Introduction to DevSecOps

Key Takeaways

techworld-with-nana.com

TECHWORLD WITH NANA

All rights reserved to nnSoftware GmbH

TECHWORLD WITH NANA

About TechWorld with Nana

TechWorld with Nana is an established name in the DevOps and Cloud industry, and it stands for the quality trainings helping 1,000s of engineers acquire the most in-demand skills in this field.

Our mission is enable individual engineers as well as companies to take advantage of the recent developments in Cloud and DevOps fields, to use technologies and concepts in order to create efficient, automated, streamlined DevSecOps processes in organisations.

Let's compare without and with DevSecOps approach

Security as an afterthought

The old way of doing security

"Shifting security left"

The new - DevSecOps - way of doing it

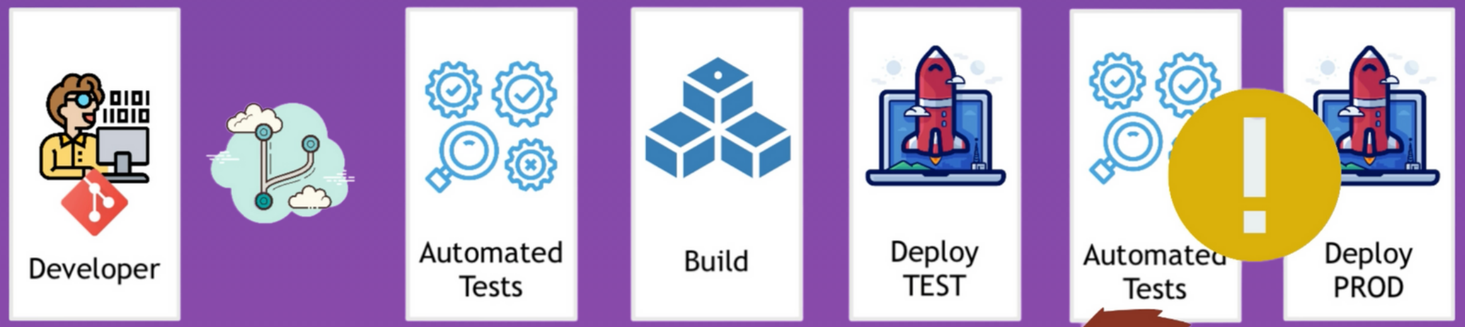
TECHWORLD WITH NANA

Issues with Traditional Approach to Security

Late Integration of Security - Blocking automated DevOps process

- Security is typically **considered late in the development process**. Often during pre-production phase

- So while DevOps enabled these automated, streamlined processes. Security checks and audits are still **blocking** the whole process **delaying the release for weeks**



TECHWORLD WITH NANA

Issues with Traditional Approach to Security

Siloed Teams - Lack of Collaboration

- While DevOps united Development and Operations, Security is often still a **separate team**
- This leads to communication gaps, delays in addressing security issues and a **lack of responsibility for security**

TECHWORLD WITH NANA

Issues with Traditional Approach to Security

Manual Processes, No automations

- Traditional security practices often rely on **manual security assessments** and reviews, which can be slow and error-prone
- Manual processes are **not well-suited to the fast-paced, automated nature of DevOps**

Slow Feedback Loop

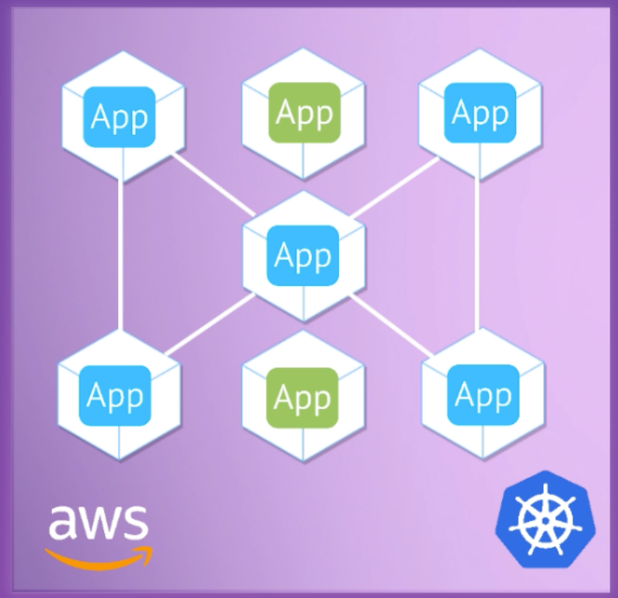
- **Delayed security feedback** can make it more challenging to fix the security issue
- The longer it takes to identify and remediate vulnerabilities, the **greater the potential impact and the higher the costs**

