Veille collaborative sur les thèmes « Cybersécurité-Cyberrésilience », « Intelligence Artificielle », « Traçabilité-Blockchain » - Bulletin N° 8

Bonjour,

Dans le cadre de la **dynamique d'Intelligence Economique Territoriale**, un **groupe de travail régional « Veille collaborative** » est en place.

Il est composé des **entités suivantes** : CA Normandie, CAP'TRONIC, CRMA/CMAI 1461/Pôle ATEN, CCI Normandie, CCI Seine-Estuaire, NAE, NWX, Pôle TES, avec le soutien de l'Etat et de la Région Normandie.

Ses membres ont défini une thématique prioritaire partagée de veille collaborative sur les thèmes : « Cybersécurité-Cyberrésilience », « Intelligence Artificielle » et « Traçabilité-Blockchain ».

1/ Les éléments de veille qui vous sont transmis ci-dessous portent sur (i) des cas d'usages (domaines d'applications), (ii) des événements, (iii) des solutions (produits/services), (iv) des technologies, (v) des acteurs.

Il vous revient, si vous le souhaitez, de **valoriser à votre convenance** tout ou partie du résultat de ce travail collaboratif auprès des acteurs de votre choix (aussi bien vers les entreprises régionales, en interne de votre organisme, ou autre).

Ce groupe de travail est par définition ouvert.

Il est possible pour tous ceux qui le souhaitent de le rejoindre ou de réagir aux informations transmises.

Enfin, une action de veille partagée peut aussi être engagée sur d'autres sujets.

Il suffit de faire connaître en retour votre ou vos souhaits.
Merci par avance de bien vouloir transmettre vos propositions ou remarques à l'adresse MissionSPIE@normandie.fr

2/ Par ailleurs, **les membres du groupe de travail ont souhaité réaliser une analyse fine des informations diffusées, dans les 7 Bulletins précédents, en termes de répartition thématique, de pertinence, de domaines d'applications et de tendances**.

Vous trouverez **ci-joint la synthèse de cette analyse**.

Très cordialement.

Bonne lecture !

745 avenue de l'Université - Bâtiment CRIANN
F - 76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00 - **www.nae.fr**

Cybersécurité & Cyberésilience

UN GUIDE POUR ORGANISER UN EXERCICE DE GESTION DE CRISE

#formation #cyber #ANSSI
16/10/2020 - spie@normandie.fr
Face à une menace informatique croissante et en mutation**, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber** n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations.
Demain, l'organisation responsable et génératrice de confiance sera celle qui s'attache à maîtriser le risque numérique et à faire preuve de sa capacité à **se relever d'une crise d'origine cyber**. Or, ces crises cyber ont du mal à être appréhendées du fait de leurs spécificités : technicité, impacts fulgurants, évolutivité, sortie de crise longue, *etc.* Il est pourtant essentiel de s'y préparer. Pour cela, l'organisation d'exercices de gestion de crise cyber apparaît fondamentale.
L'ANSSI vient de publier **un guide visant à accompagner, pas à pas, les organisations dans la mise en place d'un exercice de gestion de crise d'origine cyber**. Il s'adresse à toute organisation privée comme publique, petite ou grande, souhaitant s'entraîner à la gestion de crise cyber. Le guide propose une méthodologie basée sur le standard reconnu de la norme relative aux exercices (ISO 22398:2013).
Un exercice complet est proposé en fil rouge du document, dénommé RANSOM20 et développé progressivement pour illustrer chaque étape.
Pour aller plus loin 1 *(actualités de l'ANSSI – 14 octobre 2020)* ; Pour aller plus loin 2 *(le guide en téléchargement – 128 pages)*

DES FORMATIONS POUR LES TPE ET LES PME

#formation #cyber #télétravail
16/10/2020 - spie@normandie.fr
Google a lancé, en partenariat avec Cybermalveillance.gouv.fr et la Fédération du e-commerce et de la vente à distance (FEVAD) , un **programme de formations sur la cybersécurité pour les TPE et les PME françaises**, et particulièrement les **commerces de proximité et les petites entreprises de service**, afin de les aider à développer des compétences et à prendre en main des outils pour protéger leurs employés, leurs clients et leur entreprise.
Le programme comprend une **initiation générale** à la cybersécurité et 2 modules relatifs aux **enjeux spécifiques de la cybersécurité pour le commerce en ligne et le télétravail**.
Les formations ont lieu **dans les Ateliers Numériques de Google** à Nancy, Montpellier, Saint Etienne et Rennes ainsi que sur la plateforme en ligne des ateliers.
Pour aller plus loin *(accéder au communiqué de presse, site Web de la Fevad – 29 septembre 2020)*

UN PANORAMA DES METIERS POUR MIEUX STRUCTURER UN MARCHE DE L'EMPLOI CYBER EN PLEIN ESSOR

#métiers #cyber #ANSSI
9/10/2020 - spie@normandie.fr
Virulentes, massives et évolutives, les attaques informatiques menacent de plus en plus le fonctionnement des organisations, si ce n'est leur survie. A l'heure où structures publiques et privées ont de plus que jamais **besoin de spécialistes de la sécurité des systèmes d'information**, ces derniers sont pourtant difficiles à « dénicher ». Pour accompagner le développement de cette filière d'avenir, l'ANSSI vient de publier ce 9 octobre l'**édition 2020 du Panorama des métiers de la cybersécurité**, en partenariat avec le Syntec Numérique.

Même si l'intérêt pour la filière est grandissant, le secteur continue de faire face à une **pénurie de talents**. Et les profils sont d'autant plus difficiles à trouver que le champ des missions et compétences de la sécurité du numérique est vaste, complexe et hétérogène.
Pour répondre à ces besoins, le « Panorama des métiers de la cybesécurité » propose une vision claire et partagée des différents métiers du secteur afin de structurer le **marché de l'emploi cyber en plein essor** (les offres de postes sont plus nombreuses que les candidats). **Plus d'une vingtaine de métiers** de la cybersécurité y sont passés au crible. Ce document aborde également les **métiers connexes**, tel que le délégué à la protection des données (DPD), qui contribue lui aussi à la démarche globale de cybersécurité.
Pour aller plus loin *(accéder au documents, 74 pages – 9 octobre 2020)*

