

From IoT to Cloud – Securing the continuum

European perspectives

Vasco Gomes
Global CTO for Atos Cybersecurity Products
19/05/2022



Content overview

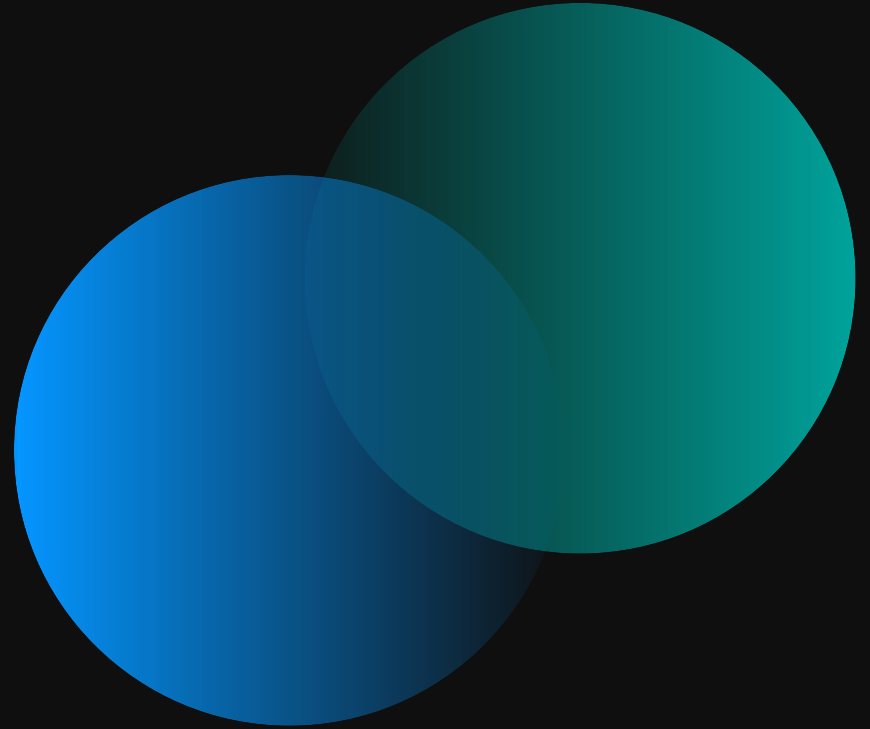
01. EU funding programs overview

02. Main principles

03. Atos Digital Security

04. Major expected benefits

01. EU funding programs overview



EU funding programs

Powering the EU's recovery



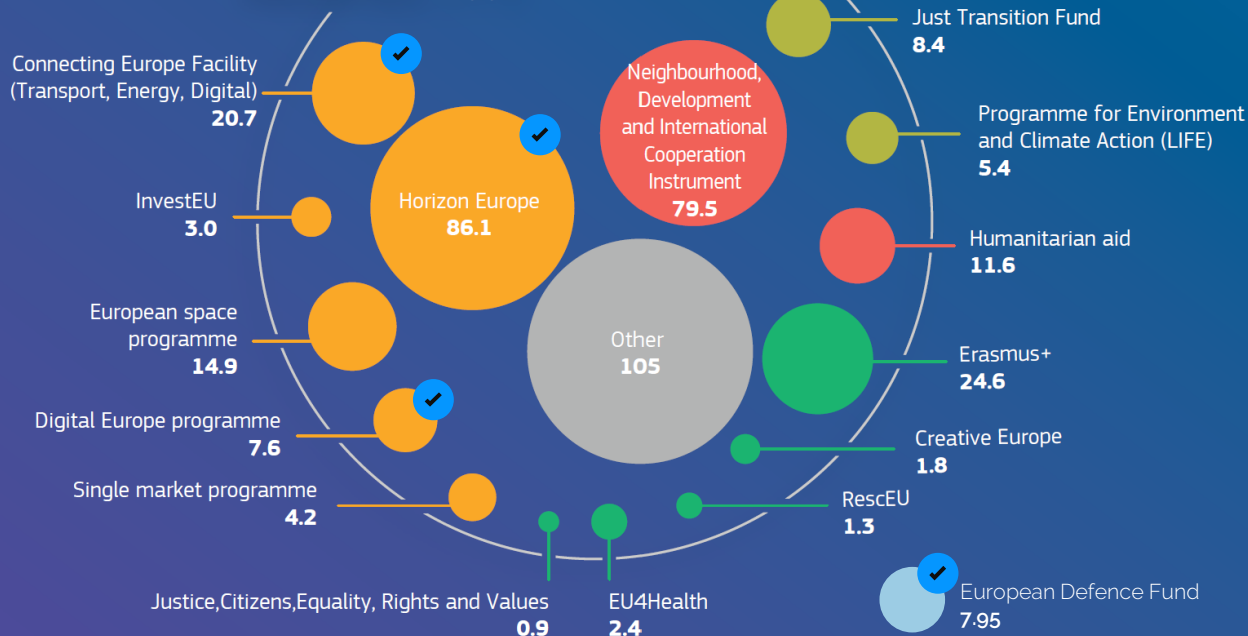
European
Commission

European Commission, Directorate-General for Budget, *The EU's 2021-2027 long-term budget and NextGenerationEU: facts and figures, 2021*, <https://data.europa.eu/doi/10.2761/808559>

Public information web page : https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes_en

Funding and Tenders portal : <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>

NEW AND REINFORCED PRIORITIES 377.3



Single Market, Innovation and Digital
149.5 (+ 11.5 from NGEU)
Cohesion, Resilience and Values
426.7 (+ 776.5 from NGEU)
Natural Resources and Environment
401 (+ 18.9 from NGEU)
Migration and Border Management
25.7
Security and Defence
14.9
Neighbourhood and the World
110.6
European Public Administration
82.5



Main Atos Digital Security involvement (more details in next slide)

EU funding programs

Main Atos Digital Security involvement



Horizon Europe