TECHWORLD WITH NANA

More attack surfaces

In addition to all of these, security has become more complex

- Microservices
- Containers
- Cloud platform
- Kubernetes



Security tools were also developed before these new developments

TECHWORLD WITH NANA

To address these issues, organizations are adopting DevSecOps

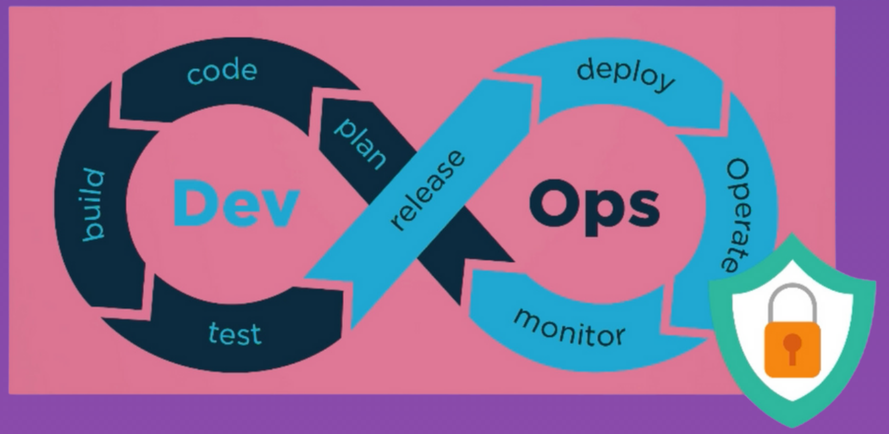
So, how does DevSecOps solve these problems?

DevSecOps Approach

- Integrating Security into DevOps
- Shifting Security to the Left

Dev **Sec** **Ops**

Developer | Security | Operations

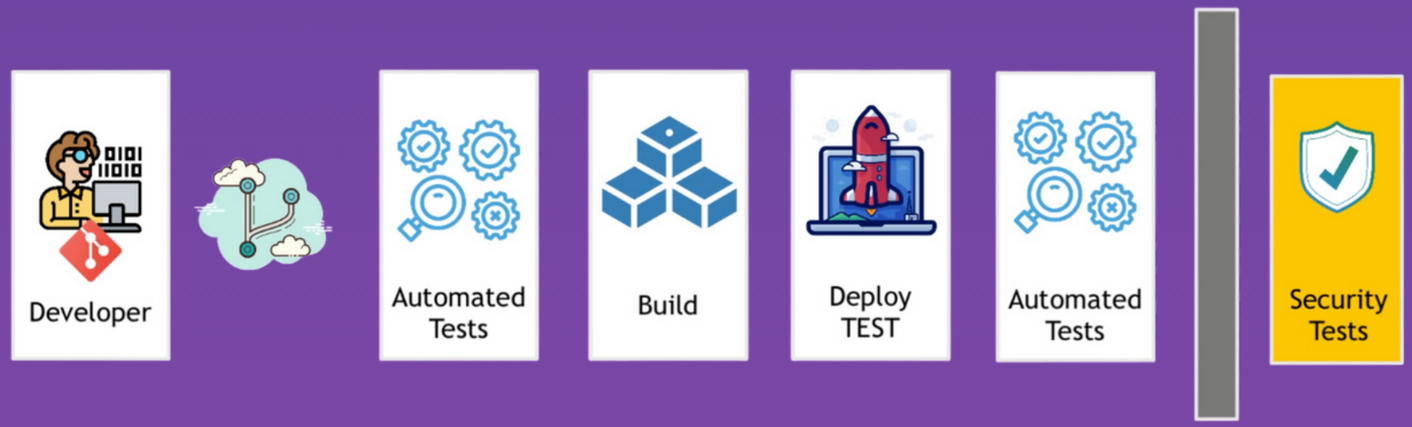


TECHWORLD WITH NANA

What is DevSecOps

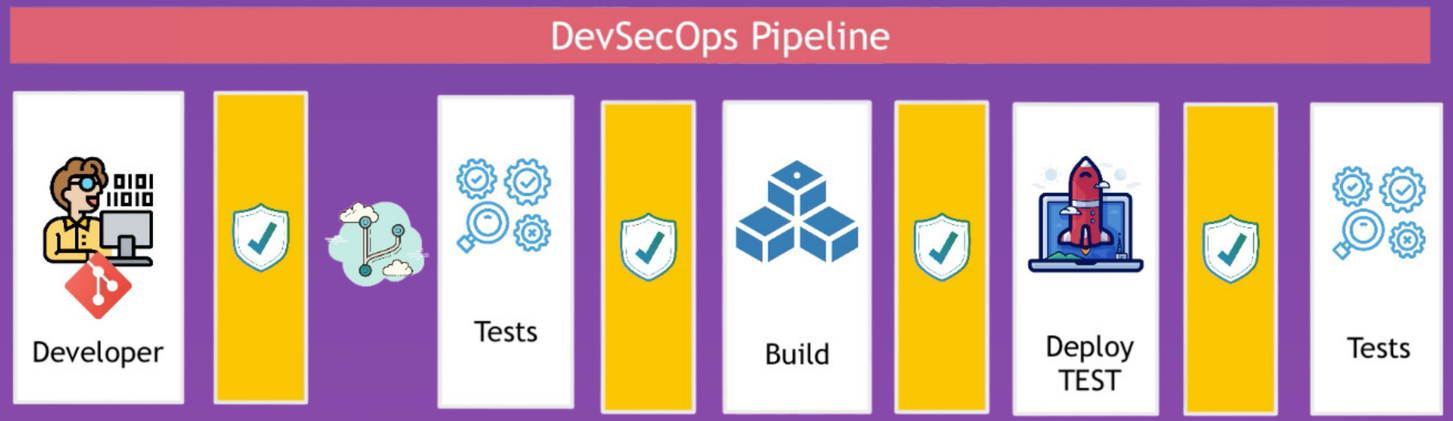
No DevSecOps

Thinking about security **after** a new feature is developed and tested, right before releasing it:



DevSecOps

Start thinking about security right at the beginning and **solve it right away as soon as security issues appear**:



TECHWORLD WITH NANA

What is DevSecOps

DevSecOps encourages

- automation
- collaboration
- and a proactive approach to security
- helping organizations identify and remediate security issues earlier in the development lifecycle

This approach improves security posture while also maintaining the speed and agility of DevOps practices

TECHWORLD WITH NANA

What is DevSecOps

Shared Responsibility and Collaboration

- Security becomes a **developer responsibility too**, instead of just being a responsibility of dedicated security professionals

- **Security team becomes a facilitator** and advisor for DEV and OPS teams

- Security team **trains engineers** on how to interpret the output of security tools, so they can identify and fix the issues themselves

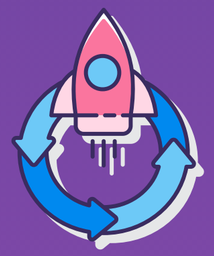
TECHWORLD WITH NANA

What is DevSecOps

Automation

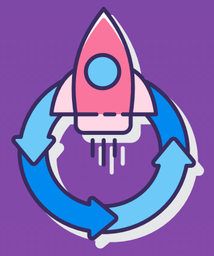
- Automation **security tools are integrated in the CI/CD pipeline** to detect security issues on every Git push
- Developers get **automated output of the application's security status** and what vulnerabilities need to be fixed

Faster Release Cycles and Shorter Feedback Cycles



No security issues?

Pipeline will deploy the application



Security issues found?

- Bugs are easier to fix the earlier they are found in the development lifecycle
- Which means less time and costs

TECHWORLD WITH NANA

How DevSecOps works in practice

Tools for Automated Security Tests

How DevSecOps works in practice

Automated tests in Software Development

Just like we have automated unit tests, integration tests to test new features, application functionality and integration with other services etc....

...In the same way, we add **automated tests for the different aspects of our application and systems' security**:

- Automated tests for application security
- Automated tests for infrastructure and cloud security
- Automated tests for platform security

Automated tests for Security

TECHWORLD WITH NANA

Different Types of Automated Tests

Automated tests in Software Development

Just like we have different types of automated tests in software development...

...In the same way, we have different types of security tests

Automated tests for Security

TECHWORLD WITH NANA

Types of Security Tests

SAST

Static Application Security Testing

- Static code analysis (app is not running)
- Identifies security vulnerabilities in app's source code, configuration files etc.
- Looks for common coding errors, deviations from secure coding practices etc.

