

## The Tasks of a CSIRT under NIS 1 and NIS 2

Art. 11(3) NIS 2 Directive	Point (2) Annex I NIS 1 Directive
(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;	(i) monitoring incidents at a national level;
(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;	(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable	(iii) responding to incidents;
(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(iv) providing dynamic risk and incident analysis and situational awareness;
(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;	
(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;	(v) participating in the CSIRTs network.
(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);	
(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).	