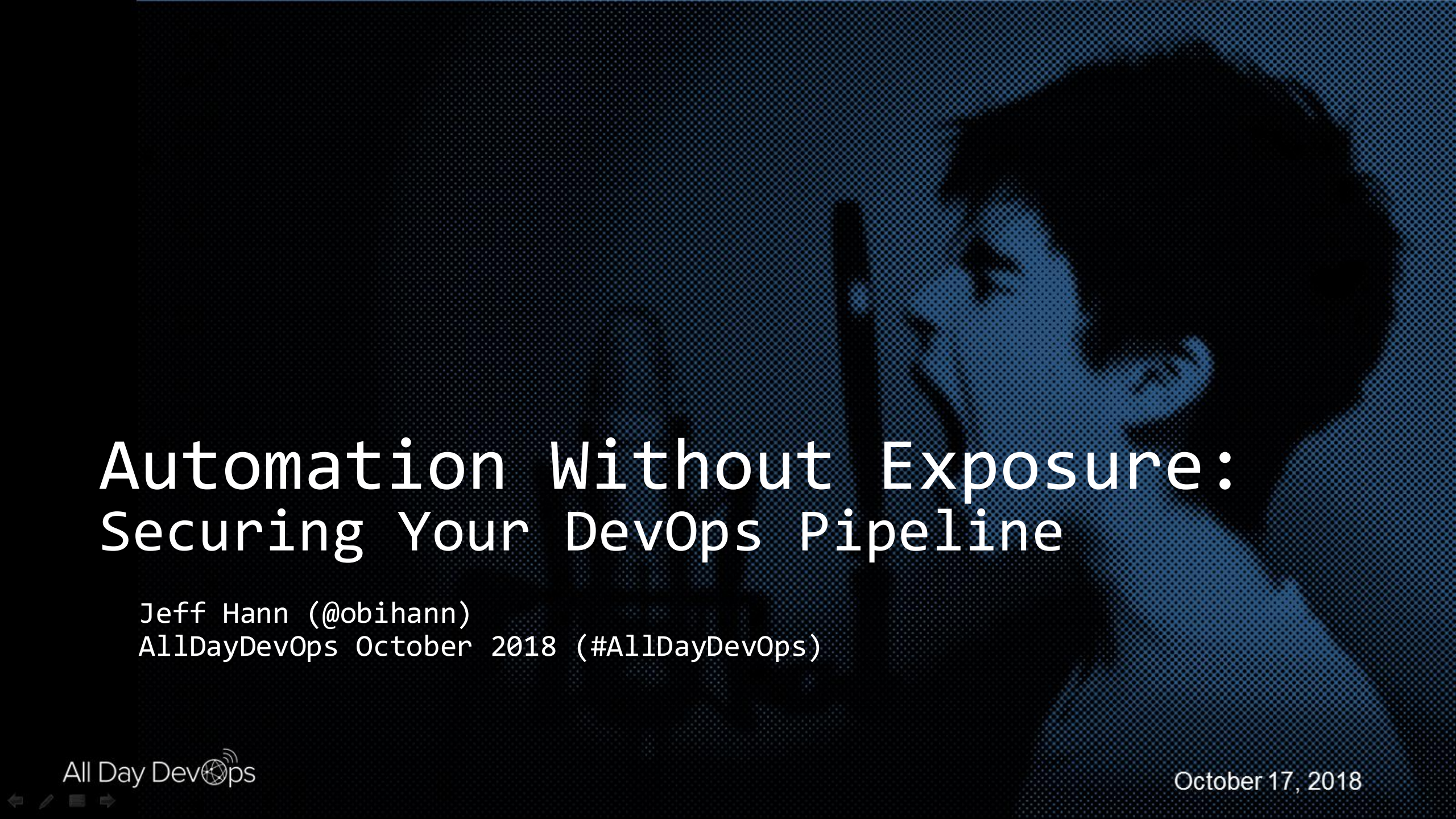


Automation Without Exposure: Securing Your DevOps Pipeline

Jeff Hann (@obihann)

