

# 12ème Congrès du CESIN à Reims du 3 au 4 décembre 2024

## Gourvenance cyber et conformité unies pour le meilleur

### Mardi 3 décembre

8:30 - 09:30	Café d'accueil		
9:30 - 10:00	Introduction Première journée	<b>Ouverture du 12ème congrès du CESIN</b>	Mylène Jarossay, CISO Groupe LVMH - Présidente du CESIN
10:00 - 10:30	Plénière 1 ouverture	<b>Panorama de la réglementation cyber actuelle et à venir</b>	Intervenant à confirmer
10:45 - 11:15	Pause networking		
11:15 – 12:45	Ateliers 1ère occurrence (choix parmi 8)		<i>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</i>
12:45 – 14:15	Déjeuner		
14:15 - 15:45	Ateliers 2de occurrence		<i>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</i>
15:45 – 16:15	Plénière 2	<b>Qu'est-ce que la gouvernance cyber et comment doit-elle évoluer ?</b>	<b>Christophe Blassiau - Schneider Electric (confirmé)</b>
16:30 – 17:30	Session networking		
17:45 – 19:00	Départ vers les hôtels		Finalisation des supports d'atelier
19 :15	Départ vers la soirée		
20 :00	Dîner		

## Mercredi 4 décembre

07:30 - 08:30	Checkout		
08:45 - 09:15	Accueil Café		
09:15 - 9:45	Plénière 3 Ouverture 2ème jour	<b>JO 2024 : bilan cyber</b>	Franz Regul - Ex RSSI des JO 2024 (confirmé)
10:00 - 10:30	Plénière 4	<b>Conformité et Sécurité ne peuvent être efficaces sans une démarche risques</b>	Cédric Voisin - Doctolib (confirmé)
10:45 - 11:15	Pause networking		
11:15 - 12:45	<b>Restitution des ateliers</b>		<i>En groupe de 12 à 20 participants, restitution croisée par les participants des conclusions de leur atelier.</i>
12:45 - 14:00	Déjeuner		
14:15 – 14:45	Plénière 5	<b>Convergence gouvernance, conformité et cyber assurance</b>	Nicolas Vurpillot - Alstom Group (confirmé)
15:00 – 15:30	Plénière 6	<b>Convergence OT/IT : les impacts sur la gouvernance</b>	Sébastien Blard - Renault Group (confirmé)
15:45 – 16:30	Plénière 7 de clôture	<b>Quelle responsabilité pénale pour le RSSI ?</b>	Eric Caprioli - avocat
16:30 – 17:00	Trajet Gare		
17h:15	Départ TGV pour Paris		

Atelier 1	Comment faire face aux multiples demandes de conformité cyber dans un environnement contraint ?	Animé par François Ehly (Almond ), Nicolas Arpagian (Headmind Partner) et Arnaud Martin (Groupe Caisse ds Dépôts) : La demande de conformités est en croissance continue avec des (multi-)référentiels de plus en plus complexes. Quelle gouvernance mettre en place pour faire face à ces exigences ? Comment compenser le manque d'experts disponibles pour conduire ces travaux ? Comment optimiser le traitement de ces dossiers d'homologations ?
Atelier 2	RSSI et Cloud : Décrypter les enjeux de Conformité	Animé par David Bizeul (Sekoial), Nicolas Fernandez (Thales), Blandine Delaporte (SentinelOne) et Vincent Lefret (Coopérative U) : Les environnements Cloud présentent des défis uniques pour la conformité et la sécurité des informations. Comment assurer le respect des normes comme le RGPD et l'ISO 27001 dans des environnements Cloud souvent complexes et multi-nuages ? Quelles sont les meilleures pratiques pour protéger les données sensibles et prévenir les violations de sécurité ? Comment identifier et évaluer les risques spécifiques au Cloud, et quelles stratégies de mitigation mettre en place ? Quel rôle prendre pour le RSSI dans la gouvernance de la sécurité Cloud et comment collaborer efficacement avec les équipes IT et les fournisseurs de services Cloud (CSP) ?
Atelier 3	Gouvernance, conformité, résilience : croisement à haut risque	Animé par Jean Larroumets (Egerie) Philippe Gillet (Gatewatcher) et Hervé Dubillot (Groupe Pomona) : En empruntant l'autoroute de la conformité, nous est-il possible de disgresser pour toujours garder une longueur d'avance sans oublier les risques métiers sur le bas-côté ? Comment poursuivre sa route après l'accident ? Construisons ensemble la voie de notre cybersécurité résiliente.
Atelier 4	Comment répondre aux nouveaux enjeux de gouvernance et conformité des accès aux données ?	Animé par Fabrice Bérose (Idecsi), Raphael Marichez (Palo Alto Networks) et Olivier Stassi (CESIN) : Face à l'essor fulgurant de l'IA et à l'explosion des volumes de données, les entreprises doivent repenser leur gouvernance des accès et conformité. L'IA offre des opportunités inédites, mais complexifie la sécurisation des données, car chaque accès doit être contrôlé pour répondre aux exigences réglementaires croissantes. Comment mettre en place une gouvernance intelligente et responsable de la donnée pour protéger les informations sensibles tout en garantissant la conformité?

