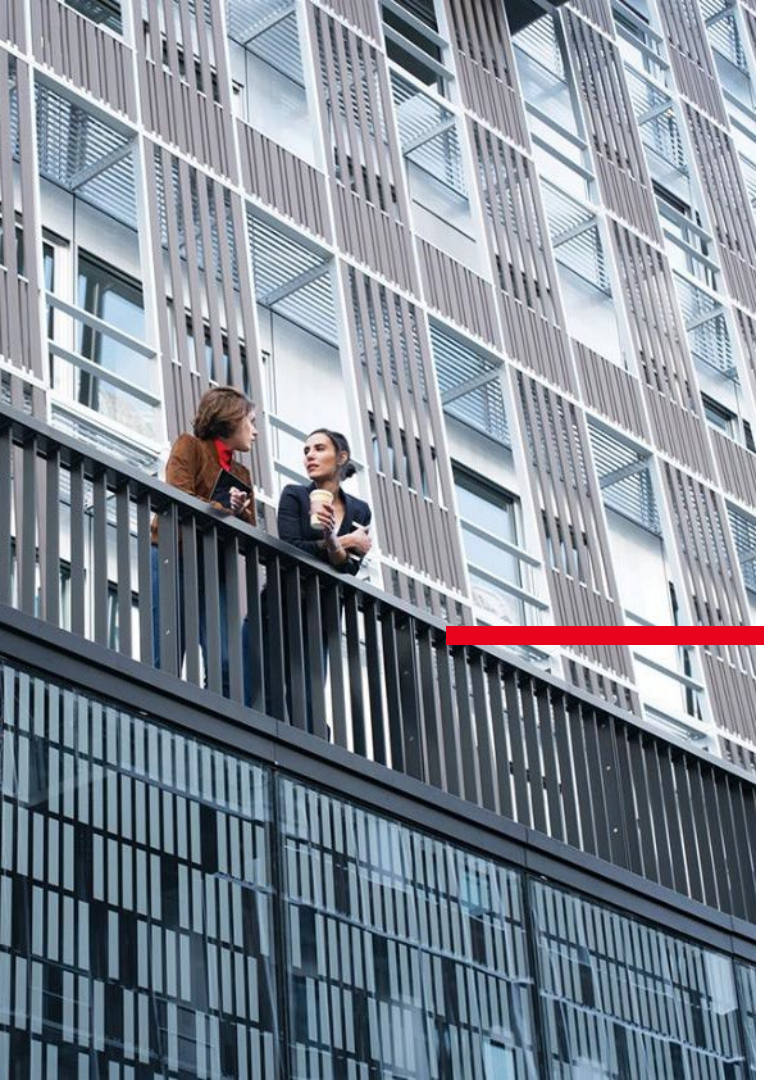


DEV SEC OPS

Praktické řešení DevSecOps v KB a důvody jeho nasazení

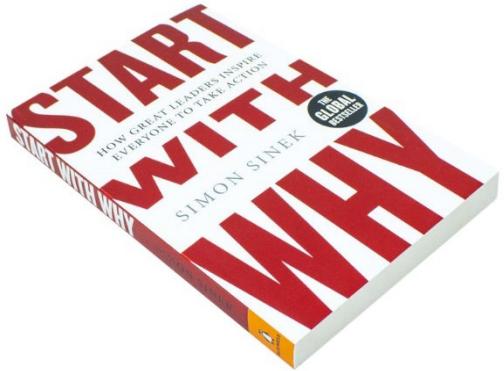
THE FUTURE IS YOU

SOCIETE GENERALE

JIŘÍ KOHOUT |
Komerční banka |
Lead Security Architect |

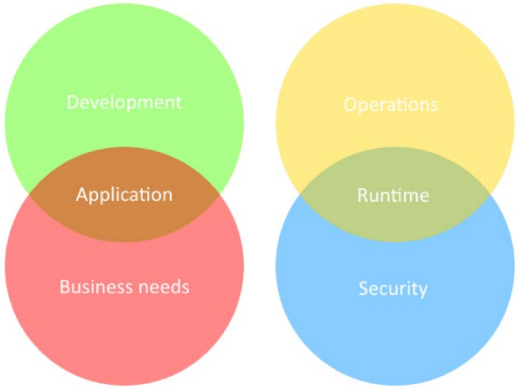
1. PROČ

Start with why…



SOCIETE GENERALE

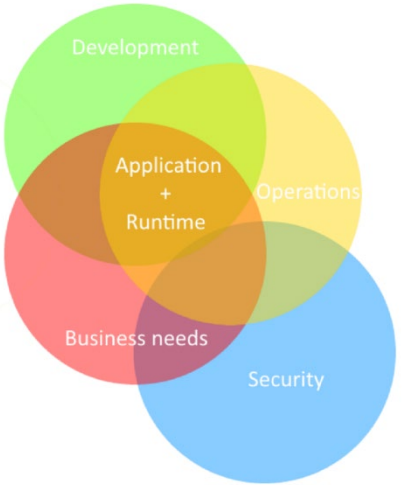
VÝCHOZÍ POZICE



HISTORICKÁ ZKUŠENOST

- Centrální tým **„IT operations“ provozoval** jednotlivé aplikace
- Vývojový tým musel při předání **plnit přísná pravidla** definovaná provozem
- **Změny** se do prostředí dělaly v zásadě **4x ročně**
- **Penetrační testy** potvrzovaly kvalitu aplikace, typicky **na konci dodávek**

