Politique Open Source : quels enjeux après la politique de licences

Camille Moulin
Benjamin Jean

hello@inno3.fr

La conformité Open Source : simple et standardisée

Vers une prise en compte généralisée de la conformité…

- Votre SI est de plus en plus dépendant de tiers. Ainsi, un projet moyen va aujourd'hui facilement faire appel à **plusieurs centaines voire milliers de composants ou dépendances tierces** soumis à leur(s) licence(s) respective(s).
- La conformité Open Source vise à s'assurer que votre *organisation respecte effectivement les obligations relatives aux contextes d'exploitation des composants Open Source qu'elle utilise, le tout conformément à la stratégie de votre organisation quant à l'opportunité de l'Open Source dans ses divers contextes métiers*.
- Cette démarche s'inscrit dans un **prise de conscience généralisée**, de nombreuses initiatives visent à harmonisier et articuler les démarches indivuelles notamment :
  - Open Chain,
  - SPDX et CyclonDX

… Sous réserve d'une mobilisation généralisée

- Il y a des outils Open Source qui permettent d'assurer le niveau de conformité attendu. Différentes étapes autour de la génération et l'alimentation d'un SBOM.
  - Détection ;
  - Génération et de gestion de SBOMS ;
  - Gestions d'analyse de licences (Shameless plug #1 Hermine)
  - Suivi des obligations

- **Les solutions sont là, tout repose maintenant sur :**
  - 1) la capacité individuelle à comprendre ces enjeux et se donner les moyens ;
  - 2) notre capacité collective à oeuvrer ensemble pour résoudre ces points.

Prendre conscience des enjeux globaux

Le SBOM, incontournable

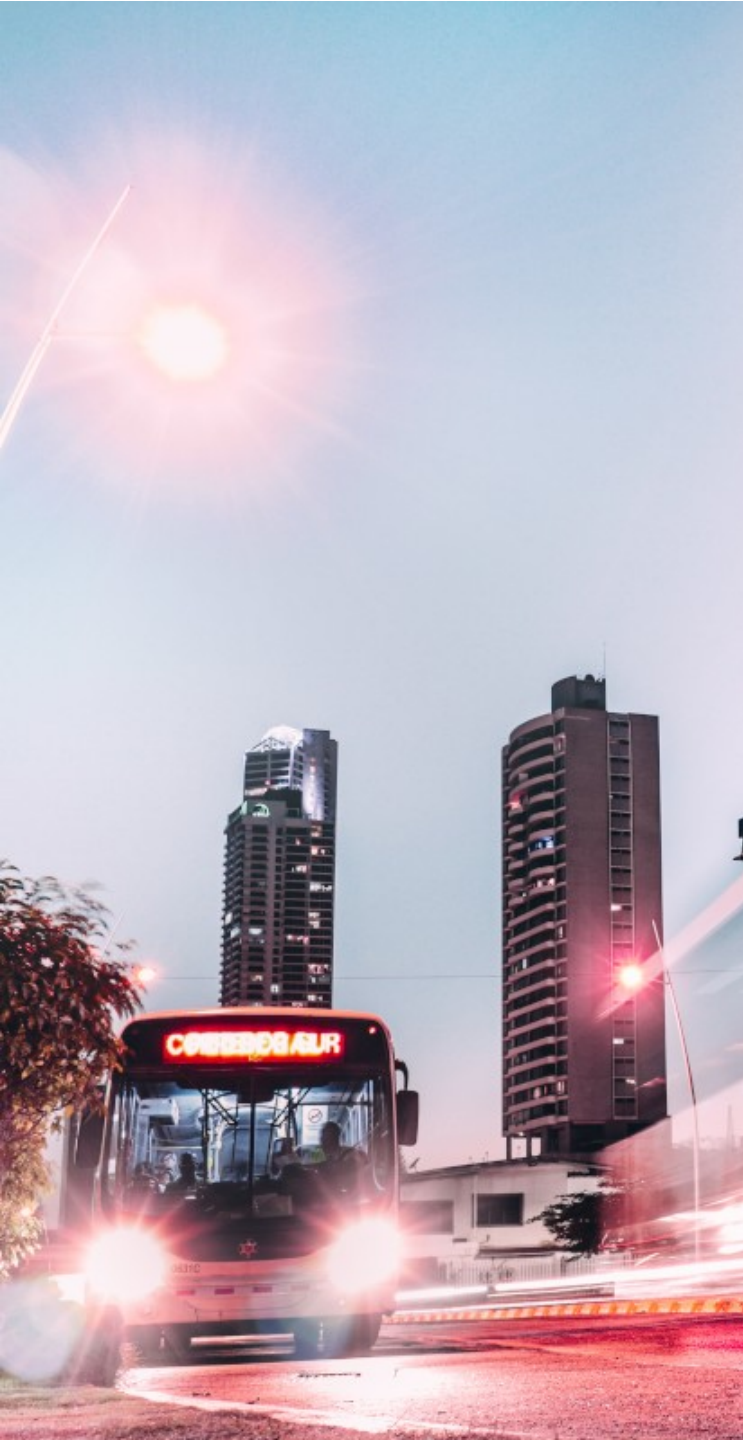
- Le numérique est devenu stratégique au point qu'il n'est plus possible aujoud'hui d'ignorer et/ou de vous désinterresser des logiciels tiers que vous utilisez.
- Cela devrait être vrai pour les logiciels commerciaux traditionnels (mais c'est normalement fait dans le cadre des procédures d'achat). Cela est d'autant plus vrai pour les logiciels Open Source qui ne passent pas par cette case.
- **Ils convient ainsi d'avoir une intelligence de son SI, de déterminer les enjeux auxquels souhaite faire face l'organisation et de concevoir une politique adéquate.**

