ECCO
European Cybersecurity COmmunity

Towards Automated Compliance to the Upcoming EU Cyber-Resilience Act

ECCO Community «Road-Mapping»
Knowledge Sharing Webinar

Agenda

ECCO
European Cybersecurity COmmunity

- Objectives of the ECCO Working Group "Road-Mapping" and Introduction of Webinar Series [5 min]
- Overview of the Upcoming Challenges and Requirements of the EU Cyber Resilience Act [10 min]
- Presentation of Early Results Working Towards Automated Compliance of the EU CRA [15 min]
- Open Q&A and discussion [15 min]

ECCO

European Cybersecurity COmmunity

Objectives of the ECCO Working Group "Road-Mapping" and Introduction of Webinar Series

Christian Banse

Fabio Martinelli

March 11 2024

ECCO Community Roadmapping WG

- **Governance & Participants**
- Chairs:
  - Roadmapping: Christian Banse and Claudia Eckert (Fraunhofer AISEC)
  - Development of the Community: Fabio Martinelli (CNR)
- ECCO Proto-Community on “Road-Mapping”:
  - The members of this Community Group are growing stemming from the ECCO experts and the ones in the initial proposal (from ECSO and the 4 Pilots).
  - The initial experts have been carefully selected to ensure a diverse composition, with contributors representing the research and industry community …
  - or with close links to ensure an interesting mix of competencies for the identification of relevant topics in support to the ECCC Strategic Agenda implementation and as such the European cybersecurity ecosystem.
- It is in the process to be expanded with other experts from ECCO proposal and according to suggestions by ECCC, NCCs, etc.

ECCO Community Roadmapping WG (II)

- **Objectives**
- The approach and objectives have been updated to meet the needs of the NCCs Network and ECCC GB, and in support of the implementation of the ECCC Strategic Agenda and its main objective: *“By 2027, the ECCC and the Network will have strengthened the research, development and innovation expertise and competitiveness of the EU cybersecurity community through the development and implementation of an efficient and coherent action plan”*.
- The initial objectives of the ECCO Community Group on road-mapping have been articulated and agreed upon. They are:
  - Build the ECCO proto-community of experts on road-mapping for capability and capacity building to address the priorities of the Strategic Agenda (future DEP projects and pan-European actions).
  - Deep dive road-mapping on priorities for DEP
  - Map concepts from the ECCC Strategic Agenda to other roadmaps (e.g. results of pilots, ECSO, ENISA, etc.) as well as to the cyber resilience landscape.
  - Consolidate and find synergies among recommendations for implementation of the Strategic Agenda from other ECCO Community Groups.
  - Support the NCCs in the implementation of the Strategic Agenda’s Action Plan for improved research, development and innovation expertise and competitiveness of the EU cybersecurity community, e.g., through a series of webinars.

Initial planned webinars

- Perform knowledge sharing webinars with ECCC, NCCs and wider community

- Initial topics identified by the community WG to be covered by June 2024

  1. **Cyber-Resilience (TODAY!)**
  2. Digital Twins and Cyber Security
  3. Trustworthy AI
  4. Data Spaces and Data Sovereignty
  5. 6G and Cyber Security
  6. ...

- We are open re-address and insert new ones for the future according to ECCC and NCCs’ needs and requests.

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Christian Banse

Challenges and Requirements Upcoming of the EU Cyber Resilience Act

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

What is *Cyber Reslience*?

Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

NIST SP 800-160 Vol 2; cyber resource = information resource in electronic form

Cyber Resilient Technologies – Working Group of the TCG

Definition of three core principles

Protection

… of persisted code and configuration

Detection

… of vulnerabilities or manipulation during runtime

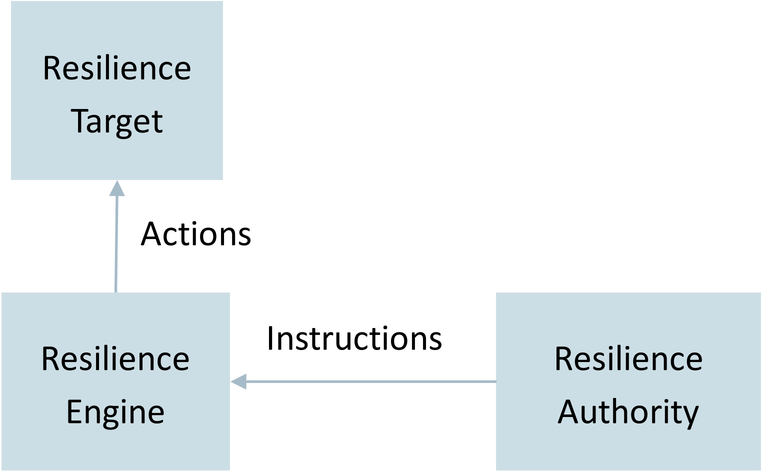
Recovering

… the system into a “good” state

Cyber Resilient Module and Building Block Requirements

Control of a “Resilience Targets” (single application, firmware or VM) through a “Resilience Engine”, acting on behalf of a “Resilience Authority”

One engine can monitor the status of multiple targets (and can reset them if necessary)



How does this apply to the CRA?

Short Disclaimer: The following slides are my own interpretation of the CRA, I am NOT a lawyer, this is NOT legal guidance

Cyber Resilience Act (CRA)

Applicable for *Products with Digital Elements*

Goals

Introduce hardware and software products with **less vulnerabilities** into the market

Manufacturers should address **security issues** during the **complete life-cycle** of the product

Users should be able to differentiate between different products with regards to their security

Who is affected?

Products with digital elements, divided into three categories

- Important Products, class I, for example password managers, browsers, VPN software, routers, …
- Important Products, class II, for example hypervisors, firewalls, …
- Critical Products, for example smart meter gateway, smartcards, secure elements, ...

Important: It is an Act, not a Regulation → "Immediate" affect (after ratification + grace period), no national laws needed

Which procedures must manufacturers follow?

Different security requirements that need to be taken care of when **introducing products** into the market (Article 10, 1)

Manufacturers must do an **assessment of the cyber security risks** (Article 10, 2, 2a). The result must be considered in:

- Planning, Design, Production, Delivery, Maintenance Phase
- Risk must be documented and updated during a support period (see below)

Impact of incidents must be as **little** as possible, especially on the health and security of the user (Article 10, 2)

Manufacturers must take care that third party components to not compromise the security of their product (Article 10, 4)

An appropriate **support period** must be set (Article 10, 6). It should be at least 5 years – unless it is expected that the product itself is used less than 5 years. During that period, **regular (security) updates must be delivered**.

Requirements related to the properties of the product

Conceptual and Architecture

- Secure default configurations (**Security-by-Default**), ability to **reset the device** to its original state (Annex I, Part I, 3a)
- Limit the attack surface (Annex I, Part I, 3h)
- Design systems in a way, so that the **impact of an exploit is limited** (Annex I, Part I, 3i)

Protection and Prevention

- Products must be **free of known exploitable vulnerabilities** (Annex I, Part I, 3-a)
- Suitable access control mechanisms, authentication, identities, etc. (Annex I, Part I, 3b)
- Encryption of relevant data who are "stored, transmitted or otherwise processed" (Annex I, Part I, 3c)

Monitoring and Reaction

- Integrity of "stored, transmitted or otherwise processed" data; **modifications must be reported** to the user (Annex I, Part I, 3d)
- **Monitoring of security-related** information during runtime; with opt-out (Annex I, Part I, 3j)

Requirements to vulnerability management

During the whole support period

Creation of a **Software-Bill-of-Material (SBOM)**, documentation of vulnerabilities and components. **SBOM must be machine-readable!** (Annex I, Part II, 1)

The security of the device must be **regularly reviewed and tested** (Annex I, Part II, 3)

Have a **coordinated disclosure process** and contact person (Annex I, Part II, 5-6)

Support an automated (security) update process and provide **updates without delay** (Annex I, Part II, 7)

Actively exploited vulnerabilities must be reported to the CSIRT (e.g., CERT-Bund in Germany) and (!) ENISA within 24h (Article 11, 1)

Some special cases about open-source

In general, **open-source that is NOT distributed for commercial activities is NOT affected by the CRA** (Article 10, 10c). It is the manufacturers duty who integrates this OSS to take care of the requirements

However, there is a “wish” to establish a voluntary program for OSS projects to fulfill these requirements (Article 10, 10f)

Some entities in the open-source community (“open-source software stewards”), e.g. certain foundations are subject to a “light” version of the regulation, at least if it is ultimately designed to be used in commercial activities (Article 10, 10d)

If manufacturer's identity vulnerability in open-source projects that they use, they must report them to the responsible person or entity (Article 10, 4a)

Cyber Resilience Act (CRA)

Applicable for *Products with Digital Elements*

How?

