

DEV SEC OPS

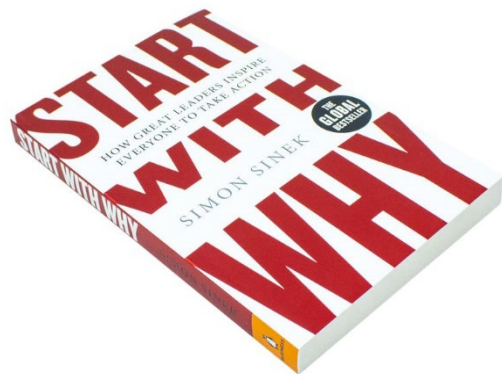
Praktické řešení DevSecOps v KB a důvody jeho nasazení

**THE FUTURE
IS YOU**  **SOCIETE
GENERALE**

JIŘÍ KOHOUT |
Komerční banka |
Lead Security Architect |

1. PROČ

Start with why...



*Simon Sinek
A bit of optimism podcast*

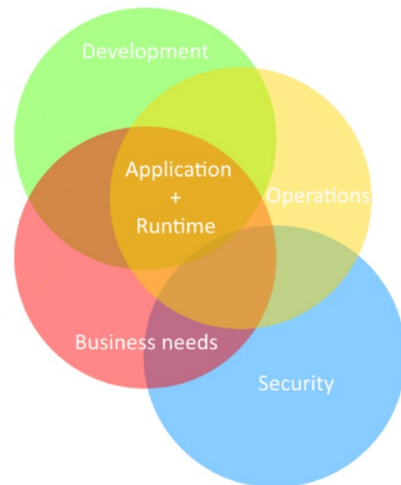
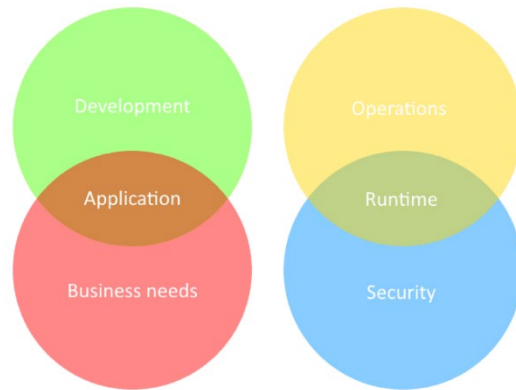
VÝCHOZÍ POZICE

