Open source
Le nouveau standard

Copyright 2023, Lorem ipsum.

THALES
Building a future we can all trust

Table des matières

Présentation de la filière Open Source

Ce qu'il faut retenir (Points clés pour un décideur)
Les licences Open Source garantissent que le code source est ouvert, favorisant ainsi l'innovation et la collaboration. Ces licences offrent la possibilité que les modifications apportées au code soient partagées, bénéficiant ainsi à l'ensemble de la communauté. Elles jouent un rôle crucial dans la promotion de la transparence et de la sécurité, permettant une vérification publique du code.

Open Source Software

Attention : par définition, Open Source software veut dire « code lisible ».
Les termes de droit d'usage sont quand à eux liés aux licences associées à ce code source.

Définition de l'Open Source Software

L'Open Source fait référence à un modèle de développement et de distribution de logiciels où le code source est ouvert, c'est-à-dire accessible par tous ses utilisateurs. Contrairement aux logiciels dits « propriétaires », dont le code source est généralement gardé secret et soumis à des licences d'usage restrictives. L'Open Source permet à ses utilisateurs non seulement d'utiliser le logiciel, mais également de l'analyser. Cette approche est fondée sur la transparence, la collaboration et l'amélioration continue par la communauté des développeurs.

L'ouverture et la mise à disposition du code source favorise la mutualisation des efforts, l'innovation collaborative et l'accélération du développement technologique. En pratique, les logiciels Open Source sont souvent gérés par des communautés de développeurs qui collaborent à distance via des plateformes comme GitHub (un service web d'hébergement et de gestion de développement de logiciels, utilisant le logiciel de gestion de versions Git), ou par des éditeurs qui portent une vision et une offre commerciale.

Ces logiciels peuvent offrir une alternative solide et flexible aux logiciels commerciaux, permettant à des entreprises, des gouvernements, des organisations et des individus :

- d'adopter et d'adapter ces logiciels à leurs besoins spécifiques sans être liés à des contrats restrictifs ou à des frais de licence élevés ;
- de s'assurer de la transparence de fonctionnement et des traitements effectués par le logiciel ;
  - l'ouverture du code facilite également les audits de sécurité (et la mise en place de correctifs) ;
- une certaine assurance de pérennité : si l'éditeur est défaillant, le logiciel pourra être repris par d'autres, notamment s'il dispose d'une base d'utilisateurs ou clients suffisante.

Les exemples notables d'Open Source Software sont :
- Le noyau Linux et les distributions
- Le système d'exploitation pour smartphone Android
- Le navigateur web Mozilla Firefox
- Les bases de données MySQL & PostgreSQL
- La suite Bureautique LibreOffice
- Les Compilateur C / C++ / Rust
- K8S – Kubernetes
- …

Le marché de l'Open Source Software

Le marché des logiciels Open Source est d'environ 8,276 milliards d'euros[1]. Ce marché a connu une croissance impressionnante, multipliée par 40 en moins de vingt ans, avec une perspective de croissance annuelle de près de 8 % jusqu'en 2027.

1 https://www.library.hbs.edu/working-knowledge/open-source-software-the-nine-trillion-resource-companies-take-for-granted

Dans l'étude récente réalisée par le Conseil National du Logiciel Libre (CNLL)[2] la France se distingue par une adoption massive des logiciels libres, représentant environ 6,4 milliards d'euros de chiffre d'affaires en 2023 pour les entreprises du secteur. La France est par conséquence le premier marché européen pour l'Open Source, suivie de près par l'Allemagne, avec une croissance annuelle de plus de 8 %.

Ce rapport met en avant plusieurs points clés :

- **Croissance soutenue :** le marché européen de l'Open Source a connu une augmentation significative, avec une projection à 20 milliards d'euros d'ici 2027. La France, grâce à ses nombreuses PME innovantes, joue un rôle essentiel dans cette croissance.
- **Dynamique des entreprises :** plus de 70 % des entreprises françaises déclarent utiliser ou contribuer à des projets Open Source, renforçant l'idée que l'Open Source est un pilier de leur transformation numérique. Dans l'ensemble des entreprises, le sujet de l'Open Source est désormais incontournable et pris en compte, au travers la création de programme Open Source (OSPO).
- **Écosystème des services Open Source :** l'étude souligne l'importance des entreprises de services et des éditeurs Open Source qui dynamisent le marché, notamment dans les secteurs critiques comme la cybersécurité, les infrastructures cloud, et les bases de données.

Open Source Hardware

Définition de l'Open Source Hardware

L'Open Hardware (matériel ouvert) fait référence à des dispositifs physiques dont les plans, les schémas, les conceptions et les informations sont partagés librement et ouvertement. Reprenant les principes d'ouverture de l'Open Source, l'Open Hardware vise à rendre les conceptions matérielles accessibles, modifiables et partageables, favorisant ainsi la collaboration, l'innovation, la transparence et l'éducation.

L'Open Hardware couvre une large gamme de produits, allant des composants électroniques aux machines complexes, en passant par les dispositifs médicaux, les équipements de télécommunication et même les véhicules. Les entreprises et les particuliers peuvent utiliser ces plans pour fabriquer leurs propres versions des produits, les améliorer ou les adapter à des besoins spécifiques.

Les exemples notables d'Open Hardware sont :

- **Arduino :** Les cartes Arduino sont des plateformes de prototypage électronique Open Source. Leurs schémas, plans et codes sources sont disponibles pour tous, permettant à chacun de les fabriquer, modifier et utiliser.
- **Prusa :** Les imprimantes 3D Prusa sont un autre exemple d'Open Hardware. Leurs plans et logiciels sont disponibles sous licence Open Source, permettant aux utilisateurs de les modifier et améliorer.
- **Open Compute Project :** Initié par Facebook, ce projet partage les spécifications techniques de certains équipements de datacenters, comme les serveurs et les réseaux, pour optimiser leur efficacité énergétique.
- **Pocket Science Lab (PSLab) :** Un dispositif de test électronique complet, incluant générateur de tension, oscilloscope, et autres outils, entièrement Open Source.

Ces exemples montrent comment l'Open Hardware permet de créer des communautés actives autour de projets matériels, favorisant l'innovation et le partage des connaissances.

Focus sur RISC-V

Les processeurs RISC-V sont également considérés comme de l'Open Hardware. RISC-V est une architecture de jeu d'instructions (ISA) Open Source basée sur les principes RISC (Reduced Instruction Set Computing). Elle a été développée à l'Université de Californie, Berkeley, et est maintenant gérée par la RISC-V Foundation. L'architecture RISC-V est libre de droits et peut être utilisée, modifiée et distribuée librement, ce qui en fait un exemple typique d'Open Hardware. Les processeurs RISC-V sont utilisés dans une variété d'applications, allant des microcontrôleurs aux supercalculateurs, et sont soutenus par une large communauté de développeurs et d'entreprises technologiques, dont Thales.

2 Etude "Open Source Monitor France 2023" https://cnll.fr/news/open-source-monitor-france-2023/

Thales, leader important dans l'Open Source hardware group

Thales soutient activement le développement de l'écosystème Open Source pour les processeurs RISC-V. Thales a organisé le Second National RISC-V Student Contest en collaboration avec le réseau de recherche SOC21 et le CNFM2. Lors de cet événement, trois équipes d'étudiants ont été récompensées pour leurs solutions visant à réduire la consommation d'énergie du processeur CORE-V CVA6, un processeur Open Source RISC-V développé par l'OpenHW Group.

Le marché de l'Open Source Hardware

Le marché de l'Open Hardware est en pleine expansion et représente un potentiel significatif. La valorisation précise du marché de l'Open Hardware n'est pas directement mentionnée dans les résultats de recherche récents. Cependant le marché de l'Open Hardware est en pleine croissance, soutenu par une communauté mondiale de développeurs, d'ingénieurs et d'enthousiastes qui contribuent à l'innovation et à l'amélioration continue des designs ouverts. Ce marché est également soutenu par des initiatives et des organisations qui promeuvent l'adoption de l'Open Hardware dans divers secteurs industriels.

Licences et propriété intellectuelle

Les logiciels propriétaires et Open Source diffèrent principalement par leurs licences et leurs philosophies de développement. Les logiciels propriétaires sont développés par des entreprises qui conservent le contrôle total sur le code source, limitant ainsi les droits des utilisateurs à modifier, distribuer ou même accéder au code.

Le modèle Open Source s'appuie sur des licences spécifiques, comme la GNU GPL (GNU General Public License) ou la BSD (Berkeley Software Distribution License). L'univers des licences Open Source est vaste et riche. Aussi, une organisation, l'OSI (Open Source Initiative[3]), porte la définition officielle de l'Open Source et labellise les licences conformes à la définition d'Open Source.

Licence Open Source ?

Une licence est un contrat qui accorde aux utilisateurs des droits spécifiques sur un logiciel, tout en imposant certaines obligations. Les licences Open Source permettent aux utilisateurs de voir, modifier et distribuer le code source du logiciel, sous réserve de respecter les termes de la licence. Elles visent à encourager la collaboration, l'innovation et le partage de connaissances.

Différents types de licences

Les licences Open Source sont diverses et chacune a ses propres caractéristiques et obligations. Voici un aperçu des principaux types de licences Open Source et de leurs différences :

Licences permissives

Ces licences imposent peu de restrictions sur l'utilisation, la modification et la redistribution du code. Elles sont généralement compatibles avec les logiciels dit "propriétaires".

- **MIT License :** Très permissive, elle permet la libre utilisation, modification et distribution du code, même dans des logiciels propriétaires. La seule obligation est de conserver le texte de la licence dans les copies du logiciel.
- **Apache License 2.0 :** permissive également, mais elle inclut une clause de protection contre les brevets, ce qui signifie que les contributeurs accordent une licence sur leurs brevets relatifs aux contributions qu'ils apportent.
- **BSD License :** Permet la libre utilisation, modification et distribution du code. Elle exige que les copies du logiciel incluent le texte de la licence et une mention des auteurs originaux.

Licences avec clause de réciprocité (copyleft)

Ces licences exigent que les modifications et les travaux dérivés soient également distribués sous la même licence, ce qui garantit que le code reste Open Source.

3 https://opensource.org

- **GNU General Public License (GPL) :** Très populaire, elle exige que tout logiciel dérivé soit également distribué sous la licence GPL. Cela signifie que les modifications doivent être partagées avec la communauté.
- **GNU Lesser General Public License (LGPL) :** Similaire à la GPL, mais elle permet la combinaison du code source dans des logiciels propriétaires sous certaines conditions.
- **GNU Affero General Public License (AGPL) :** Une variante de la GPL qui exige que le code source soit fourni même lorsque le logiciel est utilisé en tant que service en ligne (SaaS).

Différences clés entre les licences

- **Obligations de redistribution :** Les licences copyleft comme la GPL exigent que les modifications soient partagées sous la même licence, tandis que les licences permissives comme la MIT permettent une utilisation plus libre.
- **Compatibilité avec les logiciels propriétaires :** Les licences permissives sont généralement compatibles avec les logiciels propriétaires, tandis que les licences copyleft peuvent poser des restrictions.
- **Protection contre les brevets** : Certaines licences, comme l'Apache License 2.0, incluent des clauses de protection contre les brevets, ce qui n'est pas le cas de toutes les licences.
- **Utilisation en tant que service (SaaS) :** La licence AGPL exige que le code source soit fourni même lorsque le logiciel est utilisé en tant que service en ligne, ce qui n'est pas le cas des autres licences.

Le choix d'une licence Open Source dépend des objectifs du projet, des besoins en termes de compatibilité et des préférences en matière de partage et de protection du code.

Enjeux en termes de propriété intellectuelle

L'utilisation de logiciels Open Source soulève plusieurs enjeux en matière de propriété intellectuelle :

- **Compatibilité des licences :** Certaines licences Open Source ne sont pas compatibles entre elles. Par exemple, combiner du code sous licence GPL avec du code sous licence Apache peut poser des problèmes de conformité. Il est crucial de vérifier la compatibilité des licences avant de combiner des composants Open Source.
- **Obligations de redistribution :** Certaines licences, comme la GNU General Public License (GPL), exigent que les modifications apportées au code source soient également distribuées sous la même licence. Cela peut poser des défis pour les entreprises qui souhaitent garder leurs modifications propriétaires.
- **Respect des droits d'auteur :** Même si le code est Open Source, les droits d'auteur appartiennent toujours aux auteurs originaux. Il est important de respecter ces droits et de se conformer aux termes de la licence.
- **Gestion des contributions :** Lorsque des développeurs externes contribuent à un projet Open Source, il est essentiel de s'assurer que ces contributions sont faites sous une licence compatible et que les droits d'auteur sont correctement gérés.
- **Risques de contamination de licence :** Intégrer du code Open Source dans un projet propriétaire peut entraîner une "contamination" de licence, où le projet propriétaire doit être distribué sous les mêmes termes que la licence Open Source. Cela peut être problématique pour les entreprises qui souhaitent conserver la propriété exclusive de leur code.
- **Conformité et audit :** Les entreprises doivent effectuer des audits réguliers pour s'assurer qu'elles se conforment aux termes des licences Open Source qu'elles utilisent. La non-conformité peut entraîner des litiges et des pénalités.
- **Protection des brevets :** Certaines licences Open Source, comme la licence Apache, incluent des clauses de protection contre les brevets. Cela signifie que les contributeurs accordent une licence sur leurs brevets relatifs aux contributions qu'ils apportent.

En résumé, bien que les licences Open Source offrent de nombreux avantages, elles nécessitent une gestion attentive des enjeux de propriété intellectuelle pour éviter les risques juridiques et assurer la conformité.

Comment gérer les licences des logiciels Open Source

La gestion des licences Open Source est essentielle pour les entreprises utilisant des logiciels libres. Elle permet de s'assurer que l'utilisation des logiciels respecte les termes des licences Open Source, évitant ainsi les risques juridiques et de conformité. Il existe des outils de gestion des licences Open Source qui aident à automatiser ce processus en analysant les licences, en surveillant leur conformité et en gérant les utilisateurs et les droits d'auteur. Vous pouvez contacter la Software Compliance Team pour plus détails.

Définition de la compliance

La compliance, ou conformité en français, désigne l'ensemble des processus mis en place pour assurer qu'une entreprise respecte les normes juridiques, éthiques et réglementaires applicables. Elle vise à prévenir les risques de sanctions, à protéger la réputation de l'entreprise et à répondre aux exigences des parties prenantes.

Recherche & Développement

Collaboration et Partage des Connaissances

L'Open Source a permis la création de communautés de développeurs et de chercheurs qui collaborent sur des projets communs. Ces communautés peuvent inclure des membres du monde entier, apportant une diversité de perspectives et d'expertises. Les chercheurs peuvent ainsi partager leurs résultats et leurs données plus facilement, ce qui permet à d'autres de reproduire et de valider les résultats, accélérant ainsi le processus de recherche.

Réduction des Coûts

En utilisant des logiciels et des outils Open Source, les entreprises et les institutions de recherche peuvent réduire leurs coûts de développement. Cela libère des ressources pour d'autres projets de R&D. Les petites entreprises et les startups peuvent accéder à des technologies de pointe sans avoir à investir dans des licences coûteuses, ce qui démocratise l'innovation.

Transparence et Reproductibilité

Les projets Open Source sont généralement plus transparents, ce qui permet une meilleure vérification et validation des résultats de recherche. La disponibilité du code source et des données permet à d'autres chercheurs de reproduire et de valider les résultats, ce qui est crucial pour la crédibilité de la recherche scientifique.

Innovation Ouverte

L'Open Source encourage une approche d'innovation ouverte, où les entreprises et les chercheurs partagent leurs innovations avec la communauté. Cela peut conduire à des avancées technologiques plus rapides et à une meilleure adoption des nouvelles technologies. Les contributions peuvent venir de diverses sources, y compris des universitaires, des entreprises et des particuliers, ce qui enrichit les projets avec une variété de perspectives et d'expertises.

Flexibilité et Personnalisation

Les logiciels Open Source peuvent être modifiés et adaptés pour répondre à des besoins spécifiques, ce qui est particulièrement utile dans des domaines de recherche spécialisés. Les chercheurs peuvent personnaliser les outils Open Source pour répondre à leurs besoins spécifiques, ce qui peut conduire à des solutions plus innovantes et plus efficaces.

Accélération de l'Innovation

Les projets Open Source peuvent évoluer rapidement grâce aux contributions de nombreux développeurs et chercheurs. Cela permet une innovation plus rapide et une adoption plus large des nouvelles technologies. Les entreprises peuvent adopter des technologies Open Source plus rapidement, ce qui peut leur donner un avantage concurrentiel.

Cyber et Digital

L’essor des solutions ouvertes dans un monde sécuritaire

Dans l’écosystème numérique actuel, où la protection des données et l’authentification sécurisée sont devenues des préoccupations majeures, l’Open Source s’est imposé comme un paradigme incontournable. La transparence inhérente au code ouvert offre un avantage considérable : celui d’un audit permanent par la communauté, garantissant une détection rapide des vulnérabilités et une réaction immédiate. Cette approche collaborative répond parfaitement aux exigences des organisations comme Thales, qui placent la confiance et la sécurité au cœur de leurs préoccupations.

Les fondations Open Source en cybersécurité

L’une des bibliothèques fondamentales dans ce domaine reste OpenSSL, devenue pierre angulaire de la sécurisation des communications numériques grâce à ses capacités avancées de chiffrement et de gestion des certificats. Son adoption massive par l’industrie témoigne de sa fiabilité pour l’implémentation des protocoles TLS et SSL, essentiels à la protection des échanges de données.

L’écosystème Open Source ne cesse de s’enrichir avec des solutions spécialisées répondant aux défis contemporains de la cybersécurité. Des projets comme OpenVAS pour l’analyse de vulnérabilités, OSSEC pour la détection d’intrusion, ou encore Wazuh pour la surveillance de l’intégrité des systèmes, illustrent la diversité et la maturité des outils disponibles.

Des acteurs industriels engagés

De nombreuses entreprises technologiques contribuent activement à cet écosystème, apportant ressources, expertise et soutien financier :

- Les géants américains comme Google, Microsoft, Amazon, IBM et Meta (Facebook) participent massivement aux initiatives de sécurité Open Source, conscients de l’importance stratégique de la fiabilité de ces solutions.
- Les spécialistes de la cybersécurité comme Thales, Canonical et Stormshield intègrent l’Open Source dans leur approche, contribuant aux communautés tout en bénéficiant des innovations collectives.
- Les prestataires de services cloud (Red Hat, VMware) investissent dans la sécurisation de leurs infrastructures Open Source, élément essentiel de leur proposition de valeur.