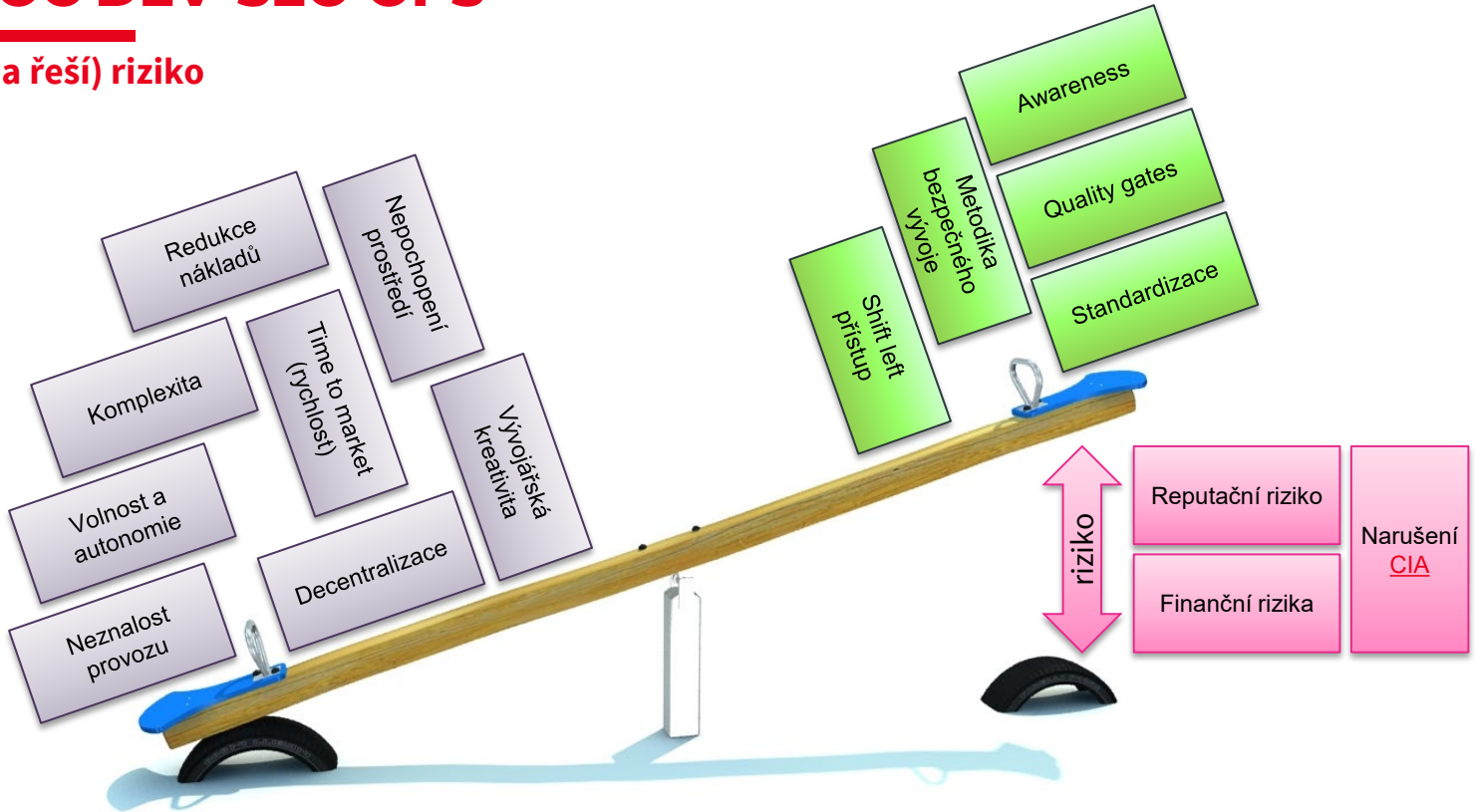
DEV OPS



- „IT operations“ provozuje pouze **sdílené velké bloky** funkcionalit (např. databáze, sítě)
- Vývoj se, nově, **učí aplikace provozovat** (role SRE v rámci vývojového týmu)
- **Množství změn** se „utrhlo ze řetězu“ (včetně oprav)
- Místo monolitu **architektura mikroslužeb**
- Větší dělba práce (**decentralizace**)

