DevSecOps bij NS

Platform voor InformatieBeveiliging / 09-04-2024

Remco Blewanus – remco.blewanus@ns.nl

Centrale Platform Organisatie

Even voorstellen

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Utrecht

Remco Blewanus

Security Test Consultant – NS

remco.blewanus@ns.nl

Software Engineering

Test Automation

Security Testing

CPO

Agenda

01 Introductie

02 DevSecOps bij NS

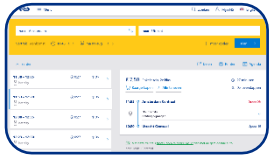
03 Faciliteren van Teams

04 Uitdagingen

05 Conclusie

IT Essentieel voor NS

Reisinformatie

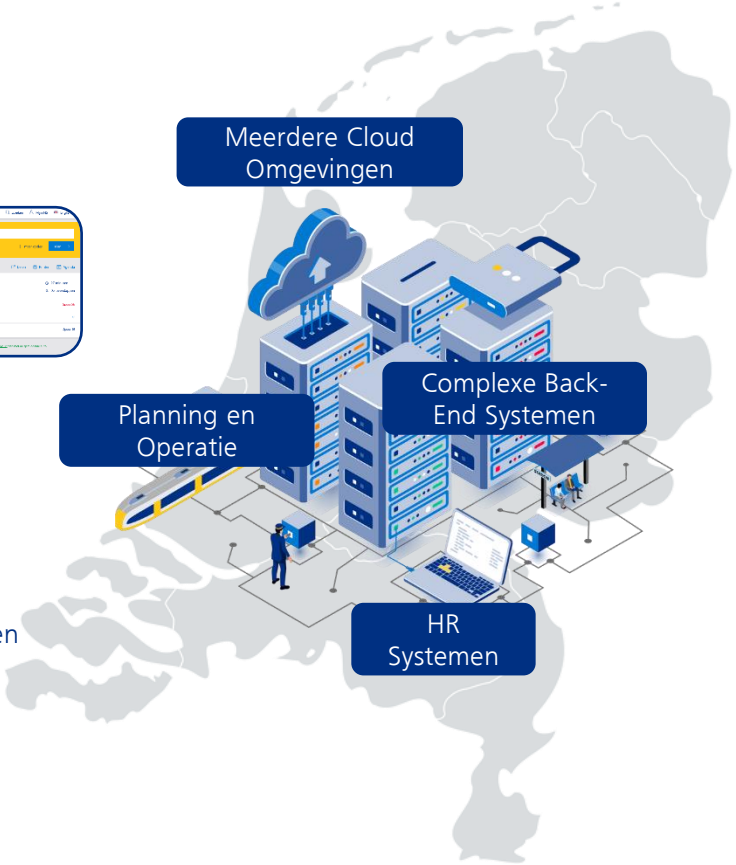


Website

Mobiele App

Kaart
Verkoop
Automaten

Check-in
Poortjes



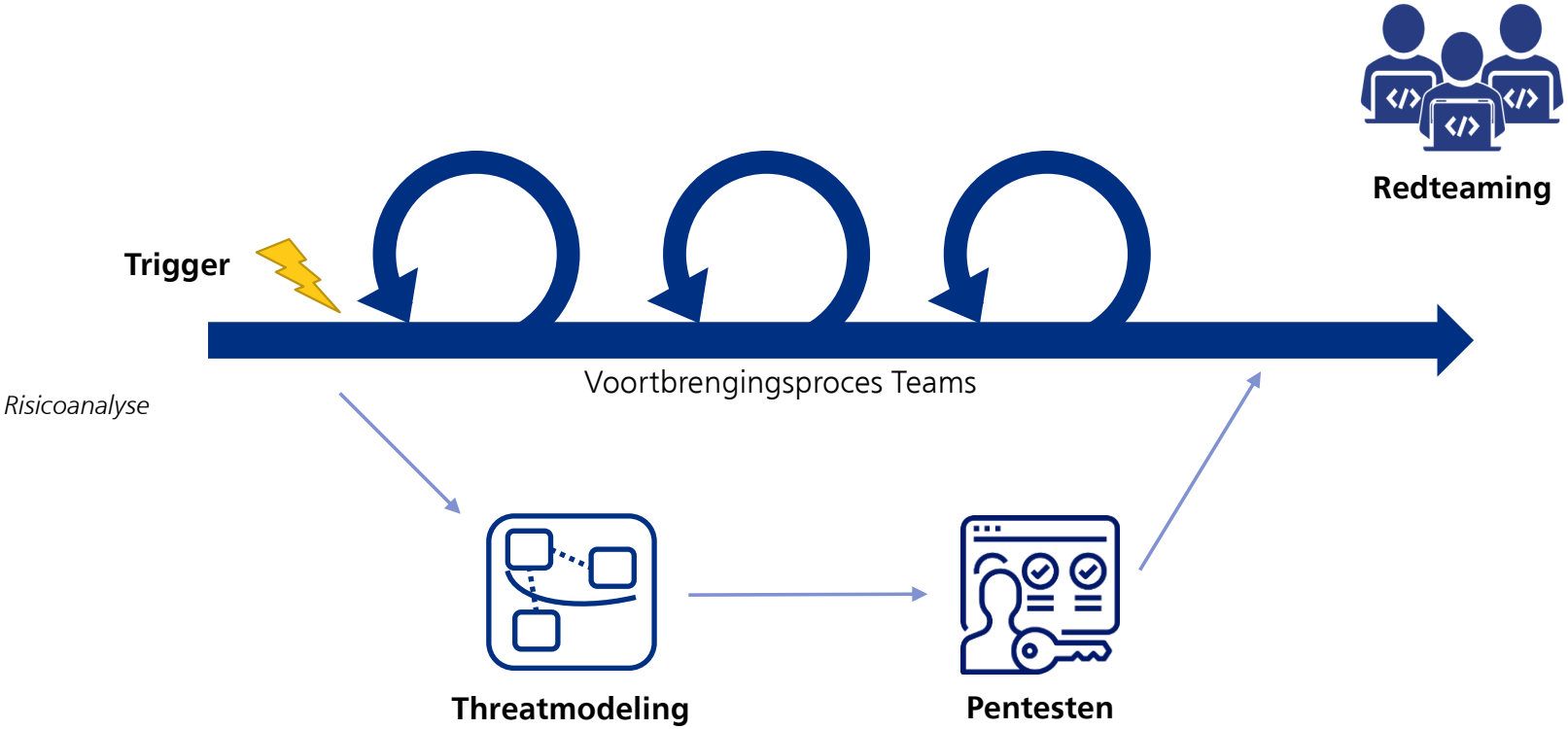
Real-Time Monitoring
Rijdend Materieel

Energiezuinig
rijden voor
Machinisten

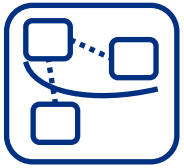
Smartwatches voor het
Vertrekproces

Slim slot OV-
Fiets

Security Testen In Vogelvlucht



Security Test Activiteiten



Threatmodeling

- Op ieder moment te starten: van conceptuele ontwerpfase t/m al jaren in productie
- Iteratieve aanpak lijkt op refinement sessie:
  1. Opstellen dataflow diagram in story/epic
  2. Brainstormen over dreigingen binnen landschap
  3. Inschatten/prioriteren security maatregelen en vertrekpunt voor pentest
- **STRIDE** methode: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege

Pentesten

- Beleid geeft richting aan hoe vaak systemen gepentest dienen te worden
- Specialistische kennis benodigd van buiten het team. Ondersteund vanuit het NS Security Test Team, aangevuld door externe security test partner
- Verschillende methodieken, gedreven door scope, marktstandaarden en gebruikte technologie

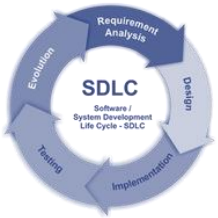
Waarom meer aandacht Security bij Teams?

Toename cybersecurity dreigingen

Teams faciliteren en motiveren in eigen verantwoordelijkheid cybersecurity

NS is een AED (Aanbieder Essentiële Dienst) en onderdeel van vitale infrastructuur NL

Vroeg voorkomen van kwetsbaarheden, goedkoper dan mitigatie achteraf



Inzicht cyberveiligheid in gehele software development lifecycle

Agenda

01 Introductie

02 **DevSecOps bij NS**

03 Faciliteren van Teams

04 Uitdagingen

05 Conclusie

Wat is DevSecOps?