CORE INFRASTRUCTURE INITIATIVE

Failles de sécurité et prise de conscience

- En 2014, une faille de sécurité majeure, surnommée Heartbleed, dans la bibliothèque de chiffrement OpenSSL affecte plus de 500 000 serveurs accessibles depuis internet, dont des institutions financières. La bibliothèque n'était maintenue que par un contributeur à plein temps. Elle est intégrée dans un grand nombre de solutions aussi bien libres que propriétaires.
- Cet incident déclenche une prise de conscience : tout le monde utilise les projets Open Source, très peu y contribuent.
- En réaction, un ensemble d'acteurs créent la Core Infrastructure Initiative, sous l'égide de la Linux Foundation. Elle finance un certain nombre de projets Open Source clés et deviendra l'Open Source Security Foundation en 2020.
- En novembre 2021, une faille critique est découverte dans la bibliothèque Java Log4J, après qu'elle a déjà été exploitée. Elle illustre l'insuffisance des mesures prises suite à Heartbleed.
- Évolution juridique :
  - Executive Order on Improving the Nation's Cybersecurity (12 mai 2021)
  - Cyber Resilience Act, en Europe (en cours d'élaboration) : de bonnes intention, mais dans son état actuel, une menace majeure pour l'Open Source.

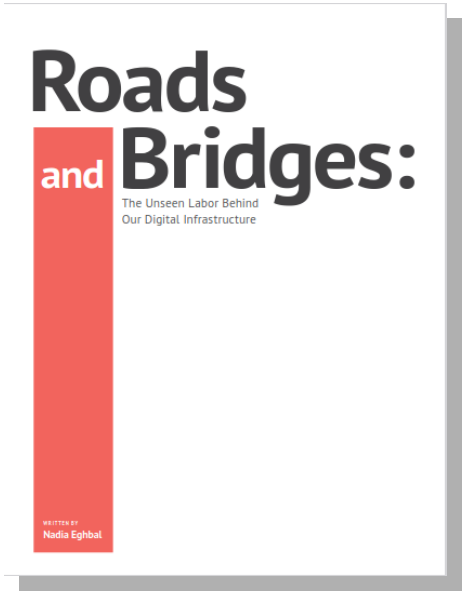
> But we didn't get so lucky the next time. When the #Log4j bug was discovered last November, it was already too late. **We'd hit snooze on Heartbleed's wakeup call and holy shit had we ever overslept**
>
> Cory Doctorow @pluralistic@mamot.fr