AllDayDevOps October 2018 (#AllDayDevOps)

All Day DevOps

October 17, 2018

My Experience

- Over a decade in development (backend, frontend, mobile)
- Two years in DevOps (focused on CI and automation)
- Now a Security Engineer (works directly with engineering and architecture teams)

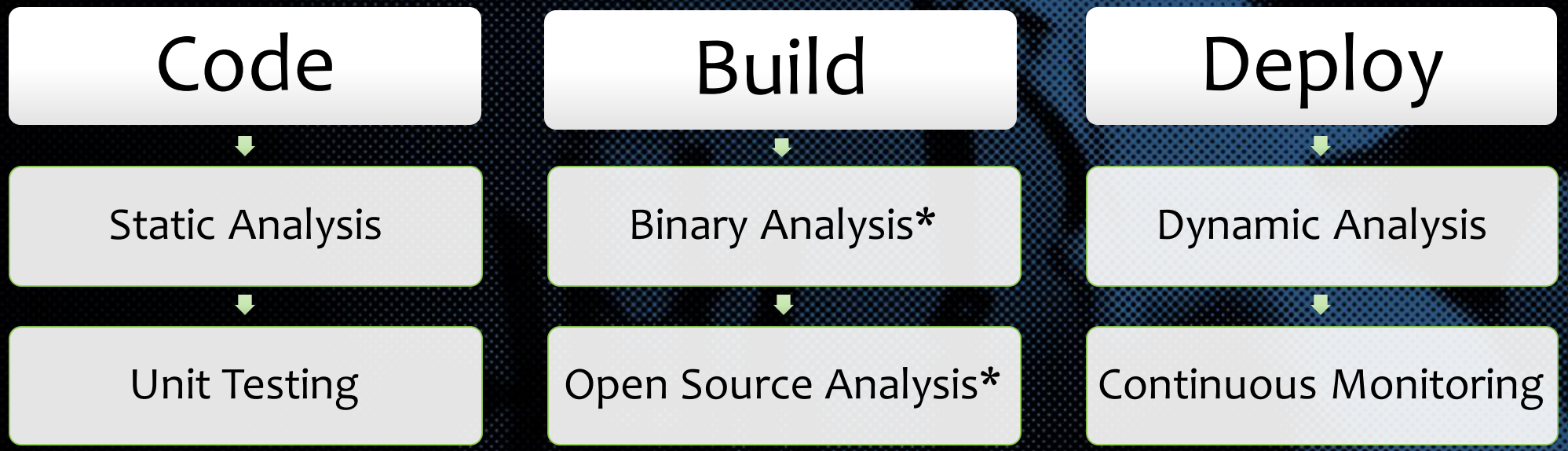
DevSecOps... SecDevOps... OpsSecDev?

In today's agile world, we have less time between releases than ever before, and this crunch is often felt by security more than any other team. The risk of a breach due to a rushed product is high but the risk of lost profit due to a missed launch is far higher, so how do we prevent both? Using the same techniques we used to automate our builds and releases we can automate our security testing.

- Pipelines (Are they the enemy?)
- Feedback Loops and Echo Chambers (What you don't know can't hurt you)
- Education Through Automation
- Automation Induced Anxiety (so many reports, somebody make it stop)

