Open source

The new standard

THALES
Building a future we can all trust

Summary

The Open Source Sector

Takeaways (Key Points for a Decision Maker)

Open Source licenses guarantee that the source code is open, encouraging innovation and collaboration. These licenses offer the possibility of code modifications being shared, thus benefiting the whole community. They play a crucial role in promoting transparency and security, enabling public verification of code.

Open Source Software

Definition

Open Source refers to a software development and distribution model where the source code is open, meaning it is accessible by all its users. Unlike proprietary software, whose source code is typically kept secret and subject to restrictive usage licenses, Open Source allows its users not only to use the software but also to analyze it. This approach is based on transparency, collaboration, and continuous improvement by the developer community.

The openness and availability of the source code promote the pooling of efforts, collaborative innovation, and the acceleration of technological development. In practice, Open Source software is often managed by communities of developers who collaborate remotely via platforms like GitHub (a web service for hosting and managing software development using the Git version control software), or by publishers who carry a vision and a commercial offering.

These software solutions may offer a robust and flexible alternative to commercial software, enabling businesses, governments, organizations, and individuals to:

- Adopt and adapt these software solutions to their specific needs without being tied to restrictive contracts or high licensing fees.
- Ensure transparency in the software's operation and processing.
    - The openness of the code also facilitates security audits (and the implementation of fixes).
- Have a certain level of assurance regarding longevity: if the publisher fails, the software can be taken over by others, especially if it has a sufficient user or customer base.

Notable examples of Open Source Software include:

- The Linux kernel and its distributions
- The Android smartphone operating system
- The Mozilla Firefox web browser
- The MySQL and PostgreSQL databases
- The LibreOffice office suite
- The C / C++ / Rust compilers
- K8S – Kubernetes
- ...

The Open Source Software Market

The Open Source software market is approximately 8,276 billion euros. This market has seen impressive growth, multiplying by 40 in less than twenty years, with an annual growth perspective of nearly 8% until 2027.

In a recent study conducted by the Conseil National du Logiciel Libre (CNLL), France stands out with a massive adoption of open-source software, representing approximately 6.4 billion euros in revenue for sector companies in 2023. Consequently, France is the leading European market for Open Source, closely followed by Germany, with an annual growth rate of over 8%.

This report highlights several key points:

- **Sustained growth:** The European Open Source market has seen significant growth, with a projection of 20 billion euros by 2027. France, thanks to its many innovative SMEs, plays a crucial role in this growth.
- **Business dynamics:** More than 70% of French companies report using or contributing to Open Source projects, reinforcing the idea that Open Source is a pillar of their digital transformation. Across all companies, the topic of Open Source is now essential and is addressed through the creation of Open Source Programs (OSPO).
- **Open Source services ecosystem:** The study emphasizes the importance of service companies and Open Source publishers that are driving the market, particularly in critical sectors such as cybersecurity, cloud infrastructures, and databases.

Open Source Hardware

Definition

Open Hardware refers to physical devices whose plans, schematics, designs, and information are shared freely and openly. Drawing on the principles of openness from Open Source, Open Hardware aims to make hardware designs accessible, modifiable, and shareable, thereby fostering collaboration, innovation, transparency, and education.

Open Hardware covers a wide range of products, from electronic components to complex machines, including medical devices, telecommunications equipment, and even vehicles. Companies and individuals can use these plans to manufacture their own versions of the products, improve them, or adapt them to specific needs.

Notable examples of Open Hardware include:

- **Arduino :** Arduino boards are open-source electronic prototyping platforms. Their schematics, plans, and source codes are available to everyone, allowing anyone to manufacture, modify, and use them.
- **Prusa :** Prusa 3D printers are another example of Open Hardware. Their plans and software are available under an open-source license, allowing users to modify and improve them.
- **Open Compute Project :** Initiated by Facebook, this project shares the technical specifications of certain data center equipment, such as servers and networks, to optimize their energy efficiency.
- **Pocket Science Lab (PSLab) :** A complete electronic testing device, including a voltage generator, oscilloscope, and other tools, entirely open-source.

These examples show how Open Hardware creates active communities around hardware projects, fostering innovation and knowledge sharing.

Focus on RISC-V

RISC-V processors are also considered Open Hardware. RISC-V is an open-source instruction set architecture (ISA) based on RISC (Reduced Instruction Set Computing) principles. It was developed at the Berkeley University of California, and is now managed by the RISC-V Foundation.

The RISC-V architecture is royalty-free and can be used, modified, and distributed freely, making it a typical example of Open Hardware. RISC-V processors are used in a variety of applications, ranging from micro controllers to supercomputers, and are supported by a large community of developers and technology companies, including Thales.

Thales, an important leader in the Open Source hardware group

Thales actively supports the development of the Open Source ecosystem for RISC-V processors. Thales organized the Second National RISC-V Student Contest in collaboration with the SOC21 research network and the CNFM2. At this event, three student teams were rewarded for their solutions to reduce the energy consumption of the CORE-V CVA6 processor, an Open Source RISC-V processor developed by the OpenHW Group.

The Open Source Hardware Market

The Open Hardware market is rapidly expanding and represents significant potential. The precise valuation of the Open Hardware market is not directly mentioned in recent search results. However, the Open Hardware market is experiencing strong growth, supported by a global community of developers, engineers, and enthusiasts who contribute to the innovation and continuous improvement of open designs. This market is also supported by initiatives and organizations that promote the adoption of Open Hardware in various industrial sectors.

Licenses and Intellectual Property

Proprietary and Open Source software differ mainly in their licenses and development philosophies. Proprietary software is developed by companies that retain full control over the source code, thereby limiting users' rights to modify, distribute, or even access the code.

The Open Source model relies on specific licenses, such as the GNU GPL (GNU General Public License) or the BSD (Berkeley Software Distribution License). The world of Open Source licenses is vast and rich. An organization, the OSI (Open Source Initiative), holds the official definition of Open Source and certifies licenses that comply with the Open Source definition.

Open Source License

A license is a contract that grants users specific rights over software while imposing certain obligations. Open Source licenses allow users to view, modify, and distribute the software's source code, subject to compliance with the license terms. They aim to encourage collaboration, innovation, and knowledge sharing.

Different Types of Licenses

Open Source licenses are diverse, and each has its own characteristics and obligations. Here is an overview of the main types of Open Source licenses and their differences:

Permissive Licenses

These licenses impose few restrictions on the use, modification, and redistribution of the code. They are generally compatible with proprietary software.

- **MIT License :** Very permissive, it allows free use, modification, and distribution of the code, even in proprietary software. The only obligation is to retain the license text in copies of the software.
- **Apache License 2.0 :** Permissive too, but it includes a patent protection clause, meaning that contributors grant a license for their patents related to the contributions they make.
- **BSD License :** Allows free use, modification, and distribution of the code. It requires that copies of the software include the license text and a mention of the original authors.

Licenses with Reciprocity Clause (Copyleft)

These licenses require that modifications and derivative works are also distributed under the same license, ensuring that the code remains Open Source.

- **GNU General Public License (GPL) :**Very popular, it requires that any derived software also be distributed under the GPL license. This means that modifications must be shared with the community.
- **GNU Lesser General Public License (LGPL) :**Similar to the GPL, but it allows the combination of the source code in proprietary software under certain conditions.
- **GNU Affero General Public License (AGPL) :** A variant of the GPL that requires the source code to be provided even when the software is used as an online service (SaaS).

Key Differences Between Licenses

- **Redistribution Obligations :** Copyleft licenses like the GPL require that modifications be shared under the same license, while permissive licenses like the MIT allow for more liberal use.
- **Compatibility with Proprietary Software :** Permissive licenses are generally compatible with proprietary software, whereas copyleft licenses may impose restrictions.

- **Patent Protection :** Some licenses, such as the Apache License 2.0, include patent protection clauses, which is not the case for all licenses.
- **Use as a Service (SaaS) :** The AGPL license requires that the source code be provided even when the software is used as an online service, which is not the case with other licenses.

The choice of an Open Source license depends on the project's objectives, compatibility needs, and preferences regarding code sharing and protection.

- **License Compatibility**: Some Open Source licenses are not compatible with each other. For example, combining code under the GPL license with code under the Apache license can pose compliance issues. It is crucial to check the compatibility of licenses before combining Open Source components.
- **Redistribution Obligations**: Some licenses, such as the GNU General Public License (GPL), require that modifications made to the source code are also distributed under the same license. This can pose challenges for companies that wish to keep their modifications proprietary.
- **Respect for Copyright**: Even if the code is Open Source, the copyright still belongs to the original authors. It is important to respect these rights and comply with the terms of the license.
- **Contribution Management**: When external developers contribute to an Open Source project, it is essential to ensure that these contributions are made under a compatible license and that copyrights are properly managed.
- **License Contamination Risks**: Integrating Open Source code into a proprietary project can lead to "license contamination," where the proprietary project must be distributed under the same terms as the Open Source license. This can be problematic for companies that wish to retain exclusive ownership of their code.
- **Compliance and Auditing**: Companies must conduct regular audits to ensure they comply with the terms of the Open Source licenses they use. Non-compliance can lead to disputes and penalties.
- **Patent Protection**: Some Open Source licenses, such as the Apache license, include patent protection clauses. This means that contributors grant a license on their patents related to the contributions they make.

In summary, while Open Source licenses offer many advantages, they require careful management of intellectual property issues to avoid legal risks and ensure compliance.

Intellectual Property Issues

The use of Open Source software raises several intellectual property issues:

- **License Compatibility :** Some Open Source licenses are not compatible with each other. For example, combining GPL-licensed code with Apache-licensed code can pose compliance issues. It is crucial to check license compatibility before combining Open Source components.
- **Redistribution Obligations :** Some licenses, like the GNU General Public License (GPL), require that modifications to the source code be distributed under the same license. This can pose challenges for companies that wish to keep their modifications proprietary.
- **Respect for Copyright :** Even if the code is Open Source, the copyright still belongs to the original authors. It is important to respect these rights and comply with the license terms.
- **Contribution Management :** When external developers contribute to an Open Source project, it is essential to ensure that these contributions are made under a compatible license and that copyrights are properly managed.
- **License Contamination Risks :** Integrating Open Source code into a proprietary project can lead to license "contamination," where the proprietary project must be distributed under the same terms as the Open Source license. This can be problematic for companies that wish to retain exclusive ownership of their code.
- **Compliance and Auditing :** Companies must conduct regular audits to ensure they comply with the terms of the Open Source licenses they use. Non-compliance can lead to disputes and penalties.
- **Patent Protection :** Some Open Source licenses, like the Apache License, include patent protection clauses. This means that contributors grant a license for their patents related to the contributions they make.

In summary, while Open Source licenses offer many advantages, they require careful management of intellectual property issues to avoid legal risks and ensure compliance.

How to Manage Open Source Software Licenses

Managing Open Source licenses is essential for companies using free software. It ensures that the use of software complies with Open Source license terms, thereby avoiding legal and compliance risks. Open Source license management tools help automate this process by analyzing licenses, monitoring compliance, and managing users and copyrights. You can contact the Software Compliance Team for further details.

Definition of Compliance

Compliance refers to the set of processes implemented to ensure that a company adheres to applicable legal, ethical, and regulatory standards. It aims to prevent the risk of sanctions, protect the company's reputation, and meet the requirements of stakeholders.

Research & Development

Collaboration and Knowledge Sharing

Open Source has enabled the creation of communities of developers and researchers who collaborate on common projects. These communities can include members from around the world, bringing a diversity of perspectives and expertise. Researchers can thus share their results and data more easily, allowing others to reproduce and validate the results, thereby accelerating the research process.

Cost Reduction

By using Open Source software and tools, companies and research institutions can reduce their development costs. This frees up resources for other R&D projects. Small businesses and startups can access cutting-edge technologies without having to invest in expensive licenses, democratizing innovation.

Transparency and Reproducibility

Open Source projects are generally more transparent, allowing for better verification and validation of research results. The availability of source code and data allows other researchers to reproduce and validate the results, which is crucial for the credibility of scientific research.

Open Innovation

Open Source encourages an open innovation approach, where companies and researchers share their innovations with the community. This can lead to faster technological advancements and better adoption of new technologies. Contributions can come from various sources, including academics, companies, and individuals, enriching projects with a variety of perspectives and expertise.

Flexibility and Customization

Open Source software can be modified and adapted to meet specific needs, which is particularly useful in specialized research fields. Researchers can customize Open Source tools to meet their specific needs, leading to more innovative and effective solutions.

Acceleration of Innovation

Open Source projects can evolve rapidly thanks to contributions from many developers and researchers. This allows for faster innovation and wider adoption of new technologies. Companies can adopt Open Source technologies more quickly, giving them a competitive advantage.

Cyber and Digital

The Rise of Open Solutions in a Secure World

In today's digital ecosystem, where data protection and secure authentication have become major concerns, Open Source has established itself as an essential paradigm. The inherent transparency of open code offers

a considerable advantage: continuous auditing by the community, ensuring rapid detection of vulnerabilities and immediate response. This collaborative approach perfectly meets the requirements of organizations like Thales, which place trust and security at the heart of their concerns.

Open Source Foundations in Cybersecurity

One of the fundamental libraries in this field remains OpenSSL, which has become a cornerstone of digital communication security thanks to its advanced encryption and certificate management capabilities. Its massive adoption by the industry testifies to its reliability for implementing TLS and SSL protocols, essential for protecting data exchanges.

The Open Source ecosystem continues to grow with specialized solutions addressing contemporary cybersecurity challenges. Projects like OpenVAS for vulnerability analysis, OSSEC for intrusion detection, and Wazuh for system integrity monitoring illustrate the diversity and maturity of available tools.

