Why you should NOT hire DevSecOps engineers

Ilya Polyakov

Head of Source Code Analysis, Angara Security

Moscow, August 26, 2022

def __str__(self):

Ilya Polyakov

- Head of Source Code Analysis at
  - Angara Security
- Previously worked on AppSec at
  - Align Technology
  - Prom Svyaz Bank
  - ABBYY
- Certifications
  - EC-Council Certified Application Security Engineer
  - Microsoft Certified Azure Security Engineer

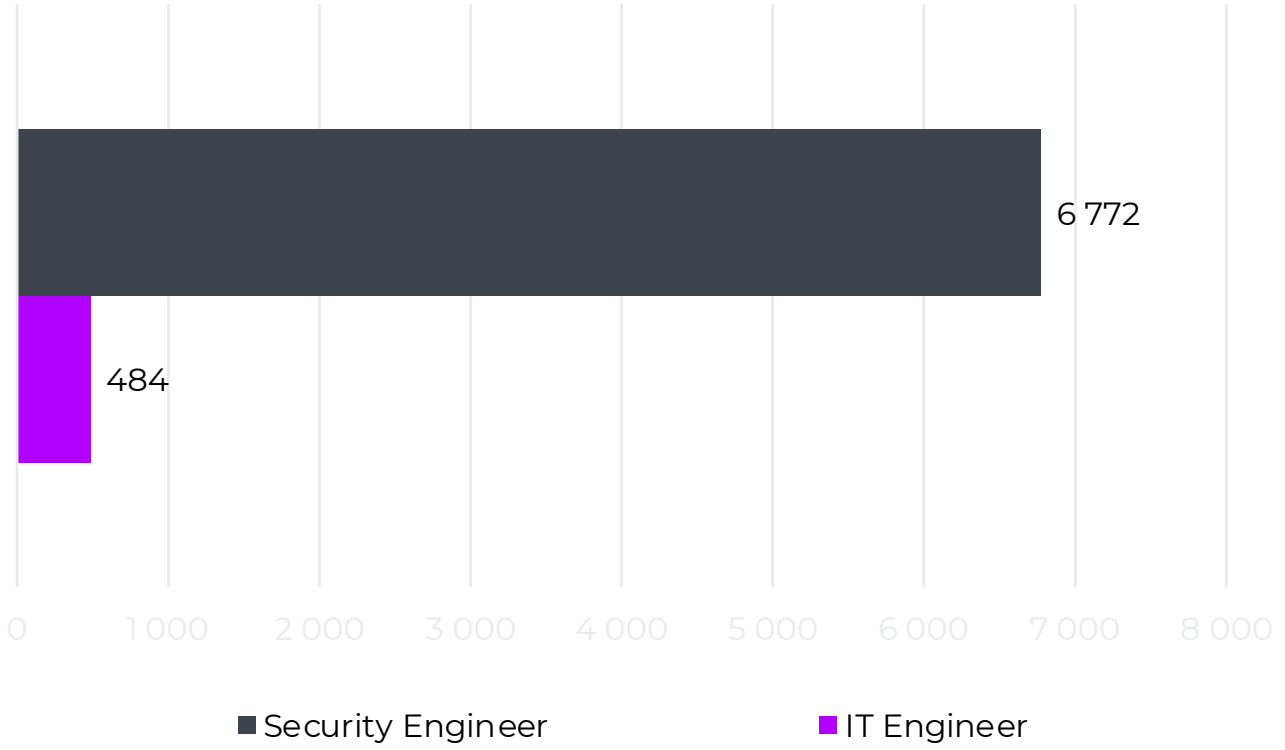
Just add “Sec” to your DevOps engineers?

- Software Development Lifecycle
- DevOps

- **Secure** Software Development Lifecycle
- Dev**Sec**Ops (or even SecDevOps!)

