

Workshops **Conference**

Munich University of Applied Sciences

The Westin Grand Munich

October 14, 2023

October 15, 2023



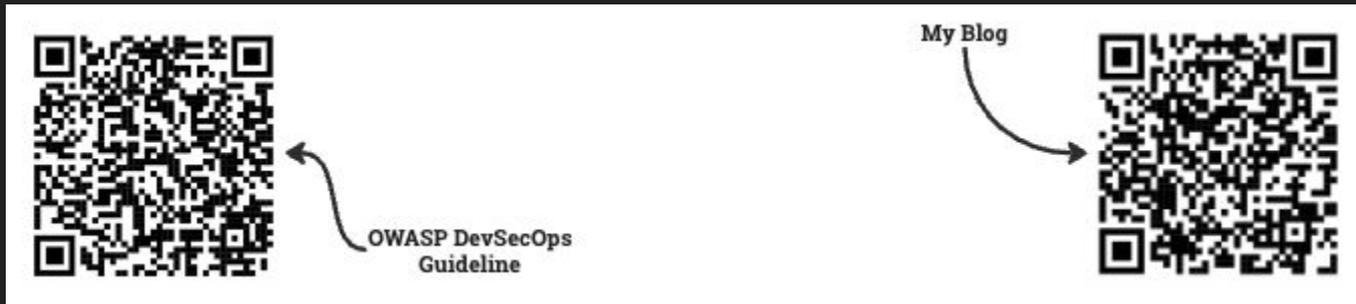
DevSecOps Culture

Ali Yazdani

OWASP DevSecOps Guideline Project lead

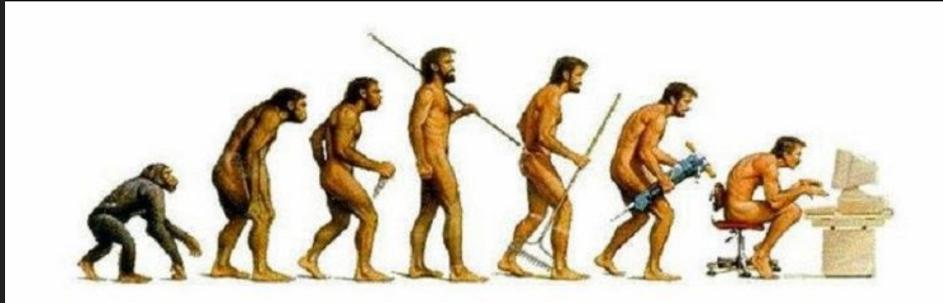
Readme!

- A Security Engineer - over 10 years experiences in AppSec in different industry sectors.
- 2016 - Present, OWASP as contributor on projects like MSTG, and Leading DevSecOps Guideline project.
- Now, Senior DevSecOps Engineer @ Scoutbee GmbH



Introduction

- In traditional software development, security measures were in the right side!
- DevOps + Security → DevSecOps
- Filling the gap!
- A culture of:
 - Collaboration
 - Shared responsibility
 - Continuous improvement



Pillars of DevSecOps

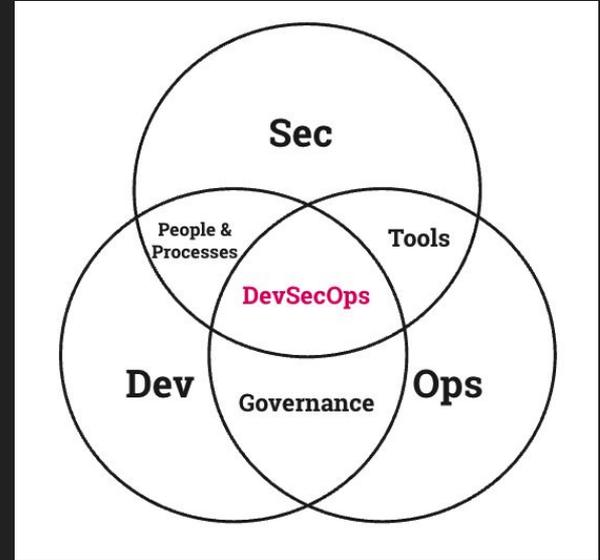
- People & Processes
- Tools (Technologies)
- Governance