TEDY PROČ DEV-SEC-OPS

Jak se „tvoří“ (a řeší) riziko



VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Shift left přístup

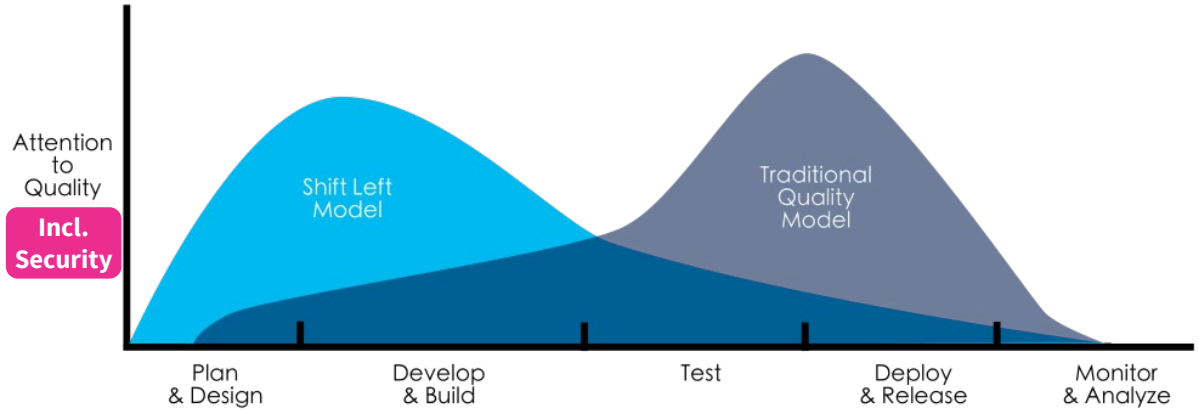
- Shift left přístup
- Metodika bezpečného vývoje
- Quality gates
- Standardizace
- Awareness

SHIFT LEFT

- Bezpečnostní **témata se přesouvají „vlevo“**, do ranějších fází vývoje – designu, buildu