Lessons from the past

why there are no "IT engineer" positions? (in fact a few still exist)

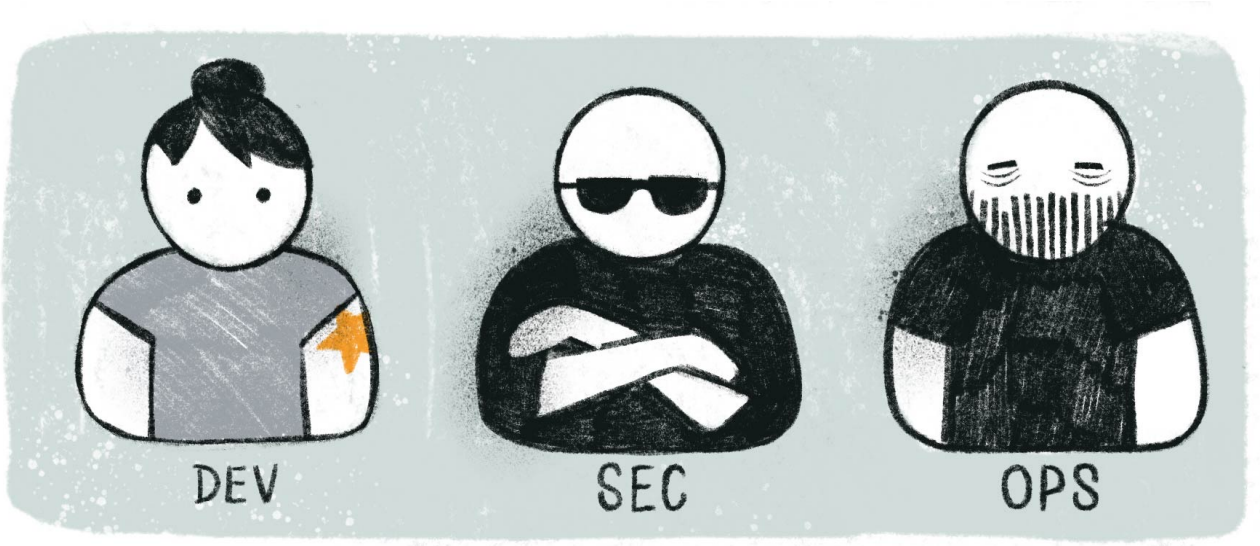


According to Indeed.com (US)

Division of labor

All-in-one = only for fun

- Dev-QA-Ops? DevSalesOps?
- Specialization rules



Separation of duties

- combining DevOps and Security violates the "separation of duties" principle
- DevOps = IaC dev nowadays

DevOps is getting complicated

- DevOps workload is getting more and more complicated (Cloud Native apps etc), no room for adding Security to it

AppSec is quite a thing

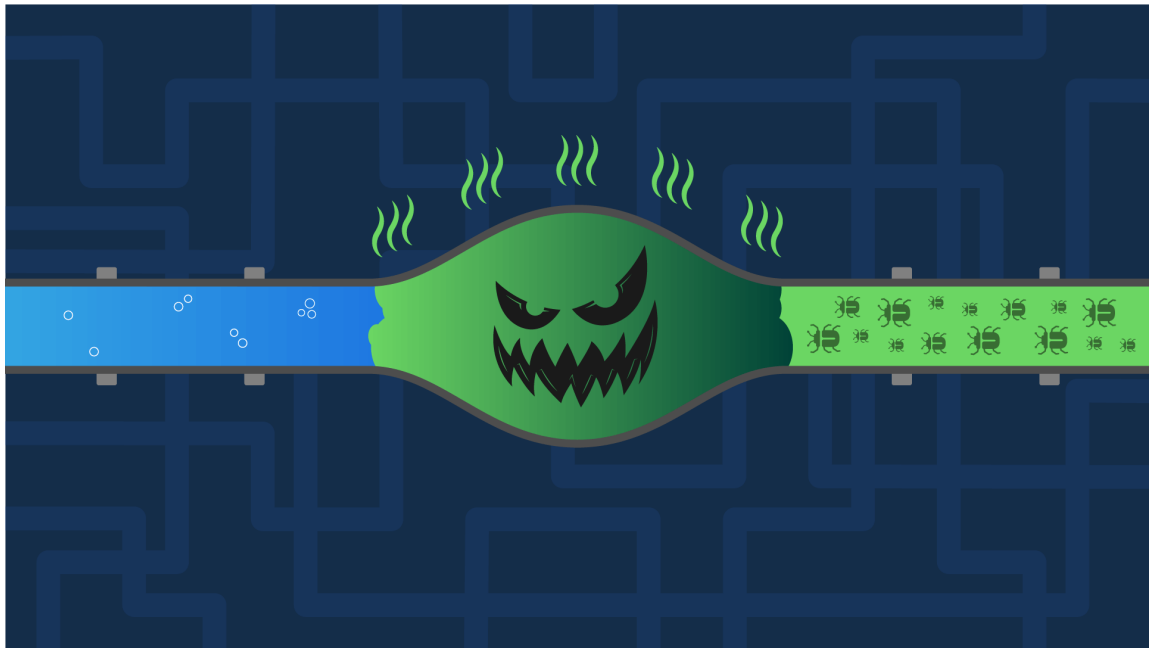
- Know a myriad of CWE's
- Triage findings
  - filter out false positives
  - assess exploitability
  - adjust severity of each findings
- DevOps engineers are no real programmers even!