Pérennité, plus large que la sécurité : LeftPad

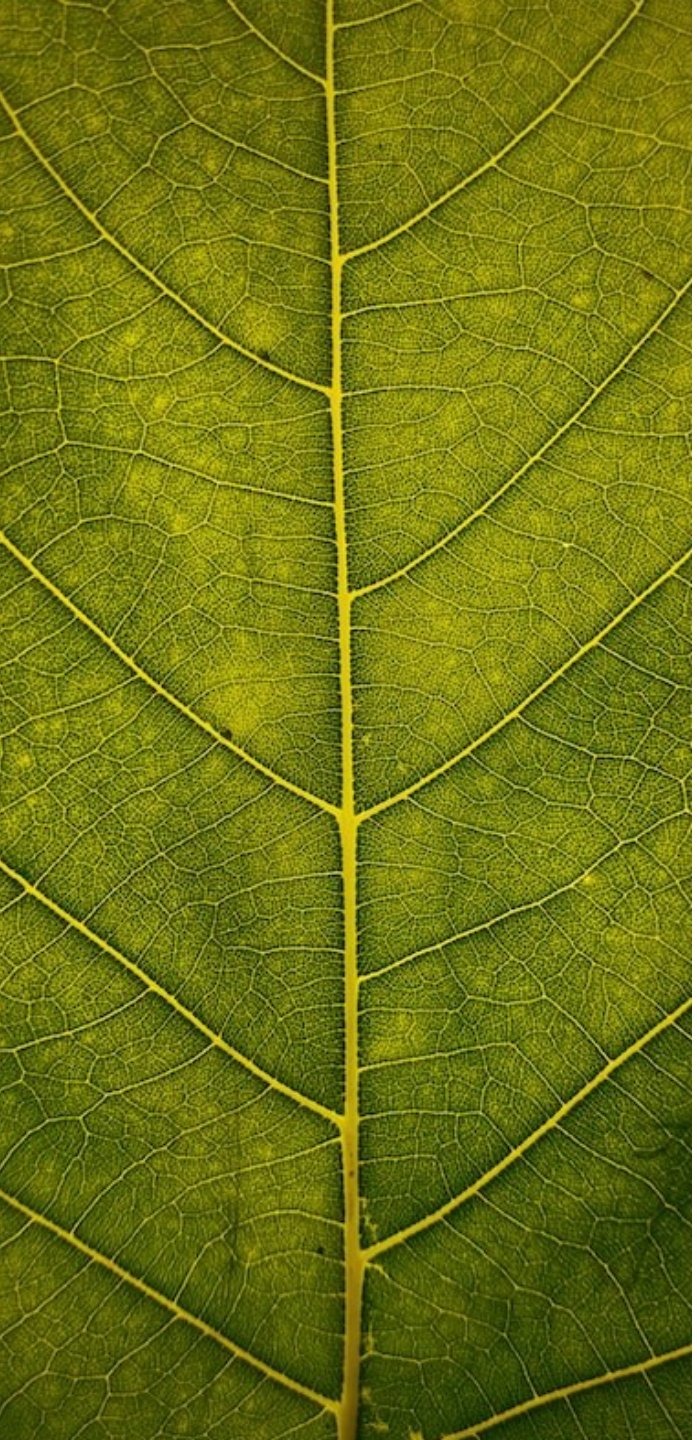
- En mars 2016, Azer Koçulu, développeur de plusieurs projets Open Source disponibles dans NPM reçoit des menaces juridiques d'une société pour leur céder un nom de module. Les mainteneurs de NPM lui ayant retiré le module de force, il dépublie l'ensemble de ses modules, dont LeftPad, un module trivial dont dépendent récursivement un grand nombre de projets (dont Babel, etc.). Ces projets se retrouvent alors incapables de fonctionner.
- Dans la prolongation d'Heartbleed, cet incident a mis en évidence l'étendue du système de dépendances, voire de micro-dépendances, sur lesquelles reposent de plus en plus de projets sans en avoir toujours conscience (contraitement à un composant majeur comme OpenSSL).
- La pérennité de ces (micro-)projets est souvent fragile, comme le montre les études sur la "résistance à l'écrasement" (bus factor).
- Les motivations sont multiples :

