



## EU CYBER SOLIDARITY ACT

18 April 2023 #DigitalEU #Cybersecurity

The Commission proposed a **regulation on the EU Cyber Solidarity Act** to reinforce the EU's solidarity and coordinated actions to detect, prepare and effectively respond to growing cybersecurity threats and incidents.

The **Cyber Solidarity Act**, funded by €1.1 billion (of which about 2/3 will come from the EU budget) introduces:



A European Cyber Shield, a pan European infrastructure of national and cross border SOCs.

The **Security Operations Centres** (SOCs), are entities that monitor and analyse insights on cyber threats. With the Cyber Shield they will be able to provide timely warnings across borders.



## A Cyber Emergency Mechanism to:



Strengthen **preparedness** by testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities.



Create an **EU Cybersecurity Reserve** with incident response services from trusted providers ready to intervene, at the request of a Member State, in case of significant and large-scale cybersecurity incidents.



Provide **financial support for mutual assistance** between Member States' national authorities.



## A Cybersecurity Incident Review Mechanism to:



Review and assess significant or large-scale incidents.



At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA should review the cybersecurity incident and response. ENISA should then deliver a report on lessons learned and recommendations.

© European Union, 2023

Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU (OJ L 330, 14.12.2011, p. 39). For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders. All images © iStock Getty Images Plus unless otherwise stated.



PRINT KK-03-23-117-EN-C PDF KK-03-23-117-EN-N ISBN 978-92-68-02632-8 ISBN 978-92-68-02633-5 doi:10.2759/614699 doi:10.2759/484609 ated 2023-04-17-1220