PROGRAMME DES TRAVAUX DE LA JOURNEE

8 heures 30 **OUVERTURE DE L'ACCUEIL** autour d'un buffet café

9 heures 00 **MOT DE BIENVENUE**

Bénédicte PILLIET, Présidente du CyberCercle

OUVERTURE DE LA JOURNEE

Denis HAMEAU, conseiller délégué de la Métropole de Dijon en charge de la smart city, On Dijon, enseignement supérieur et université, adjoint au Maire de Dijon en charge de la qualité du service public relation aux usages et innovation, représentant **François REBSAMEN**, Maire de Dijon, Président de la Métropole de Dijon

9 heures 30 **TABLE RONDE**

Quelles actions et quelle stratégie de développement pour des territoires de confiance numérique ?

Animatrice : **Bénédicte PILLIET**, présidente, CyberCercle

Denis HAMEAU, conseiller délégué de la Métropole de Dijon en charge de la smart city, On Dijon, enseignement supérieur et université, adjoint au Maire de Dijon en charge de la qualité du service public relation aux usages et innovation, conseiller régional délégué nouvelles mobilités de la Région Bourgogne-Franche-Comté
François CHARBONNIER, investisseur Confiance numérique, Banque des Territoires
Juliette KURTZMANN, directrice adjointe, Territoires Numériques Bourgogne-Franche-Comté
Véronique BRUNET, déléguée à la sécurité du numérique pour la région Bourgogne-Franche-Comté, ANSSI
Lieutenant-colonel Michel WESTRELIN, chef de bureau coordination-partenariat**,** Région Gendarmerie Bourgogne-Franche-Comté

11 heures 00 **PAUSE CAFE - NETWORKING**

11 heures 30 **KEYNOTES**

Cybermalveillance.gouv.fr : quels outils et services pour les acteurs des territoires
Alexandra KETCHEYAN, conseiller en charge des Relations Institutionnelles, Cybermalveillance.gouv.fr

L'identité numérique, une brique indispensable de sécurité et de souveraineté numériques
Dr Michel DUBOIS, adjoint au directeur de la cybersécurité, direction de la cybersécurité, Groupe La Poste

Souveraineté des données territoriales : la future réglementation européenne à travers l'exemple du secteur agricole français
François CHARBONNIER, investisseur Confiance numérique, Banque des Territoires

13 heures 00 **PAUSE DEJEUNER - NETWORKING**

14 heures 30 ATELIERS

Les ateliers durent deux heures et ont pour objectif de permettre aux participants d'échanger dans un cadre de confiance - ils sont placés sous les règles de Chatham House. Des orateurs ouvrent l'atelier par des exposés d'une douzaine de minutes chacun pour poser le cadre puis l'ensemble des participants est invité à s'exprimer, soit pour poser des questions, soit pour apporter un témoignage, un retex ou une vision du sujet. A l'issue, des points forts de ces échanges sont envoyés à l'ensemble des participants de la journée.

ATELIER 1

Quels enjeux de sécurité numérique pour les collectivités : de la sécurité numérique au quotidien à son insertion dans les projets de développement et de territoire intelligent (dématérialisation, réglementation, e-citoyen, mobilité, smart city)

Animateur : **Christian DAVIOT**, senior advisor, CyberCercle

Les collectivités sont aujourd'hui la cible de cyberattaques de plus en plus nombreuses et sont engagées dans des processus de transformation numérique et de e-administration, de projets de territoires intelligents, qui en font des cibles privilégiées pour les cyberattaquants. Enjeux de cybersécurité, réglementation, process à mettre en oeuvre, sensibilisation et formation... autant de sujets qui seront abordés au sein de cet atelier au service des élus et des agents des collectivités.

Denis HAMEAU, conseiller délégué de la Métropole de Dijon en charge de la smart city, On Dijon, enseignement supérieur et université, adjoint au Maire de Dijon en charge de la qualité du service public relation aux usages et innovation
Emmanuel PY, maître de conférences HDR, responsable du M2 « Smart City et gouvernance la donnée », membre du Centre Innovation & Droit, UFR DGSEP, Université de Bourgogne
Alain BLANC, DPO, Dijon Métropole
Mathias MURMYLO, responsable de pôle conseil assistance à maitrise d'ouvrage, innovation et inclusion numérique, Territoires Numériques Bourgogne-Franche-Comté

ATELIER 2

Les **ressources humaines** en cybersécurité : des métiers et des formations d'avenir

Animateur : **Bénédicte PILLIET**, présidente, CyberCercle – membre du conseil d'administration, Cercle des Femmes de la Cybersécurité (CEFCYS)

La filière cybersécurité souffre aujourd'hui d'un manque de ressources humaines qualifiées et formées. Près de 10 000 postes seraient à pourvoir en France… et les besoins vont encore augmenter. Quels sont aujourd'hui les métiers de la cybersécurité, les formations, et comment favoriser le développement de cette filière RH en région ?

Gaëlle PICARD, directrice des Relations extérieures, DOCAPOSTE
Diane RAMBALDINI, présidente fondatrice, Crossing Skills – présidente, ISSA France
Dr Hakima KADRI et Aurélie GANGA, membres, Cercle des Femmes de la Cybersécurité (CEFCYS)
Carine ROBLET, responsable pédagogique Pôle informatique, Centre de Formation Saint-Joseph - La Salle
Albert DIPANDA, directeur, ESIREM

ATELIER 3

Comment favoriser **l'innovation en cybersécurité**

Animateur : **Dr Michel DUBOIS**, adjoint au directeur de la cybersécurité, direction de la cybersécurité, Groupe La Poste

La cybersécurité est aujourd'hui un enjeu majeur pour l'économie et la souveraineté. Rôle des grands donneurs d'ordre, soutien des acteurs du développement local, plan de financement au niveau national, relations entre recherche fondamentale et recherche applicative, relations entre grands groupes et pmi-pmi, soutien aux start-up… autant de sujets qui seront abordés au service du développement des entreprises locales du numérique et de la cybersécurité.

François CHARBONNIER, investisseur Confiance numérique, Banque des Territoires
CCI Bourgogne-Franche-Comté

ATELIER 4

Comment sensibiliser en interne ses collaborateurs aux bonnes pratiques de la sécurité numérique

Atelier de Cybermalveillance.gouv.fr, animé par **Alexandra KETCHEYAN** et **Astrid FROIDURE**, chargée de Relations Publiques, Avant de Cliquer

80% des cyberattaques pourraient être évités grâce à la formation des collaborateurs. Elément central d'une politique vertueuse de sécurité numérique, une culture de sécurité numérique partagée doit être implémentée au sein des organisations pour faire face aux risques numériques. Quelles clefs, quels outils et quels process mettre en œuvre pour favoriser cette culture interne de sécurité numérique seront les pistes de réflexion et de travail en commun de cet atelier.

16 heures 30 **FIN DES ATELIERS**

CAFE de CLOTURE – NETWORKING

PARTENAIRES

SOUTIENS