NOVATEC

Vulnerabilities in Continuous Delivery Pipelines? A Case Study

Christina Paule

Continuous Lifecycle
Mannheim, 14. November 2019

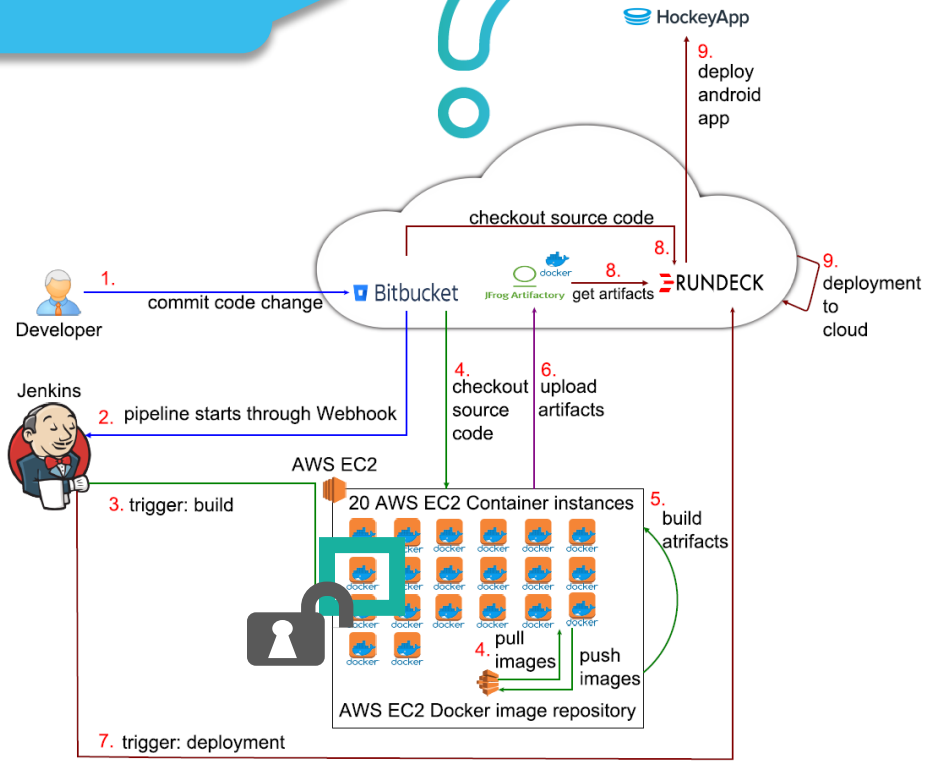
Critical vulnerability in Docker and Kubernetes allows code execution on host systems (CVE-2019-5736)

ZetNet Feb. 2019 [1]