PŘIDANÁ HODNOTA

- Dle studií až **60x nižší cena oprav** chyb v porovnáním s tradičním přístupem
- Možnost **odchytit zásadní problémy** mnohem dříve
- **Kooperace** - lidé z různých týmů (Bu, Dev, Sec, Ops) se musí bavit dříve a vzájemně se chápat a dávat informace
- Příklad činností
  - Threat modeling
  - Feasibility study, PoC, MVP
  - Identifikace bezpečnostních a funkčních potřeb jako základní vstup pro vývoj



studie: zdroj, diagram: zdroj

SOCIETE GENERALE

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Metodika bezpečného vývoje

- Shift left přístup
- Metodika bezpečného vývoje
- Quality gates
- Standardizace
- Awareness

DEVOPS HANDBOOK

- 10 hlavních témat (respektujících životní cyklus aplikace)
- **85 kapitol**
- **334 stránek textu**
- 57MB PDF

PŘIDANÁ HODNOTA

- Vývojáři **znají celý proces** vývoje
- Všichni **pracují více/méně stejně** - podpora **komunikace** a týmové práce
- **Znají specifika** našeho prostředí

INSPIRACE

- OWASP SDLC, NIST 800-64, Microsoft SDL

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Quality gates

- Shift left přístup
- Metodika bezpečného vývoje
- Quality gates
- Standardizace
- Awareness

QUALITY GATES

- **Bezpečnostní a kvalitativní kontroly** prováděné automaticky v průběhu procesu buildu aplikace
- „Brány“ mohou být **doporučující či blokující** s ohledem na související riziko / dopad do funkcionality
- „Brány“ nemusí být pouze technické – některé mohou mít vazbu na „lidské zpracování“ či posouzení

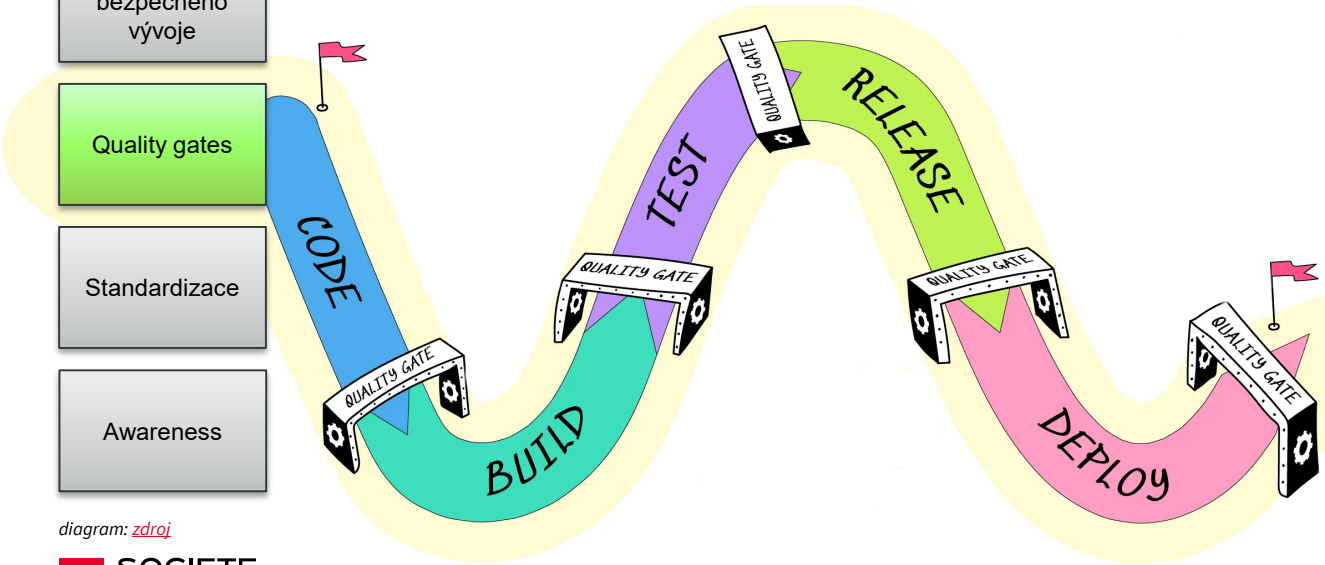


diagram: zdroj

PŘIDANÁ HODNOTA

- Úspěšný průchod **zajišťuje určitou minimální kvalitu** výsledného produktu
- Vytváří **očekávatelný stav** pro konzumenty řešení
- Snižuje **úsilí potřebné pro kontrolu** shodu se standardy
- Zmenšuje „lidovou tvořivost“ cestou **standardizace**