Committed Industrial Players

Many technology companies actively contribute to this ecosystem, providing resources, expertise, and financial support:

- American giants like Google, Microsoft, Amazon, IBM, and Meta (Facebook) Massively participate in Open Source security initiatives, aware of the strategic importance of the reliability of these solutions.
- Cybersecurity specialists like Thales, Canonical, and Stormshield Integrate Open Source into their approach, contributing to communities while benefiting from collective innovations.
- Cloud service providers (Red Hat, VMware) Invest in securing their Open Source infrastructures, an essential element of their value proposition.

These players contribute not only through financial donations but also by allocating human resources dedicated to the development and improvement of critical Open Source projects.

Identity Management: The Open Approach as a Guarantee of Trust

In the crucial field of digital identity, OpenID Connect (OIDC) has established itself as a major reference. This authentication protocol, built on the foundations of OAuth 2.0, allows for simplified yet highly secure identity management across different interoperable systems. The strength of OIDC lies in its ability to offer a seamless user experience while maintaining an optimal level of security for sensitive applications.

Other initiatives like Keycloak, an Open Source identity manager, and GLUU for multi-factor authentication, complement this ecosystem, enabling organizations to build robust identity infrastructures without dependence on proprietary solutions.

Keycloak, developed under the Apache license and supported by Red Hat, has become an essential reference in identity management. This comprehensive solution allows for single sign-on (SSO), user federation, and natively supports SAML v2 and OpenID Connect protocols. Its strength lies in its ability to centralize authentication, allowing users to log in once to access all connected applications.

Community Dynamics as a Driver of Excellence

What fundamentally distinguishes the Open Source approach in cybersecurity is the power of its community. Active and responsive, it ensures continuous improvement of tools, rapid identification of vulnerabilities, and constant evolution of solutions. Companies like Thales understand the importance of this dynamic and actively contribute to it, particularly through their participation in foundations such as Eclipse and the Linux Foundation.

This collaboration between industrial players and the Open Source community creates a virtuous circle: companies benefit from constant innovations while projects gain in maturity and adoption.

The Internet of Things Secured by Open Source

Securing connected objects represents a major challenge that the Open Source approach effectively addresses. Projects like Eclipse IoT or Zephyr OS demonstrate the ability of open solutions to ensure robust security from the design of connected devices.

The inherent adaptability of Open Source technologies facilitates their integration into heterogeneous IoT environments while ensuring compliance with high security standards. This flexibility proves particularly valuable in a field where use cases and constraints vary considerably.

A Distribution Specialized in Cybersecurity

Kali Linux is a Linux distribution specifically designed for penetration testing and security auditing. It is widely used by cybersecurity professionals, pentesters, and computer security researchers. Kali Linux includes over 600 preinstalled security tools, making it a comprehensive toolkit for penetration testing and security analysis.

Kali Linux is equipped with a vast collection of preinstalled security tools, covering various aspects such as network analysis, reverse engineering, intrusion testing, and digital forensics.

Collaborative Initiatives and Responses to Regulatory Challenges

Facing increasing regulatory challenges, particularly the European Cyber Resilience Act, Open Source stakeholders are mobilizing collectively. A recent major initiative is the collaboration between seven Open Source foundations to establish common specifications for secure software development. This approach aims to proactively meet regulatory requirements while maintaining the agility and innovation inherent to Open Source.

The OpenSSF has also set up specialized teams: the Alpha teams examine gaps in cybersecurity and develop methods and tools to address them, while the Omega teams search for critical vulnerabilities in thousands of Open Source projects using automated analysis systems.

Towards Enhanced Digital Sovereignty

The adoption of Open Source solutions in cybersecurity is also part of a digital sovereignty approach. By freeing themselves from proprietary "black boxes," organizations gain independence and control over their security infrastructure. This autonomy becomes a strategic issue, particularly for critical sectors such as defense, energy, and healthcare.

The diversity of actors involved in the Open Source ecosystem, ranging from international foundations to specialized companies, ensures a balance and prevents dependence on a single vendor. This distributed approach strengthens the overall resilience of the system and fosters the emergence of solutions tailored to the specific needs of each context.

Conclusion: Open Source as a Guarantee of Trust

In a context where cyber threats are constantly evolving, Open Source offers a development model particularly suited to the requirements of cybersecurity and identity management. Transparency, agility, collaboration, and continuous innovation are the major assets of this approach, which will continue to shape the future of digital security.

The richness of the Open Source ecosystem, both in terms of the diversity of available solutions and the commitment of the actors contributing to it, constitutes a major lever for addressing contemporary security challenges. The convergence of efforts between foundations, companies, and developer communities creates a virtuous circle of continuous improvement, essential for staying ahead of ever-evolving threats.

Defense Sector

The integration of Open Source and Open Hardware in the defense sector represents a major strategic trend, offering new perspectives in terms of sovereignty, technological independence, and cost control.

In a world where the geopolitical context is highly fluid, the defense sector must address issues and challenges of sovereignty. Dependence and sovereignty: In France, the Ministry of the Armed Forces faces growing dependence on proprietary software, particularly Microsoft's. A parliamentary report warns against the "Microsoft trap" and encourages the exploration of free software to strengthen digital sovereignty.

Open Source as a Strategic Lever

The use of Open Source solutions in defense allows state actors to reduce their dependence on proprietary technologies, often controlled by foreign actors. By directly mastering their source code, military organizations strengthen their autonomy, further secure their infrastructures, and gain resilience against cyber threats. Significant examples, such as the adoption by the French army of Open Source cybersecurity solutions (such as CLIP OS, developed by ANSSI), illustrate this approach.

Other notable use cases include the French SCORPION combat management system project, which widely integrates Open Source software components to ensure interoperability and scalability. Similarly, the U.S. Department of Defense uses Kubernetes, an Open Source container orchestration system, to improve the management and security of military applications.

The military sector also widely exploits the capabilities of the real-time Linux kernel (Real-Time Linux), used for critical embedded systems requiring high temporal precision, such as weapon systems, radars, or military drones. To simplify the integration and customization of embedded Linux systems, tools such as Yocto Project and Buildroot are commonly used, allowing defense industry players to build distributions tailored to their specific needs while fully mastering their software production chain.

The transparency of Open Source code thus allows for increased auditability, essential for ensuring the trust and robustness of critical military systems.

Open Hardware: A New Frontier for Sovereignty

In parallel, Open Hardware represents considerable potential for the defense sector. By providing accessible and modifiable plans for hardware components and systems, Open Hardware allows military organizations to produce locally, quickly adapt equipment to their specific needs, and limit risks related to supply chain disruptions.

Initiatives such as the RISC-V project illustrate this dynamic. This Open Hardware processor project offers a strategic alternative to proprietary solutions, often subject to commercial or geopolitical restrictions. In the United States, DARPA supports several Open Hardware projects, such as the POSH (Programmable Open Source Hardware) program, aimed at creating safer and more transparent electronic components.

Challenges and Limits of the Open Approach

However, openness also presents specific challenges. The potential exposure of Open Source and Open Hardware solutions to hostile actors requires robust strategies in terms of security, integration, and community governance. Managing these issues involves clear collaboration policies, appropriate legal protection mechanisms, and structured governance of open innovation.

Towards a Collaborative and Sovereign Defense

In conclusion, the intelligent integration of Open Source and Open Hardware into defense strategies constitutes a promising path to strengthen national technological sovereignty. By combining innovation, transparency, and resilience, this approach fosters a collaborative, agile defense ecosystem capable of responding to contemporary security challenges.

Aerospace Sector

The European space sector is currently undergoing a major transformation driven by the rise of Open Source technologies. Once seen as a domain reserved for large national agencies and historical industrial players, space is now seeing the emergence of an open collaboration dynamic, made possible by the democratization of access to space technologies.

Open Source Software: Democratizing Orbital Mechanics

At the heart of this transformation is Orekit, an Open Source Java library dedicated to orbital mechanics and space navigation. Supported by ESA, Orekit allows public, private, and academic actors to perform complex calculations of orbits, trajectories, and satellite pass predictions. Other tools like GMAT (General Mission Analysis Tool), initially developed by NASA and then released as Open Source, or the ESA SNAP Toolbox for satellite data processing, demonstrate the richness of this collaborative approach.

Public and Private Initiatives: Towards an Open Ecosystem

Public actors play a crucial role. ESA organizes the Summer of Code in Space (SOCIS), inspired by Google Summer of Code, thereby promoting contributions to Open Source space projects by students and researchers.

On the private side, Thales Alenia Space and Airbus Defence & Space, although traditionally oriented towards proprietary solutions, are gradually opening up to Open Source standards and tools to improve the interoperability and efficiency of their missions. Exotrail, a French NewSpace startup, develops software compatible with Open Source components to optimize the trajectories of small satellites, perfectly illustrating the integration of Open Source in the emerging private sector.

Libre Space Foundation: Pioneer of 100% Open Space

The Libre Space Foundation (LSF) represents the vanguard of the Open Source movement in space. This Greek foundation develops fully Open Source space projects, both hardware and software. The SatNOGS network, consisting of Open Hardware ground stations for communicating with satellites, and the UPSat satellite, entirely designed in Open Source, are emblematic examples of their work. LSF's approach is educational, scientific, and inclusive, concretely illustrating how Open Source enables radical democratization of space.

Open Hardware: An Emerging Dynamic

In addition to software, Open Hardware is also emerging as a promising approach, albeit still nascent. Projects such as SatNOGS ground stations, QUBIK nanosatellites, or university satellite modules show the growing interest in this approach. Public actors like ESA, through initiatives such as SDR MakerSpace, as well as European universities, regularly publish their work in Open Hardware, thereby strengthening a community of collaborative innovation.

Towards an Open and Collaborative Space Sector

Open Source is thus profoundly transforming the space sector by bringing more transparency, collaboration, and reducing barriers to entry for new players. By combining the strengths of public agencies, large industrial players, innovative startups, and the global community, European space is accelerating its development while strengthening its technological autonomy and international influence.

NASA

NASA play a significant role in the development and promotion of Open Source, particularly in the aerospace field. NASA has developed OpenVSP (Open Vehicle Sketch Pad), an Open Source tool for parametric geometric modeling of aircraft. This tool allows for the creation of 3D aircraft models and supports the technical analysis of these models. OpenVSP is widely used in the aerospace industry for aircraft design and analysis.

These contributions from NASA and demonstrate their commitment to Open Source, thereby facilitating innovation, collaboration, and efficiency in the aerospace sector.

Differentiators & Challenges

Takeaways (Key Points for a Decision Maker)

Open Source is a strategic lever to strengthen technological independence, control costs, and foster innovation. It allows for advanced customization, facilitated integration through open standards, and greater security through code transparency. Supported by a structured international ecosystem, it offers a sustainable alternative to proprietary solutions while meeting sovereignty and compliance requirements (CRA, NIS2).

Beyond technology, Open Source enhances HR attractiveness by valuing skills, retaining talent, and improving the company's image. However, its adoption requires a rigorous approach, combining evaluation methodologies (QSOS, OW2 MRL, ANSSI) and anticipation of hidden costs related to maintenance, security, and governance.

Advantages of Open Source

Governance, Independence, and Technological Sovereignty

Technological independence has become a major issue. Open Source allows for liberation from dependence on proprietary software vendors and tech giants (GAFAM) that can impose overly restrictive commercial conditions without negotiation or countervailing power. By using Open Source solutions, companies can avoid dependence on a single software vendor, reducing the risk of technological lock-in and offering more freedom in choosing technologies.

Moreover, Open Source solutions are often developed according to open standards, which can facilitate integration with other systems and technologies. This can also help ensure compliance with regulations and industry standards.

Initiatives like openDesk from the Zentrum Digitale Souveränität in Germany already show that Europe can build a secure digital ecosystem. This initiative is based on Open Source solutions developed by European publishers such as XWiki, CryptPad, OpenProject, and Nextcloud. The solutions used are safe, open-source, and independent alternatives to American platforms.

International collaboration

Open Source projects foster international collaboration, enabling countries to work together to develop advanced technologies without depending on a few large technology companies. Europe is making increasing use of Open Source solutions.

Economic Advantages

Shared Development

One of the major economic advantages of Open Source is the sharing of costs. This model is based on open collaboration where multiple organizations share the costs of development, maintenance, and improvement of software or components. Unlike proprietary solutions, where each company pays for licenses and often high maintenance fees, Open Source allows these costs to be distributed among a potentially unlimited number of stakeholders.

Reduction in License Costs

Open Source software or technical components are often free or available under very permissive licenses. This allows companies to achieve significant savings by eliminating license costs, which can represent a considerable portion of an organization's IT budget. Even if some Open Source solutions require paid services (support, training, etc.), these costs are generally lower than those of proprietary software licenses.

Technical Advantages

Collaborative Innovation

Open Source encourages unique collaborative innovation. Open Source projects benefit from contributions from a wide diversity of developers, allowing them to leverage different ideas and approaches. This collaboration leads to continuous improvements and the rapid introduction of new technologies into software. The absence of commercial constraints in Open Source projects also allows developers to experiment and innovate freely, without waiting for approval from a company or a board of directors.

Flexibility and Adaptability

One of the major strengths of Open Source is its flexibility. Companies can adapt the software to their specific needs by modifying the source code themselves. This allows for advanced customization, which is impossible to achieve with proprietary software. The adaptability of Open Source software also allows for better integration with other systems. Companies can adjust solutions to their IT and business environments without having to pay for additional modules or "premium" versions.

Longevity and Durability

Proprietary software can be abandoned by their publishers or see their license terms change arbitrarily. In contrast, Open Source software is generally long-lasting because the source code is open and accessible. Even if the original development team or publisher ceases its activity, the community or other companies can take over the project and ensure its continuity.

This provides greater long-term security, as organizations are not dependent on the commercial decisions of a single entity to continue using the software. There is also a safeguard in case the development team or publisher were to exceed limits acceptable to the majority of users.

Security

Open Source has sometimes been perceived as less secure than proprietary software, but this idea is increasingly refuted. In fact, Open Source software is often more secure precisely because its source code is open and anyone can examine it. This transparency allows for the rapid detection and correction of security vulnerabilities.