SAST/DAST: plug’n’pray?

- integrating sec tools into pipelines is no big deal (follow the manual)
- But you can't just plug in SAST/DAST tools and relax, you need to ensure they were chosen+tuned properly and don't miss vulnerabilities

Clogged pipelines

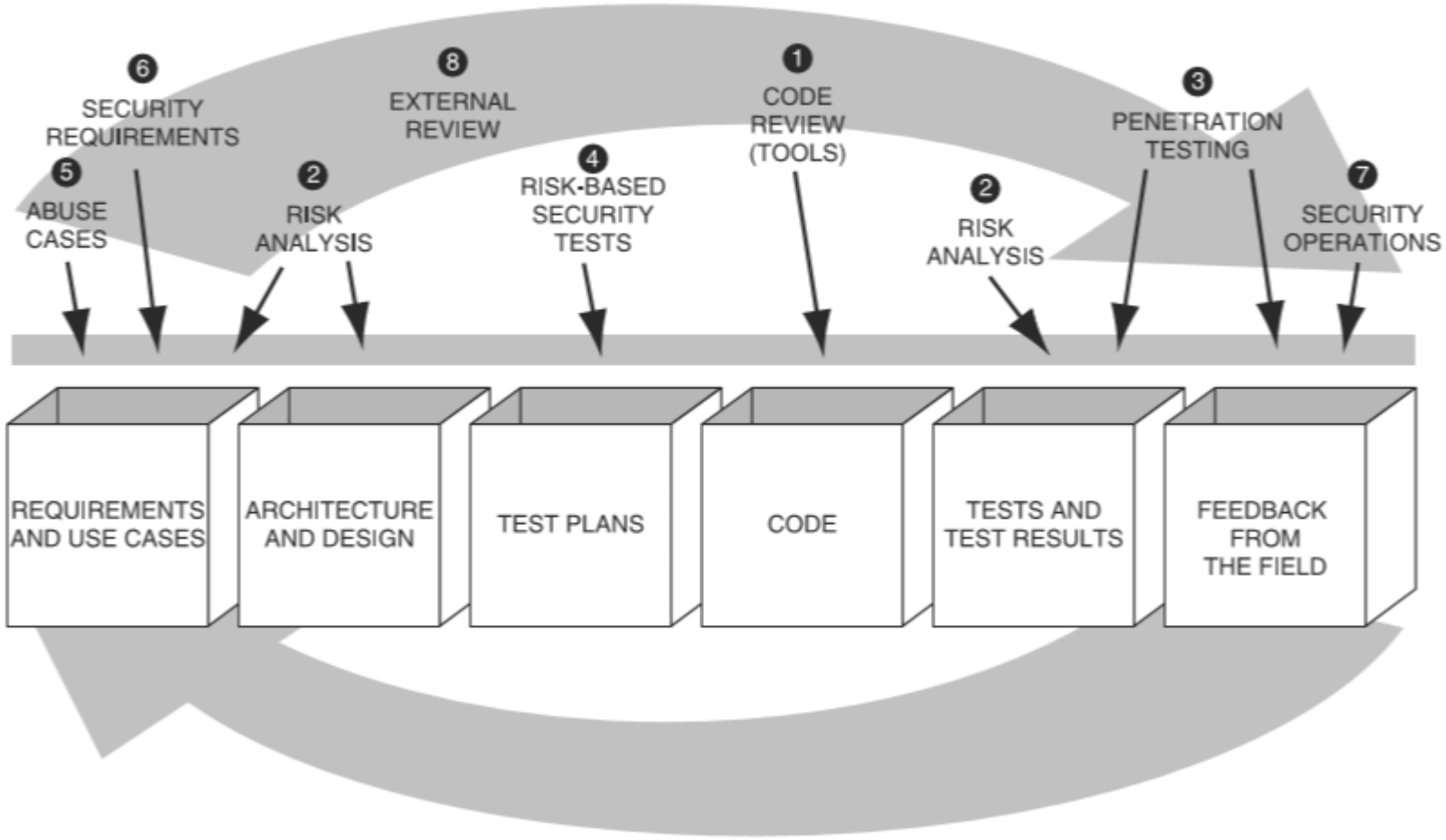
- inserting AppSec scanners into CI/CD pipelines is often questionable
- longer builds
- build failures triggered by false positive alerts