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

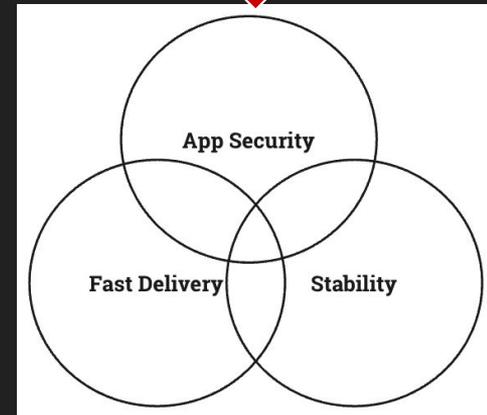
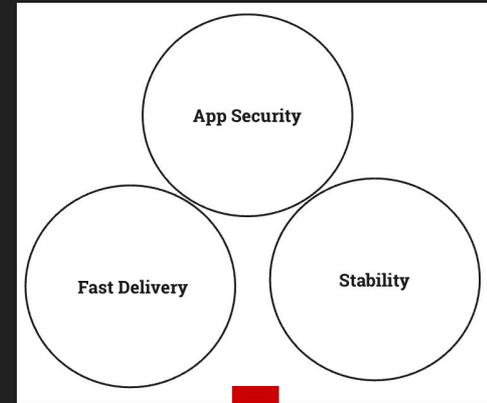
— Bruce Schneier —

AZ QUOTES



People & Processes

- The important part!
- Moving to DevSecOps increasing security team workload!!
- Traditionally:
 - Development -> fast delivery
 - Security -> application security
 - Operations -> stability
- DevSecOps: Delivering secure and stable software quickly

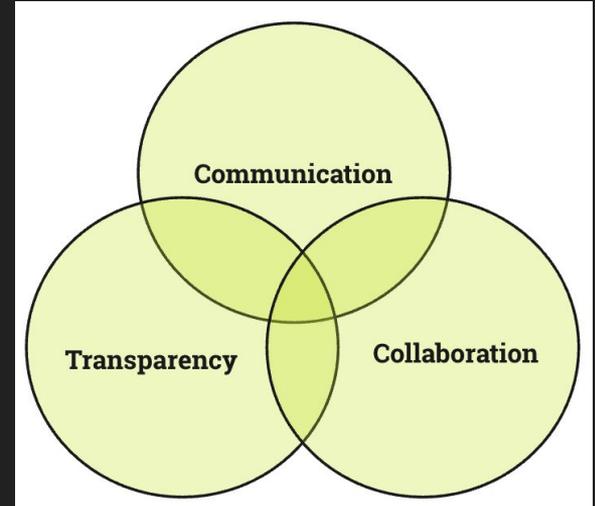


People & Processes - 2nd

- Now; we have a shared-responsibility model.
- Processes will help people to stay involved!

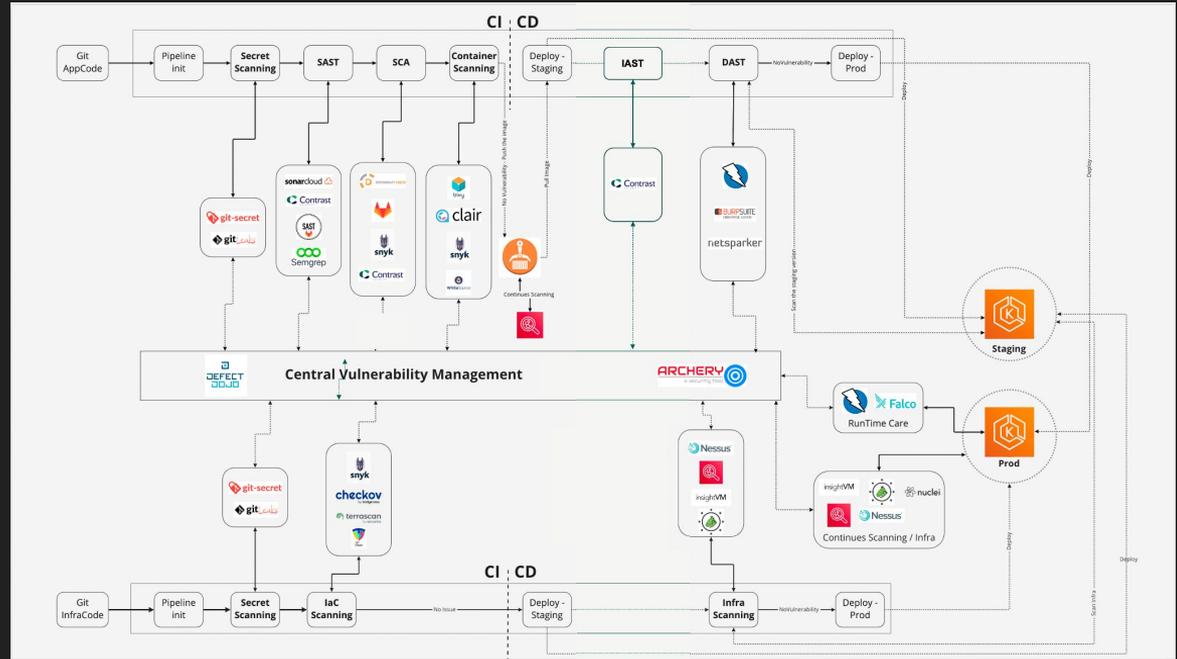
Topics to cover here:

- Shape the team (Security Champions)
- Training
 - Secure coding
 - Threat Modeling workshop
 - ...
- Awearnace



Technologies

- Let's make processes more practical!
- Automation is the key.
- Benefits:
 - Effort
 - Accuracy
 - Repeatability



Technologies - Example

Secret Scanning:

- The secrets should not be hard coded.
- The secrets should not be unencrypted.
- The secrets should not be stored in the source code.
- The code history does not contain inadvertent secrets.

#716232 JumpCloud API Key leaked via Open Github Repository.

Reported October 17, 2019 1:14pm +0200

Participants: [vinothkumar](#)

State: Resolved ()

Reported to: [Starbucks](#) | [Managed](#)

Disclosed: December 30, 2019 4:40pm +0100

Severity: Critical (9.7)

Weakness: Use of Hard-coded Credentials

Bounty: \$4,000

Time spent: None

CVE ID: None

Account de...: None

Custom data

Hacker IP...: None

Host Infor...: None

Nuclei Tem...: None

SUMMARY BY STARBUCKS

vinothkumar discovered a publicly available Github repository containing a Starbucks JumpCloud API Key which provided access to internal system information.

[@vinothkumar](#) — thank you for reporting this vulnerability and confirming the resolution.

TIMELINE - EXPORT

vinothkumar submitted a report to Starbucks. Oct 17th (3 years ago)

Summary: Open Github Repo Leaking Starbucks JumbCloud API Key

Description:
Team,
While going through Github search I discovered a public repository which contains Jumbcloud API Key of Starbucks.

Repo: <https://github.com/...> Project.
File: <https://github.com/.../Project/blob/0d56bb910923da2fbee95971778923f734a25f68/getSystemUsers.go>

Code 39 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1 req.Header.Add("x-api-key", "██████████")
```

POC

- List systems ``` curl -H "x-api-key: ██████████" "https://console.jumpcloud.com/api/systems"

Code 81 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1  
2 * - - -  
3 curl -H "x-api-key: ██████████" "https://console.jumpcloud.com/api/systemusers"
```

- SSO Applications ``` curl -H "x-api-key: ██████████" "https://console.jumpcloud.com/api/applications"

#911606 Leaked JFrog Artifactory username and password exposed on GitHub - https://snapchat.jfrog.io

Reported June 30, 2020 7:00am +0200

Participants: [kiyell](#)

State: Resolved ()

Reported to: [Snapchat](#)

Disclosed: August 12, 2021 11:40pm +0200

Severity: High (7 - 8.9)

Weakness: Information Disclosure

Bounty: \$15,000

Time spent: None

SUMMARY BY SNAPCHAT

Researcher found valid JFrog credentials which were committed to a public Github repository of a Snap employee. This allowed access to internal Snap libraries/artifacts along with the ability to push updates to existing artifacts as well.