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**

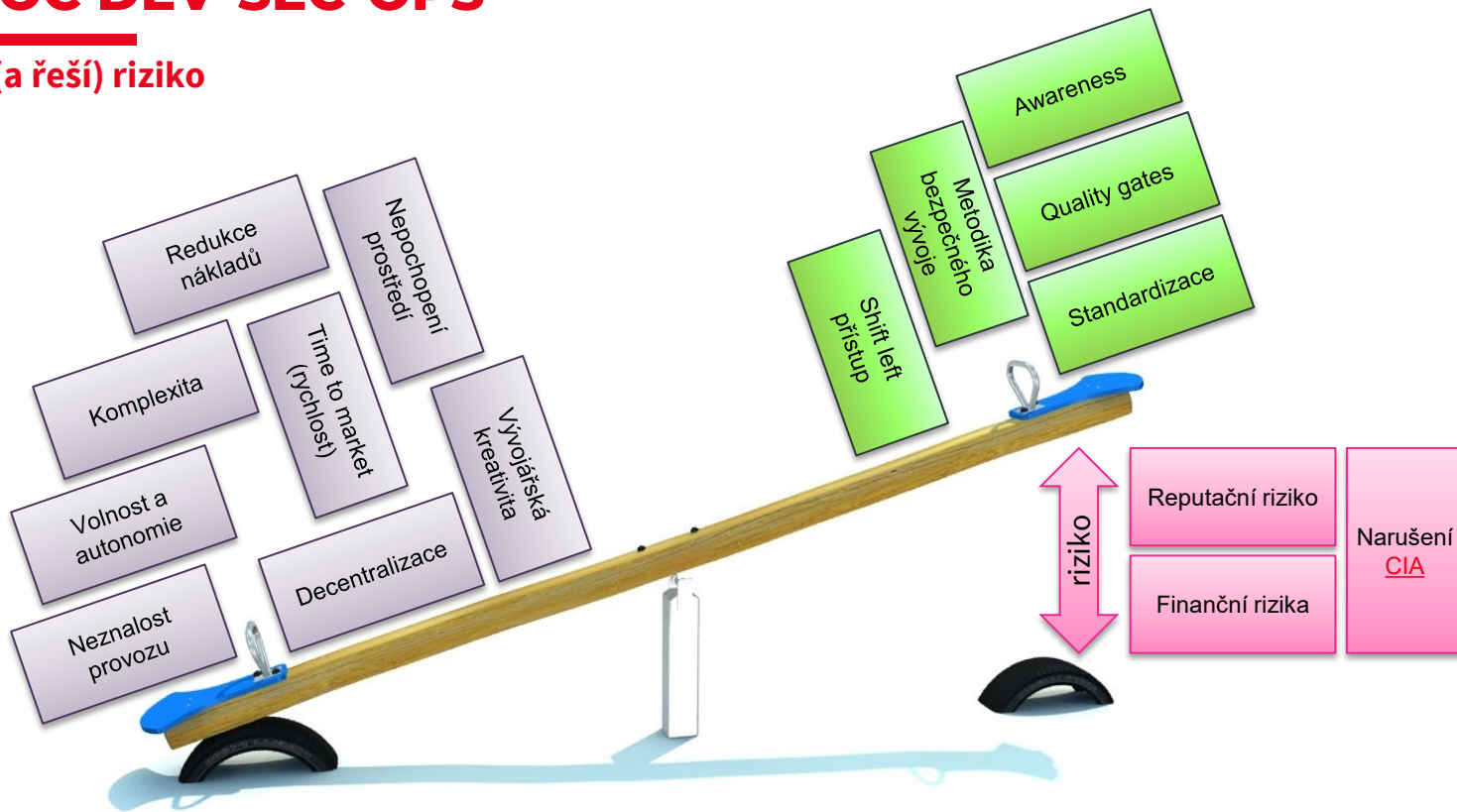
DEV OPS

- „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 „utrhllo ze řetězu“ (včetně oprav)
- Místo monolitu **architektura mikroslužeb**
- Větší dělba práce (**decentralizace**)



