DevSecOps

조민재
minjae.cho@gmail.com

오늘의 이야기

DevSecOps

We all love DevOps!

... but why?

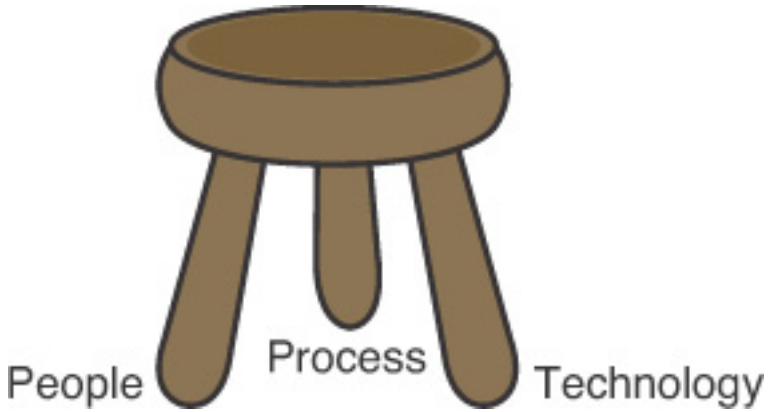
DevOps Helps
deliver value and
adopt to market needs
faster and scale

그러면.....

“Doing DevOps”

무엇일까요?

1. DevOps Technologies
2. DevOps Methodologies
3. DevOps Shared Ownership



그러면.....

“DevSecOps”

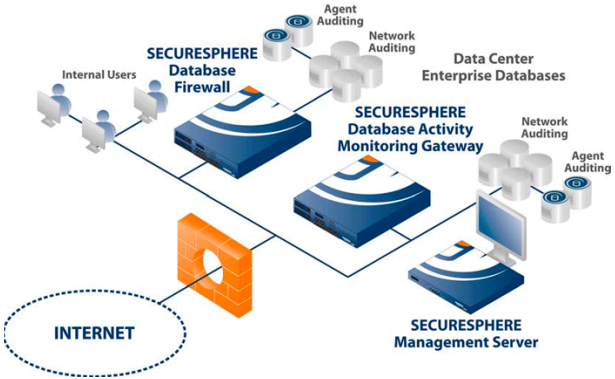
무엇일까요?

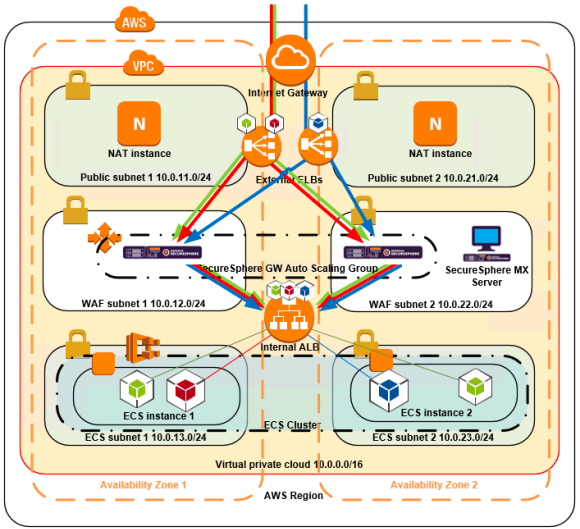
1. Securing DevOps Technologies
2. Security in DevOps Methodologies
3. Include Security
   in DevOps Shared Ownership

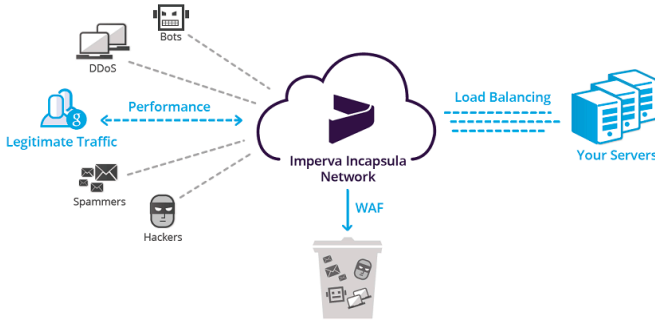
1. Securing DevOps Technologies

Security For DevOps Technologies

- 보안도구들을 새 기술에 맞도록 적용한다.
  - 기존 보안 솔루션들은 새로운 환경에서는 적합하지 않을 수 있다.







