CSA Student Symposium 2023.pptx

{

Antman & The OWASP CI/CD Top Ten

< a dive into OWASP’s latest work in reducing vulnerabilities in application development >

}

By Ian Cook, Cybersecurity ‘23

Table of Contents {

01 CI/CD Primer

< What it is, why it’s relevant to Cybersecurity>

02 OWASP & Their Top Ten

< Organizational Context >

OWASP
Open Web Application
Security Project

03 CI/CD Top Ten Recap

< Recap & How to get started>

}

01 {

[CI/CD]

What is CI/CD?
Why is this relevant to Cybersecurity?

}

Continuous Integration < /1 CI > {

<- Developers frequently push code changes to a shared repository. Involves automated testing of code before merges to identify potential conflicts>

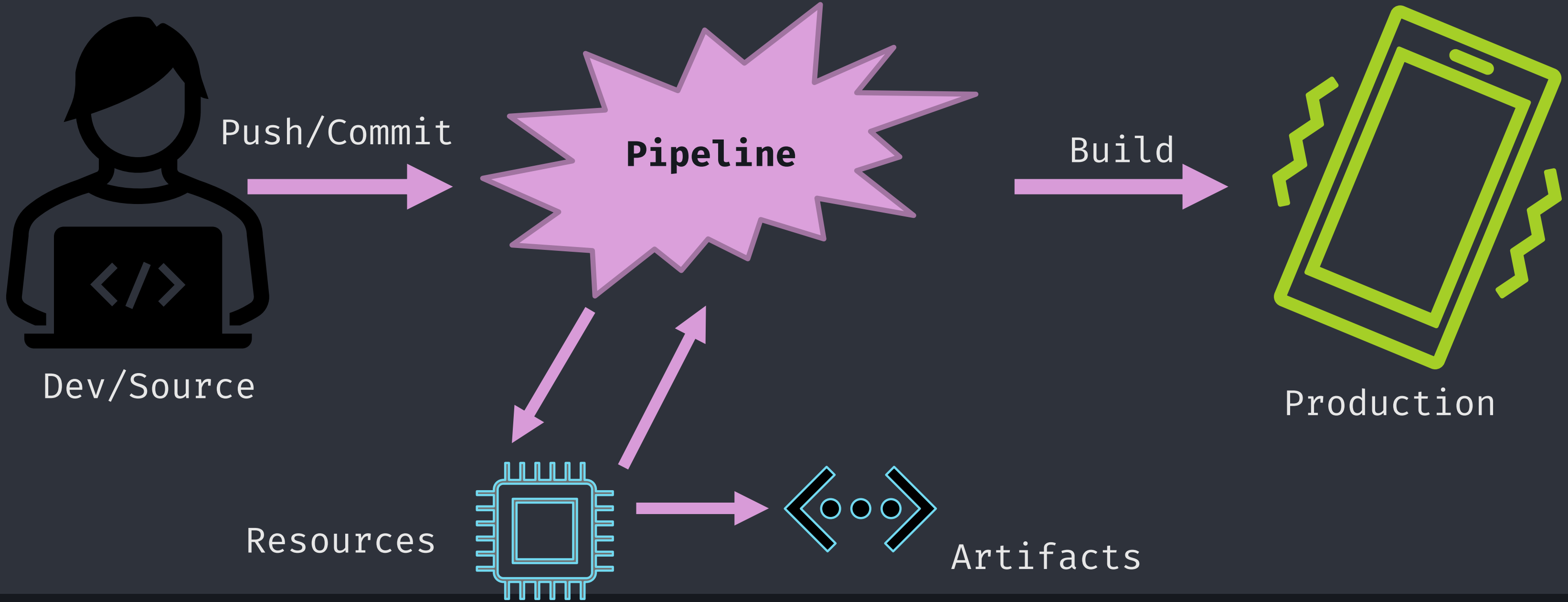
}

Continuous Deployment < /2> {

< - Once that code is tested and merged, it is then deployed to a staging or production environment>

}

Pipeline at-a-Glance



So why do we care?; {

If (future job is below):

- Security Architect
- DevSecOps Engineer
- Security Engineer
- Any security job involving development

Or (you develop anything in the future)

}

02 {

[OWASP]

Who is OWASP?
What are their Top Ten lists?