Depending on the product conformance can either be demonstrated

- through **internal controls** (Module A)
- by **a third-party assessment** through a notified body (Module B)
- conformity to type (Module C)
- full quality assurance system (Module H)
- a **suitable EU cyber security certification** (EUCS, EUCC) or

For example, critical products require an EU cyber security certification (if it exists). Also, the usage of harmonized standards lowers the type of assessment needed, but only for ”important” products (Article 24, 1 vs 2).

Who is not affected? When?

If the product or manufacturer is already otherwise regulated (e.g. the medical domain), the CRA does not affect it

It is expected to be in effect mid of 2024 (+ grace period of 3 years)

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Christian Banse

Working Towards Automated Compliance of the EU CRA

Motivation and Challenge for Automating Compliance Checking

Increasing number of security certifications and regulations: GDPR, KRITIS / IT-SIG 2.0, ***EU Cyber Resilience Act***, EU Cyber Security Act, EUCS, IEC 62443, ISO 27070, BSI C5, **BSI AIC4,** …

- Increased pressure on companies to fulfill the requirements …
- … while establishing faster and shorter development cycles

Increased Complexity of Products and Services

- Dependencies on third party (libraries)
- Increased number of lines-of-code in applications – maybe even AI generated
- Growing number of deployed cloud resources

Control Systems must be in place and possibly be demonstrated

→ Automation

Which Classes of Open-Source tools can help us with Compliance Checking?

Evidence Management and Gathering

We need to gather sufficient evidence from various sources that prove the compliance of certain resources (e.g., a Cloud infrastructure, source code)

We need to store, filter and possibly retrieve evidences in various forms, e.g., for automated assessment or to show the auditor

Security Assessment

We need to assert that the gathered evidence is adhering to the requirements of a specific control of a certification

The outcome of this assessment could be in a standardized format, such as OSCAL.

Governance and Risk Tools

Certifications also involved non-technical processes and policies. We need to document them as well.

We also need to manage the life-cycle of a certification and possibly select different controls or assurance levels based on the risk of our service or product.

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Where can we start from?

Contributions to Cloud Compliance

Based on European Projects

MEDINA

Horizon 2020 – Research and Innovation Action (2020-2023)

Design and implementation of a security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme.

Development of open-source tools within the project (TRL5)
Clouditor – Compliance orchestrator and assessment
AMOE – Assessment of organizational evidences using NLP
Catalog – Searchable catalog of controls and metrics
LifeCycleManager – Manages the digital life-cycle of a certificate
….

EMERALD

Horizon Europe – Innovation Action (2023-2026)

Increasing the TRL of the MEDINA core technologies (e.g., Clouditor) with a focus on harmonizing evidence management. Extracting semantic information into a knowledge graph.

COBALT

Horizon Europe – Innovation Action (2023-2026)

Transferring the technologies of MEDINA and other projects to a broad spectrum of use cases (e.g., Industry 4.0, AI, Quantum) using a Common Certification Model (CCM)

EMERALD

Evidence Management for Continuous Certification-as-a-Service in the Cloud

Main Objective

*Pave the road towards **Certification-as-a-Service (CaaS)** for **continuous certification** of **harmonized cybersecurity schemes**, like the European Cybersecurity Certification Scheme for Cloud Services (**EUCS**).*

Addressed Users

Cloud Service Providers and Users

- EMERALD will offer a framework to set-up, manage and monitor their certifications and enable lean recertification.