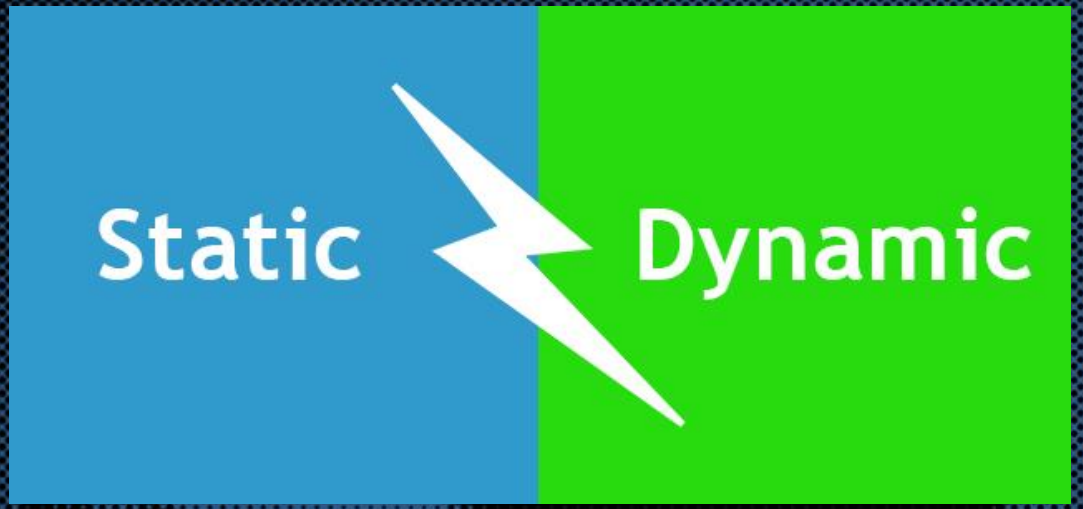
Pipelines (Are they the enemy?)

Fantastic Tools and Where to Deploy Them



Code Analysis

- Linting
- Static Application Security Testing (SAST)
- Binary Application Security Testing (BAST)
- Open Source Analysis or Dependency Analysis
- Dynamic Application Security Testing (DAST)



Jonny opened the door to the one place he always heard the truth.

Feedback Loops and Echo Chambers

If we never allow feedback, ideas, or processes we are stuck with a constant echo of our own praise

Feedback Loops and Echo Chambers

- By introducing multiple methods of testing throughout the build and release process we provide our team blunt and honest feedback
- Too often this feedback thought of as a road block and turned into a checklist of extra work required to launch
- Treat each piece of information found as a training opportunity, help your team resolve the issue and advance their skills