Ces acteurs contribuent non seulement par des dons financiers mais également par l’allocation de ressources humaines dédiées au développement et à l’amélioration des projets Open Source critiques.

Gestion des identités : l’approche ouverte comme garantie de confiance

Dans le domaine crucial de l’identité numérique, OpenID Connect (OIDC) s’est imposé comme une référence majeure. Ce protocole d’authentification, construit sur les fondations d’OAuth 2.0, permet une gestion simplifiée mais hautement sécurisée des identités à travers différents systèmes interopérables. La force d’OIDC réside dans sa capacité à offrir une expérience utilisateur fluide tout en maintenant un niveau de sécurité optimal pour les applications sensibles.

D’autres initiatives comme Keycloak, un gestionnaire d’identité Open Source, ou encore GLUU pour l’authentification multi-facteurs, viennent compléter cet écosystème, permettant aux organisations de construire des infrastructures d’identité robustes sans dépendance vis-à-vis de solutions propriétaires.

Keycloak, développé sous licence Apache et soutenu par Red Hat, est devenu une référence incontournable dans la gestion des identités. Cette solution complète permet l’authentification unique (SSO), la fédération d’utilisateurs, et prend en charge nativement les protocoles SAML v2 et OpenID Connect. Sa force réside dans sa capacité à centraliser l’authentification, permettant aux utilisateurs de s’identifier une seule fois pour accéder à l’ensemble des applications connectées.

La dynamique communautaire comme moteur d’excellence

Ce qui distingue fondamentalement l’approche Open Source en cybersécurité est la puissance de sa communauté. Active et réactive, elle assure une amélioration continue des outils, une identification rapide des

failles et une évolution constante des solutions. Des entreprises comme Thales comprennent l'importance de cette dynamique et y contribuent activement, notamment par leur participation à des fondations telles qu'Eclipse ou Linux Foundation.

Cette collaboration entre acteurs industriels et communauté Open Source crée un cercle vertueux : les entreprises bénéficient d'innovations constantes tandis que les projets gagnent en maturité et en adoption.

L'internet des objets sécurisé par l'Open Source

La sécurisation des objets connectés représente un défi majeur que l'approche Open Source permet de relever efficacement. Des projets comme Eclipse IoT ou Zephyr OS démontrent la capacité des solutions ouvertes à garantir une sécurité robuste dès la conception des dispositifs connectés.

L'adaptabilité inhérente aux technologies Open Source facilite leur intégration dans des environnements IoT hétérogènes, tout en assurant le respect de standards élevés de sécurité. Cette flexibilité s'avère particulièrement précieuse dans un domaine où les cas d'usage et les contraintes varient considérablement.

Une distribution spécialisée dans la cybersécurité

Kali Linux est une distribution Linux spécialement conçue pour les tests de pénétration et l'audit de sécurité. Elle est largement utilisée par les professionnels de la cybersécurité, les pentesters, et les chercheurs en sécurité informatique. Kali Linux inclut plus de 600 outils de sécurité préinstallés, ce qui en fait une boîte à outils complète pour les tests de pénétration et l'analyse de sécurité.

Kali Linux est équipée d'une vaste collection d'outils de sécurité préinstallés, couvrant divers aspects tels que l'analyse de réseau, l'ingénierie inverse, les tests d'intrusion, et la forensique numérique.

Initiatives collaboratives et réponses aux défis réglementaires

Face aux défis réglementaires croissants, notamment le Cyber Resilience Act européen, les acteurs de l'Open Source se mobilisent collectivement. Une initiative majeure récente est la collaboration entre sept fondations Open Source pour établir des spécifications communes pour le développement de logiciels sécurisés. Cette démarche vise à répondre proactivement aux exigences réglementaires tout en maintenant l'agilité et l'innovation propres à l'Open Source.

L'OpenSSF a également mis en place des équipes spécialisées : les équipes Alpha examinent les manques en matière de cybersécurité et développent méthodes et outils pour y remédier, tandis que les équipes Omega recherchent les vulnérabilités critiques dans des milliers de projets Open Source grâce à des systèmes d'analyse automatisés.

Vers une souveraineté numérique renforcée

L'adoption de solutions Open Source en cybersécurité s'inscrit également dans une démarche de souveraineté numérique. En s'affranchissant des "boîtes noires" propriétaires, les organisations gagnent en indépendance et en maîtrise de leur infrastructure de sécurité. Cette autonomie devient un enjeu stratégique, particulièrement pour les secteurs critiques comme la défense, l'énergie ou la santé.

La diversité des acteurs impliqués dans l'écosystème Open Source, allant des fondations internationales aux entreprises spécialisées, garantit un équilibre et prévient les situations de dépendance vis-à-vis d'un fournisseur unique. Cette approche distribuée renforce la résilience globale du système et favorise l'émergence de solutions adaptées aux besoins spécifiques de chaque contexte.

Conclusion : l'Open Source comme garant de confiance

Dans un contexte où les menaces cybernétiques évoluent constamment, l'Open Source offre un modèle de développement particulièrement adapté aux exigences de la cybersécurité et de la gestion des identités. Transparence, agilité, collaboration et innovation permanente sont les atouts majeurs de cette approche qui continuera à façonner l'avenir de la sécurité numérique.

La richesse de l'écosystème Open Source, tant par la diversité des solutions disponibles que par l'engagement des acteurs qui y contribuent, constitue un levier majeur pour relever les défis de sécurité contemporains. La convergence des efforts entre fondations, entreprises et communautés de développeurs crée un

cercle vertueux d'amélioration continue, essentiel pour maintenir une longueur d'avance face à des menaces en perpétuelle évolution.

Secteur Défense

L'intégration de l'Open Source et de l'Open Hardware dans le secteur de la défense représente une tendance stratégique majeure, offrant de nouvelles perspectives en matière de souveraineté, d'indépendance technologique et de maîtrise des coûts.

Dans un monde où le contexte géopolitique est très mouvant, le secteur de la Défense doit faire face aux problématique et aux enjeux de souveraineté. Dépendance et souveraineté : En France, le ministère des Armées est confronté à une dépendance croissante vis-à-vis des logiciels propriétaires, notamment ceux de Microsoft. Un rapport parlementaire met en garde contre le "piège Microsoft" et encourage l'exploration des logiciels libres pour renforcer la souveraineté numérique.

L'Open Source comme levier stratégique

L'utilisation de solutions Open Source dans la défense permet aux acteurs étatiques de réduire leur dépendance vis-à-vis des technologies propriétaires, souvent contrôlées par des acteurs étrangers. En maîtrisant directement leur code source, les organisations militaires renforcent leur autonomie, sécurisent davantage leurs infrastructures et gagnent en résilience face aux cybermenaces. Des exemples significatifs tels que l'adoption par l'armée française de solutions de cybersécurité Open Source (comme CLIP OS, développé par l'ANSSI) illustrent cette approche.

D'autres cas d'usage notables incluent le projet français de système de gestion de combat SCORPION, intégrant largement des briques logicielles Open Source pour assurer interopérabilité et évolutivité. De même, le ministère américain de la Défense utilise Kubernetes, un système Open Source d'orchestration de conteneurs, pour améliorer la gestion et la sécurité des applications militaires.

Le secteur militaire exploite aussi largement les capacités du noyau Linux temps réel (Real-Time Linux), utilisé pour les systèmes embarqués critiques nécessitant une précision temporelle élevée, comme les systèmes d'armement, les radars ou les drones militaires. Pour simplifier l'intégration et la personnalisation de systèmes Linux embarqués, des outils tels que Yocto Project et Buildroot sont couramment employés, permettant aux industriels de la défense de construire des distributions adaptées à leurs besoins spécifiques tout en maîtrisant parfaitement leur chaîne de production logicielle.

La transparence du code Open Source permet ainsi une auditabilité accrue, essentielle pour assurer la confiance et la robustesse des systèmes militaires critiques.

L'Open Hardware : une nouvelle frontière pour la souveraineté

Parallèlement, l'Open Hardware représente un potentiel considérable pour le secteur de la défense. En fournissant des plans accessibles et modifiables de composants et de systèmes matériels, l'Open Hardware permet aux organisations militaires de produire localement, d'adapter rapidement les équipements à leurs besoins spécifiques, et de limiter les risques liés aux ruptures d'approvisionnement.

Des initiatives telles que le projet RISC-V illustrent cette dynamique. Ce projet de processeur Open Hardware offre une alternative stratégique aux solutions propriétaires, souvent soumises à des restrictions commerciales ou géopolitiques. Aux États-Unis, la DARPA soutient plusieurs projets Open Hardware, tels que le programme POSH (Programmable Open Source Hardware), destiné à créer des composants électroniques plus sûrs et plus transparents.

Défis et limites de l'approche ouverte

Toutefois, l'ouverture présente aussi des défis spécifiques. L'exposition potentielle des solutions Open Source et Open Hardware aux acteurs hostiles requiert des stratégies robustes en matière de sécurité, d'intégration et de gouvernance des communautés. La gestion de ces enjeux implique des politiques claires de collaboration, des mécanismes de protection juridique adaptés, ainsi qu'une gouvernance structurée de l'innovation ouverte.

Vers une défense collaborative et souveraine

En définitive, l'intégration intelligente de l'Open Source et de l'Open Hardware dans les stratégies de défense constitue une voie prometteuse pour renforcer la souveraineté technologique nationale. En conjuguant innovation, transparence et résilience, cette approche favorise un écosystème de défense collaboratif, agile et capable de répondre aux défis sécuritaires contemporains.

Secteur Aérospatial

Le secteur spatial européen traverse actuellement une transformation majeure portée par l'essor des technologies Open Source. Autrefois perçu comme un domaine réservé aux grandes agences nationales et aux industriels historiques, l'espace voit désormais émerger une dynamique de collaboration ouverte, rendue possible par la démocratisation de l'accès aux technologies spatiales.

Logiciels Open Source : démocratiser la mécanique orbitale

Au cœur de cette transformation se trouve Orekit, une bibliothèque Open Source en Java dédiée à la mécanique orbitale et à la navigation spatiale. Soutenue par l'ESA, Orekit permet à des acteurs publics, privés et universitaires de réaliser des calculs complexes d'orbites, de trajectoires, ou encore de prédictions de passages satellites. D'autres outils comme GMAT (General Mission Analysis Tool), développé initialement par la NASA puis diffusé en Open Source, ou l'ESA SNAP Toolbox pour le traitement des données satellites, démontrent la richesse de cette approche collaborative.

Initiatives publiques et privées : vers un écosystème ouvert

Les acteurs publics jouent un rôle crucial. L'ESA organise le Summer of Code in Space (SOCIS), inspiré du Google Summer of Code, favorisant ainsi la contribution à des projets spatiaux Open Source par des étudiants et chercheurs.

Côté privé, Thales Alenia Space et Airbus Defence & Space, bien que traditionnellement orientés vers des solutions propriétaires, s'ouvrent progressivement aux standards et aux outils Open Source pour améliorer l'interopérabilité et l'efficacité de leurs missions. Exotrail, une startup française du NewSpace, développe des logiciels compatibles avec des briques Open Source pour optimiser les trajectoires de petits satellites, illustrant parfaitement l'intégration de l'Open Source dans le secteur privé émergent.

Libre Space Foundation : pionnier du spatial 100% ouvert

La Libre Space Foundation (LSF) représente l'avant-garde du mouvement Open Source dans le spatial. Cette fondation grecque développe intégralement des projets spatiaux Open Source, matériel et logiciel. Le réseau SatNOGS, constitué de stations sol Open Hardware pour communiquer avec les satellites, et le satellite UPSat, entièrement conçu en Open Source, sont des exemples emblématiques de leur action. L'approche de LSF est à la fois éducative, scientifique et inclusive, illustrant concrètement comment l'Open Source permet une démocratisation radicale de l'espace.

Open Hardware : une dynamique émergente

En complément des logiciels, l'Open Hardware s'impose également comme une approche prometteuse, bien qu'encore émergente. Les projets tels que les stations sol SatNOGS, les nanosatellites QUBIK, ou encore les modules de satellites universitaires montrent l'intérêt grandissant pour cette démarche. Des acteurs publics comme l'ESA, à travers des initiatives comme SDR MakerSpace, ainsi que des universités européennes publient régulièrement leurs travaux en Open Hardware, renforçant ainsi une communauté d'innovation collaborative.

Vers un spatial ouvert et collaboratif

L'Open Source bouleverse donc profondément le secteur spatial, en apportant plus de transparence, de collaboration, et en réduisant les barrières à l'entrée pour de nouveaux acteurs. En combinant les forces des agences publiques, des grands industriels, des startups innovantes, et de la communauté mondiale, l'Europe spatiale accélère ainsi son développement tout en renforçant son autonomie technologique et son influence internationale.

NASA

La NASA joue un rôle significatif dans le développement et la promotion de l'Open Source, particulièrement dans le domaine de l'aérospatial. Voici quelques implications notables :

- La NASA[4] a développé OpenVSP (Open Vehicle Sketch Pad), un outil Open Source pour la modélisation géométrique paramétrique des aéronefs. Cet outil permet de créer des modèles 3D d'aéronefs et de supporter l'analyse technique de ces modèles. OpenVSP est largement utilisé dans l'industrie aérospatiale pour la conception et l'analyse des aéronefs.

Ces contributions de la NASA montrent son engagement en faveur de l'Open Source, facilitant ainsi l'innovation, la collaboration et l'efficacité dans le domaine aérospatial.

4 https://code.nasa.gov/

Éléments différenciateurs & Enjeux

Ce qu'il faut retenir (Points clés pour un décideur)

L'Open Source est un levier stratégique pour renforcer l'indépendance technologique, maîtriser les coûts et favoriser l'innovation. Il permet une personnalisation poussée, une intégration facilitée via des standards ouverts et une plus grande sécurité grâce à la transparence du code. Soutenu par un écosystème international structuré, il offre une alternative pérenne aux solutions propriétaires, tout en répondant aux exigences de souveraineté et de conformité (CRA, NIS2).

Au-delà de la technologie, l'Open Source renforce l'attractivité RH en valorisant les compétences, en fidélisant les talents et en améliorant l'image de l'entreprise. Son adoption nécessite toutefois une approche rigoureuse, combinant méthodologies d'évaluation (QSOS, OW2 MRL, ANSSI) et anticipation des coûts cachés liés à la maintenance, à la sécurité et à la gouvernance.

Avantages de l'Open Source

Gouvernance, indépendance et Souveraineté Technologique

L'indépendance technologique est devenue un enjeu majeur. L'Open Source permet de se libérer de la dépendance envers des éditeurs de logiciels propriétaires et des géants technologiques (GAFAM) qui peuvent imposer des conditions commerciales trop restrictives sans négociation ou contre-pouvoir. En utilisant des solutions Open Source, les entreprises peuvent donc éviter la dépendance à un seul fournisseur de logiciels, réduisant le risque de verrouillage technologique et offre plus de liberté dans le choix des technologies.

De plus les solutions Open Source sont souvent développées selon des standards ouverts, ce qui peut faciliter l'intégration avec d'autres systèmes et technologies. Cela peut également aider à garantir la conformité avec les réglementations et les normes industrielles.

Des initiatives comme openDesk du Zentrum Digitale Souveränität en Allemagne montrent déjà que l'Europe peut construire un écosystème numérique sûr. Cette initiative repose sur des solutions Open Source développées par des éditeurs européens, XWiki, CryptPad, OpenProject et Nextcloud. Les solutions utilisées sont des alternatives sûres, open-source et indépendantes aux plateformes américaines.

Collaboration internationale

Les projets Open Source favorisent la collaboration internationale, permettant aux pays de travailler ensemble pour développer des technologies avancées sans dépendre de quelques grandes entreprises technologiques. L'Europe a de plus en plus recours à des solutions Open Source.

Avantages Économiques

Mutualisation des développements

L'un des avantages économiques majeurs de l'Open Source est la mutualisation des coûts. Ce modèle repose sur une collaboration ouverte où plusieurs organisations partagent les coûts de développement, de maintenance et d'amélioration des logiciels ou composants. Contrairement aux solutions propriétaires, où chaque entreprise paie des licences et souvent des frais de maintenance élevés, l'Open Source permet de distribuer ces coûts entre un nombre potentiellement illimité de parties prenantes.

Réduction des Coûts de Licence

Les logiciels ou composants Open Source techniques sont souvent gratuits ou disponibles sous des licences très permissives. Cela permet aux entreprises de réaliser des économies importantes en supprimant les coûts de licences, qui peuvent représenter une part considérable du budget informatique des organisations. Même si certaines solutions Open Source nécessitent des services payants (support, formation, etc.), ces coûts sont généralement inférieurs à ceux des licences des logiciels propriétaires.

Avantages Techniques

Innovation Collaborative

L'Open Source encourage une innovation collaborative unique. Les projets Open Source bénéficient des contributions d'une grande diversité de développeurs, ce qui permet de capitaliser sur des idées et des approches différentes. Cette collaboration conduit à des améliorations continues et à l'introduction rapide de nouvelles technologies dans les logiciels. L'absence de contraintes commerciales dans les projets Open Source permet également aux développeurs d'expérimenter et d'innover librement, sans attendre l'approbation d'une entreprise ou d'un comité de direction.

Flexibilité et Adaptabilité

Un des atouts majeurs de l'Open Source est sa flexibilité. Les entreprises peuvent adapter le logiciel à leurs besoins spécifiques en modifiant elles-mêmes le code source. Cela permet une personnalisation poussée, impossible à atteindre avec des logiciels propriétaires. L'adaptabilité des logiciels Open Source permet également une meilleure intégration avec d'autres systèmes. Les entreprises peuvent ajuster les solutions à leurs environnements informatiques et métiers sans avoir à payer pour des modules supplémentaires ou des versions "premium".

Pérennité et Durabilité

Les logiciels propriétaires peuvent être abandonnés par leurs éditeurs ou voir leurs conditions de licence changer de manière arbitraire. À l'inverse, les logiciels Open Source sont généralement pérennes, car le code source est ouvert et accessible. Même si l'équipe de développement d'origine ou l'éditeur cesse son activité, la communauté ou d'autres entreprises peuvent reprendre le projet et en assurer la continuité.

Cela confère une plus grande sécurité à long terme, car les organisations ne sont pas dépendantes des décisions commerciales d'une seule entité pour continuer à utiliser le logiciel et un garde-fou est présent au cas où l'équipe de développement ou l'éditeur sortiraient des limites acceptables par la majorité des utilisateurs.

Sécurité

L'Open Source a parfois été perçu comme moins sécurisé que les logiciels propriétaires, mais cette idée est de plus en plus réfutée. En fait, les logiciels Open Source sont souvent plus sûrs précisément parce que leur code source est ouvert et que tout le monde peut l'examiner. Cette transparence permet de détecter et de corriger rapidement les failles de sécurité.

