



zenika

State of Devops 2022 & SCS

Fabien Leite - Meetup OWASP Paris - sept. 2023

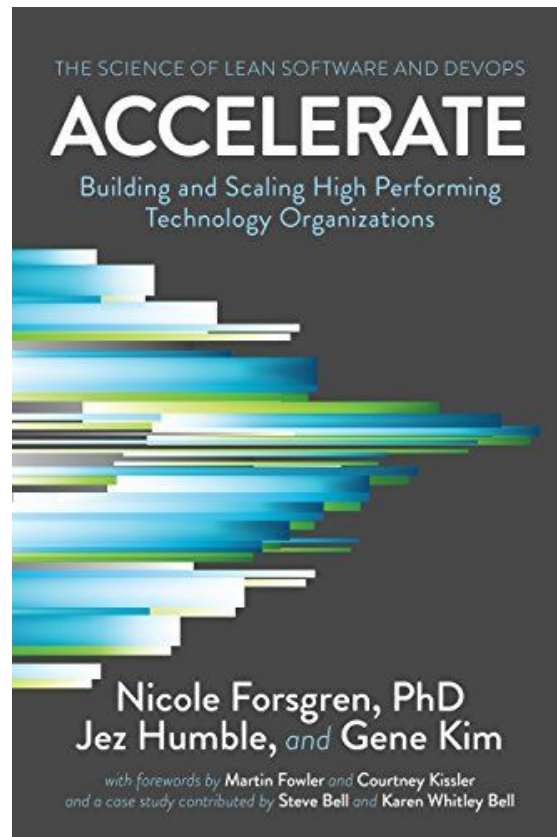




DORA, State of Devops, Accelerate



Devops, Accelerate, DORA

- DORA : DevOps Research & Assessment (racheté par Google)
- Accelerate, State of Devops :
 - Étude annuelle depuis 2014
 - Méthodes scientifiques
 - Trouver ce qui rend un delivery performant
- Accelerate (livre) : 2018



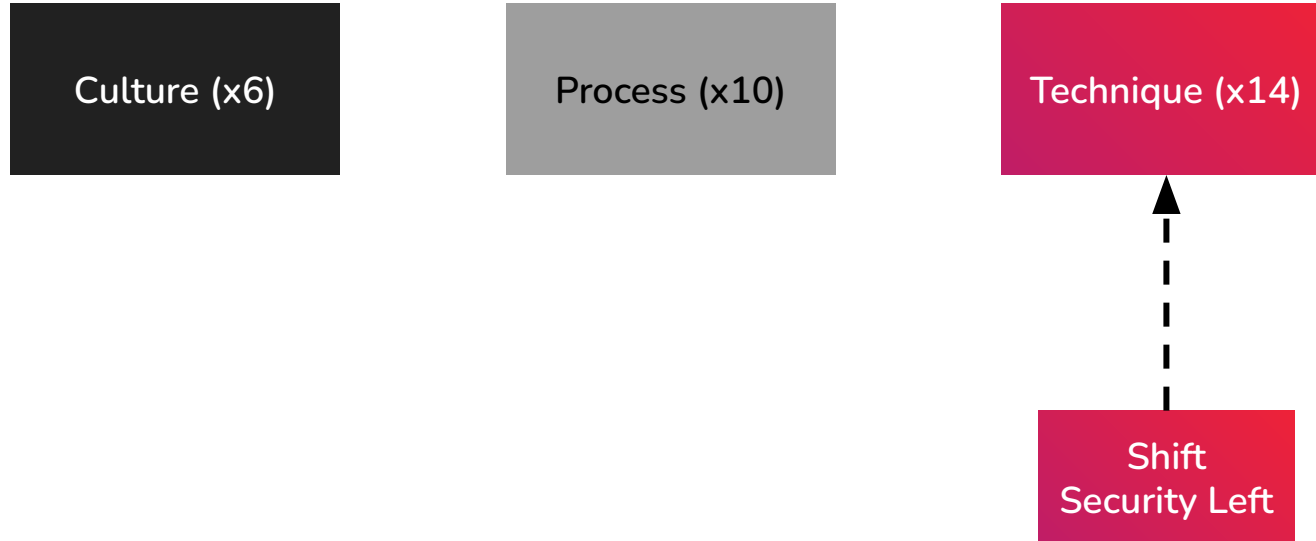


4 indicateurs

| | | | |
|-------------------------------------|---|-------------------------------------|-----------------------------------|
| Performance de livraison logicielle |  2 Indicateurs de vitesse | Lead Time | Deployment Frequency |
| |  2 Indicateurs de stabilité | MMTR Mean Time To Restore | CFR Change Failure Rate |



Une trentaine de capabilities





Pourquoi je vous parle de ça ?



Le state of Devops 2022

Securing the software supply chain

In 2021, we found that securing the software supply chain is essential to reaching many important outcomes.

This year we dug deeper on software supply chain security, making it a primary theme of our survey and report. We leveraged the [Supply Chain Levels for Secure Artifacts \(SLSA\)](#) framework to explore technical practices that support the development of software supply chain security. We also used the National Institute for Standards and Technology's [Secure Software Development Framework \(NIST SSDF\)](#) to explore attitudes, processes, and non-technical practices related to securing the software supply chain.

