DevSecOps Culture

Ali Yazdani

OWASP DevSecOps Guideline Project lead

Readme!

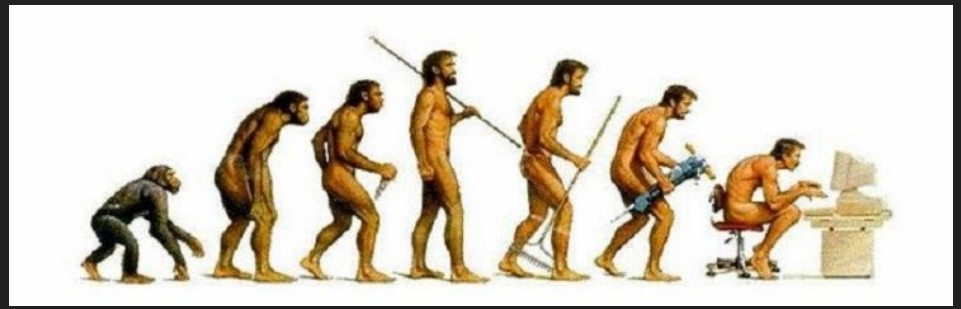
- A Security Engineer - over 10 years experiences in AppSec in different industry sectors.
- 2016 - Present, OWASP as contributor on projects like MSTG, and Leading DevSecOps Guideline project.
- Now, Senior DevSecOps Engineer @ Scoutbee GmbH

OWASP DevSecOps Guideline

My Blog

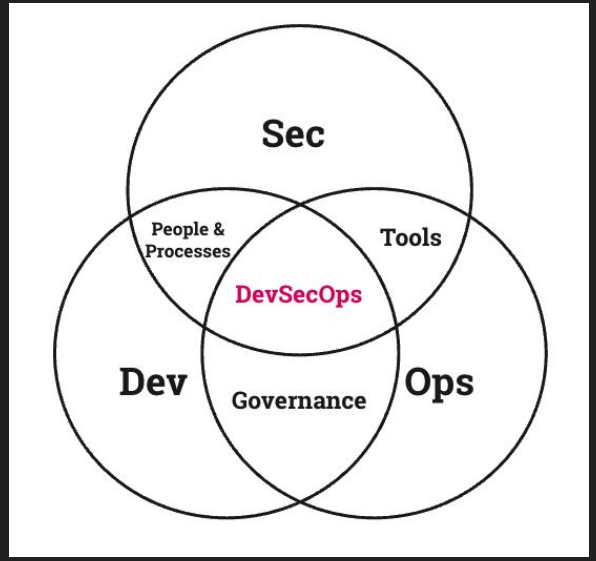
Introduction

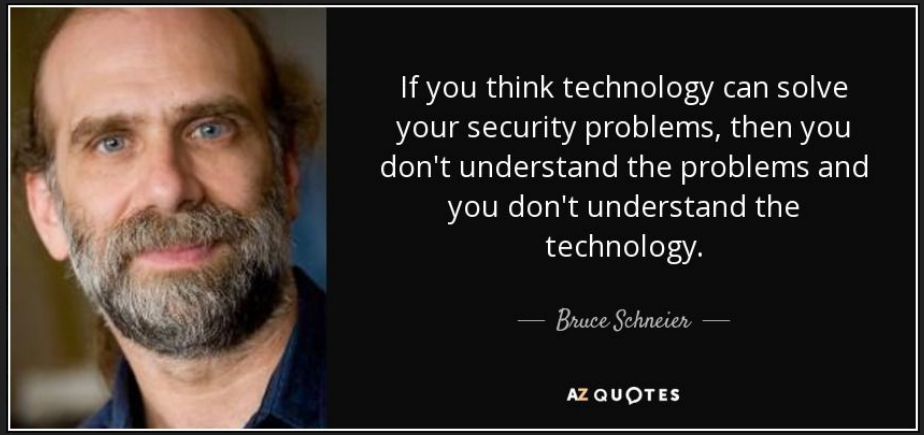
- In traditional software development, security measures were in the right side!
- DevOps + Security → DevSecOps
- Filling the gap!
- A culture of:
  - Collaboration
  - Shared responsibility
  - Continuous improvement



Pillars of DevSecOps

- People & Processes
- Tools (Technologies)
- Governance



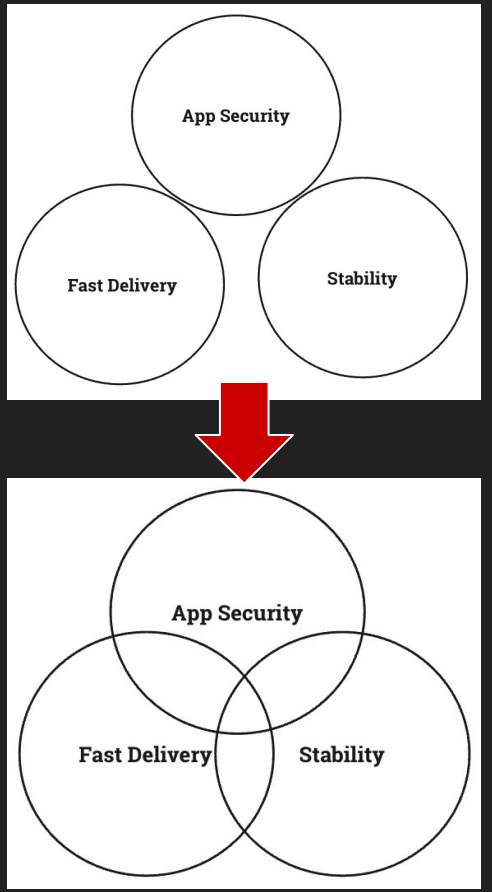


People & Processes

- The important part!
- Moving to DevSecOps increasing security team workload!!