… increase development speed

… increase frequency of product increments

… decrease time to market

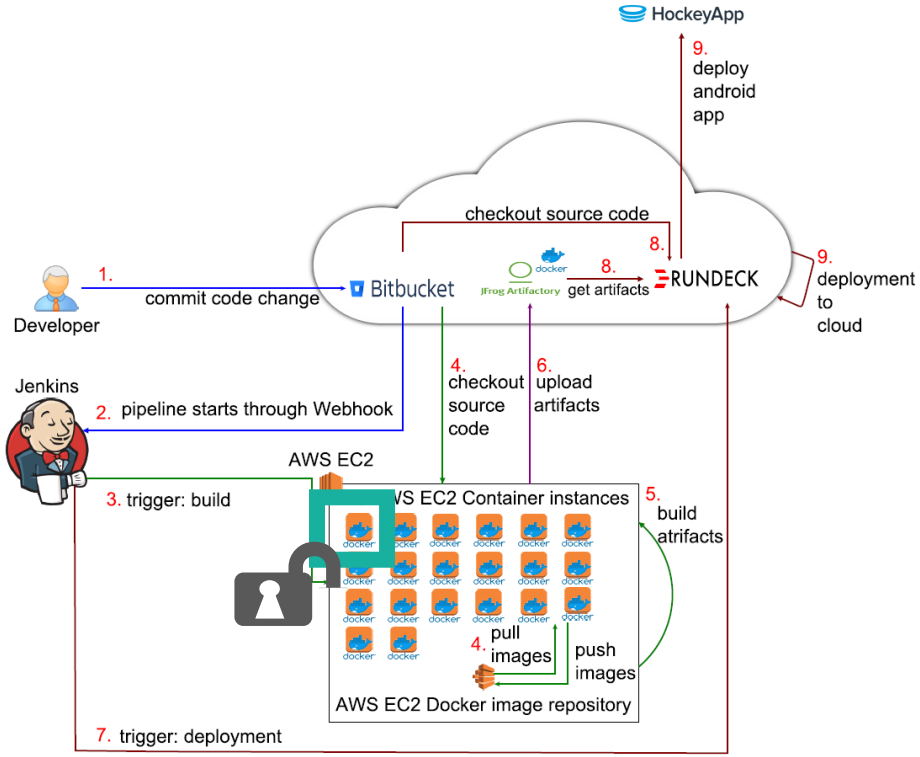


… loss of developer hours

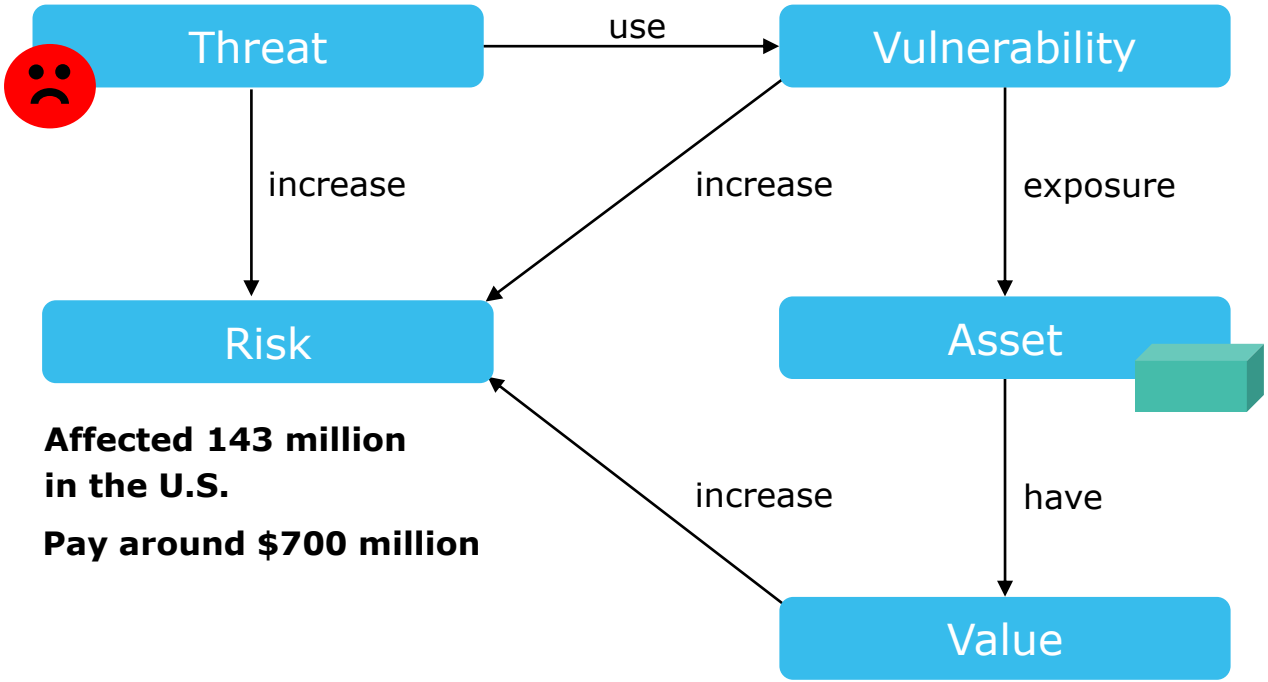
… damage to image of company

… loss of customer trust

Which vulnerabilities are present in CD pipelines & how can they be detected?



Terms



Open-Source-Framework Apache Struts

EQUIFAX

2017

Personal information, social security number, ...

Based on K.-J. Farn, S.-K. Lin, A. R.-W. Fung. “A study on information security management system evaluation—assets, threat and vulnerability.” In: *Computer Standards & Interfaces* 26.6 (2004), pp. 501–513

