

Adding DAST to CI/CD

CONF42

Tanya Janca
Director of DevRel & Community
Bright Security

I ADDED DAST
TO THE CI/CD

IT'S TOO SLOW!



Adding DAST to CI/CD, *Without Losing Any Friends*

Tanya Janca
Director of DevRel & Community
Bright Security

Tanya Janca

About Me

- Director of Developer Relations and Community at **Bright**
- CEO & Founder @ We Hack Purple
- AKA @SheHacksPurple
- Author: **Alice and Bob Learn Application Security**
- Advisor: Nord VPN, Cloud Defense, Aiya Corp.
- 25 years in tech, Sec + Dev
- Blogger, Podcaster, Streamer, Builder, Breaker
- Nerd at Large



What Problem Are We Solving?



Insecure Software is causing data breaches all over the world.



What Problem Are We Solving?



DevOps Requires:

- Accuracy
- Speed
- Automation



What Problem Are We Solving?



DevSecOps Requires:

- Testing from multiple angles
- Good relationships between sec, dev + ops
- Fixing bugs as soon as possible in the SDLC



What is DAST?



Dynamic Application Security Testing





Why
DAST?

What is DevOps?



(it's not paying one person to do two jobs, Dev and Ops)



CI/CD and DevOps – a review

- CI/CD means pipeline software, to test and release software and infrastructure
- DevOps Requires:
 - Efficiency for the entire system (not just your part)
 - Fast Feedback (that is accurate, and gets to the right people)
 - Continuous learning and improvement
- **Not all security testing needs to be in the pipeline!**



Let's Talk Strategy



For DAST
in a CI/CD






Run Your DAST
on Full Blast

And lose all
your friends...