Premier segment de l'exec sum (p4)

Focus principal de l'étude (p.42 - 12/77p)

04

Why supply chain security matters

SCS : Deux framework - complémentaires

NIST

NIST → SSDF

Le NIST

Considérations générales, définir une cible



OpenSSF → SLSA

Google, Datadog, Intel, ...

Considérations pratiques / mesure des efforts

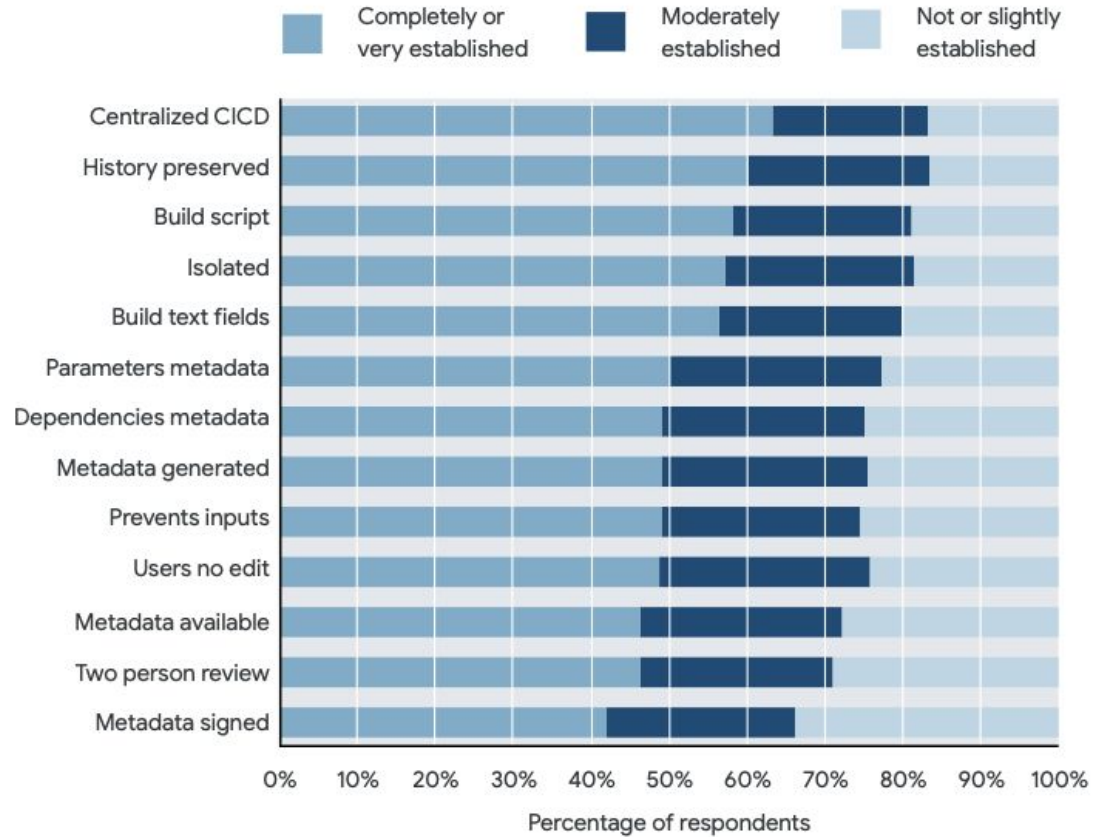


Figure 1. Establishment of SLSA practices

Survey responses about the establishment of SLSA practices. A majority of respondents indicated some establishment of all of these practices, but relatively few said they were “completely” established yet.