TEDY PROČ DEV-SEC-OPS

Jak se „tvorí“ (a řeší) riziko



VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Shift left přístup

Shift left přístup

SHIFT LEFT

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

Metodika bezpečného vývoje

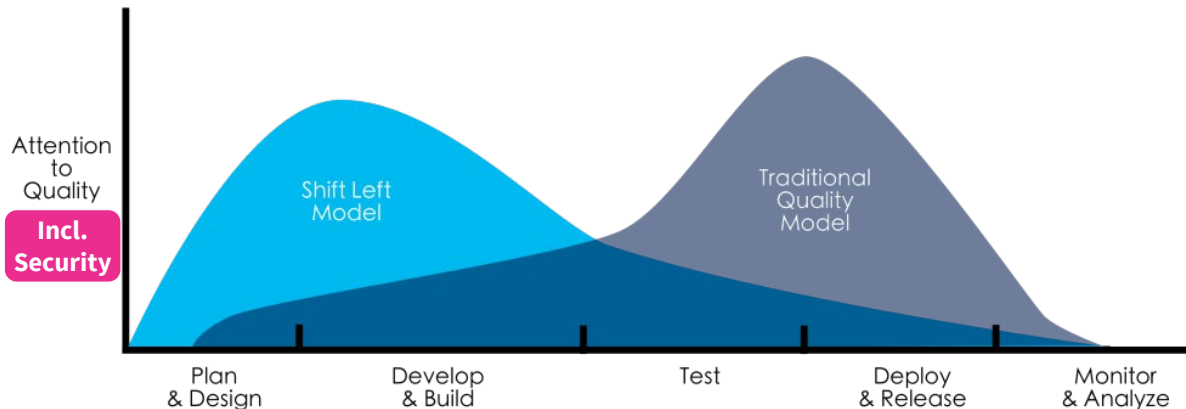
PŘIDANÁ HODNOTA

- 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

Quality gates

Standardizace

Awareness



studie: zdroj, diagram: zdroj

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Metodika bezpečného vývoje

Shift left přístup

Metodika bezpečného vývoje

Quality gates

Standardizace

Awareness

DEVOPS HANDBOOK

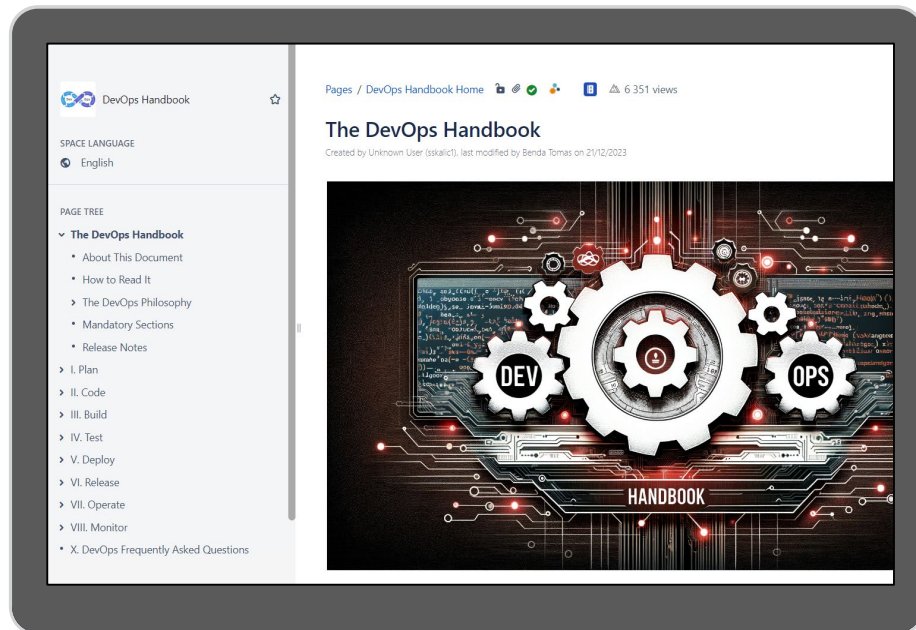
- 10 hlavních témat (respektujících životní cyklus aplikace)
- **85 kapitol**
- **334 stránek textu**
- 57MB PDF