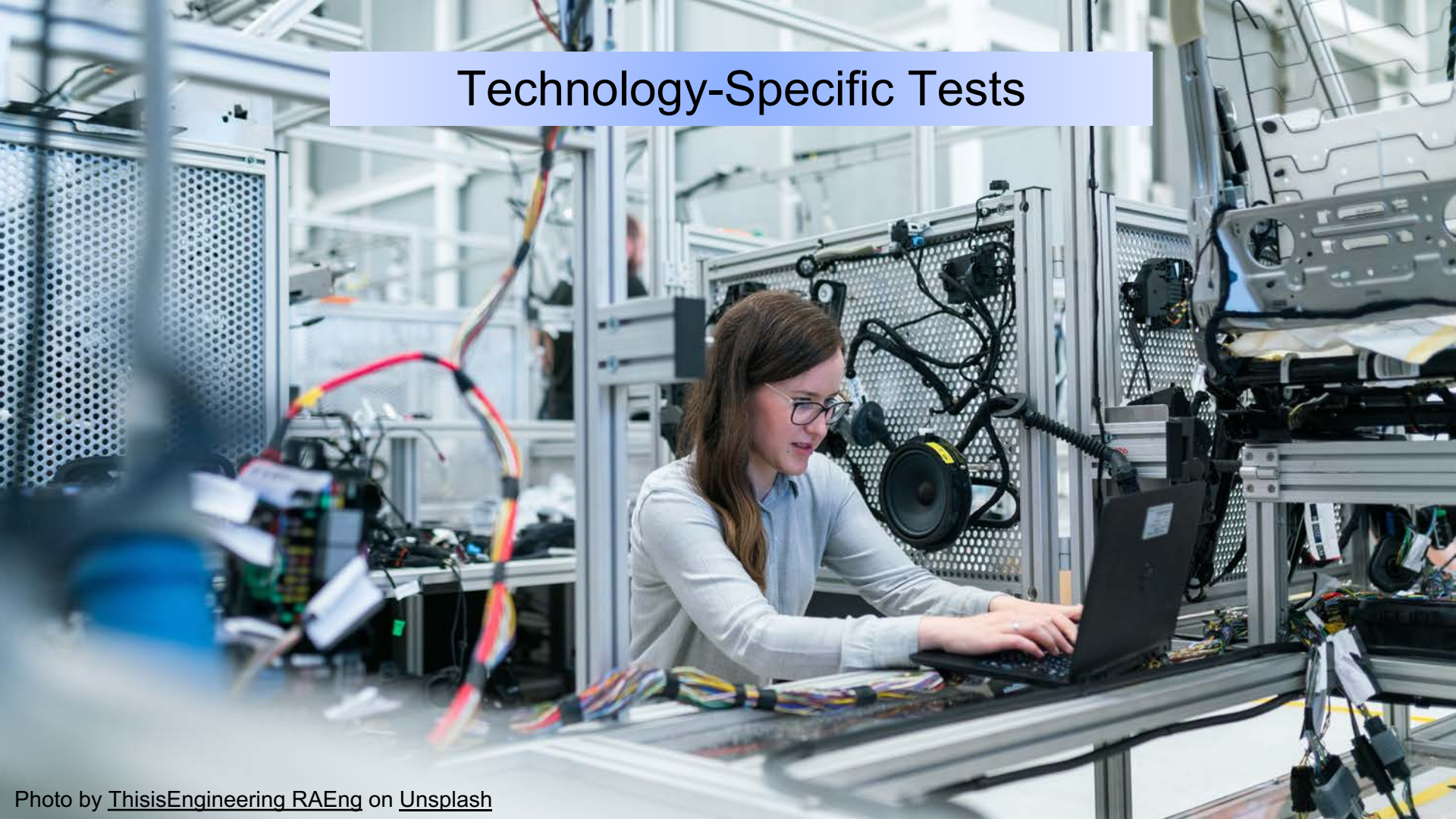


Refine Your Scope, Using a HAR File

A photograph of a sunset or sunrise. The sky is a gradient of colors from light blue at the top to orange and yellow near the horizon. In the foreground, there are several trees in silhouette. On the left, there are bare, spindly trees. In the center, there is a tall, full pine tree. On the right, there is another bare tree. The overall mood is serene and contemplative.

Only Test What Worries You

Technology-Specific Tests




Testing APIs

(tips)

You don't have to put everything in the CI/CD to do DevOps.