Horizon Europe is the EU framework programme for **research and innovation**: it promotes **excellence in research** and provides essential **support to top researchers and innovators** to drive the systemic changes needed to **ensure a green, healthy and resilient EU**.

https://ec.europa.eu/info/horizon-europe_en



Connecting Europe Facility

To accelerate investments in **Europe's transport, energy and digital infrastructure** networks. To support the twin green and digital transitions, by contributing to the ambitious infrastructure targets for the **European Green Deal and the digital decade**.

https://cinea.ec.europa.eu/connecting-europe-facility_en



Digital Europe Programme

To accelerate the recovery and drive the **EU's digital transformation**, to build the EU's strategic digital capacities and **facilitate the wide deployment** of digital technologies, to be used by **EU citizens, businesses and public administrations**.

<https://digital-strategy.ec.europa.eu/en/activities/digital-programme>



European Defence Fund

The new European Defence Fund will support **collaborative defence research and development** actions and will promote **cross-border cooperation** throughout the EU.

https://ec.europa.eu/defence-industry-space/eu-defence-industry_en

Other EU Programs

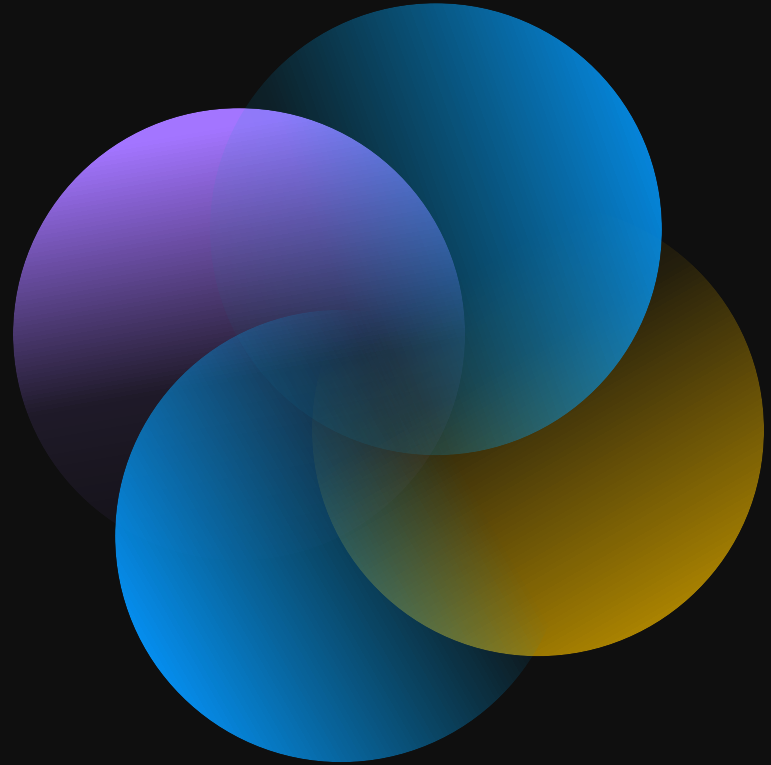
Important projects of common European interest (IPCEIs)