1

Setup

2

Survey

3

Analysis

4

Case Study

5

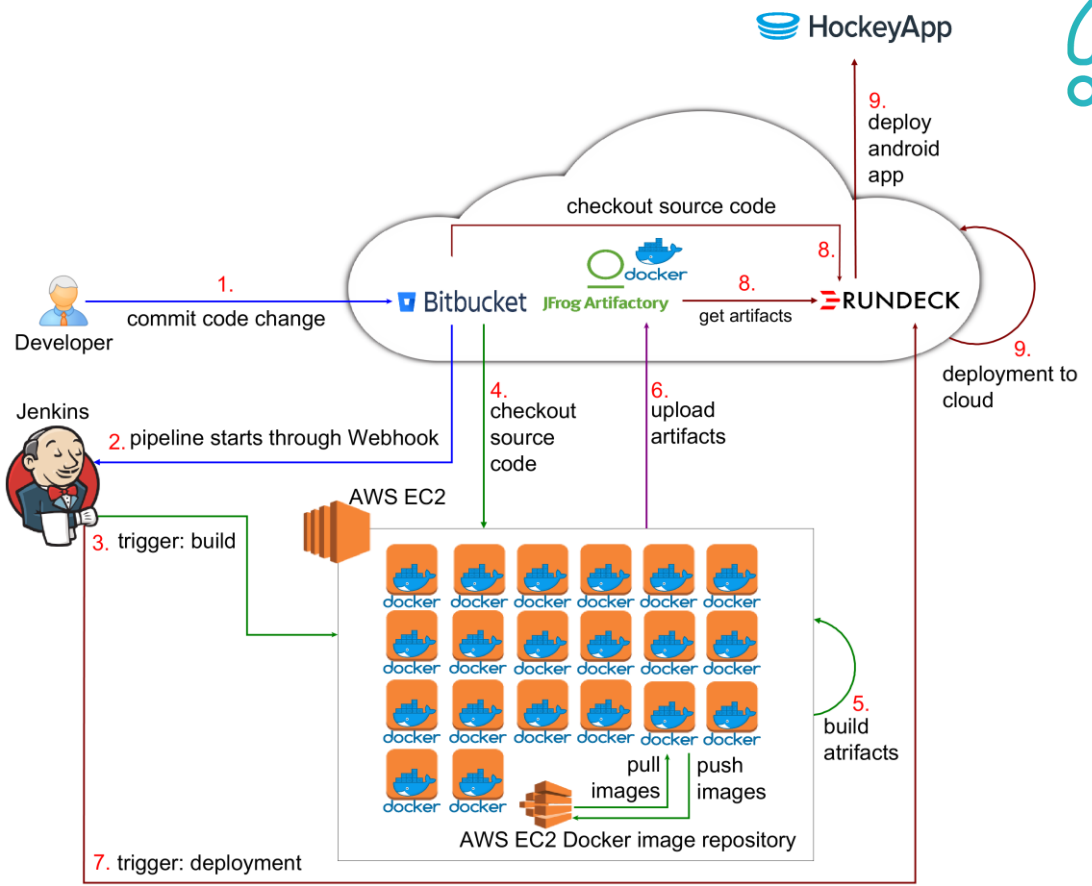
Lessons Learned

6

Conclusion

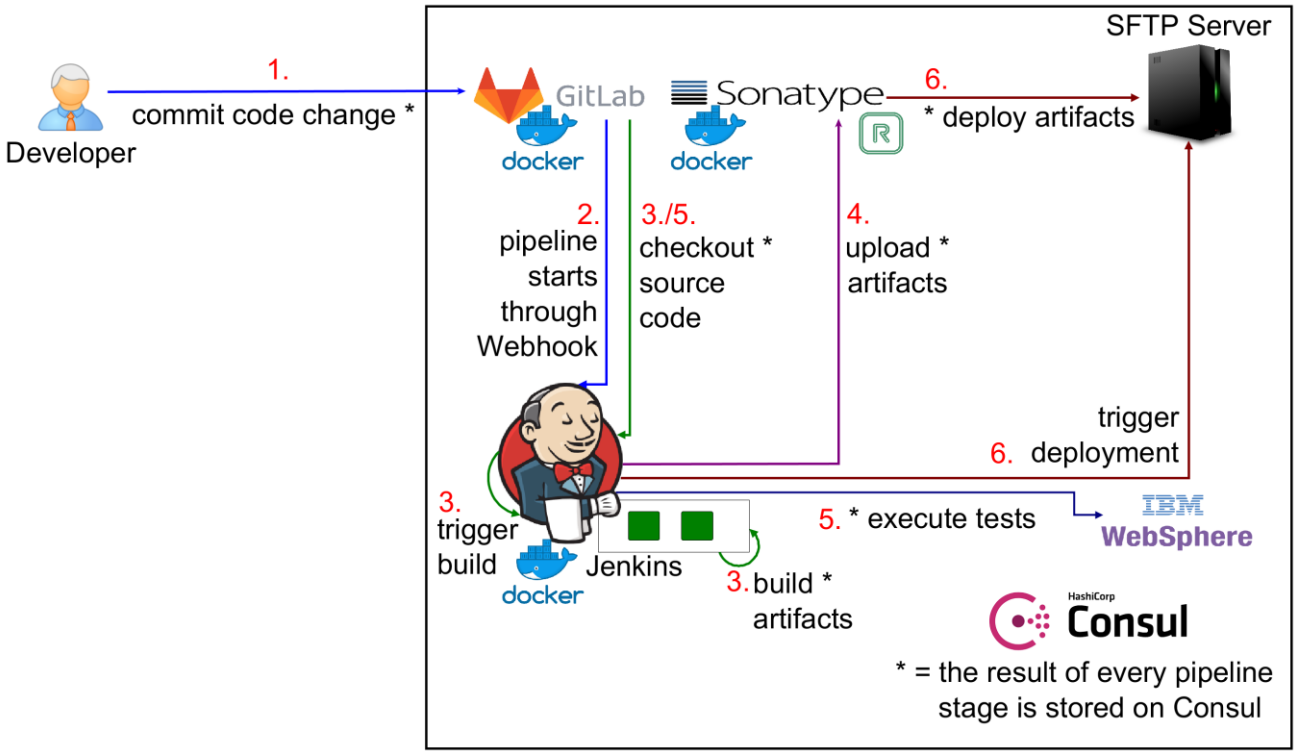
Setup

Pipeline A



Setup

Pipeline B



Survey

- **Setup:**
  - Online-survey
  - 19 participants

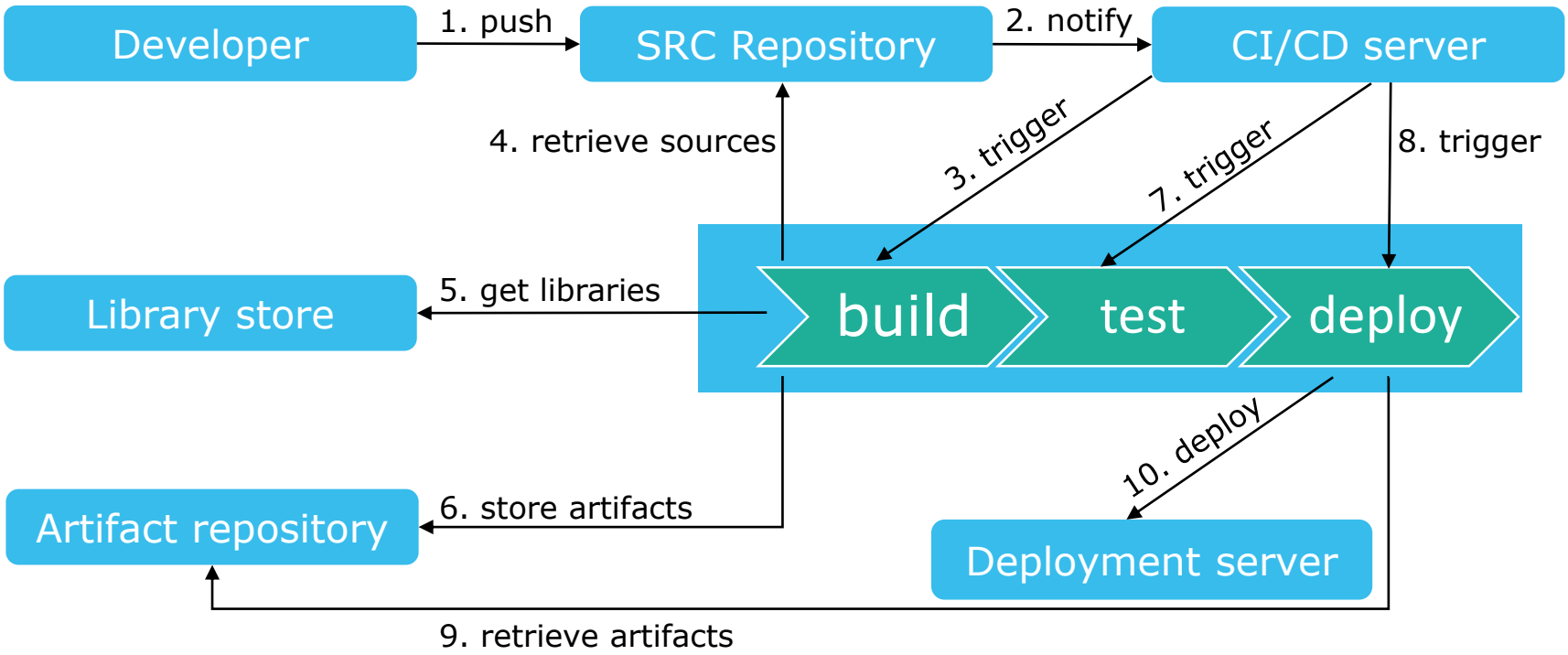
- **Questions:**
  - Participants profile
  - Security attributes
  - Attacks

- **Results:**
  - Role of developers
  - Deal with security matters
  - **TOP 3**: Integrity, availability, confidentiality

Analysis
Threat modeling approach

1. Decompose the application
2. Determine and rank threats
3. Determine countermeasures and mitigation

Analysis


Developer
1. push
SRC Repository
2. notify
CI/CD server
4. retrieve sources
3. trigger
7. trigger
8. trigger
Library store
5. get libraries
build
test
deploy
10. deploy
Artifact repository
6. store artifacts
Deployment server
9. retrieve artifacts

