Groupe de certification de la cybersÃ©curitÃ© des parties prenantes

Le groupe des parties prenantes pour la certification de cybersÃ©curitÃ© a Ã©tÃ© crÃ©Ã© pour fournir des conseils sur les questions stratÃ©giques relatives Ã la certification de cybersÃ©curitÃ©.

Ã propos du groupe

La mission gÃ©nÃ©rale du groupe des parties prenantes pour la certification de cybersÃ©curitÃ© (SCCG) est de soutenir et de faciliter les questions stratÃ©giques concernant le cadre europÃ©en de certification de cybersÃ©curitÃ©. Sur demande, le groupe conseillera lâENISA sur les questions gÃ©nÃ©rales et stratÃ©giques concernant les tÃ¢ches de lâENISA relatives au marchÃ©, Ã la normalisation et Ã la certification de cybersÃ©curitÃ©. Â

Le groupe assistera Ã©galement la Commission europÃ©enne dans lâÃ©laboration du programme de travail glissant de lâUnion visÃ© Ã lâarticleÂ 47 de la loi sur la cybsercuritÃ©. Il Ã©mettra un avis sur le programme de travail glissant de lâUnion et, en cas dâurgence, fournira des conseils Ã la Commission et au groupe europÃ©en de certification de cybersÃ©curitÃ© (GCEC) sur la nÃ©cessitÃ© de systÃ¨mes de certification supplÃ©mentaires qui ne figurent pas dans le programme de travail glissant de lâUnion.

ConformÃ©ment au rÃ¨glement sur la cybersÃ©curitÃ©, la Commission europÃ©enne, conjointement avec lâENISA, coprÃ©sidera les rÃ©unions du groupe des parties prenantes pour la certification de cybersÃ©curitÃ©. Lâ€ENISA assurera Ã©galement le secrÃ©tariat du groupe. En principe, le groupe devrait se rÃ©unir trois fois par an.Â

La Commission europÃ©enne met Ã disposition les ordres du jour et les procÃ¨s-verbaux des rÃ©unions.

Membres

Le SCCG est composÃ© dâ□□un maximum de 50 membres issus de diverses organisations, dont, entre autres, des Ã©tablissements universitaires, des organisations de consommateurs, des organismes dâ□□Ã©valuation de la conformitÃ©, des organisations de dÃ©veloppement de normes, des entreprises et des associations professionnelles et dâ□□autres organisations associatives actives en Europe ayant un intÃ©rÃªt dans la certification de cybersÃ©curitÃ©.

Le groupe comprend des membres nommÃ©s par les organisations europÃ©ennes de normalisation, tels que le ComitÃ© europÃ©en de normalisation (CEN- ComitÃ© europÃ©en de normalisation), le ComitÃ© europÃ©en de normalisation Ã©lectrotechnique et lâ□□Institut europÃ©en de normalisation des tÃ©lÃ©communications (ETSI- European Telecommunications Standards Institute). Le groupe est Ã©galement associÃ© Ã des organismes internationaux de normalisation tels que lâ□□Organisation internationale de normalisation (ISO), la Commission Ã©lectrotechnique internationale (CEI) et lâ□□Union internationale des tÃ©lÃ©communications (UIT), la coopÃ©ration europÃ©enne pour lâ□□accrÃ©ditation (EA) et le comitÃ© europÃ©en de la protection des donnÃ©es (EDPB).

AccÃ©der Ã la liste complÃ¨te des organisations membres (.pdf)

RÃ©unions

- PremiÃ¨re rÃ©union du groupe, le 24 juin 2020
  - Ordre du jour (.pdf)
  - Compte rendu (.pdf)
- DeuxiÃ¨me rÃ©union du groupe, le 22 septembre 2020
  - Ordre du jour (.pdf)
  - Compte rendu (.pdf)
- TroisiÃ¨me rÃ©union du groupe, le 27 novembre 2020
  - Ordre du jour (.pdf)
  - Compte rendu (.pdf)
- QuatriÃ¨me rÃ©union du groupe, le 23 avril 2021
  - Ordre du jour (.pdf)
  - Compte rendu (.pdf)
- CinquiÃ¨me rÃ©union du groupe, le 17 septembre 2021
  - Ordre du jour (.pdf)
  - Compte rendu (.pdf)
- SixiÃ¨me rÃ©union du groupe, le 19 novembre 2021
  - Ordre du jour (.pdf)

Documents SCCG

- Programme de travail glissant de lâ□□Union pour la certification decybersÃ©curitÃ©: Une vue des parties prenantes (.pdf)
- Rapport de consultation sur le projet de programme de travail glissant de lâ□□Union (.pdf)
- Liste des organisations membres du groupe des parties prenantes pour la certification de cybersÃ©curitÃ© (.pdf)
- Avis du GCCT sur le projet de programme de travail glissant de lâ□□Union (.pdf)

DerniÃ¨res nouvelles

COMMUNIQUÃ DE PRESSE | 16 janvier 2023
De nouvelles rÃ¨gles plus strictes commencent Ã sâappliquer pour la cyber-rÃ©silience et la rÃ©silience physique des entitÃ©s et rÃ©seaux critiques

Aujourdâhui, deux directives clÃ©s sur les infrastructures critiques et numÃ©riques entreront en vigueur et renforceront la rÃ©silience de lâUE face aux menaces en ligne et hors ligne, des cyberattaques Ã la criminalitÃ©, aux risques pour la santÃ© publique ou aux catastrophes naturelles.