> "I am no longer going to support Fortune 500s (and other smaller sized companies) with my free work [...].Take this as an opportunity to send me a six figure yearly contract or fork the project and have someone else work on it."
> **Mainteneur de Colors.js et Faker.js**



Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure, par Nadia Eghbal pour la Ford Foundation

"The Maintainers: How Bureaucrats, Standards Engineers, and Introverts Create Technologies that Kind of Work Most of the Time.", créé en réaction au livre de Walter Isaacson "The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution".
https://themaintainers.org/



Repenser ses relations dans une perspective d'écosystème

> **Il faut supprimer les intermédiaires inutiles**
>
> Henri Verdier, NGI Forum 2023

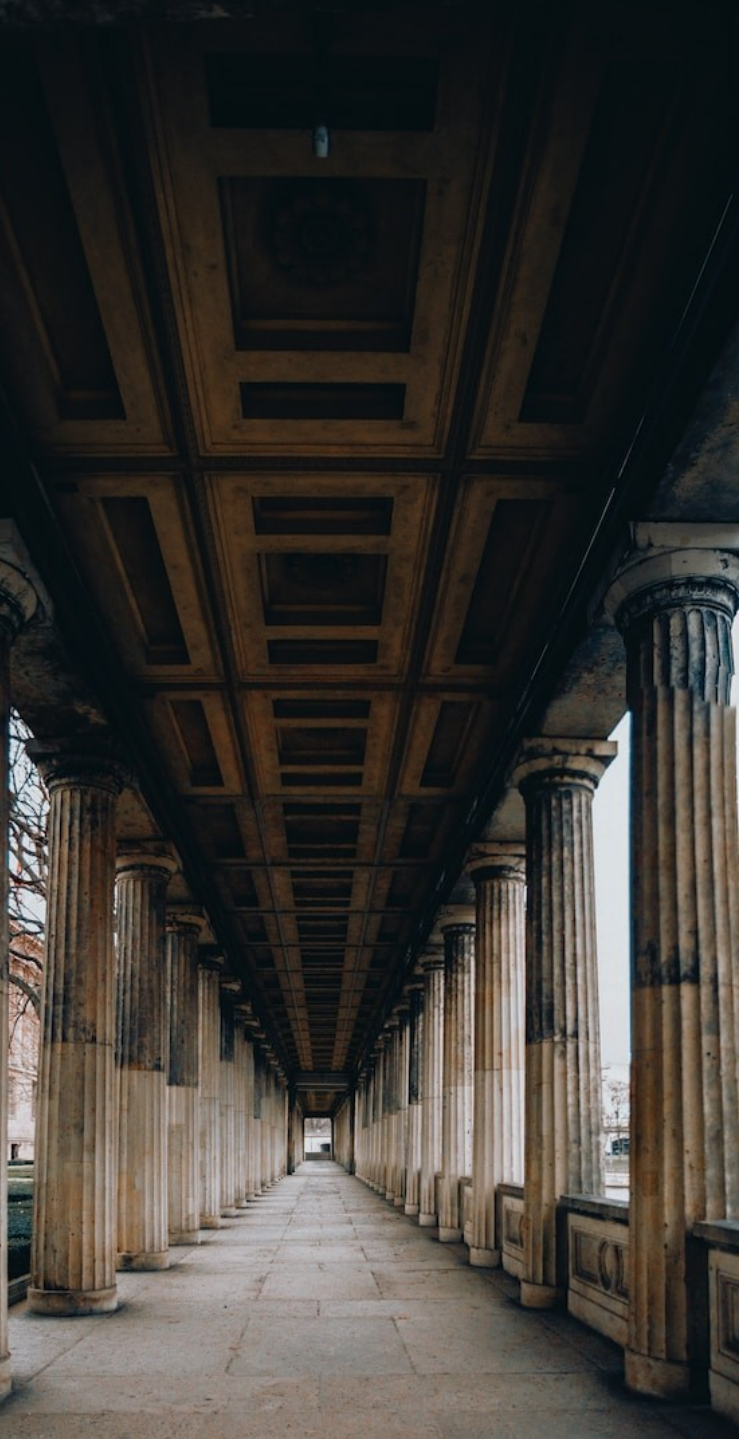
« Henri Verdier a tort ! »

