

WG3 - Cyber Resilience of Economy, Infrastructure and Services (CREIS)

The WG3 has evolved into “CREIS”. It will be structured as a three-level pyramid. At the bottom, there will be the Community of Verticals (CoV). In the middle will be the CISOs European Community (CEC). And at the top level will feature the CISOs Strategic Committee (CSC). In the different levels of the pyramid the Traffic Light Protocol (TLP) will be applied according to the discussions specific to that level. as the confidentiality setting by default – red for the CSC, amber for the CEC, green for the CoV.

CISOs STRATEGIC COMMITTEE – CSC

Trusted Cooperation and strategic intelligence sharing among CISOs of essential and important entities

The CSC will allow CISOs from essential and important entities (using the working of the NIS2) to have a confidential and trusted exchange of strategic intelligence among themselves and establish links with CSIRTs and law enforcement authorities. Membership is open to ECSO members’ CISOs only, and to non-ECSO members while they finalise their ECSO membership procedure.

Main objectives of the CSC:

- IOCs (Indicator of Compromise) pan-European platform
- Supply chain – Enhanced security related contractual engagements
- Strategic Threat Intelligence and Information sharing among Users & Operators.
- Platform / network to support Rapid Reactions of private operators: umbrella to support private sector in case of crisis for operational cyber resilience.
- Risk Management & Threat Information Coordination - red level
- Cooperation with the EU network of CSIRTs

Contact: Sebastijan Čutura – sebastijan.cutura@ecs-org.eu

“CISOs EUROPEAN COMMUNITY” – CEC

Policy support to CISOs and general information sharing

The CEC will allow CISOs from all companies and EU countries to exchange lessons learned and best practices, share information on operational issues, develop positions and/or link with the ISACs and the European institutions, through regular networking and meetings on specific issues. Membership is open for free to ECSO members’ CISOs, but also to non-ECSO members CISOs on an *ad personam* level although non-ECSO members’ CISOs will have limited/restricted rights and an annual participation with a limited fee.

Main objectives of the CEC:

- Interaction with EU Institutions on policy and legislative priorities (e.g. NIS 2)
- Link with EC initiatives, incl. Joint Cyber Unit for NIS 2 and NIS Coordination Group
- Networking of CISOs across sectors and countries
- Risk Management & Threat Information Coordination - amber level
- Cooperation with / development of efficient and trusted ISACs at EU level
- Other operational or policy initiatives from CISOs needs

Contact: Sebastijan Čutura – sebastijan.cutura@ecs-org.eu

COMMUNITY OF VERTICALS - CoV

Policy support and networking for the different vertical applications

The CoV is intended to be an open forum of exchange to facilitate the dialogue between Users (operators, companies, governments) and Suppliers/Providers of cybersecurity solutions to understand cyber threats and needs, envisage possible solutions, and support implementation of trusted and resilient solutions for key “verticals”. Membership is open to any representatives from ECSO members, but also to non-ECSO members that are part of a stakeholders’ list.

Main objectives of the CoV:

- Link with EC activities (e.g., certification – ECSO WG1 & legislative issues) – green level
- Users’ strategic needs for sovereign solutions
- Federate European SOCs providers and Users
- Support NIS-D implementation
- Other policy or legislative aspects stemming from the users / suppliers interaction

Contact: Nina Olesen – nina.olesen@ecs-org.eu