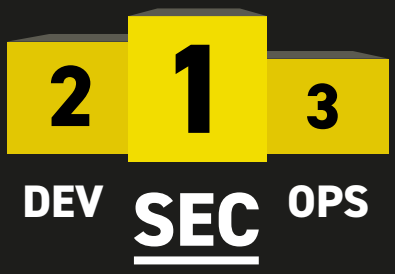

# ‘SEC’ OP NUMMER ÉÉN IN DEVSECOPS

## SECURITY IN DEVOPS

# ‘SEC’ OP **NUMMER ÉÉN** IN DEVSECOPS

**SecDevSecDevOpsSec, zo zouden wij Security (Sec) eigenlijk toe willen voegen aan DevOps. Vooraf, tijdens én na de ontwikkeling van je software. Want laten we eerlijk zijn, een innovatief en wendbaar ontwikkelproces is fantastisch, maar zonder een solide beveiligingsfundament loop je enorme risico's.**
**Maar goed, het SecDevSecDevOpsSec noemen is verre van praktisch, dus noemen wij het ‘gewoon’ DevSecOps, met de kanttekening dat ‘Sec’ wat ons betreft op nummer één staat.**




DevSecOps is een software-ontwikkelingsbenadering die gericht is op het integreren van beveiliging in alle fasen van de software-ontwikkelingslevenscyclus. Het omvat het bouwen, testen en deployen van secure software (Dev-Sec) en het monitoren, beheren en handhaven van de beveiliging van operationele systemen en applicaties (Sec-Ops). Het doel van DevSecOps is het creëren van veiligere en meer betrouwbare software.



## VOORDELEN VAN DEVSECOPS: VEILIGER ÉN EFFICIËNTER

Om onze mening over het belang van Sec in DevSecOps kracht bij te zetten, benoemen we graag eerst een paar voordelen van DevSecOps ten opzichte van het klassieke DevOps:

### MINDER RISICO’S

Bij DevSecOps wordt beveiliging een integraal onderdeel van je software. Risico's worden hierdoor kleiner en beter beheersbaar en de kans op financiële- en imagoschade wordt kleiner.

### EFFICIËNTER

Door beveiliging en testen al heel vroeg in het softwareontwikkelingsproces te integreren kun je kwetsbaarheden vroegtijdig identificeren en veel makkelijker oplossen dan wanneer je ze later in het proces zou tegenkomen. Dat noemen we ‘Shift-Left’; het verplaatsen van deze stap naar de ‘linkerkant’, eerder in het proces.

### VEREENVOUDIGDE COMPLIANCE

Door beveiligingscontroles en -tests geautomatiseerd op te nemen in de CI/CD-pijplijn, wordt bij elke uitvoering van de pipeline automatisch bewijslast gegenereerd. Dit betekent dat er audit trails en rapporten beschikbaar zijn die aantonen dat de juiste beveiligingscontroles zijn uitgevoerd, wat kan helpen bij het aantonen van naleving van regelgeving en compliancevereisten. Dit kan organisaties veel tijd en moeite besparen.

### GEZAMENLIJKE VERANTWOORDELIJKHEID

DevOps gaat over gezamenlijke verantwoordelijkheid. Draagvlak en betrokkenheid zijn bij een onderwerp als security van levensbelang. Door DevSecOps te implementeren wordt er een gezamenlijke inspanning afgedwongen om veiligheidsrisico's te beperken. Iedereen in het DevSecOps team is medeeigenaar van de security.

## HOGE KOSTEN ALS JE JE BEVEILIGING LINKS LAAT LIGGEN

Je kunt er natuurlijk voor kiezen om de beveiliging tijdens het ontwikkelproces van je software buiten beschouwing te laten. Daar zijn echter een aantal risico's mee gemoeid en het is goed om je hier bewust van te zijn. Natuurlijk is er een groter risico op cyberaanvallen, maar het effect daarvan is groter dan je in eerste instantie wellicht denkt.

Wist je dat IBM* de gemiddelde kosten van een cyberaanval inschat op 4.4 miljoen euro?

Bovendien komt er steeds meer wet- en regelgeving op het gebied van informatiebeveiliging, ook voor bedrijven en branches die daar voorheen nog niets mee van doen hadden. Het niet naleven van deze regelgeving en compliance-richtlijnen kan juridische gevolgen hebben, zoals fikse boetes.

En tenslotte leidt een cyberaanval vaak ook nog tot een verlies van vertrouwen en reputatieschade, waardoor het moeilijk wordt om klanten aan te trekken en te behouden.

**Kortom: kostentechnisch is het best slim om na te denken over security.**

** bron: www.itdaily.com*

## ZO MAAK JIJ JE SOFTWARE SAFE

Maar goed, secure software maken, hoe doe je dat dan? Als je werkt binnen een DevOps omgeving, gebruik je meestal al een CI/CD pipeline, een geautomatiseerd proces voor het integreren, bouwen, testen en implementeren van software(wijzigingen). Zo'n CI/CD pipeline is een ideale basis om security aan toe te voegen. Dat doe je bijvoorbeeld met deze tools en guidelines:

### 1. SECURITY BY DESIGN

de Security by Design benadering is een concept waarbij beveiliging vanaf het allereerste begin van het ontwikkelproces wordt ingebed in de architectuur en in het ontwerp. Beveiliging is hierbij een fundamenteel onderdeel van het systeem. Twee essentiële onderdelen van Security by Design zijn Threat Modelling en Threat Intelligence.