APPEL A FINANCEMENT POUR LES ACTEURS DE LA CYBERSECURITE EN EUROPE
#Europe #cyber #Financement
9/10/2020 - spie@normandie.fr
La **directive 2016/1148 sur la sécurité des réseaux et des systèmes d'information** (NIS), adoptée en juillet 2016, poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Pour ce faire, la directive prévoit notamment la création d'un cadre réglementaire pour **renforcer la cybersécurité des Opérateurs de services essentiels au fonctionnement de l'économie et de la société** (OSE).
Pour **accompagner la montée en maturité des acteurs concernés** par ces législations européennes en matière cyber, la Commission européenne vient de lancer un **appel à financement au titre du mécanisme de financement « CONNECTING EUROPE FACILITY ».**
Les organisations éligibles à ce financement sont les autorités nationales de certification de cybersécurite, les organismes nationaux d'accréditation, les organismes d'évaluation de la conformité ainsi que les **opérateurs de service essentiels**. Les activités financées reposent sur 4 axes :
- la **montée en compétence des organismes d'évaluation de la conformité**,
- les **échanges entre Etats membres pour partager les bonnes pratiques**,
- le **développement et l'implémentation de méthodes permettant d'améliorer les processus de certification**,
- la **création d'un écosystème cohérent en matière de gestion de risque et de partage/reporting d'information**.
La date de clôture de cet appel est fixée au 5 novembre 2020.
Pour aller plus loin 1 *(actualités de l'ANSSI)* ; Pour aller plus loin 2 *(informations sur le site Web de la Commission européenne)* ; Pour aller plus loin 3 *(Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique)*

PERENNISER L'ENTREPRISE FACE AU RISQUE CYBER OU COMMENT PASSER DE LA CYBERSECURITE A LA CYBERRESILIENCE
#résilience #cyber
9/10/2020 - spie@normandie.fr
Le constat est sans appel : **selon une étude des Nations Unies publiée en mai 2020, 60 % des PME qui subissent des cyberattaques déposent le bilan sous six mois**. Une PME sur 10, seulement, se dit apte à y faire face. Et une cyberattaque a lieu toutes les 39 secondes dans le monde.
Face à cette menace, CCI France et le département Prospective de la CCI Paris-Ile-de-France viennent de publier un document visant à alerter les TPE et les PME sur les conséquences

des cyberattaques mais aussi sur la **nécessité d'intégrer ce risque dans leur modèle économique en s'appropriant la démarche de cyberrésilience**. L'étude entend apporter des éléments utiles afin de permettre :
- l'identification pragmatique des outils de continuité et de transformation de l'activité liés à la cyberrésilience à partir des risques répertoriés ;
- la cartographie des écosystèmes de l'entreprise à prendre en compte et à intégrer dans la démarche,
- l'explicitation de la dynamique de création de valeur et de différenciation par la démarche de cyberrésilience.
Le document formule des recommandations à l'attention des chefs d'entreprises et des pouvoirs publics. L'accent est notamment mis sur l'accompagnement des TPE et PME dans l'appropriation et la mobilisation autour de la cybersécurité et de la cyberrésilience.
Pour aller plus loin *(accéder au document, 52 pages – octobre 2020)*

LA DEFENSE ET SATORY POUR LE CAMPUS CYBER FRANCE
#campus #cyber #France
25/09/2020 - spie@normandie.fr
Le **Campus Cyber France** prendra ses quartiers à La Défense, plus précisément dans les 26 000 m^2 de l'immeuble Eria. Inspiré du CyberSpark israélien, ce lieu vise à **rassembler en un même lieu toute l'expertise française en matière de cybersécurité**, qu'elle vienne du secteur privé ou du secteur public.
Dans un second temps, un autre site de taille équivalente ouvrira sur **le plateau de Satory**, à Versailles, pour pouvoir travailler sur des projets plus gourmands en espace comme la sécurité des véhicules connectés, des drones ou des chaînes de montage.
L'Etat a fait de la cybersécurité un **axe prioritaire du volet numérique de son Plan de relance**.
Un **Plan cybersécurité avec des engagements financiers forts** doit être présenté par le Président de la République d'ici à la fin du mois d'octobre.
Des satellites dans les Régions devraient être désignés dans les prochains mois. A cette fin, **un kit de création de cyber campus en région** réalisé en partenariat l'ANSSI devrait être prochainement diffusé. Il permettra d'**affiner les candidatures en termes de structuration et de gouvernance.**
Pour aller plus loin 1 *(le Figaro - 21 septembre 2020)* ; Pour aller plus loin 2 *(Le Monde Informatique - 21 septembre 2020)* ; Pour aller plus loin 3 *(accéder aux fiches mesures du Plan de relance, 296 pages 3 septembre 2020)*

OCCITANIE : LANCEMENT DE LA « FACTORY CYBERSECURITE » A L'OCCASION DES 6èmes RENCONTRES REGIONALES DE LA CYBERSECURITE
#cybersécurité #Occitanie
25/09/2020 - spie@normandie.fr
Les 6èmes « Rencontres Cybersécurité Occitanie » se tiennent ce 29 septembre *(cf. Bulletin SPIE du 26 juin dernier)*. A cette occasion, le **cluster du numérique en Occitanie** Digital 113 (plus de 400 entreprises du secteur, 17 000 emplois –*cf. Bulletin SPIE du 8 mars 2019*) lancera la « Factory Cybersécurité ». Les Factory sont des **groupes de travail thématiques** pilotés par un administrateur et des adhérents du domaine. Les groupes de travail de chaque « Factory » se réunissent régulièrement (idéalement 1 fois par mois). Ils identifient les besoins et les attentes des entreprises impliquées ou intéressées par le thème et mettent en place des **actions collectives** et des **projets collaboratifs** pour les membres (il existe notamment un **Factory dédié au « Numérique Responsable & Durable »**). Ce futur Factory Cybersécurité

s'appuiera sur le Portail régional de la Cybersécurité mis en place l'an passé *(cf. Bulletin SPIE du 14 juin 2019)*.
Pour aller plus loin 1 *(accéder à la présentation de l'événement – site Web de la Région)* ; Pour aller plus loin 2 *(accéder au site Web dédié à l'événement)* Pour aller plus loin 3 *(accéder à la présentation du Factory « Numérique Responsable & Durable »)* ; Pour aller plus loin 4 *(accéder au Portail Cybersécurité en Occitanie)*

ANTICIPER LES CYBER ATTAQUES : PASSER DE LA CYBERSECURITE A CYBERRESILIENCE
#cybersécurité #cyberrésilience #étude
24/09/2020 – renaud.kempf@normandie.cci.fr
L'étude coproduite par la CCI Paris-Île-de-France et CCI France « Pérenniser l'entreprise face au risque cyber » vise à alerter les TPE et les PME sur les conséquences des cyberattaques mais aussi sur la nécessité d'intégrer ce risque dans le modèle économique de l'entreprise. Et donc de passer de « la cybersécurité à la cyberrésilience ».
https://www.cci.fr/web/presse/actualite-fiche/-/asset_publisher/9FDf/content/etude-cybersecurite
Télécharger l'étude : https://www.cci.fr/documents/10909/183838/Etude-cybersecurite-2020_09