Interoperability and Compatibility via Open Formats

Open Source software is often designed to be interoperable with other systems and standards. This allows companies to more easily integrate Open Source solutions into heterogeneous infrastructures while ensuring compatibility with existing tools and systems. Open standards are a fundamental principle of Open Source, ensuring that systems can interact without proprietary lock-in.

An open format is a type of file format whose specifications are publicly available and can be freely used and implemented by anyone. Open formats allow interoperability between different systems and software because they are not controlled by a single publisher or specific company.

Open formats play a crucial role in the interoperability of systems and software. They allow different systems to communicate and exchange data without hindrance, thus promoting compatibility and integration between various technological solutions. Open formats are essential to ensure that data can be shared and used transparently and securely, without relying on specific proprietary solutions.

Maintainability

Open Source projects are often designed to be easily maintainable and scalable. Companies can directly contribute to code improvements or call on external service providers to maintain their Open Source solutions. Access to the source code also allows internal technical teams to perform proactive maintenance, adjust systems according to needs, and quickly correct errors without having to wait for the publisher's intervention.

Societal Advantages

Knowledge Sharing

Open Source is based on the sharing of knowledge. By opening the source code, developers allow others to understand how the software works and improve it. This contributes to the creation of a culture of collaboration and learning within the entire technological community. Open Source projects also serve as the basis for educational and academic projects. Students and researchers can freely access advanced technologies, learn complex concepts by applying them directly, and contribute to the projects themselves.

Community and Collaborative Development

Open Source creates and fosters the development of communities of developers and users. These communities are places of collaboration where people exchange ideas, share solutions to common problems, and participate in the co-creation of new technologies.

Support for the Economy

The adoption of Open Source solutions can strengthen the local and national economy by promoting the creation of local businesses specializing in the development, customization, and support of Open Source software. Rather than depending on large foreign publishers, local companies can develop in-house skills and offer services to other businesses or public organizations. This approach also encourages the development of local talent, the training of new professionals, and the creation of a sustainable technological ecosystem.

Advantages in Governance

Governance refers to the set of rules, methods, and practices that organize decision-making and the control of decision implementation within a social group, company, or organization. It aims to ensure the optimal functioning of the organization and to guarantee transparency and accountability in the management of resources and processes.

Open Source solutions enable effective governance by providing frameworks and tools to structure decision-making and project management in a transparent and collaborative manner. For example, the Open Source Program Office (OSPO) Alliance offers methodologies and best practices to help organizations implement effective Open Source governance. These initiatives promote community participation and the continuous improvement of Open Source projects.

Role of Europe

Europe advocates for governance based on Open Source solutions through various initiatives and strategies. The European Commission, for example, has implemented an Open Source strategy aimed at encouraging and leveraging the transformative, innovative, and collaborative power of Open Source. This strategy, titled "Think Open," aims to promote the sharing and reuse of software solutions, knowledge, and expertise to provide better European services beneficial to society and reduce costs.

Additionally, Europe supports initiatives such as the OSPO Alliance, which helps organizations implement effective Open Source governance. The OSPO Alliance, created by Open Source foundations like OW2, Eclipse, and Open Forum Europe, provides methodologies, best practices, and resources to structure Open Source policies and governance. Thales has been an active contributor to this initiative since 2023.

The European Commission has also launched the EU-FOSSA (Free and Open Source Software Auditing) project to improve the security and integrity of critical Open Source software. These efforts demonstrate Europe's commitment to adopting and promoting Open Source solutions for more transparent, collaborative, and effective governance.

Overview of the Ecosystem

Open Source Software

FREE SOFTWARE FOUNDATION	**Foundation pour le Logiciel Libre (FSF)** - https://www.fsf.org An organization founded by Richard Stallman in 1985, at the origin of the free software movement and the GNU project. The FSF promotes the four fundamental freedoms of free software and is responsible for the GPL licenses.
open source initiative®	**Open Source Initiative (OSI)** - https://opensource.org A pioneering organization created in 1998, responsible for the formal definition of Open Source and the official validation of Open Source licenses. The OSI plays an international reference role by ensuring legal clarity, raising awareness among companies about the benefits of the Open Source model, and guaranteeing compliance with community standards. Recently, the OSI has been working on a definition for Open Source artificial intelligence, aiming to clarify what it means to be "open" in the context of AI.
THE LINUX FOUNDATION	**Linux Foundation** - https://www.linuxfoundation.org Founded in 2000, this non-profit organization's mission is to support, protect, and standardize the development of the Linux operating system and other Open Source projects. It now plays a major federating role by hosting hundreds of leading Open Source projects, such as Kubernetes, Hyperledger, Automotive Grade Linux, or the Cloud Native Computing Foundation (CNCF).
CLOUD NATIVE COMPUTING FOUNDATION	**Cloud Native Computing Foundation (CNCF)** - https://www.cncf.io Under the auspices of the Linux Foundation, CNCF focuses on the management and promotion of Cloud Native technologies, such as Kubernetes, Prometheus, or Envoy. It has a considerable international impact on the adoption and standardization of architectures based on containers, orchestration, and micro services.
THE APACHE SOFTWARE FOUNDATION ESTABLISHED 1999	**Apache Software Foundation** - https://www.apache.org Founded in 1999, the Apache Software Foundation (ASF) is one of the largest and most influential Open Source organizations in the world. It manages over 350 projects, many of which constitute the backbone of the modern internet and cloud (Apache, Hadoop, Spark, Cassandra, and NiFi). The uniqueness of the ASF lies in its meritocratic governance model (decision-making power is earned through contribution) and its rigorous incubation process for new projects. Its Apache 2.0 license has become an industry standard for its compatibility with commercial uses, while preserving Open Source principles.
CHAOSS	**CHAOSS (Community Health Analytics Open Source Software)** - https://chaoss.-community A Linux Foundation project that develops metrics, methodologies, and tools to measure the health and sustainability of Open Source communities.
	OpenChain Project - https://www.openchainproject.org A Linux Foundation initiative that establishes standards for managing Open Source license compliance in software supply chains.
moz://a	**Mozilla Foundation** - https://foundation.mozilla.org The Mozilla Foundation, created in 2003 following the release of the Netscape Navigator source code, is a non-profit organization dedicated to preserving an open, accessible, and secure internet. It oversees the development of free technological products, the most well-known of which is the Firefox browser, while leading advo-

	cacy campaigns for privacy protection, net neutrality, and web standard interoperability. In addition to the browser, it initiated the Rust programming language, now used by Microsoft, Google, Amazon, and others for critical systems. Very recently, it decided to accelerate the development of a collaborative suite based on Thunderbird.
	**Rust Foundation** - https://rustfoundation.org/ The Rust Foundation is a non-profit organization dedicated to supporting and developing the Rust programming language. Established to ensure the longevity and growth of Rust, it fosters its adoption and evolution. The foundation oversees community contributions, coordinates development efforts, and promotes best practices. It also works to ensure the stability and security of the language. Additionally, the Rust Foundation encourages innovation and collaboration within the Rust ecosystem.

Open Source Hardware

	**RISC-V International** - https://riscv.org Founded in 2015 and based in Switzerland, RISC-V International is the standardization body overseeing the development of the RISC-V processor architecture, an open and royalty-free instruction set architecture (ISA). Unlike proprietary architectures such as ARM or x86, RISC-V allows anyone to design, manufacture, and sell processors without paying royalties. With over 3000 members in 70 countries, including giants like Google, Qualcomm, and Alibaba, this foundation sets technical specifications, maintains compatibility between implementations, and coordinates the evolution of the ecosystem. The impact of RISC-V extends from IoT to supercomputers, offering a strategic alternative in a context of geopolitical tensions around semiconductor technologies and digital sovereignty.
	**OpenHW Group** - https://www.openhwgroup.org Founded in 2019, the OpenHW Group is a non-profit organization that develops Open Source processor cores based on the RISC-V architecture and ready for industrial use. Its CORE-V project offers robust and fully verified implementations such as the CV32E40P (32-bit) and the CVA6 (64-bit). Bringing together over 90 members including Intel, NXP, and STMicroelectronics, this foundation bridges the gap between open specifications and their commercially viable implementation, while keeping all intellectual property under Open Source licenses. The OpenHW Group also provides the necessary tool ecosystem to facilitate the adoption of these technologies in applications ranging from IoT to critical embedded systems.
	**Open Compute Project (OCP)** - https://www.opencompute.org Founded in 2011 by Facebook (now Meta), the Open Compute Project is a collaborative organization that redefines the approach to hardware in data centers by applying Open Source principles to computer hardware. OCP develops and shares open designs for servers, storage, networks, and data center infrastructures, optimized for energy efficiency and cost reduction. With over 200 members including Microsoft, Intel, Google, and AT&T, the organization has enabled significant energy savings and a substantial reduction in electronic waste. OCP specifications are now implemented in more than 40% of public cloud servers, demonstrating the transformative impact of the Open Source approach applied to large-scale infrastructure hardware.
	**Open Source Firmware Foundation (OSFF)** - https://opensourcefirmware.foundation Founded in 2022, the Open Source Firmware Foundation (OSFF) is an organization dedicated to the promotion and development of Open Source firmware for modern computer systems. It focuses on low-level software layers that run before the operating system, such as BIOS/UEFI, bootloaders, and firmware for network cards or storage controllers. OSFF supports projects like coreboot, LinuxBoot, and

	OpenBMC, which aim to replace proprietary firmware with open, auditable, and secure alternatives. Created in response to growing concerns about security and digital sovereignty, this foundation brings together industrial players like Google, 9elements, and Star Labs, as well as security researchers, to bridge the last major proprietary gap in the software stack of modern computers.
	Open Source Hardware Association (OSHWA) - https://www.oshwa.org Founded in 2012, OSHWA is the reference organization for free and open hardware. It established the official definition of Open Source Hardware and manages a certification program allowing creators to identify their products as compliant with open hardware standards. OSHWA organizes the annual Open Hardware Summit and promotes best practices for documentation and sharing in the field of hardware.

Key players in the Open Source cybersecurity ecosystem

	L'OWASP (Open Web Application Security Project) - https://owasp.org OWASP is a non-profit organization focused on improving the security of software applications. Founded in 2001, OWASP has become a global reference in web application security.
	Open Source Security Foundation (OpenSSF) - https://openssf.org Founded in August 2020 under the auspices of the Linux Foundation, OpenSSF is a collaborative initiative addressing the growing urgency to secure the Open Source ecosystem. OpenSSF brings together over 100 members, including tech giants (Google, Microsoft, Amazon, Meta), major Open Source foundations (Linux Foundation, Apache Software Foundation), and specialized cybersecurity actors. OpenSSF has quickly become the reference initiative for addressing security challenges specific to the Open Source model, such as reliance on volunteer maintainers, the complexity of dependencies, and the massive use of insufficiently audited components.
	OpenID Foundation - https://openid.net The OpenID Foundation focuses on the development and promotion of digital identity standards. It has notably created a working group for the IPSIE (Interoperability Profile for Secure Identity in the Enterprise) standard, adopted by major players like Microsoft, Google, and Ping Identity.
	OpenSSL Foundation https://openssl-foundation.org The OpenSSL Foundation plays a critical role in securing communications, with its flagship project ranked in the top 10 most important projects by the Open Source Security Index.

Europe

	Eclipse Foundation - https://www.eclipse.org Initially focused on the Eclipse IDE development tool, the Eclipse Foundation has become one of the leading Open Source foundations dedicated to collaborative governance and the sustainable development of Open Source software projects across multiple sectors. It brings together a vast global community and manages over 400 projects. Since 2020, it has been based in Europe (Belgium).
	OSPO Alliance - https://ospo.zone An international initiative supported by OW2 and the Eclipse Foundation, the OSPO Alliance aims to promote and structure best practices around Open Source Program Offices (OSPOs) within companies. It fosters the professionalization of Open Source

	management in both private and public organizations, in Europe and internationally.
	OW2 - https://www.ow2.org/ An independent European Open Source community primarily dedicated to Open Source infrastructure software. OW2 promotes open and collaborative governance of software and encourages the adoption of Open Source solutions within European administrations and large enterprises. OW2 is also recognized for its work on interoperability and digital sovereignty.
	Foundation for Public Code - https://publiccode.net Founded in the Netherlands in 2019, this European organization specifically focuses on the development and maintenance of public code—Open Source software developed by and for governments and public administrations.

France

	Hub Open Source Software de Systematic Paris-Region - https://www.systematic-paris-region.org/hubs/hub-oss The OSS Hub, led by the Systematic Paris-Region competitiveness cluster, acts as a center of expertise and animation for the French Open Source ecosystem. It brings together companies, research organizations, universities, and public authorities to promote the adoption of free software.
	APELL (Association Professionnelle Européenne du Logiciel Libre) - https://apell.info A French professional association aiming to represent the economic and strategic interests of free software companies in France and Europe. It addresses legal, economic, and political issues.
	TOSIT (The Open Source I Trust) - https://tosit.fr A French collective of large companies (including Société Générale, BPCE, EDF, MAIF, Michelin, etc.) committed to the controlled adoption of Open Source. It develops best practices around sourcing, securing, and supporting strategic Open Source solutions.
	CNLL (National Council for Free Software)- https://cnll.fr A French federation of free software companies, representing approximately 300 companies through its regional member associations.
	Software Heritage - https://www.softwareheritage.org A French initiative for the preservation of software heritage, recognized internationally. Launched by Inria, it aims to collect, preserve, and share all publicly available source codes.

Methodologies for Analysis and Selection of Open Source Solutions

The growing adoption of Open Source software in organizations requires a methodical and rigorous evaluation to address the complex challenges of security, sustainability, and governance. This section presents an analysis of the main evaluation methodologies from three major methodological frameworks: QSOS, OW2 Market Readiness Levels, and the ANSSI approach.