Education Through Automation

Education Through Automation

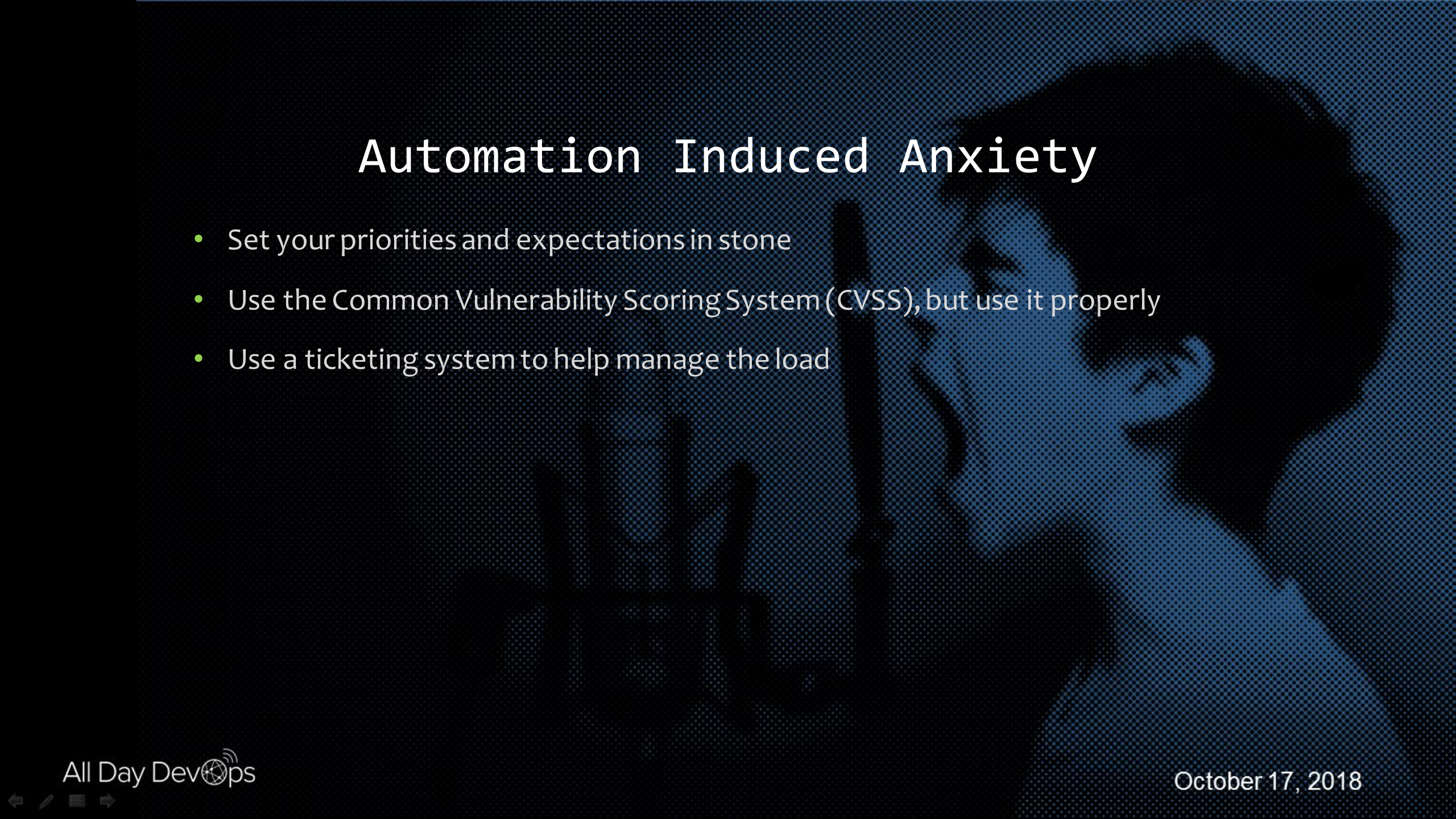
- It is very easy to just “fix” a bug via acceptance or mitigation, but then it will happen again and again
- Most good tools will provide some form of explanation on the bug as well links to third party sources to help learn more about them
- Keep track of bugs that pop up regularly and on a annual basis introduce some form of training (conferences, local meet-ups, lunch and learn, e-learning) that focuses on these topics

Automation Induced Anxiety

Ah! Yeah. It's just we're putting new coversheets on all the TPS reports before they go out now. So if you could go ahead and try to remember to do that from now on, that'd be great. All right!