RGPD, SE METTRE EN CONFORMITE GRACE AUX CCI DE NORMANDIE
#RGPD #sécuritédesdonnées #DPO #entreprises
22/09/2020 - renaud.kempf@normandie.cci.fr
L'entrée en vigueur le 25 mai 2018 du Règlement Général sur la Protection des Données (RGPD) implique de nouvelles obligations pour les établissements privés et publics.
Au vu des enjeux, la CCI Normandie a élaboré une offre modulable et adaptable aux besoins des TPE-PME, permettant d'analyser le niveau de conformité des traitements et de mettre en place les actions correctives appropriées.
Contact : dpo@normandie.cci.fr

L'offre de formation JESSICA France-Captronic en distanciel sur la cybersecurité et la securisation des systèmes industriels et des objets connectes
#cybersecurite #formation #foad #industrie
22/09/2020 – gonnet@captronic.fr
CAP'TRONIC a mis en place une offre de formations à distance afin de permettre aux salariés de continuer à se former notamment en période de télétravail. Pour identifier ces formations le mot clé sur le site ci-dessous est "DEMATERIALISEE".
https://www.captronic.fr/-Formations-.html

HAUTS-DE-FRANCE : NOUVELLE ETAPE DANS LA PRE-CONFIGURATION DU CAMPUS CYBER EN METROPOLE DE LILLE
#cybersécurité #Hauts-de-France
18/09/2020 - spie@normandie.fr
La Métropole Européenne de Lille a décidé d'apporter son **soutien à une mission de préfiguration d'un futur Campus de la Cybersécurité**, porté par CITC-EuraRFID, cluster dédié à l'Internet des Objets, associé à un Centre de Ressources Technologiques et d'Expertises des technologies sans contact. Bénéficiant du **soutien de la Région, de la Métropole, de la Ville de Lille et de la French Tech Lille**, ce Campus qui pourrait être

labellisé comme **satellite du Campus Cyber France** visera à renforcer les synergies entre acteurs publics, privés et académiques, au travers de leur rassemblement au sein d'un même lieu pour favoriser le développement de l'expertise des entreprises du territoire dans le domaine de la cybersécurité. **Un questionnaire de préfiguration d'engagement vient d'être lancé à l'attention des acteurs de la région** dans le domaine de la cybersécurité. Il va permettre d'établir une 1ère base de travail sur le niveau d'engagement des futures parties prenantes du Campus, les propositions de projets communs, les différents besoins en aménagements et les différentes attentes vis à vis du Campus afin d'en assurer la coordination. L'analyse des réponses qui doivent parvenir avant le 1er octobre serviront de document préparatoire aux prochaines rencontres de la mission de préfiguration.
Parallèlement, le CITC organise un **Ideathon Cyber Campus** le 9 décembre prochain à Villeneuve-d'Ascq dans le cadre de l'IoT Week. Cet événement sera l'occasion d'un échange avec start-ups, PME et étudiants pour imaginer à quoi pourrait ressembler le futur Cyber Campus de la Métropole Européenne de Lille.
Pour aller plus loin 1 *(iTrans – 17 août 2020)* ; Pour aller plus loin 2 *(accéder au formulaire de demande de questionnaire d'engagement sur le site de l'IoT cluster)* ; Pour aller plus loin 3 *(accéder à la délibération de la Métropole Européenne de Lille – 21 juillet 2020)* ; Pour aller plus loin 4 *(inscription à l'Idéathon Cyber Campus le 9 décembre 2020 à Villeneuve-d'Ascq)*

RELANCE DE LA FILIERE AERONAUTIQUE NORMANDE : NAE POSITIONNE SES MEMBRES SUR LES FUTURS PROGRAMMES DEFENSE/SECURITE

#cybersécurité #filière aéronautique #défense #NAE
11/09/2020 - samuel.cutullic@nae.fr
Le secteur de la Défense et de la Sécurité figurait déjà comme axe prioritaire du plan d'action de NAE pour 2020-2022. L'analyse des marchés les moins impactés durant la crise Covid et cette annonce du Gouvernement confortent la volonté de NAE d'intensifier ses actions dans ces secteurs. Ainsi, la filière va déployer un plan spécifique visant d'une part à permettre à ses industriels de mieux connaître ce secteur, et d'autre part à accélérer leur montée en puissance dans le secteur de la Défense (aérienne, terrestre et navale) par un accès facilité aux commandes publiques et aux besoins des grands comptes industriels. Ce plan comporte plusieurs volets : cartographie des marchés, des acteurs et programmes, développement des opportunités au travers d'une démarche professionnalisée vers la diversification , accélération de la Recherche Technologie Innovation, en particulier via le projet européen EDIDP, l'approfondissement des dispositifs Emploi/Formation spécifiques à ce secteur **et renforcement du niveau de cybersécurité des membres**, avec des actions ciblées.
Source : Normandinamik / https://www.normandinamik.cci.fr/relance-de-la-filiere-aeronautique-normande-nae-positionne-ses-membres-sur-les-futurs-programmes-defense-securite

ATOS VA SECURISER LES COMMUNICATIONS DU STANDARD F4 DU RAFALE

#cybersécurité #filière aéronautique #défense
9/09/2020 - samuel.cutullic@nae.fr
Mis en chantier en janvier 2019, le standard F4 du Rafale de Dassault prend forme, brique après brique. Parmi les 500 entreprises qui travaillent sur le programme, aux côtés de Dassault Aviation, Atos annonce développer les systèmes permettant de sécuriser les communications de l'avion de combat.
La dimension de travail en réseau sera au cœur du Système de combat aérien du futur (*Scaf*), attendu lui pour 2026 avec un premier démonstrateur.
Source : www.asafrance.fr / https://www.asafrance.fr/item/aeronautique-atos-va-securiser-les-communications-du-standard-f4-du-rafale.html

QUAND DEUX SMARTPHONES ET UNE APPLICATION ANDROID SUFFISENT POUR HACKER LES CARTES VISA SANS CONTACT

#cybersécurité #filière aéronautique #défense
9/09/2020 - samuel.cutullic@nae.fr
Trois chercheurs de l'École polytechnique fédérale de Zurich ont découvert une faille dans les cartes de paiement sans contact Visa. Et ce en développant une application tournant sur des smartphones du commerce, sans avoir à hacker le système Android ni bénéficier de privilèges de développeurs liés à cette plateforme.
Source : L'Usine Nouvelle / Lire la suite

BATIR UNE CYBERSECURITE EFFICACE DANS LE SECTEUR INDUSTRIEL

#cybersécurité #transactions électroniques #cartes bancaires
7/09/2020 - jessica.reffuveille@pole-tes.com
La cybersécurité est importante dans tous les secteurs, mais nulle part plus que dans le secteur industriel, où la quantité considérable d'informations confidentielles détenues par les entreprises en fait des cibles extrêmement attrayantes pour les criminels.
Source : Le Journal du Net / https://www.journaldunet.com/solutions/dsi/1493749-batir-une-cybersecurite-efficace-dans-le-secteur-industriel

POUR SECURISER LES RESEAUX D'OBJETS CONNECTES, IL FAUDRA DOPER LES PASSERELLES PERIPHERIQUES

#cybersécurité #IA #menaces #IoT
7/09/2020 - jessica.reffuveille@pole-tes.com
L'augmentation de la surface d'attaque est une faible expression lorsqu'on pense aux implications pour la sécurité que représente l'adoption des objets connectés. La sécurité reposera alors sur des passerelles survitaminées, bourrées de technologies.
Source : IT Social / https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/pour-securiser-les-reseaux-dobjets-connectes-il-faudra-doper-les-passerelles-peripheriques

MIEUX ENCORE QUE DES SALARIES SENSIBILISES : DES SALARIES VIGILANTS !