Gartner

"DevSecOps is the **integration of security** into emerging agile IT and DevOps development as **seamlessly and as transparently** as possible. Ideally, this is done without reducing the agility or speed of developers or requiring them to leave their development toolchain environment."

Amazon AWS

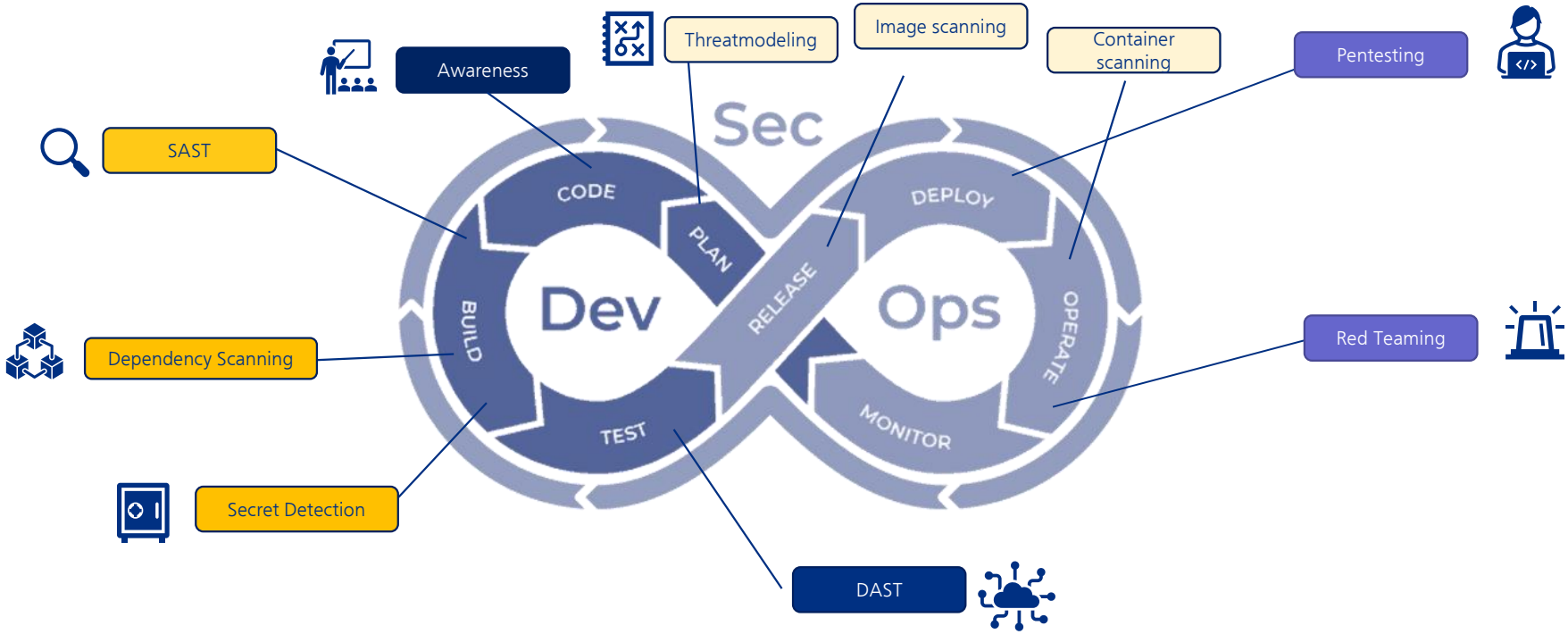
"DevSecOps is the practice of **integrating security testing** at every stage of the software development process. It includes tools and processes that encourage **collaboration between developers, security specialists, and operation teams** to build software that is both efficient and secure. DevSecOps brings cultural transformation that makes security a **shared responsibility for everyone** who is building the software."