Interopérabilité et Compatibilité via les formats ouverts

Les logiciels Open Source sont souvent conçus pour être interopérables avec d'autres systèmes et normes. Cela permet aux entreprises d'intégrer plus facilement des solutions Open Source dans des infrastructures hétérogènes, tout en assurant la compatibilité avec des outils et des systèmes déjà en place. Les standards ouverts sont un principe fondamental de l'Open Source, garantissant que les systèmes puissent interagir sans verrouillage propriétaire.

Un format ouvert est un type de format de fichier dont les spécifications sont publiquement disponibles et peuvent être librement utilisées et implémentées par n'importe qui. Les formats ouverts permettent l'interopérabilité entre différents systèmes et logiciels, car ils ne sont pas contrôlés par un seul éditeur ou une entreprise spécifique.

Les formats ouverts jouent un rôle crucial dans l'interopérabilité des systèmes et des logiciels. Ils permettent aux différents systèmes de communiquer et d'échanger des données sans entraves, favorisant ainsi la compatibilité et l'intégration entre diverses solutions technologiques. Les formats ouverts sont essentiels pour garantir que les données peuvent être partagées et utilisées de manière transparente et sécurisée, sans dépendre de solutions propriétaires spécifiques

Maintenabilité

Les projets Open Source sont souvent conçus pour être facilement maintenables et évolutifs. Les entreprises peuvent contribuer directement à l'amélioration du code ou faire appel à des prestataires externes pour assurer la maintenance de leurs solutions Open Source. L'accès au code source permet également aux équipes techniques internes d'assurer une maintenance proactive, d'ajuster les systèmes en fonction des besoins, et de corriger rapidement les erreurs sans devoir attendre l'intervention de l'éditeur.

Avantages Sociétaux

Partage des Connaissances

L'Open Source est basé sur le partage des connaissances. En ouvrant le code source, les développeurs permettent à d'autres de comprendre comment fonctionne le logiciel et de l'améliorer. Cela contribue à la création d'une culture de collaboration et d'apprentissage dans l'ensemble de la communauté technologique. Les projets Open Source servent également de base à des projets éducatifs et académiques. Les étudiants et les chercheurs peuvent accéder librement aux technologies avancées, apprendre des concepts complexes en les appliquant directement et contribuer eux-mêmes aux projets.

Développement Communautaire et Collaboratif

L'Open Source crée et favorise le développement de communautés de développeurs et d'utilisateurs. Ces communautés sont des lieux de collaboration où les gens échangent des idées, partagent des solutions à des problèmes communs et participent à la co-création de nouvelles technologies.

Soutien à l'Économie

L'adoption de solutions Open Source peut renforcer l'économie locale et nationale en favorisant la création d'entreprises locales spécialisées dans le développement, la personnalisation et le support des logiciels Open Source. Plutôt que de dépendre de grands éditeurs étrangers, les entreprises locales peuvent développer des compétences en interne et offrir des services à d'autres entreprises ou organisations publiques. Cette approche encourage également le développement des talents locaux, la formation de nouveaux professionnels et la création d'un écosystème technologique durable.

Avantages dans la gouvernance

La gouvernance désigne l'ensemble des règles, des méthodes et des pratiques qui organisent la réflexion, la prise de décision et le contrôle de l'application des décisions au sein d'un groupe social, d'une entreprise ou d'une organisation. Elle vise à assurer le fonctionnement optimal de l'organisation et à garantir la transparence et la responsabilité dans la gestion des ressources et des processus.

Les solutions Open Source permettent d'avoir une gouvernance en offrant des cadres et des outils pour structurer la prise de décision et la gestion des projets de manière transparente et collaborative. Par exemple, l'Open Source Program Office (OSPO) Alliance propose des méthodologies et des bonnes pratiques pour aider les organisations à mettre en place une gouvernance Open Source efficace. Ces initiatives favorisent la participation communautaire et l'amélioration continue des projets Open Source.

Rôle de l'Europe

L'Europe prône une gouvernance basée sur les solutions Open Source à travers diverses initiatives et stratégies. La Commission européenne, par exemple, a mis en place une stratégie Open Source visant à encourager et à tirer parti du pouvoir transformateur, innovant et collaboratif de l'Open Source. Cette stratégie, intitulée « Think Open », vise à promouvoir le partage et la réutilisation des solutions logicielles, des connaissances et de l'expertise pour offrir de meilleurs services européens bénéfiques à la société et réduire les coûts.

En outre, l'Europe soutient des initiatives telles que l'OSPO Alliance, qui aide les organisations à mettre en place une gouvernance Open Source efficace. L'OSPO Alliance, créée par des fondations Open Source comme OW2, Eclipse et Open Forum Europe, fournit des méthodologies, des bonnes pratiques et des ressources pour structurer les politiques et la gouvernance Open Source. Thales est un contributeur actif de cette initiative depuis 2023.

La Commission européenne a également lancé le projet EU-FOSSA (Free and Open Source Software Auditing) pour améliorer la sécurité et l'intégrité des logiciels Open Source critiques. Ces efforts montrent l'engagement de l'Europe à adopter et à promouvoir des solutions Open Source pour une gouvernance plus transparente, collaborative et efficace.

Panorama de l'écosystème

Open Source Software

FREE SOFTWARE FOUNDATION	**Fondation pour le Logiciel Libre (FSF)** - https://www.fsf.org Organisation fondée par Richard Stallman en 1985, à l'origine du mouvement du logiciel libre et du projet GNU. La FSF promeut les quatre libertés fondamentales du logiciel libre et est responsable des licences GPL.
open source initiative®	**Open Source Initiative (OSI)** - https://opensource.org Organisation pionnière créée en 1998, responsable de la définition formelle de l'Open Source et de la validation officielle des licences Open Source. L'OSI joue un rôle de référence internationale en assurant la clarté juridique, en sensibilisant les entreprises aux avantages du modèle Open Source et en garantissant le respect des standards communautaires. Récemment, l'OSI a travaillé sur une définition pour l'intelligence artificielle Open Source, visant à clarifier ce que signifie être "open" dans le contexte de l'IA.
THE LINUX FOUNDATION	**Linux Foundation** - https://www.linuxfoundation.org Fondée en 2000, organisation à but non lucratif dont la mission est de soutenir, protéger et standardiser le développement du système d'exploitation Linux et d'autres projets Open Source. Elle joue aujourd'hui un rôle de fédération majeure en hébergeant des centaines de projets Open Source de premier plan, comme Kubernetes, Hyperledger, Automotive Grade Linux, ou la Cloud Native Computing Foundation (CNCF).
CLOUD NATIVE COMPUTING FOUNDATION	**Cloud Native Computing Foundation (CNCF)** - https://www.cncf.io Sous l'égide de la Linux Foundation, se concentre sur la gestion et la promotion des technologies Cloud Native, comme Kubernetes, Prometheus ou Envoy. Elle a un impact international considérable sur l'adoption et la standardisation des architectures basées sur des conteneurs, l'orchestration, et les micro-services.
THE APACHE SOFTWARE FOUNDATION ESTABLISHED 1999	**Apache Software Foundation** - https://www.apache.org Fondée en 1999, l'Apache Software Foundation (ASF) est l'une des plus grandes et des plus influentes organisations Open Source au monde. Elle gère plus de 350 projets, dont beaucoup constituent l'épine dorsale de l'internet et du cloud moderne (Apache, Hadoop, Spark, Cassandra et NiFi). La particularité de l'ASF réside dans son modèle de gouvernance méritocratique (le pouvoir décisionnel est gagné par la contribution) et son processus d'incubation rigoureux pour les nouveaux projets. Sa licence Apache 2.0 est devenue un standard de l'industrie pour sa compatibilité avec les usages commerciaux, tout en préservant les principes Open Source.
CHAOSS	**CHAOSS (Community Health Analytics Open Source Software)** - https://chaoss.-community Projet de la Linux Foundation qui développe des métriques, des méthodologies et des outils pour mesurer la santé et la durabilité des communautés Open Source.

	OpenChain Project - https://www.openchainproject.org Initiative de la Linux Foundation qui établit des standards pour la gestion de la conformité des licences Open Source dans les chaînes d'approvisionnement logicielles.
	Fondation Mozilla - https://foundation.mozilla.org La Fondation Mozilla, créée en 2003 suite à la libération du code source de Netscape Navigator, est une organisation à but non lucratif dédiée à la préservation d'un internet ouvert, accessible et sécurisé. Elle supervise le développement de produits technologiques libres, dont le plus connu est le navigateur Firefox, tout en menant des campagnes de plaidoyer pour la protection de la vie privée, la neutralité du net et l'interopérabilité des standards web. En plus du navigateur, elle est à l'initiative du langage de programmation Rust, désormais utilisé par Microsoft, Google, Amazon et d'autres pour des systèmes critiques. Tout récemment elle a décidé d'accélérer le développement d'une suite collaborative basée sur Thunderbird.
	Fondation Rust - https://rustfoundation.org/ La Fondation Rust est une organisation à but non lucratif dédiée au soutien et au développement du langage de programmation Rust. Elle a été créée pour garantir la pérennité et la croissance de Rust, en favorisant son adoption et son évolution. La fondation supervise les contributions de la communauté, coordonne les efforts de développement et promeut les meilleures pratiques. Elle travaille également à assurer la stabilité et la sécurité du langage. Enfin, la Fondation Rust encourage l'innovation et la collaboration au sein de l'écosystème Rust.

Open Source Hardware

	RISC-V International - https://riscv.org Fondée en 2015 et basée en Suisse, RISC-V International est l'organisme de standardisation qui supervise le développement de l'architecture processeur RISC-V, une instruction set architecture (ISA) ouverte et libre de droits. Contrairement aux architectures propriétaires comme ARM ou x86, RISC-V permet à quiconque de concevoir, fabriquer et commercialiser des processeurs sans payer de redevances. Avec plus de 3000 membres dans 70 pays, incluant des géants comme Google, Qualcomm et Alibaba, cette fondation établit les spécifications techniques, maintient la compatibilité entre implémentations et coordonne l'évolution de l'écosystème. L'impact de RISC-V s'étend aujourd'hui de l'IoT aux supercalculateurs, offrant une alternative stratégique dans un contexte de tensions géopolitiques autour des technologies de semi-conducteurs et de souveraineté numérique.
	OpenHW Group - https://www.openhwgroup.org Fondée en 2019, l'OpenHW Group est une organisation à but non lucratif qui développe des cœurs de processeurs Open Source basés sur l'architecture RISC-V et prêts pour une utilisation industrielle. Son projet CORE-V propose des implémentations robustes et entièrement vérifiées comme le CV32E40P (32-bit) et le CVA6 (64-bit). Rassemblant plus de 90 membres incluant Intel, NXP et ST Microelectronics, cette fondation comble le fossé entre les spécifications ouvertes et leur implémentation commercialement viable, tout en maintenant l'ensemble de la propriété intellectuelle sous licences Open Source. L'OpenHW Group fournit également l'écosystème d'outils nécessaire pour faciliter l'adoption de ces technologies dans des applications allant de l'IoT aux systèmes embarqués critiques.
	Open Compute Project (OCP) - https://www.opencompute.org Fondé en 2011 par Facebook (désormais Meta), l'Open Compute Project est une organisation collaborative qui redéfinit l'approche du hardware dans les centres de données en appliquant les principes de l'Open Source au matériel informatique. L'OCP développe et partage des designs ouverts pour les serveurs, le stockage, les

	réseaux et les infrastructures de data centers, optimisés pour l'efficacité énergétique et la réduction des coûts. Avec plus de 200 membres incluant Microsoft, Intel, Google et AT&T, l'organisation a permis des économies d'énergie considérables et une réduction significative des déchets électroniques. Les spécifications OCP sont désormais implémentées dans plus de 40% des serveurs de cloud public, démontrant l'impact transformateur de l'approche Open Source appliquée au matériel d'infrastructure à grande échelle.
OPEN SOURCE FIRMWARE FOUNDATION	**Open Source Firmware Foundation (OSFF)** - https://opensourcefirmware.foundation Fondée en 2022, l'Open Source Firmware Foundation (OSFF) est une organisation dédiée à la promotion et au développement de firmwares Open Source pour les systèmes informatiques modernes. Elle se concentre sur les couches logicielles de bas niveau qui s'exécutent avant le système d'exploitation, comme le BIOS/UEFI, les bootloaders et les firmwares de cartes réseaux ou de contrôleurs de stockage. L'OSFF soutient des projets comme coreboot, LinuxBoot et OpenBMC, qui visent à remplacer les firmwares propriétaires par des alternatives ouvertes, auditables et sécurisées. Créée en réponse aux préoccupations croissantes concernant la sécurité et la souveraineté numérique, cette fondation rassemble des acteurs industriels comme Google, 9elements et Star Labs, ainsi que des chercheurs en sécurité, pour combler le dernier grand fossé propriétaire dans la pile logicielle des ordinateurs modernes.
Open Source Hardware Association OSHWA	**Open Source Hardware Association (OSHWA)** - https://www.oshwa.org Fondée en 2012, l'OSHWA est l'organisation de référence pour le matériel libre et ouvert. Elle a établi la définition officielle du Open Source Hardware et gère un programme de certification permettant aux créateurs d'identifier leurs produits comme conformes aux standards du hardware ouvert. L'OSHWA organise le Open Hardware Summit annuel et promeut les bonnes pratiques de documentation et de partage dans le domaine du matériel.

Les acteurs clés de l'écosystème Open Source en cybersécurité

OWASP	**L'OWASP (Open Web Application Security Project)** https://owasp.org L'OWASP est une organisation à but non lucratif qui se concentre sur l'amélioration de la sécurité des applications logicielles. Fondée en 2001, l'OWASP est devenue une référence mondiale en matière de sécurité des applications web.
OpenSSF OPEN SOURCE SECURITY FOUNDATION	**Open Source Security Foundation (OpenSSF)** - https://openssf.org Fondée en août 2020 sous l'égide de la Linux Foundation, l'OpenSSF est une initiative collaborative qui répond à l'urgence croissante de sécuriser l'écosystème Open Source. L'OpenSSF rassemble plus de 100 membres, incluant les géants technologiques (Google, Microsoft, Amazon, Meta), les principales fondations Open Source (Linux Foundation, Apache Software Foundation) et des acteurs spécialisés en cybersécurité. L'OpenSSF est devenue en peu de temps l'initiative de référence pour répondre aux défis de sécurité spécifiques au modèle Open Source, comme la dépendance à des mainteneurs bénévoles, la complexité des dépendances, et l'utilisation massive de composants insuffisamment audités.
OpenID	**L'OpenID Foundation -** https://openid.net Elle se concentre sur le développement et la promotion des standards d'identité numérique. Elle a notamment créé un groupe de travail pour la norme IPSIE (Interoperability Profile for Secure Identity in the Enterprise), adoptée par des acteurs majeurs comme Microsoft, Google et Ping Identity.
openSSL FOUNDATION	**La Fondation OpenSSL** https://openssl-foundation.org

	Elle joue un rôle critique dans la sécurisation des communications, son projet phare étant classé dans le top 10 des projets les plus importants par l'Open Source Security Index.

Europe

ECLIPSE FOUNDATION	**Eclipse Foundation** - https://www.eclipse.org Initialement centrée sur l'outil de développement Eclipse IDE, est devenue l'une des principales fondations Open Source dédiées à la gouvernance collaborative et au développement durable de projets logiciels Open Source dans de multiples secteurs. Elle rassemble une vaste communauté mondiale et gère plus de 400 projets. Désormais basée en Europe (Belgique) depuis 2020.
OSPO ALLIANCE	**OSPO Alliance** - https://ospo.zone Initiative internationale soutenue par OW2 et Eclipse Foundation, vise à promouvoir et structurer les bonnes pratiques autour des OSPO (Open Source Program Offices) au sein des entreprises. Elle favorise la professionnalisation de la gestion de l'Open Source dans les organisations privées comme publiques, en Europe et à l'international.
OW2	**OW2** - https://www.ow2.org/ Communauté Open Source européenne indépendante, dédiée principalement aux logiciels d'infrastructure Open Source. Elle promeut une gouvernance ouverte et collaborative des logiciels et encourage l'adoption de solutions Open Source au sein des administrations et grandes entreprises européennes. OW2 est également reconnue pour ses travaux sur l'interopérabilité et la souveraineté numérique.
Foundation for Public Code	**Foundation for Public Code** - https://publiccode.net Fondée aux Pays-Bas en 2019, cette organisation européenne se concentre spécifiquement sur le développement et la maintenance de code public - logiciels Open Source développés par et pour les gouvernements et administrations publiques.

France

Systematic Paris Region Deep Tech Ecosystem	**Hub Open Source Software de Systematic Paris-Region** - https://www.systematic-paris-region.org/hubs/hub-oss Le Hub OSS, porté par le pôle de compétitivité Systematic Paris-Region, agit comme un centre d'expertise et d'animation de l'écosystème Open Source français. Il rassemble des entreprises, organismes de recherche, universités et pouvoirs publics afin de promouvoir l'adoption des logiciels libres.
APELL	**APELL (Association Professionnelle Européenne du Logiciel Libre)** - https://apell.info Association professionnelle française visant à représenter les intérêts économiques et stratégiques des entreprises du logiciel libre en France et en Europe. Elle intervient sur des sujets juridiques, économiques et politiques.
TOSIT The Open Source I Trust	**TOSIT (The Open Source I Trust)** - https://tosit.fr Collectif français regroupant de grandes entreprises (Société Générale, BPCE, EDF, MAIF, Michelin...) engagé dans l'adoption maîtrisée de l'Open Source. Il développe des bonnes pratiques autour du sourcing, de la sécurisation et du support des solutions Open Source stratégiques.
CNLL Les entreprises du numérique ouvert	**CNLL (Conseil National du Logiciel Libre)** - https://cnll.fr Fédération française des entreprises du logiciel libre, représentant environ 300 entreprises via ses associations régionales membres.

	Software Heritage - https://www.softwareheritage.org Initiative française de préservation du patrimoine logiciel, reconnue à l'international. Lancée par Inria, elle vise à collecter, préserver et partager tous les codes sources publiquement disponibles.

Méthodologies d'Analyse et de Sélection des Solutions Open Source

L'adoption croissante de logiciels Open Source dans les organisations nécessite une évaluation méthodique et rigoureuse pour répondre aux enjeux complexes de sécurité, pérennité et gouvernance. Cette section présente une analyse des principales méthodologies d'évaluation de trois cadres méthodologiques majeurs : QSOS, l'OW2 Market Readiness Levels et l'approche de l'ANSSI.