Security For DevOps Technologies

- 보안도구들을 새 기술에 맞도록 적용한다.
  - 새 환경은 보안에 대한 또다른 생각을 만들어낸다.

문제있는 컨테이너 인스턴스에 패치를 하라고?

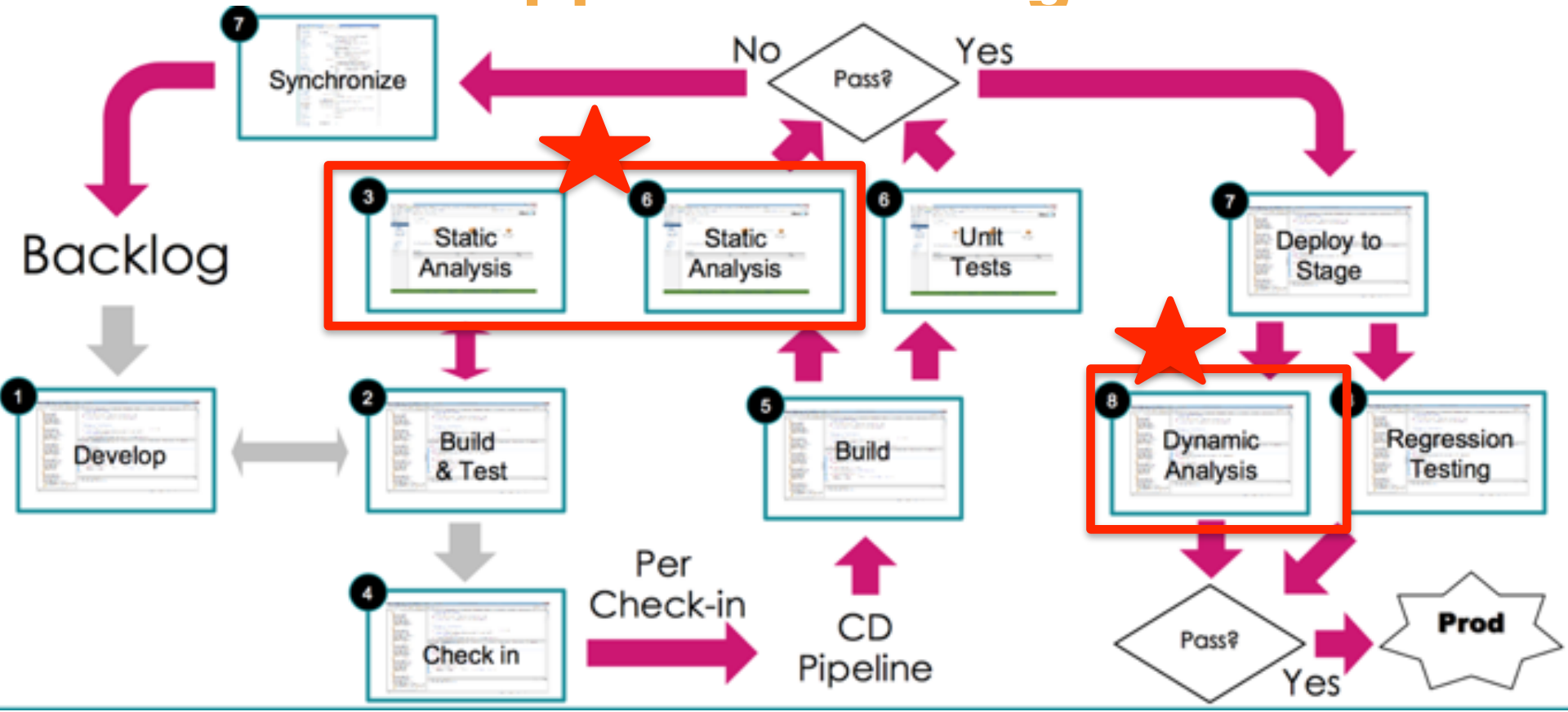
조금 있다가 그거 버릴건데….