<b>Atelier 5</b>	<b>Évolutions réglementaires et gestion des tiers : Analyse d'impact et meilleures pratiques.</b>	Animé par Thierry Lim (Kudelski), Edouard Lacarrière (Cybervadis) et Frank Van Caenegem (Schneider Electric) : Contrôle de toute la supply chain dans un cadre réglementaire de plus en plus contraignant; Quelles équivalences entre NIS2, Règlement Machines, ISO 62443 ? Quels défis à l'avènement de l'AI dans la gestion des fournisseurs ?
<b>Atelier 6</b>	<b>Comment impliquer les directions et particulièrement les directions financières, dans la gouvernance cyber et la gestion des risques ?</b>	Animé par Frédéric Renau (I-Tracing), Julien Chamonal (Citalid), Benjamin Taieb (CrowdStrike) et Estelle Tchigique-Boyer (CNP Assurances) : Cet atelier explore les stratégies pour fournir aux directions, notamment financières, les informations nécessaires afin de prendre des décisions éclairées en matière de cybersécurité. L'objectif est d'affiner votre roadmap en mettant en perspective les risques quantifiés et les différents chantiers pour une meilleure visibilité des risques et des investissements cyber. Cela est d'autant plus vrai avec la directive NIS2, qui exige que les organes de direction évaluent les risques et prennent les mesures nécessaires pour les couvrir, sous peine de sanctions financières, voire d'interdictions temporaires d'exercer.
<b>Atelier 7</b>	<b>Comités Sécurité, opérationnels, stratégiques... Que doit-on faire évoluer en 2025 pour concilier efficacité, exhaustivité et motivation ?</b>	Animé par Benjamin Leroux (Advens), Aymeric Taddei (Intrinsec) et Fabrice Bru (Les Mousquetaires) : A l'heure où l'IA pourrait remplacer de nombreuses interactions humaines, à l'heure où les organisations sont de plus en plus complexes, à l'heure où les agendas sont de plus en plus chargés.... Faut-il revoir la comitologie propre à la filière Cyber ? Quels sont les comités pertinents pour le RSSI ? Qui doit être invité ? Comment s'organiser ?

<b>Atelier 8</b>	<b>Expositions, risques, menaces et impacts : quelles données permettent de construire et de maintenir la vision d'ensemble nécessaire aux décideurs ,</b>	<p>Animé par Claire Loffler (Vectra), Aimad Berady (YesWeHack) et Lois Samain (EDF Hydro) : Avoir des indicateurs sur son niveau d'exposition et sur les activités réelles dans son environnement est essentiel pour la gouvernance cyber. Cet atelier sera un lieu d'échange sur les problématiques et les solutions concernant la prise de conscience de l'exposition réelle d'une organisation sur Internet et les risques associés, identifiés de manière proactive. Cette première étape sera suivie d'une réflexion sur les moyens nécessaires pour identifier, mesurer et intercepter les activités parasites et malveillantes au sein de l'organisation, permettant ainsi d'évaluer les impacts métiers réels des risques résiduels non couverts par la prévention. Ces discussions mettront au centre du débat les données opérationnelles collectées sur les actifs de l'organisation et la manière dont elles peuvent être valorisées, contextualisées et utilisées pour fournir en permanence des métriques au service de la gouvernance cyber.</p>
------------------	--	---