Les Trois Méthodologies Essentielles

QSOS : l'approche globale et comparative

Principe : Créée en 2004, QSOS (Qualification and Selection of Open Source Software) propose une méthodologie en quatre phases pour évaluer objectivement les solutions Open Source. Elle repose sur une notation standardisée qui permet de comparer différentes alternatives sur une base commune.

Processus d'évaluation :

- **La phase de définition** établit le référentiel d'évaluation adapté au contexte spécifique de l'organisation ;
- **La phase d'évaluation** proprement dite consiste à noter chaque solution sur une échelle de 0 à 2 selon trois dimensions principales : les aspects intrinsèques (maturité, gouvernance, communauté), les aspects techniques (architecture, standards, sécurité) et les services associés (documentation, support, formation) ;
- **La phase de qualification** permet ensuite de pondérer ces critères selon les priorités organisationnelles ;
- Enfin, l**a phase de sélection** facilite la comparaison objective des solutions évaluées pour éclairer la décision finale.

Avantages:
La force principale de QSOS réside dans son approche standardisée qui facilite grandement la comparaison entre plusieurs solutions concurrentes. Sa flexibilité permet d'adapter l'évaluation aux priorités spécifiques de chaque organisation. L'existence d'une base de référence partagée au sein de la communauté permet également de réduire les coûts d'évaluation en mutualisant les efforts.

Limites :
La mise en œuvre complète de QSOS peut s'avérer chronophage, particulièrement pour des organisations disposant de ressources limitées. Par ailleurs, les évaluations nécessitent des mises à jour régulières pour rester pertinentes dans un écosystème Open Source en constante évolution.

OW2 Market Readiness Levels : la maturité commerciale

Principe :
Inspirée des TRL (Technology Readiness Levels) développés par la NASA, cette méthodologie se concentre sur l'évaluation de la maturité commerciale d'un projet Open Source. Elle propose une échelle progressive de 1 à 9 qui permet d'identifier clairement le stade de développement d'une solution.

Processus d'évaluation :

L'évaluation selon OW2 MRL repose sur trois piliers complémentaires.

- Le premier consiste à **vérifier la présence de 50 bonnes pratiques** réparties en 12 catégories essentielles ;
- Le deuxième s'appuie sur l'**analyse de 15 indicateurs** extraits automatiquement des environnements de développement ;
- Le troisième **examine 48 situations** liées au marché pour évaluer le positionnement commercial de la solution.

Niveaux de maturité :
Les 9 niveaux proposés par la méthodologie permettent de situer précisément chaque solution.

- Les niveaux 1 à 3 correspondent à la phase d'émergence, caractérisée par la recherche et le développement initial ;
- Les niveaux 4 à 6 représentent la phase d'adoption, allant de l'utilité vérifiée à l'adoption significative ;
- Les niveaux 7 à 9 marquent la phase de leadership, depuis l'établissement comme acteur reconnu jusqu'à la position dominante sur le marché.

Avantages :
Cette approche offre une évaluation particulièrement claire du risque commercial et de la pérennité des solutions. Son langage est spécifiquement adapté aux décideurs non techniques, facilitant ainsi la communication au sein des comités de direction. Elle fournit des indicateurs précis de viabilité à long terme, essentiels pour des investissements stratégiques.

Limites :
La méthodologie OW2 MRL accorde une attention moindre aux aspects purement techniques des solutions évaluées. Son orientation principalement B2B peut également la rendre moins pertinente pour certains contextes spécifiques, notamment dans le secteur public ou associatif.

L’approche de l’ANSSI : sécurité et souveraineté

Principe :
Développée par l'Agence Nationale de la Sécurité des Systèmes d'Information, cette approche place la sécurité et la souveraineté numérique au cœur du processus d'évaluation. Elle vise à garantir que les solutions Open Source adoptées répondent aux exigences les plus strictes en matière de cybersécurité.

Axes d'évaluation :
L'approche ANSSI s'articule autour de sept dimensions complémentaires.

- **Qualité du socle technique :** documentation, configuration sécurisée, standards ouverts ;
- **Bonnes pratiques de développement :** conformité aux référentiels de sécurité, revue de code, tests ;
- **Gestion des dépendances :** inventaire (SBOM), surveillance, mise à jour ;
- **Maintien en Conditions de Sécurité (MCS) :** gestion des vulnérabilités, correctifs ;
- **Maintien en Conditions Opérationnelles (MCO) :** pérennité des mainteneurs, mises à jour ;
- **Audit et support externe :** audits de sécurité, contrats de support ;
- **Soutien au projet :** réponse aux besoins du projet pour sa pérennisation Cette approche place la sécurité et la souveraineté au cœur du processus d'évaluation.

Avantages :
Cette méthodologie garantit un niveau de sécurité conforme aux exigences réglementaires nationales et européennes. Son approche pragmatique orientée risques permet d'identifier précisément les vulnérabilités potentielles. Elle s'avère particulièrement pertinente pour les secteurs sensibles et réglementés, notamment les opérateurs d'importance vitale.

Limites :
L'approche ANSSI offre une couverture limitée des aspects fonctionnels et commerciaux des solutions évaluées. La complexité de certains critères d'évaluation peut s'avérer difficile à appréhender pour des décideurs non spécialistes de la cybersécurité.

Conclusion

Les méthodologies d'évaluation des logiciels Open Source constituent des outils décisionnels stratégiques dans un contexte où ces solutions deviennent incontournables. QSOS, OW2 MRL et l'approche ANSSI offrent des perspectives complémentaires permettant d'objectiver les décisions d'adoption et de réduire les risques associés. De ce fait, la mise en place d'une approche hybride, regroupant les 3 méthodes, permet d'adapter l'effort d'évaluation aux enjeux spécifiques de chaque contexte organisationnel, tout en couvrant l'ensemble des dimensions critiques: fonctionnelles, commerciales et sécuritaires.

Approche économique et stratégique

ROI & Open Source

Les solutions Open Source peuvent offrir un ROI (retour sur investissement en français) attractif pour plusieurs raisons :

- **Coûts initiaux réduits :** Les logiciels Open Source sont souvent gratuits ou ont des coûts d'acquisition beaucoup plus bas que les logiciels propriétaires. Cela réduit les coûts initiaux et augmente potentiellement le ROI ;
- **Flexibilité et personnalisation :** Les solutions Open Source peuvent être modifiées et adaptées aux besoins spécifiques de l'entreprise, ce qui peut améliorer l'efficacité et la productivité ;
- **Communauté et support :** Une communauté active peut fournir un support gratuit ou à faible coût, réduisant ainsi les coûts de maintenance et de support technique ;
- **Évolutivité :** Les solutions Open Source peuvent souvent être mises à l'échelle plus facilement et à moindre coût que les solutions propriétaires ;
- **Pas de coûts de licence :** L'absence de coûts de licence récurrents peut entraîner des économies substantielles à long terme ;
- **Innovation rapide :** Les projets Open Source bénéficient souvent de contributions rapides et continues de la part de développeurs du monde entier, ce qui peut accélérer l'innovation et l'amélioration du produit.

Cependant, il est important de noter que le ROI des solutions Open Source peut également être influencé par des facteurs tels que les coûts de formation, les coûts de support technique, et les ressources nécessaires pour personnaliser et maintenir le logiciel. Une évaluation complète doit prendre en compte tous ces aspects pour déterminer le véritable ROI.

Modèles économiques

Éditeurs et fournisseurs de solutions Open Source : modèles et positionnements

- **Modèles économiques et approches d'adoption**
- **Best of Breed :** utilisation de solutions Open Source communautaires (Vanilla)
- **Modèle Open Core :** solution Open Source avec des fonctionnalités payantes
- **Solutions sous souscription :** versions "Entreprise" avec support éditeur
- **Stratégie Dual Sourcing :** arbitrage entre solutions propriétaires et Open Source

Les changements de licences et les forks

Le risque principal du changement de licence d'une solution Open Source, lorsque le logiciel est développé par un seul éditeur, réside dans plusieurs facteurs clés :

- **Perte de la Communauté :** Les changements de licence peuvent aliéner la communauté des utilisateurs et des contributeurs qui ont soutenu le projet. Si la nouvelle licence est perçue comme restrictive ou contraire aux valeurs de l'Open Source, les contributeurs peuvent cesser de participer, ce qui peut ralentir le développement et l'innovation.

- **Forks et Fragmentation :** Un changement de licence peut entraîner la création de forks du projet original. Cela peut conduire à une fragmentation de la communauté et des ressources, diluant ainsi les efforts de développement et créant des versions concurrentes du logiciel.
- **Dépendance à un seul acteur :** Lorsqu'un seul éditeur contrôle le développement, il peut imposer des décisions unilatérales qui ne sont pas toujours dans l'intérêt de la communauté. Cela peut inclure des changements de licence qui restreignent l'utilisation du logiciel ou imposent des coûts.
- **Risques Juridiques :** Les utilisateurs et les entreprises qui ont intégré le logiciel dans leurs systèmes peuvent se retrouver en situation de non-conformité avec la nouvelle licence, ce qui peut entraîner des risques juridiques et des coûts de mise en conformité mais également des risques de sécurité. Chez Thales l'équipe Software Compliance Team est là pour vous aider à éviter tous ces désagréments.
- **Innovation Réduite :** La diversité des contributeurs est souvent un moteur d'innovation. Si un changement de licence décourage la participation communautaire, le projet peut souffrir d'un manque d'idées nouvelles et de perspectives variées.
- **Coûts Accrus :** Les entreprises qui dépendent du logiciel peuvent être confrontées à des coûts supplémentaires si la nouvelle licence impose des frais pour certaines utilisations ou si elles doivent migrer vers une alternative.

Ces risques peuvent avoir des impacts significatifs sur la viabilité à long terme du projet, la satisfaction des utilisateurs et l'écosystème global construit autour du logiciel.

Le fork peut aussi être une opportunité

Plusieurs exemples de fork de solution Open Source liés à des changements de licences par l'éditeur existent. On pourra citer le cas de la solution MariaDB, fork de MySQL. MariaDB a été créé en 2009 après l'acquisition de MySQL par Oracle. La communauté a créé MariaDB pour garantir que le projet reste Open Source et pour continuer à développer des fonctionnalités sans les restrictions imposées par Oracle. En 2010, la communauté OpenOffice.org a créé The Document Foundation et lancé LibreOffice, un fork d'OpenOffice.org, en réponse à des préoccupations concernant la direction prise par Oracle après son acquisition de Sun Microsystems, l'éditeur d'OpenOffice.org. Jenkins est un fork de Hudson, créé en 2011 après qu'Oracle ait pris le contrôle du projet Hudson. La communauté a décidé de créer Jenkins pour garantir que le projet reste Open Source et pour continuer à développer des fonctionnalités sans les restrictions imposées par Oracle.

Ces exemples montrent comment les forks peuvent être utilisés pour maintenir l'ouverture et la communauté autour des projets Open Source lorsque les éditeurs changent les licences ou imposent des restrictions.

Quels cas de fork récents

OpenTofu

OpenTofu est un outil d'infrastructure as code (IaC) qui permet de définir des ressources cloud et on-premises dans des fichiers de configuration lisibles par l'homme. Ces fichiers peuvent être versionnés, réutilisés et partagés, offrant un flux de travail cohérent pour provisionner et gérer l'infrastructure tout au long de son cycle de vie.

L'histoire d'OpenTofu commence le 10 août 2023, lorsque HashiCorp a annoncé un changement de licence pour ses produits, y compris Terraform, passant de la Mozilla Public License (MPL v2) à la Business Source License (BSL). Contrairement à la MPL v2, la BSL n'est pas une licence Open Source, ce qui a incité la communauté à créer une alternative Open Source. OpenTofu a été créé en réponse à ce changement de licence, en tant que fork de Terraform version 1.5.6, conservant toutes les fonctionnalités populaires de Terraform tout en introduisant des améliorations et des améliorations.

Le projet a été initialement soutenu par des entreprises telles que Gruntwork, Spacelift, Harness, Env0 et Scalr. En septembre 2023, OpenTofu est devenu un projet officiel de la Linux Foundation, garantissant son développement continu et sa disponibilité en tant que solution Open Source.

Depuis sa création, OpenTofu a connu une croissance rapide et un soutien communautaire, avec des contributions de nombreux développeurs et organisations. Le projet vise à rester fidèle à ses principes d'ouverture

et de modularité, en publiant régulièrement de nouvelles versions avec des fonctionnalités améliorées et des correctifs de bugs.

TDP - Trunk Data Platform

La plateforme Trunk Data Platform (TDP) est une distribution Hadoop Open Source, conçue pour fournir une solution centralisée et évolutive pour le stockage, le traitement et la gestion de grands volumes de données. Elle est basée sur l'écosystème Apache Hadoop et est compatible avec HDP.

L'histoire de TDP commence par des discussions entre EDF (Électricité de France) et la Direction Générale des Finances Publiques (DGFiP) au sujet de leurs plateformes Big Data. Ces discussions ont conduit à la création de TDP, une plateforme conçue pour offrir une gouvernance partagée, être accessible gratuitement et être entièrement Open Source. Le projet a été initié en 2021 et est soutenu par l'association TOSIT (The Open Source I Trust), qui regroupe EDF, la DGFiP et d'autres partenaires.

TDP a été officiellement présentée lors de divers événements, tels que le salon Big Data Paris en septembre 2023, et continue d'évoluer avec le soutien de la communauté Open Source et des contributions de diverses organisations.

OpenSearch

OpenSearch est une suite de recherche et d'analyse Open Source, sous licence Apache 2.0, qui facilite l'ingestion, la recherche, la visualisation et l'analyse des données. Elle est conçue pour être évolutive, distribuée et pilotée par la communauté, offrant une large gamme de fonctionnalités pour divers cas d'utilisation, notamment la surveillance des applications en temps réel, l'analyse des journaux et la recherche sur les sites web.

L'histoire d'OpenSearch commence en 2021, lorsque AWS a annoncé qu'elle créerait un fork d'Elasticsearch et de Kibana en réponse à un changement de licence d'Elastic NV. Ce changement a conduit à la création d'OpenSearch, une suite de recherche et d'analyse Open Source, pilotée par la communauté, qui a supprimé les marques et la télémétrie d'Elastic NV. OpenSearch a été initialement développé par AWS et a ensuite été transféré à la OpenSearch Software Foundation, une organisation technique ouverte au sein de la Linux Foundation, en septembre 2024.

La OpenSearch Software Foundation a été créée pour superviser le développement continu d'OpenSearch, avec le soutien de membres de premier plan tels qu'Amazon Web Services, SAP et Uber. Cette fondation vise à garantir que le projet reste Open Source, transparent et indépendant, tout en favorisant l'innovation et la collaboration communautaire.

Sécurité et correction des failles

L'Open Source n'est pas intrinsèquement moins sécurisé que les logiciels propriétaires. En fait, la sécurité d'un logiciel dépend de plusieurs facteurs, indépendamment de son modèle de licence. Voici quelques points à considérer :

- **Transparence du Code :** Les logiciels Open Source permettent à quiconque d'examiner leur code source. Cela signifie que les vulnérabilités peuvent être identifiées et corrigées plus rapidement par une communauté mondiale de développeurs. Les logiciels propriétaires, en revanche, reposent sur des équipes internes pour la détection et la correction des bugs.
- **Communauté et Contributions :** La communauté Open Source est souvent vaste et active. De nombreux yeux scrutent le code, ce qui peut conduire à une détection plus rapide des problèmes de sécurité. Les logiciels propriétaires dépendent des ressources de l'éditeur, qui peuvent être limitées.
- **Mises à Jour et Correctifs :** Les projets Open Source bien gérés publient régulièrement des mises à jour et des correctifs de sécurité. La rapidité de ces mises à jour peut parfois surpasser celle des logiciels propriétaires, surtout pour les logiciels moins populaires ou en fin de vie.
- **Audits de Sécurité :** Les entreprises et les organisations peuvent effectuer des audits de sécurité indépendants sur les logiciels Open Source, ce qui n'est généralement pas possible avec les logiciels propriétaires. Cela permet une évaluation plus approfondie de la sécurité du logiciel.
- **Dépendances et Chaîne d'Approvisionnement :** Que ce soit pour les logiciels Open Source ou propriétaires, la gestion des dépendances et de la chaîne d'approvisionnement logicielle est cru-

ciale. Les deux types de logiciels peuvent être affectés par des vulnérabilités dans les bibliothèques tierces qu'ils utilisent.

En résumé, la sécurité d'un logiciel dépend davantage de la qualité de son développement, de la gestion des mises à jour, et de la réactivité face aux vulnérabilités, plutôt que de son modèle de licence. Les logiciels Open Source peuvent offrir des avantages en termes de transparence et de rapidité de correction des bugs, mais cela ne garantit pas automatiquement une meilleure sécurité.

Vitesse de correction des failles

Les failles de sécurité dans les logiciels Open Source peuvent être corrigées à des vitesses variables en fonction de plusieurs facteurs, notamment la gravité de la vulnérabilité, la disponibilité des ressources et la réactivité de la communauté ou des mainteneurs du projet. Voici quelques exemples de la vitesse à laquelle certaines failles célèbres ont été corrigées :

- Découverte en Mars 2014, **Heartbleed** était une vulnérabilité présente dans la bibliothèque de cryptographie OpenSSL, qui permettait à un attaquant de lire la mémoire d'un serveur ou d'un client, récupérant ainsi des informations sensibles utilisées lors d'une communication avec le protocole Transport Layer Security (TLS). Un correctif a été rendu public en avril 2014, peu de temps après la divulgation de la vulnérabilité.
- **Log4J** est une vulnérabilité de type Zero Day qui a été découverte en décembre 2021. Elle permettait aux attaquants d'exécuter du code arbitraire sur des serveurs vulnérables, ce qui pouvait entraîner des compromissions graves des systèmes affectés. Cette faille a eu un impact mondial, affectant des milliers d'applications et de services. Même plusieurs mois après sa découverte, certaines entreprises étaient encore confrontées à des attaques basées sur cette vulnérabilité. Des correctifs ont été publiés rapidement après la divulgation de la vulnérabilité, mais l'application de ces correctifs a varié en fonction des organisations et de leurs infrastructures.

Ces exemples montrent que, bien que les failles puissent être découvertes et corrigées rapidement, l'application des correctifs peut prendre plus de temps en fonction de la complexité des systèmes affectés et de la réactivité des organisations. Il faut également noter qu'en cas de besoin, il est possible de faire appel à des entreprises partenaires comme Open Source Experts qui sont capables de mettre en place des SLA (Service Layer Agreement) sur la maintenance de logiciels Open Source.