SOCIETE GENERALE

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Quality gates

- Shift left přístup
- Metodika bezpečného vývoje
- **Quality gates**
- Standardizace
- Awareness

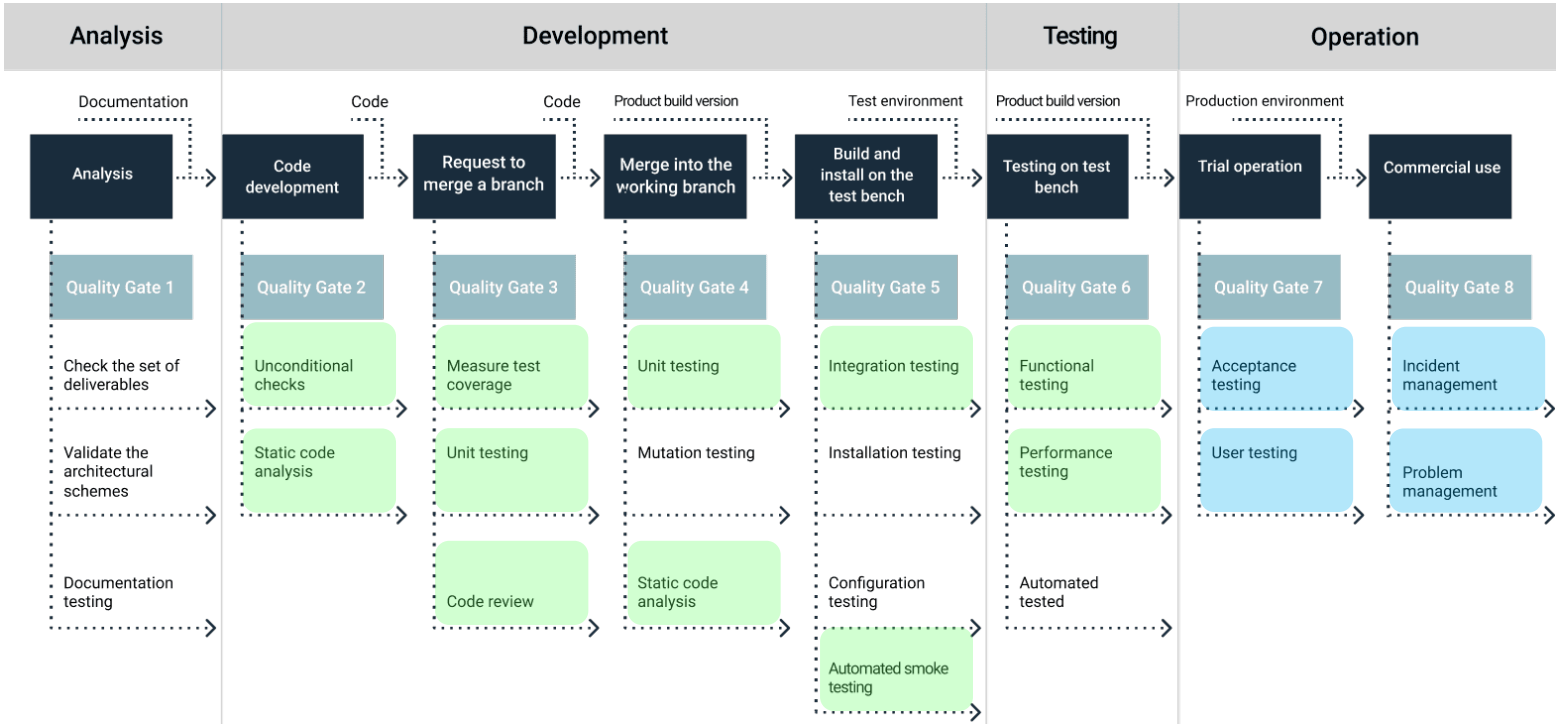


diagram: zdroj

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Standardizace

- Shift left přístup
- Metodika bezpečného vývoje
- Quality gates
- **Standardizace**
- Awareness