}

Who Is OWASP? {

Open Web Application Security Project

Non-Profit Foundation dedicated to improving the security of software.

Through:

- Trainings
- Publications
- Projects
- Local Chapters

}

OWASP Top Ten Lists {

Most Well Known:
Web Application Vulnerabilities

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery

}

03 {

[The CI/CD Top Ten]

The Vulnerabilities
How to (start to) Secure?
Getting Started in pipelines

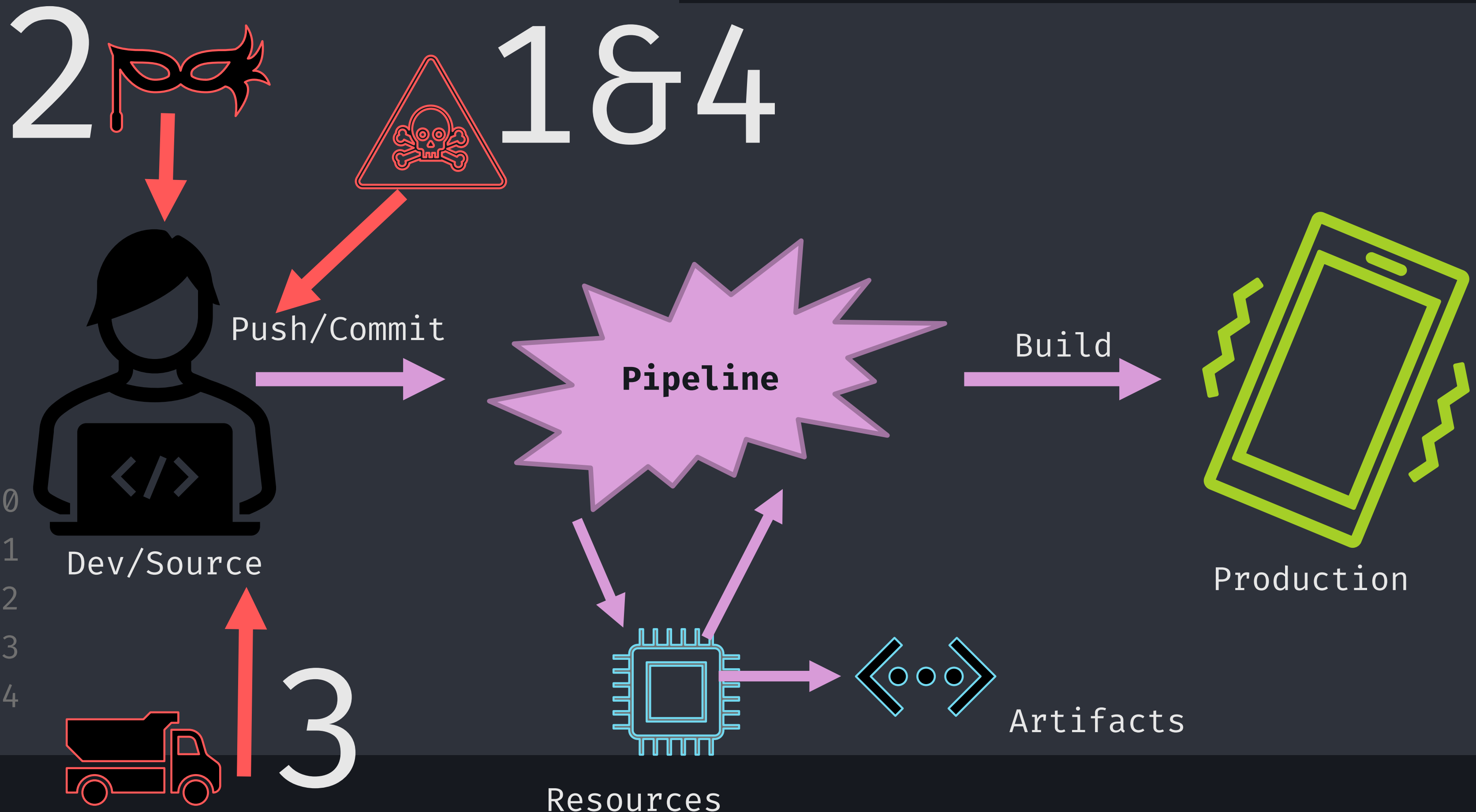
}

CI/CD Vulnerabilities 1-4 {

- 0x01 Insufficient Flow Control Mechanisms
- 0x02 Inadequate Identity and Access Management
- 0x03 Dependency Chain Abuse
- 0x04 Poisoned Pipeline Execution