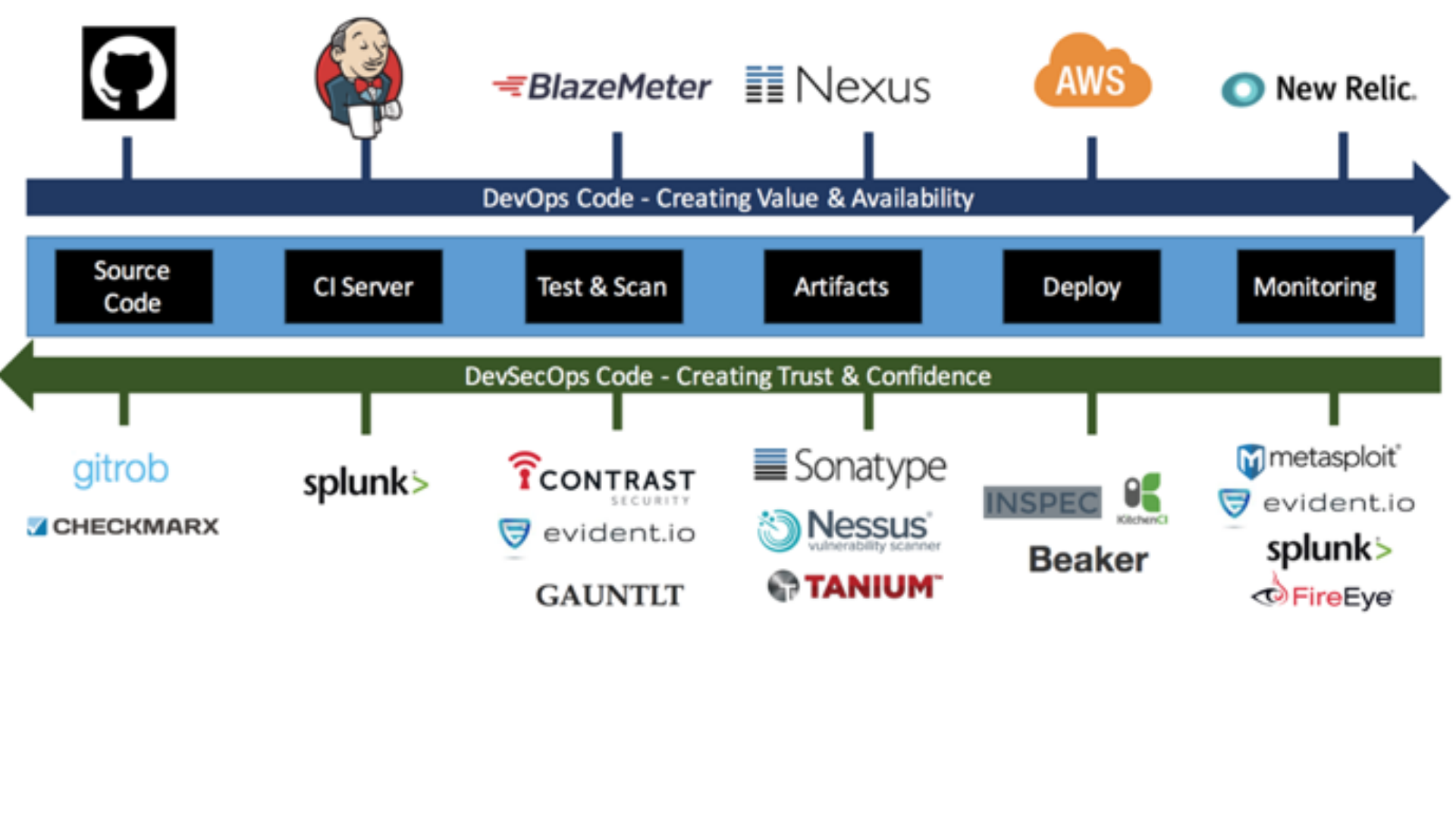
=> dockerfile scanner

2. Security in DevOps

Methodologies

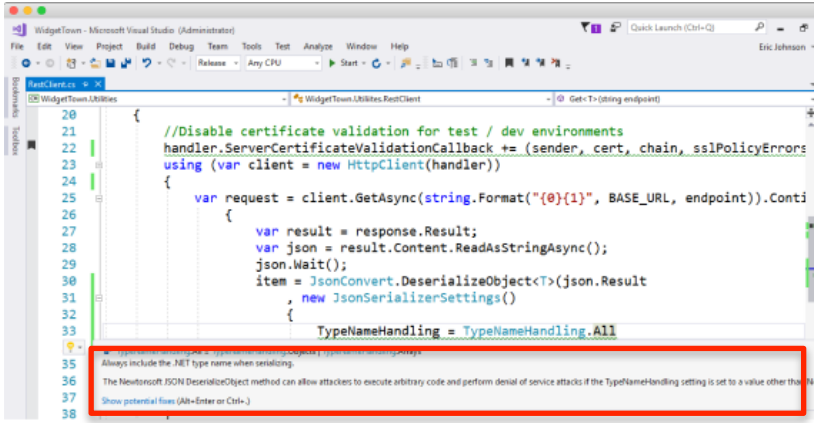
Automated App Sec Testing!




BlazeMeter
Nexus
AWS
New Relic
DevOps Code - Creating Value & Availability
Source Code
CI Server
Test & Scan
Artifacts
Deploy
Monitoring
DevSecOps Code - Creating Trust & Confidence
gitrob
CHECKMARX
splunk>
CONTRAST SECURITY
evident.io
GAUNTLT
Sonatype
Nessus vulnerability scanner
TANIUM
INSPEC
KitchenCI
Beaker
metasploit
evident.io
splunk>
FireEye

Security For DevOps Methodologies

- 정적분석도구
  - IDE Security Plugins
    - **FindSecurityBugs plugin : Eclipse, IntelliJ**
    - **Puma Scan plugin : Visual Studio**
    - **Microsoft DevSkim : VSCode, Sublime, Visual Studio**
    - **SonarLint : Visual Studio, IntelliJ, Eclipse, VSCode, Atom**



Security For DevOps Methodologies

- 정적분석도구
  - pre-commit hook
    - AWS Labs git-secrets (https://github.com/awslabs/git-secrets)