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

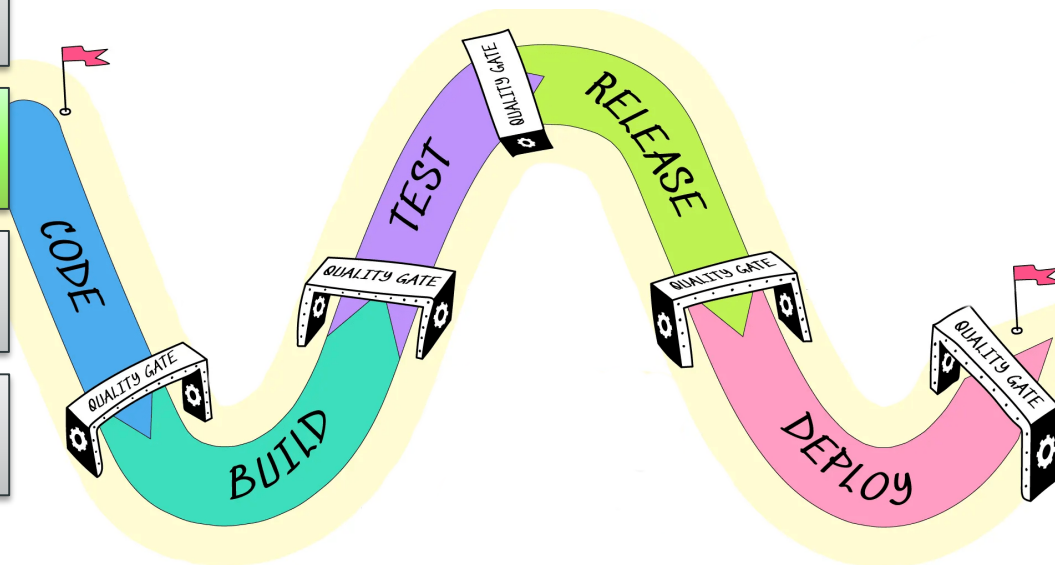
Quality gates

Standardizace

Awareness

QUALITY GATES

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



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**

diagram: zdroj

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Quality gates

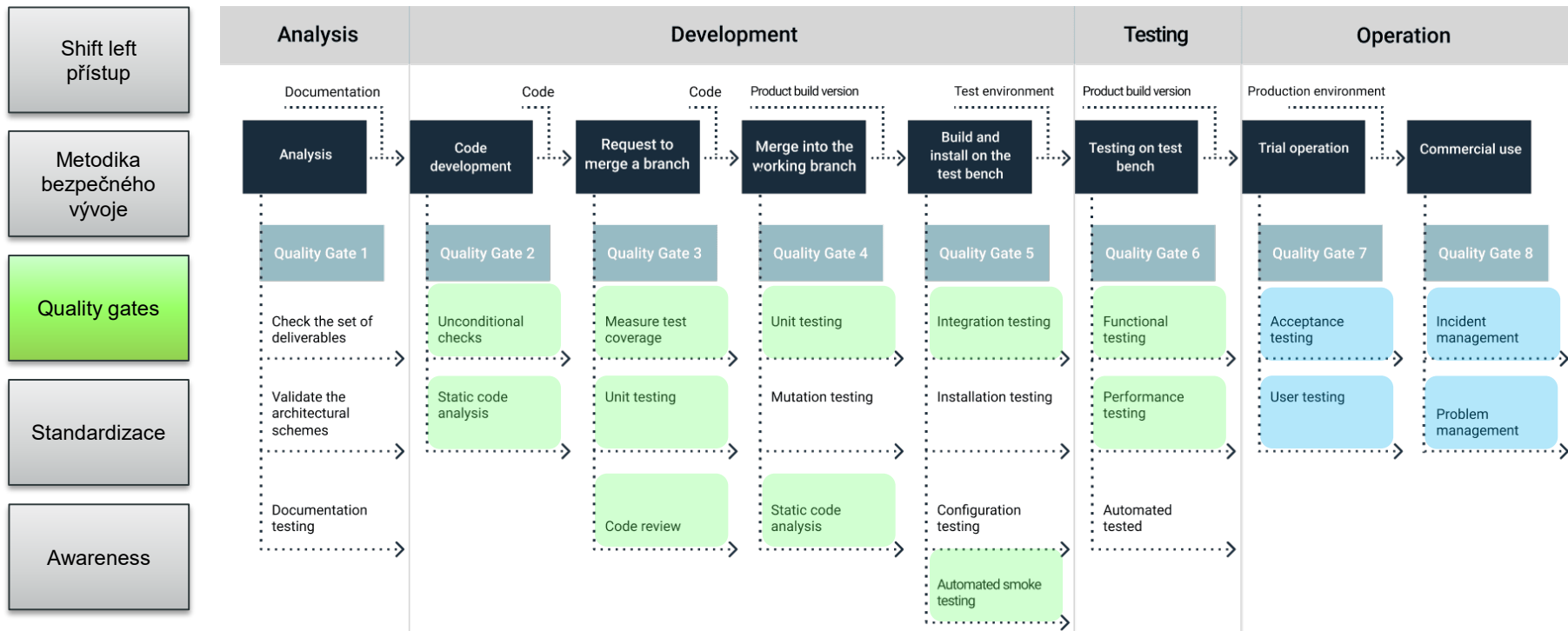


diagram: zdroj

VÝBĚR NAŠICH ZÁSADNÍCH OPATŘENÍ

Standardizace

Shift left přístup

Metodika bezpečného vývoje

Quality gates

Standardizace

Awareness

PAAS INTEGRAČNÍ VÝVOJOVÁ PLATFORMA

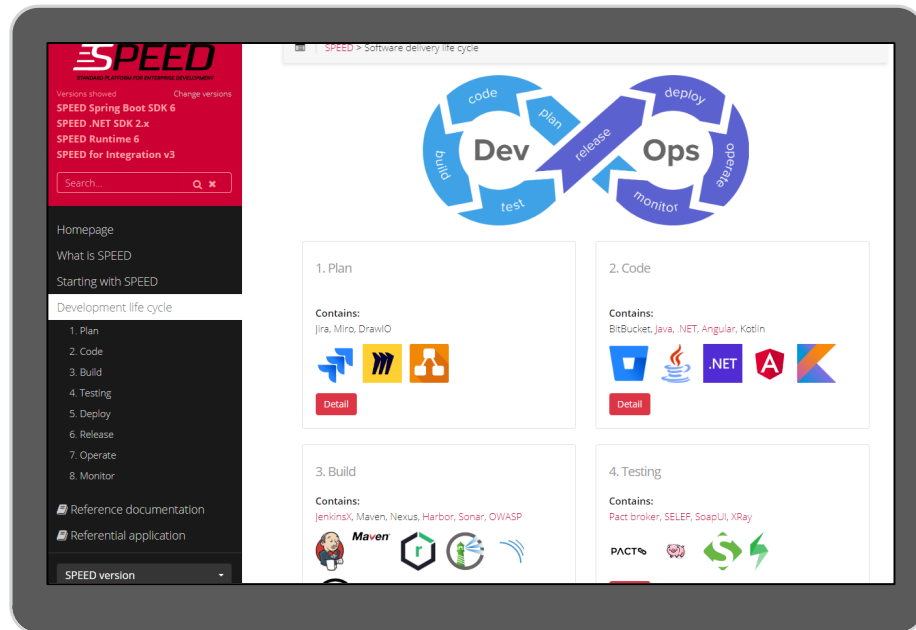
Standard Platform for Enterprise Development

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

The screenshot shows a document titled "Security Level 1" with a sidebar menu containing "Security Level 1", "Certified developers", "Security Level 1 - English", "Governance", and "Workgroup". The main content includes a checklist for "Security Level 1" with items like "Checklist jednotlivých kroků, jak si připravit tým na Security Level 1", "Bohužel manuální kroky" (with sub-items: "ASA zpracovanou / pravidelný update", "Security Measures Assessment - SMA: osvoj si práci s analýzou rizik aplikace", "Evidence v Jira", "Certifikovaného nebo přezkoušeného vývojáře", "Threat Modeling", "Autorizační testy"), and "Automatizace, které mi pomohou s plněním" (with sub-items: "SAST/DAST", "Dependency Checker"). Below the checklist is a note: "The goal is to guide the team through all the necessary tasks that need to be completed in order to deliver a secure application as quickly as possible." followed by "My motivation:" and a list of reasons: "I don't want to deal with security incidents on production", "I want to save time when performing penetration tests", "Security is my friends 😊", and "I can use internal pentester". A warning note states: "Pozor oproti Level 0 platí tato úroveň pouze na kombinaci seznamu aplikací/komponent a certifikované vývojáře. Tj. pro BackEnd = backed vývojář, FrontEnd = frontend vývojář - v daném programovacím jazyce nebo technologii." A final note says: "!!! Domluv se Security Specialistou na onboardingu !!! - celý proces ti zabere nějaký čas (odhad 4 až 6 hodinových sezení + čas na dopracování požadovaných věcí) - je potřeba si to naplánovat a zatahovat Security už od návrhu toho co chceš dělat".