Auditors

- EMERALD will be an audit assistance framework with a strong focus on a user interaction concept
- Offering a uniform way to address audits and complexity reduction through the customization of the audit process

Approach

Promoting scalability and re-usability

Target and Scope of Audit

Definition of target catalogs and schemes, e.g., EUCS

Select suitable security metrics from a (to-be-established) repository that map to the selected security scheme(s)

Evidence Collection

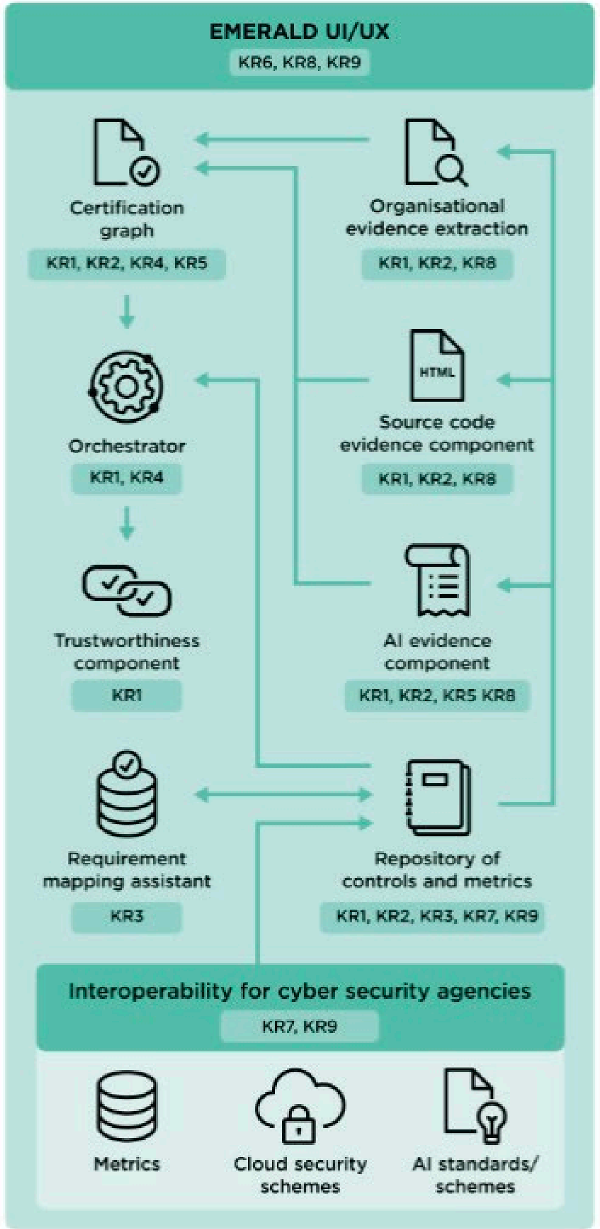
Collection of appropriate evidence from different sources

- Cloud infrastructure configuration, e.g. through CSPM
- Source code, e.g. through static code analysis
- Application specific data, e.g. AI models

Assessment and Evaluation

Assessment of evidence according to metrics

Aggregation of results and certificate decision



EMERALD UI/UX
KR6, KR8, KR9

Certification graph
KR1, KR2, KR4, KR5

Organisational evidence extraction
KR1, KR2, KR8

Orchestrator
KR1, KR4

Source code evidence component
KR1, KR2, KR8

Trustworthiness component
KR1

AI evidence component
KR1, KR2, KR5 KR8

Requirement mapping assistant
KR3

Repository of controls and metrics
KR1, KR2, KR3, KR7, KR9

Interoperability for cyber security agencies
KR7, KR9

Metrics

Cloud security schemes

AI standards/ schemes

Clouditor

A reference implementation within the EMERALD framework

Clouditor enables a continuous assessment of the security of cloud resources, across different cloud environments

- **Discovery** of resources of well-established cloud providers and technologies, such as AWS, Azure, Kubernetes and OpenStack
- Translation of discovered resource into **evidence** in the form of an "ontology" [1, 2]. This ontology contains information about generic cloud resources, their properties and relations to other resources.
- **Assessment** of evidence based on metrics written in a high-level logic programming language → Rule language and assessment works independently of the actual technology used
- Addresses security controls such as EUCS, BSI C5 or others

Community Edition available in GitHub:
https://github.com/clouditor/clouditor

[1] Christian Banse, Immanuel Kunz, Angelika Schneider and Konrad Weiss. Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis. IEEE CLOUD 2021. https://doi.org/10.1109/CLOUD53861.2021.00014
[2] Immanuel Kunz, Konrad Weiss, Angelika Schneider and Christian Banse. Privacy Property Graph: Towards Automated Privacy Threat Modeling via Static Graph-based Analysis. Proceedings on Privacy Enhancing Technologies 2022.