    - Talisman (https://github.com/thoughtworks/talisman)
    - Auth0 repo-supervisor (https://github.com/auth0/repo-supervisor)

```
$ git commit -m "testing git-secrets"

Web/Licensing/appsettings.json:5:
    "AccessKey": "AKIAJNQ7C2FCRR6B4VWA",
Web/Licensing/appsettings.json:6:
    "SecretKey": "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"

[ERROR] Matched one or more prohibited patterns
```

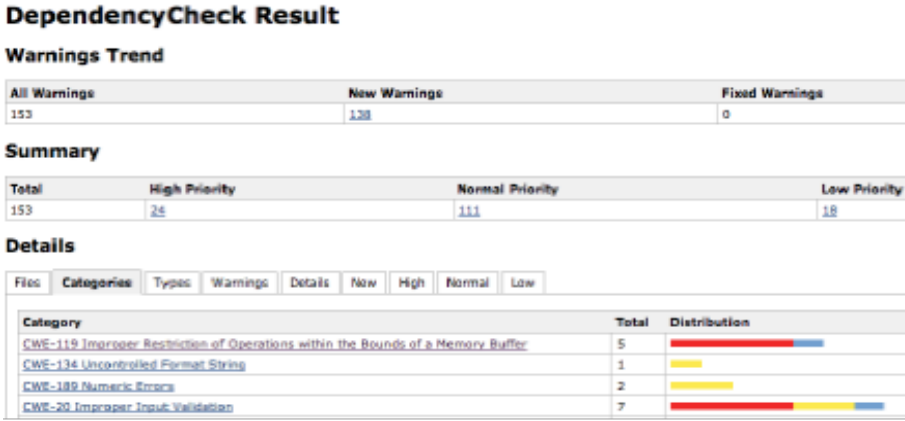
Security For DevOps Methodologies

- 정적분석도구
  - CI 결합

- FindSecurityBugs : Java(Spring, Struts)
  - http://find-sec-bugs.github.io
- Phan : PHP (with composer)
  - http://github.com/etsy/phan
- NodeJsScan : Node.js
  - https://github.com/ajinabraham/NodeJsScan
- Brakeman : Ruby
  - https://brakemanscanner.org/
- Bandit : Python
  - https://github.com/PyCQA/bandit/
- Flawfinder : C/C++
  - https://dwheeler.com/flawfinder/
- Puma Scan : C#
  - https://github.com/pumasecurity/puma-scan
- Gosec : Golang
  - https://github.com/securego/gosec/