DEV-SEC-OPS OBECNĚ

„Jen“ taková ležatá osmička

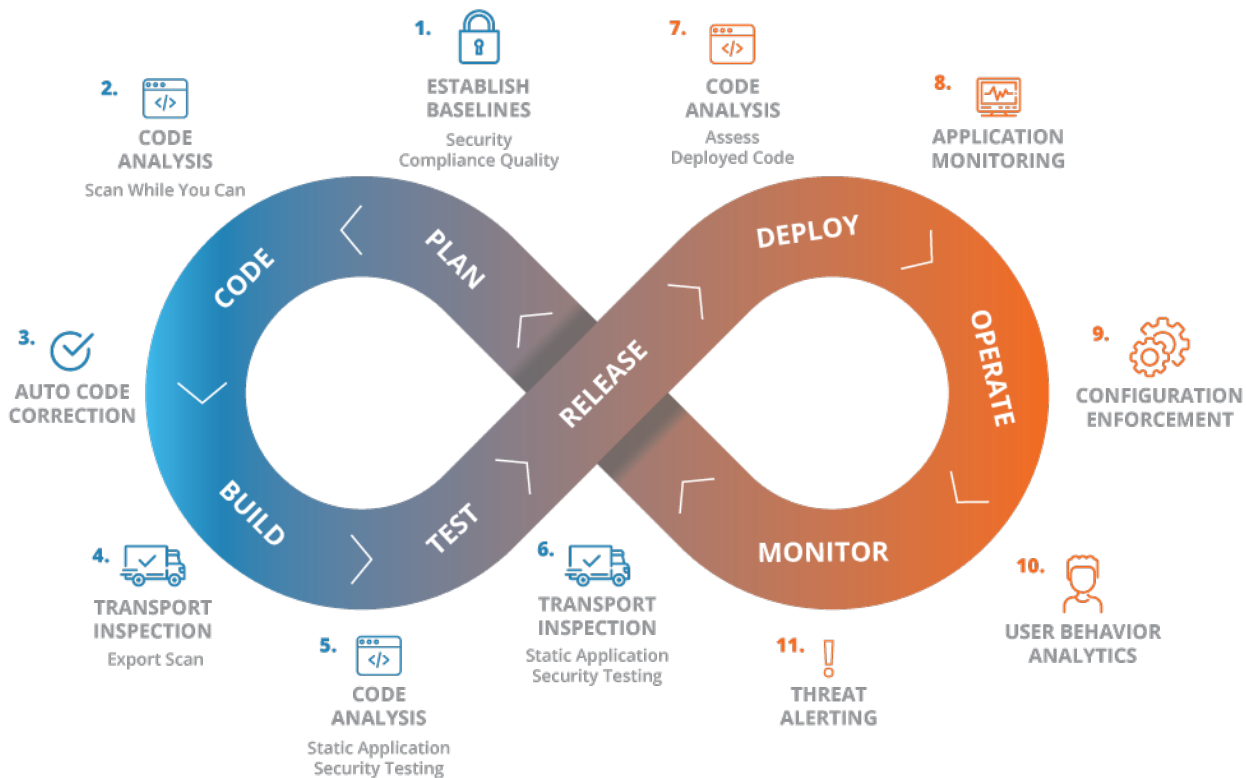
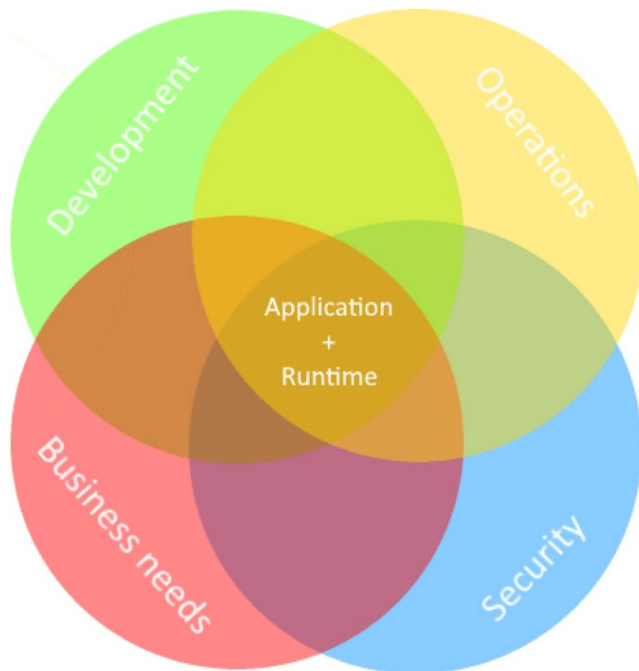


diagram: zdroj

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

obrázek 1: [zdroj](#), obrázek 2: [zdroj](#), Mr. Steve Jobs: [zdroj](#)

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 potřebujete, chcete, nebo musíte dělat – **zaměřte se na cíl**

Bez vize není úspěch – **buďte vizionáři**

Změna bolí, počítejte s tím

DevSecOps Benefits

Shift-Left
Security

Faster Time
to Market

Collaboration

Continuous
Improvement

**THE FUTURE
IS YOU**



**SOCIETE
GENERALE**