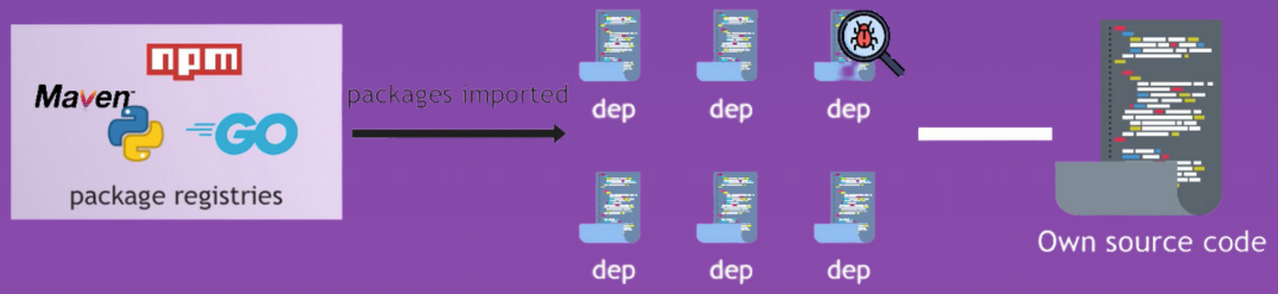
TECHWORLD WITH NANA

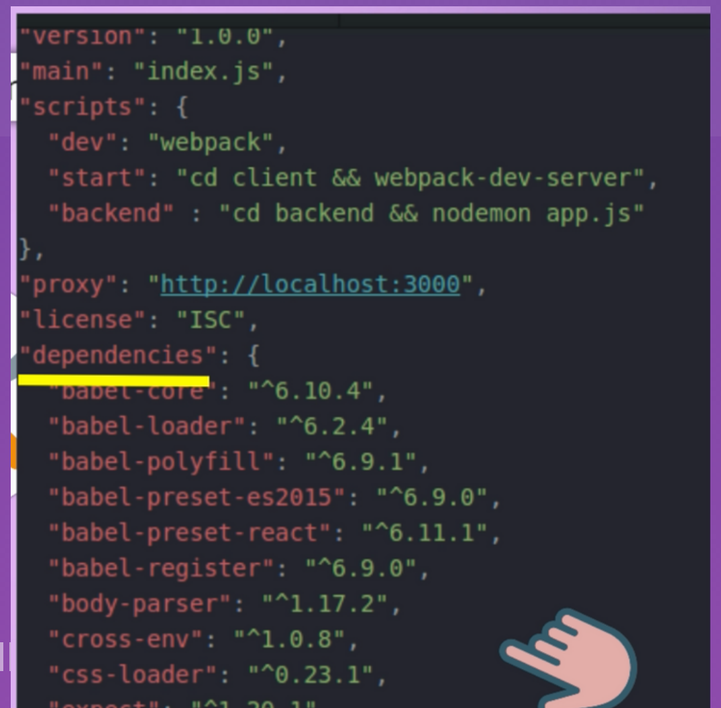
Types of Security Tests

SCA

Software Composition Analysis

- Check third-party and open-source libraries and frameworks
- SCA tool goes through the **dependencies of your application** and checks whether any known vulnerabilities for that dependency and the specific version you use
- It's also static code analysis





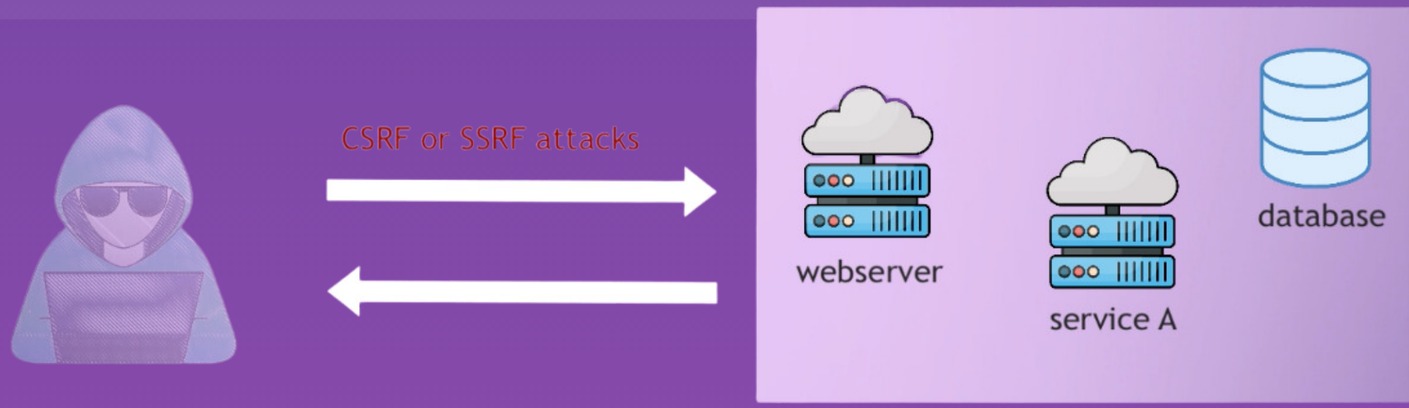
TECHWORLD WITH NANA

Types of Security Tests

DAST

Dynamic Application Security Testing

- Testing the app's running instance or deployed version
- Simulating security attacks and analyzing behavior and responses in real-time
- Does not require access to the code



TECHWORLD WITH NANA

White Box vs Black Box Testing

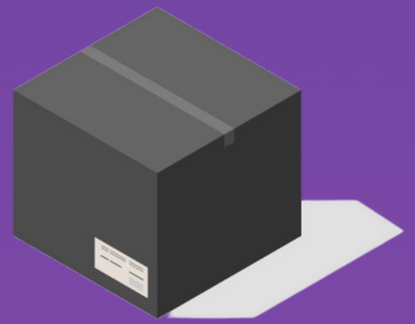
White Box Testing

SAST Tools belong to this category

- **Knowledge:** Tester has detailed knowledge of the internal workings, code and architecture.
- **Focus:** Examining the internal logic, code paths and data flows within the application.
- **Advantages**: Can provide precise information about the security flaws. Also helpful for addressing issues related to code quality and design flaws.
- **Limitations**: Does not capture vulnerabilities that only surface when interacting with the application.

