

COMMUNIQUÉ DE PRESSE

Paris, le 19/09/2025

REMPAR25 : retour sur l'exercice de crise de grande ampleur organisé pour faire monter d'un niveau la résilience cyber de la France

Pour préparer la France à la menace cyber croissante, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le Campus Cyber national et des campus cyber régionaux, le Club de la continuité d'activité (CCA), le Club de la sécurité de l'information français (CLUSIF) et le Club des experts de la sécurité de l'information et du numérique (CESIN) ont organisé l'exercice de crise REMPAR25 ce jeudi 18 septembre 2025. Grâce à cet exercice de crise cyber de grande ampleur, entreprises et entités publiques à travers toute la France ont pu se confronter aux impacts fulgurants d'une crise d'origine cyber, autour d'un scénario unique créé pour l'occasion.

Avec plus de 5 000 participants, issus de 1 000 organisations sur tout le territoire national, dans 16 sites d'accueil, REMPAR25 a su fédérer de nombreux acteurs autour d'un exercice hors du commun, avec un scénario - extrême mais réaliste - basé sur un *blackout* numérique¹.

S'entraîner pour faire face à l'inéluctable

A l'heure où les cybermenaces sont devenues systémiques, la nouvelle *Revue nationale stratégique* et la transposition de la directive NIS2 visent à doter la France d'une résilience cyber de premier rang. L'exercice REMPAR25 s'inscrit concrètement dans cet objectif en permettant une montée en compétences rapide et massive des organisations. En effet, après REMPAR22 en décembre 2022 qui avait alors rassemblé plus de 200 participants, cette nouvelle édition s'adressait cette fois à plus de 5 000 participants issus d'entreprises et d'entités publiques de tailles, secteurs d'activité et maturité en gestion de crise divers et variés.

¹ *Blackout* numérique : interruption complète des systèmes ou services numériques, souvent due à une panne technique, une surcharge ou un incident de sécurité.

Lors de cette journée hors normes, REMP25 a pu éprouver les participants via deux modalités de jeu : l'une leur permettait de mettre en œuvre l'exercice au sein même de leur organisation, tandis que l'autre les amenait à rejoindre une cellule de crise fictive dans l'un des lieux d'accueil dans leur territoire. Dirigeants, métiers du numérique, du juridique, des ressources humaines et de la communication ont ainsi fait face ensemble aux événements prévus dans le scénario de l'exercice pensé par l'ANSSI.

Le collectif, la clé du succès

Cet exercice de grande ampleur a déjà permis de tirer certains enseignements. Plus de 5 000 joueurs ont pu se confronter à un scénario prouvant que le recours massif à un seul outil numérique génère une hyper-dépendance, tant dommageable pour les organisations qu'à l'échelle de la Nation. Cela confirme les besoins de mettre en œuvre des plans continuité au sein des organisations, qui doivent faire l'objet de réflexions en amont de la crise.

Afin de proposer cet exercice simultané, c'est tout l'écosystème territorial et cyber qui a travaillé collectivement (CSIRT territoriaux et sectoriels, campus cyber national et campus cyber régionaux, associations professionnelles et services de l'Etat). Avec succès. Ce maillage territorial, amorcé depuis plusieurs années sous l'impulsion de l'ANSSI, s'est en effet matérialisé par plus de cinquante partenaires soutiens de l'évènement. Alors que la menace n'épargne plus personne, joueurs et partenaires ont su démontrer leur capacité à aller collectivement dans la même direction pour atteindre une résilience collective.

Pour que chaque organisation puisse (re)jouer l'exercice, le kit REMP25 fera prochainement l'objet d'une publication. En parallèle, seront publiés les enseignements tirés de cette expérience, tant sur la méthode utilisée que sur le scénario adressé, ainsi que sur la capacité à faire face à ce type de crise à l'échelle nationale.

« Organiser un exercice de cette ampleur, avec 5 000 participants à travers toute la France, était un défi que nous avons collectivement relevé. La menace cyber est une réalité au quotidien. La France doit se préparer à gérer des crises d'origine cyber multiples. Toute organisation peut être amenée à gérer une crise cyber, d'où l'importance de s'entraîner pour être prêt le jour J. », souligne Vincent Strubel, directeur général de l'ANSSI.