Analysis
Threat Analysis with STRIDE

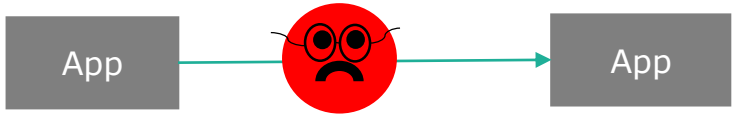
- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

Analysis
Threat Analysis with STRIDE

Tampering with Data

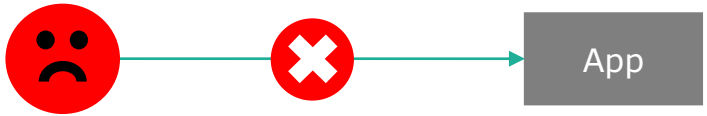
Integrity

Information Disclosure



Confidentiality

Denial of Service



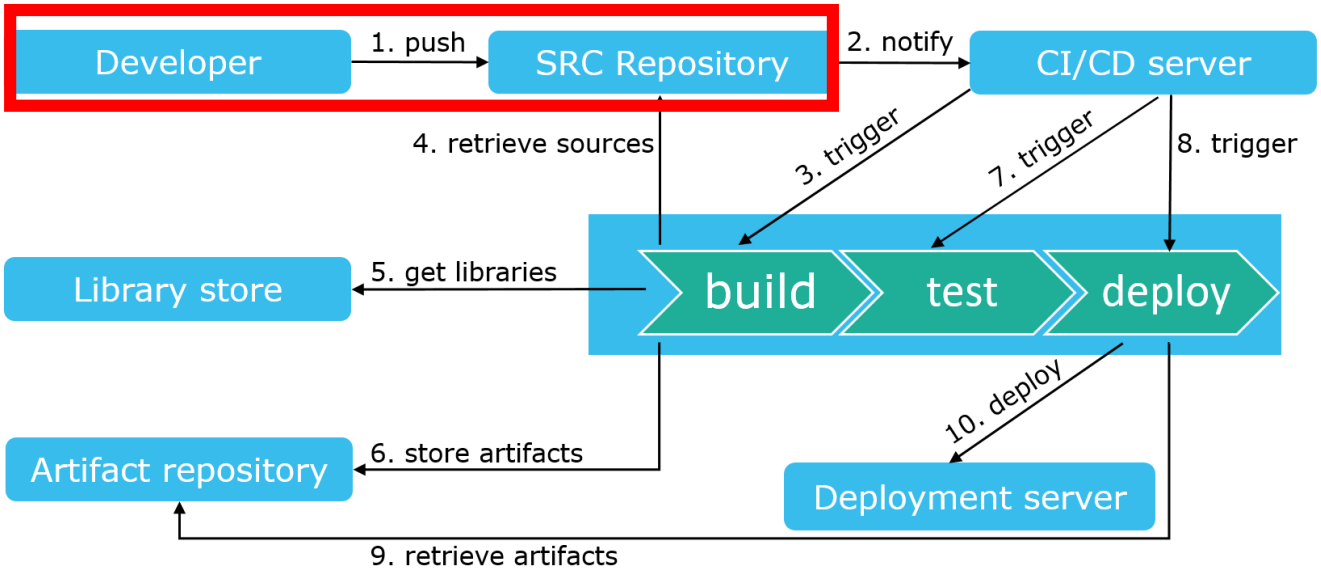
Availability

Analysis
Threat risk assessment

- **Over all risk severity**

	Impact			
Likelihood		Low	Medium	High
	Low	None	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

