D3.6 "ECHO INFORMATION SHARING MODELS"

ECHO information sharing model is the result of a qualitative multiple-case study analysis made in ECHO Task 3.2. It consists of theory development by systematic reviews of academic articles, seven case studies, and cross-case conclusions, from which a set of system requirements and features were established to support a model that promotes information sharing among partners, while also meeting regulatory requirements. Moreover, the final analysis includes the requirements for information sharing within and between partners across organisational boundaries as derived from multi-sector analysis. Three of the case studies were presented as research papers at DIGILIENCE conference in October 2019.

ECHO envisages the creation of a community of a large pool of stakeholders who will engage in joint intelligence activities and reliably share information and collaborate in handling security incidents in an effective and timely manner, leveraging on the ECHO Early Warning System (E-EWS). The main goals of ECHO intelligence information sharing are: 1) trust, 2) enhanced threat understanding, 3) situational awareness, 4) knowledge maturation, 5) increased degree of protection, and 6) improved preventive functions.

ECHO's information sharing and its instantiation as the E-EWS will adopt the joint intelligence process comprising of the 6 operations (planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; evaluation and feedback) and adapt and extend - if necessary - the MISP taxonomies.

D3.6 deliverable consists of a comprehensive review of information sharing and trust models from within the cyber domain (n > 50, see Annex 2), as well as models from other domains, such as healthcare, maritime and critical infrastructure protection.

Read more about the information sharing models here:
https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D3.6-ECHO-Information-Sharing-Models-v1.0.pdf