GIDS

De complete gids voor DevSecOps & Secure Software Development

SAST, DAST, SCA, shift-left security, kosten en compliance. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Security vroeg in het ontwikkelproces integreren bespaart tijd, geld en voorkomt incidenten. Deze cijfers onderbouwen de business case.

100×
duurder om een kwetsbaarheid in productie te fixen dan in ontwikkeling
IBM Cost of Data Breach 2025 [1]

USD 7.600
kosten per kwetsbaarheid opgelost in productie
IBM 2025 [1]

USD 80
kosten per kwetsbaarheid opgelost in ontwikkeling
IBM 2025 [1]

73%
minder kritieke kwetsbaarheden in productie bij volledige DevSecOps
AppSecSanta 2026 [2]

USD 1,7M
lagere datalekkosten bij hoge DevSecOps-adoptie
IBM Cost of Data Breach 2024 [1]

60%
van datalekken door ongepatchte bekende kwetsbaarheden
Ponemon 2025 [3]

44%
van datalekken bevat ransomware (2025)
Verizon DBIR 2025 [4]

USD 10,3B
globale DevSecOps marktomvang (2025)
Precedence Research [5]

1. Wat is DevSecOps?

DevSecOps is de integratie van security in elke fase van de softwareontwikkelingscyclus, van ontwerp tot productie en onderhoud.

Traditioneel werd beveiliging pas aan het einde van het ontwikkelproces getest -- een "security gate" vlak voor release. Dit model is duur en ineffectief: kwetsbaarheden die laat worden ontdekt kosten 100x meer om op te lossen [1]. DevSecOps draait dit om door security "shift-left" te maken: geautomatiseerde security scanning in de CI/CD pipeline, threat modeling in de ontwerpfase en continue monitoring in productie.

De drie technische pijlers zijn SAST (Static Application Security Testing, broncode-analyse), DAST (Dynamic Application Security Testing, runtime testing) en SCA (Software Composition Analysis, open source componenten scannen) [6].

2. Waarom is het belangrijk?

De kosten van onveilige software zijn enorm, en de regelgeving verscherpt. DevSecOps is niet langer optioneel.

60% van datalekken wordt veroorzaakt door ongepatchte bekende kwetsbaarheden [3]. De gemiddelde kosten van een datalek bedragen USD 4,44 miljoen [1]. Voor Nederlandse MKB-bedrijven ligt de gemiddelde schade per cyberincident op EUR 75.000--150.000. DevSecOps reduceert deze risico's structureel: organisaties met hoge DevSecOps-adoptie betalen USD 1,7 miljoen minder per datalek [1].

Daarnaast vereist de Cyberbeveiligingswet (NIS2) security-by-design, en de EU Cyber Resilience Act (CRA) maakt fabrikanten verantwoordelijk voor de beveiliging van digitale producten gedurende de hele levenscyclus [7].

> **De business case in een zin:** Een kwetsbaarheid fixen in de ontwerpfase kost USD 80. Dezelfde kwetsbaarheid in productie kost USD 7.600. DevSecOps maakt het verschil.

3. Hoe werkt het? De DevSecOps pipeline

DevSecOps integreert security checks op elk punt in de softwareontwikkelingscyclus.

1 Plan en ontwerp: Threat Modeling

BIJ ELKE FEATURE

Identificeer bedreigingen in de architectuur voordat je begint met bouwen. Gestructureerd threat modeling kan post-deployment kwetsbaarheden met tot 70% reduceren [8].

2 Code: SAST en Pre-commit Hooks

BIJ ELKE COMMIT

Geautomatiseerde broncode-analyse detecteert kwetsbaarheden voordat code wordt gemerged. 72% van enterprises heeft SAST in de pipeline [6].

3 Build: SCA en Container Scanning

BIJ ELKE BUILD

Scan open source dependencies en container images op bekende kwetsbaarheden. Supply chain-aanvallen nemen sterk toe [4].

4 Test: DAST en Security Testing

BIJ ELKE RELEASE

Test de draaiende applicatie op runtime kwetsbaarheden zoals injection, authentication en authorization fouten.