Analysis
STRIDE example

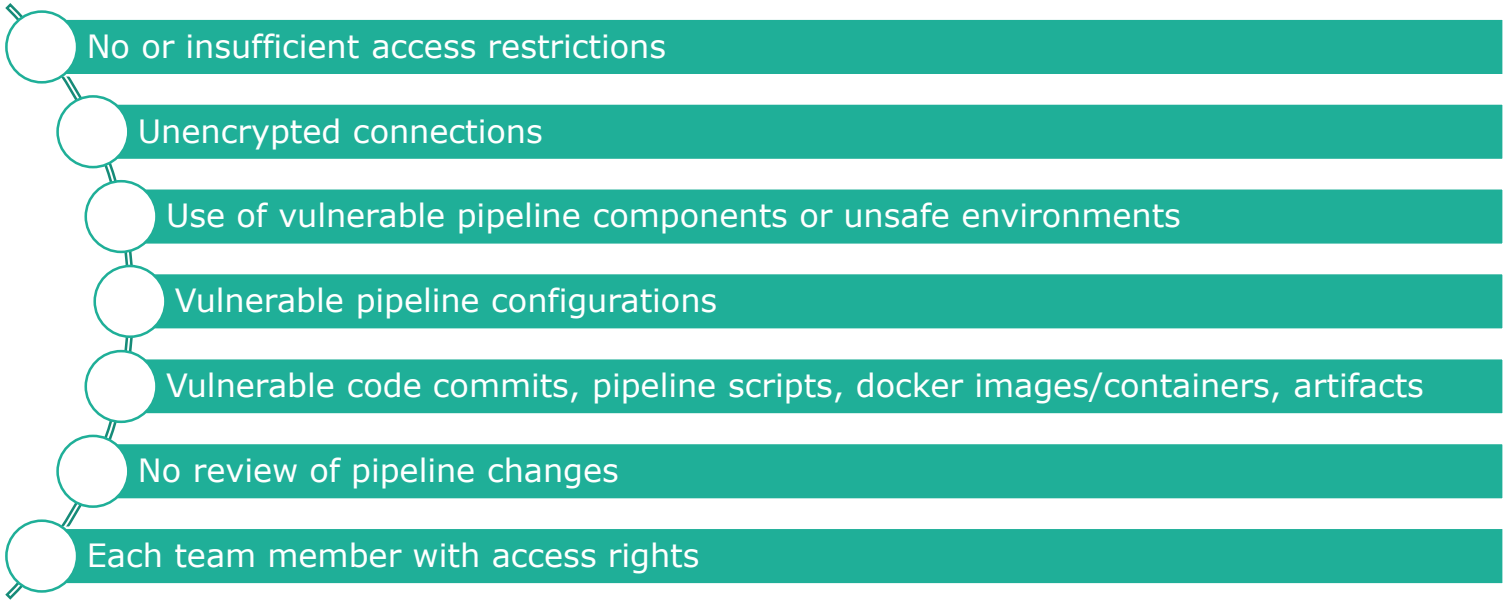


Analysis
STRIDE example

Occurrence	**1. Push**
Threat	Commit arbitrary code; manipulate or remove pipeline scripts
Effect	Malicious code; no delivery
Vulnerability	• None or few access restrictions • No review of code changes • No testing of pipeline scripts