#cybersécurité #comportements #sensibilisation
4/09/2020 - jessica.reffuveille@pole-tes.com
Les cybercriminels ont toujours un temps d'avance sur les entreprises. Selon Accenture, sur les 12 derniers mois, 66 % des PME ont signalé une cyberattaque, 49 % ont été victimes d'un ransomware, et 78 % d'entre elles ont payé une rançon. La faute à un manque de sensibilisation ?
Source : Chef d'entreprise / https://www.chefdentreprise.com/Thematique/digital-innovation-1074/cybersecurite-2020/Breves/Mieux-encore-que-employes-sensibilises-employes-vigilants-351901.htm

DEJA DEUX FOIS PLUS DE RANÇONGICIELS EN 2020 QU'EN 2019

#cybersécurité #ANSSI #attaque #rançongiciel #bonnes pratiques
4/09/2020 - jessica.reffuveille@pole-tes.com
Au 1er septembre, les spécialistes de l'Agence nationale de sécurité des systèmes d'information (Anssi) étaient déjà intervenus à 104 reprises contre ces attaques qui paralysent les entreprises. Leurs auteurs exigent parfois des millions d'euros de rançons.

Source : Les Echos / https://www.lesechos.fr/tech-medias/hightech/cybersecurite-deja-deux-fois-plus-de-rancongiciels-en-2020-quen-2019-1239439

UN PANORAMA DES METIERS POUR MIEUX STRUCTURER UN MARCHE DE L'EMPLOI CYBER EN PLEIN ESSOR

#cybersécurité #emplois #métiers
02/09/2020 – spie@normandie.fr

Virulentes, massives et évolutives, les attaques informatiques menacent de plus en plus le fonctionnement des organisations, si ce n'est leur survie. A l'heure où structures publiques et privées ont de plus que jamais **besoin de spécialistes de la sécurité des systèmes d'information**, ces derniers sont pourtant difficiles à « dénicher ». Pour accompagner le développement de cette filière d'avenir, l'ANSSI vient de publier ce 9 octobre l'**édition 2020 du Panorama des métiers de la cybersécurité**, en partenariat avec le Syntec Numérique. Même si l'intérêt pour la filière est grandissant, le secteur continue de faire face à une **pénurie de talents**. Et les profils sont d'autant plus difficiles à trouver que le champ des missions et compétences de la sécurité du numérique est vaste, complexe et hétérogène.

Pour répondre à ces besoins, le « Panorama des métiers de la cybersécurité » propose une vision claire et partagée des différents métiers du secteur afin de structurer le **marché de l'emploi cyber en plein essor** (les offres de postes sont plus nombreuses que les candidats). **Plus d'une vingtaine de métiers** de la cybersécurité y sont passés au crible. Ce document aborde également les **métiers connexes**, tel que le délégué à la protection des données (DPD), qui contribue lui aussi à la démarche globale de cybersécurité.

Pour aller plus loin *(accéder au document, 74 pages – 9 octobre 2020)*

APPEL A FINANCEMENT POUR LES ACTEURS DE LA CYBERSECURITE EN EUROPE

#cybersécurité #appelàfinancement #Europe
02/09/2020 – spie@normandie.fr

La **directive 2016/1148 sur la sécurité des réseaux et des systèmes d'information** (NIS), adoptée en juillet 2016, poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Pour ce faire, la directive prévoit notamment la création d'un cadre réglementaire pour **renforcer la cybersécurité des Opérateurs de services essentiels au fonctionnement de l'économie et de la société** (OSE).

Pour **accompagner la montée en maturité des acteurs concernés** par ces législations européennes en matière cyber, la Commission européenne vient de lancer un **appel à financement au titre du mécanisme de financement « CONNECTING EUROPE FACILITY ».**

Les organisations éligibles à ce financement sont les autorités nationales de certification de cybersécurité, les organismes nationaux d'accréditation, les organismes d'évaluation de la conformité ainsi que les **opérateurs de service essentiels**. Les activités financées reposent sur 4 axes :

- la **montée en compétence des organismes d'évaluation de la conformité**,
- les **échanges entre Etats membres pour partager les bonnes pratiques**,
- le **développement et l'implémentation de méthodes permettant d'améliorer les processus de certification**,
- la **création d'un écosystème cohérent en matière de gestion de risque et de partage/reporting d'information**.

La date de clôture de cet appel est fixée au 5 novembre 2020.

Pour aller plus loin 1 *(actualités de l'ANSSI)* ; Pour aller plus loin 2 *(informations sur le site Web de la Commission européenne)* ; Pour aller plus loin 3 *(Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique)*

PERENNISER L'ENTREPRISE FACE AU RISQUE CYBER OU COMMENT PASSER DE LA CYBERSECURITE A LA CYBERRESILIENCE

#cybersécurité #cyberrésilience #PME #guide
02/09/2020 – spie@normandie.fr
Le constat est sans appel : **selon une étude des Nations Unies publiée en mai 2020, 60 % des PME qui subissent des cyberattaques déposent le bilan sous six mois**. Une PME sur 10, seulement, se dit apte à y faire face. Et une cyberattaque a lieu toutes les 39 secondes dans le monde.
Face à cette menace, CCI France et le département Prospective de la CCI Paris-Ile-de-France viennent de publier un document visant à alerter les TPE et les PME sur les conséquences des cyberattaques mais aussi sur la **nécessité d'intégrer ce risque dans leur modèle économique en s'appropriant la démarche de cyberrésilience**. L'étude entend apporter des éléments utiles afin de permettre :
- l'identification pragmatique des outils de continuité et de transformation de l'activité liés à la cyberrésilience à partir des risques répertoriés ;
- la cartographie des écosystèmes de l'entreprise à prendre en compte et à intégrer dans la démarche,
- l'explicitation de la dynamique de création de valeur et de différenciation par la démarche de cyberrésilience.
Le document formule des recommandations à l'attention des chefs d'entreprises et des pouvoirs publics. L'accent est notamment mis sur l'accompagnement des TPE et PME dans l'appropriation et la mobilisation autour de la cybersécurité et de la cyberrésilience.
Pour aller plus loin *(accéder au document, 52 pages – octobre 2020)*