- Part of the EU Commission's State aid modernisation (SAM) ⁽¹⁾ initiative
- Supports major cross-border innovation and infrastructure projects
- IPCEI examples
 - Microelectronics and Communication Technologies
 - Next Generation Cloud Infrastructure and Services
 - Battery value chain
- From Cloud to Edge, including 5G, chips, batteries, etc.
 - Cloud – Edge continuum
 - OT platform
 - Smart City Platform (IoT data exchange)



(1) SAM : https://ec.europa.eu/commission/presscorner/detail/en/IP_12_458

02. Main principles



Main principles

RIA TRL 1-6 3-4 years 100%
IA TRL 5-8 2.5-3 years 70%
CSA, ERC, MSCA...

Horizon Europe ratings example (10/15)⁽¹⁾

- Excellence (3/5)
- Impact (3/5)
- Implementation (3/5)

(1) (Threshold/Max)



Mix of organizations

- Industrials,
- SMEs,
- Public institutions (universities & labs)

Pan-European

- multiple member states cooperation (NB : not from the same industrial)

Collaborative consortiums

Variable funding rates

Technology Readiness Levels

- e.g., RIA (90% or 100%), IA (70%), Deploy (50%)...

Organizations types

- Public/private
- for profit or not



Reuse and/or alignment

- cross programs and calls.

Alignment with other pan-European programs

- e.g., Gaia-X for Cloud

Consistency



Numerous consortiums proposals, very high quality required

Competitive proposals

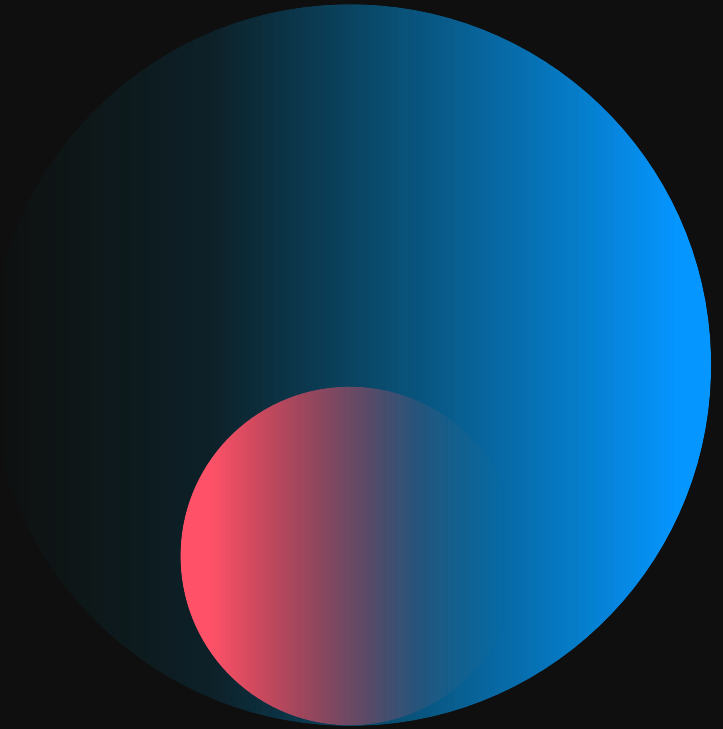
Evaluation criteria

Vary according to program

- Attentive to ethics, safety, AI robustness if applicable, etc.

