Soutenance de fin d'étude

Comprendre pour mieux placer efficacement la sécurité dans une approche DevOps

Julien Briault - EISI 22.3 CS - IPSSI

Avant-propos

Les sources (code) sont disponibles sur Github.

Cette présentation est sous licence **CC BY-SA FR 2.0** (tout comme le mémoire).

Ainsi chacun est libre de le *diffuser*, de le *modifier*, sans oublier de **citer** l'auteur !

~$ whoami

Julien BRIAULT

- System Engineer chez **Rudder/Normation**
- Responsable Informatique aux Restos du Coeur (~ 1 an)
- Auteur principal sur blog.jbriault.fr
- Développeur C/Golang/Python

#mao-dj #dev #net #automation #open-source #free-software

Rudder, qu'est-ce que c'est ?

- Entreprise éditrice de logiciel **Open Source** du même nom
  - Basée à Paris (3ème proche de République)
  - A une dizaine d'années
  - 14 collaborateurs (dont une majorité de devs)
- Créatrice du **DevOps Rex** (conférence autour du DevOps)
- Le logiciel :
  - Seul acteur *français* et *européen* dans la gestion de configuration et sa mise en conformité des systèmes.

Sommaire

Introduction

Pourquoi avoir fait ce choix de sujet ?

- Sujet qui me tient à coeur
  - Contributeur à des projets comme **naxsi** ou encore **crowdsec**. Mais également Rudder...
- Rudder est un outil qui se veut ***DevSecOps****

* Terme marketing pour désigner le fait que l'outil est à destination à la fois des *ops*, des *devs* (dans une certaine mesure) et des *équipes de sécu*.

Introduction

Pourquoi avoir fait ce choix de sujet ?

- Beaucoup d'informations autour du DevOps mais peu finalement sur la sécurité dans celui-ci
- Le sujet n'est pas toujours bien compris
  - Détailler pour mieux comprendre pour installer les bonnes pratiques de sécurité
- Une réponse souvent logique mais pas évidente à comprendre : **DevSecOps**

Introduction

Pourquoi avoir fait ce choix de sujet ?

Des programmes de recherche autour du DevOps n'incluant pas la sécurité et mettant l'accent sur les performances.

Exemple : **DORA** (Devop Research and Assessment) de **Google**.

Conduite et démarche de recherche

- L'acquisition des connaissances se traduit par l'***intuition*** et l'***expérience personnelle***.
- J'entends par :
  - L'**intuition** : connaissance immédiate du sujet abordé
  - L'**expérience personnelle** : l'essai et l'errreur
- Cette démarche ne resulte en rien d'un *raisonnement logique* (au sens scientifique du terme).

Les origines

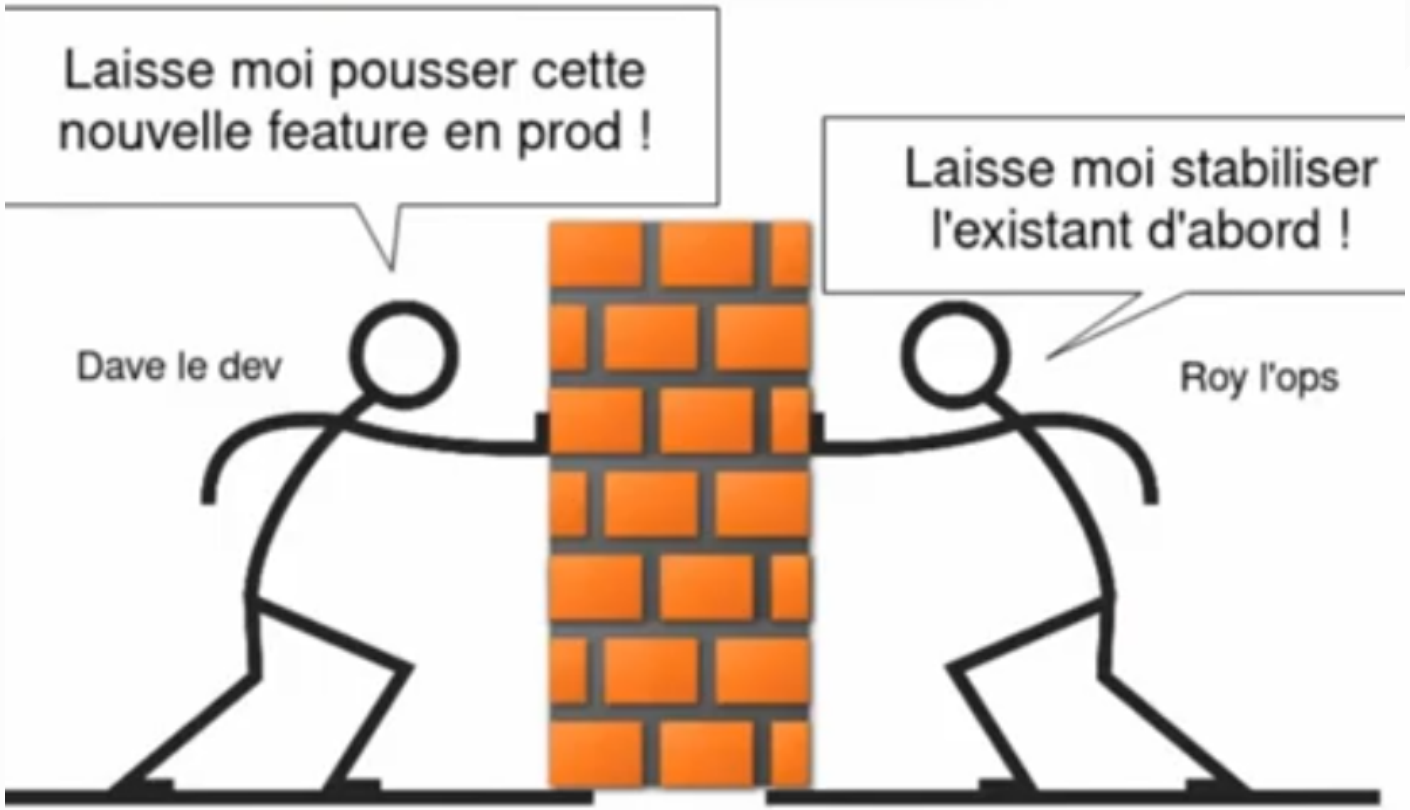


*Image tirée du talk de Denis GERMAIN nommé **SRE**.

