L//P
DIGITAL PROGRESS

Embarking on DevSecOps

Customer commitment and interactive approach

—

Fribourg, 28.09.23

Hello!

Olivier Wenger

DevOps Engineer

https://github.com/owngr

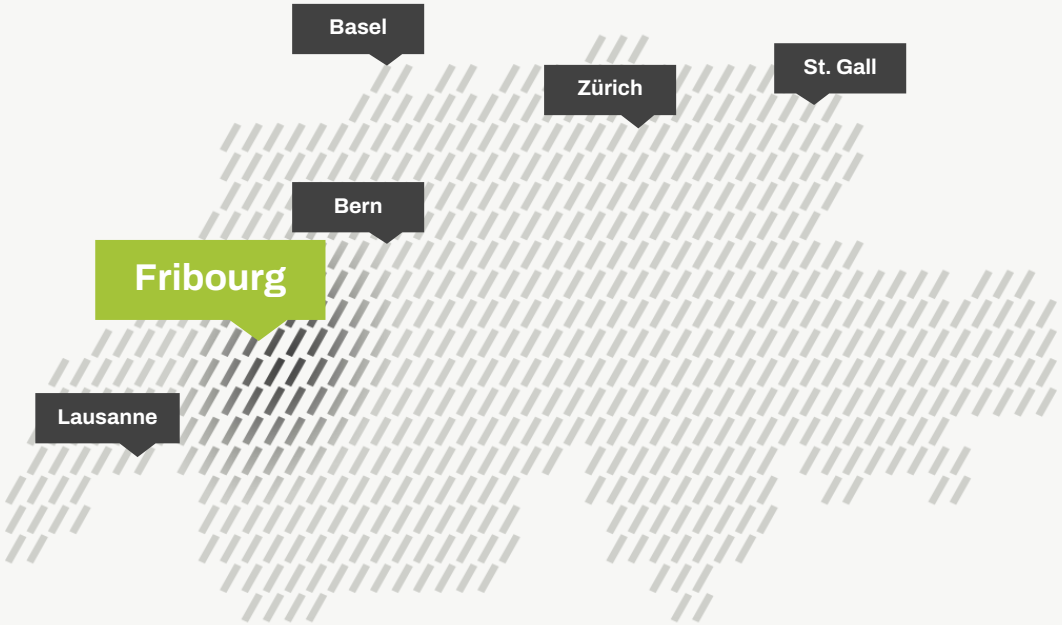
https://www.linkedin.com/in/olivier-wenger/

Agenda

- About Liip
- DevOps vs DevSecOps
- Incident management
- Security in a maintenance contract
- Communication Channels and Sensible Data
- Roles and accounts management
- Dev and Test data

About us

Let’s introduce ourselves



Liip

220 employees

6 locations

1 purpose

Liip Purpose

Create long-lasting social, environmental and economic value, by striving for digital, human progress.

Areas of expertise

User Experience

- Service Design
- UX Design
- Design Thinking
- Content

Development

- Custom Development
- E-commerce
- CMS
- Mobile Apps
- Moodle
- Open Data

SEO & Analytics

- Analytics
- SEO

DevOps vs DevSecOps

Key differences

DevOps vs DevSecOps

DevOps

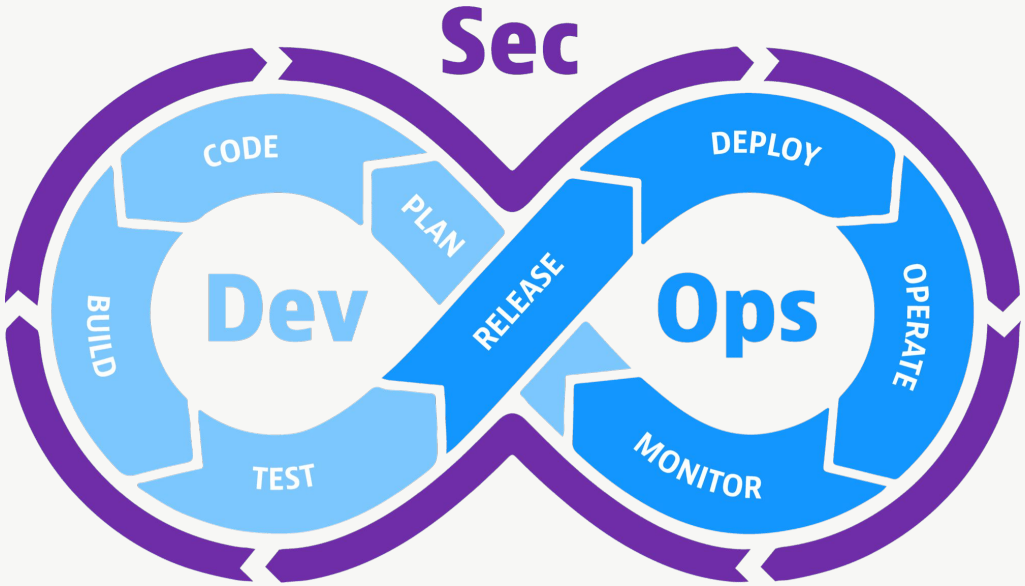
- Priority: increase deployments frequency
- Continuous integration, continuous delivery, continuous deployment

DevSecOps

- Priority: increase the app security
- Continuous integration, continuous delivery, continuous deployment, **automated security testing, test modeling, incident management and common weakness enumeration**

DevSecOps

- Security must be present at **every** stage
- DevSecOps cannot happen without having implemented DevOps
- Security testing doesn't stop when development is at halt



