#ANSSI10+
Synthèse de l'atelier « #TADA la magie de la donnée »

Le 22 novembre 2019 s'est tenu l'**atelier collaboratif « #Tada la magie de la donnée » pour**

- **réfléchir à l'enjeu de la valorisation des données au service des missions et des métiers de la cybersécurité ;**
- **identifier des axes de travail** et s'interroger sur le rôle de l'ANSSI à leur égard.

Organisé dans les locaux du dispositif cybermalveillance.gouv.fr et ouvert à l'extérieur, **cet atelier a réuni une cinquantaine de spécialistes de l'ANSSI et de l'écosystème du public, du privé et du monde académique.**

En guise d'inspiration :

- **Françoise Soulié, conseiller scientifique du Hub France IA,** a partagé des éléments de réflexion sur le sujet de la donnée. Selon elle, l'Intelligence Artificielle n'a « rien de magique », et pour toute structure souhaitant s'y intéresser, la priorité devrait être de construire des grandes bases / lacs de données, en partant de tous types de données disponibles, plutôt que de se concentrer sur les algorithmes d'intelligence artificielle, peu nombreux à être réellement efficaces et dont la performance encore difficile à démontrer formellement constitue un enjeu majeur pour l'avenir. Il est, par ailleurs, nécessaire de développer des standards et algorithmes pour permettre la production et le partage de données, prérequis pour la constitution de vastes bases ou lacs de données utiles au sein d'un écosystème.
- **Mathilde Hoang, Open Data Officer à Etalab**, a présenté les missions de ce service du Premier ministre, chargé de coordonner la politique de la donnée de l'Etat, en vue d'améliorer l'action publique. Lors de la création d'Etalab en 2011, la priorité était avant tout de mettre en œuvre la plus large ouverture possible des données publiques. Au cours des années, un volume conséquent de données publiques a été publié en open data. Désormais, Etalab se consacre à la production de données de qualité, à leur ouverture et circulation et à leur exploitation. L'enjeu est de proposer des données accessibles et facilement réutilisables. Ce travail se fait en collaboration avec la communauté de producteurs et de réutilisateurs de données.

1. Des orientations générales et des rôles pour l'ANSSI

Une première séquence de « projection dans le succès » (voir annexe) a permis de faire émerger plusieurs orientations générales de politique publique et le rôle d'impulsion ou d'opérateur que pourrait jouer l'ANSSI à cet égard :

1. **Définir une vision française de la politique de la donnée pour la cybersécurité, que l'ANSSI devrait aider à bâtir** : grâce à ses compétences et son rôle d'autorité nationale, l'agence est un interlocuteur privilégié pour co-

construire les orientations stratégiques de la France et permettre à l'écosystème de se mobiliser, autour du défi de la donnée.

2. **Développer la standardisation des données pour faciliter leur partage et, ce faisant, la constitution de larges bases ou lacs de données, nécessaires pour permettre de produire des résultats intéressants.** En l'absence quasi-totale aujourd'hui de standards en la matière, la puissance publique – au travers de l'ANSSI – devrait avoir un rôle d'impulsion et devenir force de proposition, tout en co-construisant avec les autres acteurs de l'écosystème.

3. **Développer et garantir la confiance dans la collecte, le partage et l'accès aux bases et lacs de données. A cet égard, le rôle de l'ANSSI en tant que tiers de confiance a été évoqué à plusieurs reprises, sous plusieurs angles :**

    - L'ANSSI pourrait elle-même stocker des données et gérer des accès, cette option trouvant rapidement des limites : quelles données au profit de qui, quel passage à l'échelle ?
    - L'ANSSI pourrait qualifier des prestataires de lacs et bases de données, ainsi reconnus de confiance pour le stockage et la valorisation de données de clients ;
    - L'ANSSI pourrait également explorer l'idée d'une labélisation des entités de confiance aptes à accéder à des bases ou lacs de données qu'elles n'auraient pas elles-mêmes constituées, pour en tirer parti dans le cadre de leurs activités.

4. **Apporter des solutions techniques et juridiques pour concilier partage et protection** des données et notamment d'éléments de confidentialité. En particulier, tirer parti de l'expérience de secteurs ou d'entités spécialistes de la donnée telle qu'Etalab, pour développer un panel de modes de partage et d'accès la donnée (ex. accès à une donnée brute ; accès à des données retravaillées, éventuellement anonymisées ; partage des résultats d'analyses ; application d'algorithmes sur une base de données au profit d'une entité sans lui permettre d'y accéder directement)

5. **Fédérer et maintenir un écosystème d'acteurs de confiance engagés dans le partage de la donnée pour la cybersécurité. Le rôle du futur Cyber Campus** dans la fédération d'un écosystème et dans le développement des communs de la cybersécurité a été souligné comme une orientation très positive à cet égard.