TIMELINE - EXPORT

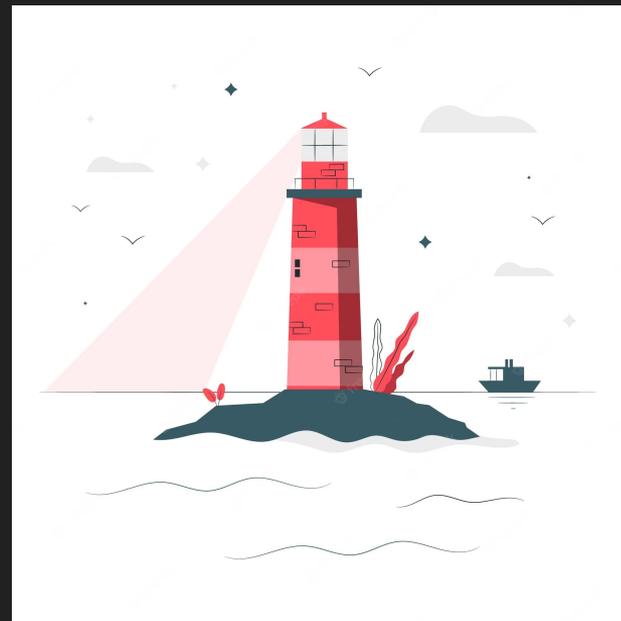
- [kiyell](#) submitted a report to [Snapchat](#). Jun 30th (2 years ago)
- [bugtriage-ryan](#) posted a comment. Jun 30th (2 years ago)
- [sfrisk](#) | [Snapchat staff](#) changed the status to [Triage](#). Jun 30th (2 years ago)
- [kiyell](#) posted a comment. Jun 30th (2 years ago)

Governance

- Measuring results
- Continuous improvement
- Compare results with expectations

Topics to cover here:

- Compliance Audit/Check
 - Policy as Code
 - Security Benchmarking
 - Security Standards (ISO, SOC2, ...)
- Data Protection
- Visualisation
 - Tracking maturities
 - Monitoring



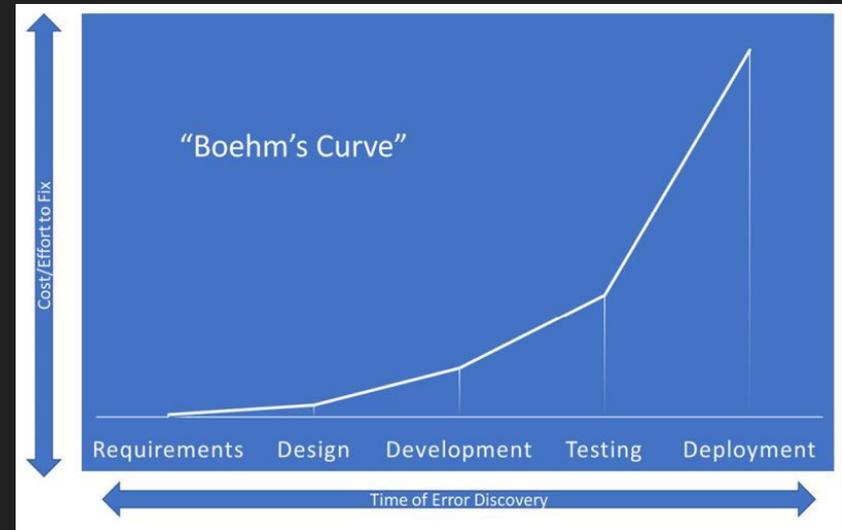
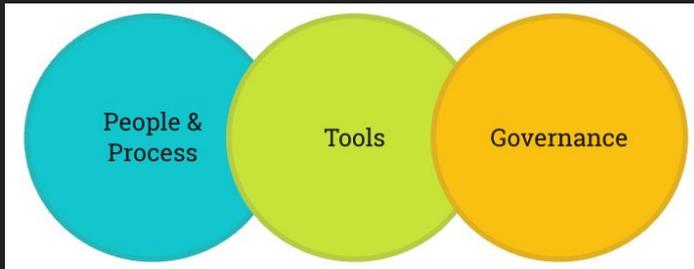
Challenges and Mitigations

- Overcoming Cultural Resistance
- Seamless Tool Integration
- Addressing Compliance and Regulations



Conclusion

- DevSecOps journey, is a long-term investment!
- The good implementation makes it a cost-reduction activity.
- Shifting to the left → Catching issues as fast as possible.



Q&A

Thanks



OWASP DevSecOps
Guideline

My Blog