Security For DevOps Methodologies

- 정적분석도구
  - Dependency Check
    - OWASP Dependency Check : Java, .NET, Ruby, Python, Node.js
      - https://www.owasp.org/index.php/OWASP_Dependency_Check
    - PHP Security Checker : PHP
      - http://github.com/etsy/phan
    - Bundler-Audit : Ruby
      - https://github.com/rubysec/bundler-audit
    - NPM Audit / Retire.JS : Node.js
      - https://docs.npmjs.com/cli/audit
      - https://retirejs.github.io/retire.js/



DependencyCheck Result

Warnings Trend

All Warnings	New Warnings	Fixed Warnings
153	138	0

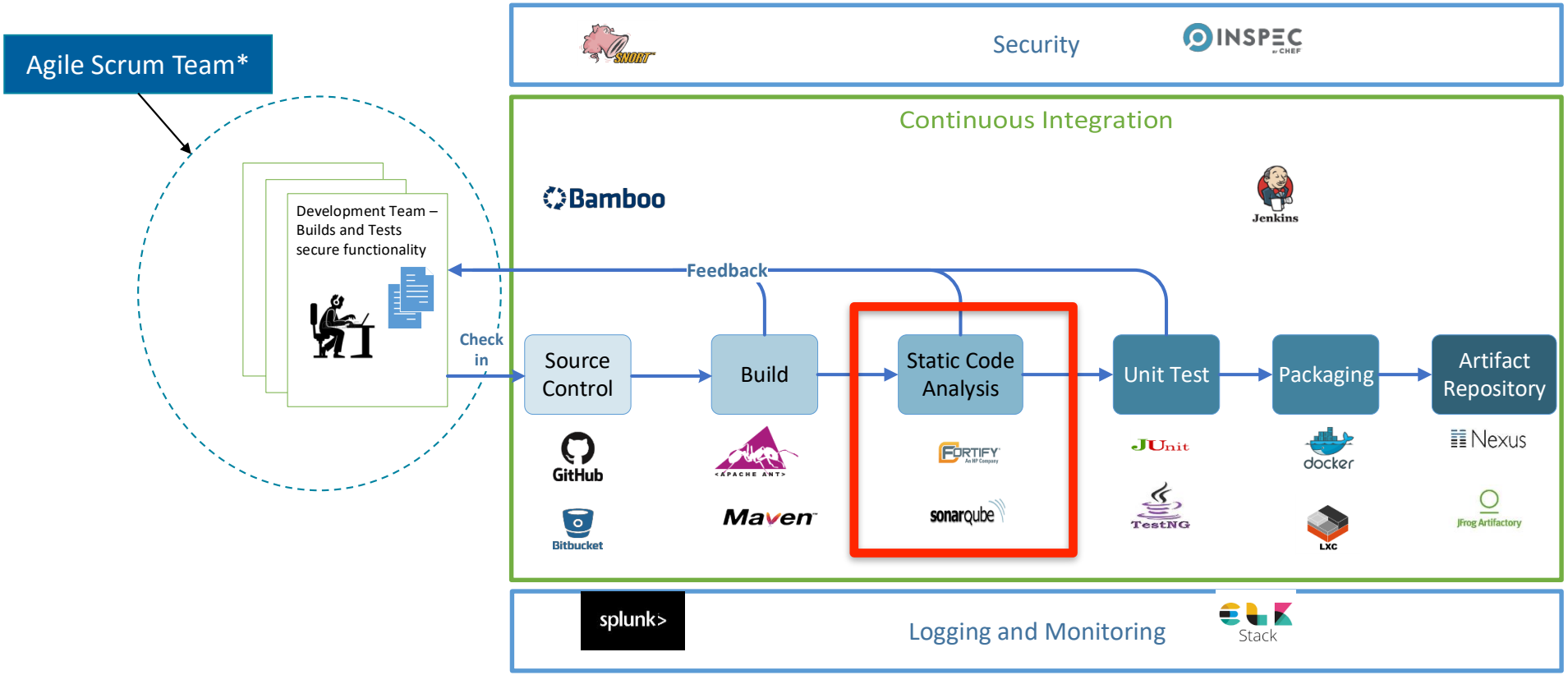
Summary

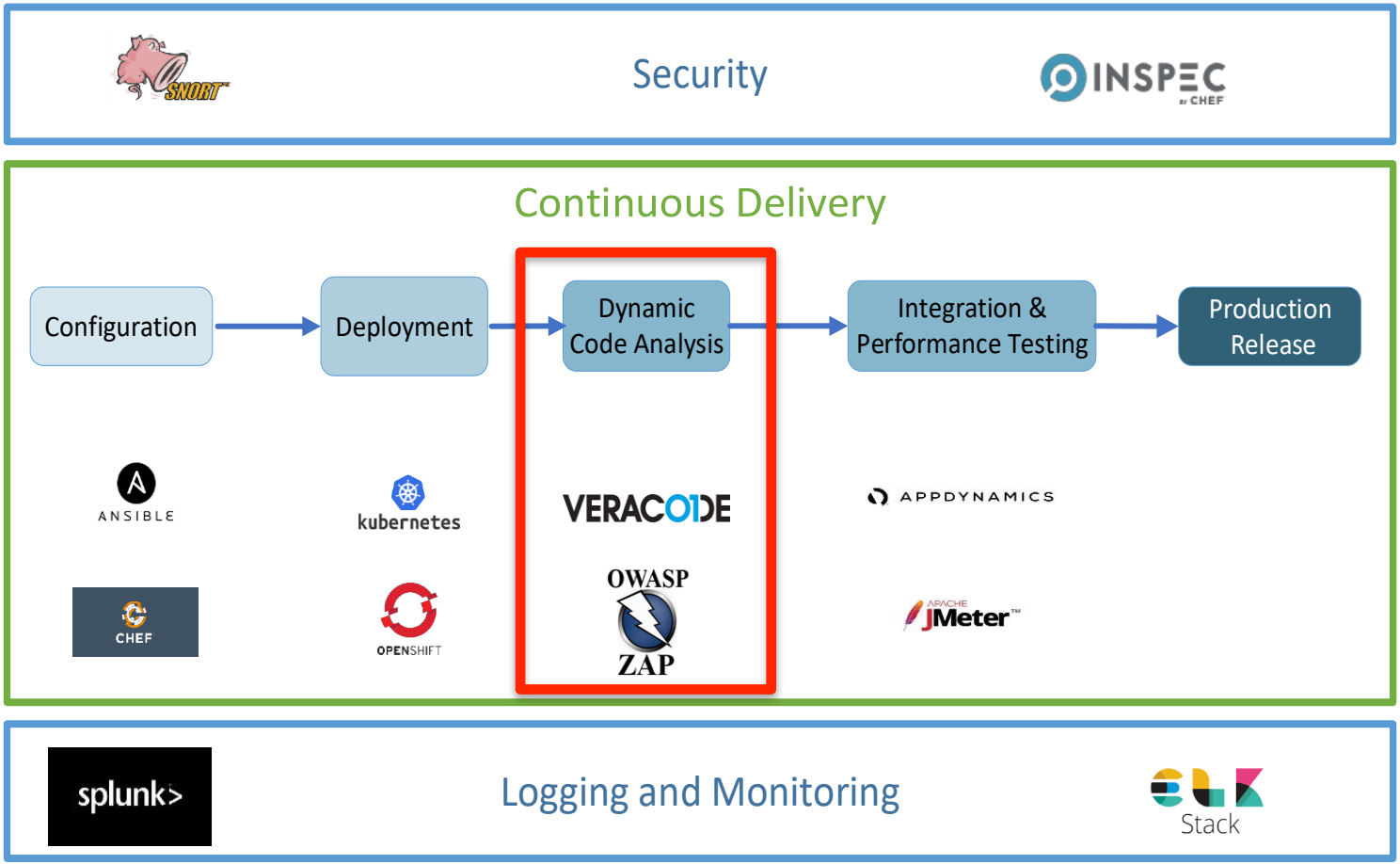
Total	High Priority	Normal Priority	Low Priority
153	24	111	18