*Bij Threat Modelling wordt een gestructureerde analyse uitgevoerd waarbij mogelijke bedreigingen, aanvals-vectoren en kwetsbaarheden in het ontwerp worden geïdentificeerd en beoordeeld. Dit stelt teams in staat om passende beveiligingsmaatregelen te implementeren en zo deze bedreigingen te beperken of te elimineren.*

*Threat Intel(ligence) omvat het verzamelen en analyseren van informatie over actuele en opkomende bedreigingen, inclusief de technieken en hulpmiddelen die door aanvallers worden gebruikt. Door (Cyber) Threat Intelligence (CTI) mee te nemen in het ontwerpproces, kunnen teams later in het proces proactief reageren op bekende bedreigingen en potentiële zwakke punten aanpakken. Dit stelt hen in staat om effectieve en actuele beveiligingsmaatregelen te implementeren.*

Security by Design is vaak wat kostbaar, maar niet te vergelijken met de kosten van een mogelijk beveiligingslek of – aanval. En uiteraard is het voorkomen van securityproblemen veel makkelijker dan het aanpassen van de architectuur van je applicatie of infrastructuur achteraf.

### 2. SSDLC

De Secure Software Development Life Cycle (SSDLC) is een aanpak om software te ontwikkelen waarbij beveiliging een integraal onderdeel is. Het maakt deel uit van alle stappen in het proces. Door het toevoegen van tests en controles aan je CI/CD pipeline krijg je veilige en meer betrouwbare software.

### 3. TOOLING

Tooling die kwetsbaarheden en beveiligingslekken opspoort in je broncode of op je draaiende applicatie. Een bekende DAST (Dynamic Application Security Testing) tool is OWASP ZAP, dat aanvallen op je software simuleert om zwakheden te vinden. Daarnaast is er de OWASP dependency checker, die je

waarschuwt als er bepaalde bekende weaknesses en vulnerabilities uit de CVE en CWE databases zijn gebruikt in jouw software.

## 4. LOGGING EN MONITORING.

Bij Security Logging worden relevante beveiligingsgebeurtenissen en -activiteiten gelogd waardoor er inzicht komt in potentiële bedreigingen en kwetsbaarheden. Security Monitoring is het voortdurend monitoren van systemen en netwerken op verdachte activiteiten. Hierdoor kunnen potentiële beveiligingsincidenten snel worden gedetecteerd. Bij CTI – zoals hierboven genoemd – wordt informatie over gebruikers gelogd en gemonitord, waardoor bekende bedreigingen en verdachte activiteiten al in een vroeg stadium worden opgemerkt. Zowel security logging als security monitoring stelt ontwikkelaars in staat om proactief te reageren en, indien nodig, passende maatregelen te nemen om de software veilig te maken en houden.

## EEN LAATSTE TIP: BREID JE TEAM(S) UIT

Het belang van security is duidelijk. Bovendien is security alleen effectief als het cross-the-board wordt meegenomen. Het simpelweg toevoegen van een aantal security scanners in je pipeline is niet genoeg. Het toevoegen van 'Sec' aan DevOps zonder dit echt goed uit te denken is ook niet genoeg. Het gaat om een significante verandering in de mindset, waarbij beveiliging als een integraal onderdeel wordt beschouwd en waarin samenwerking tussen ontwikkeling, beveiliging en operations centraal staat.

Enerzijds is het belangrijk om je huidige teams meer security-minded te maken. Je developers moeten ook meewerken om de software beter, efficiënter en vooral veiliger te maken. Maar, om te zorgen dat 'Sec' echt de aandacht krijgt die het verdient is het volgens ons noodzakelijk om je team uit te breiden. Wij vinden securityspecialisten of analisten in je team onmisbaar. Zij kunnen zich vastbijten in onderwerpen waar developers geen tijd of kennis voor, of interesse in hebben. Denk hierbij aan logging en monitoring of vulnerability management. Daarnaast is het goed om de beschikking te hebben over een aantal externe specialisten die kunnen worden ingeschakeld waar nodig. Denk dan aan een ethical hacker die gaat proberen om in te breken in jouw systemen. Zo leg je nog meer mogelijke kwetsbaarheden bloot.

**BEN JE OP KORTE TERMIJN OP ZOEK NAAR SECURITY ENGINEERS OF EXTERNE ANALISTEN VOOR JOUW DEVSECOPS TEAM(S)? TEAM ROCKSTARS IT HEEFT DE BESTE IT SECURITY ROCKSTARS IN HUIS DIE STAAN TE POPELEN OM BIJ JOU AAN DE SLAG TE GAAN. NEEM CONTACT MET ONS OP VOOR MEER INFORMATIE.**

Tenslotte willen we je nog meegeven dat het werken met DevSecOps niet betekent dat een aparte securityafdeling nooit (meer) nodig is. Bij een bepaalde omvang of complexiteit van de IT-omgeving, bij strikte regelgeving of gevoeligheid van gegevens, of in het geval zeer specifieke beveiligingsexpertise is een groep specialisten met een diepgaande kennis van security wat ons betreft alsnog noodzakelijk.

**Wil je hierover verder sparren of wil je meer weten over DevSecOps in het algemeen? Neem dan contact op met Team Rockstars IT. Wij vertellen je er graag (nóg) meer over.**