Evaluation of Proposals Process

EC3 Cyber Innovation Forum

Admission to the event

All submitted proposals reviewed and assessed by a panel composed of Europol staff, taking into consideration the following criteria:

- Alignment of the proposal with the topics referenced in the Call-for-Proposals (Annex I);
- Innovative nature of the new concept, technique, approach, tool, report, service, solution;
- Suitability of the proposal to the needs of European Law Enforcement Agencies as users of technology with a strong interest in compliance;
- Maturity level of the proposed solution;
- Non promotional intend or commercial nature.

The proposal must include information of the submitting organisation and/or person(s).

Each member of the Panel signs a declaration of absence of conflict of interest and of confidentiality.

The panel evaluates and scores each proposal individually against every criterion. A first shortlist of proposals will be drawn and preselected organisations or persons who pass the minimum admissible score (of 50% per criterion) might be invited to participate in interviews, allowing for a more in-depth discussion of their proposals and giving the Panel an opportunity to address any questions or clarifications. A final total score will be given after the interviews to the entities that are eventually selected.

By the end of the process, Europol will communicate the outcome of the evaluation to the relevant entities. Europol reserves the right to only contact the organisations or persons of selected proposals who will be invited to present their work at the EC3 Cyber Innovation Forum 2026.

Europol's intention is to invite up to 20 entities which have received the highest total scores to participate at the second edition of the EC3 Cyber Innovation Forum 2026.

Selected organisations or persons will need to confirm participation by the date mentioned in the relevant communication message. In the absence of confirmation, Europol may invite the next organisation or person in line on the admission list.

Organisations and persons may request additional information about the non-admission of their proposal. Upon request to O3-22@europol.europa.eu, Europol may provide further clarifications about the non-admission of their proposal.

The admission of a proposal and a presentation at the EC3 Cyber Innovation Forum 2026 shall not be understood as an endorsement by Europol of the participating organisations or persons or their products/services. Participation also does not indicate that Europol intends to purchase the products or services of any selected entity.

Award

The selected proposals presented during the Cyber Innovation Forum 2026 will undergo an additional evaluation with scoring done by a jury composed by Europol staff and the audience of the forum, with the purpose of selecting the best proposal of the CIF2026.

All presented proposals are scored by the jury, taking into consideration the following criteria:

- Innovative nature of the tool, report, service, solution;
- Suitability of the proposal to the needs of European Law Enforcement Agencies as users of technology with a strong interest in compliance;
- Maturity level of the proposed solution.

Each Europol staff, who is a member of the jury signs a declaration of absence of conflict of interest and of confidentiality.

The jury evaluates and scores each proposal individually against the criteria with a single scoring. The proposal with the highest scoring will be presented with a Certificate of Best Proposal/Achievement and/or award.

Annex I

The following list is non-exhaustive. Original and impactful ideas that support law enforcement in addressing cybercrime are welcomed:

- AI (ML, Automation, Robotics, Tool development and testing, etc.)
- Quantum computing, PQC, QKD, etc.
- Mobile communications: 5G, 6G, Satellite communications etc.
- Standardisation of technologies
- Extended reality (AR/VR/Digital twins)
- IoT, intelligent assistants and smart policing
- De-anonymisation techniques
- Penetration testing, ethical hacking and cyber incident response
- Vulnerability management and frameworks
- Digital forensics
- UAV
- Legal challenges (legislative, regulatory and compliance standards and/or tools that facilitate the use of innovative techniques)
- Capacity building and cybercrime prevention
- Biometrics: face recognition, ETCT, etc.
- Malware analysis, steganography, etc.