Un intermédiaire inutile, en off, NGI Forum 2023

> **I am not your supplier**
>
> Thomas Depierre, mainteneur de projet Open Source

- **« Ne considérez pas l'upstream comme des fournisseurs mais comme des partenaires. »**

Conclusions et perspectives



- **Intégrer pleinement l’Open Source dans la stratégie d’une organisation (privée ou publique) impose :**
  - De prendre en compte et d’investir dans la **maintenance**
  - De faire **évoluer** les programmes (ex Bug bounties)
  - De changer les,relations entre acteurs pour construire des **relations partenariales** avec les communautés éditrices de projets Open Source.
  - D’utiliser et **contribuer aux solutions qui participent à la conformité** Open Source

- **Appliquer les leçons de l’Open Source aux APIs :**
  - Nécessiter de standardiser les contrats (ToS) pour renforcer la prédicitibilité juridique
  - Associer ces contrats standardisés à des identifiants techniques pour permettre une automatisation rendue nécessaire par le nombre croissants de services utilsés ;
  - Shameless plug #2 : API ToS / FACT (cf conférence précédente).

FACT WIZARD

Crédits des illustrations

- **Slide 1, 3 : Photo by Christine Roy on Unsplash https://unsplash.com/photos/ir5MHI6rPg0**
- **Slide 2 : Photo by Andre Benz on Unsplash https://unsplash.com/photos/JCjGpD84N0I**
- **Slide 5 : Photo by Pawel Czerwinski on Unsplash https://unsplash.com/photos/_nqApgG-QrY**
- **Slide 6 : Photo by Jac Alexandru on Unsplash https://unsplash.com/photos/K1KkVk_u9gg**
- **Slide 9 : Photo by JOSHUA COLEMAN on Unsplash https://unsplash.com/photos/_yVRLC75Ma8**
- **Slide 10, 14 : Photo by Kai Gradert on Unsplash https://unsplash.com/photos/07KxLPfH0l4**
- **Slide 12 : Photo by Luis Quintero on Unsplash https://unsplash.com/photos/xk1pV_Nx2bc**
- **Slide 13 : Photo by Dex Ezekiel on Unsplash https://unsplash.com/photos/nzuBlWKpUIE**
- **Slide 15 : Photo by Sean Pollock on Unsplash https://unsplash.com/photos/PhYq704ffdA**
- **Slide 17 :**
  - Jiahui Huang https://www.flickr.com/photos/huangjiahui/ sous CC-BY-SA-2.0
  - Bart Lumber https://www.flickr.com/photos/bartoszjanusz/ sous CC0-1.0
  - Nicolas Raymond http://freestock.ca/ireland_g53-poulnabrone_dolmen__hdr_p1689.html sous CC-BY-2.0
- **Slide 18 : Photo by Kvistholt Photography on Unsplash https://unsplash.com/photos/oZPwn40zCK4**
- **Slide 19 : Photo by Girl with red hat on Unsplash : https://unsplash.com/photos/6SDyqhHb4rg**
- **Slide 20 : Photo by Ivan Bandura on Unsplash https://unsplash.com/photos/vHsh8PtJ0jk**

https://unsplash.com/license