Aspects Réglementaires

CRA – Cyber Resilliance Act

Le Cyber Resilience Act (CRA) est une réglementation de l'Union européenne visant à renforcer la cybersécurité des produits numériques. Entré en vigueur le 10 décembre 2024 (les entreprises ayant jusqu'au 11 décembre *2027* pour s'y conformer en intégrant les prescriptions), il impose des normes de cybersécurité pour tous les produits (matériels ou logiciels) comportant des éléments numériques, y compris ceux fournis en tant que services (SaaS).

Le Cyber Resilience Act (CRA) a un impact significatif sur les logiciels Open Source, car il impose des exigences spécifiques pour renforcer leur sécurité.

Voici les principaux points d'impact :

1. **Obligations pour les "stewards" (gestionnaires de projets Open Source)**
   - Les gestionnaires de projets Open Source, appelés "stewards", sont responsables de la mise en œuvre de politiques de cybersécurité pour les logiciels qu'ils maintiennent.
   - Ils doivent encourager la divulgation responsable des vulnérabilités et collaborer avec les autorités pour gérer les risques de sécurité.
2. **Exigences de sécurité renforcées**
   - Les logiciels Open Source doivent respecter des normes de cybersécurité tout au long de leur cycle de vie, comme les logiciels propriétaires.
   - Cela inclut la gestion proactive des vulnérabilités et la fourniture de mises à jour de sécurité régulières.
3. **Certification et conformité**

- Les projets Open Source devront prouver leur conformité aux exigences du CRA, ce qui pourrait nécessiter des audits de sécurité et des certifications.
- Cela pourrait représenter un défi pour les petits projets ou les développeurs individuels, qui manquent souvent de ressources pour se conformer à des réglementations complexes.

4. **Collaboration avec les autorités**
   - Les gestionnaires de projets Open Source devront travailler avec les autorités européennes pour signaler les vulnérabilités et coordonner les correctifs.
   - Cette collaboration vise à garantir que les logiciels Open Source, souvent utilisés dans des infrastructures critiques, restent sécurisés.
5. **Impact sur la communauté Open Source**
   - Le CRA pourrait encourager une meilleure gestion de la sécurité dans les projets Open Source, en imposant des pratiques plus rigoureuses.
   - Cependant, il pourrait aussi créer des tensions, car certains développeurs pourraient percevoir ces exigences comme une charge administrative trop lourde.
6. **Opportunités pour les projets Open Source**
   - Les projets Open Source qui se conforment au CRA pourraient gagner en crédibilité et en adoption, car ils seront perçus comme plus sécurisés.
   - Cela pourrait également encourager une meilleure collaboration entre les projets Open Source et les entreprises, qui recherchent des solutions sécurisées.
7. **Défis pour les petits projets**
   - Les petits projets Open Source pourraient avoir du mal à se conformer aux exigences du CRA en raison de leur manque de ressources et d'expertise en matière de sécurité.
   - Cela pourrait créer une inégalité entre les grands projets bien financés et les petits projets communautaires.

Le CRA vise à renforcer la sécurité des logiciels Open Source en imposant des normes strictes et en responsabilisant les gestionnaires de projets. Bien que cela puisse améliorer la sécurité globale, cela pourrait également poser des défis pour les petits projets et nécessiter des efforts de collaboration accrus au sein de la communauté Open Source.

NIS2

La directive NIS 2 (Network and Information Systems 2) est une législation européenne qui vise à renforcer la cybersécurité au sein de l'Union européenne. Elle remplace la directive NIS initiale et introduit des exigences plus strictes et plus larges en matière de cybersécurité.

Les principaux impacts de NIS 2 sur les solutions Open Source sont les suivants :

- **Promotion des Solutions Open Source :** NIS 2 encourage explicitement l'utilisation de solutions Open Source pour améliorer la cybersécurité. Les outils et applications de cybersécurité Open Source sont reconnus pour leur transparence, leur interopérabilité et leur capacité à favoriser l'innovation industrielle. La directive met en avant que les solutions Open Source peuvent contribuer à une plus grande ouverture et à une meilleure efficacité dans l'innovation industrielle. Elle recommande également l'utilisation de standards ouverts pour améliorer la sécurité des infrastructures.
- **Réduction des Coûts pour les PME :** NIS 2 souligne que les solutions Open Source peuvent aider les petites et moyennes entreprises (PME) à réduire les coûts liés à la mise en conformité avec les nouvelles exigences de cybersécurité. En adoptant des outils Open Source, les PME peuvent minimiser les dépenses tout en respectant les normes de sécurité imposées par la directive.
- **Communauté et Transparence :** La directive promeut une approche communautaire pour l'identification des vulnérabilités, ce qui est un principe fondamental des projets Open Source. La transparence inhérente aux solutions Open Source permet une vérification plus facile et une identification plus rapide des failles de sécurité.
- **Obligations de Conformité :** Les entreprises doivent mettre en place des mesures de gestion des risques de cybersécurité, y compris l'utilisation de solutions Open Source pour se conformer aux exigences de NIS 2. Cela inclut la mise en œuvre de politiques de sécurité, la notification des incidents et la réalisation d'audits de sécurité.

- **Impact sur les Fournisseurs de Solutions de Cybersécurité :** NIS 2 crée des opportunités pour les fournisseurs de solutions de cybersécurité, y compris ceux qui proposent des outils Open Source. Les entreprises et les organisations publiques devront se conformer aux nouvelles exigences, ce qui peut stimuler la demande pour des solutions de cybersécurité Open Source.

En résumé, NIS 2 favorise l'adoption de solutions Open Source pour améliorer la cybersécurité en Europe, en mettant en avant leur transparence, leur interopérabilité et leur potentiel de réduction des coûts, notamment pour les PME.

CVE & Open Source

Une CVE, ou "Common Vulnerabilities and Exposures" (Vulnérabilités et Expositions Communes), est un système de référencement public pour les vulnérabilités de sécurité informatique et les expositions. Chaque entrée CVE est identifiée par un numéro unique (ID CVE) et contient une description de la vulnérabilité ou de l'exposition, ainsi que des références publiques pertinentes. Les CVE jouent un rôle crucial dans la gestion de la sécurité informatique en permettant une communication claire et unifiée sur les vulnérabilités, ce qui aide les organisations à identifier, prioriser et corriger les failles de sécurité de manière plus efficace.

Il n'est pas possible de dire de manière catégorique que les logiciels Open Source présentent plus de failles de sécurité que les logiciels propriétaires, ou vice versa. La sécurité dépend davantage de la qualité du développement, des pratiques de sécurité suivies, et de la rapidité avec laquelle les vulnérabilités sont corrigées.

La gestion des CVE pour les solutions Open Source

Pour les solutions Open Source, la gestion des CVE est cruciale pour maintenir la sécurité et l'intégrité des projets.

Dans le contexte de l'Open Source, la gestion des CVE est la suivante :

- **Détection des vulnérabilités :** Les vulnérabilités peuvent être découvertes par des chercheurs en sécurité, des développeurs, ou des utilisateurs. Une fois identifiées, elles sont signalées aux mainteneurs du projet.
- **Attribution d'un CVE :** Les vulnérabilités confirmées reçoivent un identifiant CVE unique. Cela permet de suivre et de référencer la vulnérabilité de manière standardisée.
- **Notification et communication :** Les mainteneurs du projet informent la communauté des utilisateurs et des développeurs de la vulnérabilité. Cela peut se faire via des listes de diffusion, des forums, des annonces sur le dépôt de code (comme GitHub), ou des bulletins de sécurité.
- **Développement de correctifs :** Les développeurs travaillent sur des correctifs pour résoudre la vulnérabilité. Ces correctifs sont ensuite testés pour s'assurer qu'ils résolvent le problème sans introduire de nouvelles vulnérabilités.
- **Publication des correctifs :** Une fois les correctifs validés, ils sont publiés dans une nouvelle version du logiciel. Les utilisateurs sont encouragés à mettre à jour leurs installations pour bénéficier des correctifs de sécurité.
- **Suivi et maintenance :** Les mainteneurs continuent de surveiller les rapports de vulnérabilités et de publier des mises à jour de sécurité au besoin. Les outils d'analyse de sécurité peuvent également être utilisés pour détecter automatiquement les vulnérabilités dans le code.
- **Collaboration communautaire :** La communauté Open Source joue un rôle clé dans la gestion des CVE. Les contributions de développeurs du monde entier permettent de détecter et de corriger rapidement les vulnérabilités.

La gestion des CVE dans les projets Open Source repose sur la transparence, la collaboration, et la réactivité. Les mainteneurs et les contributeurs travaillent ensemble pour assurer que les logiciels restent sécurisés et fiables pour tous les utilisateurs.

Les outillages de sécurité dans les forges GitHub & GitLab

GitHub et GitLab offrent plusieurs mécanismes pour vérifier la sécurité du code source. GitHub et GitLab permettent d'intégrer des tests de sécurité dans les workflows de développement, ce qui aide à identifier et à corriger les vulnérabilités de manière proactive. Les fonctionnalités offertes par ces outils pour gérer la sécurité des codes sources hébergés dans les projets sont les suivantes :

- **Code Scanning :** Analyse automatique du code pour détecter les vulnérabilités et les erreurs de sécurité.
- **Secret Scanning :** Détection les secrets (comme les clés API, les mots de passe, etc.) qui ont été accidentellement mis dans le code.
- **Dependency Review :** Analyse des dépendances (version des librairies utilisées…) pour identifier les vulnérabilités connues sur les versions obsolètes ou non à jour.

Des outils de sécurité tiers comme Snyk, Dependabot, ou OWASP ZAP peuvent être utilisés pour des analyses plus approfondies.

Version LTS

Une version LTS (Long Term Support) d'un logiciel Open Source est une version spécifique qui reçoit des mises à jour et un support étendu pendant une période plus longue que les versions standards. Les versions LTS sont conçues pour offrir une plus grande stabilité et sécurité, ce qui les rend idéales pour les environnements de production où la fiabilité est cruciale.

Voici quelques caractéristiques clés des versions LTS :

- **Stabilité :** Les versions LTS sont généralement plus stables car elles ont été testées de manière approfondie.
- **Sécurité :** Elles reçoivent des mises à jour de sécurité régulières pour corriger les vulnérabilités.
- **Support étendu :** Le support peut s'étendre sur plusieurs années, offrant aux utilisateurs une période prolongée pendant laquelle ils peuvent compter sur des mises à jour et des correctifs.
- **Compatibilité :** Les versions LTS sont souvent utilisées dans des environnements où la compatibilité à long terme est importante, comme les infrastructures critiques et les applications d'entreprise.

Les versions LTS sont particulièrement populaires dans les distributions Linux comme Ubuntu, où elles sont utilisées par les entreprises et les organisations qui ont besoin d'une base logicielle fiable et durable.

La version ESR (Extended Support Release) de Firefox est similaire à une version LTS. Elle est conçue pour les organisations, les entreprises et les institutions qui ont besoin d'une version stable et sécurisée de Firefox sur une période prolongée.

Certaines entreprises, comme Red Hat, SUSE et Canonical, offrent des versions de leurs produits Open Source avec un support à long terme. Elles fournissent des mises à jour de sécurité, des correctifs et un support technique dans le cadre d'une offre soumise à une souscription payante. Par exemple, avec son offre payante Extended Support Maintenance (ESM), Canonical offre pour sa distribution « 10 ans de gestion des vulnérabilités pour les problèmes de sécurité critiques, élevés et moyens sélectionnés pour tous les logiciels livrés avec Ubuntu ».

Ces différentes formes de support long terme permettent aux utilisateurs de bénéficier de la stabilité et de la sécurité des logiciels Open Source sur une période assez longue, compatible avec le cycle de vie des applications en entreprise.

Bonnes pratiques (OWASP, ANSSI)

L'OWASP fournit différents outils qu'il est recommandé d'utiliser dans l'analyses du code source des solutions Open Source.

- **OWASP Top Ten :** Il s'agit d'une liste des dix risques de sécurité les plus critiques pour les applications web. Cette liste est mise à jour régulièrement et est largement utilisée par les développeurs et les professionnels de la sécurité pour évaluer et améliorer la sécurité de leurs applications.
- **OWASP Testing Guide :** Un guide complet pour tester la sécurité des applications web. Il fournit des méthodologies et des techniques pour identifier les vulnérabilités de sécurité.
- **OWASP Code Review Guide :** Un guide pour effectuer des revues de code axées sur la sécurité. Il aide les développeurs à identifier les failles de sécurité potentielles dans le code source.
- **OWASP ZAP (Zed Attack Proxy) :** Un outil open-source pour tester la sécurité des applications web. ZAP permet d'identifier automatiquement les vulnérabilités de sécurité dans les applications web.

- **OWASP Cheat Sheets :** Des guides pratiques et concis sur divers sujets de sécurité des applications. Ils fournissent des conseils et des meilleures pratiques pour sécuriser les applications web.
- **OWASP Dependency-Check :** Un outil qui identifie les vulnérabilités connues dans les dépendances d'un projet. Il aide à gérer les risques associés aux bibliothèques et frameworks tiers.
- **OWASP ModSecurity Core Rule Set (CRS) :** Un ensemble de règles pour le pare-feu d'applications web ModSecurity. Il aide à protéger les applications web contre les attaques courantes.

L'OWASP joue un rôle crucial dans la sensibilisation et l'éducation sur la sécurité des applications. Ses ressources et outils sont largement utilisés par les développeurs, les testeurs de sécurité et les organisations pour améliorer la sécurité de leurs applications web.

Rôle de l'ANSSI

L'ANSSI (Agence nationale de la sécurité des systèmes d'information, France) joue un rôle clé dans la promotion et la sécurisation des logiciels Open Source, notamment en contribuant à des projets comme Suricata et en menant des audits de sécurité sur des produits Open Source. L'ANSSI tient également des listes référentes d'outils Open Source qualifiés pour les besoins de l'administration et évalués selon des critères de sécurité.

Voici quelques-unes des principales recommandations de l'ANSSI concernant les logiciels Open Source :

- **Évaluation des Risques :**
  - Effectuer une évaluation des risques pour chaque composant Open Source utilisé. Cela inclut l'identification des vulnérabilités connues et l'évaluation de l'impact potentiel sur la sécurité.
- **Provenance et Fiabilité :**
  - Vérifier la provenance des logiciels Open Source. Utiliser des sources fiables et vérifiées pour télécharger les composants Open Source.
  - Privilégier les projets Open Source bien maintenus et soutenus par une communauté active.
- **Gestion des Vulnérabilités :**
  - Mettre en place un processus de veille sécuritaire pour suivre les vulnérabilités découvertes dans les composants Open Source utilisés.
  - Appliquer régulièrement les mises à jour de sécurité et les correctifs.
- **Analyse de Code :**
  - Utiliser des outils d'analyse statique et dynamique pour détecter les vulnérabilités dans le code Open Source.
  - Effectuer des revues de code pour identifier les failles de sécurité potentielles.
- **Intégration Sécurisée :**
  - Intégrer les composants Open Source de manière sécurisée dans les systèmes d'information. Cela inclut la configuration sécurisée et l'isolation des composants critiques.
  - Utiliser des conteneurs et des environnements virtualisés pour isoler les composants Open Source.
- **Documentation et Traçabilité :**
  - Documenter l'utilisation des composants Open Source, y compris les versions utilisées et les sources de téléchargement.
  - Maintenir une traçabilité des modifications apportées aux composants Open Source.
- **Formation et Sensibilisation :**
  - Former les équipes de développement et de sécurité sur les bonnes pratiques de sécurité pour les logiciels Open Source.
  - Sensibiliser les utilisateurs aux risques associés à l'utilisation de logiciels Open Source non sécurisés.
- **Conformité et Licences :**
  - Vérifier la conformité des licences Open Source utilisées avec les politiques internes et les réglementations applicables.
  - Assurer la compatibilité des licences Open Source avec les autres composants logiciels utilisés.

- **Tests de Sécurité :**
  - Intégrer des tests de sécurité dans les processus de développement et de déploiement des solutions Open Source.
  - Utiliser des outils de test de sécurité pour valider la robustesse des composants Open Source.
- **Plan de Réponse aux Incidents :**
  - Mettre en place un plan de réponse aux incidents pour gérer les vulnérabilités et les attaques affectant les composants Open Source.
  - Définir des procédures pour la notification et la correction rapide des vulnérabilités.

Ces recommandations visent à aider les organisations à utiliser les logiciels Open Source de manière sécurisée et à minimiser les risques associés. L'ANSSI encourage une approche proactive et rigoureuse pour la gestion de la sécurité des solutions Open Source.

Impact RH : attractivité du secteur pour le recrutement

L'Open Source constitue un puissant levier d'attractivité pour les jeunes talents. Ces derniers, habitués à collaborer de cette manière dès leur sortie de l'école, s'attendent naturellement à retrouver cette approche dans le monde professionnel. Ainsi, l'Open Source représente non seulement un moyen de les attirer, mais surtout de les fidéliser. En effet, il est essentiel de recruter de nouveaux collaborateurs, mais il serait dommage de les voir partir au bout de trois ans. Dans cette optique, l'Open Source se révèle être un excellent outil pour les inciter à nous rejoindre et pour les retenir sur le long terme.

L'Open Source présente donc plusieurs avantages pour le recrutement dans une entreprise, notamment :

1. **Accès à un vivier de talents :** Les projets Open Source attirent des développeurs passionnés et talentueux du monde entier. Les entreprises peuvent identifier et recruter des contributeurs actifs qui ont déjà démontré leurs compétences dans des projets réels.
2. **Évaluation des compétences techniques :** Les contributions à des projets Open Source permettent aux recruteurs d'évaluer directement les compétences techniques des candidats. Le code est souvent public, ce qui permet de juger de la qualité du travail, de la capacité à collaborer et de la compréhension des bonnes pratiques de développement.
3. **Engagement et passion :** Les développeurs qui contribuent à des projets Open Source montrent souvent un engagement et une passion pour leur travail. Ces qualités sont précieuses dans un environnement professionnel, car elles peuvent conduire à une plus grande productivité et innovation.
4. **Réseautage et visibilité :** Participer à des projets Open Source peut augmenter la visibilité d'une entreprise dans la communauté technologique. Cela peut attirer des candidats qui recherchent des entreprises ayant une culture de l'innovation et de la collaboration.
5. **Formation et développement :** Les projets Open Source offrent des opportunités de formation continue. Les développeurs peuvent apprendre de nouvelles technologies, méthodologies et meilleures pratiques en travaillant sur des projets Open Source.
6. **Innovation et collaboration :** L'Open Source favorise une culture de l'innovation et de la collaboration. Les entreprises qui adoptent ces valeurs peuvent attirer des talents qui recherchent un environnement de travail dynamique et collaboratif.
7. **Réduction des coûts de recrutement :** En identifiant des talents via des contributions Open Source, les entreprises peuvent réduire les coûts associés aux processus de recrutement traditionnels, tels que les frais d'agence ou les coûts de publicité.
8. **Prémiumisation de la marque Thales :** la publication de projets et de solution en Open Source démontre les compétences de l'entité qui publie et peut servir d'attracteur vers les produits de Thales.