Analysis
Results

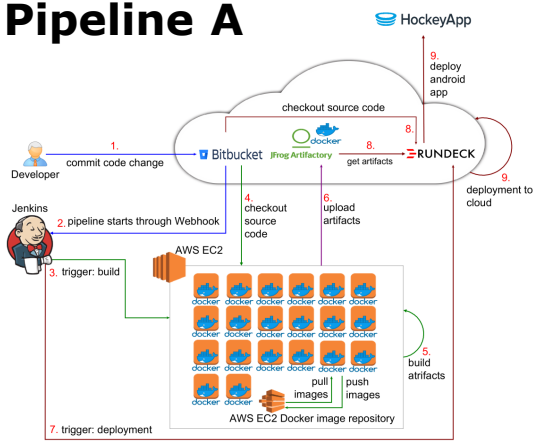
- Focus on T, I, and D



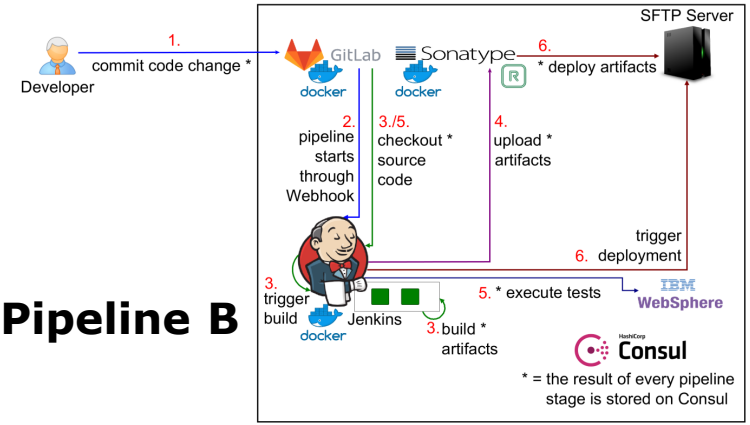
Case Study
Execution

STRIDE results

Pipeline A



Pipeline B



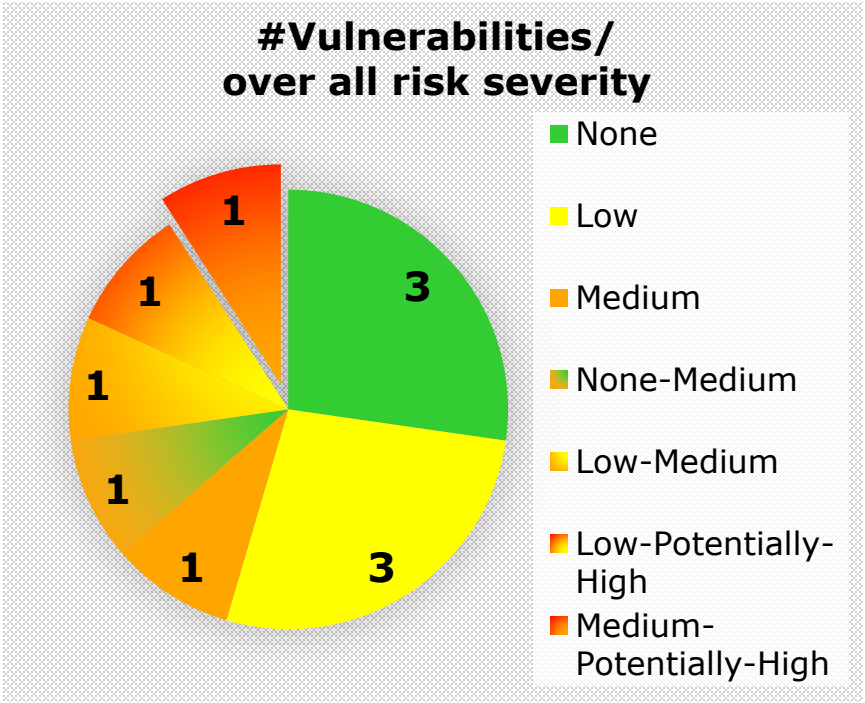
Vulnerabilities and risks

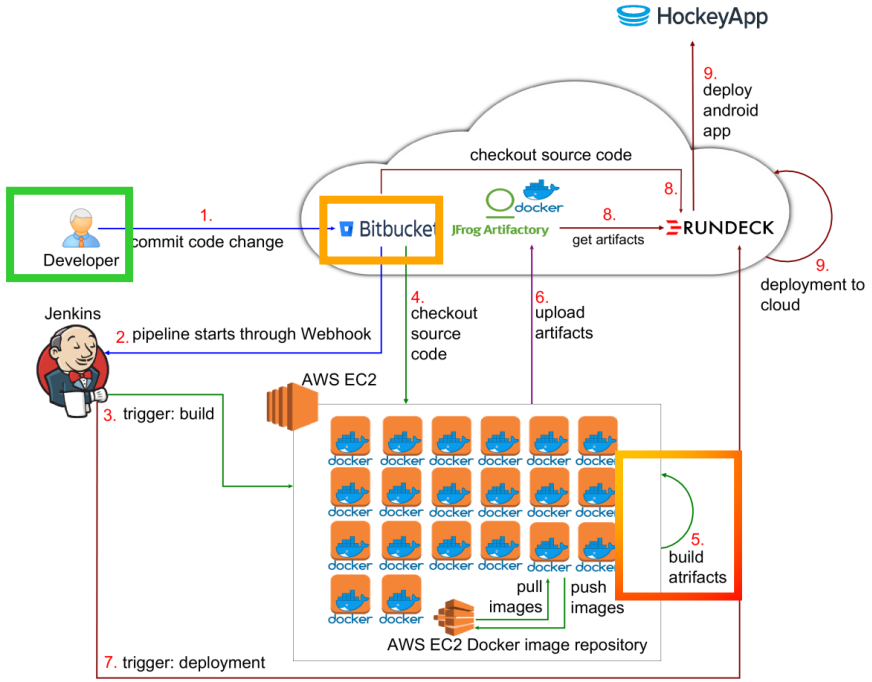
Case Study
Tools and Methods

- Manually
- VulDB
- Owasp Dependency Check 

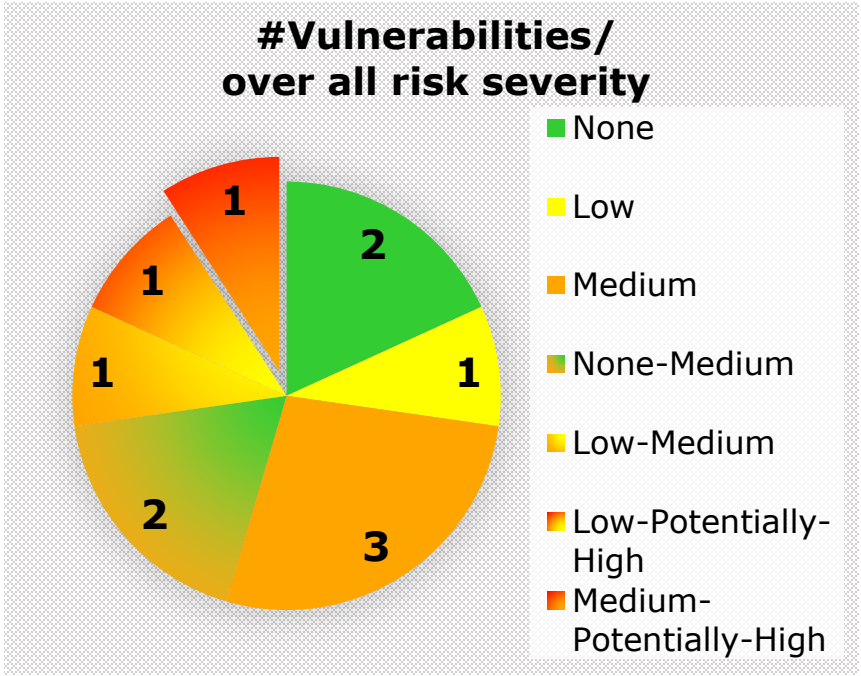
- Vulnerability Checks in Pipeline Components