DevSecOps

Secure Software Development

Shift-Left Cybersecurity

Security Testen & Activiteiten binnen DevSecOps



DevSecOps - Activiteiten

Technology

SAST – Static Application Security Testing

Whitebox test benadering en ondersteunt teams via buildpipelines tijdens de bouwfase, inclusief linting

Dependency Scanning

Voorkomt kwetsbaarheden vanuit dependencies tijdens de bouwfase

Secret Detection

Voorkomen dat secrets (bijvoorbeeld credentials of keys) uitlekken door het scannen in CI/CD pipeline

DAST – Dynamic Application Security Testing

Blackbox test benadering en ondersteunt teams tijdens integratie en deploy fase met testautomatisering en detectie tools om regressie op vlak van security te voorkomen

DevSecOps- Activiteiten

People & Process

Threat Modeling

Tijdens refinement fase meedenken over oplossingen voor security kwetsbaarheden

Awareness en Kennis

De juiste kennis en awareness binnen het team is essentieel.

Prioritering

Een juiste prioritering van security items door de Product Owner

Way of Working

Security is een integraal onderdeel van de WoW binnen de teams (DoD en acceptatiecriteria), inclusief het oplossen van security bevindingen en incidenten

Agenda

01 Introductie

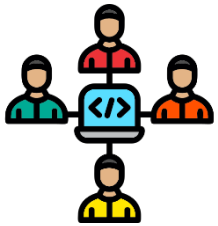
02 DevSecOps bij NS

03 **Faciliteren van Teams**

04 Uitdagingen

05 Conclusie

Quality Engineering Solutions



DevOps Team

Plan > Code > Build > Test > Release ...

- Gestandaardiseerde Oplossingen:
  - Performance
  - Testautomation
  - Security

- Faciliteren Threat Modeling
- Pentest
- Redteaming

Quality Engineering Solutions

Paved Roads

Niet opnieuw het wiel uitvinden…

1

Fase 1 - Decentraal

- Low Config
- Clone & Update
- Gemakkelijke Integratie

2

Fase 2 - Centraal

- Medium Config
- CPO Beheer
- Gegarandeerde Integratie

3

Fase 3 – Product

- High Config
- CPO Product
- Volledig Geïntegreerd

Paved Road SAST

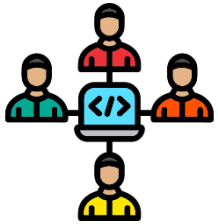
Standaard tooling en diensten die door CPO worden geboden om een DevOps team te ontzorgen in haar development journey

Scannen van broncode op security kwetsbaarheden met **SonarQube.** Voldoen aan NS baseline voor codekwaliteit. Inclusief dashboarding oplossing in de pipeline.

Voorkomen van kwetsbaarheden in dependencies. Dit wordt gescand met **OWASP Dependency Check**. De tool wordt uitgevoerd in de pipeline en de rapporten worden ingelezen in SonarQube.

Scannen van de codebase op secrets met **Gitleaks**. Dit is een krachtige secret scanner die wordt uitgevoerd in de pipeline. De rapporten worden wederom ingelezen in SonarQube.

Adoptie door Teams



Voortbrengingsproces
DevOps Teams

Paved Roads!

Beleid, richtlijnen, kaders…

Capture the Flag!

Hackathons!