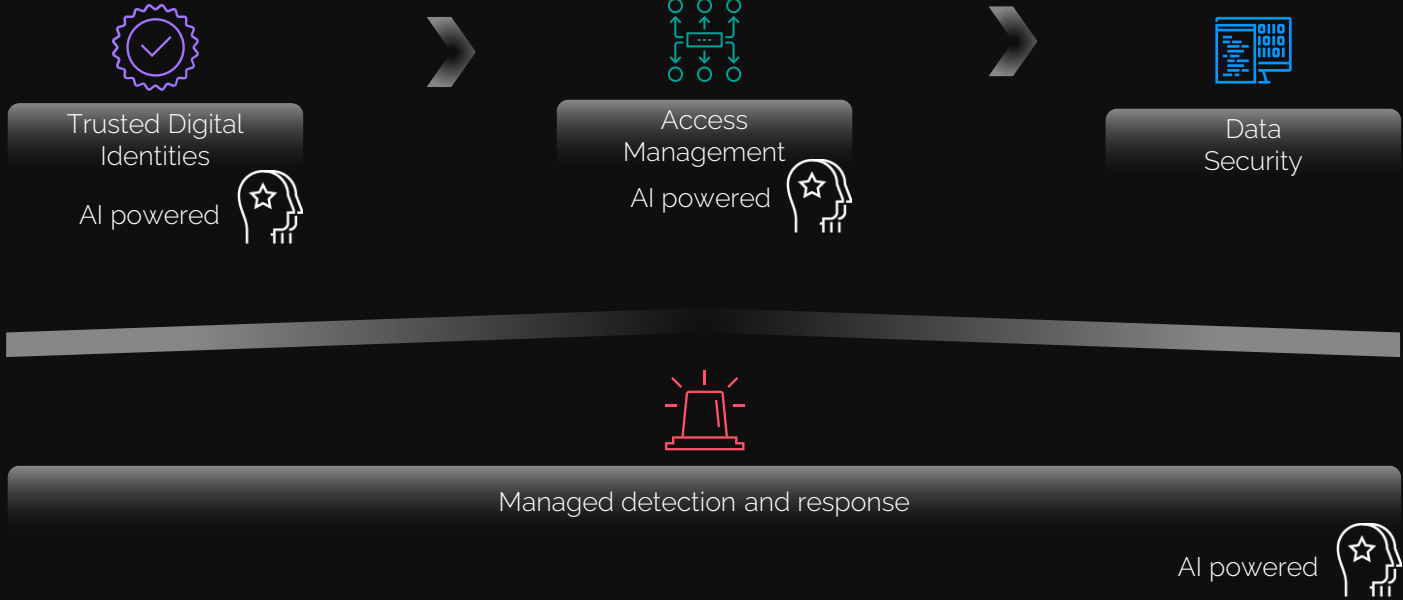


03. Atos Digital Security



Atos Digital Security Confideo

Major areas of focus (amongst a comprehensive portfolio)



Key targeted use cases



Trusted Identities

Democratize it

- SSI/DID
- ZTO

Extend it

- IDs for OT, IoT...
- Vehicles, harbors, 5G, etc.
- Gaia-X standards

Make it smart

- ID misbehavior detection



Data access management

Democratize it

- All features as a service

Extend it

- OT & IoT access control
- Gaia-X standards

Make it smart

- Risk engine
- Actions to risk level
- Ease human processes



Data Encryption

Democratize it

- Cloud & Edge B/H Your Own K/E
- Client-side & gateway encryption

Extend it

- Privacy Enhancing Technologies
- Entropy increase
- Quantum safe
- Hardware Security



Managed Detection & Response

Democratize it

- Enterprise Security Dashboard
- Trainings & exercises

Extend it

- IT / OT / IoT Detection & Response
- Specific Cloud threats

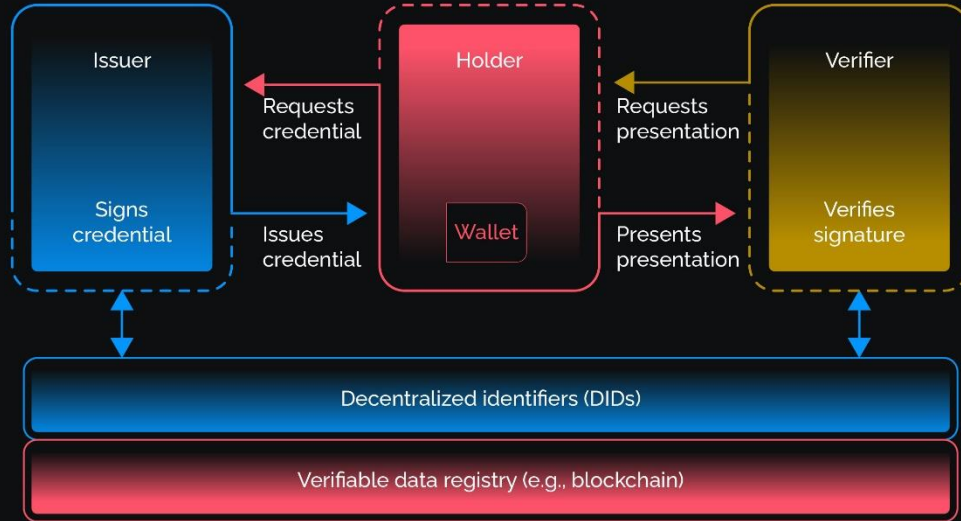
Make it smart

- Extend AI algorithms for unknown attacks
- Threats prediction & Vulnerabilities assessments and response
- Frugal AI for Cybersecurity