TECHWORLD WITH NANA

White Box vs Black Box Testing



Black Box Testing

DAST Tools belong to this category

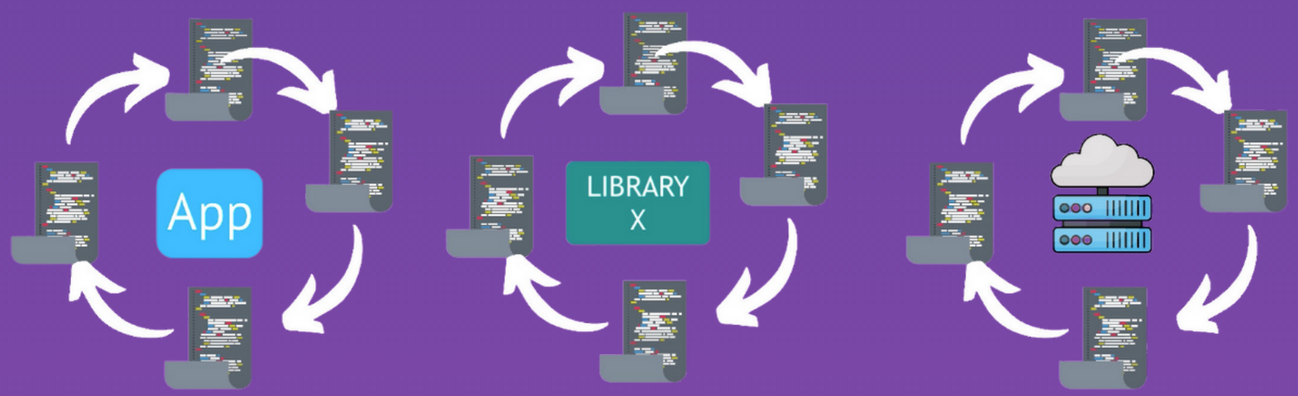
- **Knowledge:** No access to the source code and relies solely on the system's inputs and outputs.
- **Focus:** Focuses on evaluating the system's functionality, its external behavior, and how it responds to various inputs and scenarios.
- **Advantages**: Simulates real-world attacks and provides a more user-centric perspective on security. Testers do not need to be familiar with the application's codebase.
- **Limitations**: May not uncover all security vulnerabilities that can be identified through code-level inspection, and it may miss some complex or logic-based vulnerabilities.

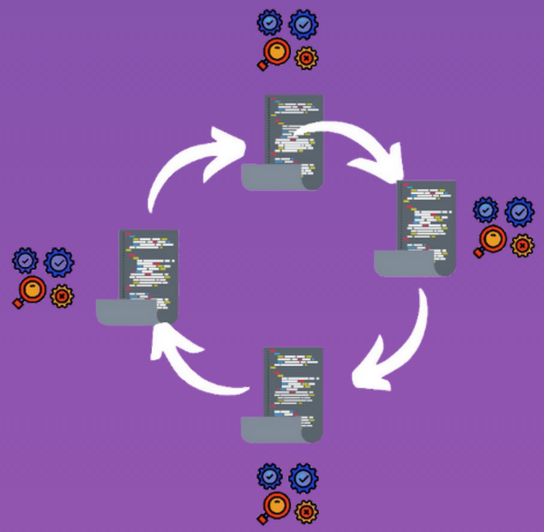
TECHWORLD WITH NANA

Continuous Testing necessary

Code changes constantly

- Scanning code once is not enough
- **Applications are developed continuously**, libraries are developed continuously and new versions are released. Infrastructure changes.





Applications are developed continuously

Continuous testing and fixing

Continuously test and fix

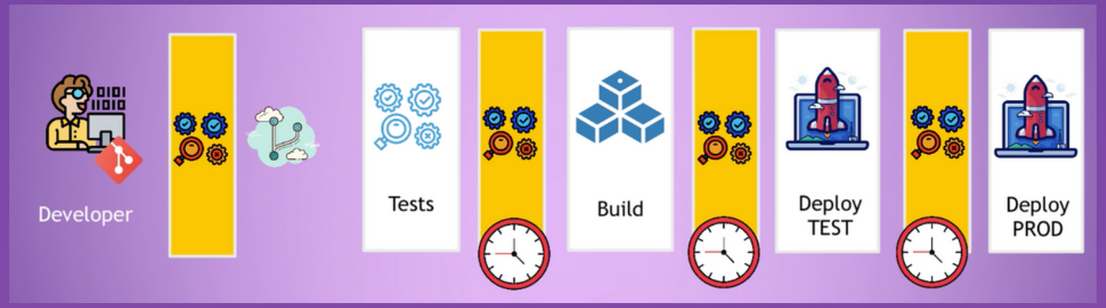
- So we need to continuously test and fix security vulnerabilities in the software development lifecycle

TECHWORLD WITH NANA

When to run which security scans

Pipeline becomes a bottleneck

- Security scans and tests can slow down the CI/CD pipeline



Approaches to solve this

Pipeline for basic security tests

- Runs on every commit
- Security checks only for **affected code** parts
- Run 3rd-party library checks when dependencies changed