COMMENT LE RENSEIGNEMENT SUR LES MENACES PROFITE A LA CYBERSECURITE ? [GUIDE TELECHARGEABLE]

#cybersécurité #bonnes pratiques
09/2020 - fbuvry@pole-aten.fr
Le renseignement sur les menaces est essentiel pour aider à comprendre leurs risques externes les plus courants et les plus graves. En exploitant les sources et les flux de renseignements sur les cybermenaces, les équipes responsables de la sécurité obtiennent des informations approfondies sur des risques spécifiques, essentielles pour bien se protéger.
https://media.bitpipe.com/io_14x/io_142996/item_1715447/EZINE_security15_Comment_le_renseignement_sur_les_menaces_profite_a_la_cybersecurite.pdf

COMMENT PROTEGER LES VEHICULES CONNECTES CONTRE LES TENTATIVES DE PIRATAGE ?

16/08/2020 - samuel.cutullic@nae.fr
#cybersécurité #privacy
Les nouvelles générations de véhicules connectés ou semi-autonomes embarquent des technologies de plus en plus complexes, les rendant plus vulnérables aux tentatives de cyberattaques. La meilleure défense étant parfois l'attaque, la sécurité offensive semble s'imposer comme une approche payante auprès des principaux constructeurs mondiaux.
Source : L'Usine Nouvelle - Lire la suite

SOCIAL ENGINEERING ET CYBERATTAQUE : QUAND LE CERVEAU DEVIENT LA CIBLE
8/08/2020 - samuel.cutullic@nae.fr
#cybersécurité #véhicules connectés
Les récentes attaques ayant pris pour cibles Twitter ou encore Doctolib ont permis de mettre en lumière deux problématiques majeures. La première est la gestion des données. Trop d'employés de la firme avaient accès aux comptes des utilisateurs. Ce problème est le même pour TOUS les services en ligne : clouds ou serveurs mutualisés, données médicales (*cf.* Doctolib), sites de rencontres, Facebook…
Source : L'Usine Nouvelle - Lire la suite

POUR LA PREMIERE FOIS, L'UE SANCTIONNE DES ENTITES RUSSES, CHINOISES ET NORD-COREENNES
31/07/2020 - samuel.cutullic@nae.fr
#cybersécurité #UE #sanctions
Le Conseil de l'Union européenne a sanctionné une unité des renseignements russes, deux entreprises nord-coréenne et chinoise ainsi que six ressortissants pour leurs implications dans des attaques informatiques. Ces entités ne peuvent plus rentrer dans l'UE et subissent un gel de leurs avoirs. C'est la première fois que l'Europe prend de telles mesures dans le cadre de cyberattaques.
Source : L'Usine Digitale / Lire la suite

CYBERSECURITE ET COLLECTIVITES TERRITORIALES : DES EFFORTS MAIS PEUT MIEUX FAIRE
24/07/2020 - jessica.reffuveille@pole-tes.com
#cybersécurité #collectivités #ransomware
Un dernier rapport du Clusif consacré à la sécurité dans les collectivités territoriales souligne des lacunes dans la détection et la gestion des incidents. Seulement 35% d'entre elles recourent à du chiffrement pour sécuriser et transporter des données.
Sources : Lemondeinformatique.fr / https://www.lemondeinformatique.fr/actualites/lire-cybersecurite-et-collectivites-territoriales-des-efforts-mais-peu-mieux-faire-79825.html
Siècle digital / https://siecledigital.fr/2020/07/27/rapport-les-lacunes-des-collectivites-territoriales-en-matiere-de-cybersecurite

UN DRONE CHINOIS POPULAIRE PRESENTE DES FAIBLESSES EN MATIERE DE SECURITE
23/07/2020 - samuel.cutullic@nae.fr
#cybersécurité #drones
Des chercheurs en cybersécurité ont révélé une nouvelle vulnérabilité dans une application qui contrôle les drones grand public les plus populaires au monde, menaçant d'intensifier les tensions croissantes entre la Chine et les États-Unis.
Source : news-24.fr – Lire la suite

SENSIBILISEZ VOS SALARIES AUX RISQUES CYBER
#cybersécurité #entreprises
16/07/2020 – renaud.kempf@normandie.cci.fr

Un collaborateur averti en vaut deux, surtout avec l'explosion du télétravail. Les entreprises doivent trouver le moyen le plus efficace de toucher leurs équipes. Jusqu'à évaluer leur vigilance.
Source : Usine Nouvelle 3668-3669, 16 juillet 2020, pages 80-81 / https://www.usinenouvelle.com/editorial/trois-conseils-pour-sensibiliser-vos-salaries-aux-risques-cyber.N985069

PUBLICATION DE L'OBSERVATOIRE DES SIGNALEMENTS D'INCIDENTS DE SECURITE DES SI DE SANTE
#sécurité #santé #cyberattaque
8/07/2020 - jessica.reffuveille@pole-tes.com
L'année 2019 a été marquée par une recrudescence de cyberattaques, qui n'ont épargné aucun secteur d'activités, y compris celui de la santé. De nombreux établissements ont subi des attaques, avec parfois des conséquences importantes sur la prise en charge des patients.
Source : E-santé.gouv / https://esante.gouv.fr/actualites/publication-de-lobservatoire-des-signalements-dincidents-de-securite-des-si-de-sante

LES 4 PROFILS DE COLLABORATEURS
#cybersécurité #comportements #usages
6/07/2020 - jessica.reffuveille@pole-tes.com
Plus aucun doute sur l'importance d'être sensibilisé à la sécurité informatique, mais les entreprises doivent prendre en compte la diversité des profils, les mentalités et les usages. Qu'en est-il par exemple des comportements à risque ?
Source : ITPro.fr / https://www.itpro.fr/cybersecurite-les-4-profils-de-collaborateurs/

