

Soutenance de fin d'étude

Comprendre pour mieux placer efficacement la sécurité dans une approche DevOps

Julien Briault

Promotion 2021/2022 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 !

“L’Homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique” - **Albert Einstein**

~\$ **whoami**

Julien BRIAULT

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

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





Rudder, qu'ésaquo ?

- 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
- Conduite et démarche de recherche
- Les origines/ le contexte
- La sécurité dans le DevOps, oui mais comment ?
- Des solutions pour garantir cette sécurité ?
- Conclusion
- Le futur / les projets

Introduction

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 y insérer les bonnes pratiques de sécurité
- Une réponse souvent logique mais pas évidente à comprendre ni à mettre en place : **DevSecOps**

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**.

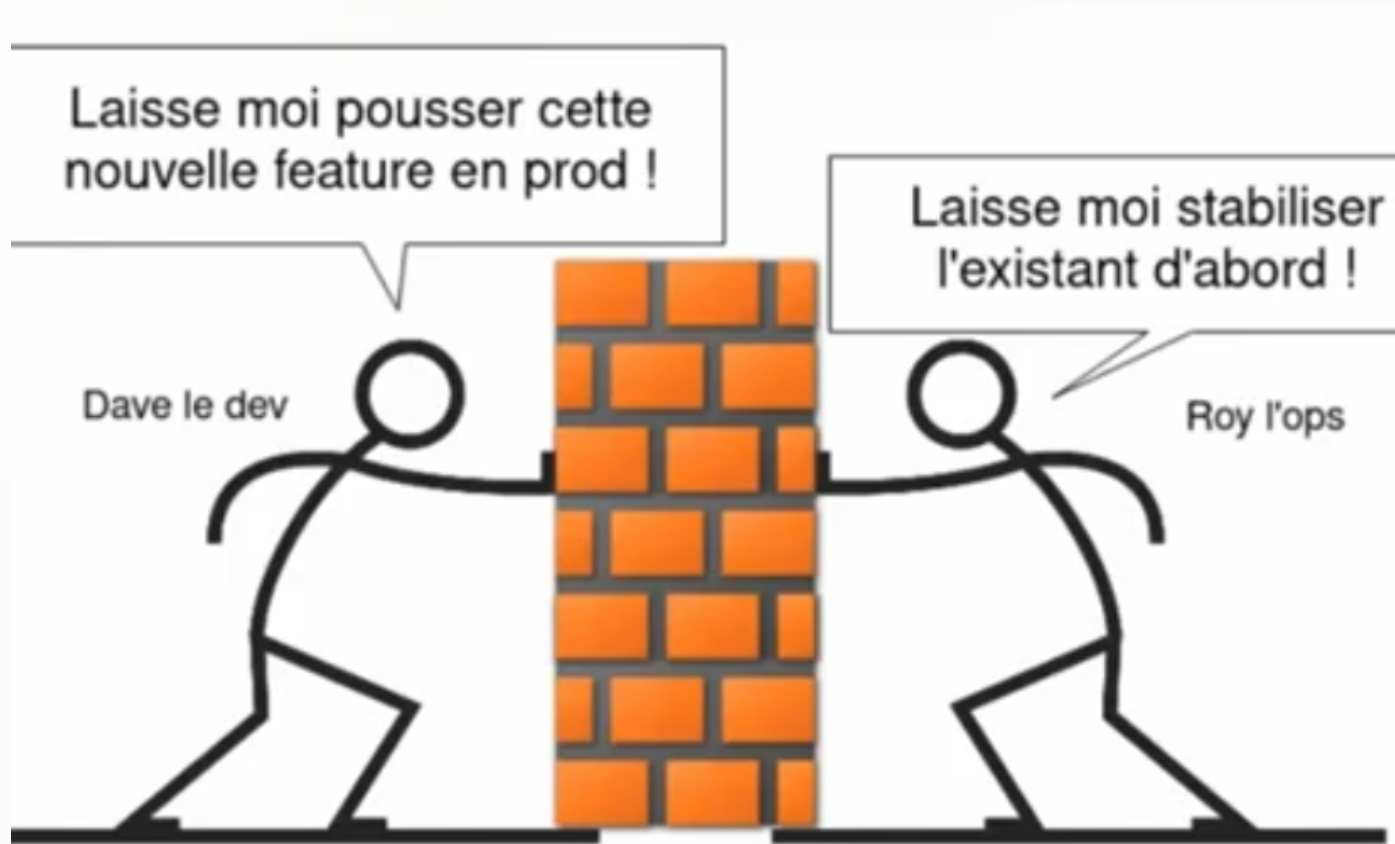
Conduite et démarche de recherche

Conduite et démarche de recherche

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

Les origines/le contexte

Les origines



* Image tirée du talk de Denis GERMAIN nommé [SRE](#).

Un contexte particulier...

- Besoin clients qui changent continuellement
- Time-to-market réduit (concurrents, réglementations)

Emergence des pratiques agiles et de la culture DevOps

- Limites de l'approche de sécurisation traditionnelle
 - Séparation des rôles
 - Droit de veto de l'équipe sécurité
 - Sécurisation sur des besoins figés, spécifications formalisées
 - Stopper pour auditer

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

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

Rentrer dans le vif du sujet

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

- Apporter des solutions méthodologiques et techniques à chaque pan du DevOps.
- Mais, ce n'est pas que de la technique...
 - D'après le **DEDSORD**, il est souvent oublié, le point de vue *business* (des histoires de ROI par exemple).
 - Le **BIA** (Business Impact Analysis) plus qu'important mais trop souvent oublié

Finalité

Des solutions

Le choix des solutions c'est principalement basé sur une analyse de recueils de bonnes pratiques et d'expériences personnelles/professionnelles.