Pipeline for comprehensive and complete tests

- Runs once per night
- Nobody's work is interrupted

TECHWORLD WITH NANA

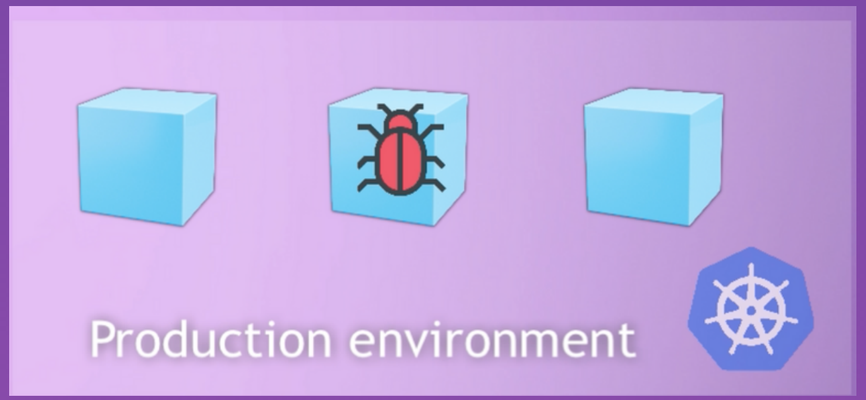
Logging and Monitoring

- There is always a chance that security issues slip into production environment
- Or that 3rd-party vulnerabilities appear after production deployment

That's why we need proper continuous logging, monitoring and alerting in place, that:

Continuously monitors the systems

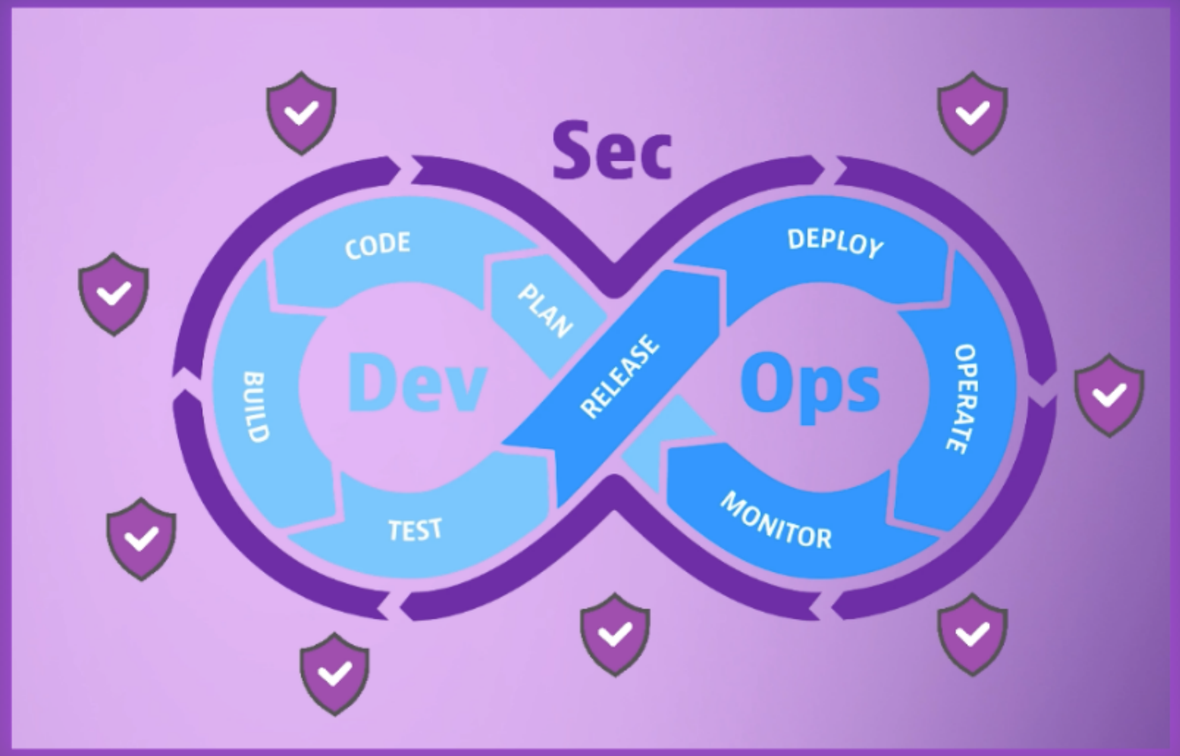
Alerts the team when security threats are detected or suspicious behavior is detected



TECHWORLD WITH NANA

Benefits of DevSecOps

Integrating security across the whole software development lifecycle can be challenging, but has many benefits



- More **efficient**
- **Saves costs**, as security fixes are more expensive the later they are discovered
- **Avoiding security breaches**, which eventually would mean losing customers' trust

TECHWORLD WITH NANA

DevSecOps Engineer

Role and Skills

Shared Responsibility

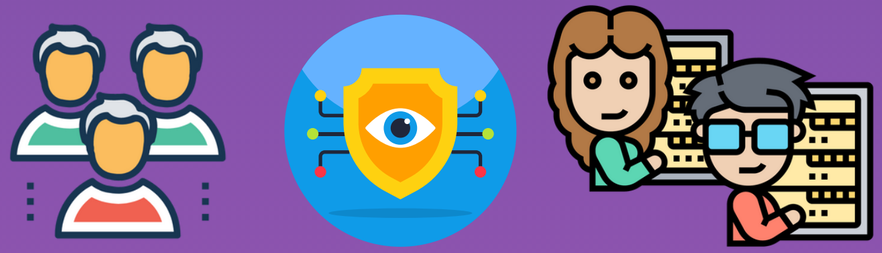
Architect of DevSecOps processes

- The idea of DevOps and DevSecOps is to **distribute responsibility** for security across teams
- DevSecOps professional **helps team integrate these automated checks into the pipeline**. They work to embed security practices and controls by collaborating with Dev and Ops teams