Intelligence Artificielle

IA AU TRAVAIL : 82% DES SALARIES DANS LE MONDE PREFERENT SE TOURNER VERS DES ROBOTS POUR PRESERVER LEUR SANTE MENTALE
Profondément marquée par la pandémie mondiale de la COVID-19, **l'année 2020 est considérée par les salariés comme la plus stressante de l'histoire**. Anxiété, fatigue, répercussions négatives sur la santé mentales mais aussi sur la vie privée, IA, robots, avenir, autant de thématiques qui sont au cœur d'une étude menée par Oracle et Workplace Intelligence (cabinet de recherche et de conseil en RH), auprès de **12 000** employés, cadres, responsables des ressources humaines et dirigeants de **11 pays**, parmi lesquels la France :
- 70% au niveau mondial affirment avoir subi davantage de stress et d'anxiété au travail cette année par rapport aux années précédentes (**71% des Français**) ; les salariés allemands semblent avoir été moins affectés puisqu'ils ne sont que 52% à se déclarer plus stressés et anxieux au travail, les salariés indiens partageant les taux les plus élevés (84%),
- 68 % des répondants préfèreraient parler de leurs problèmes de stress et d'anxiété au travail à un robot plutôt qu'à leur manager (60% en France),
- **80% sont favorables** à l'idée d'avoir un robot comme thérapeute ou conseiller. En France cette tendance est moins flagrante mais 68% y seraient tout de même favorables. C'est en Chine où cela est beaucoup plus marqué car ils sont 97% à partager ce point de vue.
- **83% des salariés** dans le monde souhaiteraient que leur entreprise mette à disposition les technologies nécessaires pour soutenir leur santé mentale (77% en France) comme l'accès en libre-service à des ressources en matière de santé (36%), des services de conseil à la demande (35%), des outils de monitoring proactif de la santé (35%), l'accès à des applications

dédiées au bien-être et à la méditation (35%) et des chatbots pour répondre aux questions de santé (28%).
Pour aller plus loin *(accéder au communiqué – 7 octobre 2020)*

AUTOMOBILE ET IA : UN CODE D'ETHIQUE POUR L'UTILISATION DE L'IA
#automobile #IA #éthique
16/10/2020 - spie@normandie.fr
Le groupe BMW a récemment joué un **rôle actif** dans le processus de consultation en cours de la Commission européenne sur l'usage de l'IA. En collaboration avec d'autres entreprises et organisations, la société BMW a activement participé à l'élaboration et au développement d'un ensemble de règles pour travailler avec l'IA. S'appuyant sur les **exigences fondamentales formulées par l'Union européenne pour une IA digne de confiance**, le groupe a élaboré **7 principes de base couvrant l'utilisation de l'IA au sein de l'entreprise** :
- **action humaine et supervision** : mise en œuvre d'une surveillance humaine appropriée des décisions prises par les applications d'IA et examen des moyens possibles par lesquels les humains peuvent annuler les décisions algorithmiques,
- **robustesse technique et sécurité** : développement des applications d'IA robustes et respect des normes de sécurité applicables conçues pour réduire le risque d'erreurs,
- **confidentialité des données** : extensions des mesures de confidentialité et de sécurité des données de pointe pour couvrir le stockage et le traitement dans les applications d'IA,
- **transparence** : explicabilité des applications d'IA et communication ouverte sur les technologies utilisées,
- **diversité, non-discrimination et équité** : respect de la dignité humaine et création d'applications d'IA équitables (comprenant la prévention de la non-conformité des applications d'IA),
- **bien-être environnemental et sociétal** : engagement à développer et à utiliser des applications d'IA qui favorisent le bien-être des clients, des employés et des partenaires,
- **responsabilité** : mise en œuvre des applications d'IA de manière à ce qu'elles fonctionnent de manière responsable.
Pour aller plus loin *(accéder au communiqué – 12 octobre 2020)*

FORMATION ET IA : UNE FORMATION OUVERTE A TOUS LES PROFILS NON TECHNIQUES
#formation #IA
16/10/2020 - spie@normandie.fr
L'essor de l'IA crée une **galaxie de nouveaux métiers** pour des profils business et métiers. Quasiment tous les compartiments métiers de l'entreprise et secteur d'activités impliquent, ou impliqueront, cette technologie et ses différents avatars. Contrairement à une croyance courante, **bon nombre de ces métiers ne requièrent aucune connaissance technique**, mais une bonne appréhension des possibilités métiers et business offertes par l'IA. Que ce soit pour résoudre un problème, optimiser un process ou créer une entreprise pour porter une idée. **L'intégration pertinente de l'IA et son acceptation est un enjeu pour l'entreprise** (et tout organisme en général). Sans cette adhésion, l'entreprise peut être à terme ralentie dans sa capacité productive d'une part, mais aussi être en difficulté concurrentielle et compétitive du fait de produits vieillissants pour l'entreprise, et in fine poser la question de l'employabilité pour les collaborateurs. **Comprendre l'IA est un enjeu de compétitivité et d'employabilité**. C'est sur cette conviction qu'a été élaborée au sein de Mines Télécoms une **formation dédiée, ouverte à tous les profils non techniques**.
Pour aller plus loin *(accéder à la présentation de la formation)*

UNE APPROCHE EUROPEENNE DE L'INTELLIGENCE ARTIFICIELLE : EIT DIGITAL FAIT PART DE SES RECOMMANDATIONS

#IA #Europe #recommandations

23/09/2020 - fbuvry@pole-aten.fr

EIT Digital a présenté son troisième rapport de sa série Policy Perspective. Il aborde la manière dont l'Europe devrait gérer l'intelligence artificielle et fournit aux décideurs économiques et politiques un instrument d'analyse d'impact basé sur des scénarios pour l'élaboration de politiques d'IA.

https://www.actuia.com/actualite/une-approche-europeenne-de-lintelligence-artificielle-eit-digital-fait-part-de-ses-recommandations/?utm_source=Actu+IA&utm_campaign=4f590b0740-newsletter_quotidienne&utm_medium=email&utm_term=0_984fe5c378-4f590b0740-152542305&mc_cid=4f590b0740&mc_eid=3be8708b10

L'OFFRE DE FORMATION JESSICA FRANCE-CAPTRONIC EN DISTANCIEL SUR L'INTELLIGENCE ARTIFICIELLE ET LE MACHINE LEARNING

#IA #machine learning #ia embarquée #formation #foad

22/09/2020 – gonnet@captronic.fr

CAP'TRONIC a mis en place une offre de formations à distance afin de permettre aux salariés de continuer à se former notamment en période de télétravail. Pour identifier ces formations le mot clé sur le site ci-dessous est "DEMATERIALISEE".

https://www.captronic.fr/-Formations-.html

POLYTECHNIQUE ET HEC CREENT UN CENTRE MONDIAL DEDIE A L'IA ET AUX DATAS

18/09/2020 - spie@normandie.fr / samuel.cutullic@nae.fr

#IA #ESR

L'**Institut Polytechnique** et **HEC Paris** ont annoncé ce 15 septembre la création d'un **centre de recherche interdisciplinaire et d'enseignement consacré à l'IA et aux sciences des données**. De niveau mondial, il interviendra dans des domaines tels que l'énergie et l'environnement, la défense et la sécurité, la santé, le retail et l'industrie du luxe, les télécoms, l'alimentation, la finance ou encore l'assurance.