En résumé, l'Open Source peut être un atout stratégique pour le recrutement, en permettant aux entreprises d'attirer des talents qualifiés et passionnés tout en renforçant leur image dans la communauté technologique.

Recrutement et attractivité

L'utilisation de l'Open Source par une entreprise peut avoir un impact significatif sur son recrutement RH, particulièrement dans le cadre de l'attraction des talents. En effet les développeurs et les professionnels de l'informatique sont souvent attirés par les entreprises qui utilisent et contribuent à des projets Open Source.

Il est donc important de préciser dans les fiches de poste si des solutions Open Source sont utilisées, si le collaborateur sera amené à contribuer et participer à l'écosystème Open Source dans le cadre de ses activités professionnelles.

Mindset des candidats

Il y a une vraie valeur à avoir participé (voire créé) une communauté ou un projet Open source. Les candidats qui font part de leurs implications dans un projet ou une communauté Open Source sur leur CV ont une valeur plus grande. L'Open Source et ses mindsets sont une évolution de l'industrie du logiciel et le fait que le candidat possède déjà les bonnes pratiques est un plus. L'expérience acquise dans leurs contributions à l'Open Source sera précieuse pour Thales.

Enfin il est également possible pour l'employeur potentiel d'aller voir les codes publiés par le candidat et de jauger et juger la qualité de ce qu'il a produit.

Fidélisation

Les collaborateurs ont besoin de perspectives et de pouvoir se projeter dans leur carrière au sein d'une entreprise. Les projets Open Source permettent aux employés de développer et de maintenir des compétences techniques, leur permettant de rester à la pointe des technologies. Cela peut augmenter leur satisfaction professionnelle et leur engagement envers l'entreprise.

L'usage de solution Open Source mais surtout la participation à la création et l'amélioration de solutions Open Source donne un sens complémentaire et important au travail des collaborateurs.

Image de marque

L'usage de l'Open Source mais surtout la contribution à l'écosystème Open Source, avec une communication à ce sujet, améliore la réputation de l'entreprise et attire des candidats de haute qualité.

Collaborer à l'écosystème Open Source a un impact très positif sur l'image d'une entreprise pour plusieurs raisons :

- **Renforcement de la réputation :** Les entreprises qui contribuent activement à des projets Open Source sont souvent perçues comme des leaders technologiques et des innovateurs. Cela peut améliorer leur réputation auprès des clients, des partenaires et des talents potentiels.
- **Attraction des talents :** Les développeurs et les professionnels de l'informatique sont souvent attirés par les entreprises qui soutiennent et contribuent à l'Open Source. Cela peut aider à attirer et à retenir des talents de haute qualité.
- **Transparence et confiance :** L'Open Source favorise la transparence et la confiance. Les entreprises qui adoptent ces principes peuvent renforcer la confiance de leurs clients et partenaires, ce qui peut améliorer leur image de marque.
- **Innovation et leadership technologique :** En contribuant à l'Open Source, les entreprises peuvent démontrer leur engagement envers l'innovation et le leadership technologique. Cela peut les positionner comme des acteurs clés dans leur secteur.
- **Responsabilité sociale :** Collaborer à l'écosystème Open Source peut être vu comme une forme de responsabilité sociale. Les entreprises peuvent montrer qu'elles sont engagées dans le partage des connaissances et le développement de solutions ouvertes et accessibles.
- **Visibilité et marketing :** Les contributions à des projets Open Source peuvent offrir une visibilité accrue à l'entreprise. Les projets Open Source sont souvent largement utilisés et reconnus, ce qui peut améliorer la notoriété de l'entreprise.
- **Collaboration et partenariats :** En participant à l'écosystème Open Source, les entreprises peuvent établir des collaborations et des partenariats avec d'autres organisations, ce qui peut renforcer leur réseau et leur influence dans l'industrie.
- **Engagement communautaire :** Les entreprises qui s'engagent dans l'Open Source peuvent bénéficier d'un fort soutien de la communauté. Cela peut renforcer leur image en tant qu'entreprise collaborative et orientée vers la communauté.

En résumé, collaborer à l'écosystème Open Source peut renforcer la réputation, attirer des talents, favoriser la transparence et la confiance, démontrer l'innovation et le leadership technologique, et améliorer la visibilité et les partenariats de l'entreprise, tout en renforçant son engagement communautaire.

Intelligence Artificielle & Open Source

Ce qu'il faut retenir (Points clés pour un décideur)
L'Open Source Initiative (OSI) a proposé une définition stricte de l'IA Open Source. Cette vision, qui exige que les jeux d'entraînement soient eux aussi Open Source, a suscité de nombreuses réactions, car elle remet en question plusieurs modèles dits "open weights", mais qui ne répondent pas aux critères d'ouverture.

Introduction

Dans le domaine de l'intelligence artificielle, les technologies Open Source offrent des outils puissants et accessibles pour développer des applications robustes. Le domaine de l'Open Source offre un ensemble d'assets Open Source, des modèles de langage étendu (LLM), de frameworks de développement d'interfaces utilisateur, outils essentiels pour accélérer la création d'applications d'IA au sein des S.I. d'enterprises.

I.A. Open source : la définition par l'OSI

L'Open Source Initiative (OSI), organisme de référence pour définir ce qu'est l'Open Source (notamment les licences conformes), a récemment proposé une définition stricte de l'IA Open Source[5].

Sur le principe des logiciels libres, dans sa définition, l'OSI exige d'une IA Open Source qu'elle offre quatre libertés à ses utilisateurs :

- Utiliser le système à n'importe quelle fin et sans avoir à demander la permission.
- Étudier le fonctionnement du système et inspecter ses composants.
- Modifier le système dans n'importe quel but, y compris pour changer ses résultats.
- Partager le système pour que d'autres puissent l'utiliser, avec ou sans modifications, dans n'importe quel but.

Dit autrement,

- L'outil est-il ouvert/Open Source ?
  - Son code, son algorithme ?
  - Ses jeux de données ?
  - Ses interfaces et applications ?
- D'où viennent les données ?
  - Sources volontaires, cédées, accaparées ?
  - Sources libres ou propriétaires ?

Un modèle est réellement Open Source si :

- il est disponible sous une licence d'usage sans restriction,
- sa méthodologie d'entraînement est fournie en toute transparence,
- son data set est fourni sous une licence libre.

A noter que dans cette définition de l'OSI, il n'y a pas d'obligation de donner les scripts d'entraînement ni d'expliquer comment l'IA a été entraînée.

Model Openness Framework (MOF) de la Linux Fundation

Linux Foundation AI & Data Foundation

La Linux Foundation AI & Data Foundation (LF AI & Data) est une organisation parapluie sous l'égide de la Linux Foundation, dédiée à soutenir et à promouvoir l'innovation Open Source dans les domaines de l'intelligence artificielle (IA), de l'apprentissage automatique (ML), de l'apprentissage profond (DL) et des données.

5 https://opensource.org/ai/open-source-ai-definition

La méthodologie Model Openness Framework (MOF)

Sur le principe des méthodologies d'évaluation des solutions Open Source, le Generative AI Commons de la Linux Fundation AI & Data Foundation a conçu et développé le Model Openness Framework (MoF), un système complet d'évaluation et de classification de l'exhaustivité et de l'ouverture des modèles d'apprentissage automatique. Ce cadre évalue quels composants du cycle de vie du développement du modèle sont rendus publics et sous quelles licences, garantissant ainsi une évaluation objective.

L'objectif est d'offrir un outil simple pour évaluer les modèles d'apprentissage automatique par rapport au cadre du MOF. Cet outil aide les utilisateurs à comprendre quels sont les composants inclus dans chaque modèle et les licences associées à ces composants, en clarifiant ce qui peut et ne peut pas être fait avec le modèle et ses composants.

Le MOT présente aux utilisateurs 16 questions sur leur modèle. Les utilisateurs doivent fournir des réponses détaillées pour chaque question. Sur la base de ces données, l'outil calcule un score, classant l'ouverture du modèle sur une échelle de 1, 2 ou 3.

Impact de l'IA sur l'Open source

L'émergence et la démocratisation de l'IA a bouleversé toute l'industrie du logiciel et les solutions Open Source. Les solutions Open Source intègrent de plus en plus des fonctionnalités d'IA en exploitant les API des solutions d'IA existantes. Cette intégration fait désormais parti des feuilles de routes et des évolutions de ces solutions.

Hugging Face

La nature collaborative de l'Open Source favorise l'innovation en IA. Les développeurs du monde entier peuvent contribuer à des projets Open Source, partager des idées, et améliorer continuellement les fonctionnalités liées à l'IA. Des plateformes comme Hugging Face facilitent cette collaboration en permettant aux développeurs de partager du code, de signaler des problèmes, et de proposer des améliorations.

Hugging Face[6] est une plateforme collaborative de référence dans le domaine de l'intelligence artificielle, offrant des outils et des modèles avancés pour des applications variées. Elle met à disposition une vaste collection de modèles d'apprentissage automatique et de jeux de données, permettant aux développeurs et aux chercheurs d'accéder à des ressources de pointe pour leurs projets d'IA.

Focus sur l'écosystème de l'IA, Machine Learning, et Data Science

Machine Learning

Le Machine Learning (ML) est un sous-ensemble de l'intelligence artificielle (IA) qui se concentre sur le développement d'algorithmes et de modèles statistiques permettant aux systèmes informatiques d'effectuer des tâches complexes sans instructions explicites. Les systèmes de ML s'appuient sur des modèles et des inférences pour analyser de grandes quantités de données, identifier des motifs et produire des résultats informés. Le ML est une composante clé de l'IA qui permet aux machines d'apprendre et de s'améliorer à partir de données, tandis que l'IA englobe une gamme plus large de technologies visant à imiter l'intelligence humaine.

Il existe de nombreux outils de Machine Learning en Open Source, les plus connus étant :

- **Scikit-learn :** Une bibliothèque Python Open Source pour le Machine Learning et l'analyse de données. Elle offre des algorithmes efficaces pour la classification, la régression et le clustering.
- **TensorFlow :** Une plateforme Open Source populaire pour le Machine Learning et le Deep Learning, développée par Google. Elle est largement utilisée pour créer et déployer des modèles de ML sur diverses plateformes et appareils.

6 https://huggingface.co/

- **PyTorch :** Une bibliothèque Open Source pour le Machine Learning, particulièrement appréciée pour sa flexibilité et sa capacité à gérer les calculs dynamiques. PyTorch est soutenue par une communauté active et est utilisée par des entreprises comme Facebook et Tesla.

Scikit-learn / Probable

Scikit-learn[7] est une bibliothèque Open Source en Python conçue pour le machine learning. Elle fournit des outils simples et efficaces pour l'analyse de données et le développement de modèles prédictifs.

Voici quelques-unes de ses principales caractéristiques :

- **Simplicité d'utilisation :** Scikit-learn est conçu pour être facile à utiliser, même pour les débutants en machine learning. Il offre une interface cohérente et intuitive pour les différentes étapes du processus de modélisation.
- **Large gamme d'algorithmes :** La bibliothèque inclut une vaste collection d'algorithmes de machine learning, couvrant la régression, la classification, le clustering, la réduction de dimensionnalité, la sélection de caractéristiques, et bien plus encore.
- **Interopérabilité :** Scikit-learn est conçu pour fonctionner de manière transparente avec d'autres bibliothèques Python populaires telles que NumPy, SciPy, et Pandas, ce qui facilite l'intégration dans les workflows de données existants.
- **Documentation complète :** Scikit-learn est bien documentée, avec des exemples de code, des tutoriels et une documentation détaillée pour chaque algorithme et fonctionnalité.
- **Communauté active :** En tant que projet Open Source, Scikit-learn bénéficie d'une communauté active de contributeurs et d'utilisateurs, ce qui garantit des mises à jour régulières et un support continu.
- **Performance :** Bien que Scikit-learn soit conçue pour être simple à utiliser, il est également optimisé pour les performances, ce qui le rend adapté à des tâches de machine learning de taille moyenne à grande.

En résumé, Scikit-learn est une bibliothèque puissante et polyvalente pour le machine learning en Python, offrant une large gamme d'algorithmes et d'outils pour l'analyse de données et le développement de modèles prédictifs.

Les LLM Open Source

Un LLM, ou Large Language Model (Modèle de Langage de Grande Taille en français), est un type de modèle d'intelligence artificielle conçu pour comprendre et générer du langage humain. Ces modèles sont entraînés sur de vastes quantités de texte pour apprendre les motifs et les structures du langage, ce qui leur permet de générer des réponses cohérentes et contextuellement appropriées à une variété de questions ou de demandes.

Les LLM peuvent être utilisés dans diverses applications, telles que les chatbots, la traduction automatique, la génération de texte, et bien plus encore. Ils sont capables de comprendre et de répondre dans plusieurs langues et peuvent même effectuer des tâches complexes comme résumer des textes ou répondre à des questions factuelles.

Frameworks pour interfaces conversationnelles

De nombreux frameworks Open Source permettent la création d'interfaces utilisateur de chatbot ou la construction d'applications conversationnelles de façon efficace et rapide.

Autres ressources Open Source

D'autres ressources Open Source, incluant des bibliothèques, API, et services utiles permettent de créer une application d'IA performante.

L'intelligence artificielle (IA) peut aider les développeurs de plusieurs façons, notamment en automatisant les tâches répétitives, en fournissant des suggestions pour améliorer le code et la conception d'une application,

7 https://probabl.ai/

en optimisant les images et les vidéos pour une meilleure performance d'un site web, et en générant de la documentation de qualité ou des chatbots personnalisés.

IA et développement de logiciels

Avec l'intégration croissante de l'intelligence artificielle (IA) dans le développement de logiciels, de nouveaux défis se posent dans le domaine de la conformité des logiciels libres. Les systèmes d'IA conçus pour générer du code sont entraînés sur de grands ensembles de données, qui comprennent souvent une variété de codes OSS.

Par conséquent, il est probable que l'IA, lorsqu'elle génère un nouveau code, reproduise des parties d'un code Open Source original. Les licences copyleft exigent que les nouveaux logiciels basés sur des OSS soient publiés sous la licence copyleft. Par conséquent, l'utilisation et la commercialisation d'un code généré par l'IA peuvent présenter le risque de violer les licences OSS correspondantes, ce qui entraîne des problèmes de sécurité.

Il convient donc d'utiliser des outils d'audit statique de code source afin de vérifier la conformité du code source généré, l'équipe Software Compliance Team est outillée et disponible pour vous aider sur ces sujets.

Les modèle spécialisés (Génération de code)

La problématique est que le code généré par les IA n'est pas exempt de bug. Au contraire, le code créé avec l'IA génère plus de bugs et par conséquence, plus de maintenance et plus de retard. Référence : rapport DORA de 2024 (rapport de Google sur l'utilisation de l'IA).

Il y a donc nécessité de tester rigoureusement le code et de corriger les éventuels problèmes avant la mise en production, car le code généré par l'IA peut être imparfait ou non optimisé. L'IA est donc là pour assister et non remplacer l'expertise des développeurs.

GitHub Copilot

GitHub Copilot est un assistant de code alimenté par l'IA qui aide les développeurs à écrire et à déboguer du code. Il peut suggérer des éléments d'autocomplétion lorsque l'on commence à rédiger du code, mais également répondre à des requêtes textuelles qui décrivent ce que l'on souhaite que le code réalise comme action. Alimenté par un modèle d'IA générative conçu par GitHub, OpenAI et Microsoft, cet assistant IA est disponible en extension pour Visual Studio Code, Neovim, JetBrains, Azure Data Studio…

Enjeux et intérêts stratégiques pour Thales

Pour les entreprises

L'intelligence artificielle (IA) présente de nombreux enjeux et intérêts stratégiques pour les entreprises.

Voici quelques-uns des principaux aspects à considérer :

1. **Compétitivité :** L'IA peut offrir un avantage concurrentiel en améliorant l'efficacité opérationnelle, en réduisant les coûts et en augmentant la productivité.
2. **Innovation :** L'IA permet de développer de nouveaux produits et services, ou d'améliorer ceux existants, en exploitant des données et des analyses avancées.
3. **Personnalisation :** Les entreprises peuvent utiliser l'IA pour offrir des expériences client personnalisées, ce qui peut améliorer la satisfaction et la fidélité des clients.
4. **Prise de Décision :** L'IA peut aider à prendre des décisions plus éclairées grâce à l'analyse de grandes quantités de données en temps réel.
5. **Automatisation :** L'automatisation des tâches répétitives permet de libérer du temps pour des activités à plus forte valeur ajoutée.
6. **Gestion des Risques :** L'IA peut être utilisée pour identifier et atténuer les risques, qu'ils soient financiers, opérationnels ou liés à la sécurité.

Intérêts Stratégiques :

1. **Amélioration de l'Expérience Client :** Les chatbots et les assistants virtuels peuvent offrir un service client 24/7, améliorant ainsi l'expérience globale.
2. **Optimisation des Processus :** L'IA peut optimiser les chaînes d'approvisionnement, la gestion des stocks et d'autres processus opérationnels.
3. **Analyse Prédictive :** Les entreprises peuvent utiliser l'IA pour prévoir les tendances du marché, les comportements des clients et d'autres variables importantes.
4. **Sécurité et Conformité :** L'IA peut aider à détecter les fraudes, les cybermenaces et à assurer la conformité réglementaire.
5. **Développement Durable :** L'IA peut contribuer à des pratiques plus durables en optimisant l'utilisation des ressources et en réduisant les déchets.
6. **Talent et Compétences :** Investir dans l'IA peut attirer des talents spécialisés et encourager une culture d'innovation au sein de l'entreprise.

Cependant, l'adoption de l'IA comporte également des défis, tels que les préoccupations éthiques, la protection des données et la nécessité de former les employés à utiliser ces nouvelles technologies. Les entreprises doivent donc adopter une approche équilibrée pour maximiser les avantages tout en gérant les risques associés.

Thales cofondateur de Confiance.IA

Confiance.IA est une fondation européenne pour une IA de confiance. Cette organisation à but non lucratif a été créée par des leaders industriels dont Thales. Sa mission est de fournir à l'industrie une méthodologie et des outils Open Source de pointe, permettant la conception de systèmes basés sur l'IA qui peuvent être dignes de confiance et conformes aux réglementations.