Details

Files | Categories | Types | Warnings | Details | New | High | Normal | Low

Category	Total	Distribution
CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer	5	
CWE-134 Uncontrolled Format String	1	
CWE-189 Numeric Errors	2	
CWE-20 Improper Input Validation	7	


Agile Scrum Team*
Development Team – Builds and Tests secure functionality
Check in
Security
Continuous Integration
Bamboo
Jenkins
Feedback
Source Control
Build
Static Code Analysis
Unit Test
Packaging
Artifact Repository
GitHub
Bitbucket
Maven
FORTIFY
sonarqube
JUnit
TestNG
docker
LXC
Nexus
JFrog Artifactory
splunk>
Logging and Monitoring
ELK Stack

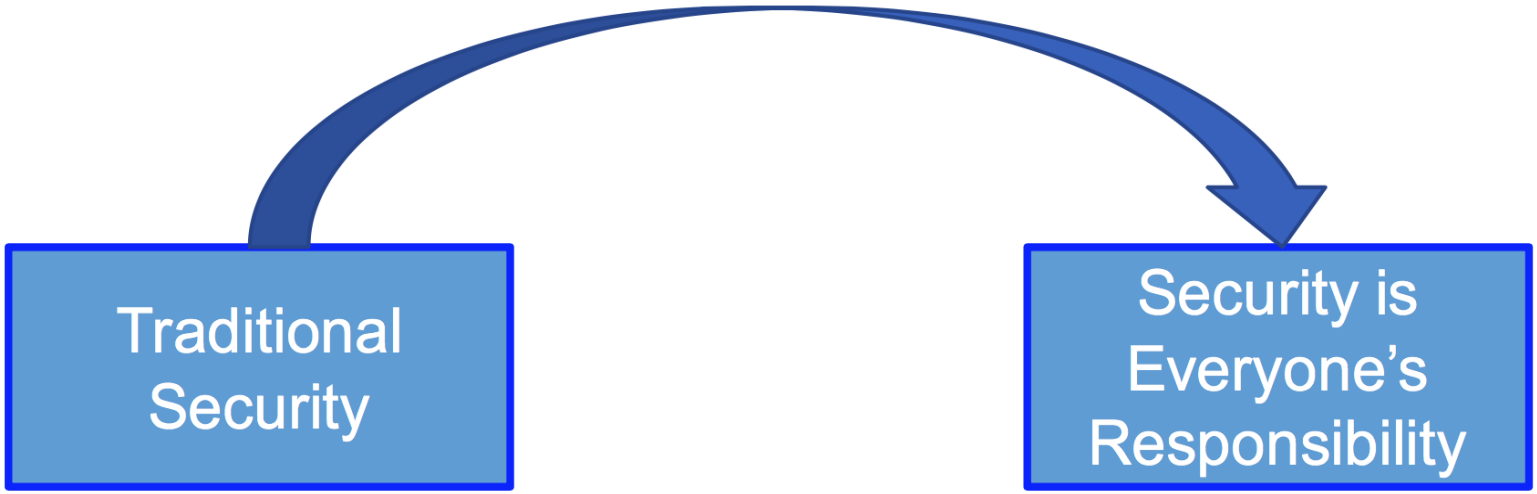

Security
Continuous Delivery
Configuration
Deployment
Dynamic Code Analysis
Integration & Performance Testing
Production Release
ANSIBLE
kubernetes
VERACODE
APPDYNAMICS
CHEF
OPENSHIFT
OWASP ZAP
JMeter
splunk>
Logging and Monitoring
Stack

3. Include Security in DevOps Shared Ownership

문화적 충돌

DevOps Culture	Traditional Security Culture
Team-based decision making	Top-down risk management
Extended information sharing	Need-to-know restrictions
Fail fast and Fix forward	Zero failure
Limiting Changes	Ready to say “No!”
Dev + Ops	Separation of Duties

Culture Hacking



DEVSECOPS

1. Securing DevOps Technologies
2. Security in DevOps Methodologies
3. Include Security
   in DevOps Shared Ownership

DevSecOps!

조민재
(minjae.cho@gmail.com)