Baptisé « **Hi ! Paris** », ce nouvel espace s'appuiera sur les **300 chercheurs et infrastructures** des 2 grandes écoles pour former la future génération d'ingénieurs et de managers spécialisés dans l'IA et la data science. « Hi ! Paris » a pour ambition de **recruter 30 nouveaux professeurs et 150 doctorants parmi les meilleurs au monde** et son objectif est de **doubler tous les 5 ans le nombre d'étudiants formés dans ces domaines**. Il vise à **contribuer au développement d'une souveraineté numérique de la France et de l'Europe**, en assurant la compétitivité des entreprises dans ce domaine.

D'un **budget annuel de 50 M€**, le centre bénéficie du soutien des 5 mécènes fondateurs que sont L'Oréal, Capgemini, Total, Kering et Rexel.

Pour aller plus loin 1 *(L'Usine Digitale – 16 septembre 2020)* ; Pour aller plus loin 2 *(accéder au communiqué, site Web de l'Institut Polytechnique – 15 septembre 2020)* ; Pour aller plus loin 3 *(accéder au communiqué, site Web de l'Institut Polytechnique – 15 septembre 2020)*

L'IA AIDE A PERCER LES SECRETS DE L'HYDROGENE METALLIQUE AU CŒUR DES PLANETES GEANTES

#IA #astrophysique

9/09/2020 –samuel.cutullic@nae.fr

L'hydrogène isolant devient un solide métallique conducteur à très haute pression. Cette transition de phase étonnante a été observée mais elle reste mal comprise alors qu'elle pourrait révolutionner la technologie et aider à comprendre ce qui se passe au cœur des planètes géantes largement composées d'hydrogène. L'IA aide aujourd'hui à simuler sur ordinateur le comportement de l'hydrogène métallique pour percer ses secrets.

Source : www.futura-sciences.com / Lire la suite

NEW ARTIFICIAL INTELLIGENCE SYSTEM FOR AMERICAN DRONE – ISRAELDEFENSE

#IA #drones

8/09/2020 –samuel.cutullic@nae.fr

So The Reaper MQ-9 is now equipped with an ultramodern pod that enables location and identification of targets and tracking of them using algorithms based on machine learning. The first test flight took place last week

Source : www.israeldefense.co.il / Lire la suite

ARTIFICIAL INTELLIGENCE FOR MONITORING AND CONTROL OF METAL ADDITIVE MANUFACTURING

#IA #impression additive

8/09/2020 –samuel.cutullic@nae.fr

Quality monitoring in Additive Manufacturing (AM) is currently mostly based on temperature measurements of the process zone or on layer/piecewise high-resolution surface imaging. To this aim, various sensors, such as pyrometers, photodiodes, and matrix CCD detectors, have been tested. These standard temperature measurements, however, do not provide a comprehensive description of the process dynamics, as they are just limited to surface observations.

Source : dx.doi.org / Lire la suite

EVALUATION AND DEVELOPMENT OF MODERN METHODS OF ARTIFICIAL INTELLIGENCE FOR AUTOMATIC WEED DETECTION SORGHUM USING DRONES (EWIS) (PROJECT)

#IA #agriculture #drones

02/09/2020 – florian.fougy@normandie.chambagri.fr

Sorghum serves as an energy crop and is used in Bavaria primarily for Biogas production. The high biomass output and the large variety in combination with its drought and nutrient efficiency make sorghum a promising raw material crop. Novel technologies, combined with intelligent software, open up great potential in the area of increasing efficiency in agriculture. With help of the most modern methods of machine learning (e.g. artificial neural networks / deep learning), drone-based images of the cultivated areas are to be analyzed.

https://fisaonline.de/en/findprojects/details/?tx_fisaresearch_projects%5Bp_id%5D=14416&tx_fisaresearch_projects%5Baction%5D=projectDetails&tx_fisaresearch_projects%5Bcontroller%5D=Projects&cHash=65c1ac875db7753ffe9730b4105155ed#more

DECLARATION D'INTENTION CONJOINTE FORMALISANT LES LIENS ENTRE LES RESEAUX FRANÇAIS ET ALLEMANDS EN INTELLIGENCE ARTIFICIELLE

#IA #coopération

01/09/2020 - renaud.kempf@normandie.cci.fr
La signature du Traité d'Aix-la-Chapelle le 22 janvier 2019 a marqué un tournant dans le développement de la relation entre la France et l'Allemagne. L'enseignement supérieur, la recherche et l'innovation sont au cœur de cette refondation. Parmi les projets prioritaires annexés au Traité figure la création d'un **centre virtuel franco-allemand en intelligence artificielle.**
Pour soutenir les futures initiatives bilatérales, le **lancement d'un appel à propositions conjoint est prévu pour le mois d'octobre 2020**.
Source : Frédérique VIDAL, ministre de l'Enseignement supérieur, de la Recherche et de l'Innovation
Pour aller plus loin : https://www.enseignementsup-recherche.gouv.fr/cid153650/www.enseignementsup-recherche.gouv.fr/cid153650/declaration-d-intention-conjointe-formalisant-les-liens-entre-les-reseaux-francais-et-allemands-en-intelligence-artificielle.html

REALISATION DE PIECES AERONAUTIQUES DE GRANDES DIMENSIONS PAR FABRICATION ADDITIVE WAAM
#IA #Impression additive
26/08/2020 - samuel.cutullic@nae.fr
Dans le domaine de la fabrication additive plusieurs technologies cohabitent et présentent des maturités et des applications différentes : le lit de poudre, la projection de poudre et le dépôt de fil pour ne citer que les principales. Nous avons étudié, dans le cadre de cette thèse, la réalisation de pièces de grandes dimensions du domaine aéronautique en alliage d'aluminium, par technologie WAAM (Wire Arc Additive Manufacturing) robotisée.
Source : www.semanticscholar.org / Lire la suite

COMMENT LES ENTREPRISES EUROPEENNES UTILISENT LES TECHNOLOGIES BASEES SUR L'IA ?
#IA #Europe #entreprises
29/07/2020 - jessica.reffuveille@pole-tes.com
A la demande de la Commission Européenne, l'institut IPSOS vient de réaliser une étude intéressante qui révèle que 42% des entreprises utilisent actuellement au moins une technologie d'IA, un quart d'entre elles utilisent au moins deux types et 18% prévoient d'adopter les technologies d'IA au cours des deux prochaines années.
Images & Réseaux / https://www.images-et-reseaux.com/comment-les-entreprises-europeennes-utilisent-les-technologies-basees-sur-lia/

USING ARTIFICIAL INTELLIGENCE TO SMELL THE ROSES
28/07/2020 – florian.fougy@normandie.chambagri.fr
#IA #agriculture
UC Riverside study applies machine learning to olfaction with possible vast applications in flavors and fragrances.
https://www.eurekalert.org/pub_releases/2020-07/uoc--uai072820.php