The Three Essential Methodologies

QSOS: The Global and Comparative Approach

Principle: Created in 2004, QSOS (Qualification and Selection of Open Source Software) offers a four-phase methodology for objectively evaluating Open Source solutions. It is based on a standardized scoring system that allows for the comparison of different alternatives on a common basis.

Evaluation Process:

- **Definition Phase**: Establishes the evaluation framework tailored to the specific context of the organization;
- **Evaluation Phase**: Involves scoring each solution on a scale from 0 to 2 based on three main dimensions: intrinsic aspects (maturity, governance, community), technical aspects (architecture, standards, security), and associated services (documentation, support, training);
- **Qualification Phase**: Allows for the weighting of these criteria according to organizational priorities;
- **Selection Phase**: Facilitates the objective comparison of evaluated solutions to inform the final decision.

Advantages
The main strength of QSOS lies in its standardized approach, which greatly facilitates the comparison of several competing solutions. Its flexibility allows for adapting the evaluation to the specific priorities of each organization. The existence of a shared reference base within the community also helps reduce evaluation costs by pooling efforts.

Limitations
The full implementation of QSOS can be time-consuming, particularly for organizations with limited resources. Additionally, evaluations require regular updates to remain relevant in a constantly evolving Open Source ecosystem.

OW2 Market Readiness Levels: Commercial Maturity

Principle
Inspired by the TRL (Technology Readiness Levels) developed by NASA, this methodology focuses on evaluating the commercial maturity of an Open Source project. It proposes a progressive scale from 1 to 9, which clearly identifies the development stage of a solution.

Evaluation Process
The evaluation according to OW2 MRL is based on three complementary pillars:

- The first involves verifying the presence of 50 best practices distributed across 12 essential categories;
- The second relies on the analysis of 15 indicators automatically extracted from development environments;
- The third examines 48 market-related situations to assess the commercial positioning of the solution.

Maturity Levels
The 9 levels proposed by the methodology allow for the precise positioning of each solution:

- Levels 1 to 3 correspond to the emergence phase, characterized by initial research and development;
- Levels 4 to 6 represent the adoption phase, ranging from verified utility to significant adoption;
- Levels 7 to 9 mark the leadership phase, from being established as a recognized player to a dominant position in the market.

Advantages
This approach offers a particularly clear evaluation of commercial risk and the sustainability of solutions. Its language is specifically adapted to non-technical decision-makers, thus facilitating communication within management committees. It provides precise indicators of long-term viability, essential for strategic investments.

Limits
The OW2 MRL methodology pays less attention to the purely technical aspects of the evaluated solutions. Its primarily B2B orientation may also make it less relevant for certain specific contexts, particularly in the public or non-profit sectors.

The ANSSI Approach: Security and Sovereignty

Principle
Developed by the National Agency for the Security of Information Systems (ANSSI), this approach places digital security and sovereignty at the heart of the evaluation process. It aims to ensure that the adopted Open Source solutions meet the strictest cybersecurity requirements.

Evaluation Axes
The ANSSI approach is structured around seven complementary dimensions:

- **Quality of the Technical Foundation**: Documentation, secure configuration, open standards;
- **Best Development Practices**: Compliance with security frameworks, code review, testing;
- **Dependency Management**: Inventory (SBOM), monitoring, updates;
- **Security Maintenance (MCS)**: Vulnerability management, patches;
- **Operational Maintenance (MCO)**: Sustainability of maintainers, updates;
- **External Audit and Support**: Security audits, support contracts;
- **Project Support**: Addressing the project's needs for its sustainability.

This approach places security and sovereignty at the heart of the evaluation process.

Advantages
This methodology ensures a level of security compliant with national and European regulatory requirements. Its pragmatic, risk-oriented approach allows for the precise identification of potential vulnerabilities. It is particularly relevant for sensitive and regulated sectors, including operators of vital importance.

Limits
The ANSSI approach offers limited coverage of the functional and commercial aspects of the evaluated solutions. The complexity of some evaluation criteria may be difficult for decision-makers who are not cybersecurity specialists to grasp.

Conclusion

The methodologies for evaluating Open Source software are strategic decision-making tools in a context where these solutions are becoming essential. QSOS, OW2 MRL, and the ANSSI approach offer complementary perspectives that help objectify adoption decisions and reduce associated risks. Therefore, implementing a hybrid approach that combines these three methods allows for tailoring the evaluation effort to the specific challenges of each organizational context, while covering all critical dimensions: functional, commercial, and security-related.

Economic and Strategic Approach

ROI & Open Source

Open Source solutions can offer an attractive ROI (Return on Investment) for several reasons:

- **Reduced Initial Costs**: Open Source software is often free or has much lower acquisition costs than proprietary software. This reduces initial costs and potentially increases ROI.
- **Flexibility and Customization**: Open Source solutions can be modified and adapted to the specific needs of the company, which can improve efficiency and productivity.
- **Community and Support**: An active community can provide free or low-cost support, thereby reducing maintenance and technical support costs.
- **Scalability**: Open Source solutions can often be scaled more easily and at a lower cost than proprietary solutions.
- **No License Costs**: The absence of recurring license costs can result in substantial long-term savings.
- **Rapid Innovation**: Open Source projects often benefit from rapid and continuous contributions from developers worldwide, which can accelerate innovation and product improvement.

However, it is important to note that the ROI of Open Source solutions can also be influenced by factors such as training costs, technical support costs, and the resources needed to customize and maintain the software. A comprehensive evaluation must take all these aspects into account to determine the true ROI.

Economic Models

Publishers and Providers of Open Source Solutions: Models and Positioning

- **Economic Models and Adoption Approaches**
- **Best of Breed**: Utilization of community Open Source solutions (Vanilla)
- **Open Core Model**: Open Source solution with paid features
- **Subscription-based Solutions**: "Enterprise" versions with publisher support
- **Dual Sourcing Strategy**: Arbitration between proprietary and Open Source solutions

License Changes and Forks

The main risk of changing the license of an open-source solution, when the software is developed by a single publisher, lies in several key factors:

- **Loss of Community**: License changes can alienate the community of users and contributors who have supported the project. If the new license is perceived as restrictive or contrary to open-source values, contributors may stop participating, which can slow down development and innovation.

- **Forks and Fragmentation**: A license change can lead to the creation of forks of the original project. This can result in fragmentation of the community and resources, thus diluting development efforts and creating competing versions of the software.

- **Dependence on a Single Actor**: When a single publisher controls development, it can impose unilateral decisions that are not always in the community's interest. This can include license changes that restrict the use of the software or impose costs.

- **Legal Risks**: Users and companies that have integrated the software into their systems may find themselves in non-compliance with the new license, which can lead to legal risks and compliance costs, but also security risk. At Thales, the Software Compliance Team is here to help you to mitigate all these issues.

- **Reduced Innovation**: The diversity of contributors is often a driver of innovation. If a license change discourages community participation, the project may suffer from a lack of new ideas and varied perspectives.

- **Increased Costs**: Companies that depend on the software may face additional costs if the new license imposes fees for certain uses or if they have to migrate to an alternative.

These risks can have significant impacts on the long-term viability of the project, user satisfaction, and the overall ecosystem built around the software.

Fork can also be an opportunity

Several examples of open-source solution forks related to license changes by the publisher exist. One notable case is MariaDB, a fork of MySQL. MariaDB was created in 2009 following Oracle's acquisition of MySQL. The community created MariaDB to ensure that the project remained open-source and to continue developing features without the restrictions imposed by Oracle. In 2010, the OpenOffice.org community created The Document Foundation and launched LibreOffice, a fork of OpenOffice.org, in response to concerns about the direction taken by Oracle after its acquisition of Sun Microsystems, the publisher of OpenOffice.org. Jenkins is a fork of Hudson, created in 2011 after Oracle took control of the Hudson project. The community decided to create Jenkins to ensure that the project remained open-source and to continue developing features without the restrictions imposed by Oracle.

These examples show how forks can be used to maintain openness and community around open-source projects when publishers change licenses or impose restrictions.

Recent fork cases

OpenTofu

OpenTofu is an Infrastructure as Code (IaC) tool that allows for the definition of cloud and on-premises resources in human-readable configuration files. These files can be versioned, reused, and shared, providing a consistent workflow for provisioning and managing infrastructure throughout its lifecycle.

The history of OpenTofu began on August 10, 2023, when HashiCorp announced a license change for its products, including Terraform, switching from the Mozilla Public License (MPL v2) to the Business Source License (BSL). Unlike the MPL v2, the BSL is not an Open Source license, which prompted the community to create an Open Source alternative. OpenTofu was created in response to this license change, as a fork of Terraform version 1.5.6, retaining all of Terraform's popular features while introducing improvements and enhancements.

The project was initially supported by companies such as Gruntwork, Spacelift, Harness, Env0, and Scalr. In September 2023, OpenTofu became an official project of the Linux Foundation, ensuring its continued development and availability as an Open Source solution.

Since its inception, OpenTofu has experienced rapid growth and community support, with contributions from many developers and organizations. The project aims to stay true to its principles of openness and modularity, regularly releasing new versions with enhanced features and bug fixes.

TDP - Trunk Data Platform

The Trunk Data Platform (TDP) is an Open Source Hadoop distribution designed to provide a centralized and scalable solution for storing, processing, and managing large volumes of data. It is based on the Apache Hadoop ecosystem and is compatible with HDP (Hortonworks Data Platform).

The history of TDP began with discussions between EDF (Électricité de France) and the Directorate General of Public Finance (DGFiP) about their Big Data platforms. These discussions led to the creation of TDP, a platform designed to offer shared governance, be freely accessible, and be entirely Open Source. The project was initiated in 2021 and is supported by the TOSIT association (The Open Source I Trust), which includes EDF, DGFiP, and other partners.

TDP was officially presented at various events, such as the Big Data Paris trade show in September 2023, and continues to evolve with the support of the Open Source community and contributions from various organizations.

OpenSearch

OpenSearch is an Open Source search and analytics suite, licensed under Apache 2.0, that facilitates the ingestion, search, visualization, and analysis of data. It is designed to be scalable, distributed, and community-driven, offering a wide range of features for various use cases, including real-time application monitoring, log analysis, and website search.

The history of OpenSearch began in 2021 when AWS announced it would create a fork of Elasticsearch and Kibana in response to a license change by Elastic NV. This change led to the creation of OpenSearch, a community-driven, Open Source search and analytics suite that removed Elastic NV's branding and telemetry. OpenSearch was initially developed by AWS and was later transferred to the OpenSearch Software Foundation, an open technical organization within the Linux Foundation, in September 2024.

The OpenSearch Software Foundation was established to oversee the continued development of OpenSearch, with support from leading members such as Amazon Web Services, SAP, and Uber. This foundation aims to ensure that the project remains Open Source, transparent, and independent, while fostering innovation and community collaboration.

Security and Vulnerability Remediation

Open Source software is not inherently less secure than proprietary software. In fact, the security of software depends on several factors, regardless of its licensing model. Here are some points to consider:

- **Code Transparency**: Open Source software allows anyone to examine its source code. This means that vulnerabilities can be identified and fixed more quickly by a global community of developers. Proprietary software, on the other hand, relies on internal teams for bug detection and correction.
- **Community and Contributions**: The Open Source community is often vast and active. Many eyes scrutinize the code, which can lead to faster detection of security issues. Proprietary software depends on the publisher's resources, which can be limited.
- **Updates and Patches**: Well-managed Open Source projects regularly release updates and security patches. The speed of these updates can sometimes surpass that of proprietary software, especially for less popular or end-of-life software.
- **Security Audits**: Companies and organizations can conduct independent security audits on Open Source software, which is generally not possible with proprietary software. This allows for a more thorough evaluation of the software's security.
- **Dependencies and Supply Chain**: Whether for Open Source or proprietary software, managing dependencies and the software supply chain is crucial. Both types of software can be affected by vulnerabilities in the third-party libraries they use.

In summary, the security of software depends more on the quality of its development, update management, and responsiveness to vulnerabilities, rather than its licensing model. Open Source software can offer advantages in terms of transparency and speed of bug fixes, but this does not automatically guarantee better security.

Speed of Vulnerability Patching

Security vulnerabilities in Open Source software can be fixed at varying speeds depending on several factors, including the severity of the vulnerability, the availability of resources, and the responsiveness of the community or project maintainers. Here are some examples of how quickly certain famous vulnerabilities were patched:

- Heartbleed, discovered in March 2014, was a vulnerability in the OpenSSL cryptography library that allowed an attacker to read the memory of a server or client, thereby retrieving sensitive information

used during communication with the Transport Layer Security (TLS) protocol. A patch was made public in April 2014, shortly after the vulnerability was disclosed.

- Log4j is a Zero-Day vulnerability that was discovered in December 2021. It allowed attackers to execute arbitrary code on vulnerable servers, which could lead to serious compromises of affected systems. This flaw had a global impact, affecting thousands of applications and services. Even several months after its discovery, some companies were still facing attacks based on this vulnerability. Patches were released quickly after the vulnerability was disclosed, but the application of these patches varied depending on the organizations and their infrastructures.

These examples show that, although vulnerabilities can be discovered and corrected quickly, patching can take longer depending on the complexity of the systems affected and the responsiveness of organizations. If needed it is also possible to contract with externals partners such as Open Source Experts who can put in place specific SLA (Service Layer Agreement) on Open Source software maintenance.

Regulatory Aspects

CRA – Cyber Resilience Act

The Cyber Resilience Act (CRA) is a European Union regulation aimed at strengthening the cybersecurity of digital products. Effective from December 10, 2024 (with companies having until December 11, 2027, to comply by integrating the requirements), it imposes Cybersecurity standards for all products (hardware or software) with digital elements, including those provided as services (SaaS).

The Cyber Resilience Act (CRA) has a significant impact on open-source software, as it imposes specific requirements to enhance their security.