SDLC segments not covered by CI/CD tools

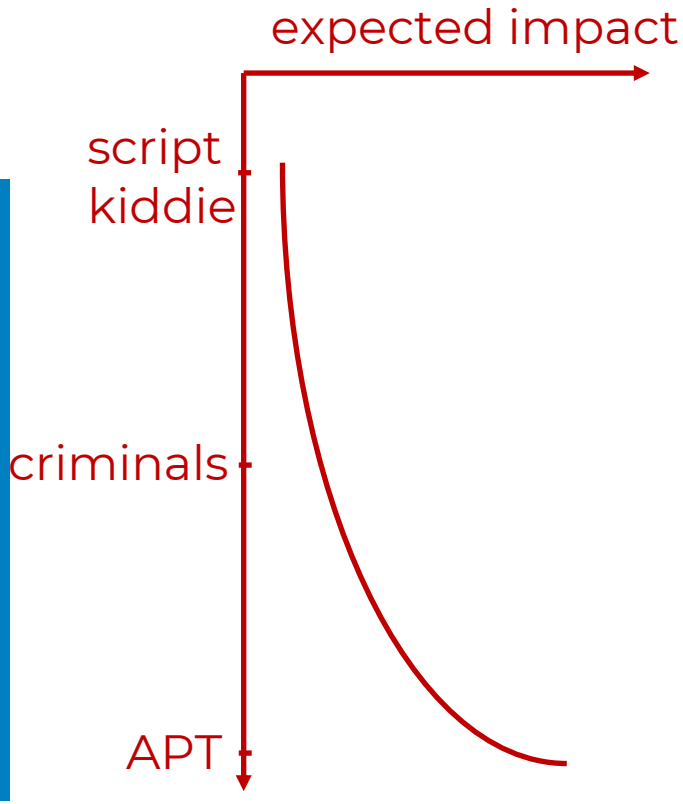
Above DevOps' paygrade:

- Threat modelling
- Security requirements
- Incident response
- WAF tuning
- Devs training
- Manual pentest



AppSec is a Digging Contest

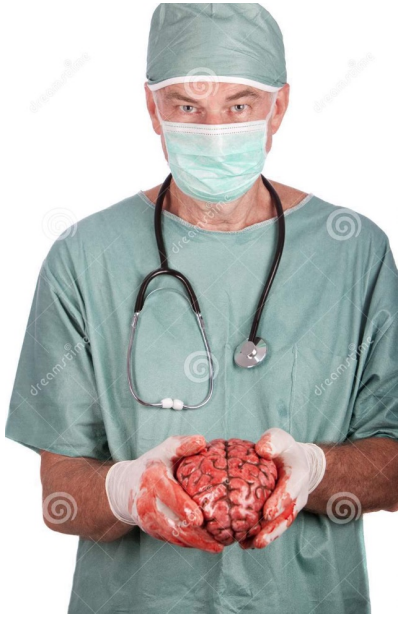
And qualification matters



Meet the Brain Surgery Dentist

(Recruiter's Nightmare)

- Brain surgeons an dentists deal with heads
- AppSec and DevOps engineers deal with code
- So why don't let DevOps do application security?..



I can feed only one person at a time. Just one, one, one.