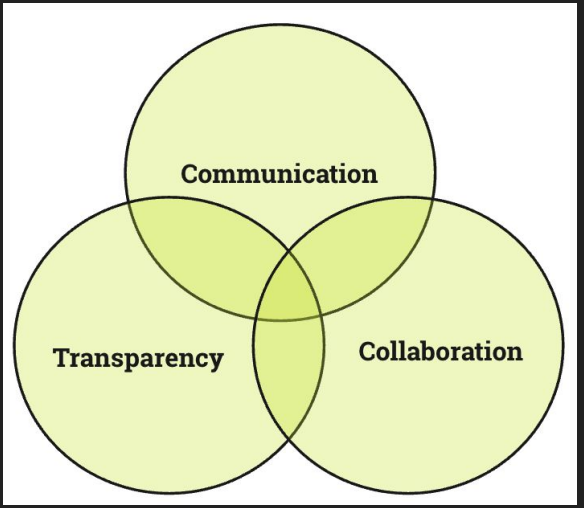
- Traditionally:
  - Development -> fast delivery
  - Security -> application security
  - Operations -> stability

- **DevSecOps:** Delivering secure and stable software quickly



People & Processes - 2nd

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

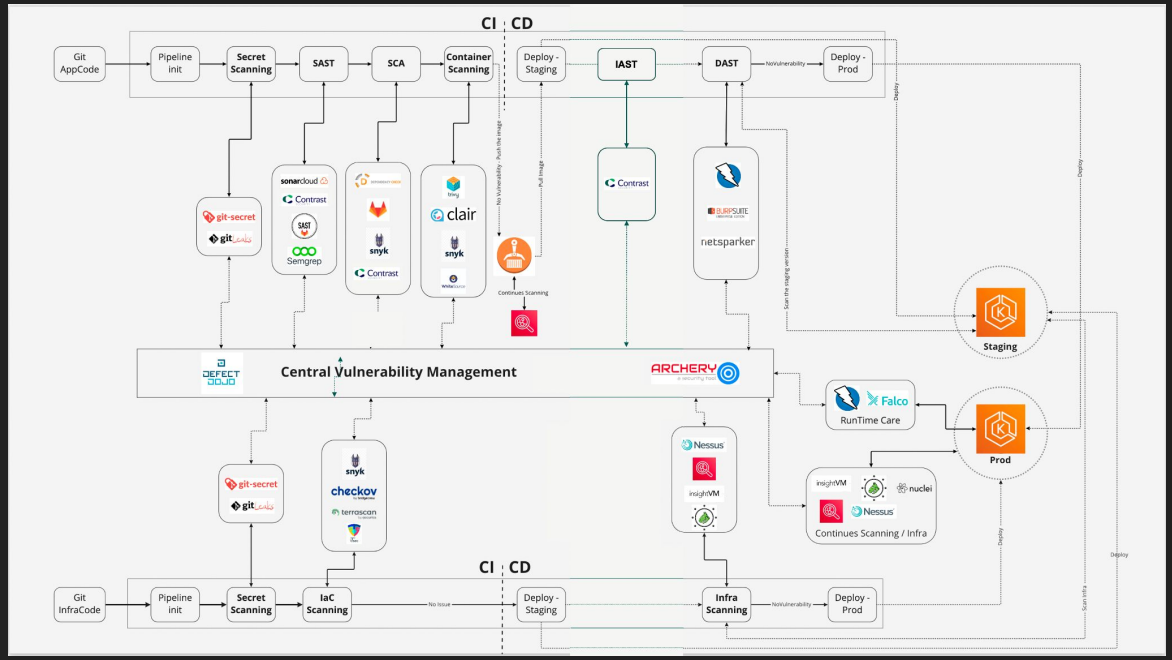


Topics to cover here:

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

Technologies

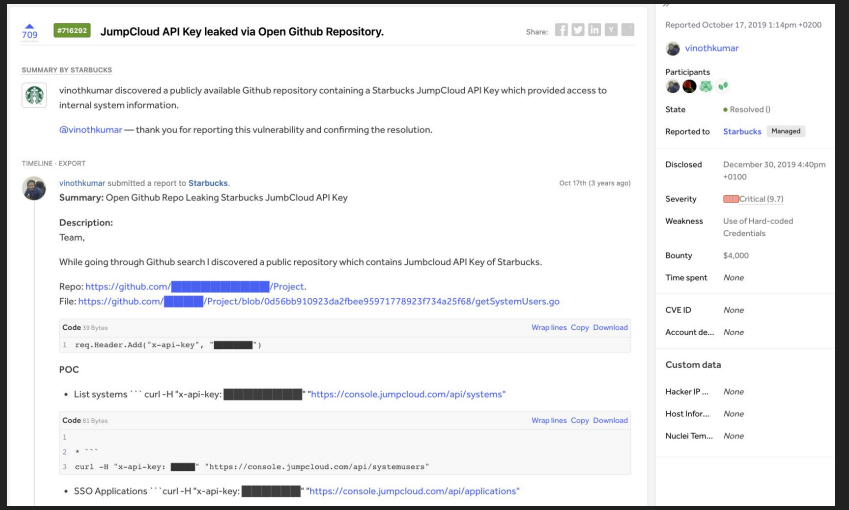
- Let’s make processes more practical!
- Automation is the key.
- Benefits:
  - Effort
  - Accuracy
  - Repeatability

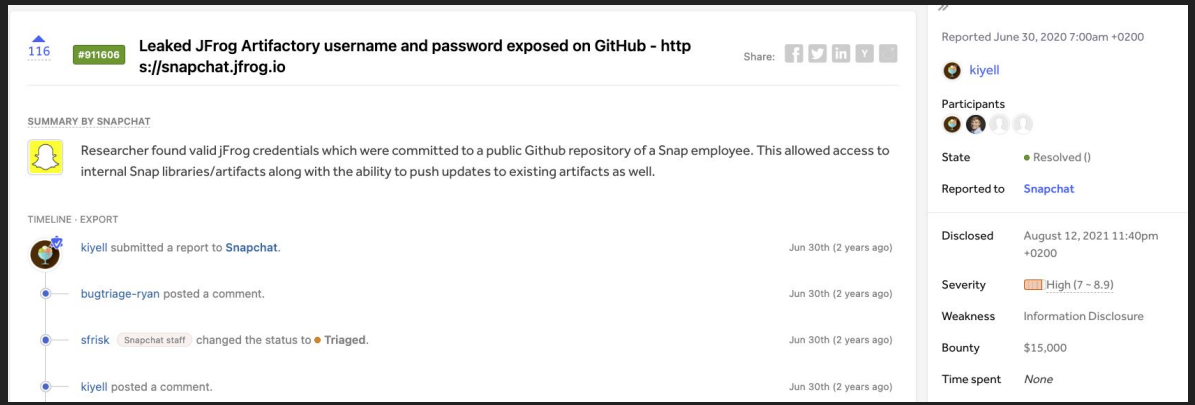


Technologies - Example

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.





Governance

- Measuring results
- Continuous improvement
- Compare results with expectations

Topics to cover here:

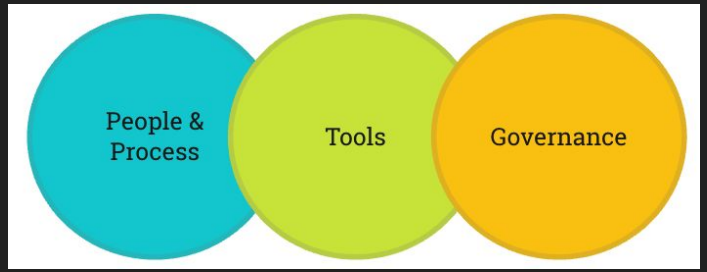
- Compliance Audit/Check
  - Policy as Code
  - Security Benchmarking
  - Security Standards (ISO, SOC2, …)
- Data Protection
- Visualisation
  - Tracking maturities
  - Monitoring

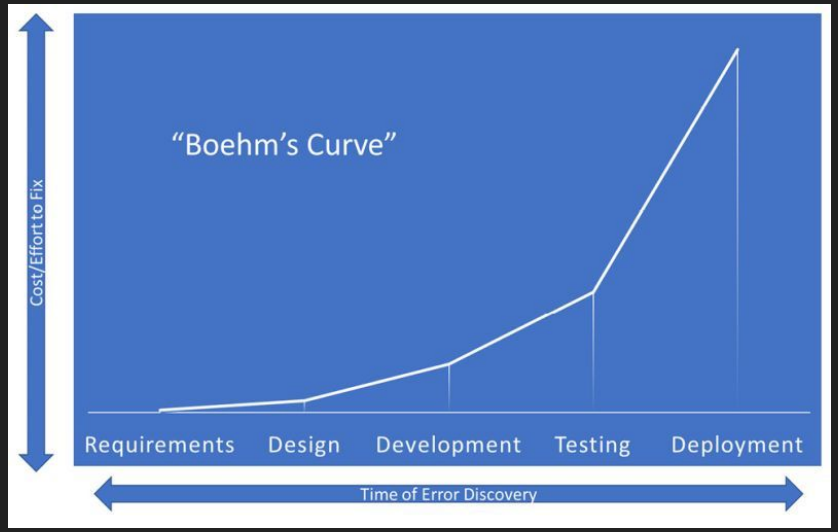
Challenges and Mitigations

- 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