

Joint Cyber Unit

The Joint Cyber Unit is a new platform that aims to strengthen cooperation among EU Institutions, Agencies, Bodies and the authorities in the Member States.



The EU cybersecurity eco-system does not yet have a common space to work together across different communities and fields which allow the existing networks to tap their full potential.

The EU Cybersecurity Strategy outlined the need for a Joint Cyber Unit (JCU), identifying the main problems that it would contribute to solve, its objectives and the steps needed to achieve it.

It builds on the work started with the Recommendation on a coordinated response to incidents and crises - so called Blueprint in 2017. The JCU will be set close to the Brussels offices of ENISA, the EU Agency for Cybersecurity, and CERT-EU, the Computer Emergency Response Team for the EU Institutions, bodies and agencies.

The JCU will help civilian, law-enforcement, diplomatic and cyber defence communities cooperate to prevent, deter and respond to cyberattacks. In this way, it will benefit from the expertise of all relevant actors in the cybersecurity field. Those involved will be able to act swiftly against cyber threats and work to mobilise resources for mutual assistance.

The Commission has proposed to build the JCU through a gradual and transparent process **in 4 steps**:

1. assess the organisational aspects and identify EU operational capabilities **by 31 December 2021**;
2. prepare national incident and crisis response plans and roll out joint preparedness activities **by 30 June 2022**;
3. operationalise the JCU by mobilising EU Rapid Reaction teams, following procedures defined in the EU incident and crisis response plan **by 31 December 2022**;
4. involve private sector partners, users and providers of cybersecurity solutions and services, to

increase information sharing and to be able to escalate EU coordinated response to cyber threats **by June 2023**.

Key actions of the JCU include:

- setting up a physical platform built around ENISA and CERT-EU adjacent offices in Brussels;
- establishing a virtual platform composed of tools for secure and rapid information-sharing;
- delivering the EU cybersecurity incident and crisis response plan (based on national plans proposed in NIS2);
- producing integrated EU cybersecurity situation reports, including information and intelligence about threats and incidents;
- establishing and mobilising EU Cybersecurity Rapid Reaction Teams;
- concluding memoranda of understanding for cooperation and mutual assistance;
- concluding information-sharing as well as operational cooperation agreements with private sector companies, both user and providers of cybersecurity solutions and services;
- putting together an inventory of operational and technical capabilities available in the EU;
- defining structured synergies with enhanced detection capabilities tools, notably SOCs;
- setting a multi-annual plan to coordinate exercises and organizing joint exercise and training;
- reporting: Interim report assessing roles and responsibilities of participants and final activity report.

These webpages will keep you updated on this gradual process.

Recommendation: Joint Cyber Unit

Factsheet: Join Cyber Unit

Infographic: EU cybersecurity ecosystem

Follow the latest progress and learn more about getting involved.

Follow the Commission's work on cybersecurity @CyberSec_EU

Latest News

PRESS RELEASE | 15 September 2022
New EU cybersecurity rules ensure more secure hardware and software products

The Commission presented yesterday a proposal for a new Cyber Resilience Act to protect consumers and businesses from products with inadequate security features.

NEWS ARTICLE | 26 August 2022
Flash information on call results

These are the results of the evaluations conducted in the second quarter of 2022 for three calls managed by DG Connect.

NEWS ARTICLE | 30 June 2022

Boosting Germany's cybersecurity capabilities to the next level

The German Agency for Innovation in Cybersecurity (Cyberagentur) is inviting interested suppliers to submit offers to its new pre-commercial procurement. Objective is to push innovations in the field of operational cybersecurity in order to prepare the authorities in the field of internal and external security in Germany for future threats in the digital space. Deadline for submission of offers: 23 August 2022

DIGIBYTE | 20 June 2022

Team Europe - Winners of the 1st International Cybersecurity Challenge

ENISA, the EU agency for Cybersecurity, has organized for the first time an International Cybersecurity Challenge (ICC) for young cyber players.

[Browse Cybersecurity](#)

Related Content

Big Picture

The Cybersecurity Strategy

The EU Cybersecurity Strategy aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies.

Source URL: <https://digital-strategy.ec.europa.eu/policies/joint-cyber-unit>