- Advies
- Hulp implementatie
- Workshops

Agenda

01 Introductie

02 DevSecOps bij NS

03 Faciliteren van Teams

04 **Uitdagingen**

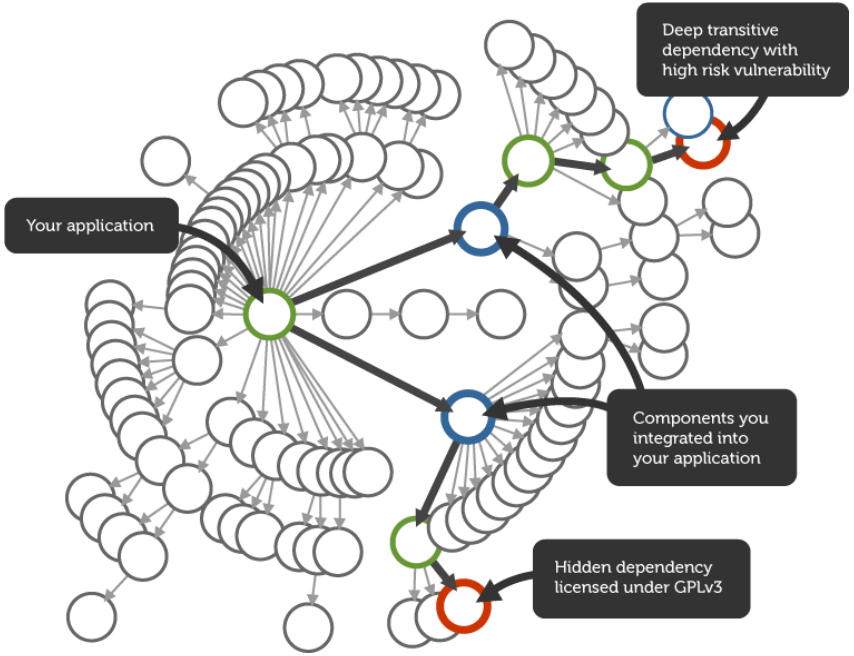
05 Conclusie

Uitdaging: Mitigatie Bevindingen Dependencies

Analyse:

- Kwetsbaar of niet?
- Zo ja, versneld lifecycle management of mitigatie!
- **Belang recurring lifecycle management!**
- Bevinding niet onderdrukken

- Mitigatie soms niet mogelijk door andere dependencies
- Geen upgrade mogelijkheid, dan andere mitigatie…



Uitdaging: Mitigatie Bevindingen Secrets

Kluis oplossingen nog niet overal ingeburgerd:

- Credentials, certificaten en API-keys horen niet in een broncode repository!
- Gebruik pre-commit hooks om lekken te voorkomen
- Geldt ook voor Infrastructure-as-Code/configuratie!
- Rotatie in geval van lekken secrets

- **<u>Maak gebruik van standaard platformoplossingen, probeer niet zelf secrets te managen</u>**

Uitdaging: Vloedgolf aan Bevindingen

Inzetten (SAST-) tooling leidt tot erg veel bevindingen:

- Doe het gefaseerd met heldere doelstellingen/plateaus
- Implementeer Quality Gates volgens groeipad
- Onderdruk false positives na analyse
- Stimuleer kennisdeling tussen teams

- Begin simpelweg met linters in IDE
- **Voorkom regressie door opnemen van abuse cases of security bevindingen in bestaande testautomatisering!**

Uitdaging: Waar is mijn Broncode?

Steeds meer systemen 'zonder' broncode:

- Low-Code systemen
- SAP systemen
- Afspraken met leverancier over secure development
- Altijd valideren met pentest ipv blind vertrouwen
- Awareness bij het team, bijvoorbeeld OWASP Low-Code/No-Code Top 10

- Meenemen in monitoring omgeving SOC / SIEM
- **Inzetten DAST tools**

Uitdaging: Wanneer is het goed?

Soms wil een team meer of minder doen:

- Geen one-size-fits-all
- Balans verleiding en compliance
- Ruimte voor innovatie, beter mag altiijd
- Bewaking van groeipad
- Threat model geeft richting

- Inzetten op maturiteitsmodel, bv OWASP SAMM
- **Stickers en badges**

Agenda

01 Introductie

02 DevSecOps bij NS

03 Faciliteren van Teams

04 Uitdagingen

05 Conclusie

Conclusie

Faciliteren vanuit platform

Teams kunnen zelf veel doen door gebruik te maken van (platform-) faciliteiten. Enige verleiding/lichte push is nodig om ze in beweging te zetten.

Support door onderkennen belang

De omgeving van het team (Product Owner, business) moet meegenomen worden in het belang van security. Bevindingen moeten niet als een molensteen om de nek van het team worden ervaren.

Baselines niet te rigide

Integrale aanpak van DevSecOps laat mogelijkheid open tot innovatie door de teams. Voldoen aan baseline betekent niet blind staren op quality gates omdat het moet.

Betrek de teams

Er is geen one-size-fits-all. Betrek de teams, bijvoorbeeld door hackathons, bij het selecteren van tools en werkwijze. Hun ervaring helpt in de verdere adoptie.

> **The best theory is inspired by practice.**
> **The best practice is inspired by theory.**

Donald Knuth, Selected Papers on Computer Science

Zijn er nog vragen?