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
<table>
<thead>
<tr>
<th>Performance de livraison logicielle</th>
<th>2 Indicateurs de vitesse</th>
<th>Lead Time</th>
<th>Deployment Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>MMTR</strong></td>
<td><strong>CFR</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mean Time To Restore</td>
<td>Change Failure Rate</td>
</tr>
</tbody>
</table>
Une trentaine de capabilities

Culture (x6)  
Process (x10)  
Technique (x14)

Shift Security Left
Pourquoi je vous parle de ça ?
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.
SCS : Deux framework - complémentaires

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 SSDF practices

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

a.k.a Westrum Culture
« 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.
Cl/CD, sécurité - corrélation

![Diagram showing correlation between CI/CD and security practices](chart.png)

- Above average CI:
  - Below average security practices: 0.33%
  - Above average security practices: 0.45%
- Below average CI:
  - Below average security practices: 0.46%
  - Above average security practices: 0.66%
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.

* voir le SPACE framework de Nicole Forsgren
MERCI