}

CSA Student Symposium 2023.pptx

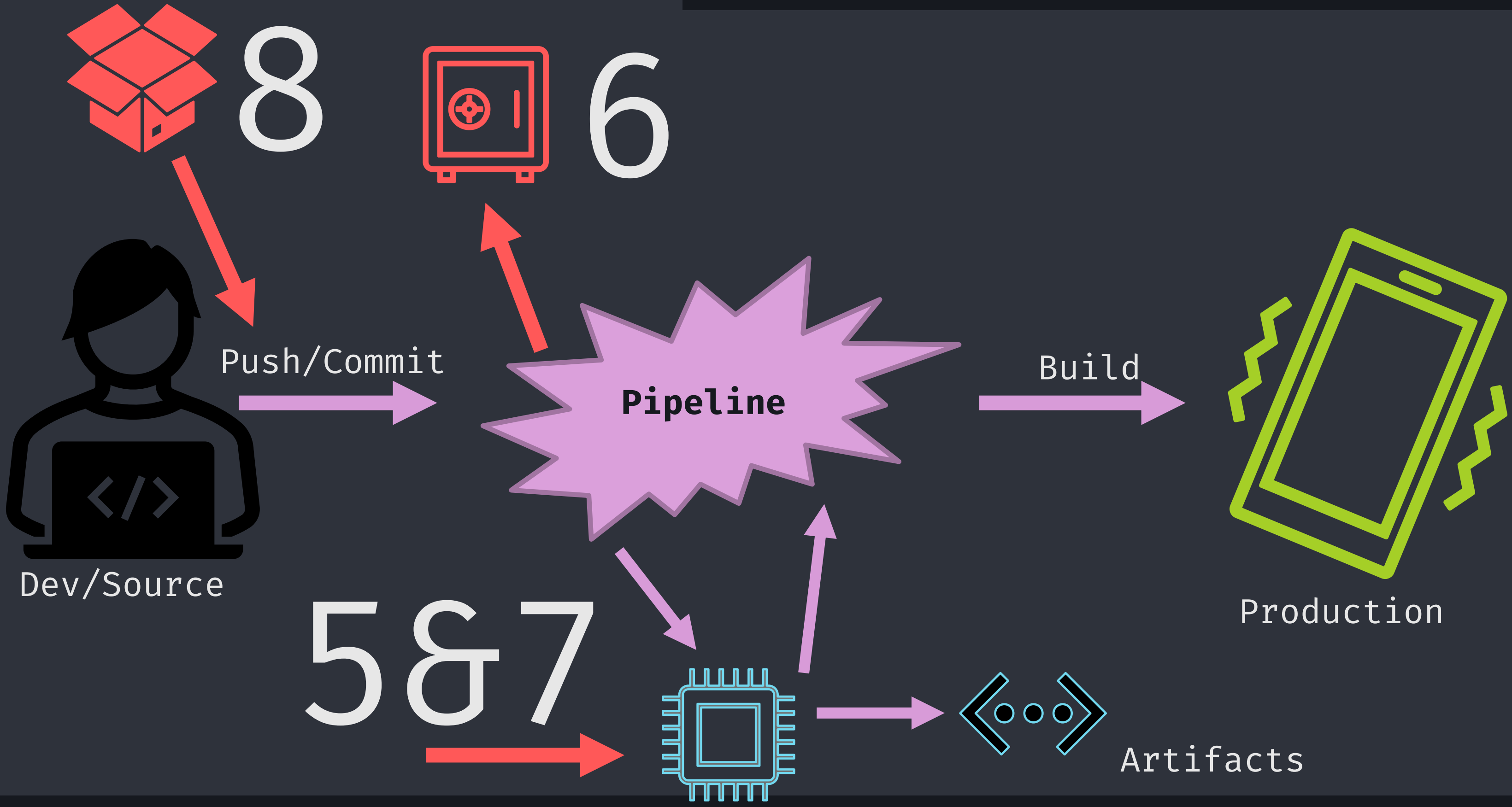


CI/CD Vulnerabilities 5-8 {

- 0x05 Insufficient Pipeline-Based Acces Controls
- 0x06 Insufficient Credential Hygiene
- 0x07 Insecure System Configuration
- 0x08 Ungoverned Usage of 3rd Party Services