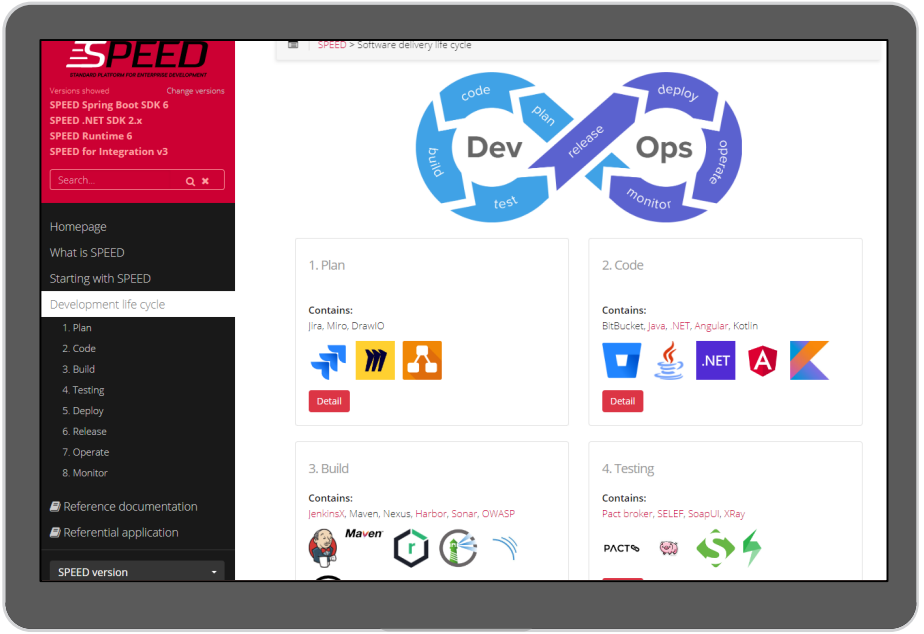
PAAS INTEGRAČNÍ VÝVOJOVÁ PLATFORMA

Standard Platform for EnterprisE Development

The recommended way to develop microservice applications enabling effective and scalable development up to production.

- Certifikované a standardizované **CI/CD pipelines**
- Speed for integration (**lightweight** verze)
- **Feature flag** pro podporu trunk-based development
- Maximální podpora **automatizace**
- REST **API podpora**
- Využívá spolupráci 30 technologií
  - Kubernetes, Spring Boot SDK, .NET SDK, Git, Redis, ActiveMQ, Nginx, Maven, Bitbucket, Jenkins, Nexus, Sonarcube, Helm, Argo, Kafka, Grafana, Zipkin, Elasticsearch, Kibana, LogStash, InfluxData, Istio,…

SPEED is an KB internal, cloud-native development platform for applications with microservice architecture.
It provides necessary end-to-end functionality to shorten development time, simple scalability and release flexibility.



VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Školení a certifikace

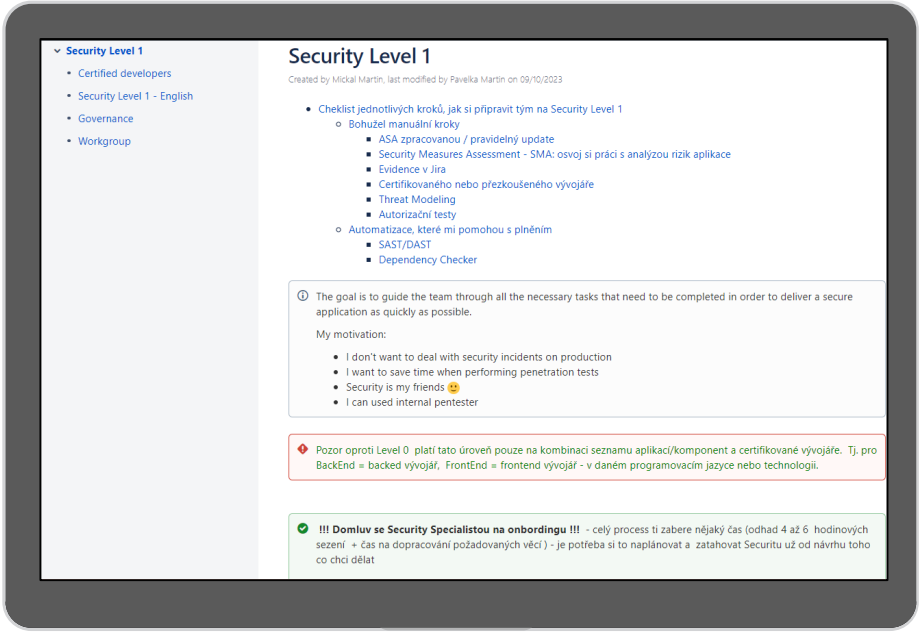
- Shift left přístup
- Metodika bezpečného vývoje
- Quality gates
- Standardizace
- Awareness

SML1 CERTIFIKACE

- Certifikace **aplikací a vývojářů**
- **Zlepšení znalosti** v bezpečnostních oblastech spojených s vývojem – OWASP top 10, hacking techniky, threat modeling, SAST, DAST, dependency checker, apod.
- Součástí **certifikace** není pouze **školení**, ale i test + **kontrola** znalostí každý rok

NAŠE STATISTIKY

- Certifikováno 77 vývojářů
- 32 certifikovaných aplikací, 24 v procesu certifikace a dalších 22 má podanou přihlášku



