DevSecOps Worst Practices

Tanya Janca
Head of Community and Education
What are we going to talk about today?

DevSecOps
What are we going to talk about today?

Tried, tested and FAILED Approaches
What are we going to talk about today?

How and why to avoid these problems
Let’s go!
Your Nerd: Tanya Janca

AKA SheHacksPurple

- Head of Education and Community at Semgrep
- Author: Alice and Bob Learn Application Security
- 27+ years in tech, Sec + Dev
- Advisor: Katilyst, NordSec
- Faculty: IANS Research
- Previous: Counterterrorism, CISO of Canadian Election, Pentester, Microsoft, startup founder, developer, AppSec Nerd
“You did what now?”
My definition of DevSecOps:
An AppSec person who works in a DevOps Shop.
A more common definition of DevSecOps:

The AppSec person who owns tooling in the CI/CD
DevSecOps isn’t easy, and sometimes it goes poorly. People rarely share WHY.
#1

The Boy Who Cried Wolf...
Artificial Gates

Instead of creating a policy to create a gating process, you abuse the CI/CD to "make your own" gate.
#4

Missing Test Results
Run Away Tests...
Using up all the resources, so that no one else can run tests.
Impossible SLAs
Untrained Staff
Forgotten Bugs

“Don’t worry Tanya, it’s in the backlog.”
No Positive Reinforcement

Negative Nellys, everywhere!
Only worrying about YOUR Part!
#11

Multiple Bug Trackers
Insecure SDLC
Overly Permissive CI/CD

Some employees will disable tests in order to ‘get to prod’.

Lock this down!
Automation **ONLY** in the CI/CD

We should automate every chance we can get!

(This tends to happen only if the AppSec person was never a dev.)
Hiding Mistakes and Errors

How can we learn if we never share information?
We Learned:

• Some people learn best from what went wrong and understanding the ‘why’
• How to see DevSecOps ‘from the other side’, so that we can do better
• Several strategies for better roll outs!
Resources
PDF Summary

https://newsletter.shehackspurple.ca/
DevSecOps-Worst-Practices
Resources: Semgrep!


Semgrep Academy!

https://academy.semgrep.dev/
Resources: Meeeeeeeeee!

@SheHacksPurple

Twitter/TikTok/Mastodon/GitHub/Instagram/etc.

YouTube.com/SheHacksPurple

https://SheHacksPurple.ca/blog

https://Newsletter.SheHacksPurple.ca
THANK YOU

Tanya Janca
Semgrep
SheHacksPurple.ca