Regulatory Aspects

CRA – Cyber Resilience Act

The Cyber Resilience Act (CRA) is a European Union regulation aimed at strengthening the cybersecurity of digital products. Effective from December 10, 2024 (with companies having until December 11, 2027, to comply by integrating the requirements), it imposes cybersecurity standards for all products (hardware or software) with digital elements, including those provided as services (SaaS).

The Cyber Resilience Act (CRA) has a significant impact on Open Source software, as it imposes specific requirements to enhance their security.

Here are the main impact points:

1. **Obligations for "Stewards" (Open Source Project Managers)**

- Open Source project managers, known as "stewards," are responsible for implementing cybersecurity policies for the software they maintain.
- They must encourage the responsible disclosure of vulnerabilities and collaborate with authorities to manage security risks.

2. **Enhanced Security Requirements**

- Open Source software must adhere to cybersecurity standards throughout its lifecycle, similar to proprietary software.
- This includes proactive vulnerability management and the provision of regular security updates.

3. **Certification and Compliance**

- Open Source projects will need to demonstrate their compliance with CRA requirements, which may involve security audits and certifications.
- This could pose a challenge for small projects or individual developers, who often lack the resources to comply with complex regulations.

4. **Collaboration with Authorities**

- Open Source project managers will need to work with European authorities to report vulnerabilities and coordinate fixes.
- This collaboration aims to ensure that Open Source software, often used in critical infrastructures, remains secure.

5. **Impact on the Open Source Community**

- The CRA could encourage better security management in Open Source projects by imposing stricter practices.
- However, it could also create tensions, as some developers might see these requirements as an excessive administrative burden.

6. **Opportunities for Open Source Projects**

- Open Source projects that comply with the CRA could gain credibility and adoption, as they will be perceived as more secure.
- This could also foster better collaboration between Open Source projects and companies seeking secure solutions.

7. **Challenges for Small Projects**

- Small Open Source projects might struggle to meet CRA requirements due to their lack of resources and security expertise.
- This could create inequality between well-funded large projects and small community projects.

The CRA aims to strengthen the security of Open Source software by imposing strict standards and holding project managers accountable. While this could improve overall security, it could also pose challenges for small projects and require increased collaborative efforts within the Open Source community.

NIS2

The NIS 2 Directive (Network and Information Systems 2) is European legislation aimed at strengthening cybersecurity within the European Union. It replaces the initial NIS Directive and introduces stricter and broader cybersecurity requirements.

The main impacts of NIS 2 on open-source solutions are as follows:

- **Promotion of Open Source Solutions**: NIS 2 explicitly encourages the use of open-source solutions to improve cybersecurity. Open-source cybersecurity tools and applications are recognized for their transparency, interoperability, and ability to foster industrial innovation. The directive highlights that open-source solutions can contribute to greater openness and better efficiency in industrial innovation. It also recommends the use of open standards to improve the security of infrastructures.

- **Cost Reduction for SMEs**: NIS 2 emphasizes that open-source solutions can help small and medium-sized enterprises (SMEs) reduce the costs associated with complying with new cybersecurity requirements. By adopting open-source tools, SMEs can minimize expenses while meeting the security standards imposed by the directive.

- **Community and Transparency**: The directive promotes a community approach to identifying vulnerabilities, which is a fundamental principle of open-source projects. The inherent transparency of open-source solutions allows for easier verification and faster identification of security flaws.

- **Compliance Obligations**: Companies must implement cybersecurity risk management measures, including the use of open-source solutions to comply with NIS 2 requirements. This includes implementing security policies, incident notification, and conducting security audits.

- **Impact on Cybersecurity Solution Providers**: NIS 2 creates opportunities for cybersecurity solution providers, including those offering open-source tools. Companies and public organizations will

need to comply with the new requirements, which can stimulate demand for open-source cybersecurity solutions.

In summary, NIS 2 promotes the adoption of open-source solutions to improve cybersecurity in Europe, highlighting their transparency, interoperability, and potential for cost reduction, particularly for SMEs.

CVE & Open Source

A CVE, or "Common Vulnerabilities and Exposures," is a public referencing system for computer security vulnerabilities and exposures. Each CVE entry is identified by a unique number (CVE ID) and contains a description of the vulnerability or exposure, as well as relevant public references. CVEs play a crucial role in computer security management by enabling clear and unified communication about vulnerabilities, helping organizations identify, prioritize, and fix security flaws more effectively.

It is not possible to categorically state that Open Source software has more security flaws than proprietary software, or vice versa. Security depends more on the quality of development, the security practices followed, and the speed at which vulnerabilities are addressed.

Managing CVEs for Open Source Solutions

For Open Source solutions, managing CVEs is crucial to maintaining the security and integrity of projects.

In the context of Open Source, the management of CVEs (Common Vulnerabilities and Exposures) follows these steps:

- **Vulnerability Detection**: Vulnerabilities can be discovered by security researchers, developers, or users. Once identified, they are reported to the project maintainers.
- **CVE Assignment**: Confirmed vulnerabilities receive a unique CVE identifier. This allows for standardized tracking and referencing of the vulnerability.
- **Notification and Communication**: Project maintainers inform the community of users and developers about the vulnerability. This can be done through mailing lists, forums, announcements on the code repository (such as GitHub), or security bulletins.
- **Patch Development**: Developers work on patches to fix the vulnerability. These patches are then tested to ensure they resolve the issue without introducing new vulnerabilities.
- **Patch Release**: Once the patches are validated, they are released in a new version of the software. Users are encouraged to update their installations to benefit from the security patches.
- **Monitoring and Maintenance**: Maintainers continue to monitor vulnerability reports and release security updates as needed. Security analysis tools can also be used to automatically detect vulnerabilities in the code.
- **Community Collaboration**: The open-source community plays a key role in CVE management. Contributions from developers worldwide help in quickly detecting and fixing vulnerabilities.

CVE management in open-source projects relies on transparency, collaboration, and responsiveness. Maintainers and contributors work together to ensure that the software remains secure and reliable for all users.

Security Tooling in GitHub & GitLab Forges

GitHub and GitLab offer several mechanisms to verify the security of the source code. GitHub and GitLab allow the integration of security tests into development workflows, which helps identify and fix vulnerabilities proactively. The features offered by these tools to manage the security of source codes hosted in projects are as follows:

- **Code Scanning**: Automatic analysis of the code to detect vulnerabilities and security errors.

- **Secret Scanning**: Detection of secrets (such as API keys, passwords, etc.) that have been accidentally included in the code.

- **Dependency Review**: Analysis of dependencies (versions of libraries used, etc.) to identify known vulnerabilities in outdated or non-updated versions.

Third-party security tools like Snyk, Dependabot, or OWASP ZAP can be used for more in-depth analyses.

LTS Version

An LTS (Long Term Support) version of an Open Source software is a specific version that receives updates and extended support for a longer period than standard versions. LTS versions are designed to provide greater stability and security, making them ideal for production environments where reliability is crucial.

Here are some key features of LTS versions:

- **Stability:** LTS versions are generally more stable as they have been thoroughly tested.
- **Security:** They receive regular security updates to fix vulnerabilities.
- **Extended Support:** Support can extend over several years, offering users a prolonged period during which they can rely on updates and patches.
- **Compatibility:** LTS versions are often used in environments where long-term compatibility is important, such as critical infrastructures and enterprise applications.

LTS versions are particularly popular in Linux distributions like Ubuntu, where they are used by businesses and organizations that need a reliable and durable software base.

The ESR (Extended Support Release) version of Firefox is similar to an LTS version. It is designed for organizations, businesses, and institutions that need a stable and secure version of Firefox over an extended period.

Some companies, such as Red Hat, SUSE, and Canonical, offer versions of their Open Source products with long-term support. They provide security updates, patches, and technical support as part of a paid subscription offering. For example, with its paid Extended Support Maintenance (ESM) offering, Canonical provides for its distribution "10 years of vulnerability management for selected critical, high, and medium security issues for all software shipped with Ubuntu."

These various forms of long-term support allow users to benefit from the stability and security of Open Source software over a sufficiently long period, compatible with the lifecycle of enterprise applications.

Best Practices (OWASP, ANSSI)

OWASP provides various tools that are recommended for use in analyzing the source code of open-source solutions.

- **OWASP Top Ten**: This is a list of the ten most critical security risks for web applications. This list is regularly updated and widely used by developers and security professionals to assess and improve the security of their applications.

- **OWASP Testing Guide**: A comprehensive guide for testing the security of web applications. It provides methodologies and techniques for identifying security vulnerabilities.

- **OWASP Code Review Guide**: A guide for conducting security-focused code reviews. It helps developers identify potential security flaws in the source code.

- **OWASP ZAP (Zed Attack Proxy)**: An open-source tool for testing the security of web applications. ZAP automatically identifies security vulnerabilities in web applications.

- **OWASP Cheat Sheets**: Practical and concise guides on various application security topics. They provide tips and best practices for securing web applications.

- **OWASP Dependency-Check**: A tool that identifies known vulnerabilities in a project's dependencies. It helps manage risks associated with third-party libraries and frameworks.

- **OWASP ModSecurity Core Rule Set (CRS)**: A set of rules for the ModSecurity web application firewall. It helps protect web applications against common attacks.

OWASP plays a crucial role in raising awareness and educating about application security. Its resources and tools are widely used by developers, security testers, and organizations to improve the security of their web applications.

Best Practices (OWASP, ANSSI)

OWASP provides various tools that are recommended for use in analyzing the source code of Open Source solutions.

- **OWASP Top Ten:** This is a list of the ten most critical security risks for web applications. This list is regularly updated and widely used by developers and security professionals to assess and improve the security of their applications.
- **OWASP Testing Guide:** A comprehensive guide for testing the security of web applications. It provides methodologies and techniques for identifying security vulnerabilities.
- **OWASP Code Review Guide:** A guide for conducting security-focused code reviews. It helps developers identify potential security flaws in the source code.
- **OWASP ZAP (Zed Attack Proxy):** An open-source tool for testing the security of web applications. ZAP automatically identifies security vulnerabilities in web applications.
- **OWASP Cheat Sheets:** Practical and concise guides on various application security topics. They provide tips and best practices for securing web applications.
- **OWASP Dependency-Check:** A tool that identifies known vulnerabilities in a project's dependencies. It helps manage risks associated with third-party libraries and frameworks.
- **OWASP ModSecurity Core Rule Set (CRS):** A set of rules for the ModSecurity web application firewall. It helps protect web applications from common attacks.

OWASP plays a crucial role in raising awareness and educating about application security. Its resources and tools are widely used by developers, security testers, and organizations to improve the security of their web applications.

Role of ANSSI

ANSSI (National Agency for the Security of Information Systems, France) plays a key role in promoting and securing Open Source software, particularly by contributing to projects like Suricata and conducting security audits on Open Source products. ANSSI also maintains reference lists of qualified Open Source tools for the needs of the administration, evaluated according to security criteria.

Here are some of the main recommendations from ANSSI regarding Open Source software:

- **Risk Assessment:**
  - Conduct a risk assessment for each Open Source component used. This includes identifying known vulnerabilities and evaluating the potential impact on security.
- **Provenance and Reliability:**
  - Verify the provenance of Open Source software. Use reliable and verified sources to download Open Source components.
  - Prefer well-maintained Open Source projects supported by an active community.
- **Vulnerability Management:**
  - Implement a security monitoring process to track vulnerabilities discovered in the Open Source components used.
  - Regularly apply security updates and patches.
- **Code Analysis:**
  - Use static and dynamic analysis tools to detect vulnerabilities in Open Source code.

    - Conduct code reviews to identify potential security flaws.
- **Secure Integration:**
    - Integrate Open Source components securely into information systems. This includes secure configuration and isolation of critical components.
    - Use containers and virtualized environments to isolate Open Source components.
- **Documentation and Traceability:**
    - Document the use of Open Source components, including the versions used and download sources.
    - Maintain traceability of changes made to Open Source components.
- **Training and Awareness:**
    - Train development and security teams on best security practices for Open Source software.
    - Raise user awareness of the risks associated with using unsecured Open Source software.
- **Compliance and Licenses:**
    - Verify the compliance of used Open Source licenses with internal policies and applicable regulations.
    - Ensure the compatibility of Open Source licenses with other software components used.
- **Security Testing:**
    - Integrate security tests into the development and deployment processes of Open Source solutions.
    - Use security testing tools to validate the robustness of Open Source components.
- **Incident Response Plan:**
    - Implement an incident response plan to manage vulnerabilities and attacks affecting Open Source components.
    - Define procedures for the rapid notification and correction of vulnerabilities.

These recommendations aim to help organizations use Open Source software securely and minimize associated risks. ANSSI encourages a proactive and rigorous approach to managing the security of Open Source solutions.

HR Impact: Sector Attractiveness for Recruitment

Open Source is a powerful lever for attracting young talent. Accustomed to collaborating in this manner from their school days, these individuals naturally expect to find this approach in the professional world. Thus, Open Source represents not only a means to attract them but also to retain them. Indeed, while it is essential to recruit new employees, it would be unfortunate to see them leave after three years. In this context, Open Source proves to be an excellent tool for encouraging them to join and stay with us in the long term.

Open Source offers several advantages for recruitment in a company, including:

1. **Access to a Talent Pool:** Open Source projects attract passionate and talented developers from around the world. Companies can identify and recruit active contributors who have already demonstrated their skills in real projects.
2. **Assessment of Technical Skills:** Contributions to Open Source projects allow recruiters to directly assess the technical skills of candidates. The code is often public, making it possible to judge the quality of work, the ability to collaborate, and the understanding of best development practices.
3. **Engagement and Passion:** Developers who contribute to Open Source projects often show a strong commitment and passion for their work. These qualities are valuable in a professional environment as they can lead to greater productivity and innovation.
4. **Networking and Visibility:** Participating in Open Source projects can increase a company's visibility within the tech community. This can attract candidates who are looking for companies with a culture of innovation and collaboration.
5. **Training and Development:** Open Source projects offer opportunities for continuous training. Developers can learn new technologies, methodologies, and best practices by working on Open Source projects.
6. **Innovation and Collaboration:** Open Source fosters a culture of innovation and collaboration. Companies that adopt these values can attract talent seeking a dynamic and collaborative work environment.
7. **Reduction in Recruitment Costs:** By identifying talent through Open Source contributions, companies can reduce the costs associated with traditional recruitment processes, such as agency fees or advertising costs.