L'INTELLIGENCE ARTIFICIELLE, CERVEAU NUMERIQUE DE L'INDUSTRIE DU FUTUR
#IA #Industrie #logistique #énergie #collaboration homme-machine
13/07/2020 - jessica.reffuveille@pole-tes.com
L'utilisation de l'intelligence artificielle (IA) est encore récente. Pourtant, son potentiel dans l'industrie, mais aussi la gestion de l'énergie ou la logistique sont de plus en plus reconnus

pour une production optimisée, de meilleurs services, une diminution des coûts et des délais mais aussi une amélioration de la collaboration homme-machine (robotique collaborative ou réalité augmentée).
Filière 3E / https://www.filiere-3e.fr/2020/07/13/lintelligence-artificielle-cerveau-numerique-de-lindustrie-du-futur/

TRACTEURS, SERVICES ET INTELLIGENCE ARTIFICIELLE FONT REBONDIR KUBOTA
#IA #agriculture
16/06/2020 – florian.fougy@normandie.chambagri.fr
Comme tous les tractoristes, Kubota a subi de plein fouet la crise sanitaire depuis mars 2020. Les conséquences sont importantes économiquement. Néanmoins, la machine repart, les nouveautés sont prêtes et la R&D toujours inspirée.
https://www.entraid.com/articles/tracteurs-services-et-intelligence-artificielle-font-rebondir-kubota

Blockchain :

RENAULT S'ESSAIE A LA BLOCKCHAIN DANS SON USINE DE DOUAI, ET EMBARQUE FAURECIA, SAINT-GOBAIN, PLASTIC OMNIUM
#Blockchain #Automobile
11/09/2020 - samuel.cutullic@nae.fr
Le constructeur Renault a annoncé, jeudi 10 septembre, avoir testé une solution blockchain développée par IBM. Sa vocation : garantir la traçabilité des éléments relatifs à la conformité de ses véhicules.
L'Usine Nouvelle / Lire la suite

BY STAMP, TAMPON NUMERIQUE
#Cybersécurité #Blockchain
03/09/2020 – renaud.kempf@normandie.cci.fr
By Stamp (www.bystamp.com) Startup bretonne qui a mis au point un tampon (physique) qui permet de signer un document numérique en tamponnant son smartphone. Primé au CES Las Vegas en 2020.
Source : Usine Nouvelle 3672, 3 septembre 2020, pages 20 / https://www.usinenouvelle.com/editorial/by-stamp-tampon-numerique.N998119

BLOCKCHAINS & DEVELOPPEMENT DURABLE – LIVRE BLANC
#blockchain #développement durable
31/08/2020 - jessica.reffuveille@pole-tes.com
Le livre blanc présente 200 cas d'usages illustrant les diverses applications de blockchains qui contribuent à la réalisation des 17 Objectifs de Développement Durable (ODD) fixés en 2015 dans le cadre de « l'agenda 2030 », par 193 membres de l'ONU.
All news / https://www.allnews.ch/content/livres/blockchains-d%C3%A9veloppement-durable-%E2%80%93-livre-blanc

DU LAIT CONNECTE POUR MIEUX RASSURER
#blockchain #sécurité alimentaire #traçabilité
22/08/20 - jessica.reffuveille@pole-tes.com

Objectif traçabilité. La coopérative laitière Prospérité Fermière mise sur la blockchain pour certifier l'ensemble de sa chaîne de production et contrôler le respect de son cahier des charges
L'Usine Nouvelle / https://www.usinenouvelle.com/editorial/reportage-du-lait-connnecte-pour-mieux-rassurer.N933204

HONEYWELL GAGNE (BEAUCOUP) D'ARGENT GRACE A UNE BLOCKCHAIN
#blockchain #commerce électronique #aéronautique
13/08/20 - jessica.reffuveille@pole-tes.com
Honeywell Aerospace a créé une plate-forme de commerce électronique pour l'une des industries les plus réglementées des États-Unis – les pièces détachées et les pièces détachées pour l'aviation.
Mon Livret / http://www.mon-livret.fr/actualite/crypto/honeywell-gagne-beaucoup-dargent-grace-a-une-blockchain

LA TROISIEME GENERATION DE BLOCKCHAIN OUVRE LA VOIE A UN USAGE PAR LES ENTREPRISES
#blockchain #usage #entreprise
27/07/20 - jessica.reffuveille@pole-tes.com
La technologie blockchain a-t-elle un intérêt pour un usage en entreprise ? Philippe Ensarguet, CTO de Orange Business Services, en est convaincu. Il revient dans cette tribune sur la façon dont la nouvelle génération de blockchains permissionnées permet des scénarios de plus en plus crédibles pour le monde B2B.
L'Usine Digitale / https://www.usine-digitale.fr/article/la-troisieme-generation-de-blockchain-ouvre-la-voie-a-un-usage-par-les-entreprises.N989104

KALIMA MET LA BLOCKCHAIN AU SERVICE DE L'INTERNET DES OBJETS
#blockchain #IoT #industrie #données
16/07/20 - - jessica.reffuveille@pole-tes.com
L'entreprise a développé une technologie blockchain dédiée et adaptée à l'internet des objets industriels afin de sécuriser les échanges et de permettre la restitution de l'intégralité des données qui transitent par le système.
Source : Forbes / https://www.forbes.fr/business-inside/kalima-met-la-blockchain-au-service-de-linternet-des-objets

EVENEMENT :

AGREEN STARTUP NORMANDIE
02/09/2020 – florian.fougy@normandie.chambagri.fr
Vous avez une idée innovante pour le monde agricole ? Particpez au concours AGREEN STARTUP Normandie à Caen (14) le 1er décembre 2020
AGREEN STARTUP, c'est le concours pour les porteurs de projets nouveaux, audacieux et ambitieux, alliant innovation, technologie, agro-écologie, environnement, alimentation... au service de l'agriculture de demain. La Chambre d'agriculture de Normandie organise le concours AGREEN STARTUP afin de mettre en avant des porteurs de projets, petits ou grands, afin de les propulser au maximum dans leurs projets !

En Normandie, on innove jusqu'au bout : on fait donc une nouvelle version en 12 h ! Attention les neurones vont chauffer. Heureusement, l'ambiance sera conviviale et motivante grâce à tous les partenaires que nous avons réunis pour vous booster ! Vous serez entouré par les meilleurs experts agricoles, financiers, commerciaux, technologiques, juridiques…
Pour plus d'informations : https://agreen-startup.chambres-agriculture.fr/choisir-un-concours/agreen-startup-normandie/

Si vous disposez d'une information que vous souhaitez partager, merci par avance de la communiquer à MissionSPIE@normandie.fr

745 avenue de l'Université - Bâtiment CRIANN
F - 76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00 - **www.nae.fr**