Incident management

How to prepare yourself

Incident management

Security vulnerability not visible to the customer

- Be informed when the vulnerabilities appear (mail, renovate, dependabot)
- Fix the problem, if specified in the contract, deploy the patch without coordinating with the customer
- Inform the customer

Incident management

Incidents impacting customers' user experience - roles

Form a core team rapidly:

- **Coordinator:** Form a team with the persons available and coordinate them
- **Secretary:** Write everything that happens and at which time, responsible for the logbook
- **Communication:** Inform the customers, answer their questions, forward useful information to the coordinator
- **Dev/Ops/Sys/Sec:** Solve the incident

Incident management

Incidents impacting customers' user experience - steps by step

1. The person who notices the problem notifies their team
2. A coordinator is chosen, and this one distributes the roles
3. The communications manager notifies customers using a template created before the incident
4. The developers start to solve the problem, the secretary takes note of what is being done.
5. Continuous communication is kept with customers
6. Once the incident is solved, reflect with the logbook of what went well, what could have been better and what are your next actions to do it better next time

Security in maintenance contract

Non-optional security

Security in maintenance contract

- Non-optional
- Include backup
- Include security updates
- Allow enough time for the unexpected
- What cannot be included must be communicated to the customer (major updates)

SAAS-PACKAGE

— 1 live and 1 staging server;

— Moodle security updates and other periodical updates included;

— 24/7 monitoring;

— daily live and staging environment backups;

— retention of backups for at least one month (weekly snapshots).

Security in additional plugins

- Installation by end-user disabled
- Any new plugin is reviewed
  - Is it still maintained?
  - Does it respect licenses?
  - Does it respect GDPR?
  - Does it pass automated analysis tests?
  - Does it properly require authentication and capabilities?
  - Any CWE found in code?
- Results are transmitted to the customer and explained
- Plugins per instance are documented and updated

Communications channels

Avoid passwords leaks

Communications channels

Avoid passwords leaks

- Which channel is safe?
- Restrict password access when sharing
- Randomly generate password
- Change insecure passwords and anything that leaks
- Makes sure that everyone/all roles do that

Roles and account management

Didn't he leave the company 6 years ago?

Roles and account management

Good practices

- Avoid generic accounts as much as possible, as they are never suspended
- Use SSO with In/Off boarding when possible
- Periodically ask your customers to list their users that should have access to your services, notify them when someone leaves your team
- Use a default deny approach and give more rights if necessary
- Set reminders to remove roles, document administrators
- It’s 2023, but I guess we still have to say it, use MFA

Dev and Test data

How to ensure confidentiality

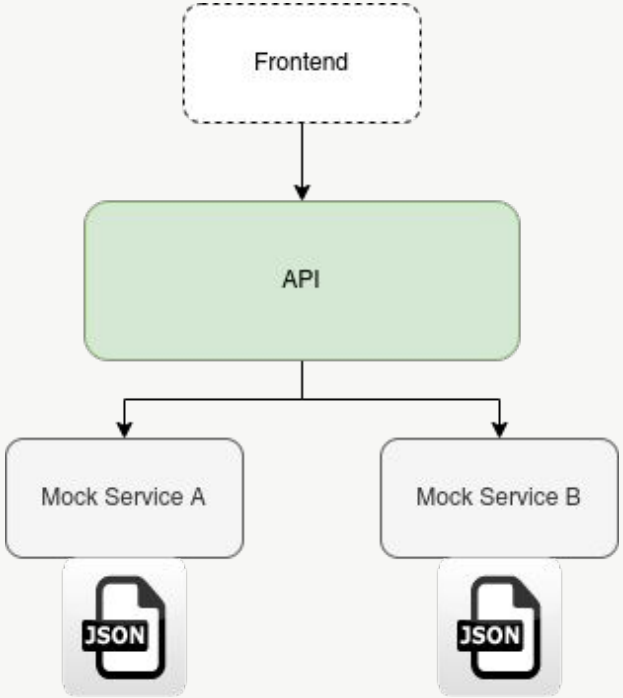
Dev and test data

Considerations at the early phase

- Depending on the size and prerequisites of an application, at least one environment before production should have the data of production
- If the data of production is used elsewhere, it should be anonymized
- Restoring and anonymization of data should be automated as well
- The capability to provide anonymized data should be considered when choosing a hosting provider
- Ability to provide data for development might affect the functionalities that can be implemented

BCF

- At BCF we work on the API and the frontend; the API fetches data from Services not developed by LIIP
- Only the API is continuously tested in our pipelines



Dev data on BCF

At BCF we work with mocked data on development environments

- \+ No need to anonymize it
- \+ Lightweight
- \+ Is great to cover some edge cases
- \+ Not dependent on the hosting provider to have data
- – Hard or even impossible to test performance issues with it
- – Might not cover all edge cases
- – Might not reflect the prod environment in terms of typical usage

Staging data on BCF

At BCF we work with a mix of dummy data and real data on staging environments

- Prod has a fake user in production
- When restoring the staging from prod, the hoster provides us with access to the fake user
- All other users are still unavailable

\+ Good to test general performance
\+ Easy to setup
− The data isn’t anonymized, even if we don’t have access to it, it’s still sensible data
− Can only test from one user perspective

Thank you

Olivier Wenger
olivier.wenger@liip.ch


L//P
DIGITAL PROGRESS

Links

- DevSecOps diagram https://dt-cdn.net/images/devsecops-image-2000-6557ba1b00.png