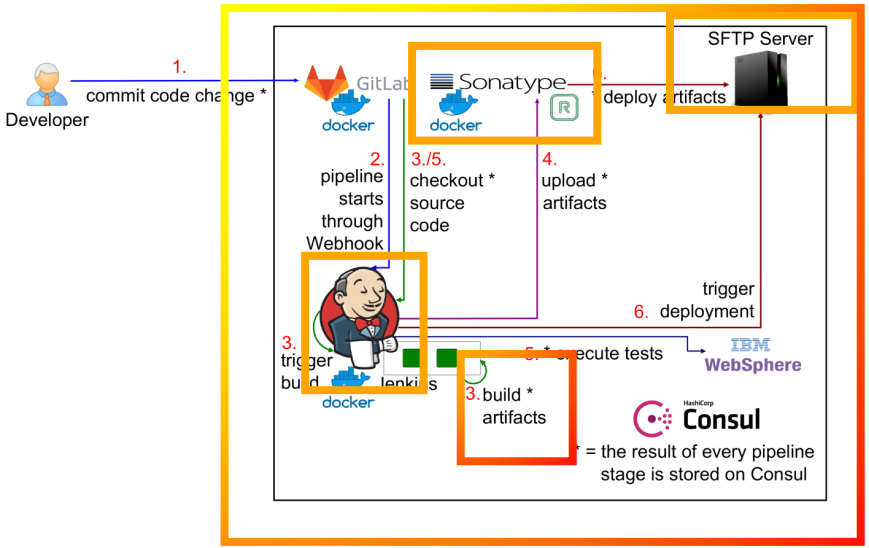
Case Study Results
Pipeline A





Case Study Results
Pipeline B





Lessons Learned

- Security has not a high priority
- Findings improve security awareness
- Important factors: time, budget

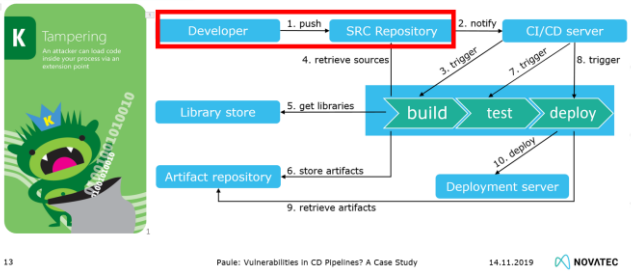
Conclusion

Survey

- **Setup:**
  - Online-survey
  - 19 participants
- **Questions:**
  - Participants profile
  - Security attributes
  - Attacks
- **Results**
  - Role of developers
  - Deal with security matters
  - **TOP 3**: Integrity, availability, confidentiality

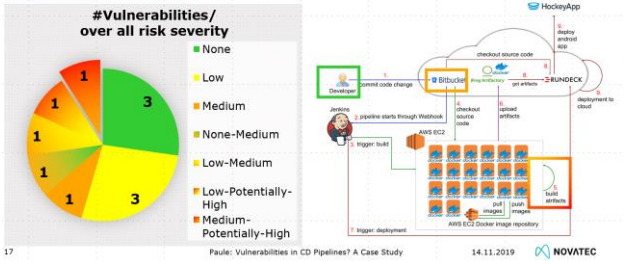
7 Paule: Vulnerabilities in CD Pipelines? A Case Study

Analysis & Abstraction
STRIDE example



13 Paule: Vulnerabilities in CD Pipelines? A Case Study 14.11.2019 NOVATEC

Case Study Results
Pipeline A



17 Paule: Vulnerabilities in CD Pipelines? A Case Study 14.11.2019 NOVATEC

START NOW – SECURE YOUR CD PIPELINE!

NOVATEC

Application Security Training for Developers by Jim Manico
4. – 5. Mai 2020

Christina Paule
Consultant

Novatec Consulting GmbH
Dieselstraße 18/1
D-70771 Leinfelden-Echterdingen

T. +49 711 22040-700
info@novatec-gmbh.de
www.novatec-gmbh.de

Sources

- [1] https://www.zdnet.de/88353687/kritische-luecke-in-docker-und-kubernetes-erlaubt-codeausfuehrung-auf-host-systemen/
- [2] Elevation of Privilege (EoP) Threat Modeling Card Game https://www.microsoft.com/en-us/download/details.aspx?id=20303