Codyze

An open-source tool for checking **source code** for **correct implementation patterns**

Model and Rules

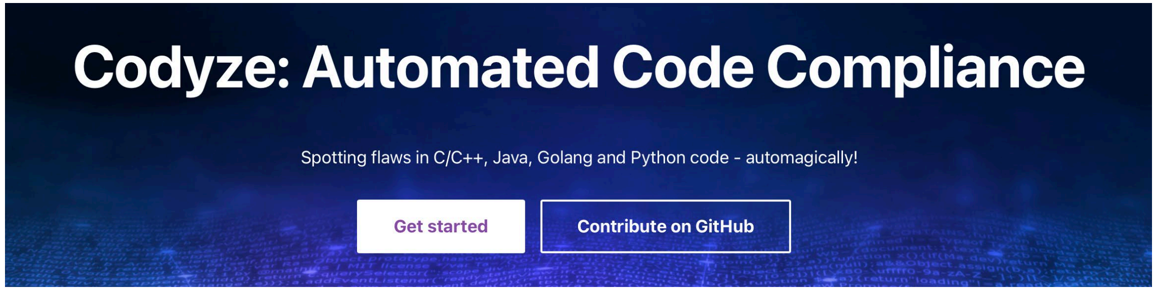
Codyze can be used to impose certain **rules** on abstract **models**, representing concepts found in applications. Example concepts can be the correct behavior of encryption, authentication or logging.

The validation of a piece of application code against this rule and model can be regarded as **evidence**.

Freely available on https://www.codyze.io

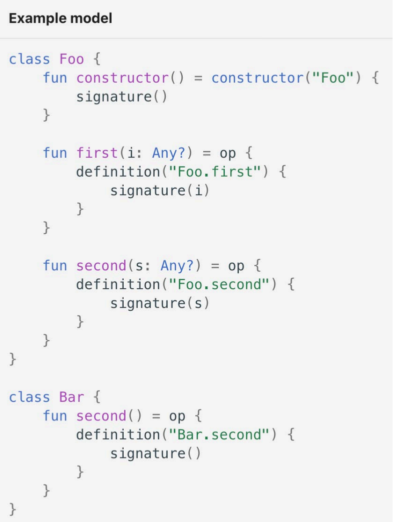
Powered by the Code Property Graph (CPG)

Source code is translated into a language-independent representation: Code Property Graph supporting C/C++, Java, Go, Python, Ruby and Typescript.



Codyze: Automated Code Compliance

Spotting flaws in C/C++, Java, Golang and Python code - automagically!



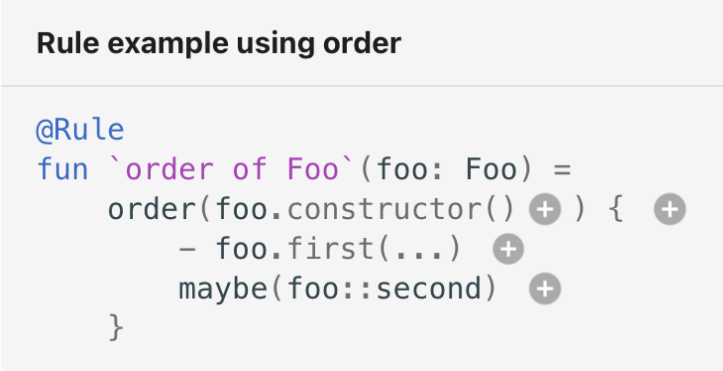
Example model

```
class Foo {
    fun constructor() = constructor("Foo") {
        signature()
    }

    fun first(i: Any?) = op {
        definition("Foo.first") {
            signature(i)
        }
    }

    fun second(s: Any?) = op {
        definition("Foo.second") {
            signature(s)
        }
    }
}

class Bar {
    fun second() = op {
        definition("Bar.second") {
            signature()
        }
    }
}
```



Rule example using order

```
@Rule
fun `order of Foo`(foo: Foo) =
    order(foo.constructor() ⊕ ) { ⊕
        - foo.first(...) ⊕
        maybe(foo::second) ⊕
    }
```

Codyze has been funded by the Bundesamt für Sicherheit in der Informationstechnik (BSI).

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Can evidences be gathered in a structured and re-usable way?