Scheduled,
Automated,
Regular
Scanning



1-off or Manual Scans

Penetration Testing



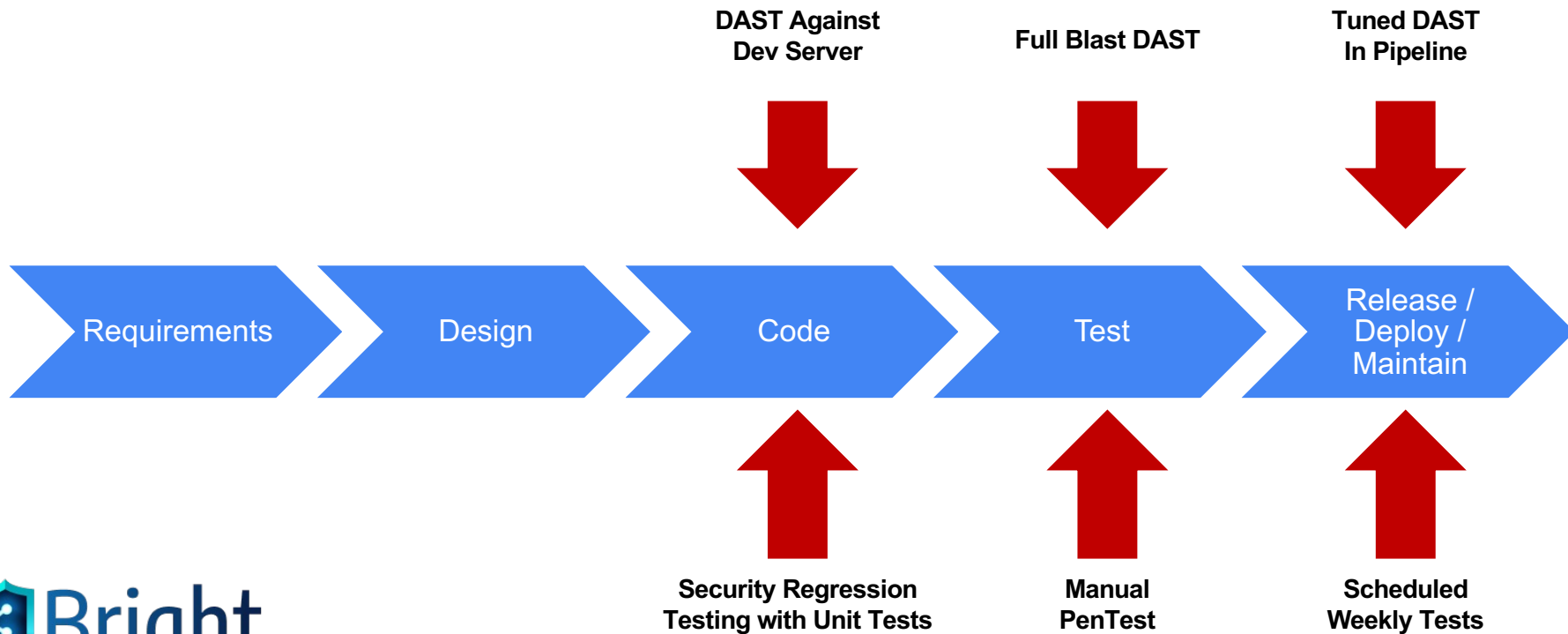
Other
Tests

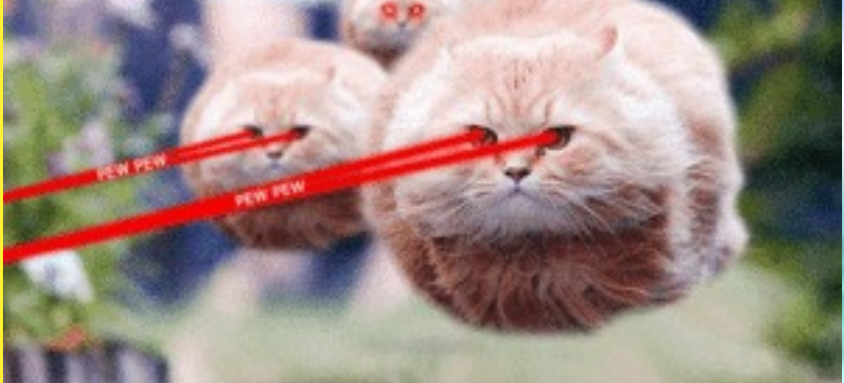
SAST
SCA
IAST
Secrets



DAST in the SDLC

Dynamic Scanning





Conclusion

- We must do dynamic testing
- Automation is our friend
- Dynamic testing in a pipeline must be fast and accurate
- We can do dynamic testing outside the pipeline, and still be DevOps-friendly
- Other types of testing are still needed to find as many vulnerabilities as possible
- The people from Bright can be rather silly





Resources!





I have a podcast!!!!!!

We Hack Purple Podcast, season 2, offers short security lessons and best practices! Watch it on YouTube or subscribe on any podcast platform.



youtube.com/WeHackPurple



Awesome Books!

42

- The DevOps Handbook
- The Phoenix Project
- Accelerate
- The Unicorn Project
- Alice and Bob Learn Application Security





Join the community!!!!!!

The We Hack Purple
Community is FREE!

Community.WeHackPurple.com



Meet like-minded people and nerd out!



Every Monday!

#CyberMentoringMonday





Resources: Bright!!!!



<https://BrightSec.com/blog>





Resources: ME!!!!

Twitter: @SheHacksPurple

<https://SheHacksPurple.ca/blog>

<https://YouTube.com/SheHacksPurple>

<https://NewsLetter.SheHacksPurple.ca>



CONF42



THANK YOU

Tanya Janca
DevRel @ Bright
We Hack Purple