In summary, Open Source can be a strategic asset for recruitment, enabling companies to attract skilled and passionate talent while strengthening their image in the tech community.

Recruitment and Attractiveness

The use of Open Source by a company can have a significant impact on its HR recruitment, particularly in attracting talent. Developers and IT professionals are often attracted to companies that use and contribute to Open Source projects.

It is therefore important to specify in job descriptions if Open Source solutions are used and if the employee will be required to contribute and participate in the Open Source ecosystem as part of their professional activities..

Employee Retention

Employees need perspectives and the ability to envision their careers within a company. Open Source projects allow employees to develop and maintain technical skills, enabling them to stay at the forefront of technology. This can increase their job satisfaction and commitment to the company.

The use of Open Source solutions, and especially participation in the creation and improvement of Open Source solutions, provides an additional and important sense of purpose to the work of employees.

Brand Image

The use of Open Source, and especially contributing to the Open Source ecosystem with communication on this subject, enhances the company's reputation and attracts high-quality candidates.

Collaborating with the Open Source ecosystem has a very positive impact on a company's image for several reasons:

- **Reputation Enhancement:** Companies that actively contribute to Open Source projects are often seen as technological leaders and innovators. This can improve their reputation with clients, partners, and potential talents.
- **Talent Attraction:** Developers and IT professionals are often attracted to companies that support and contribute to Open Source. This can help attract and retain high-quality talent.
- **Transparency and Trust:** Open Source fosters transparency and trust. Companies that adopt these principles can strengthen the trust of their clients and partners, thereby improving their brand image.
- Innovation and Technological Leadership: By contributing to Open Source, companies can demonstrate their commitment to innovation and technological leadership. This can position them as key players in their industry.
- **Social Responsibility:** Collaborating with the Open Source ecosystem can be seen as a form of social responsibility. Companies can show that they are committed to sharing knowledge and developing open and accessible solutions.
- **Visibility and Marketing:** Contributions to Open Source projects can provide increased visibility for the company. Open Source projects are often widely used and recognized, which can enhance the company's reputation.
- **Collaboration and Partnerships:** By participating in the Open Source ecosystem, companies can establish collaborations and partnerships with other organizations, which can strengthen their network and influence in the industry.
- **Community Engagement:** Companies that engage in Open Source can benefit from strong community support. This can enhance their image as a collaborative and community-oriented company.

In summary, collaborating with the Open Source ecosystem can strengthen the company's reputation, attract talent, promote transparency and trust, demonstrate innovation and technological leadership, and improve the company's visibility and partnerships, while strengthening its community engagement.

Artificial Intelligence & Open Source

Key points for decision-makers

The Open Source Initiative (OSI) has proposed a strict definition of Open Source AI. This vision, which requires training sets to be Open Source too, has provoked numerous reactions, as it calls into question several so-called "open weights" models, but which do not meet the criteria of openness.

Introduction

In the field of artificial intelligence, Open Source technologies offer powerful and accessible tools for developing robust applications. The Open Source domain offers a set of Open Source assets, extended language models (LLMs) and user interface development frameworks, essential tools for accelerating the creation of AI applications within enterprise I.S..

Open Source A.I. : the OSI definition

The Open Source Initiative (OSI), the reference organization for defining what Open Source is (including compliant licenses), recently proposed a strict definition of Open Source AI1.
Based on the principle of free software, the OSI definition requires Open Source AI to offer its users four freedoms:

- Use the system for any purpose without having to ask permission.
- Study the system's operation and inspect its components.
- Modify the system for any purpose, including changing its results.
- Share the system so that others can use it, with or without modifications, for any purpose.

Put another way,

- Is the tool open/Open Source?
  - Its code, its algorithm?
  - Its data sets?
  - Its interfaces and applications?
- Where does the data come from?
  - Voluntary sources, ceded, monopolized?
  - Free or proprietary sources?

A model is truly Open Source if :

- it is available under an unrestricted license,
- its training methodology is provided in full transparency
- its data set is supplied under a free license.

Note that in this OSI definition, there is no obligation to provide training scripts or to explain how the AI was trained.

Model Openness Framework (MOF) from the Linux Foundation

Linux Foundation AI & Data Foundation

The Linux Foundation AI & Data Foundation (LF AI & Data) is an umbrella organization under the Linux Foundation, dedicated to supporting and promoting open-source innovation in the fields of artificial intelligence (AI), machine learning (ML), deep learning (DL), and data.

The Model Openness Framework (MOF)

Methodology Based on the principles of open-source solution evaluation methodologies, the Generative AI Commons of the Linux Foundation AI & Data Foundation has designed and developed the Model Openness Framework (MOF), a comprehensive system for evaluating and classifying the completeness and openness of machine learning models. This framework assesses which components of the model development lifecycle are made public and under which licenses, thereby ensuring an objective evaluation. The goal is to provide a simple tool for evaluating machine learning models against the MOF framework. This tool helps users understand which components are included in each model and the licenses associated with these components, clarifying what can and cannot be done with the model and its components. The MOF presents users with 16 questions about their model. Users must provide detailed answers for each question. Based on this data, the tool calculates a score, ranking the model's openness on a scale of 1, 2, or 3.

Impact of AI on Open Source

The emergence and democratization of AI have revolutionized the entire software industry and open-source solutions. Open-source solutions are increasingly integrating AI features by leveraging the APIs of existing AI solutions. This integration has now become a part of the roadmaps and evolutions of these solutions.

Hugging Face

The collaborative nature of Open Source fosters innovation in AI. Developers from around the world can contribute to open-source projects, share ideas, and continuously improve AI-related features. Platforms like Hugging Face facilitate this collaboration by allowing developers to share code, report issues, and suggest improvements.

Hugging Face is a leading collaborative platform in the field of artificial intelligence, offering advanced tools and models for various applications. It provides a vast collection of machine learning models and datasets, enabling developers and researchers to access cutting-edge resources for their AI projects.

Focus on the AI, Machine Learning, and Data Science Ecosystem

Machine Learning

Machine Learning (ML) is a subset of artificial intelligence (AI) that focuses on the development of algorithms and statistical models enabling computer systems to perform complex tasks without explicit instructions. ML systems rely on models and inferences to analyze large amounts of data, identify patterns, and produce informed results. ML is a key component of AI that allows machines to learn and improve from data, while AI encompasses a broader range of technologies aimed at mimicking human intelligence.

There are many Open Source Machine Learning tools, the most well-known being:

- **Scikit-learn:** An Open Source Python library for Machine Learning and data analysis. It offers efficient algorithms for classification, regression, and clustering.
- **TensorFlow:** A popular Open Source platform for Machine Learning and Deep Learning, developed by Google. It is widely used to create and deploy ML models on various platforms and devices.
- **PyTorch:** An Open Source library for Machine Learning, particularly appreciated for its flexibility and ability to handle dynamic computations. PyTorch is supported by an active community and used by companies like Facebook and Tesla.

Scikit-learn / Probable

Scikit-learn is an Open Source Python library designed for machine learning. It provides simple and efficient tools for data analysis and the development of predictive models.

Here are some of its main features:

- **Ease of Use:** Scikit-learn is designed to be easy to use, even for beginners in machine learning. It offers a consistent and intuitive interface for the different stages of the modeling process.
- **Wide Range of Algorithms:** The library includes a vast collection of machine learning algorithms, covering regression, classification, clustering, dimensionality reduction, feature selection, and more.
- **Interoperability:** Scikit-learn is designed to work seamlessly with other popular Python libraries such as NumPy, SciPy, and Pandas, facilitating integration into existing data workflows. Comprehensive
- **Documentation:** Scikit-learn is well-documented, with code examples, tutorials, and detailed documentation for each algorithm and feature.
- **Active Community:** As an Open Source project, Scikit-learn benefits from an active community of contributors and users, ensuring regular updates and continuous support.
- **Performance:** Although Scikit-learn is designed to be easy to use, it is also optimized for performance, making it suitable for medium to large-scale machine learning tasks. In summary, Scikit-learn is a powerful and versatile library for machine learning in Python, offering a wide range of algorithms and tools for data analysis and the development of predictive models.

In summary, Scikit-learn is a powerful and versatile library for machine learning in Python, offering a wide range of algorithms and tools for data analysis and the development of predictive models.

Open Source LLM

An LLM, or Large Language Model, is a type of artificial intelligence model designed to understand and generate human language. These models are trained on vast amounts of text to learn language patterns and structures, enabling them to generate coherent and contextually appropriate responses to a variety of questions or requests.

LLMs can be used in various applications, such as chatbots, machine translation, text generation, and more. They are capable of understanding and responding in multiple languages and can even perform complex tasks like summarizing texts or answering factual questions.

Frameworks for Conversational Interfaces

Many Open Source frameworks enable the efficient and rapid creation of chatbot user interfaces or the development of conversational applications.

Other Open Source Resources

Other Open Source resources, including useful libraries, APIs, and services, allow for the creation of high-performance AI applications.

Artificial intelligence (AI) can assist developers in several ways, including automating repetitive tasks, providing suggestions to improve code and application design, optimizing images and videos for better website performance, and generating quality documentation or customized chatbots.

AI and Software Development

With the increasing integration of artificial intelligence (AI) in software development, new challenges arise in the field of free software compliance. AI systems designed to generate code are trained on large datasets, which often include a variety of OSS codes.

As a result, it is likely that AI, when generating new code, reproduces parts of an original Open Source code. Copyleft licenses require that new software based on OSS be published under the copyleft license. Therefore, the use and commercialization of AI-generated code may present the risk of violating the corresponding OSS licenses, leading to security issues.

Specialized Models (Code Generation)

The issue is that the code generated by AI is not bug-free. On the contrary, code created with AI generates more bugs and consequently, more maintenance and more delays. Reference: 2024 DORA report (Google report on AI usage).

There is therefore a need to rigorously test the code and fix any issues before production, as AI-generated code can be imperfect or not optimized. AI is therefore there to assist and not replace the expertise of developers.

You must then always use static code analysis tool to check the compliance of the generated source code. The Software Compliance Team is there to help you on this topic.

GitHub Copilot

GitHub Copilot is an AI-powered code assistant that helps developers write and debug code. It can suggest auto completion elements when you start writing code, but also respond to text queries that describe what you want the code to achieve as an action. Powered by a generative AI model designed by GitHub, OpenAI, and Microsoft, this AI assistant is available as an extension for Visual Studio Code, Neovim, JetBrains, Azure Data Studio, etc.

Strategic Issues and Interests for Thales

For Companies

Artificial Intelligence (AI) presents numerous strategic challenges and interests for companies.

Here are some of the main aspects to consider:

- **Competitiveness:** AI can provide a competitive advantage by improving operational efficiency, reducing costs, and increasing productivity.
- **Innovation:** AI enables the development of new products and services, or the improvement of existing ones, by leveraging data and advanced analytics.
- **Personalization:** Companies can use AI to offer personalized customer experiences, which can improve customer satisfaction and loyalty.
- **Decision Making:** AI can help make more informed decisions through the analysis of large amounts of real-time data.
- **Automation:** Automating repetitive tasks frees up time for higher value-added activities.
- Risk Management: AI can be used to identify and mitigate risks, whether financial, operational, or security-related.

Strategic Interests:

- **Improving Customer Experience:** Chatbots and virtual assistants can provide 24/7 customer service, enhancing the overall experience.
- **Process Optimization:** AI can optimize supply chains, inventory management, and other operational processes.
- **Predictive Analysis:** Companies can use AI to forecast market trends, customer behaviors, and other important variables.
- **Security and Compliance:** AI can help detect fraud, cyber threats, and ensure regulatory compliance.
- **Sustainable Development:** AI can contribute to more sustainable practices by optimizing resource use and reducing waste.
- **Talent and Skills:** Investing in AI can attract specialized talent and foster a culture of innovation within the company. However, the adoption of AI also comes with challenges, such as ethical concerns, data protection, and the need to train employees to use these new technologies. Companies must therefore adopt a balanced approach to maximize benefits while managing associated risks.

Thales, Co-founder of Confiance.IA

Confiance.IA is a European foundation for trustworthy AI. This non-profit organization was created by industrial leaders including Thales. Its mission is to provide industry with cutting-edge open-source methodologies and tools, enabling the design of AI-based systems that can be trusted and compliant with regulations.

The foundation aims to be a driving force behind an ambitious European strategy for responsible and industrial AI. Its ambition is to propel Europe to the forefront of innovation in trustworthy AI, making its methodologies and tools an international reference and thus supporting the wider adoption of responsible AI in industry.

The foundation addresses all stakeholders involved in the development and adoption of responsible and industrial AI, including industrial companies, researchers and laboratories, technological start-ups and SMEs, as well as standardization bodies and regulators. By joining the foundation, these stakeholders gain access to a privileged network to collaborate, innovate, and actively contribute to shaping the future of industrial AI in Europe.

The foundation has four main missions for trustworthy AI:

- Lead and expand the community dedicated to responsible and industrial AI engineering, forging close links with various initiatives.
- Ensure regulatory compliance and contribute to standards, ensuring that methodologies and tools comply with the AI Act and other regulations.
- Manage and distribute open-source assets resulting from the Confiance.ai program, offering industries a range of courses tailored to each type of use.
- Support the transition to responsible AI by co-designing training for new professions and helping to build the skills of future trustworthy AI experts.

Open Hardware & AI at Thales

As part of its embedded hardware activities, an entire branch of AI-related activities specializes in the encountered issues. To do this, teams work and collaborate in co-design mode, between RISC-V architecture experts and AI algorithm experts.