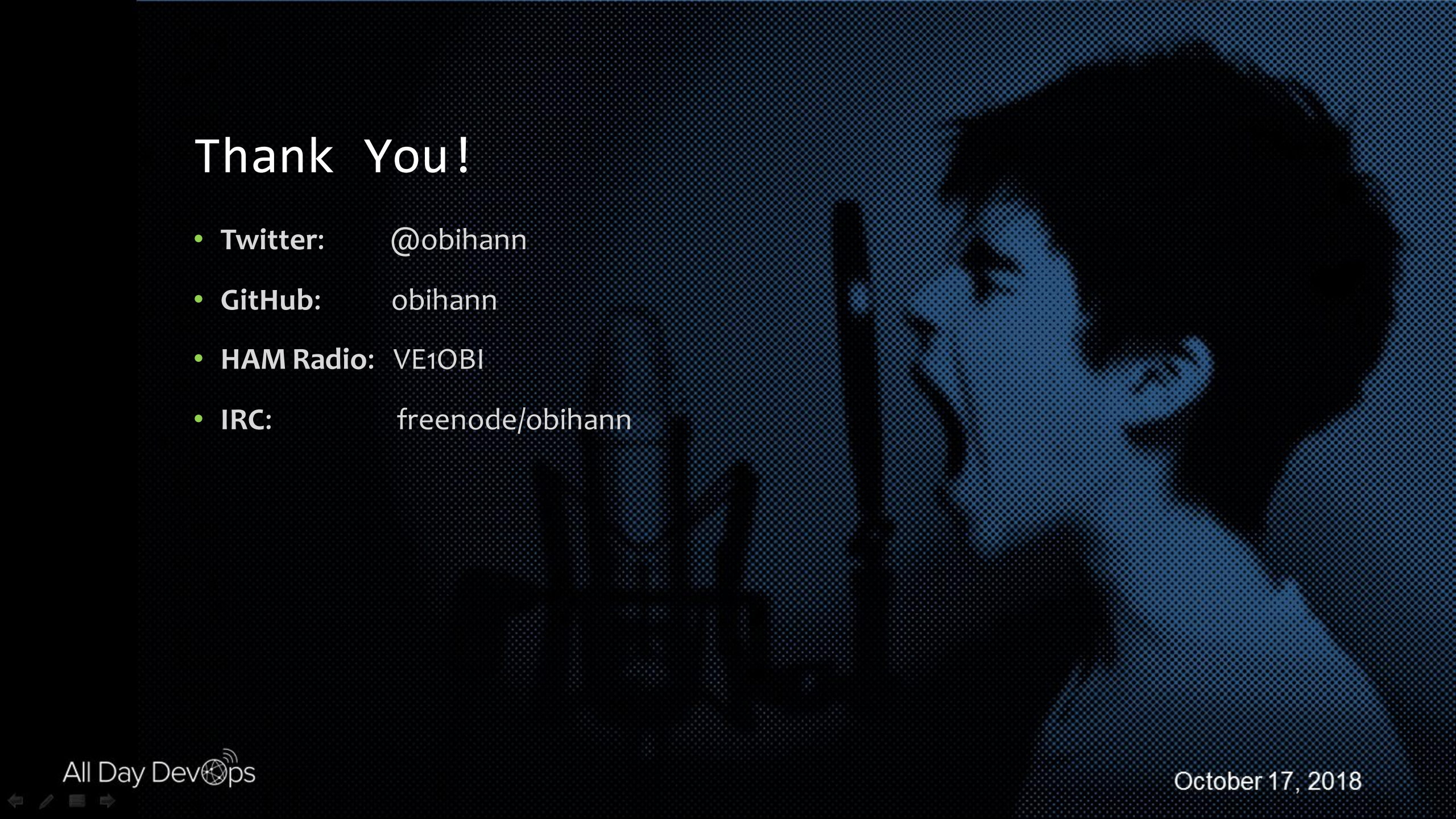
All Day DevOps

October 17, 2018



Automation Induced Anxiety

- Set your priorities and expectations in stone
- Use the Common Vulnerability Scoring System (CVSS), but use it properly
- Use a ticketing system to help manage the load



Thank You!

- **Twitter:** @obihann
- **GitHub:** obihann
- **HAM Radio:** VE1OBI
- **IRC:** freenode/obihann