Ontology

Combination of different taxonomies

Example „Virtual Machine“

Security Features

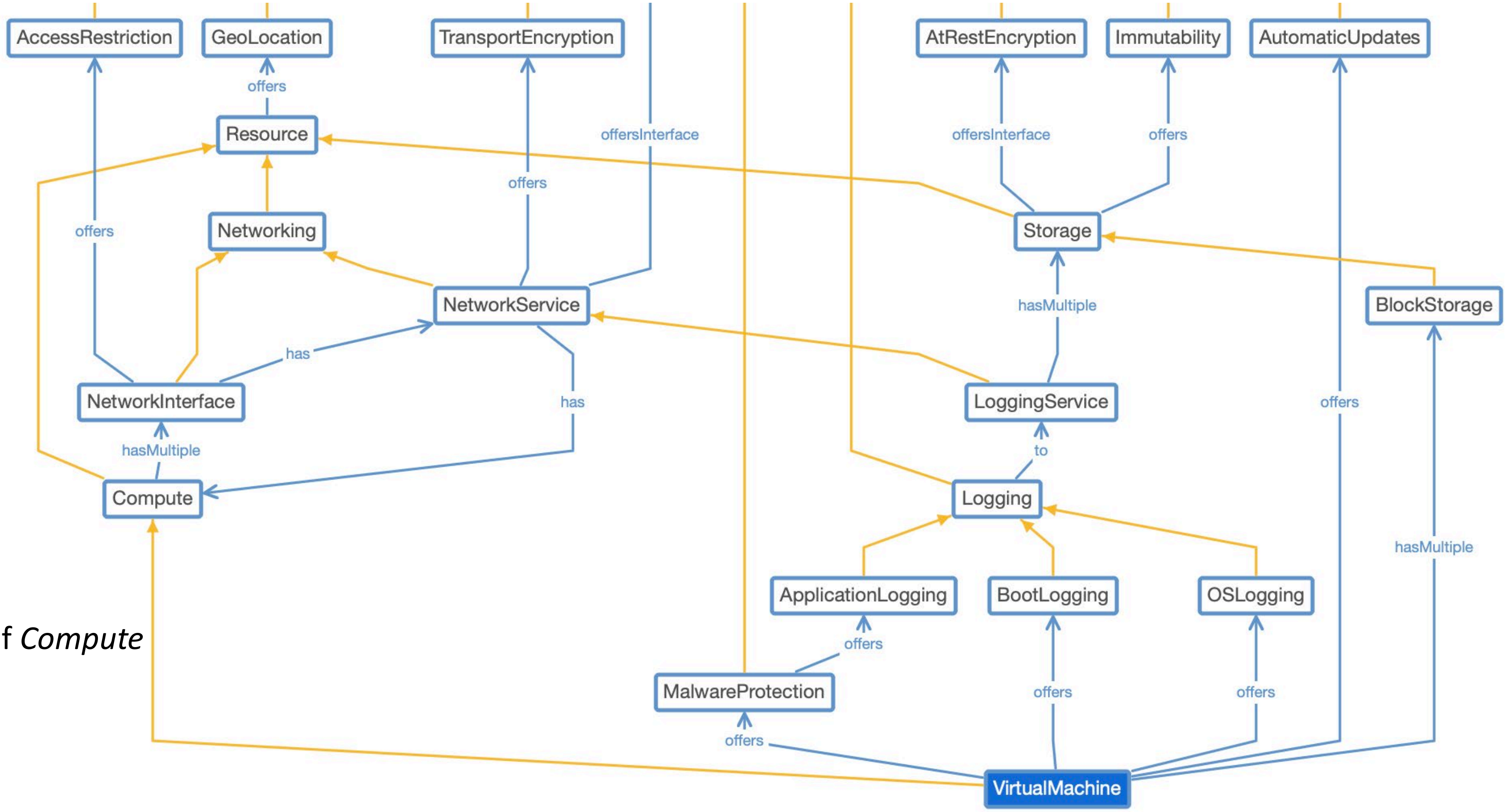
- *Logging*
- *MalwareProtection*

Relations to other resources

- *BlockStorage* (for the Disk Image)
- *LoggingService* (as target of log files)