Although this approach requires the development of new specific methods and algorithms, it allows for the simultaneous optimization of different aspects rather than treating them sequentially.

Open Data & AI

Given the importance of having data with "ground truth" to train and validate AI models, open data is interesting. Indeed, AI models require data to be trained, and open data provides a valuable source of accessible and usable data. Open data can thus help obtain high-quality and well-labeled datasets, essential for the development of reliable and robust AI solutions.

On the same principles as Inner Source (internal sharing of software source code), there is the possibility of internal data sharing, similar to open data, but in a restricted and secure manner. This allows different departments and teams at Thales to access common datasets for their projects while respecting confidentiality and security constraints.

Evolution of Licenses and Impact: The Case of the YOLO Library

YOLO (You Only Look Once) is an open-source library used for real-time object detection. It is particularly known for its speed and accuracy in identifying and locating objects in images or videos. YOLO uses convolutional neural networks (CNN) to perform this task, making it a powerful tool in the field of computer vision. YOLO is a specific application of AI, more precisely machine learning and deep learning.

The YOLO library has gone through several versions over the years, and the licenses associated with these versions have also evolved.

Version 1 of this library had a proprietary license, allowing free use. Version 2 corresponds to the transition to a simpler license (a few lines). With version 3, the project's source code moved to a more official and recognized open-source license, namely the GPLv3 (GNU General Public License version 3). This license is copyleft, meaning that any modification or extension of the code must also be published under the same license.

Version 5 is published under the GNU AGPL-3.0 license (Affero General Public License version 3.0). This license is similar to GPLv3 while including additional provisions to cover SaaS usage cases.

The latest open-source license used allows the community to contribute to the development of YOLO, use the code for their own projects, and share modifications with others. However, it is important to respect the terms of the license, particularly regarding the redistribution and modification of the source code.

These changes in licenses over the versions illustrate the necessity and the challenge of monitoring and keeping up with the evolution of projects, libraries, and other software used.

Open Source Program at Thales

"Open Source is the best way to stimulate creativity and ensure the performance, security, and maintainability of Thales' products and services."
Daniel GLAZMAN, VP Software Technologies at Thales

Key Takeaways

Open Source is a strategic pillar for the Thales Group.

1. Our mindset towards Open Source is to Use / Contribute / Publish.
2. All employees are encouraged to contribute: share assets, contribute to Open Source projects, submit a ticket, or participate in a working group.
3. Governance and tooling processes are in place to assist employees.
4. Each Thales Open Source asset must be published in our Thales GitHub_organization
5. The Open Source team is available to support you: oss@thalesgroup.com

Open Source Hardware at Thales

Thales' approach aligns with the proactive European policy aimed at establishing a sovereign Open Hardware ecosystem. This addresses a dual challenge: enhancing the design and manufacturing capabilities of microprocessors and advancing these technologies in current and future markets such as automotive, industrial automation, communications, data infrastructure, healthcare, and defense.

While the European Commission has established a roadmap with the Chips Act to develop sustainable, next-generation semiconductor production capabilities, Open Hardware constitutes the new sovereignty and resilience challenge. It enables Europe to protect itself from disruptions in the hardware supply chains.

Why Thales Invests in RISC-V

RISC-V is an open instruction set that has been gaining increasing interest over the past few years. It allows the execution of complex software on a processor without dependency on proprietary solutions, reducing access costs and enabling customers to regain their technological sovereignty.

Thales invests in RISC-V for several reasons:

- Presence of a strong Open Source community
- Sovereignty of the model
- Security and safety
- SWaP and customization

RISC-V has a vast ecosystem offering compatibility across its various implementations. There is no proprietary lock-in (Vendor Locking), which facilitates commercial opportunities for support and customization. The model is state-of-the-art in processors and allows for high performance.

- Thales brings its expertise in the design of secure and safe microprocessors.
- Thales aims to federate the industrial and academic stakeholders involved in this field.
- The stakes of this revolution touch most embedded systems in aeronautics, space, automotive, railway, security, and defense.

Now a member of the RISC-V Foundation, Thales affirms its commitment to advancing the adoption and implementation of free and open hardware architectures based on RISC-V processors. This is an opportunity for Thales to become a major player in a new era of microprocessor design. The stakes are high as Open

Source in the hardware domain draws inspiration from the philosophy and success of Linux in the software world.

Leveraging its expertise in the security and safety of critical embedded systems, Thales aims to contribute to the RISC-V community by developing best safety practices with all industrial and academic stakeholders. This will focus on improving safety for Internet of Things devices, embedded systems, and machine learning implementations.

RISC-V has distinguished itself in recent years in improving the security of microprocessors against cyber threats. Thales' expertise in this field will further enhance functional safety. The Group will collaborate with Open Source communities to design microprocessors compatible with the requirements of future critical systems.

By combining an open approach to hardware and software, Thales and the RISC-V community are opening new perspectives in the design of critical mission systems present in all fields, including aeronautics, space, automotive, railway, security, and defense.

Thales' initiatives are fully aligned with the objectives of European policy aimed at:

- Creating a sovereign Open Source hardware ecosystem to strengthen microprocessor design and manufacturing capabilities in Europe.
- Promoting the use of these technologies in current and future markets, including the automotive industry, industrial automation, communications, data infrastructure, healthcare, and defense.

While the Chips Act proposed by the European Commission provides a roadmap for sustainable production of next-generation semiconductors, Open Source hardware helps ensure technological sovereignty and resilience to protect Europe from disruptions in hardware supply chains.

Open Source Software at Thales

How Open Source is Implemented at Thales

The Thales Open Source initiative was launched in 2020 at the initiative of the Group's Technical Directorate, with the following main objectives:

- Becoming a leading Open Source player
- Deploying a common Open Source tooling process across all GBUs
- Developing software and hardware communities around Open Source

The strategy to apply the Open Source model and change the mindset within Thales over the long term was achieved by:

- Building on the success of Thales Inner Source
- Providing a unique process and tools for Open Source
- Facilitating communication between all contributors

On December 10, 2025, Thales received the “Best Open Source Strategy” award at the Open Source Experience trade show. Presented by the CNLL (*Conseil national du logiciel libre*/National Free Software Council), this award recognizes the work carried out over the past five years by the Group’s Technical Directorate.
It primarily rewards:

- The structural and methodical transformation undertaken to promote Open Source
- The maturity of internal processes
- The actual impact within the Open Source community
- The commitment of teams across the company

This award confirms Thales’ focus on openness, collaboration, and innovation in software development.


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

Thales Open Source Governance and Process

Since 2020, Thales has established its Open Source Program Office to encourage Open Source practices across all business sectors. With the help of the Software Compliance team, each employee is supported to provide optimal quality Open Source resources and to carefully manage associated risks, particularly legal risks (IP, licenses, export control) and security risks (vulnerabilities, CVE).

Different profiles are involved in this governance:

- **Technical experts**
- **Legal experts**
- **Managers**
- **Compliance specialists**

The tooling process covers two main use cases for Open Source:

- **Publication:** when an employee, team, or project wants to share a Thales asset as Open Source.
- **Contribution:** when an employee, team, or project wants to contribute to an existing Open Source project, most often to correct a technical issue.

For both use cases, a publication/contribution request must first be submitted, consisting of a form describing the objectives, the desired license, the team in charge, and questions that will help the Thales Open Source team guide the requester throughout the process.

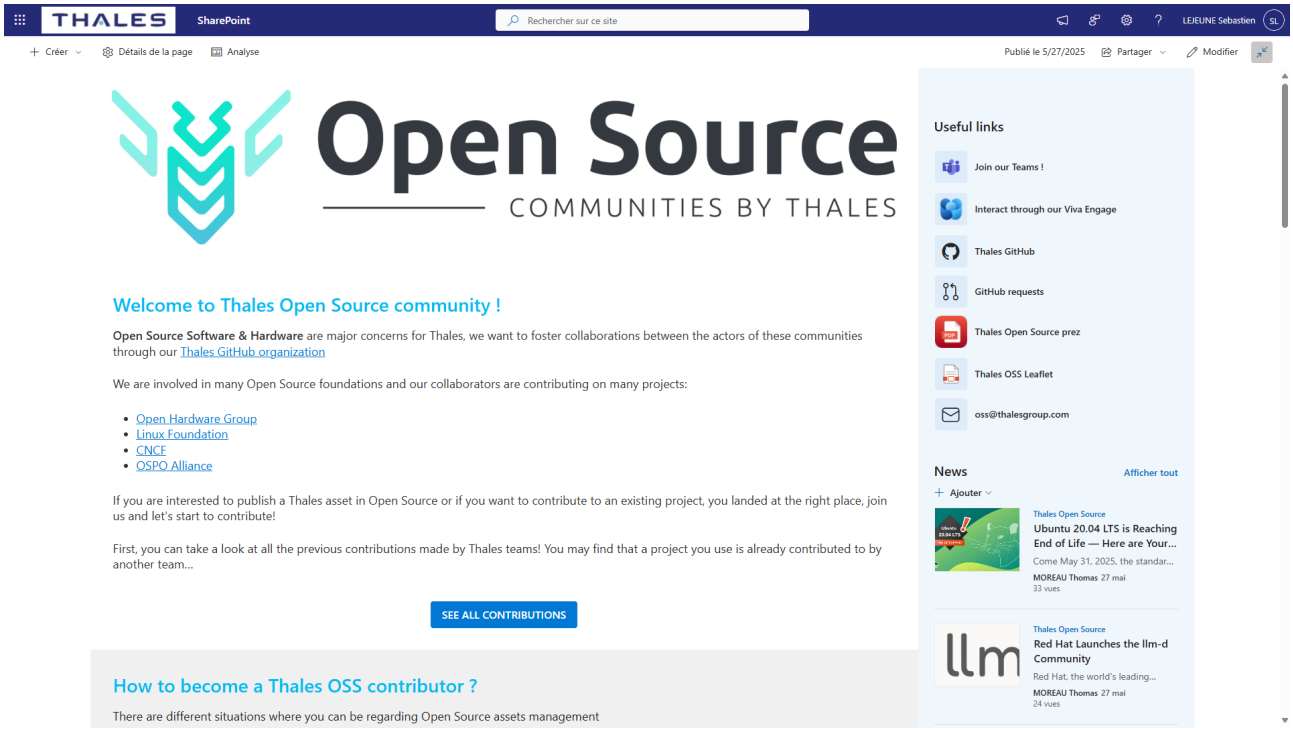
The request must then be approved by:

- A **manager** to verify alignment with the company's strategy.
- A **technical** expert to review the code and architecture.
- The **software compliance team** to ensure compliance with free software regarding intellectual property and cyber risks.
- A **legal expert** to validate the choice of Open Source license.

Once the request is approved, an invitation is made to the Thales GitHub organization to push the code into a repository that will be publicly visible once all approvals are obtained.

This process is the same for all Thales GBUs and countries wishing to interact with the Open Source ecosystem on behalf of Thales. It aims to ensure the quality of all our contributions, as a global leader in security, we pay particular attention to compliance issues.

Collaboration Tools



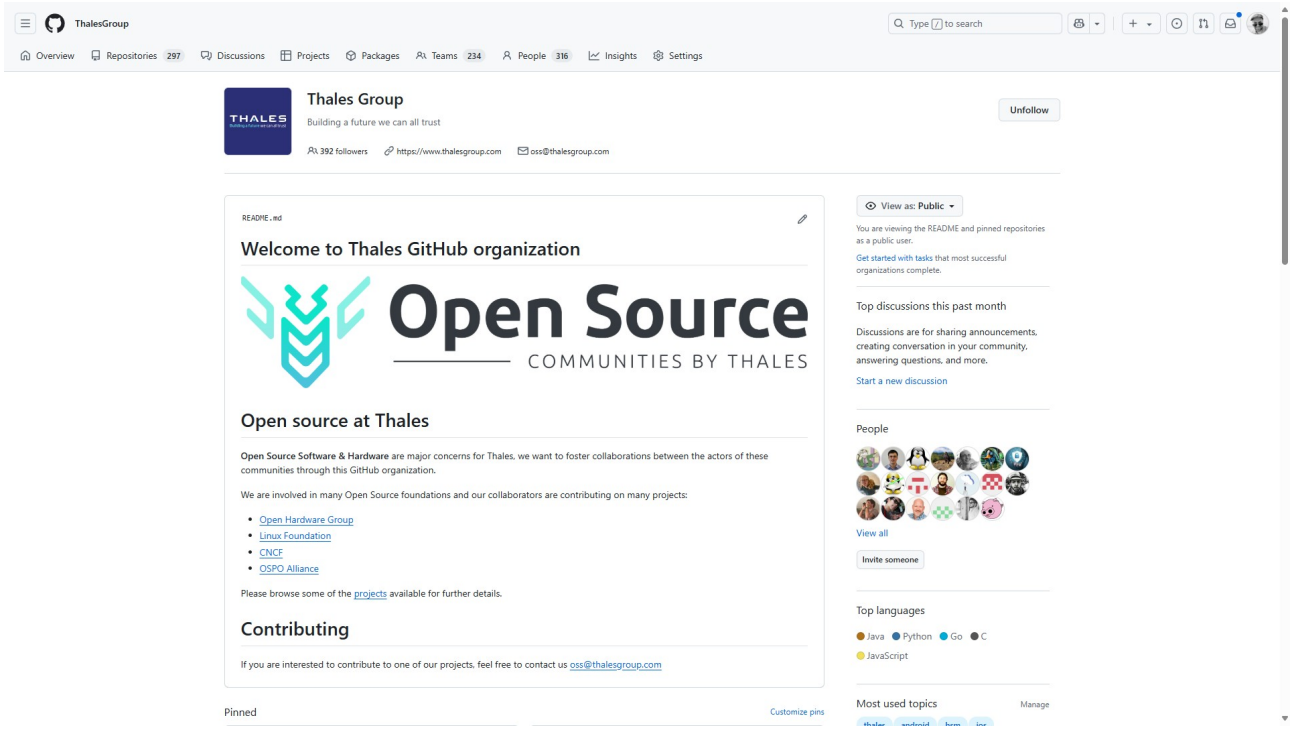
The Thales Open Source team has set up various collaboration tools:

- **Thales Open Source Portal :** this space contains all the information about the process, how to submit a publication or contribution request, contact the Software Compliance team, browse all the news and events...
- **Thales_GitHub_Organization:** It brings together all Thales' Open Source projects.
- **Viva Engage :** allows interaction with Thales' internal Open Source community.
- **oss@thalesgroup.com** : a single email to contact the Thales Open Source team.
- **uLearn module**: the employee explores the process and tools available to best integrate the Thales Open Source community.

