READY, UNITED, SECURE.
THE EU IS CYBER PREPARED.

The EU Cybersecurity Blueprint outlines a coordinated framework for managing large-scale cyber crises in Europe, uniting Member States, EU institutions, and relevant actors to detect, respond and recover together. It also establishes a multilayered structure that bridges technical, operational, and political levels. The EU is ready to manage cyber crises.
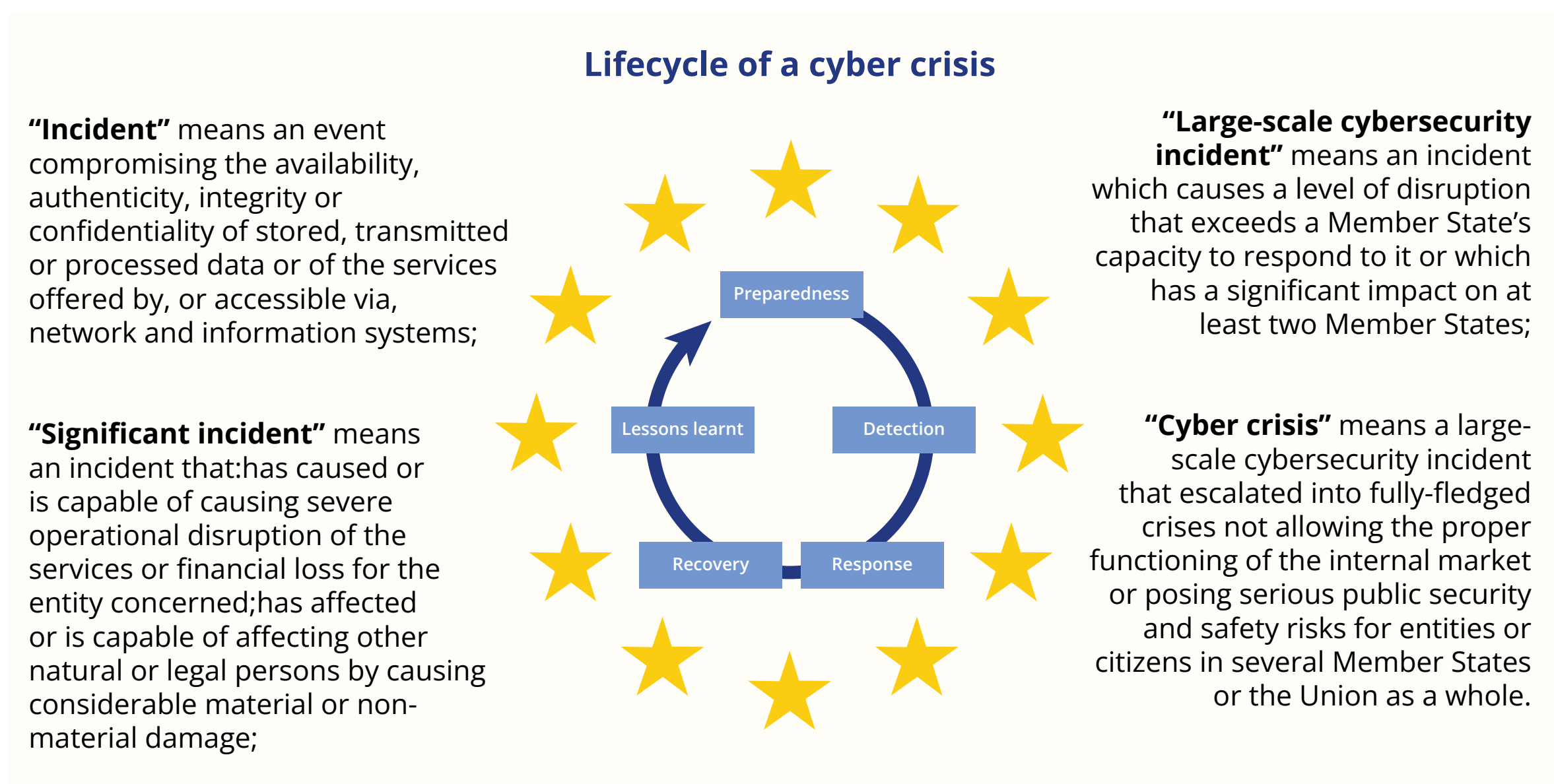

EMPOWERED BY ENISA

ENISA works to bring closer all networks and communities in order to enable an empowered and organized EU cyber crisis management ecosystem.

ENISA	CSIRTs Network	EU-CyCLONe
Streamline its **support** to the **EU-CyCLONe** and the **CSIRTs network** with the goal to further **bolster cooperation across all networks and communities**, improve information **sharing** regarding incidents, **vulnerabilities** and **situational awareness** as a whole.	Is the main technical network to **exchange relevant information about incidents**, in particular in the scope of the revised Cyber Blueprint, in accordance with Article 15 of NIS2. It **contributes to the development of confidence and trust** and promotes swift and effective **operational cooperation** among Member States.	Works as an **intermediary** between the **technical and political level**, in particular **during** large-scale cybersecurity **incidents** and cyber crisis. It **supports the coordinated management at operational level** and ensures the regular **exchange** of relevant **information** among Member States and Union institutions, bodies, offices and agencies in accordance with Article 16 of NIS2.

BLUEPRINT STRUCTURE

The EU Cybersecurity Blueprint provides a comprehensive, coordinated approach to managing cyber crises. Its structure covers the full lifecycle of a cyber crisis:

Lifecycle of a cyber crisis

"Incident" means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

"Significant incident" means an incident that:has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage;

"Large-scale cybersecurity incident" means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States;

"Cyber crisis" means a large-scale cybersecurity incident that escalated into fully-fledged crises not allowing the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole.

LEARN MORE ABOUT CYBER CRISIS MANAGEMENT IN EU

DOWNLOAD