5 Deploy en Monitor: Runtime Protection

CONTINU

Continue monitoring in productie, vulnerability management en incident response. Detecteer en reageer op bedreigingen in real-time.

4. Wat kost het?

De kosten hangen af van de complexiteit van je ontwikkelomgeving en het gewenste beschermingsniveau.

TIER	OMSCHRIJVING	PRIJSINDICATIE	EENHEID
Basis	SAST/SCA scanning setup, CI/CD security integratie, developer training, eerste kwetsbaarheidsscan	EUR 5.000 -- 15.000	per project
Standaard	Volledige DevSecOps pipeline: SAST, DAST, SCA, container security, threat modeling, security gates	EUR 15.000 -- 50.000	per jaar
Premium	Managed DevSecOps: continue monitoring, dedicated security engineer, compliance rapportage, code review	EUR 4.000 -- 15.000	per maand

MKB-TIP

Begin met open source tools (OWASP ZAP, SonarQube Community) en een eenmalige DevSecOps assessment (EUR 5.000--15.000). Veel MKB-bedrijven hebben al een CI/CD pipeline waar security scanning relatief eenvoudig aan toe te voegen is.

5. Waar moet je op letten bij een aanbieder?

Een DevSecOps-partner moet zowel security als development begrijpen. Zoek een aanbieder die in jouw ontwikkelomgeving kan werken.

- **Ervaring met jouw tech stack** -- .NET, Java, Python, Node.js, containerized, cloud-native?
- **OWASP SAMM kennis** -- Kan de aanbieder je security maturity meten en verbeteren?
- **Developer-vriendelijke aanpak** -- Security moet in de workflow passen, niet ertegen werken
- **Tooling-onafhankelijk** -- Adviseert de aanbieder op basis van jouw situatie, niet op basis van eigen productverkoop?
- **Kennis van compliance** -- NIS2, CRA, OWASP Top 10, PCI DSS waar relevant

10 VRAGEN VOOR JE AANBIEDER

1. Hoeveel DevSecOps-implementaties hebben jullie gedaan in onze tech stack?
2. Welke SAST/DAST/SCA tools adviseren jullie en waarom?
3. Hoe integreren jullie security in onze bestaande CI/CD pipeline?
4. Hoe gaan jullie om met false positives zonder developers te frustreren?
5. Welke metrics gebruiken jullie om security maturity te meten?
6. Bieden jullie secure coding training voor onze developers?
7. Hoe helpen jullie met SBOM-management en supply chain security?
8. Wat is de doorlooptijd van implementatie tot werkende pipeline?
9. Hoe ondersteunen jullie NIS2/CRA compliance?
10. Kunnen jullie referenties geven van vergelijkbare projecten?

> **RED FLAGS**
>
> Wees alert als een aanbieder: alleen tools verkoopt zonder implementatie-ervaring, geen ervaring heeft met CI/CD pipelines, security als "gate" aan het einde plaatst in plaats van doorlopend, of geen aandacht besteedt aan developer experience en false positive management.

6. Veelgemaakte fouten

1. Security als eindcontrole behouden

Een security scan alleen voor release is geen DevSecOps. Het hele punt is integratie in elke fase. Shift-left betekent dat je bij de eerste regel code al scant.

2. Te veel false positives negeren

Als developers overspoeld worden met meldingen, gaan ze alles negeren. Tuning van scanners en prioritering van bevindingen is cruciaal voor adoptie.

3. Open source dependencies niet scannen

Moderne applicaties bestaan voor 70--80% uit open source code. Zonder SCA mis je kwetsbaarheden in het grootste deel van je codebase.

4. Alleen tooling, geen cultuur

DevSecOps vereist een cultuurverandering: developers moeten security als hun verantwoordelijkheid zien. Training en incentives zijn minstens zo belangrijk als tooling.

5. Geen SBOM bijhouden

Zonder Software Bill of Materials weet je niet welke componenten in je software zitten, en kun je niet reageren op nieuwe kwetsbaarheden in dependencies.