Thank You All Day DevOps Sponsors

Platinum Sponsors

Sonatype

cloudbees

Gold Sponsors

puppet

GitLab

XebiaLabs
Enterprise DevOps

GENERAL DYNAMICS
Information Technology

cisco DEVNET
developer.cisco.com

Carnegie Mellon University
Software Engineering Institute

CHEF

SCALED AGILE

Media Sponsors

TechBeacon

DevOps.com

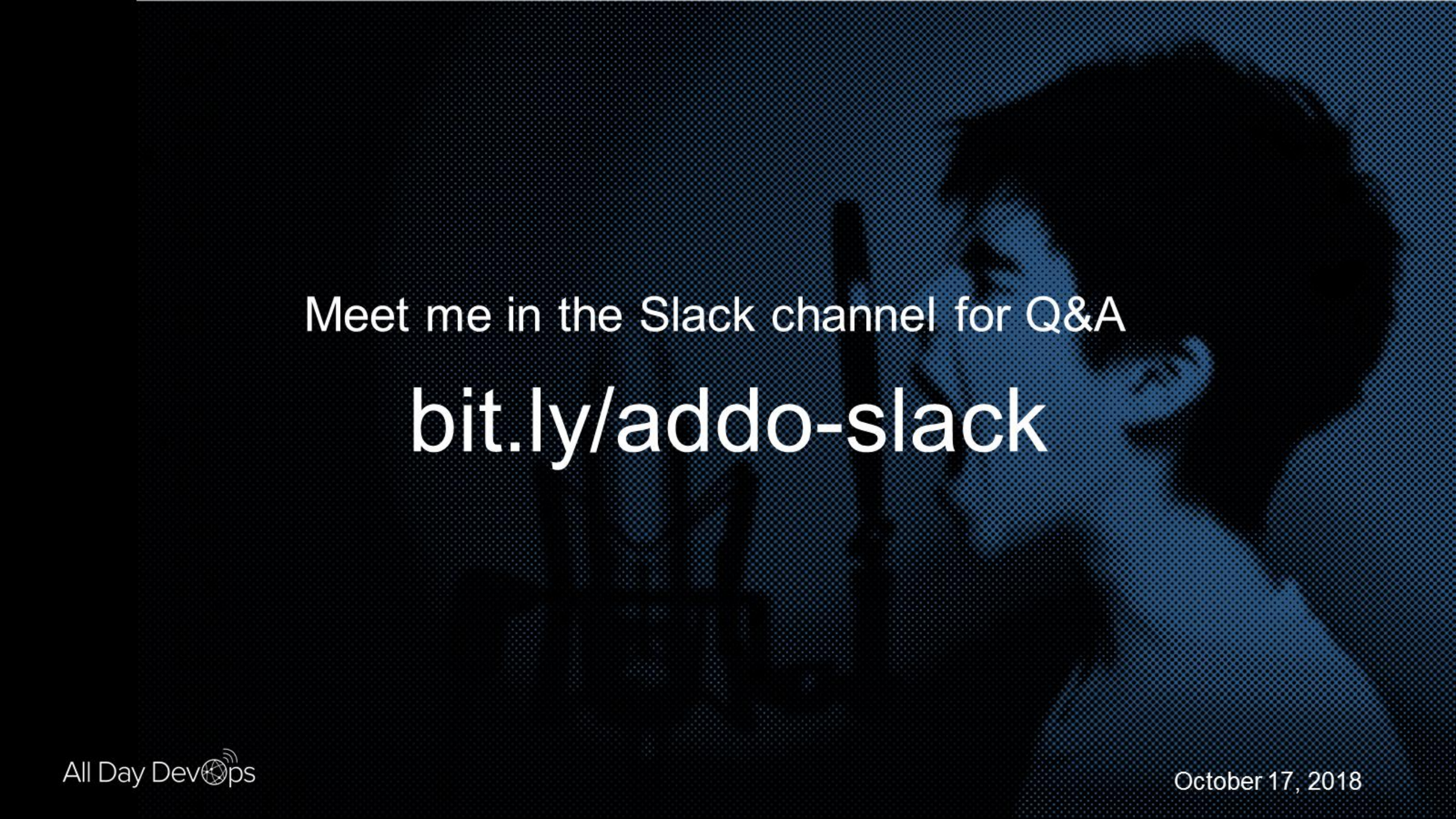
DZone

Solutions Review

Thank You All Day DevOps Supporters

Links and Resources

- [Resource] OWASP AppSec Pipeline - https://www.owasp.org/index.php/OWASP_AppSec_Pipeline
- [Resource] Awesome DevSecOps - https://github.com/devsecops/awesome-devsecops
- [Education] Hacksplaining - https://www.hacksplaining.com/
- [Education] Hacker101 - https://www.hacker101.com/
- [Education] Cybrary - https://www.cybrary.it/
- [Resource] CVSS - https://www.first.org/cvss/specification-document
- [Education] - WebGoat - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- [Education] DecSecOps Bootcamp - https://github.com/devsecops/bootcamp


Meet me in the Slack channel for Q&A
bit.ly/addo-slack
All Day DevOps
October 17, 2018