Les origines

La sécurité, encore une fois oublié... Vraiment ?

- Analyse des concepts fondamentaux
  - **Kaizen** (amélioration continue)
  - **Scrum** (méthode : comment collaborer ?)
  - **Lean Startup** (constuire, mesurer, apprendre)

La sécurité, oui mais comment ?

- Reprendre les différentes étapes du DevOps (*plan*, *build*, *release*, *deploy*, *operate*, *monitor*).
  - Comprendre
  - Déterminer les actions pour la sécurité déjà apportés
  - Améliorer

La sécurité, oui mais comment ?

- Ce n'est pas que de la technique !
  - D'après le **DEDSORD**, il est souvent oublié le point de vu *business* (des histoires de ROI par exemple).

Le futur

Le retour aux sources

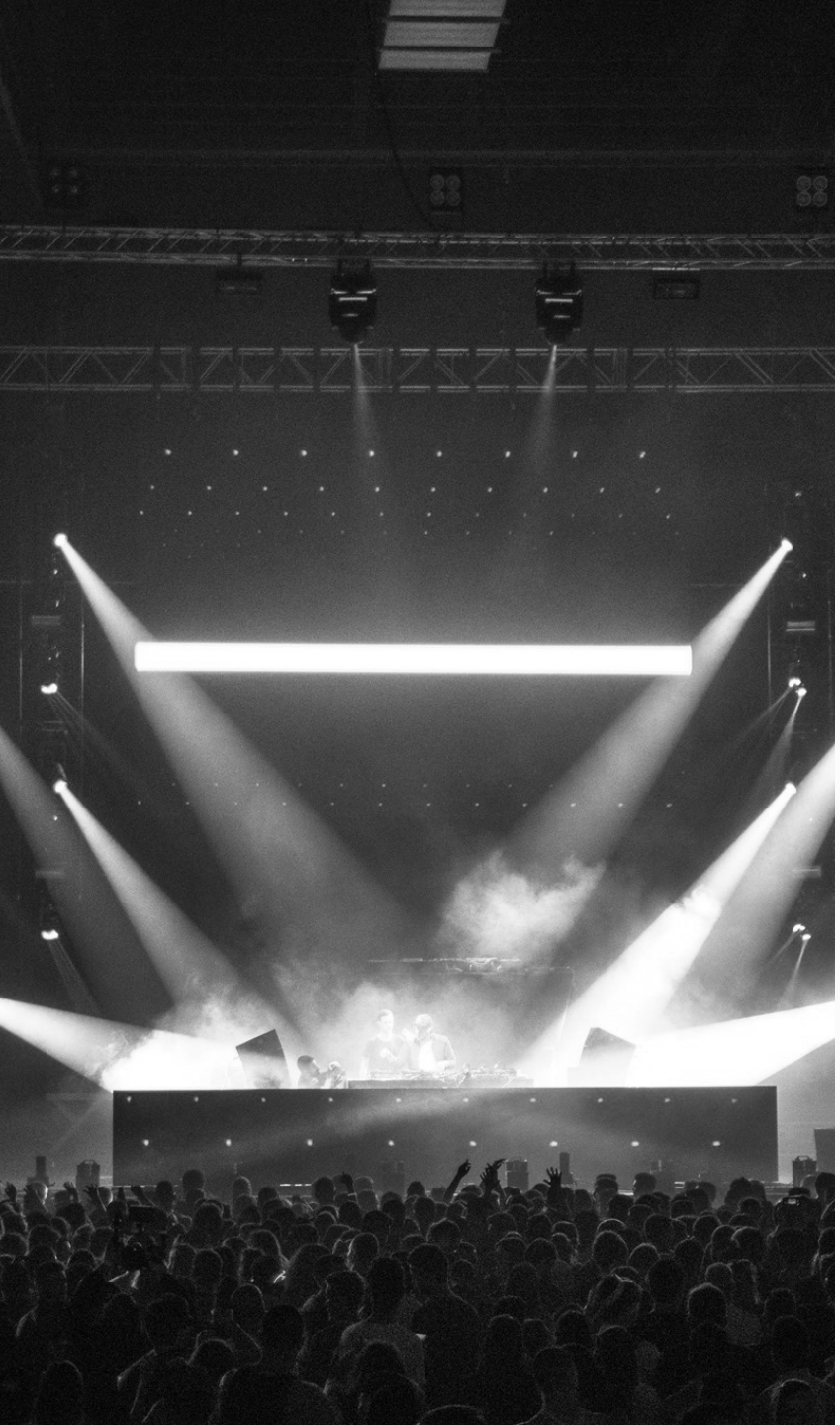
- Premier CDI *signé*
- Poste : **Network Engineer SRE**

#network #sre #core-infra #automation

Le futur

Créer une startup autour du projet **Ichigo**.

- Projet à orientation **NetDevOps**
  - Automatisation
  - Déploiement
  - Audit
  - Sauvegarde



Merci pour votre écoute !

Place aux questions !