7. Compliance: NIS2, CRA en regelgeving

NIS2 / CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet vereist "passende maatregelen" voor de beveiliging van netwerk- en informatiesystemen [7]. Voor softwareontwikkelaars betekent dit security-by-design en supply chain security. Boetes tot EUR 10 miljoen of 2% van jaaromzet.

EU CYBER RESILIENCE ACT (CRA)

De CRA maakt fabrikanten van digitale producten verantwoordelijk voor security gedurende de hele levenscyclus. DevSecOps is de meest praktische manier om aan deze eis te voldoen. Verwachte inwerkingtreding: 2027.

OWASP TOP 10

De OWASP Top 10 voor webapplicaties is de de facto standaard voor applicatiebeveiliging. SAST en DAST tools scannen specifiek op deze kwetsbaarheden [9].

8. Verschil met verwante oplossingen

DISCIPLINE	FOCUS	VERSCHIL MET DEVSECOPS
DevSecOps	Security in de hele SDLC	Geintegreerd in het ontwikkelproces, continu, geautomatiseerd
Pentesting	Eenmalige security test	Momentopname, DevSecOps is continu
Code Review	Handmatige code-inspectie	DevSecOps automatiseert dit met SAST
Vulnerability Management	Beheer van kwetsbaarheden	DevSecOps voorkomt ze, VM beheert de rest
Security Awareness	Medewerkertraining	DevSecOps richt zich op developers, niet op eindgebruikers

9. Trends 2025--2026

AI-Assisted Security Scanning

AI-tools helpen bij het detecteren van kwetsbaarheden en het reduceren van false positives. Maar AI-gegenereerde code bevat ook nieuwe risico's die traditionele scanners missen.

Software Supply Chain Security

SBOM (Software Bill of Materials) wordt standaard. De EU CRA maakt dit verplicht voor digitale producten. Supply chain-aanvallen zijn in 2025 een van de snelst groeiende dreigingen [4].

Platform Engineering

Unified DevSecOps platforms consolideren SAST, DAST, SCA en container security in een dashboard, waardoor complexiteit afneemt en adoptie toeneemt.

10. Aan de slag

DRIE DIRECTE ACTIES

1. Meet je huidige security maturity met OWASP SAMM -- waar sta je nu?
2. Integreer minimaal een SAST-tool in je CI/CD pipeline (open source opties zijn gratis)
3. Plan een DevSecOps assessment om je specifieke verbeterpunten te identificeren

Hulp nodig? Op ibgids.nl/word-gematcht word je vrijblijvend gematcht met DevSecOps specialisten die passen bij jouw tech stack, bedrijfsgrootte en budget.

Bronnenlijst

[1] **IBM Cost of Data Breach Report 2025** -- ibm.com/reports/data-breach

[2] **AppSecSanta DevSecOps Statistics 2026** -- appsecsanta.com/research/devsecops-statistics

[3] **Ponemon Vulnerability Response Study** -- servicenow.com/lpayr/ponemon-vulnerability-survey.html

[4] **Verizon DBIR 2025** -- verizon.com/business/resources/reports/dbir/

[5] **Precedence Research DevSecOps Market** -- precedenceresearch.com/devsecops-market

[6] **Datadog State of DevSecOps** -- datadoghq.com/state-of-devsecops/

[7] **NCSC Cyberbeveiligingswet (NIS2)** -- ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor

[8] **StrongDM DevSecOps Statistics** -- strongdm.com/blog/devsecops-statistics

[9] **OWASP Top 10** -- owasp.org/www-project-top-ten/

[10] **HackerOne Cost of Fixing Security Flaws** -- hackerone.com/blog/cost-savings-fixing-security-flaws

[11] **CBS Cybersecuritymonitor 2024** -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[12] **Grand View Research Application Security Market** -- grandviewresearch.com/industry-analysis/application-security-market

[13] **Practical DevSecOps Statistics 2026** -- practical-devsecops.com/devsecops-statistics-2026/

[14] **Sogeti Nederland DevSecOps** -- sogeti.nl/services/cyber-security/devsecops/

[15] **Oligo Security DevSecOps 2025** -- oligo.security/academy/devsecops-in-2025-principles-technologies-best-practices