}

CSA Student Symposium 2023.pptx



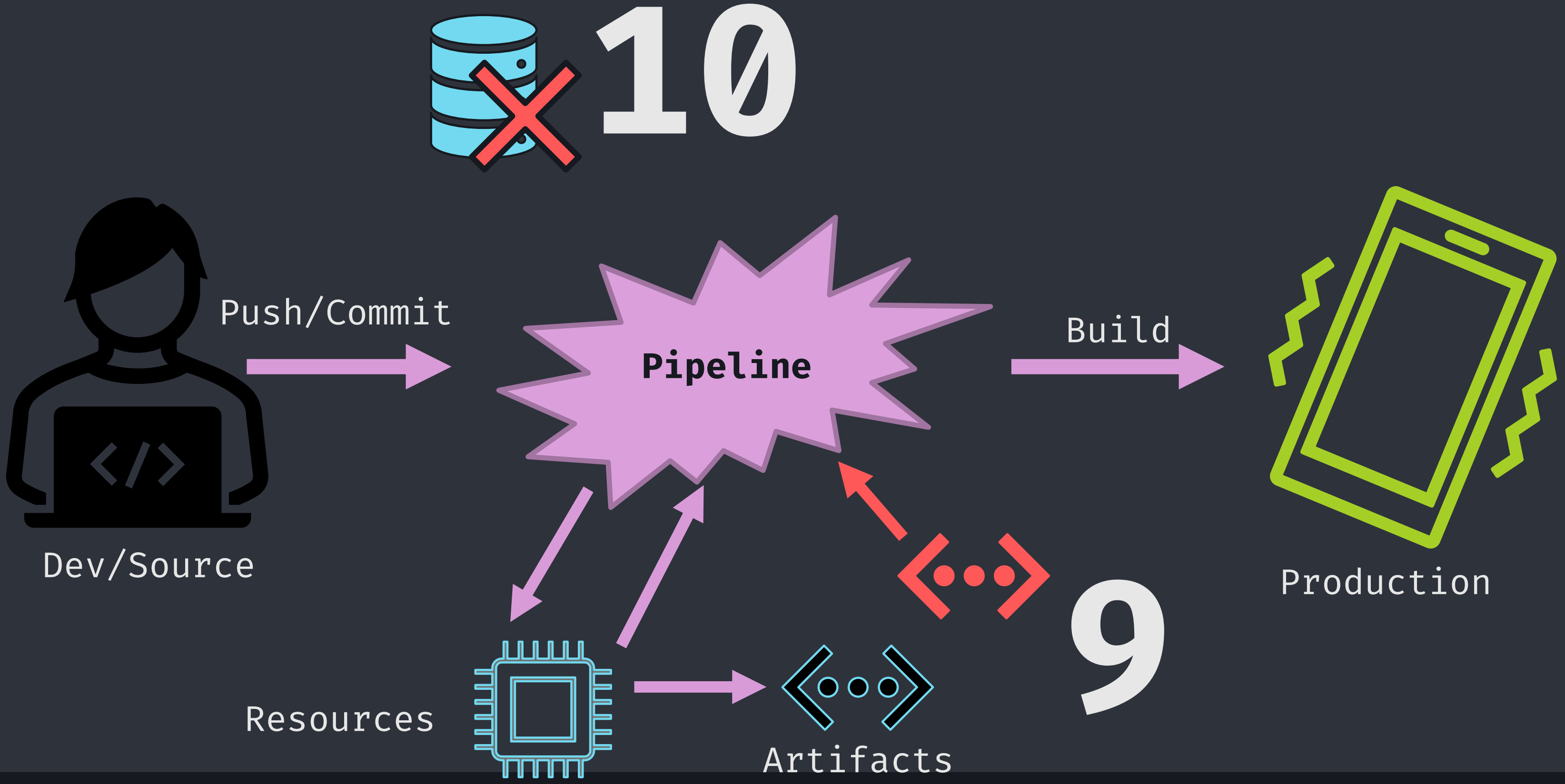
Resources

CI/CD Vulnerabilities 9-10 {

0x09 Improper Artifact Integrity Validation

0x10 Insufficient Logging and Visibility

}


10
Push/Commit
Pipeline
Build
Dev/Source
9
Production
Resources
Artifacts

Quick & Dirty Security steps:

Really, it’s just the basics,
done well & done comprehensively.

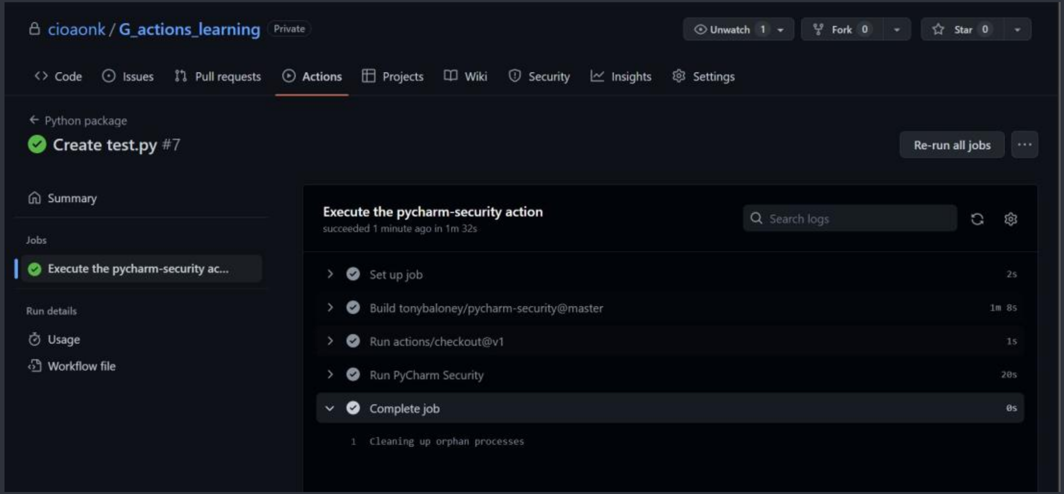
Those basics?
Principle of Least Privilege, Defense in Depth,
Understanding and enforcing a Trust Boundary.

< That was cool and all, but how do I learn and practice these things? >

— Someone

CI/CD Implementations {

GitHub Actions
Gitlab Pipeline
CircleCI
AWS CodePipeline
Azure Pipelines



← Python package

Create test.py #7

Execute the pycharm-security ac...

Execute the pycharm-security action

succeeded 1 minute ago in 1m 32s

```
Set up job                                   2s
Build tonybaloney/pycharm-security@master    1m 8s
Run actions/checkout@v1                      1s
Run PyCharm Security                         20s
Complete job                                 0s
  Cleaning up orphan processes
```

}

References & Acknowledgements {

A huge thank you to

Omer Gil, Daniel Krivelevich

of Cider Security, and OWASP

https://pycharm-security.readthedocs.io/en/latest/github.html

https://infosec-jobs.com/list/cicd-related-jobs/

https://owasp.org/www-project-top-10-ci-cd-security-risks/

https://about.gitlab.com/platform/?byuctf{n0w-y0u-C-m3}/link/index.html

https://www.rapid7.com/fundamentals/cicd/

https://docs.github.com/en/actions/learn-github-actions

}

The end; {

Questions?

Contact me:
Email: icook@byu.edu,
or slack: ian

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

}