



Competence Center



We master the innovation wave

Competence Center

Competence areas:

- digital transformation
- cybersecurity
- data protection



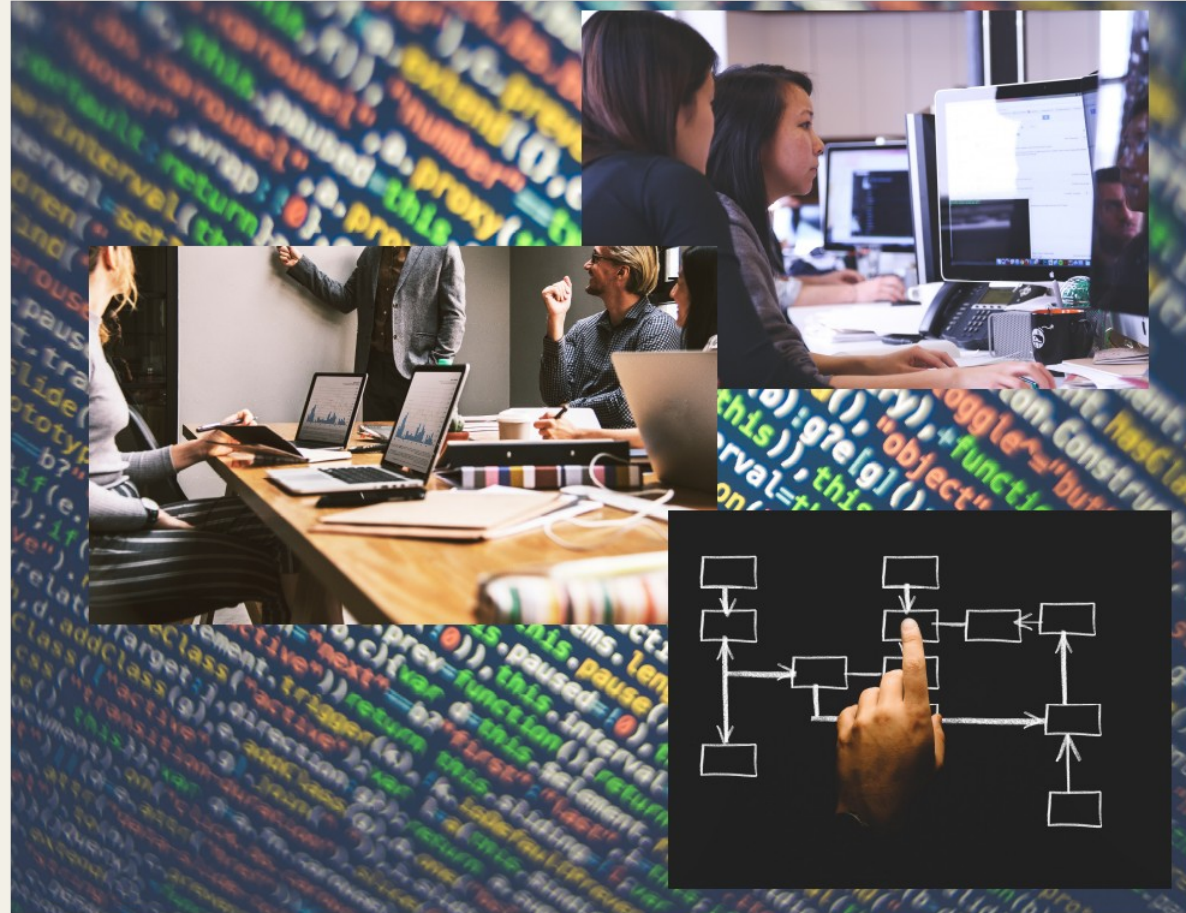
Services

- consultancy
- assistance
- tutoring
- new technical solutions design
- legislation rules education



Technological design and development

- tools focused on specific functional services
- enabling platforms realization
- e-learning systems
- compliance tools
- risk assessment and risk evaluation tools
- risk assessment dashboards



Why Pragmema



Many companies offer a 360°
assistance, consultancy and
development...