La fondation vise à être une force motrice derrière une stratégie européenne ambitieuse pour une IA industrielle et responsable. Son ambition est de propulser l'Europe au premier plan de l'innovation en matière d'IA de confiance, en faisant de ses méthodologies et outils une référence internationale et en soutenant ainsi l'adoption plus large d'une IA responsable dans l'industrie.

La fondation s'adresse à tous les acteurs engagés dans le développement et l'adoption d'une IA industrielle et responsable, notamment les industriels, les chercheurs et laboratoires, les start-ups et PME technologiques, ainsi que les organismes de normalisation et les régulateurs. En rejoignant la fondation, ces acteurs accèdent à un réseau privilégié pour collaborer, innover et contribuer activement à façonner l'avenir de l'IA industrielle en Europe.

La fondation a quatre missions principales pour une IA de confiance :

- Diriger et élargir la communauté dédiée à l'ingénierie de l'IA industrielle et responsable, en forgeant des liens étroits avec diverses initiatives.
- Garantir la conformité réglementaire et contribuer aux normes, en veillant à ce que les méthodologies et outils soient conformes à l'AI Act et à d'autres réglementations.
- Gérer et distribuer les actifs Open Source résultant du programme Confiance.ai, offrant aux industriels une gamme de cours adaptés à chaque type d'utilisation.
- Soutenir la transition vers une IA responsable en co-concevant des formations pour de nouveaux métiers et en aidant à construire les compétences des futurs experts en IA de confiance.

Open hardware & IA chez Thales

Dans le cadre ses activités de matériel embarqué, une branche entière des activités liées à l'IA se spécialisent sur les problématiques rencontrées. Pour ce faire, les équipes travaillent et collaborent en mode co-design, entre les experts en architectures (RISC-V) et ceux en algorithmie de l'IA.

Bien que cette démarche nécessite le développement de nouvelles méthodes et algorithmes spécifiques, cela permet d'optimiser simultanément les différents aspects plutôt que de les traiter de manière séquentielle.

Open data & IA

De part l'importance d'avoir des données avec une "vérité terrain" pour entraîner et valider les modèles d'IA, l'open data est intéressant. En effet, les modèles d'IA nécessitent des données pour être entraînés, et l'open data fournit une source précieuse de données accessibles et utilisables. L'open data peut ainsi aider à obtenir des ensembles de données de haute qualité et bien labellisés, essentiels pour le développement de solutions d'IA fiables et robustes.

Sur les mêmes principes que l'Inner source (partage en interne de code source logiciel), il existe la possibilité de faire un partage des données en interne, similaires à l'open data, mais de manière restreinte et sécurisée. Cela permet à différents départements et équipes de Thales d'accéder à des ensembles de données communs pour leurs projets, tout en respectant les contraintes de confidentialité et de sécurité.

Evolution des licences et impact, le cas de la bibliothèque YOLO

YOLO (You Only Look Once) est une bibliothèque Open Source utilisée pour la détection d'objets en temps réel. Elle est particulièrement connue pour sa rapidité et sa précision dans l'identification et la localisation d'objets dans des images ou des vidéos. YOLO utilise des réseaux de neurones convolutifs (CNN) pour effectuer cette tâche, ce qui en fait un outil puissant dans le domaine de la vision par ordinateur. YOLO est une application spécifique de l'IA, plus précisément du machine learning et du deep learning.

La bibliothèque YOLO a connu plusieurs versions au fil des années, et les licences associées à ces versions ont également évolué.

La version 1 de cette bibliothèque était une licence propriétaire, permettant la gratuité. La version 2 correspond au passage à une licence assez simple (quelques lignes). Avec la version 3, le code source du projet passe sous une licence plus officielle et reconnue du monde de l'Open Source, à savoir la licence GPLv3 (GNU General Public License version 3). Cette licence est copyleft, ce qui signifie que toute modification ou extension du code doit également être publiée sous la même licence. La version 5 est quant à elle publiée sous la licence GNU AGPL-3.0 (Affero General Public License version 3.0). Cette licence est similaire à la GPLv3 tout en incluant des dispositions supplémentaires pour couvrir les cas d'utilisation en mode SaaS.

La dernière licence Open Source utilisée permet à la communauté de contribuer au développement de YOLO, d'utiliser le code pour leurs propres projets, et de partager ses modifications avec d'autres. Cependant, il est important de respecter les termes de la licence, notamment en ce qui concerne la redistribution et la modification du code source.

=> Ces changements de licences au fil des versions illustrent bien la nécessité et la problématique de faire un suivi et une veille des évolutions des projets, librairies et autres logiciels utilisés.

Programme Open Source chez Thales

« L'Open Source est le meilleur moyen de stimuler la créativité et de garantir la performance, la sécurité et la maintenabilité des produits et services de Thales »
Daniel GLAZMAN, VP Software Technologies chez Thales

Ce qu'il faut retenir
L'Open Source est un pilier stratégique pour le groupe Thales.
1 Notre état d'esprit vis-à-vis de l'Open Source est d'utiliser / Contribuer / Publier.
2 Tous les collaborateurs sont encouragés à contribuer : partager les assets, contribuer aux projets Open Source, soumettre un ticket, participer à un groupe de travail.
3 Une gouvernance et un processus outillé sont en place pour aider les collaborateurs
4 Chaque asset Open Source de Thales doit être publié dans notre organisation GitHub Thales
5 L'équipe Open Source est disponible pour vous accompagner : oss@thalesgroup.com

L'Open Source Hardware chez Thales

La démarche de Thales est en ligne avec la politique européenne volontariste en faveur de la constitution d'un écosystème Open Hardware souverain, permettant de répondre à un double défi : favoriser les capacités de conception et de fabrication de microprocesseurs et faire progresser ces technologies sur les marchés actuels et à venir tels que l'automobile, l'automatisation industrielle, les communications, les infrastructures de données, la santé ou encore la défense.

Alors que la Commission européenne a établi avec le Chips Act une feuille de route en faveur du développement des capacités de production des semi-conducteurs de dernière génération et durables, l'Open Hardware constitue le nouvel enjeu de souveraineté et de résilience pour permettre à l'Europe de se protéger des perturbations des chaînes d'approvisionnement en matériels.

Pourquoi Thales investit-il dans RISC-V ?

RISC-V est un jeu d'instructions ouvert qui connaît un attrait croissant depuis plusieurs années. Il permet d'exécuter des logiciels complexes sur un processeur, sans dépendance vis-à-vis d'une solution propriétaire, en diminuant les coûts d'accès et en permettant aux clients de regagner leur souveraineté technologique.

Thales investit dans RISC-V pour plusieurs raisons:

- Présence d'une forte communauté Open Source
- Souveraineté du modèle
- Sécurité et sûreté
- SWaP et personnalisation

RISC-V dispose d'un vaste écosystème offrant une compatibilité au travers de ses différentes implémentations. Il n'y a pas d'enfermement propriétaire (Vendor Locking), ce qui facilite les opportunités commerciales pour du support et de la personnalisation. Le modèle est à l'état de l'art des processeurs et permet de grande performance.

- Thales apporte son expertise à la conception de microprocesseurs sûrs et sécurisés
- Thales ambitionne de fédérer les industriels et académiques impliqués dans ce domaine
- L'enjeu de cette révolution touche la plupart des systèmes embarqués dans l'aéronautique, le spatial, l'automobile, le ferroviaire, la sécurité et la défense.

Désormais membre de la RISC-V Foundation, Thales affirme ainsi sa volonté de faire avancer l'adoption et la mise en œuvre des architectures matérielles libres et ouvertes basées sur des processeurs RISC-V. C'est

une opportunité pour Thales de devenir un acteur majeur d'une nouvelle ère dans la conception des microprocesseurs. L'enjeu est important puisque l'Open Source dans le domaine du matériel s'inspire de la philosophie et du succès qu'a connu Linux dans le monde du logiciel.

Fort de son expertise en sécurité et sûreté des systèmes critiques embarqués, Thales vise à contribuer au sein de la communauté RISC-V au développement des meilleures pratiques de sûreté avec tous les acteurs industriels et académiques. Cela portera sur l'amélioration de la sûreté pour les dispositifs Internet des Objets, les systèmes embarqués et les implémentations d'apprentissage automatique.

RISC-V s'est distinguée ces dernières années dans l'amélioration de la sécurité des microprocesseurs contre les cyber-menaces. L'expertise de Thales dans ce domaine apportera en plus la sûreté de fonctionnement. Le Groupe collaborera avec les communautés Open Source pour concevoir des microprocesseurs compatibles avec les exigences des futurs systèmes critiques.

En combinant une approche ouverte du matériel et du logiciel, Thales et la communauté RISC-V ouvrent de nouvelles perspectives dans la conception des systèmes de missions critiques présents dans tous les domaines, notamment l'aéronautique, le spatial, l'automobile, le ferroviaire, la sécurité et la défense.

Les initiatives de Thales sont pleinement alignées avec les objectifs de la politique européenne visant à :

- créer un écosystème de matériel Open Source souverain pour renforcer les capacités de conception et de fabrication de microprocesseurs en Europe
- promouvoir l'utilisation de ces technologies dans les marchés actuels et futurs, y compris l'industrie automobile, l'automatisation industrielle, les communications, l'infrastructure de données, la santé et la défense.

Alors que le *Chips Act* proposé par la Commission européenne offre une feuille de route pour une production durable de semi-conducteurs de dernière génération, le matériel Open Source aide à garantir la souveraineté technologique et la résilience afin de protéger l'Europe des perturbations dans les chaînes d'approvisionnement en matériel.

L'implication de Thales dans l'OpenHW Group

L'OpenHW Group est une organisation à but non lucratif qui vise à favoriser l'adoption de matériel Open Source en fournissant une infrastructure et des ressources pour le développement de cœurs de processeurs basés sur l'architecture RISC-V. L'objectif est de créer une communauté collaborative où les entreprises, les universitaires et les développeurs peuvent contribuer à la conception et à l'amélioration de matériel Open Source.

Thales est impliqué dans l'OpenHW Group de plusieurs manières. L'entreprise soutient activement le développement de l'écosystème Open Source pour les processeurs RISC-V. Thales a organisé et sponsorisé des concours étudiants pour encourager l'innovation dans ce domaine, comme le Second National RISC-V Student Contest, où des étudiants ont été récompensés pour leurs solutions visant à réduire la consommation d'énergie du processeur CORE-V CVA6.

De plus, Thales travaille sur des solutions de sécurité pour les processeurs Open Source afin de répondre aux besoins des clients dans les secteurs de l'espace, de l'aérospatiale et de la cybersécurité. Les initiatives de Thales sont alignées sur les objectifs de la politique européenne de création d'un écosystème open hardware souverain pour renforcer les capacités de conception et de fabrication de microprocesseurs en Europe.

Thales contribue également à des projets spécifiques liés à l'OpenHW Group, comme le développement de scripts pour générer des chaînes d'outils pour le CPU CVA6, ce qui facilite la reproductibilité des environnements de travail pour le flux de vérification de CVA6.

L’Open Source Software chez Thales

Comment l'Open Source est mis en œuvre chez Thales ?

L'initiative Thales Open Source a été lancée en 2020 à l’initiative de la Direction Technique du Groupe, les principaux objectifs étaient alors les suivants:

- Devenir un acteur Open Source de premier plan
- Déployer un processus outillé Open Source commun dans toutes les GBUs
- Développer les communautés logicielles et matérielles autour de l’Open Source

La stratégie pour appliquer le modèle Open Source et changer l'état d'esprit au sein de Thales sur le long terme s'est faite :

- En s'appuyant sur le succès de Thales Inner Source
- En fournissant un processus et des outils uniques pour l'Open Source
- En facilitant la communication entre tous les contributeurs

Le 10 décembre 2025, Thales a reçu le prix de la « **meilleure stratégie Open Source** » au salon **Open Source Experience**. Décerné par le **Conseil national du logiciel libre (CNLL)**, ce prix reconnaît le travail mené depuis cinq ans par la Direction Technique du Groupe.
Il récompense principalement :

- la transformation structurelle et méthodique engagée pour promouvoir l’Open Source ;
- la maturité des processus internes ;
- l’impact réel dans la communauté Open Source ;
- l’engagement des équipes à travers l’entreprise.

Ce prix confirme l’orientation de Thales vers l’ouverture, la collaboration et l’innovation dans le développement logiciel.


Sébastien Lejeune, Thales Open Source Community Manager © OHE! William JEZEQUEL

Gouvernance et processus Thales Open Source

Depuis 2020, Thales a mis en place son Open Source Program Office pour encourager les pratiques Open Source dans tous les secteurs d'activité. Avec l'aide de l'équipe Software Compliance, chaque collaborateur est accompagné pour fournir des ressources Open Source de qualité optimale et pour qu'il gère soigneusement les risques associés, en particulier les risques juridiques (IP, licences, export control) et les risques de sécurité (vulnérabilités, CVE).

Différents profils interviennent dans cette gouvernance

- **des experts techniques**
- **des experts juridiques**
- **des managers**
- **des spécialistes de la conformité**

Le processus outillé couvre eux cas d'utilisation principaux de l'Open Source:

- **publication :** lorsqu'un collaborateur, une équipe ou un projet souhaite partager un asset Thales en Open Source
- **contribution :** lorsqu'un collaborateur, une équipe ou un projet souhaite contribuer à un projet Open Source existant, la plupart du temps pour y corriger un fait technique.

Pour ces deux cas d'utilisation, il faut d'abord soumettre une requête de publication/contribution qui consiste en un formulaire dans lequel sont décrits les objectifs, la licence souhaitée, qui est l'équipe en charge et des questions qui aideront l'équipe Open Source de Thales à guider au mieux le porteur de la demande tout au long du processus.

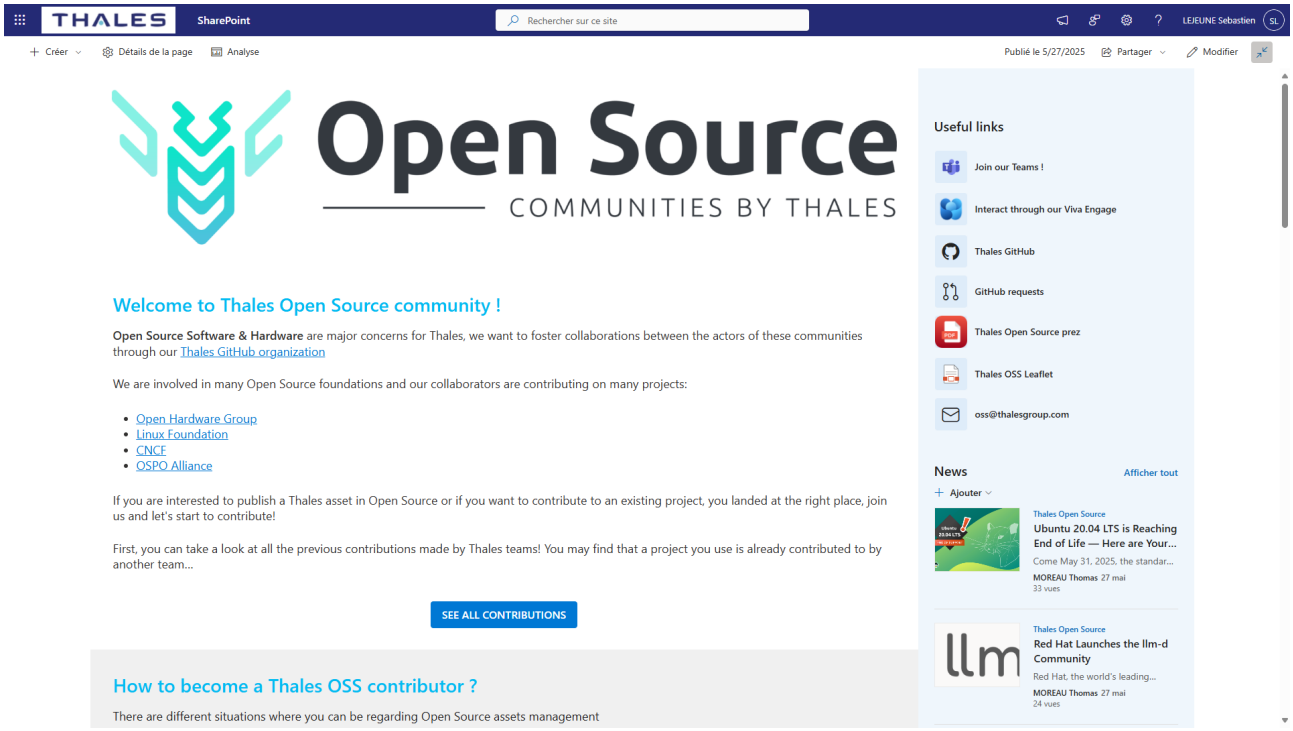
Ensuite, la requête doit être approuvée par :

- **un manager** pour vérifier l'alignement avec la stratégie de l'entreprise
- **un expert technique** pour examiner le code et l'architecture
- **l'équipe de conformité logicielle** pour assurer la conformité du logiciel libre en ce qui concerne la propriété intellectuelle et les cyber-risques
- **un expert juridique** pour valider le choix de licence Open Source.

Une fois la demande approuvée, une invitation est faite sur l'organisation GitHub Thales afin de pousser le code dans un dépôt qui sera visible publiquement une fois toutes les approbations obtenues.

Ce processus est le même pour toutes les GBUs de Thales et les pays qui souhaitent interagir avec l'écosystème Open Source au nom de Thales. Il vise à garantir la qualité de toutes nos contributions car, en tant que leader mondial de la sécurité, nous accordons une attention particulière aux questions de conformité.