Thales' GitHub Organization

To consult Thales' Open Source repositories, simply go to the Thales GitHub organization: https://github.-com/thalesgroup.

This organization constitutes the single entry point for the Thales Open Source community, and it is essential that any new Thales asset made Open Source be hosted there.



Repository and User Management

Thales developers contributing to OSS components will be invited to join the Thales GitHub organization.
A Thales employee is designated as the administrator of each Thales Open Source repository (public or fork) and will be responsible for:

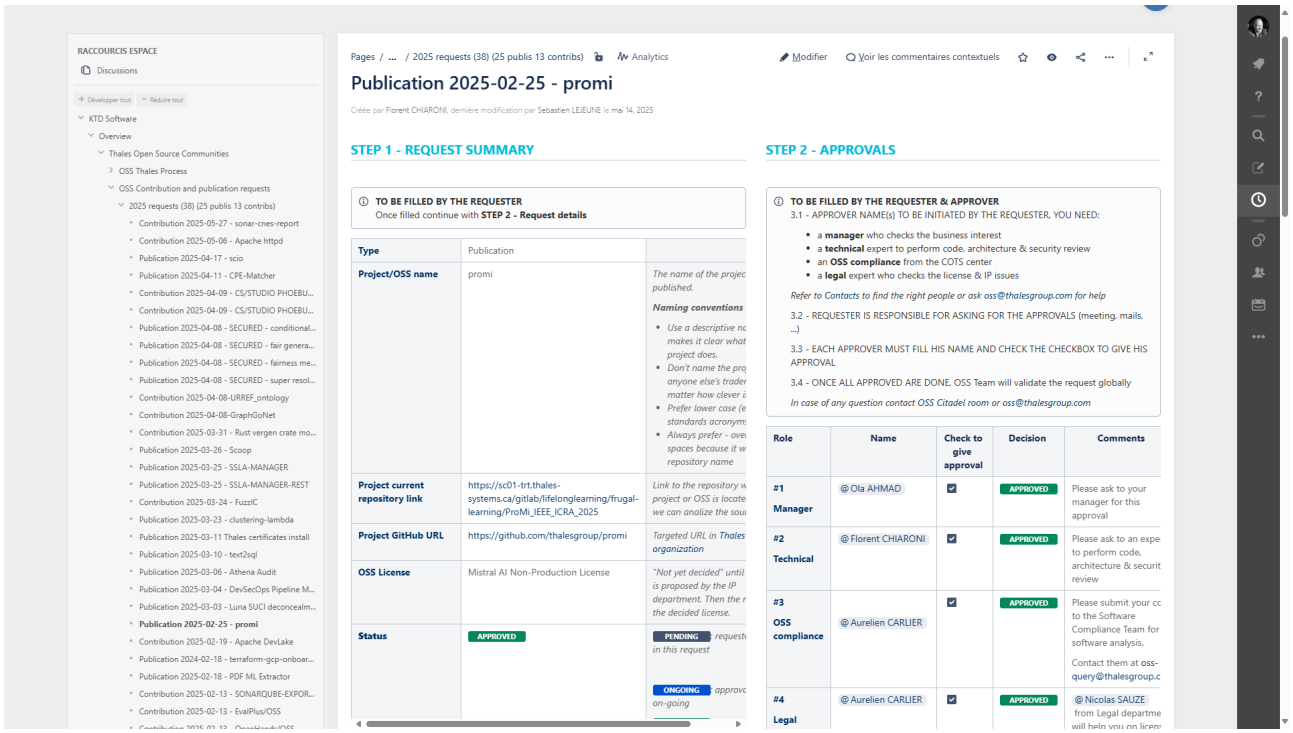
- Publishing and merging updates to the main codebase.
- Monitoring and fixing security issues.
- Responding to issues and pull requests.
- Managing repository users.

If there is a need to add or remove a member from a repository, it must go through the Thales Open Source ticketing system to request the necessary changes, which will be made by the Open Source team.

How to Share an Asset or Contribute to Open Source

The publication and contribution process is very simple:

1. Submit a new publication/contribution request to the Thales OSS team.
2. Fill in all the details and answer the questions.
3. Obtain approvals: management and technical first, OSS compliance and legal next.
4. Once this is done, the Thales GitHub repository (publication) or fork (contribution) is set up by the Thales OSS team.



Key Points about Thales' GitHub Organization

Thales has an official space on GitHub where a set of Open Source solution repositories are grouped: https://github.com/thalesgroup

The organization of this GitHub space by Thales is based on a code of conduct:

- Provision of good practice models.
- Thales OSS process for publication.
- All new assets must be deployed in this repository.
- Monitoring of source code security alerts.

Encouragement to Contribute

Thales strongly encourages contributions to Open Source solutions, whatever they may be, in compliance with the following rules:

- Preserve Thales' reputation.
- Follow the Thales OSS process.
- Respect the foundation's rules.
- Fork the project in Thales' GitHub space.

Thales Solutions Based on Open Source Components

First and foremost, Thales adopted Open Source because it allows us to fully master our solutions and their evolution over time, in the service of our customers, and particularly on the primordial aspect of security. Furthermore, Thales was convinced that the free offer of the time had the potential for scalability to integrate, over time, the functions that were deemed necessary. Thales has a strongly rooted culture in Open Source, and for several years, all "digital" solutions (Cloud, Big Data, AI, etc.) have been primarily market-driven by Open Source technologies.

Memberships in Foundations, Associations, and Organizations

As a member of the Eclipse Foundation, the Linux Foundation, and RISC-V International (since 2018), and CNCF – Cloud Native Computing Foundation (in 2023), Thales is among the leading European players in the Open Source movement and is committed to promoting the adoption and implementation of Open Source solutions.

Logo	Name	Date
	Foundation Eclipse	Since 2004[1]
	Foundation Linux	Since 2017[2]
	RISC-V International	Since 2018
	CNCF Cloud Native Computing Foundation	Since 2023

Through its involvement in Open Hardware and the broader Open Source movement, Thales has been committed for over 15 years to open and collaborative design and development practices.

Major External Events

The Open Source world is marked each year by a number of events, specialized around technologies or more generalist. These events are an opportunity for the different communities and professionals to meet and exchange, to keep abreast of developments, and to attend conferences.

These events can take place thanks to the support of sponsors who financially support the organizations.
As part of its involvement in the Open Source ecosystem, Thales participates in a few key events through sponsorship and conference presentations.
Break down silos with Inner Source!" (“Boostez la collaboration et cassez les silos grâce à l’Inner Source !”)

OSXP - Open Source Experience

Supported by the Systematic Paris-Region competitiveness cluster, Open Source Experience is the Tech - Usage - Business event dedicated to Open Source IT solutions, bringing together more than 4,000 profes-

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

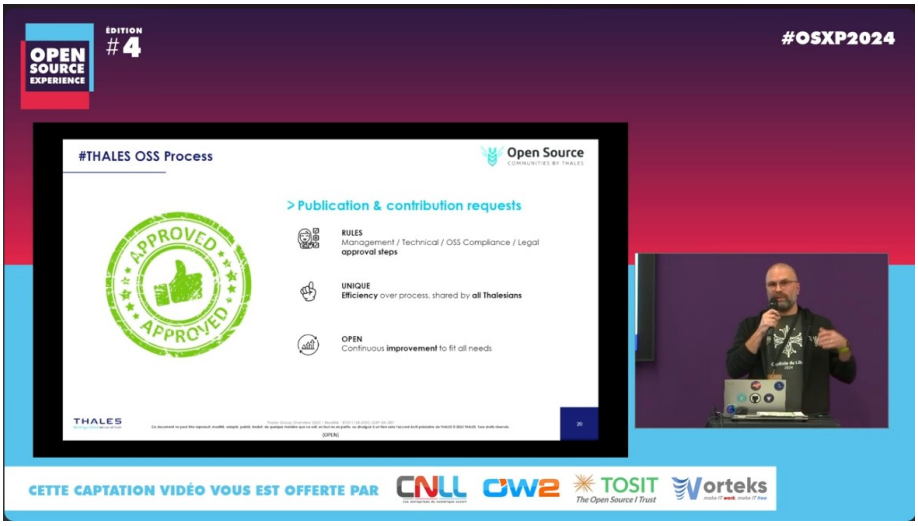
2 https://www.linuxfoundation.org/press/press-release/thales-joins-linux-foundations-core-infrastructure-initiative

sionals and digital players over 2 days. It is the main national event for the Open Source sector, held in Paris.

The show focuses on the technologies, solutions, and challenges of Open Source in France and Europe, and highlights the driving role of Open Source innovations in the digital transformation of organizations in technologies such as AI, Data Management, IoT, Cloud, and Blockchain.

An international showcase for technological excellence and the economic dynamism of the French Open Source sector, the event brings together global technological players, professional associations, companies and communities, a vast network of SMEs, and research organizations.

In 2022, the Open Source market in France was worth 6 billion euros, or 11% of the global digital market. This growth is sustainable and has multiplied by 40 in less than 20 years. With growth of 8.6% compared to the previous year, France is consolidating its position as the European leader.



During the 2024 edition, Sébastien LEJEUNE, OSPO of Thales, presented a conference "Happy birthday Thales OSPO!". In 2023, Anthony BORD (CDI) and Jérôme VENANT (SIX) came to talk about Open Source Hardware and Thales' involvement in RISC-V and the Open Compute Project (OCP).

RISC V Summit

RISC-V is the processor instruction set architecture (ISA) standard. The standard is open and allows for a series of new applications and research that will define the future of computing in Europe. Europe has played a central role in the success of RISC-V, with one-third of the global RISC-V community based in Europe.

The RISC-V Summit Europe is an annual event that, in 2025, was held in Paris. The objective of this event is to offer a cycle of conferences designed to help participants explore commercial & industrial, research, and academic applications.

As part of its Open Hardware-related program, Thales participates in the event as a Platinum-level sponsor (highest level), giving conferences such as "The case for Open Source Hardware at Thales: Motivations and Recent Milestones with CVA6" by Bernhard QUENDT, Chief Technical Officer of Thales Group.

Rust Paris

Organized by the Systematic Open Source Hub, the RUST PARIS conference brings together users and developers of the RUST programming language for a day of feedback and exchanges in French on the use of RUST in industry.

The aim is to offer developers, project managers, and decision-makers a place to share ideas and use cases and learn from each other about the best way to apply this language and its tools to constantly evolving challenges in various fields: embedded systems (especially for automotive and energy), formal verification and industrial certification, cybersecurity, WebAssembly for cloud and data processing, OS development, and high-frequency trading.

Thales has been a sponsor of the event for the last two editions in 2024 and 2025.

Kubecon

KubeCon

KubeCon is a conference dedicated to Kubernetes technology and the cloud-native ecosystem. Organized by the Cloud Native Computing Foundation (CNCF), it brings together developers, operators, architects, and decision-makers to discuss the latest advances, share knowledge, and explore best practices around Kubernetes and associated technologies. The conference offers technical sessions, workshops, keynotes, and networking opportunities, making KubeCon a must-attend event for the cloud-native community.

As a Silver member of the CNCF, Thales participated for the first time in KubeCon Europe 2024 in Paris by presenting its solutions and innovations in the field of cloud-native and Kubernetes. The Thales booth was a place where visitors could discover how Thales integrates these technologies to offer secure and high-performance solutions.

Thales' objective during this convention was twofold: on the one hand, to present CipherTrust, a cutting-edge solution for cloud security, and on the other hand, to highlight its deep commitment to Open Source within the Kubernetes community through its R&D activities and contributions.

Capitole du Libre

Capitole du Libre is an event that takes place every November at the ENSEEIHT computer science school in Toulouse (France). The event is a major one in the Open Source community. It takes place over a weekend and includes about 100 conferences and 25 workshops for experts and the general public.

For the 2023 and 2024 editions, Thales was a Platinum sponsor of the event. In 2024, Marius MOULIS, Global Inner Source Leader @ Thales (Corporate Software Factory Product Owner & Digital Transformation Leader), presented a conference entitled "Boost collaboration and bre

Internal Events

Thales I/O Days

The Thales I/O Days are an annual event aimed at bringing together Thales' Inner & Open Source communities, with the first edition held in 2024 at Hélios and repeated in 2025 in Paris with a strong opening to our external partners. It is sponsored by Bernhard QUENDT (CTO), Olivier FLOUS (SVP Engineering & Digital Transformation), and Philippe NETO (VP Talent & Performance).

The event consists of a day of conferences bringing together keynotes, talks, and demonstrations, as well as creative workshops allowing all community actors to exchange during a convivial moment. It is also an opportunity to thank the most involved through an awards ceremony.

Finally, each year the conference ends with the announcement of the upcoming hackathon with the theme of the challenges. In 2025, the theme was Cyber + AI, and the event was a success with over 400 participants, 110 ideas submitted, and 3 winners rewarded in the end.

Thales Rust Day

The Thales Rust Day brings together the Rust programming language community at Thales Research & Technology in Palaiseau, France. The event, organized under the aegis of the CTO Office/KTD Software, brings together software and cybersecurity engineers for technical sessions, leveraging cross-fertilization around Rust across the Group.

THALES

Building a future we can all trust