...but your business has more
than one dimension



Pragmema innovative holistic approach
can increase your business in every
dimension

The range of our experts includes:

- an ontology and language expert
- multidisciplinary experts
- an engineering team with expertise in every field
- a development team using the latest technologies



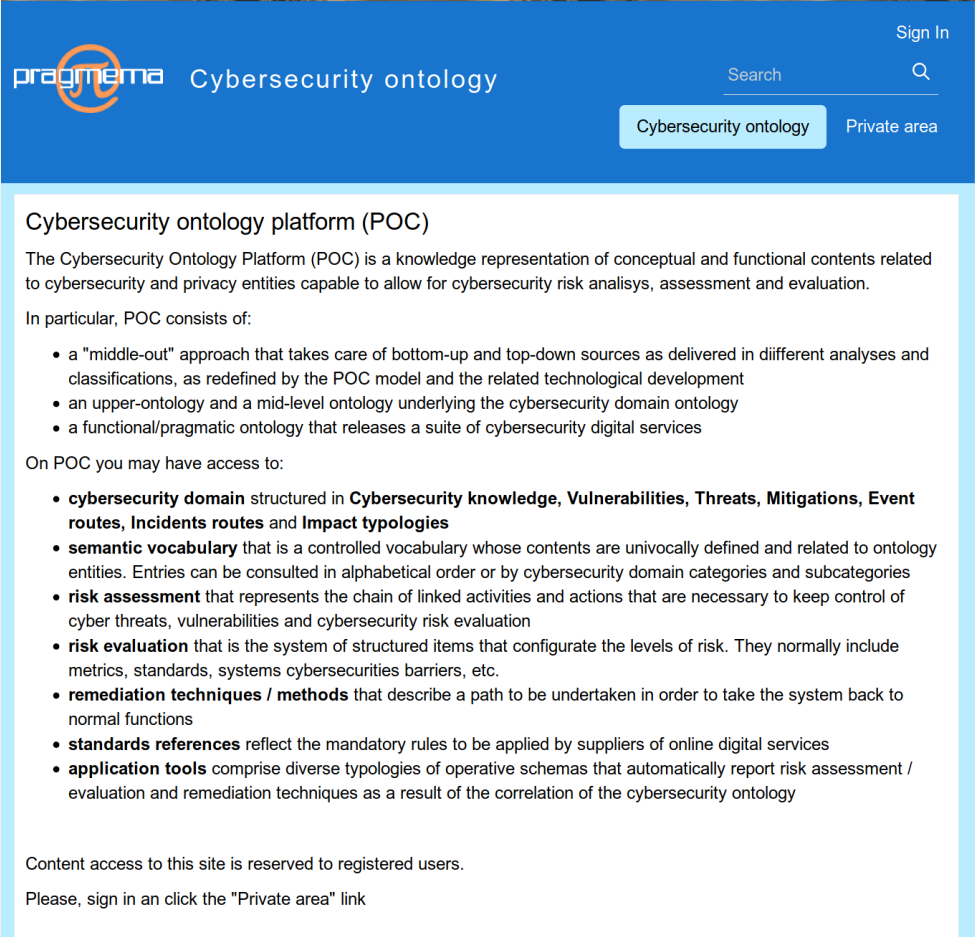
Pragmema application case



Cybersecurity ontology

Pragmema cybersecurity ontology portal gives access to:

- a high level cybersecurity domain ontology
- a middle level cybersecurity pragmatic ontology
- a series of ontology based services



The screenshot shows the Pragmema Cybersecurity ontology portal. The header is blue with the Pragmema logo (an orange circle with a stylized 'p') and the text 'Cybersecurity ontology'. On the right of the header, there is a 'Sign In' link, a search bar with a magnifying glass icon, and two buttons: 'Cybersecurity ontology' and 'Private area'. The main content area has a white background. It starts with the title 'Cybersecurity ontology platform (POC)' followed by a paragraph: 'The Cybersecurity Ontology Platform (POC) is a knowledge representation of conceptual and functional contents related to cybersecurity and privacy entities capable to allow for cybersecurity risk analysis, assessment and evaluation.' Below this, it says 'In particular, POC consists of:' followed by a bulleted list: 'a "middle-out" approach that takes care of bottom-up and top-down sources as delivered in different analyses and classifications, as redefined by the POC model and the related technological development', 'an upper-ontology and a mid-level ontology underlying the cybersecurity domain ontology', and 'a functional/pragmatic ontology that releases a suite of cybersecurity digital services'. Then it says 'On POC you may have access to:' followed by another bulleted list: 'cybersecurity domain structured in Cybersecurity knowledge, Vulnerabilities, Threats, Mitigations, Event routes, Incidents routes and Impact typologies', 'semantic vocabulary that is a controlled vocabulary whose contents are univocally defined and related to ontology entities. Entries can be consulted in alphabetical order or by cybersecurity domain categories and subcategories', 'risk assessment that represents the chain of linked activities and actions that are necessary to keep control of cyber threats, vulnerabilities and cybersecurity risk evaluation', 'risk evaluation that is the system of structured items that configure the levels of risk. They normally include metrics, standards, systems cybersecurity barriers, etc.', 'remediation techniques / methods that describe a path to be undertaken in order to take the system back to normal functions', 'standards references reflect the mandatory rules to be applied by suppliers of online digital services', and 'application tools comprise diverse typologies of operative schemas that automatically report risk assessment / evaluation and remediation techniques as a result of the correlation of the cybersecurity ontology'. At the bottom, it states 'Content access to this site is reserved to registered users.' and 'Please, sign in and click the "Private area" link'.