Outils de collaboration



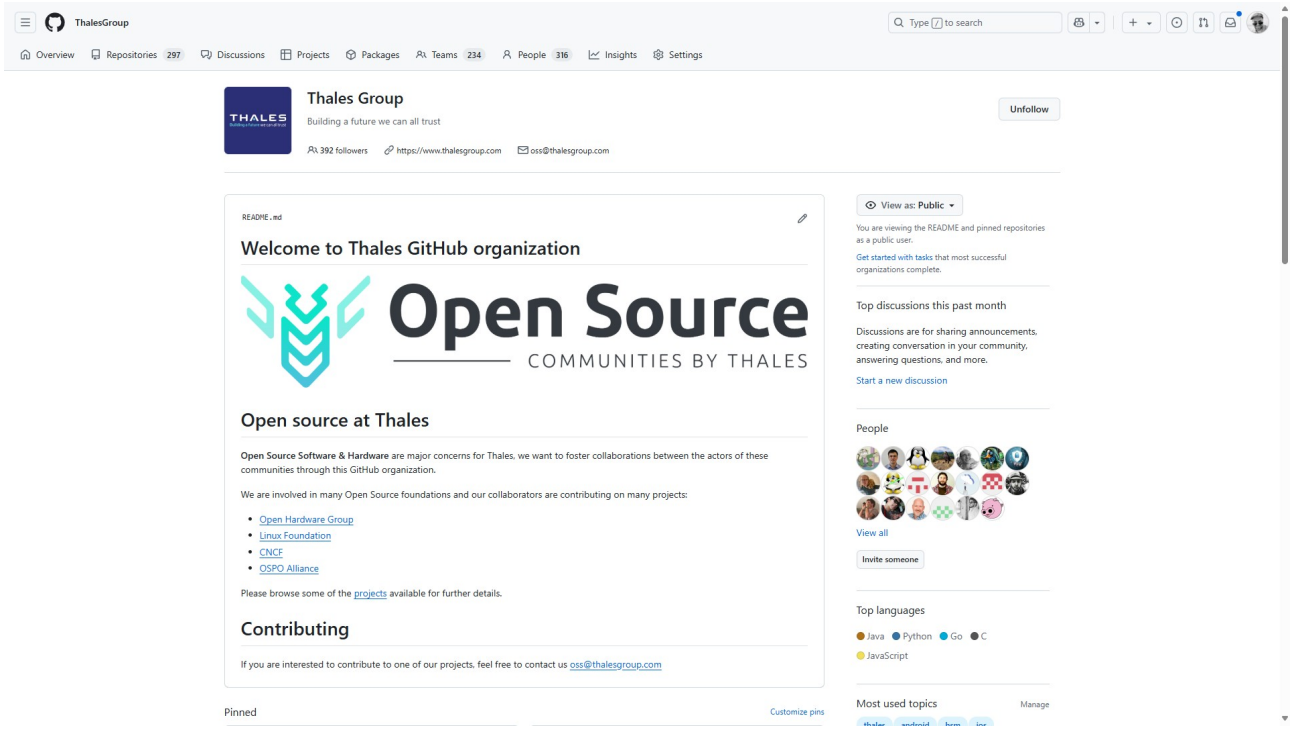
L'équipe Open Source de Thales a mis en place différents outils de collaboration.

- **Thales Open Source Portal :** Cet espace contient toutes les informations sur le processus, comment soumettre une publication ou une demande de contribution, permet de contacter l'équipe Software Compliance, de parcourir toutes les nouvelles et les événements...
- **Organisation GitHub Thales:** elle regroupe tous les projets Open Source de Thales
- **Viva Engage :** permet d'interagir avec la communauté Open Source interne de Thales
- **oss@thalesgroup.com** : un mail unique pour contacter l'équipe Thales Open Source
- **un module uLearn** : le collaborateur explore le processus et les outils disponibles pour intégrer au mieux la communauté Thales Open Source

L'organisation GitHub de Thales

Pour consulter les repositories Open Source de Thales, il suffit de se rendre sur l'organisation GitHub de Thales: https://github.com/thalesgroup.

Cette organisation constitue le point d'entrée unique pour la communauté Open source de Thales et il est essentiel que tout nouvel asset Thales mis en Open Source y soit hébergé.



Gestion des dépôts et des utilisateurs

Les développeurs de Thales contribuant à des composants OSS seront invités à rejoindre l'organisation GitHub de Thales.

Un collaborateur Thales est désigné comme administrateur de chaque dépôt Thales Open Source (public ou fork) et sera responsable de :

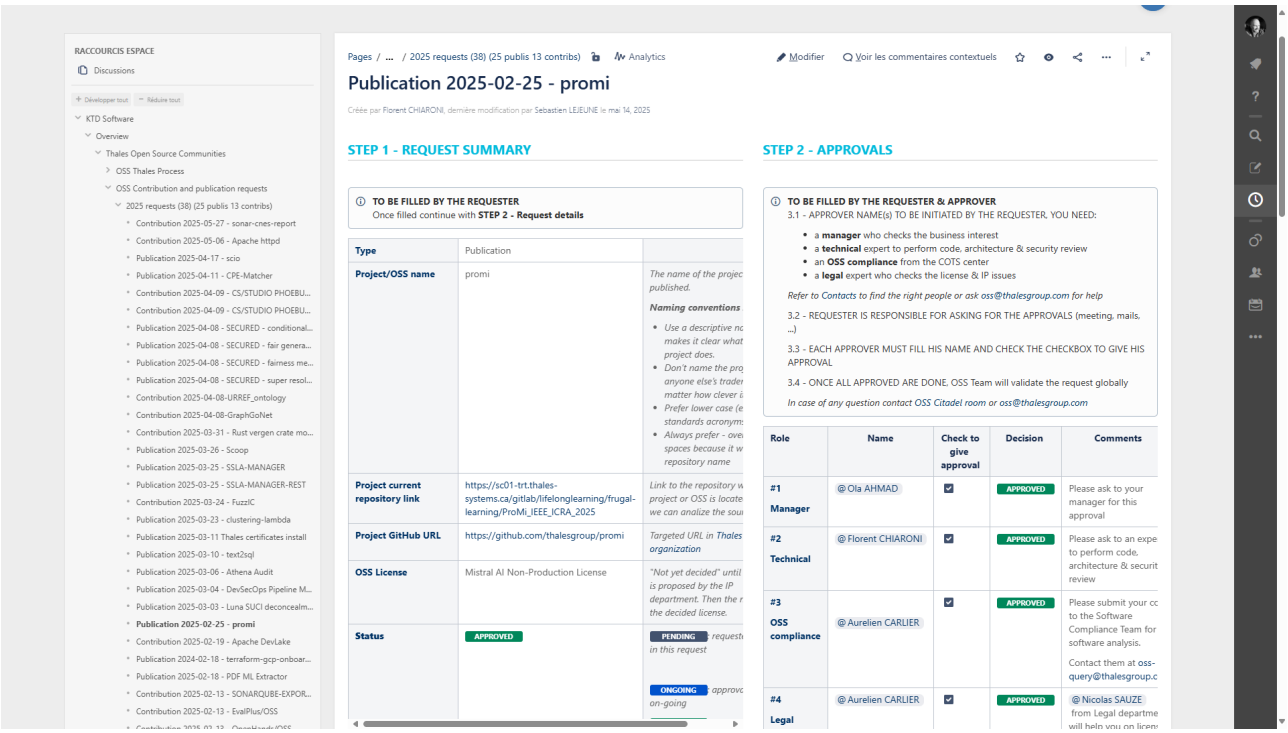
- publier et fusionner les mises à jour de la base de code principale
- surveiller et corriger les problèmes de sécurité
- répondre aux problèmes et aux demandes d'extraction
- gérer les utilisateurs du repository (dépôt)

S'il y a besoin d'ajouter ou de supprimer un membre d'un dépôt, il faut passer par le système de ticketing Thales Open Source pour demander les changements nécessaires qui seront effectués par l'équipe Open Source.

Comment partager un asset ou contribuer en Open Source ?

Le processus de publication et de contribution est très simple :

1. Soumettre une nouvelle demande de publication/contribution à l'équipe OSS de Thales
2. Remplir tous les détails et répondre aux questions
3. Obtenir les approbations : gestion et technique d'abord, conformité OSS et juridique ensuite.
4. Une fois cela fait, la mise en place du dépôt Thales GitHub (publication) ou du fork (contribution) est faite par l'équipe OSS de Thales.



Ce qu'il faut retenir sur l'organisation GitHub de Thales

Thales dispose d'un espace officiel sur GitHub où un ensemble de dépôt de solutions Open Source sont regroupées : https://github.com/thalesgroup

L'organisation de cet espace GitHub par Thales repose sur un code de conduite :
* Mise à disposition de modèles de bonnes pratiques
* Processus Thales OSS pour la publication
* Tous les nouveaux actifs doivent être déployés sur ce dépôt
* Surveillance des alertes de sécurité des codes sources

Un encouragement à la contribution
Thales encourage fortement à la contribution à des solutions Open Source quelle qu'elle soit, dans le respect des règles suivantes :
* Préserver la réputation de Thales
* Suivre le processus OSS de Thales
* Respecter les règles de la fondation
* Fork du projet dans l'espace GitHub de Thales

Des solutions Thales s'appuyant sur des briques Open Source

En premier lieu, Thales a adopté l'Open Source parce qu'il permet de maîtriser totalement nos solutions et leurs évolutions dans le temps, au service de nos clients, et en particulier sur l'aspect primordial de la sécurité. Par ailleurs Thales était convaincu que l'offre libre de l'époque avait le potentiel d'évolutivité pour intégrer, dans le temps, les fonctions qui était jugées nécessaires. Thales a une culture fortement ancrée dans l'Open Source et par ailleurs, depuis plusieurs années, toutes les solutions « digitales » (Cloud, Big Data, IA, …) sont principalement tirées sur le marché par des technologies Open Source.

Adhésions aux fondations, associations et organisations

En tant que membre de la Fondation Eclipse, de la Fondation Linux et de RISC-V International (depuis 2018[8]), CNCF – Cloud Native Computing Foundation (en 2023), Thales compte parmi les principaux acteurs européens du mouvement Open Source et s'engage à promouvoir l'adoption et la mise en œuvre de solutions Open Source.

Logo	Nom	Date
	Fondation Eclipse	Depuis 2004[9]
	Fondation Linux	Depuis 2017[10]
	RISC-V International	Depuis 2018
	CNCF Cloud Native Computing Foundation	Depuis 2023

Par son implication dans l'Open Hardware et le mouvement plus large de l'Open Source, Thales s'est engagé depuis plus de 15 ans dans des pratiques de conception et de développement ouvertes et collaboratives.

8 https://www.thalesgroup.com/fr/group/journaliste/press-release/thales-rejoint-fondation-risc-v-participer-securisation-des

9 https://www.eetimes.com/thales-nouveau-venu-declipse-foundation/

10 https://www.linuxfoundation.org/press/press-release/thales-joins-linux-foundations-core-infrastructure-initiative

Les événements majeurs externes

Le monde de l'Open Source est rythmé chaque année par un certains nombres d'événements, spécialisés autour de technologies ou plus généralistes. Ces événements sont l'occasion pour les différentes communautés et les professionnels de se retrouver et d'échanger, de faire de la veille, de suivre des conférences. Ces événements peuvent avoir lieu grâce au soutien de sponsor qui soutiennent financièrement les organisations.

Dans le cadre de son implication à l'écosystème Open Source, Thales participe à quelques événements clefs, à travers du sponsoring et la tenue de conférence.

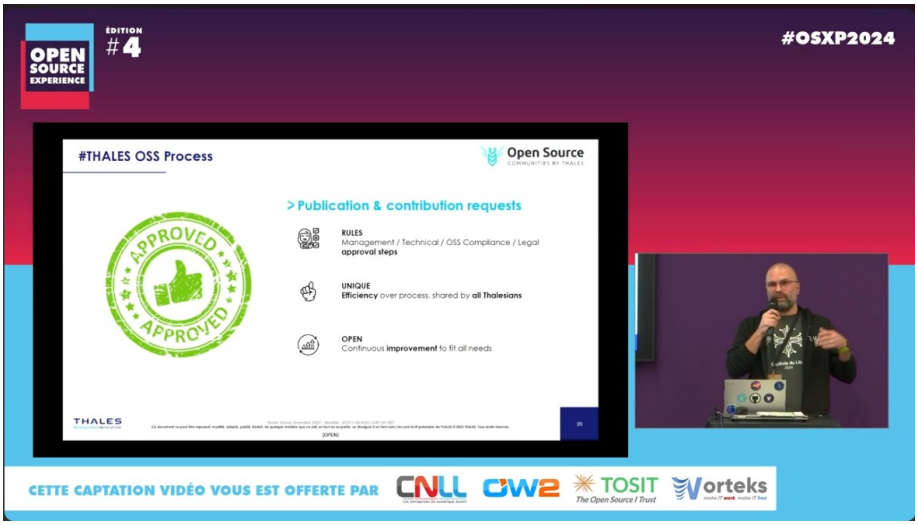
OSXP - Open Source Expérience

Soutenu par le pôle de compétitivité Systematic Paris-Region, Open Source Expérience[11] est l'événement Tech - Usage - Business dédié aux solutions informatiques Open Source, réunissant plus de 4.000 professionnels et acteurs du numérique sur 2 jours. Il s'agit du principal événement national de la filière Open Source, qui se tient sur Paris.

Le salon met l'accent sur les technologies, solutions et enjeux de l'Open Source en France et en Europe, et souligne le rôle moteur des innovations Open Source dans la transformation digitale des organisations sur des technologies telles que l'IA, le Data Management, l'IoT, le Cloud et la Blockchain.

Vitrine internationale de l'excellence technologique et du dynamisme économique de la filière Open Source française, l'événement rassemble des acteurs technologiques mondiaux, des associations professionnelles, des entreprises et des collectivités, un vaste réseau de PME et des organismes de recherche.

En 2022, le marché de l'Open Source en France était de 6 milliards d'euros, soit 11% du marché numérique mondial. Cette croissance est durable, et a été multipliée par 40 en moins de 20 ans. Avec une croissance de 8,6 % par rapport à l'année précédente, la France consolide sa position de leader européen.



11 https://www.opensource-experience.com/

Lors de l'édition 2024, Sébastien LEJEUNE, OSPO de Thales, présentait une conférence "Happy birthday Thales OSPO !"[12]. En 2023, Anthony BORD (CDI) et Jérôme VENANT (SIX) étaient venus parler de l'Open Source Hardware de l'implication de Thales dans RISC-V et Open Compute Project (OCP).

RISC-V Summit

RISC-V est l'architecture de jeux d'instructions (ISA) de processeurs. La norme est ouverte et permet une série de nouvelles applications et des recherches qui définiront l'avenir de l'informatique en Europe. L'Europe a d'ailleurs joué un rôle central dans le succès du RISC-V, un tiers de la communauté mondiale du RISC-V étant basé en Europe.

Le RISC-V Summit Europe[13] est un événement annuel qui, en 2025, se tenait à Paris. L'objectif de cet événement est de proposer un cycle de conférences conçues pour aider les participants à explorer les applications commerciales & industrielles, de recherche et académiques.

Dans le cadre de son programme lié à l'Open Hardware, Thales participe à l'événement en étant sponsor niveau Platinium (plus haut niveau), en donnant des conférences comme par exemple "The case for Open Source Hardware at Thales: Motivations and Recent Miletones with CVA6" par Bernhard QUENDT, Chief Technical Officer Thales Group.

Rust Paris

Organisée par le Hub Open Source Systematic, la conférence RUST PARIS réunit les utilisateurs et développeurs du langage de programmation RUST pour une journée de retours d'expériences et d'échanges en français sur l'utilisation de RUST dans l'industrie.

L'objectif est de proposer aux développeurs, chefs de projets et décideurs un lieu pour partager des idées et des cas d'usage et apprendre les uns des autres sur la meilleure façon d'appliquer ce langage et ses outils face à des défis en constante évolution dans des domaines variés : systèmes embarqués (notamment pour l'automobile et l'énergie), vérification formelle et certification industrielle, cybersécurité, WebAssembly pour le cloud et le traitement de données, développement d'OS, et trading haute fréquence.

Thales a été sponsor de l'événement lors de ces deux dernières éditions en 2024 et 2025.

12 https://www.youtube.com/watch?v=VXRNtagK-kE

13 https://riscv-europe.org/

Kubecon

La KubeCon[14] est une conférence dédiée à la technologie Kubernetes et à l'écosystème cloud-native. Organisée par la Cloud Native Computing Foundation (CNCF), elle rassemble des développeurs, des opérateurs, des architectes et des décideurs pour discuter des dernières avancées, partager des connaissances et explorer les meilleures pratiques autour de Kubernetes et des technologies associées. La conférence propose des sessions techniques, des ateliers, des keynotes et des opportunités de networking, faisant de la KubeCon un événement incontournable pour la communauté cloud-native.

En sa qualité de membre Silver de la CNCF, Thales participe pour la première fois à la KubeCon Europe 2024 à Paris en présentant ses solutions et innovations dans le domaine du cloud-native et de Kubernetes. Le stand de Thales est un lieu où les visiteurs peuvent découvrir comment Thales intègre ces technologies pour offrir des solutions sécurisées et performantes.

L'objectif de Thales durant cette convention fut double: d'une part, présenter CipherTrust, une solution de pointe en matière de sécurisation du cloud. Et d'autre part, mettre en avant son engagement profond envers l'Open Source au sein de la communauté Kubernetes via ses activités de R&D et ses contributions.

14 https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/

Capitole du Libre

Le Capitole du Libre[15] est un événement qui se déroule au mois de novembre de chaque année, au sein de l'école informatique ENSEEIHT de Toulouse (France). L'événement est un événement important de la communauté Open Source. Il se déroule sur le temps d'un week-end et regroupe environ 100 conférences et 25 ateliers à destination des experts comme du grand public.

Pour les éditions 2023 & 2024, Thales était sponsor Platine de l'événement. En 2024, Marius MOULIS, Global Inner Source Leader @ Thales (Corporate Software Factory Product Owner & Digital Transformation Leader) a présenté une conférence intitulée "Boostez la collaboration et cassez les silos grâce à l'Inner Source !"

15 https://capitoledulibre.org/

Événements Internes

Thales I/O Days

Les Thales I/O Days sont un événement annuel visant à réunir les communautés Inner & Open Source de Thales, la première édition ayant eu lieu en 2024 à Hélios et reconduite en 2025 à Paris avec une forte ouverture vers nos partenaires externes. Il est sponsorisé par Bernhard QUENDT (CTO), Olivier FLOUS (SVP Engineering & Digital Transformation) et Philippe NETO (VP Talent & Performance).

L'événement se compose d'une journée de conférence réunissant des keynotes, des talks et des démonstrations ainsi que des ateliers créatifs permettant à tous les acteurs des communautés d'échanger à l'occasion d'un moment convivial. C'est également l'occasion de remercier les plus impliqués au travers de la cérémonie des awards.

Enfin, chaque année la conférence finit par l'annonce du hackathon à venir avec la thématique des challenges, en 2025 il s'agissait de Cyber + AI et le succès fut au rendez-vous avec plus de 400 participants, 110 idées soumises et 3 vainqueurs récompensés au final.

Thales Rust Day

Le Thales Rust Day rassemble la communauté du langage de programmation Rust au Thales Research & Technology à Palaiseau, France. L'événement, organisé sous l'égide du CTO Office/KTD Software, rassemble des ingénieurs en logiciel et en cybersécurité pour des sessions techniques, tirant parti de la fertilisation croisée autour de Rust à travers le Groupe.

THALES

Building a future we can all trust