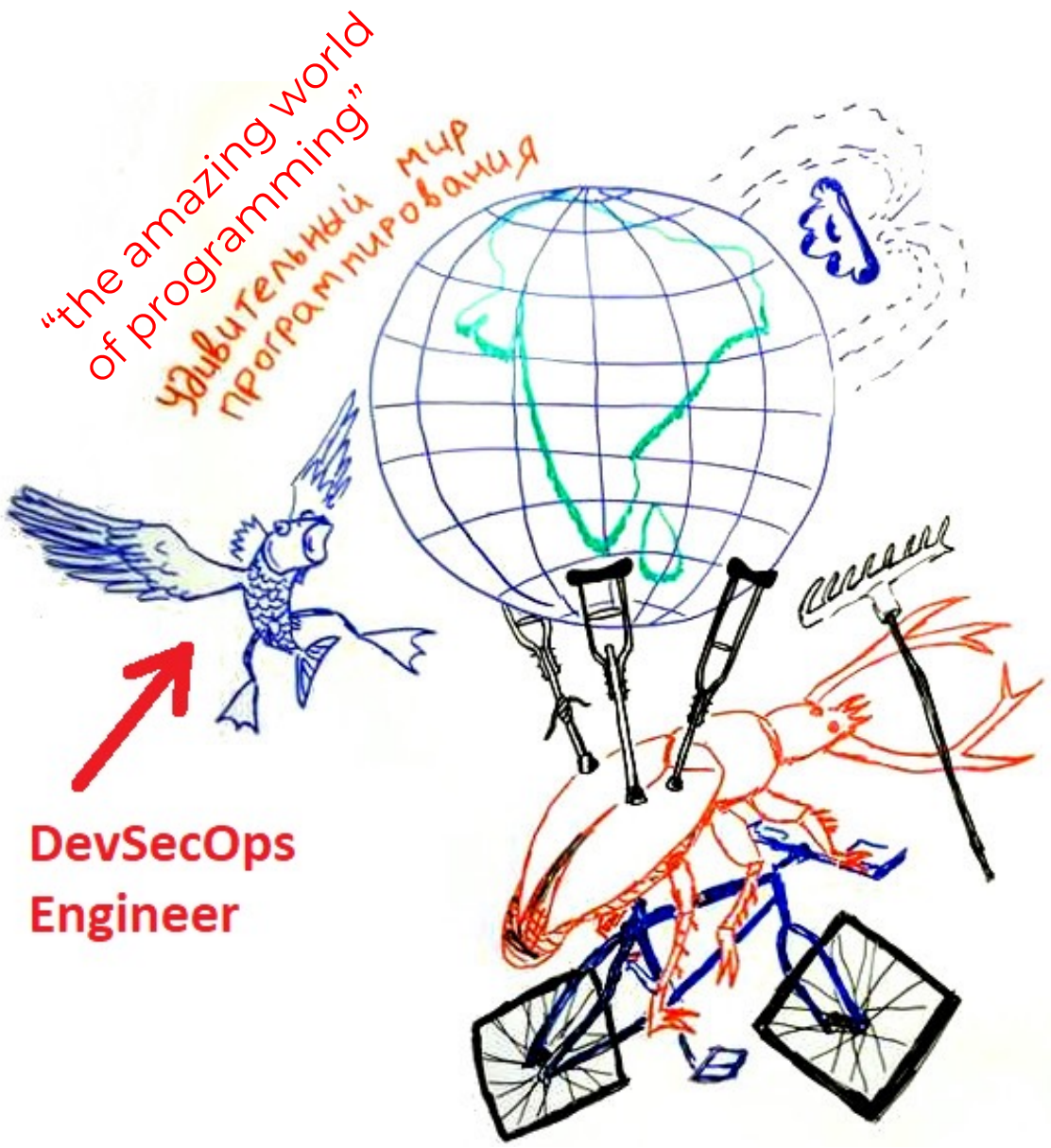
Mother Teresa

- No budget for AppSec + DevOps?
- Maybe you are just not ready for DevSecOps
- Or you should outsource AppSec functions
  - Easier to manage
  - Less risk of the wrong pick
  - HR will be grateful

Miser pays twice

- attempts of saving money by aggregating everything in one DevSecOps role will likely result in spending more resources with no positive impact on product security

- DevSecOps is a feasible concept.
- DevSecOps engineer is a phantom chimera.




ON
FF
ONE
2022
ANGARA
SECURITY