DEV-SEC-OPS OBECNĚ

„Jen“ taková ležatá osmička

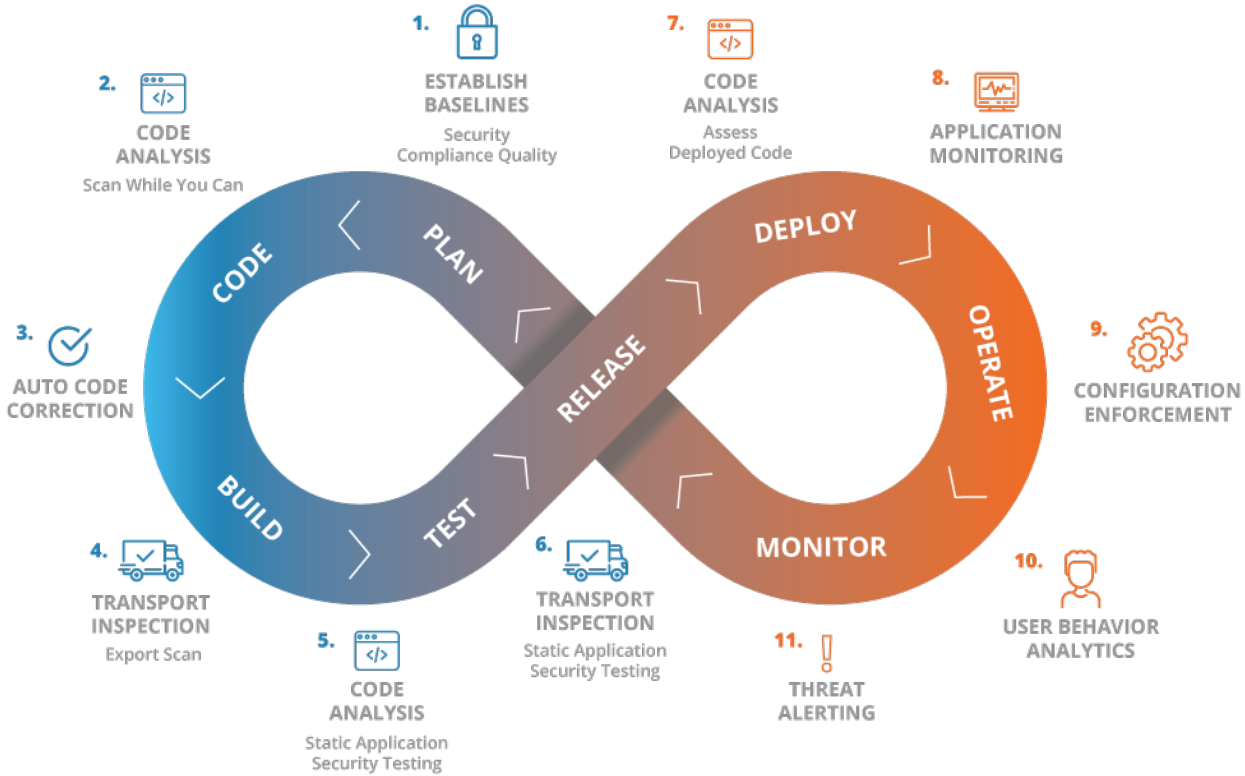
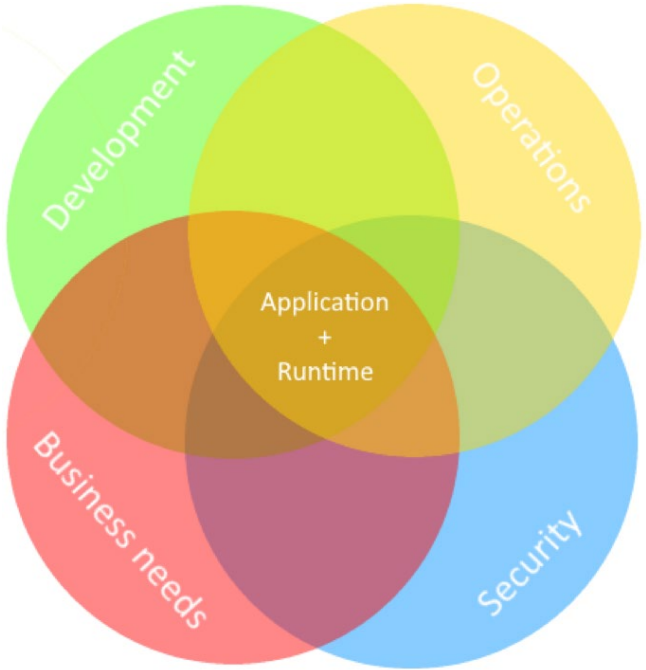


diagram: zdroj

DEV-SEC-OPS V KB

HLAVNÍ PŘÍNOSY

- Rychlost
- Vyšší základní kvalita
- Lepší spolupráce
- Flexibilita
- Bezpečnost
- Nižší náklady



HLAVNÍ PILÍŘE

- Standardizace
- Automatizace
- Komunikace
- Monitoring
- Awareness

JE TOHO HROZNĚ MOC, TO NEDÁME

Začněte

Bezpečnost je ochrana podnikání, nejde ignorovat, **nejde „ošidit“**

Správný přístup **stojí úsilí**, ale ve finále umí ušetřit – a ocení to zákazníci

Útočník se neptá, nečeká

Nikdy **není pozdě** začít

Rozsah

Každá společnost je jiná, **univerzální přístup neexistuje**

Vytvořte si vlastní funkční set opatření, která vám reálně pomohou tam, kde to dává smysl

Inspirujte se, ale **neklonujte**

Nezapomeňte

Vždy se ptejte **proč** něco potřebujte, chcete, nebo musíte dělat – **zaměřte se na cíl**

Bez vize není úspěch – **buďte vizionáři**

Změna bolí, počítejte s tím

obrázek 1: zdroj, obrázek 2: zdroj, Mr. Steve Jobs: zdroj

THE FUTURE IS YOU

SOCIETE GENERALE