Zoom on use case 1

Self-Sovereign Identities



With adequate governance in place, people will be able to manage their own personal and/or sensitive data with self-sovereign digital identities.

Zoom on use case 2

Sovereign Managed Detection and Response

Technology: Client data remains in a same geography to ensure greater control over the data collected and processed on trusted servers.

MDR in action: Monitor solution to detect events against sovereignty

Experts within the geography



Alsaac

AI based MDR platform
reduces time to detect and
time to respond

Running on



BullSequana

Secured by design
Supercomputer
designed, manufactured
and located in Europe

Atos sovereign MDR conforms to data sovereignty principles by country, and to organization's unique data and operational needs.

- Manage vulnerabilities and risks
- Maintain compliance
- Enhance end-to-end security posture
- With complete, hands-free MDR services.

04. Major expected benefits



Major expected benefits (generic, includes security)

« Shape Europe's post-coronavirus future » (Ursula von der Leyen European Commission President)

For EU

Foster EU technology innovation, deployment and usage

For industrials

Accelerate roadmaps, explore disruptive technos, enhance partnerships

For customers

Promote use cases, early adoption, influence choices, competitive advantage

For SMEs

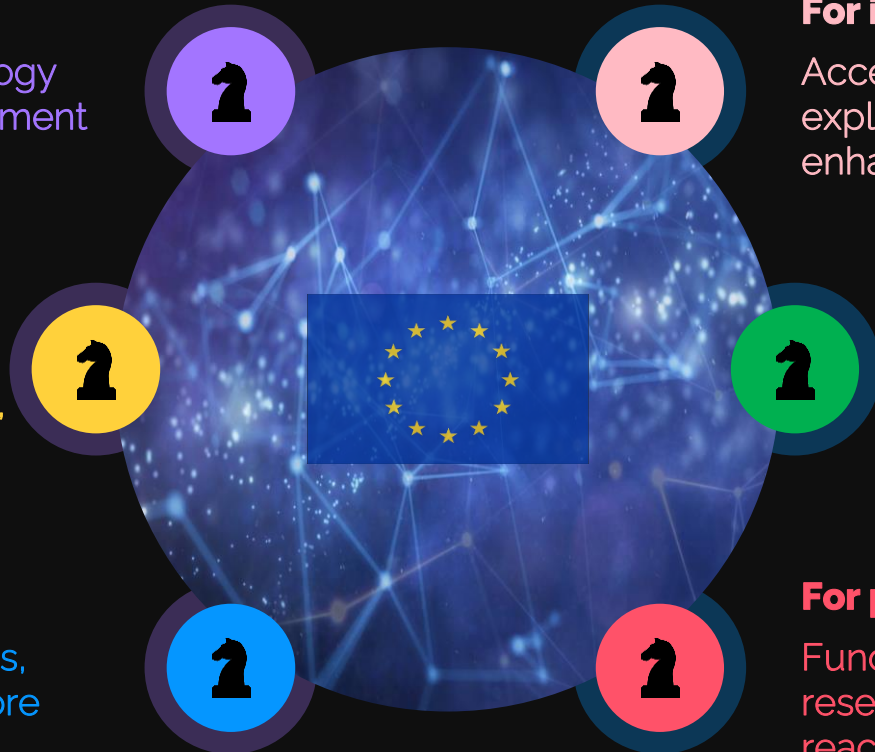
Increase visibility, test technology, fund growth

For employees

International projects, develop skills, explore innovative topics

For public institutions

Fund research, align research on market needs, reach test beds



Questions



Thank you!



Vasco GOMES

Cybersecurity Products CTO
Cybersecurity Distinguished Expert | Scientific Community member

M +33 633 867 565

vasco.gomes@atos.net  

Atos, the Atos logo, Atos|Syntel are registered trademarks of the Atos group.
June 2021. © 2021 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

Follow Atos:
atos.net



© Atos



Atos