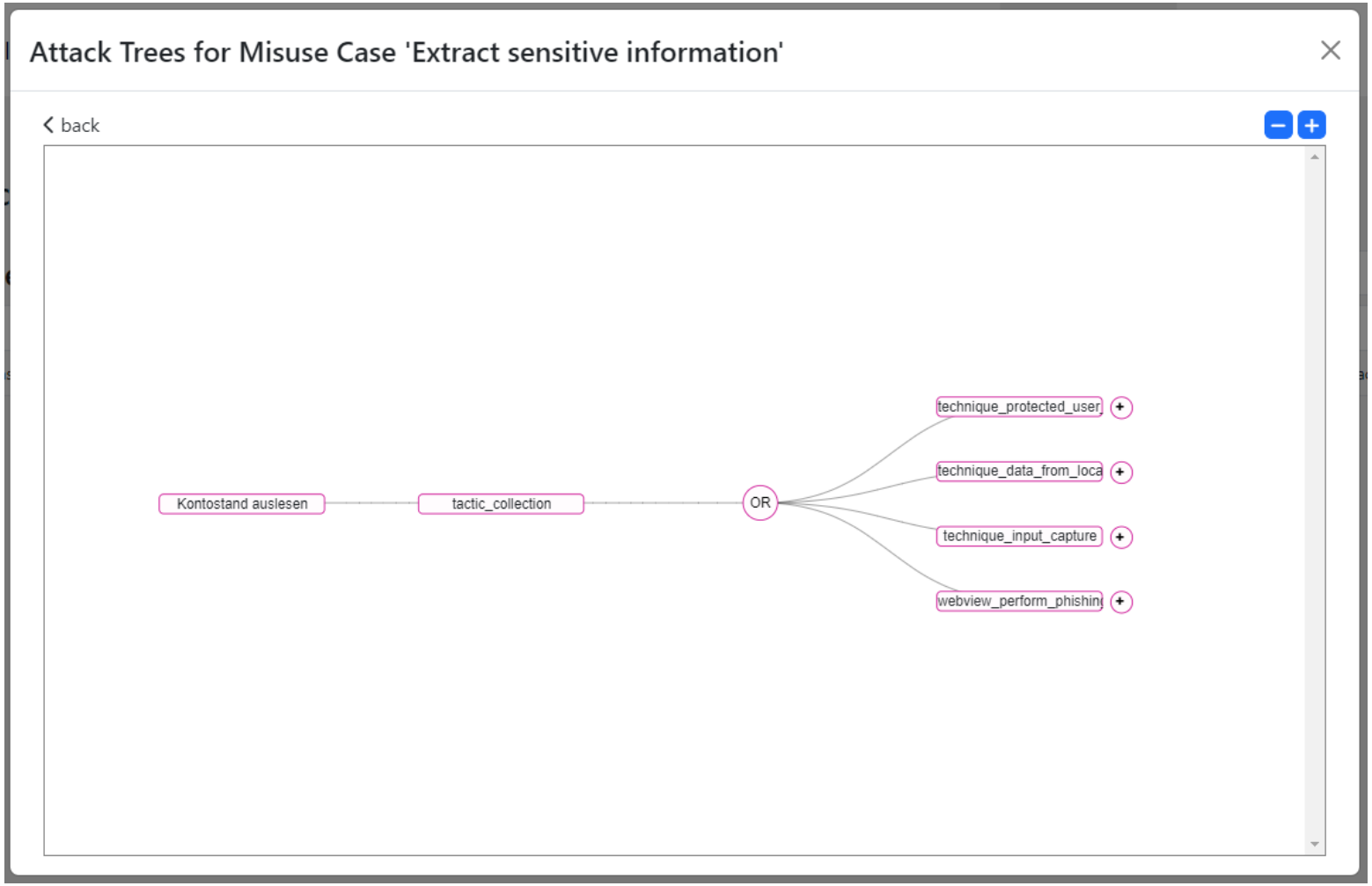
- Link code scanner results to risk model
- Identify affected assets
- Assess attack complexity

Attack Trees

- Model potential attack paths
- Each node is an intermediate goal
- Vulnerabilities help realize intermediate goals

