14ème Congrès du CESIN à Reims du 1 au 2 décembre 2026
Thème : Au-delà de la cyber : infrastructures, IA, conflits, confiance - les nouvelles frontières de la sécurité

Mardi 1 décembre

8:30 - 09:30	Café d'accueil		
9:30 - 10:00	Introduction Première journée	Ouverture du 14ème congrès du CESIN	Fabrice BRU - Président du CESIN
10:00 - 10:30	Plénière 1	Les nouvelles frontières de la sécurité	Jean-Philippe Lecouffe, Directeur exécutif adjoint, Europol
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 - 15:15	Session networking avec les partenaires du CESIN		
15:30 - 17:00	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*
17:00 - 17:30	Plénière 2 Clôture 1er jour	Quand une entreprise à fait le choix de l'indépendance	François Delzant - Directeur Cybersécurité et Risques IT Groupe Crédit Agricole
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 2 décembre

07:30 - 08:30	Checkout		
08:45 - 09:15	Accueil Café		
09:15 - 09:45	Plénière 3	Guerre invisible : les répercussions des conflits sur le terrain civil	Thomas WITHINGTON Associate Fellow Royal United Services Institute Senior non resident Fellow, NATO defense college
10:00 - 10:30	Plénière 4	Les nouvelles frontières de la Cyber: IA, infra, conflits, confiance l'évolution du métier de CISO	Stéphane Lenco - CISO Group Thales
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	Intervention du Directeur Général de l'ANSSI	Vincent STRUBEL - Directeur Général de l'ANSSI à confirmer
15:00 - 15:30	Plénière 6	Cybersécurité, Trust et multi-souveraineté dans un environnement international	Mathieu FEUILLET - CISO Groupe - Dassault Système
15:45 - 16:15	Plénière 7	Innovation, confiance et résilience : se réinventer, toujours	Interview de Pierre Mignoni, manager du Rugby Club Toulon par Mélanie Benard-Crozat à confirmer
16:30 - 17:00	Trajet Gare		
17:00	Départ TGV pour Paris		

Atelier 1	**Confiance par la preuve : rendre les activités cyber auditables à l'ère de l'IA :** Tant pour les SOC boostés à l'IA, pour l'exploitation de vulns, pour les accompagnements à la gouvernance, l'IA est déjà partout et va étendre son scope. On parle toujours du Human In/On the loop, mais pour cela, il faut gérer la politique et l'auditabilité des parcours IA. Cet atelier permettrait de lister des attendus de RSSI pour les activités cyber utilisatrices d'IA	Animé par Vincent Lefret - Thibault Lapedagne (Cybervadis) - Laurent Besset (I-Tracing) - Arnaud Gaugé (Cloudflare)
Atelier 2	**IA offensive vs IA défensive : qui gagne en 2026 et comment le RSSI peut bouger le curseur? :** Cet atelier permettra de balayer les principales briques et activités qui participent aux angles défensives en entreprise et attaquante en externe, de cerner les actions les plus critiques pour ne pas être totalement exposé et à risque demain	Animé par Didier Gras - Anouck Teiller (Harfanglab) - Benjamin Leroux (Advens) - Philippe Gillet (Gatewatcher)
Atelier 3	**Partager ou mourir : la coopération cyber à l'épreuve du réel :** Cet atelier permettrait de décrire en quoi les composants modernes doivent s'ouvrir à MCP au risque d'être relégués sur le banc de touche par la vague agentique. Mais ce raisonnement sera aussi vrai à l'échelle des hommes pour partager leurs agents, leurs dataset au risque de ne plus être compétitifs	Animé par Frank van Caenegem - David Bizeul (Sekoia) - Sébastien Baron (Mimecast)
Atelier 4	**L'IA va tous nous remplacer ou sommes nous tous Mythos? :** De quoi a accouché Claude Mythos 9 mois après ? Comment la cyber s'est réinventée ? Modèle de sécurité, organisation des équipes et gestion des compétences, quelles leçons tirer de 2026.	Animé par Mylène Jarossay - Maxime de Jabrun (Headmind Partners) - Blandine Delaporte (SentinelOne) - Adrien Merveille (Check Point)

Atelier 5	**Confiance et coopération : quels leviers au sein de l'organisation pour renforcer le leadership du RSSI dans la gestion des risques ? :** la fonction cybersécurité joue un rôle structurant face à la menace et son évolution, sans pour autant être en position d'exécution directe sur l'ensemble des processus de gestion du risque. Elle dépend d'autres fonctions au sein de l'organisation. Cela renvoie à un enjeu central de coopération et de cadre de confiance pour maximiser les capacités des différentes fonctions à jouer leur rôle dans la durée. Le rôle de RSSI est primordial pour faire bouger l'organisation d'ou le sujet sur le leadership et ce qui peut contribuer à le renforcer.	Animé par François Bidondo - Cyril Guillet (Tenacy) - Pierre François Chastenet (Riot)
Atelier 6	**Rebâtir la confiance à l'ère du post-quantique :** comment adopter l'hybridation, stratégie de réduction de risques pendant la phase de transition, avec crypto agilité comme capacité organisationnelle et technique,	Animé par Estelle Tchigique-Boyer - Frédéric Urvoy (Thales) - François Ehly (Almond)
Atelier 7	**Les frontières s'élargissent :** Cloud, Edge, Supply Chain, Ecosystem, Agentic-AI: comment assurer la sécurité dans un contexte d'hybridation des infrastructures et de complexification des chaînes de valeurs avec de nouveaux modèles d'architectures/d'interconnexions et la gestion de l'identité parfois non humaine ?	Animé par Eric Doyen -Gilles Casteran (Memority) - Thierry Lim (Kudelski Security)
Atelier 8	**La sécurité by-design à l'air tensions géopolitiques, des contraintes réglementaires et des nouveaux modèles d'IA : Q**uels impacts sur la livraison de composants logiciels ? Comment s'adapter et garantir le MCS des environnements métiers ?	Animé par Loïs Samain - Emmanuel Orlando - Guillaume Vassault-Houlière (Yes We Hack)
Atelier 9	**La nouvelle frontière invisible :** Aujourd'hui, la donnée est devenue la première surface d'exposition des entreprises… et pourtant la moins visible. Dans un contexte de crises multiples (géopolitiques, cloud, incidents cyber majeurs) la résilience est encore largement pensée sous l'angle de l'infrastructure et de la disponibilité du SI. Or, de plus en plus souvent, l'incident n'est pas une attaque frontale : c'est une exposition silencieuse de la donnée, accumulée au fil du temps. Ces risques latents, rarement visibles et priorisés, sont immédiatement exploitables le jour où la pression monte (crise, audit, incident) et l'arrivée de l'IA générative et des agents renforce la nécessité d'agir. »	Animé par Olivier Stassi - Fabrice Bérose (Idecsi) - Benjamin Nabet (Bsecure)