pragmema Cybersecurity ontology

Sign In

Search

Cybersecurity ontology Private area

Cybersecurity ontology platform (POC)

The Cybersecurity Ontology Platform (POC) is a knowledge representation of conceptual and functional contents related to cybersecurity and privacy entities capable to allow for cybersecurity risk analysis, assessment and evaluation.

In particular, POC consists of:

- a "middle-out" approach that takes care of bottom-up and top-down sources as delivered in different analyses and classifications, as redefined by the POC model and the related technological development
- an upper-ontology and a mid-level ontology underlying the cybersecurity domain ontology
- a functional/pragmatic ontology that releases a suite of cybersecurity digital services

On POC you may have access to:

- **cybersecurity domain** structured in **Cybersecurity knowledge, Vulnerabilities, Threats, Mitigations, Event routes, Incidents routes and Impact typologies**
- **semantic vocabulary** that is a controlled vocabulary whose contents are univocally defined and related to ontology entities. Entries can be consulted in alphabetical order or by cybersecurity domain categories and subcategories
- **risk assessment** that represents the chain of linked activities and actions that are necessary to keep control of cyber threats, vulnerabilities and cybersecurity risk evaluation
- **risk evaluation** that is the system of structured items that configure the levels of risk. They normally include metrics, standards, systems cybersecurity barriers, etc.
- **remediation techniques / methods** that describe a path to be undertaken in order to take the system back to normal functions
- **standards references** reflect the mandatory rules to be applied by suppliers of online digital services
- **application tools** comprise diverse typologies of operative schemas that automatically report risk assessment / evaluation and remediation techniques as a result of the correlation of the cybersecurity ontology

Content access to this site is reserved to registered users.

Please, sign in and click the "Private area" link

The background of the slide is a dark, textured surface covered with numerous 3D question marks. Most of these question marks are black and appear to be recessed into the surface. Three specific question marks are highlighted in a bright orange color, standing out from the black ones. One orange question mark is located in the upper right quadrant, another is in the upper left quadrant, and the third, which is the largest, is positioned centrally below the main text. The text 'Why this three levels approach?' is centered on the slide in a white, sans-serif font.

Why this three levels approach?

Any people can develop tools
that acquire and manage data...

...but the lack of a unique data
interpretation, the different
languages used and the lack of
a data structure severely limit
the utility of these tools



Pragmema tools based on the pragmatic ontology guarantee:

- a unique data definition related to the ontology
- a common language avoiding confusion and misinterpretation
- a solid ground to analyze congruent data



The pragmatic ontology is related to a particular domain

Pragmatic ontologies related to different domains need a unifying upper ontology

Pragmema cybersecurity domain ontology includes related sub-domain ontologies:

- the cybersecurity pragmatic domain
- the automotive cybersecurity sub-domain
- the financial cybersecurity sub-domain

The image displays two overlapping screenshots of the Pragmema Cybersecurity ontology website. The top screenshot shows the 'Cybersecurity domain' page, which lists components like Cybersecurity knowledge, Vulnerabilities, Threats, Mitigations, Event routes, Incidents routes, and Impact typologies. The bottom screenshot shows the 'Cybersecurity subdomains' page, which lists Automotive and Financial subdomains.

Cybersecurity domain

The cybersecurity domain is structured in:

- **Cybersecurity knowledge** that represents the articulation of the cybersecurity ontology as related to specific conceptual fields
- **Vulnerabilities** that are the ontology components describing weaknesses in the computational logic found in products or devices that could be exploited by a threat source
- **Threats** that is the typology of prospective cybersecurity exploits / attacks as a result of vulnerabilities / weaknesses
- **Mitigations** that are the ontology components such as techniques, methods, software, devices, etc. that constitute a barrier or a resilience tool against cyber attacks
- **Event routes** that are the ontology components that describe cybersecurity attack routes from reconnaissance to logical impacts
- **Incidents routes** that are the ontology components that describe the incident routes / paths of the attack from installation / delivery / activation
- **Impact typologies**

Cybersecurity subdomains

The articulation of the cybersecurity domain ontology into spheres of virtual interactions/sectors of digital interactions.

Ready to start a collaboration with Pragmema?

