13ème Congrès du CESIN à Reims du 2 au 3 décembre 2025
La cyber dans les turbulences géopolitiques

Mardi 2 décembre

8:30 - 09:30	Café d'accueil		
9:30 - 10:00	Introduction Première journée	Ouverture du 13ème congrès du CESIN	Fabrice BRU - Président du CESIN
10:00 - 10:30	Plénière 1	Keynote 1	Sylvie BERMANN - Présidente du Conseil d'Administration de l'IHEDN
10:45 - 11:15	Pause networking		
11:15 - 12:45	Ateliers 1ère occurrence (choix parmi 8)		*En groupe de 12 à 20 participants, échange autour d'un thème d'actualité de la sécurité de l'information. Ateliers coanimés par deux membres du CESIN*
12:45 – 14:15	Déjeuner		
14:15 - 15:45	Ateliers 2de occurrence		*En groupe de 12 à 20 participants, échange autour d'un thème d'actualité de la sécurité de l'information. Ateliers coanimés par deux membres du CESIN*
16:00 - 17:00	Session networking avec les partenaires du CESIN		
17:00 - 17:30	Plénière 2 Clôture 1er jour	Quand les frictions géopolitiques entrent dans le quotidien des cyber-guerriers : témoignages des champs de bataille	Haude COSTA - Directrice Intercert - Fabian COSSET (CERT Advens) et Tristan PINCEAUX (CERT Almond)
17:45 - 19:00	Départ vers les hôtels		Finalisation des supports d'atelier par les animateurs
19:30	Départ vers la soirée		
20:00	Dîner		

Mercredi 3 décembre

07:30 - 08:30	Checkout		
08:45 - 09:15	Accueil Café		
09:15 - 09:45	Plénière 3	Intervention du Directeur Général de l'ANSSI	Vincent STRUBEL - Directeur Général de l'ANSSI
10:00 - 10:30	Plénière 4	Peut-on mesurer la souveraineté numérique ?	Arno PONS - Délégué Général Digital New Deal
10:45 - 11:15	Pause networking		
11:15 - 12:45	**Restitution des ateliers**		*En groupe de 12 à 20 participants, restitution croisée par les participants des conclusions de leur atelier.*
12:45 - 14:00	Déjeuner		
14:15 - 14:45	Plénière 5	Quels impacts des soubresauts géopolitiques au niveau international ?	Pascal FORTIN - Président de Cybereco Francisco ANDRADE E SILVA - Market & Regional Policies Manager - ECSO
15:00 - 15:30	Plénière 6	Au-delà du cadre réglementaire, quelles stratégies, et initiatives européennes pour une plus grande autonomie ?	Camille BOULENGUER - Directrice de l'Observatoire Géopolitique du Numérique à l'IRIS
15:45 - 16:30	Plénière 7 de clôture	Désinformation/déstabilisation (dissymétrie)	Marc-Antoine BRILLANT - Viginum
16:30 - 17:00	Trajet Gare		
17:15	Départ TGV pour Paris		

Atelier 1	**Régionalisation des solutions et services : quel rôle pour RSSI sur ce sujet dans la tourmente géopolitique ?**	Animé par Lois Samain, Headmind (Nicolas Arpagian) et Tenacy (Julien Coulet) : Lors du FIC, le sujet de l'utilisation d'hébergement sur des stacks US commençaient à faire hésiter certains acteurs. Frémissement ou mouvement long terme ?
Atelier 2	**Le cloud de confiance 2.0 : pour quoi faire et à quelles conditions ? Comment le RSSI est impliqué dans ces choix ?**	Animé par Arnaud Martin, Memority (Gilles Casteran), Sekoia (David Bizeul) et Thalès (Nicolas Fernandez) : Les offres Bleu, S3NS, SecNumCloud arrivent, les CSP sont en train de solliciter les offreurs applicatifs pour avoir du contenu mais on entend peu l'avis des consommateurs. Les choix seront-ils régulatoires seulement ou bien y aura-t-il une vraie volonté ?
Atelier 3	**Rationalisation: plateformisation ou interopérabilité ? Quels avantages et inconvénients pour une stratégie cyber ?**	Animé par Mylène Jarossay, I-Tracing (Laurent Besset), Gatewatcher (Philippe Gilet) et Cloudflare (Thomas Garreau) : Tous les grands acteurs ont l'objectif de rationnaliser les budgets et simplifier les workflows. Les deux approches plateformisation et interopérabilité permettent de répondre à cela avec chacun des argumentaires, mais quels seraient les préférences de nos RSSI ?
Atelier 4	**La CTI et les obligations de mettre à jour / d'élargir la CTI pour intégrer plus sources, plus de canaux, plus de menaces**	Animé par Vincent Lefret, Advens (B. Leroux), Crowdstrike (Mickael Le Gall) et Yes We Hack (Aimad Berady) : La CTI doit désormais dépasser sa dimension purement technique, englober toutes les menaces et être un vrai apport pour différentes solutions de sécurité. Comment la faire évoluer pour couvrir désinformation et déstabilisation ? Comment intégrer efficacement toutes les sources disponibles ? Comment structurer cette collecte multi source pour un renseignement véritablement opérationnel ?

Atelier 5	**Comment la menace interne (Insider threat) évolue dans ce contexte géopolitique et comment le RSSI y fait face ?**	Animé par Frank van Caenegem , Proofpoint (Loic Guézo), PaloAltoNetworks (Eric Antibi) et Citalid (Pierre-François Chastenet). Comment choisir et surveiller les personnels sensibles dans les turbulences géopolitiques et singulièrement pour les recrues locales dans les entreprises internationales ? Risque de radicalisation
Atelier 6	**Géopolitique et Analyse de Risques**	Animé par Didier Gras, Almond (François Ehly), Kudelski (Olivier Herson) : Quand les états nation remplacent les cybercriminels ou s'associent avec eux : - Comment cela modifie vos Analyses de Risques ? - Comment concilier la protection des intérêts vitaux et la compétitivité ? - Comment cela affecte au jour le jour les décisions des RSSI ?
Atelier 7	**Guerre informationnelle : le RSSI en première ligne face à la désinformation et à la manipulation numérique**	Animé par Fabrice Bru, Sentinelone (Blandine Delaporte), Sophos (Benjamin Mercusot) : La désinformation, les fake news et les deepfakes ne visent plus seulement les États, elles deviennent des armes de déstabilisation contre les entreprises. Dans ce nouvel espace de confrontation, comment les RSSI peuvent-ils anticiper, détecter et réagir face à des attaques qui manipulent l'information plutôt que le code ?
Atelier 8	**Chaînes globales sous tension : sécuriser la supply chain mondiale avant qu'elle ne vous compromette**	Animé par Olivier Stassi, HarfangLab (Anouck Teiller), Purplemet (Axel Tessier) et Cybervadis (Thibault Lapedagne) : Aujourd'hui, votre sécurité ne dépend plus uniquement de vos défenses internes. Chaque maillon de votre supply chain est une porte d'entrée potentielle pour les cyberattaques les plus sophistiquées. Comment passer d'une posture réactive à une stratégie proactive? Comment évaluer les risques fournisseurs ? Quels outils pour monitorer en continu votre écosystème tiers ? Comment intégrer la sécurité de la supply chain dans votre gouvernance cyber globale?