TECHWORLD WITH NANA

Shared Responsibility

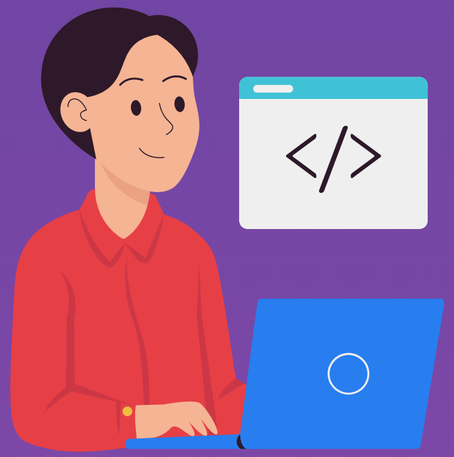
- **Visibility**: Setting up processes that shows the teams what current security posture is
- Help them understand the security findings and fix these issues
- **Build security know-how** step by step with the help of these tools



- **Educate and raise awareness** among teams about security best practices

TECHWORLD WITH NANA

Shared Responsibility



- This promotes a **security-first mindset** within the team
- By getting constant and immediate feedback, engineers will learn how to **write secure code**

TECHWORLD WITH NANA

Working with Security Engineers

- **Security experts** with specialized expertise in the field of cybersecurity
- Well-versed in regulatory requirements and compliance frameworks

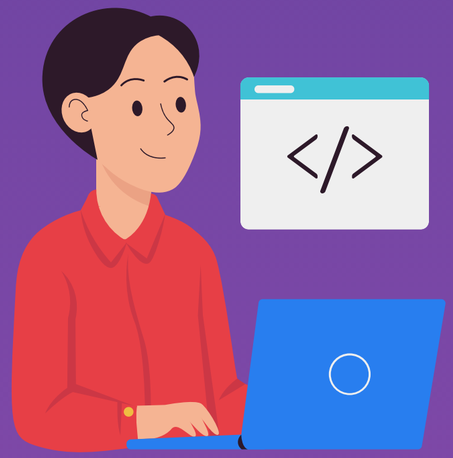
- DevSecOps engineers **work closely** with security engineers
- They can **tap into their deep understanding** of security principles to implement effective security measures

TECHWORLD WITH NANA

Working with Security Engineers

- Experts in **code security**

Intermediary between different teams

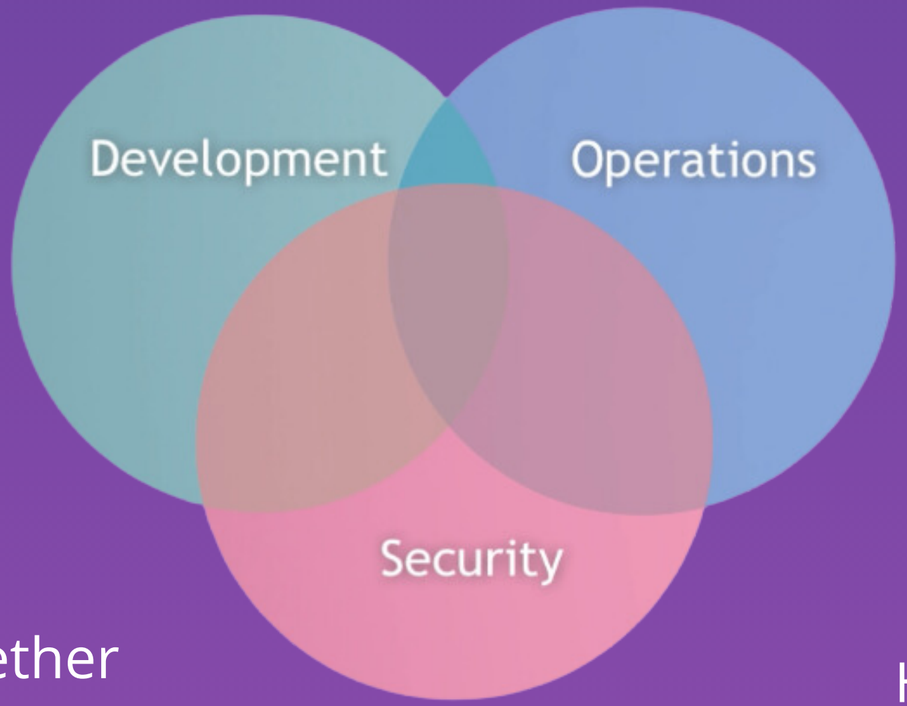


- Experts in **coding**

TECHWORLD WITH NANA

DevSecOps is all about collaboration

Different roles working together towards the **same goal**



Having a **security-conscious culture** within the organization

TECHWORLD WITH NANA

Summary of Tasks and Responsibilities

- **Architect** of DevSecOps processes

- **Facilitates** the integration of security testing into the development and deployment process

- **Provide guidance** on security coding standards, perform code reviews etc.