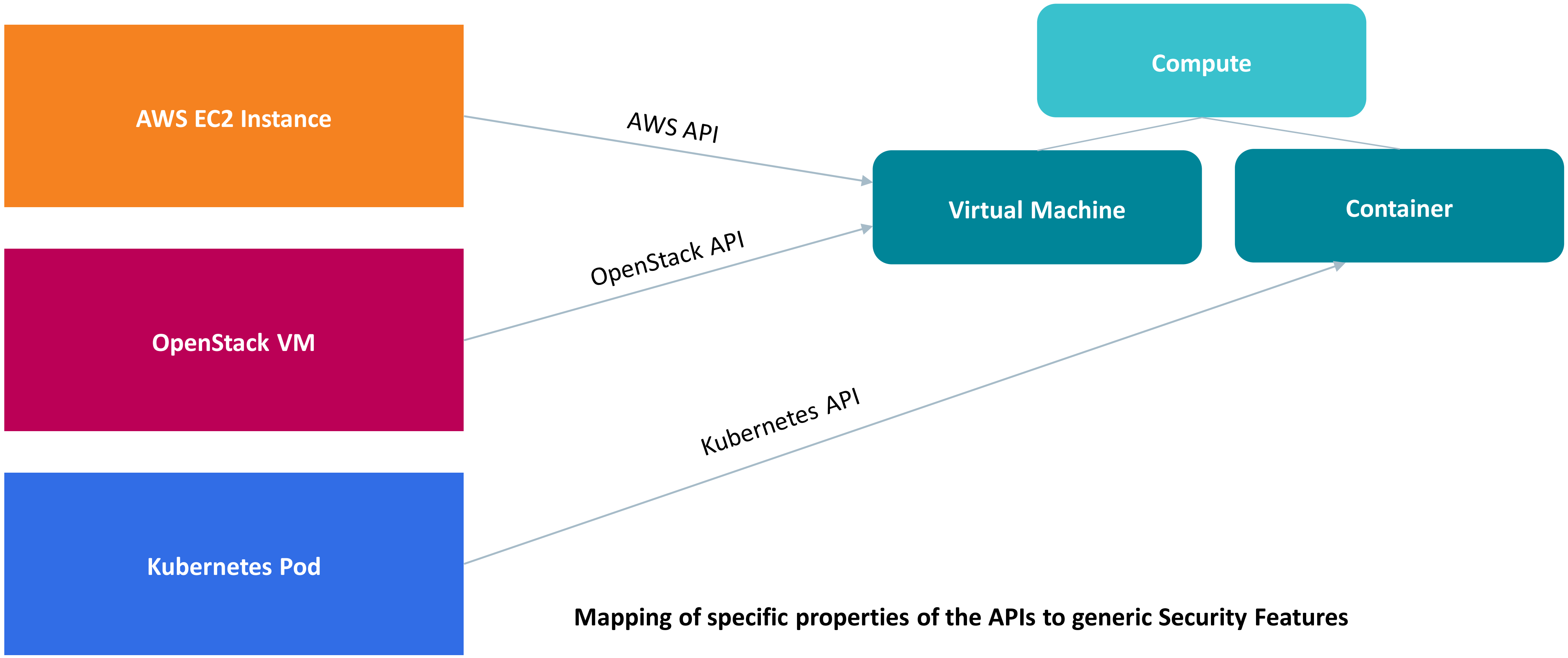
Cross-connections and inheritance

- *LoggingService* connects to a *Storage*
- *VirtualMachine* derives certain base properties of *Compute*



