HORIZON EUROPE
CIVIL SECURITY FOR SOCIETY

DESTINATION
INCREASED CYBERSECURITY

EU INFO DAY
28 June 2022

European Commission

Cybersecurity in Horizon Europe 2021-2022

Resilient digital infrastructures and interconnected systems

- Dynamic business continuity and recovery methodologies
- Monitoring of threats and intrusion detection

Hardware, software and supply chain security

- Improved security in open-source and open-specification hardware for connected devices
- Trustworthy methodologies, tools and data security for dynamic testing

Cybersecurity and disruptive technologies

- AI for cybersecurity reinforcement
- Transition towards Quantum-Resistant Cryptography

Smart and quantifiable security assurance & certification across Europe

- Agile certification of ICT products, ICT services and ICT processes

Human-centric security, privacy and ethics

- Technologies for cross-border federated computation in Europe involving personal data

Expected impact of the Cybersecurity Actions (1/2)

4. Destination – Increased Cybersecurity

“*Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States’ capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.*” (Strategic Plan 2021-2024)

Expected impact of the Cybersecurity Actions (2/2)

Proposals should contribute to the achievement of one or more of the following impacts:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and a common cyber security management and culture

Cybersecurity Topics in 2022

Resilient digital infrastructures and interconnected systems

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

Hardware, software and supply chain security

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components

Cybersecurity and disruptive technologies

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography

Smart and quantifiable security assurance and certification shared across Europe

HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

HORIZON-CL3-2022-CS-01-01
Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

European Commission

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures (1/4)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Improved disruption preparedness and resilience of digital infrastructure in Europe
- Improved capacity building in digital infrastructure security including organisational and operational capabilities
- Robust evidence used in cybersecurity decisions and tools
- Better prediction of cybersecurity threats and related risks
- Improved response capabilities based on effective collaboration and/or coordination with other relevant national or EU bodies in charge of Cybersecurity, including holistic incident reporting and enabling coordinated cyber-incident response

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures (2/4)

Scope

- State of the art technologies should support the logging, categorisation, data aggregation from different sources, automatic information extraction and analysis of cybersecurity incidents.
- Advanced methods for cyber threats intelligence and cyber-incident forensics enabling better prediction of cyber security threats.
- Develop and validate demonstration prototypes of tools and technologies to monitor and analyse cybersecurity incidents in an operational environment in line with the NIS directive and the GDPR.
- Contribute to improved penetration testing methods and their automation by using machine learning and other AI technologies.
- Support effective network traffic analysis applying detection techniques in network operations based on advanced security information management and threat intelligence.

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures (3/4)

Scope

- Include validation or piloting of cyber threat intelligence with early-stage detection, prediction and contributions towards response capability using predictive analytics.
- Validate the approach to intrusion detection and incident monitoring with real end-users and their needs.
- For expanding the proposed work in terms of additional pilot sites, additional user groups additional applications → Financial Support to Third Parties (aka Cascading Grants)
  - Typically in the order of EUR 50 000 to 300 000 per party. Up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties
- Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side. Participation of SMEs is strongly encouraged.

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures (4/4)

Expected EU contribution per project:	EUR 4 – 6 MEUR
Indicative topic budget:	EUR 21 MEUR
Type of Action:	IA (Innovation Action)
Technology Readiness Level:	TRL 7 (by the end of the project)

HORIZON-CL3-2022-CS-01-02
Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components (1/5)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Effective access control to system components and management of trustworthy updates
- Modelling of security and privacy properties and frameworks for validating and integration on the testing process
- Integrated process for testing, formal verification, validation and consideration of certification aspects
- Tools providing assurance that third-party and open source components are free from vulnerabilities, weaknesses and/or malware
- Data security “by design” e.g. via secure crypto building blocks

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components (2/5)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Instrumentation and secured communication with system components for dynamic testing
- Methods and environments for secured coding by-design and by-default and secure hardware and software construction
- Effective audit procedures for cybersecurity testing
- Methods or procedures to make supply chains secure

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components (3/5)

Scope

- Trustworthy methodologies and tools for advanced analysis and verification, and dynamic testing of potentially vulnerable, insecure hardware and software components
  - Focus on software development tools, IT security metric and guidelines for secure products and services throughout their lifetime
- Integration of runtime methods for monitoring and enforcement as well as design-time methods for static analysis and programme synthesis.
- Develop hybrid, agile and high-assurance tools capable of automating evaluation processes, accountability tools for audit results and updates and lightweight, isolated virtualisation environments capable of securely inspecting and orchestrating appliances in heterogeneous hardware and software architecture
- Supply chain issues, including integration of software and hardware, should be considered appropriately.