6. **Etayer les enjeux de gouvernance, politiques et commerciaux, liés à la donnée** :

    - Œuvrer à l'équilibre des intérêts public, individuel et commercial, par exemple en désignant une institution responsable de juger les conflits d'intérêt ;
    - Assurer un pilotage des enjeux aux niveaux national et européen en s'appuyant sur un écosystème de confiance ;

- Protéger, le cas échéant, la souveraineté nationale et les intérêts nationaux

7. **Former et sensibiliser** de manière inclusive le grand public sur les données et ce depuis le plus jeune âge.

2. Des cas d'usages d'utilisation des données pour la cybersécurité

Dans une seconde séquence, plus pratique, l'ensemble des participant(e)s a été invité à imaginer des cas d'usage de valorisation de la donnée dans le cadre des missions de cybersécurité, par la combinaison de 3 cubes créés en séance représentatifs de flux de données, de bénéficiaires et de modes d'utilisation des données (visualisation, agrégation, service, etc.).

On retiendra, à titre d'exemple, deux cas d'usage fictifs :

1. ***Energyware*** : anticiper les attaques pour aider le travail des experts de la détection, en agrégeant des flux de données issus de la détection et de la BDD de consommation énergétique afin de trouver des corrélations entre les cyber-attaques et la consommation énergétique.
2. ***Cyber-protection dynamique des voyageurs*** : chaque entreprise transportant des voyageurs peut comparer des rapports d'analyse de la menace avec des flux de passive DNS issus de ses points d'accès mis à disposition des voyageurs afin de les alerter et les protéger.

N.B. Cette synthèse a été élaborée sur la base des restitutions orales et écrites effectuées lors de cet atelier collaboratif, dans le cadre d'une démarche expérimentale.

Bien qu'un effort particulier ait été fait pour capter et retranscrire l'essence des travaux, ce document ne saurait être parfaitement exhaustif.

Conçu pour recueillir et documenter les idées issues de l'atelier, il ne saurait par ailleurs être considéré comme un document engageant pour l'ANSSI..

La cybersécurité française a relevé le défi de la donnée

22 Novembre 2025 I Les Échos (abonné)

Au cœur de la révolution numérique des deux dernières décennies, la massification des données a été très tôt perçue comme une source d'opportunités pour de nombreux acteurs. Pour les experts de la cybersécurité et de la protection des données à caractère personnel, la donnée a d'abord constitué une valeur à protéger, contre les risques pour leur confidentialité, leur intégrité et leur disponibilité.

De la donnée à protéger à la donnée à valoriser

Après plusieurs années d'efforts internes et collectifs, la communauté de la sécurité et de la confiance numérique se félicite aujourd'hui d'avoir, à son tour, pris le virage de la donnée. En l'espace de cinq ans, industriels, startups, hackers et makers, acteurs du monde de la recherche, Etat - notamment sous l'impulsion de l'ANSSI - se sont mobilisés et permis des transformations profondes permettant à la France de rester dans le peloton de tête des Nations cyber du monde.

De cette transformation, la souveraineté numérique de la France et par extension de l'Europe ressort renforcée.

La donnée, un commun de la cybersécurité

Un virage qui n'a pas été sans nécessiter un changement de culture, sans renoncer pour autant aux principes sous-tendant la sécurité et la protection des données. Au-delà de la capitalisation et de la valorisation des données pour leur propre usage, les acteurs de l'écosystème français ont également appris à mettre davantage la donnée en commun.

Pour Guillaume Poupard : "les données associées à la cybersécurité, notamment opérationnelles, sont souvent très sensibles. Il y a quelques années, la façon d'en tirer parti ne s'imposait pas comme une évidence. Le partage des données dans l'intérêt commun du renforcement de la sécurité du cyberespace encore moins. Aujourd'hui, tout le monde est d'accord pour dire que la donnée a apporté de la confiance".

S'intéresser à la donnée mise au profit de la cybersécurité a également réservé des surprises : au-delà des données techniques et opérationnelles, des données plus inattendues se sont révélées riches en enseignements à l'instar de... *Lire la suite de l'article – abonnés*