« En hébergeant en de nombreux points de France l'exercice de crise de grande ampleur REMP25 organisé par l'ANSSI, le Campus Cyber et le réseau des Campus territoriaux partenaires montrent qu'ils sont durablement mobilisés pour faire progresser la cybersécurité dans tous les territoires. Car le moindre interstice de vulnérabilité peut être exploité pour causer des dommages majeurs le long des chaînes d'approvisionnement. Faisons-en sorte que les bons réflexes et les meilleures pratiques se diffusent encore plus vite que les malwares : partout, chez les grands donneurs d'ordre comme chez leurs fournisseurs critiques, au sein des entités européennes régulées et au-delà. Rien de tel qu'un moment d'intelligence collective comme REMP25 pour accélérer cette dynamique. @Campus Cyber : un écosystème qui bouge et qui s'ouvre », déclare Joffrey Célestin-Urbain, président du Campus Cyber.

« L'organisation de ce type d'exercice de grande ampleur constitue un temps fort pour tous, dans un esprit de partage, d'entraide et d'enrichissement mutuel. Il permet de tisser des liens pour être résilient collectivement le jour où ce type de situation se produira. », note Monique Tinas, présidente du CCA.

« En confrontant des milliers d'acteurs à un scénario extrême, REMP25 démontre que la résilience nationale repose sur l'anticipation, la coopération et la souveraineté numérique. Au-

delà de la technique, c'est la préparation collective et la coordination des décisions qui font la différence. », déclare Alain Bouillé, délégué général du CESIN.

« Participer à REMPARG illustre notre engagement : renforcer la coopération de l'ensemble de l'écosystème cyber afin d'améliorer notre résilience collective. », indique Loïc Guézo, vice-président du Clusif.

REMPARG25 en chiffres :

- **5 000 participants**, représentant **1 000 organisations** distinctes
- **16 sites d'accueil** dans toute la France et dans **8 fuseaux horaires**, des Antilles à la Polynésie en passant par toutes les régions de l'Hexagone
- Plus de **6 000 stimuli injectés**, et une pression médiatique très réaliste, pour maintenir les joueurs en condition réelle

A propos de l'ANSSI

Service du Premier ministre placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France. Elle a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

cyber.gouv.fr

A propos du Campus Cyber

Le Campus Cyber est un projet privé-public qui vise à structurer la filière cybersécurité en France. Il se concrétise au sein d'un lieu totem fédérant plus de 250 acteurs – grands groupes, PME, start-ups, services de l'État, centres de recherche, associations organismes de formation – ainsi que cinq Campus Territoriaux répartis sur le territoire.

En favorisant la coopération entre acteurs privés et publics, le Campus encourage l'innovation, renforce les synergies et facilite la mise en réseau des expertises. Il contribue à renforcer la cohésion de la communauté cyber et à créer les conditions d'une action collective, coordonnée et durable, au service de la souveraineté numérique.

<https://campuscyber.fr/>

A propos du CCA

Réseau d'échanges et de veille, le Club de la Continuité d'Activité (C.C.A) permet à ses adhérents de développer et parfaire leurs connaissances, de comparer, conforter et orienter leurs choix en matière de « Continuité d'Activité » et "Gestion de de Crise". Il est un acteur essentiel de la Continuité d'Activité et la Gestion de Crise, en France.

<https://www.linkedin.com/company/club-de-la-continuite-d'activite/?viewAsMember=true>

<https://club-continuite-activite.com/>

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation et de promotion de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique, et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber,

Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN rassemble plus de 1 200 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr

A propos du CLUSIF

Le Clusif est une association professionnelle de cybersécurité qui rassemble plus de 550 organisations. Reconnu d'utilité publique, sa mission consiste à favoriser les échanges d'idées et de retours d'expérience à travers des groupes de travail, des conférences et des publications. Il réunit tous les secteurs d'activité de l'économie autour de la cybersécurité et de la confiance numérique.

<https://clusif.fr/>

Contacts presse :

ANSSI

Roxane ROSELL - roxane.rosell@ssi.gouv.fr / presse@ssi.gouv.fr / 06 49 21 63 80

presse@ssi.gouv.fr

Campus Cyber

Perrine Aufolle – perrine@campuscyber.fr / 06 81 68 24 49

CCA

Monique TINAS - president@club-continuite-activite.com / 06 76 75 01 68

CESIN

Véronique LOQUET - vloquet@alx-communication.com / 06 68 42 79 68

CLUSIF

Juliette GIRAULT - presse@clusif.fr / 07 88 39 03 24