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components (4/5)

Scope

- KPIs, metrics, procedures and tools for dynamic certification of implementation security and scalable security, from chip-level to software-level and service-level, should be developed.
- The participation of SMEs is strongly encouraged

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components (5/5)

● Expected EU contribution per project:	EUR 3 – 5 MEUR
● Indicative topic budget:	EUR 17,30 MEUR
● Type of Action:	RIA (Research and Innovation Action)
● Technology Readiness Level:	TRL 4 (by the end of the project)

HORIZON-CL3-2022-CS-01-03
Transition towards Quantum-Resistant Cryptography

European Commission

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography (1/4)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Measuring, assessing and standardizing/certifying future-proof cryptography
- Addressing gaps between the theoretical possibilities offered by quantum resistant cryptography and its practical implementations
- Quantum resistant cryptographic primitives and protocols encompassed in security solutions
- Solutions and methods that could be used to migrate from current cryptography towards future-proof cryptography
- Preparedness for secure information exchange and processing in the advent of large-scale quantum attacks

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography (2/4)

Scope

- Applicants should propose approaches to tackle the challenges, and seize the opportunities that quantum technologies will bring. Preparations are needed today in order to widely implement the relevant mitigations in the future.
- Applicants should demonstrate innovative ways to design, build, and deploy the new quantum-resistant infrastructures (including relevant hardware, software and IT processes)
  - Including switching from nowadays infrastructures to the proposed new ones with practical migration paths.
- Applicants should look at the implementation of quantum-resistant algorithms on software as well as specific hardware, such as. resource constrained IoT devices, smart cards, high-speed field-programmable gate arrays.
- Proposals should devise, develop and validate metrics, methodologies, conformity assessment tests and tools for assessing and quantifying the security and the privacy of the proposed systems and services.

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography (3/4)

Scope

- Proposals may analyse how to develop combined quantum-classical 108 cryptographic solutions in Europe, for those use cases where these hybrid solutions might bring gains to the overall security. To this end, the analysis should take into account relevant actions in quantum cryptography (e.g. H2020 OpenQKD project, EuroQCI)
- Proposals should validate their concept by exercising and deploying pilot demonstrators in relevant use cases.
- For expanding the proposed work in terms of including additional quantum-resistant infrastructures, additional pilot sites, additional countries and users → Financial Support to Third Parties (aka Cascading Grants)
  - Typically in the order of EUR 50 000 to 300 000 per party. Up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography (4/4)

● Expected EU contribution per project:	EUR 3,50 – 6 MEUR
● Indicative topic budget:	EUR 11 MEUR
● Type of Action:	IA (Innovation Action)
● Technology Readiness Level:	TRL 6 (by the end of the project)

HORIZON-CL3-2022-CS-01-04
Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

European Commission

HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes (1/4)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Availability of applicable tools and procedures for partial and continuous assessment and lean re-certification of ICT products, ICT services and ICT processes.
- Reduction of time and efforts spent for (re-) certifying ICT products, ICT services and ICT processes.
- Improved stakeholder collaboration on cybersecurity certification information, including manufacturers and end users from different Member States.
- Efficient (re-)use of information and evidence relevant to certification and in support of multi-scheme (re-)use.
- Integration of certification on the whole system modelling, verification, testing and verification process

HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes (2/4)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Increased comparability of assurance statements arising from certification schemes and the standards used therein; avoidance of multi-certification.
- Advancing test and simulation facilities, including incident and threat analysis.
- Increased Digital Twin capabilities for continuous assessment and integration of new solutions.

HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes (3/4)

Scope

- Harmonising, packaging and distributing of certification processes for contemporary ICT products, services, and processes but to new and disruptive technologies as well, such as AI and High Performance Computing.
- To support cybersecurity autonomy of the EU, approaches concerning a dynamic, real time, collaborative vulnerability testing and information sharing should be developed and build on existing resources (including the work carried out in preparation of the EU cybersecurity certification framework, as established by the EU Cybersecurity Act).
- The resources may range from tools, procedures, practices, and information sources, such as checklists, flaw repositories deployment and configuration guidance, and impact assessments posted by European industries, manufacturers, developers, CSIRTs, ISACs (Information Sharing and Analysis Centres), or national and international authorities (e.g. NIST, JVN) and relevant standards.
- The actions should aim at improving certification processes, tools, evidence presentation and assurance statements, at least in quantifiable terms.

HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes (4/4)

● Expected EU contribution per project:	EUR 3 – 5 MEUR
● Indicative topic budget:	EUR 18 MEUR
● Type of Action:	IA (Innovation Action)
● Technology Readiness Level:	TRL 7 (by the end of the project)

Overview & Timing

- Submission Deadline: **16/11/2022** for the 2022 topics in Cybersecurity
- Successful proposals to be notified: March 2023 (tentatively)
- Indicative Time to Grant Signature: 8 months (July 2023)

TOPIC	Title	Type of Action	Open Date	Deadline	Budget	Recommended budget per proposal
HORIZON-CL3-2022-CS-01-01	Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures	RIA	30/06/2022	16/11/2022	21 MEUR	4 – 6 MEUR
HORIZON-CL3-2022-CS-01-02	Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components	RIA	30/06/2022	16/11/2022	17,3 MEUR	3 – 5 MEUR
HORIZON-CL3-2022-CS-01-03	Transition towards Quantum-Resistant Cryptography	RIA	30/06/2022	16/11/2022	11 MEUR	3,5 – 6 MEUR
HORIZON-CL3-2022-CS-01-04	Smart and quantifiable security assurance and certification shared across Europe	RIA	30/06/2022	16/11/2022	18 MEUR	3 – 5 MEUR

For more information:

[HE Programme 2021/22 - 6. Civil Security for Society]

[General Annexes of the WP]
[Standard application form (RIAs/IAs)]

[Participant Portal]

For questions contact

us: CNECT-H1-EVALUATIONS@ec.europa.eu

European Commission

European
Commission

Thank you!

# HorizonEU

http://ec.europa.eu/horizon-europe

European
Commission