DIGIBYTE | 16 dÃ©cembre 2022
CybersÃ©curitÃ©: LâUE tient le 8e dialogue avec les Ãtats-Unis

Les 15 et 16 dÃ©cembre 2022, lâUnion europÃ©enne et les Ãtats-Unis ont tenu le huitiÃ¨me dialogue UE-Ãtats-Unis sur le cyberespace Ã Washington DC. Cela sâest produit dans le contexte dâun environnement de cybermenace dramatiquement dÃ©tÃ©riorÃ© en raison de lâagression militaire illÃ©gale de la Russie contre lâUkraine, qui a soulignÃ© la nÃ©cessitÃ© de renforcer la coopÃ©ration et la coordination transatlantiques pour prÃ©venir les actes de cybermalveillance, les dÃ©tecter et y rÃ©agir, et a soulignÃ© la nÃ©cessitÃ© de veiller Ã ce que les infrastructures critiques soient sÃ»res et rÃ©silientes.

COMMUNIQUÃ DE PRESSE | 28 novembre 2022
DÃ©claration commune de la prÃ©sidente von der Leyen et du prÃ©sident Yoon sur le partenariat numÃ©rique UE-RÃ©publique de CorÃ©e

Nous nous fÃ©licitons du lancement aujourdâhui dâun nouveau partenariat numÃ©rique entre lâUE et la RÃ©publique de

CorÃ©e. Dans un monde de plus en plus instable, la nÃ©cessitÃ© de travailler avec des partenaires partageant des valeurs dÃ©mocratiques est plus importante que jamais pour relever les dÃ©fis communs.

COMMUNIQUÃ DE PRESSE | 24 novembre 2022
CybersÃ©curitÃ©: Lâ□□UE lance la premiÃ¨re phase de dÃ©ploiement de lâ□□infrastructure europÃ©enne des centres dâ□□opÃ©rations de sÃ©curitÃ© transfrontaliÃ¨re

La Commission, en coordination avec le Centre europÃ©en de compÃ©tences en matiÃ¨re de cybersÃ©curitÃ© (ECCC), lance un appel Ã manifestation dâ□□intÃ©rÃªt pour sÃ©lectionner, dans les Ã□tats membres, des entitÃ©s qui hÃ©bergeront et exploiteront des plateformes transfrontiÃ¨res de dÃ©tection des cybermenaces, chacune rÃ©unissant des entitÃ©s publiques pertinentes de plusieurs Ã□tats membres, ainsi que des entitÃ©s privÃ©es.

Parcourir CybersÃ©curitÃ©

Contenu associÃ©

Vue dâ□□ensemble

Politiques de cybersÃ©curitÃ©

Lâ□□Union europÃ©enne travaille sur diffÃ©rents fronts pour promouvoir la cyberrÃ©silience, prÃ©server nos communications et nos donnÃ©es et assurer la sÃ©curitÃ© de la sociÃ©tÃ© et de lâ□□Ã©conomie en ligne.

Ã□ lire Ã©galement

22 projets de cybersÃ©curitÃ© sÃ©lectionnÃ©s pour bÃ©nÃ©ficier de 10,9 millions dâ□□euros

Les opÃ©rateurs de services essentiels (OES), les autoritÃ©s nationales de certification de cybersÃ©curitÃ© (ANC) et les autoritÃ©s nationales compÃ©tentes (ANC) en matiÃ¨re de cybersÃ©curitÃ© figurent parmi les candidats sÃ©lectionnÃ©s qui recevront un financement de 11 millions dâ□□euros...

RÃ©seau et centre europÃ©en de compÃ©tences en matiÃ¨re de cybersÃ©curitÃ©

Le rÃ©seau europÃ©en de cybersÃ©curitÃ© et le Centre de compÃ©tences en cybersÃ©curitÃ© aident lâ□□UE Ã conserver et Ã dÃ©velopper les capacitÃ©s technologiques et industrielles en matiÃ¨re de cybersÃ©curitÃ©.

La loi sur la cybersÃ©curitÃ© de lâ□□UE

La loi sur la cybersÃ©curitÃ© renforce lâ□□Agence de lâ□□UE pour la cybersÃ©curitÃ© (ENISA) et Ã©tablit un cadre de certification de cybersÃ©curitÃ© pour les produits et services.

Le cadre de certification de cybersÃ©curitÃ© de lâ□□UE

Le cadre de certification de cybersÃ©curitÃ© de lâ□□UE pour les produits TIC permet la crÃ©ation de systÃ¨mes de certification europÃ©ens adaptÃ©s et fondÃ©s sur les risques.

Directive relative Ã des mesures pour un niveau commun Ã©levÃ© de cybersÃ©curitÃ© dans lâ□□ensemble de lâ□□Union (directive SRI2)

La directive SRI2 est la lÃ©gislation europÃ©enne sur la cybersÃ©curitÃ©. Il prÃ©voit des mesures juridiques visant Ã renforcer le niveau global de cybersÃ©curitÃ© dans lâ□□UE.