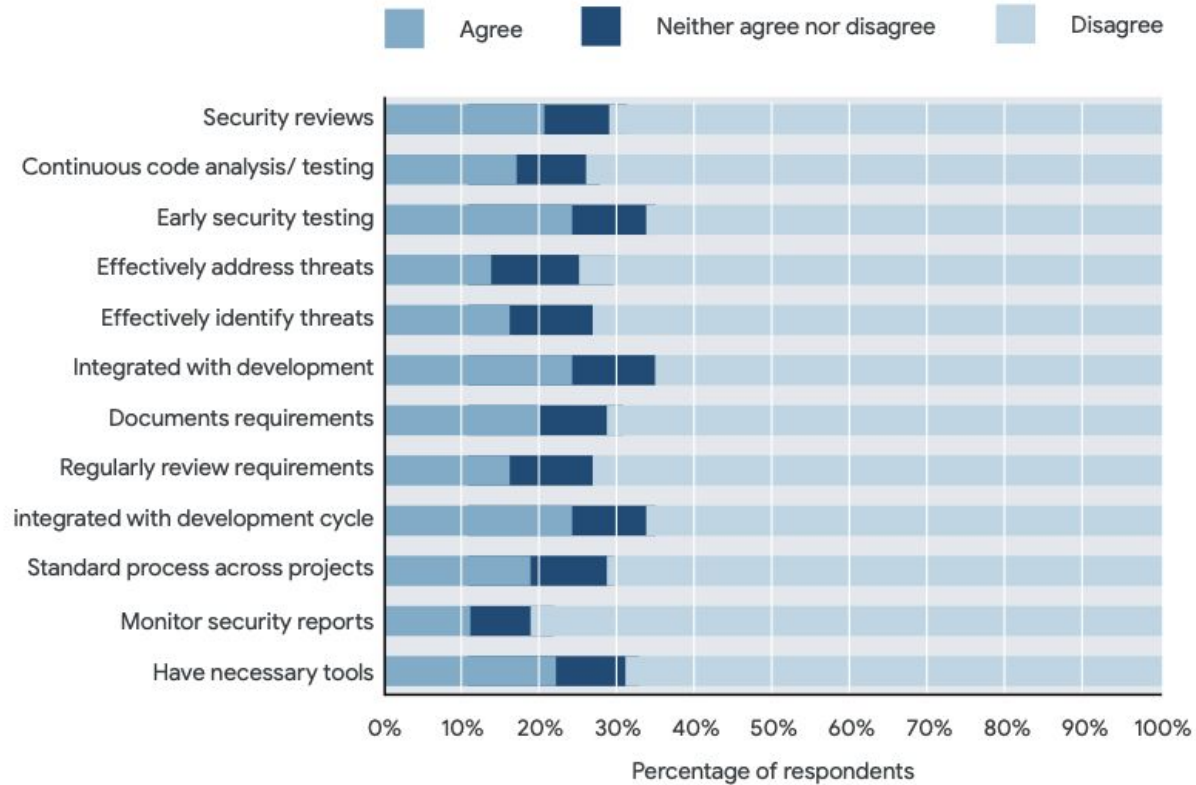


Figure 2. Establishment of SSDL practices

Survey responses about the establishment of SSDL practices. Similar to SLSA, a majority of respondents agreed that their organization followed all of these practices.



La sécurité a un problème de posture

```
« [...] a set of research interviews with professional software engineers found that their touchpoints with security teams were limited to either the start or end of a project, and the teams could be difficult to engage with. In the words of one participant, "We have an application security team, but I have never had my code reviewed by them... I am like most engineers, I avoid them usually." »
```

L'impact le plus important sur la SCS

CAPACITÉS POUR PILOTER L'AMÉLIORATION AVEC

ACCELERATE

1-8: Capacités liées à la Livraison Continue
9-10: Capacités liées à l'Architecture
11-14: Capacités liées au Produit & Processus
15-19: Capacités liées au Lean Management
20-24: Capacités liées à la Culture

- 1 CONTRÔLE DE VERSION
- 2 DÉPLOIEMENT AUTOMATISÉ
- 3 INTÉGRATION CONTINUE
- 4 DÉVELOPPEMENT À BRANCHE UNIQUE
- 5 AUTOMATISATION DES TESTS
- 6 GESTION DES DONNÉES DE TESTS
- 7 LA SÉCURITÉ AU PLUS TÔT
- 8 LIVRAISON CONTINUE

- 9 ARCHITECTURE FAIBLEMENT COUPLÉE
- 10 ARCHITECTE AU SERVICE DES ÉQUIPES AUTONOMISÉES
- 11 FEEDBACKS DES CLIENTS
- 12 FLUX DE VALEUR VISIBLE
- 13 TRAVAIL EN PETITS LOTS
- 14 EXPÉRIMENTATION EN ÉQUIPE
- 15 VALIDATION SIMPLIFIÉE DES CHANGEMENTS
- 16 SURVEILLANCE DU SYSTÈME

- 17 SUIVI DE L'ÉTAT / SANTÉ DU SYSTÈME
- 18 LIMITES D'ENOURS
- 19 VISUALISER LE TRAVAIL
- 20 CULTURE GÉNÉRATIVE
- 21 CULTURE DE L'APPRENTISSAGE
- 22 COLLABORATION DANS L'ÉQUIPE
- 23 SENS DANS LE TRAVAIL
- 24 LEADERSHIP TRANSFORMATIONNEL

a.k.a Westrum Culture



Résumé des datas

« This data leads us to believe organizational culture and modern development processes (such as continuous integration) are the biggest drivers of an organization's application development security, and the best place to start for organizations looking to increase their security posture.



CI/CD, sécurité - corrélation



CI/CD, sécurité - efficacité, burnout

« Along with a reduction in perceived security risks, respondents also reported less burnout among team members and an increased willingness to recommend their organization as a great place to work » *

Tools and processes that help them incorporate secure practices into their existing development workflow, as opposed to unplanned work or “fire drills” when a threat is discovered, provide a mechanism for reducing security risks **and** increasing developer joy.

The image features a dark blue background filled with numerous small, white, star-like specks of varying sizes, creating a starry or cosmic effect. A prominent, diagonal stripe of a lighter, medium blue color runs from the upper left towards the lower right, crossing the center of the frame. The word "MERCI" is written in a clean, white, sans-serif font, centered horizontally and vertically within the lighter blue stripe.

MERCI