- **Establish mechanisms** for continuous security monitoring, threat detection and vulnerability scanning

TECHWORLD WITH NANA

DevSecOps Engineer vs Security Engineer

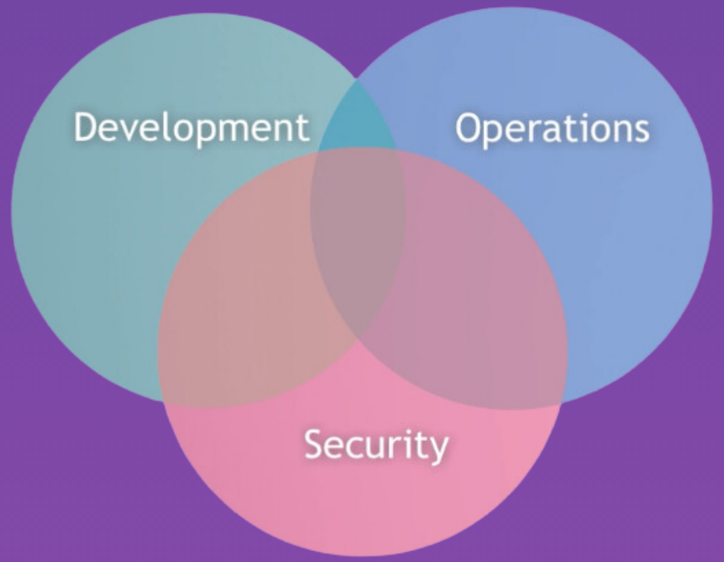
- Security Engineer **focuses on securing** systems, networks and infrastructure

- **Broader approach** by integrating security into entire DevOps process
- **Bridging the gap** between Dev, Ops and Security teams
- Help automate security checks
- Help Devs and Security Engineers to discover, visualize and fix efficiently

TECHWORLD WITH NANA

Skills of a DevSecOps Engineer

Combination of skills in software development, operations & security



- **Bridge** between DEV, OPS and SECURITY
- Create the processes and demonstrate what needs to be done
- **Train** people in different aspects of security
- Facilitate knowledge sharing

Strong collaboration, communication & leadership skills are essential

So it's not just about learning the tools to implement the DevSecOps processes, but about working with people

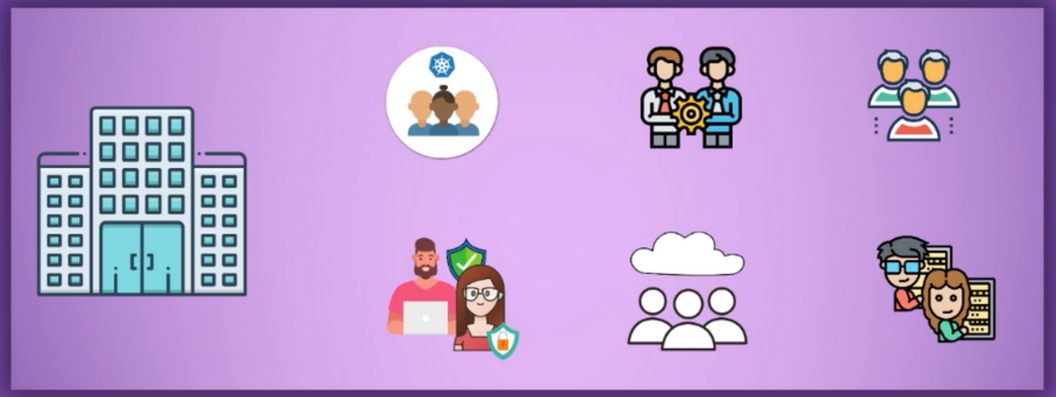
TECHWORLD WITH NANA

DevSecOps Concept vs Role

DevSecOps as a Concept

DevSecOps is a concept or philosophy

- It’s a way of working together
- It ‘s about shared responsibility and shifting security left
- Catch security issues early and develop more secure applications



In Theory:
Implementation without DevSecOps Engineer role

- Many roles working together to integrate security
- Divide and share responsibilities
- No dedicated DevSecOps engineer that orchestrates everything, teams should pro-actively collaborate

TECHWORLD WITH NANA

DevSecOps as a Role

In Reality:

- **Everybody is busy with their daily tasks** and responsibilities
- Engineers don’t have time to think about DevSecOps
- Concepts are not yet ingrained into every single engineer, so that they pro-actively build DevSecOps processes

Need for a dedicated person

- Often someone is needed in the company that actually make things happen
- **Someone whose main focus and task is to set up processes** and making sure teams work together, share knowledge and responsibility

TECHWORLD WITH NANA

Varies between organizations

Specific roles and responsibilities associated with implementing DevSecOps vary between organizations

- Self-driven and efficient teams that can work together,
- No need for a separate DevSecOps engineer

- In most cases: no efficient, self-directed teams
- So having a separate DevOps and/or DevSecOps engineer is essential for the company

TECHWORLD WITH NANA