La collaboration

- L'équipe sécurité travaille avec les développeurs (l'équipe "DevOps")
 - Dès le début des projets ("*shift security to the left*")
 - Rédiger des user stories orientées sécurité (> scénarios d'abus)
 - Partage d'expérience (communication ++)
- Aller plus loin :
 - Nomination de **security champions**
 - + Scalabilité
 - + Diffusion naturelle des bonnes pratiques

La formation/sensibilisation

- Formation au développement sécurisé
 - OWASP Top 10
 - CWE Top 25
 - Certifications : *GWEB, CSSLP, CASE*
- Sensibilisation
 - Par l'équipe sécurité
 - Démonstrations de piratage (DVWA, Metasploitable)
 - E-Learning
 - OWASP Top 10 (bis)

L'automatisation!

- Le pipeline de CI/CD doit inclure les tests de sécurité
 - **Antifragilité** : amélioration par le stress!
- Freins pour l'adoption
 - Faux positifs
 - Findins non activables
 - Lenter des outils SAST/DAST
 - CVE sans solution, ça peut stopper complètement un déploiement!

L'outillage

- **Lint**

- Vérification des bonnes pratiques de développement
- Contrôles basiques de sécurité
 - Appels systèmes (injection de commandes)
 - Expressions régulières (ReDoS, safe-regex)

- **SCA - Software Composition Analysis**

- Identification des dépendances open-source vulnérables
- Possibilité de configurer des politiques (CVSS)

- **SAST** Static Application Security Testing / White box
 - Recherche de vulnérabilités dans le code source
- **DAST** Dynamic Application Security Testing / Black box
 - Analyse de vulnérabilités sur l'application qui tourne
 - Appelé aussi "stress test"

Recueil des bonnes pratiques

DevSecOps une évidence, expliqué, détaillé avec un ensemble de bonnes pratiques, c'est mieux!

Naissance du **DoD Enterprise DevSecOps Reference Design**
([DEDSORD](#))

- Donne une vision claire des bonnes pratiques DevSecOps à avoir
- Essaie d'apporter toutes les réponses sur l'implémentation de ces bonnes pratiques
 - Fournissant des *méthodes* et non de la technique.

Le futur / les projets

Le futur / les projets

Le retour aux sources

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

**#network #sre #core-infra
#automation**



Le futur / les projets

Créer une startup autour du projet [Ichigo](#).

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





Merci pour votre écoute !

Place aux questions !