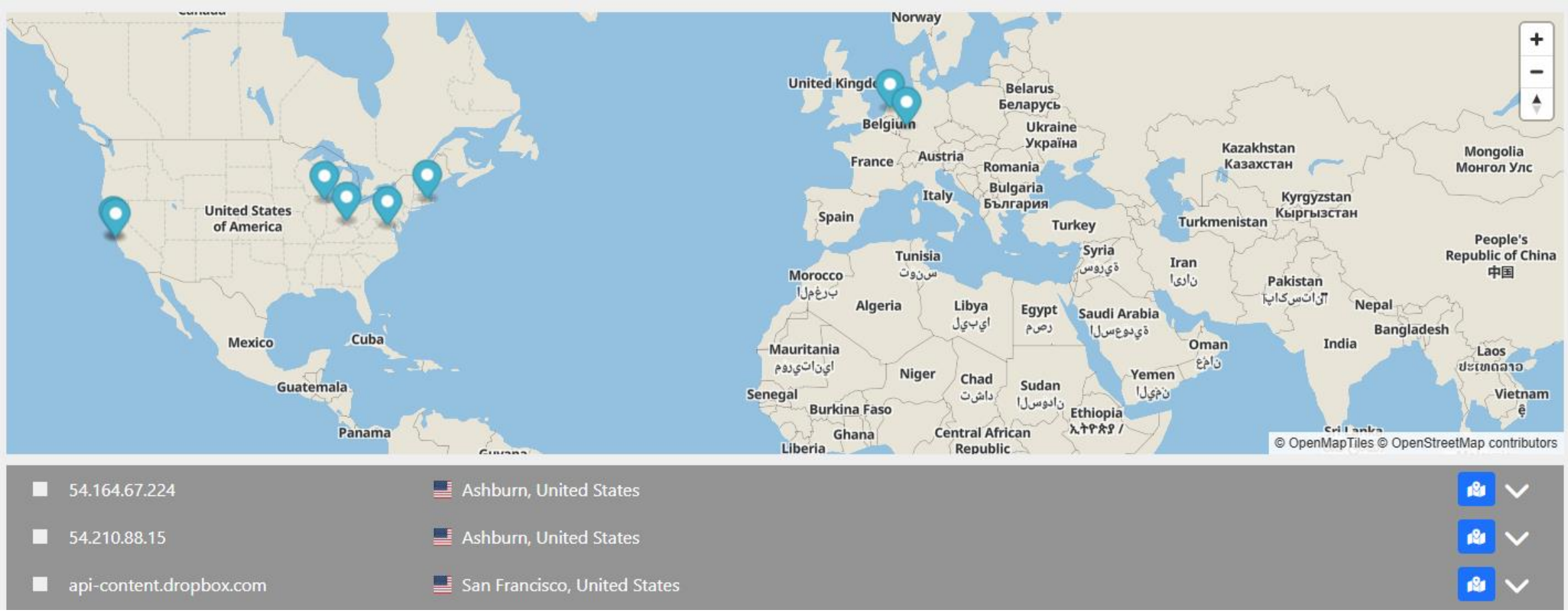
Automatic Matching

- Based on MITRE ATT&CK
- Prototype shown at Fraunhofer booth



GDPR and CRA – Check Your Data Use

Example on the Map



Coordinated Vulnerability Disclosure

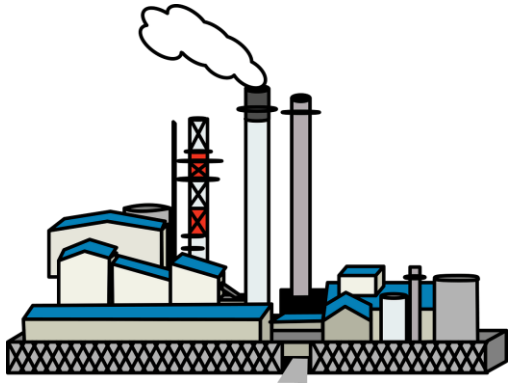
Mandated by the CRA

Researcher

Vulnerability Reports

Arbitrary Person

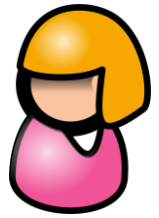
User



Manufacturer

Information

Updates



Customer

Customer

Reporting Responsibilities

Deadlines for Official Reporting

Within 24 Hours: Early Warning

- Affected member states where the product was made available

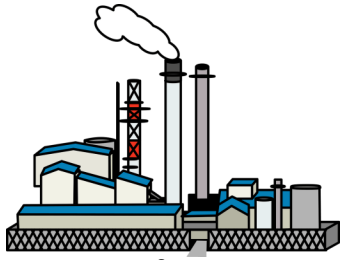
Within 72 Hours: Vulnerability Notification (if Exploited)

- Affected product
- General nature of the exploit
- Vulnerability concerned
- Corrective or mitigating measures taken
- Measured available to users

Within 14 Days: Final Report

- Description of vulnerability & its severity and impact
- If available: Information on malicious actor
- Details about security update or corrective measures

Similar structure for incident reporting



Manufacturer

Government

Orthogonal to Other Regulation

Other Duties May Apply

GDPR

- May require reporting to data protection authority
- May require informing the data subject

NIS-2 Directive and National Law

- Applies to critical infrastructure

DORA

- Banking and financial sector

Dates and Fines

What if we don’t get it right?

Essential Cybersecurity Requirements

- Fine up to 15,000,000 EUR
- Up to 2,5% of total worldwide annual turnover

Documentation and Formals

- Fine up to 10,000,000 EUR
- Up to 2% of total worldwide annual turnover

Failure in Reporting Duties

- Fine up to 5,000,000 EUR
- Up to 1% of total worldwide annual turnover

ATHENE

Fraunhofer SIT

Contact

Dr.-Ing. Steven Arzt
Head of Department Secure Software Engineering
Tel. +49 6151 869-336
Fax +49 6151 869-224
steven.arzt@sit.fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de

Visit us!
Hall 6, booth 314