Public

Translation of Resources into the Ontology



Mapping of specific properties of the APIs to generic Security Features

Rules based on the Ontology

Compliance-as-Code to Assess Evidences

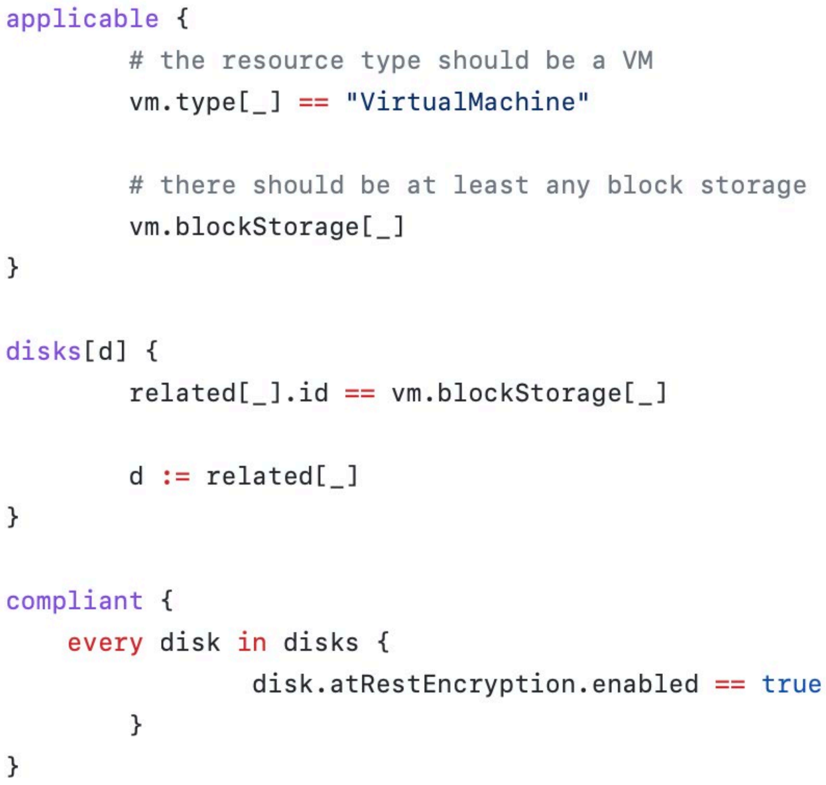
Cryptography

- Transport encryption enabled
- Suitable TLS cypher suites selected; min TLS version
- Storage encryption of VM disk images
- …

Logging

- Logging enabled (OS level, application level)
- Suitable retention time, e.g., 90 days
- Logs are only stored on immutable storage
- …

Implementation in Rego



```
applicable {
        # the resource type should be a VM
        vm.type[_] == "VirtualMachine"

        # there should be at least any block storage
        vm.blockStorage[_]
}

disks[d] {
        related[_].id == vm.blockStorage[_]

        d := related[_]
}

compliant {
    every disk in disks {
                disk.atRestEncryption.enabled == true
        }
}
```

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

How can we translate this to the CRA?

From The Cloud To Cyber-Resilience

Different, but comparable Stakeholders

Cloud Service Provider → Manufacturer

Cloud Service → Product with digital Elements

Auditor → Auditor; although only required for certain classes of products

The Technological Basis is already there

We need to extend our ontology to fit to product classes affected by the CRA, e.g., a Firewall

We can adopt a lot of existing metrics, e.g., regarding key management, authentication, encryption, logging

We probably need to define new metrics, e.g., regarding

- Dependencies
- SBOMs, supply chain security
- Incident handling
- …

We also need to extend the existing discoverers (which are mostly Cloud based) into things like network scanning, dependency scans, …

Why Open-Source Approaches to Compliance are Important

Openness

A lot of commercial tools only look at the “big” technologies, e.g., in the Cloud: only the hyperscalers

But there are a lot of smaller manufacturers (often SMEs) that are similarity affected by regulations. They are often also using open-source technologies to provide their products and services

We can more easily on-board new technologies in an open-source implementation. Providers can even contribute to the tools themselves

Why Open-Source Approaches to Compliance are Important

Trust and Verifiability

With open-source, we can have a look into how things work “behind the scenes”

This is especially critical for evidence “assessment” evaluation, where we want to deduce certain metrics, or a compliance status based out of the presented evidence

We need to make sure that we trust this mechanism and that it also works as intended

Reference Implementations

Open-source projects could service as a “reference” to a correct implementation of a particular standard, which then other tools (even commercial ones) could follow

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Conclusions

Conclusions

The CRA will introduce some challenging requirements

Data protection, authentication

Minimization of attack surface and mitigation of the impact of vulnerabilities

Security Monitoring, Vulnerability Management and Reporting

Companies and communities should start to get ready

Read and understand the CRA and the product classes → **Are you affected?**

Check the requirements → **Are you fulfilling them?**

Automation is key in order to demonstrate or implement compliance

Open-Source can have an enabling factor, especially for smaller and medium enterprises that are affected

ECCO

European Cybersecurity COmmunity

Q&A and Discussion

Christian Banse

Fabio Martinelli

March 11 2024