DevOps Security:
Ignore It As Much As You Would Ignore Regular Security
DevOps security?
What is “DevOps security”?

“DevOps security” isn’t a thing. We’re talking about minding your security in the context of the cultural and technological shift toward DevOps.
Poll: At what point do you consider security?

A) At the very beginning  
B) Sometime in the middle  
C) Toward the end  
D) Not at all
Is DevOps, itself, a security problem?

- Automation
- False sense of security, about security
- Security as a fourth arm to DevOps
- Docker
- Using DevOps principles for security analysis
- Security and everyone but you
Automation

- Increased attack surface with added third-party tools and services, each with additional scripts and configuration

- Straightforward to automate a manual process, but easy to leave behind all the paranoia you had when you wrote that manual process

- Not everything needs to be, or should be, automated

- Tip: draw perimeters around things you trust and let that guide where human interaction and verification is needed
False sense of security
(security about security)

- DevOps makes everything better, so relax
- Application code is stronger, but infrastructure just blew up
- Continuous integration sabotage
How to Security, DevOps-like

- Do have a security team, with domain expertise
- Don’t merge the security role with development, operations, or QA roles
- Do include the security team and collaborate with them from Day 1
- Do generate security tests with every change
- [https://www.ruggedsoftware.org](https://www.ruggedsoftware.org)
- [http://gauntlt.org](http://gauntlt.org)
Poll: Does your organization have a dedicated security role?
Docker as an attack vector?

Containers
- Could have access to the root of the host file system
- Kernel namespaces help isolate containers

The Docker daemon
- The daemon must run as root
- Multi-tenant systems share the daemon
- Control over the daemon is control over all containers

The Docker registry
- Anyone can post an image
- No checking is done to enforce the security of images
Poll: Do you use Docker?
Docker Wrangling

- Use certificates for registry access
- Be mindful of what services run as what users and with what permissions
- Don’t assume images downloaded from the registry are safe to use without close inspection first
- Be mindful of how third-party hosts operate with Docker and other containerizing or virtualization technologies – your code may not be where you think it is
How to Security Analysis, DevOps-like

- Are there security signals in your feedback loop?
- We want to quantify security analysis results, but there is a particular difficulty in quantifying security
- Cannot always get actionable results from automated security tests
- Cannot always respond in an automated way to security issues
Security and everyone else

Interaction with customers to identify their goals is necessary to determine what is important to them in terms of \( x \).

- Let \( x \) be security
  - Your security focus can break the thing they need to work
  - What they need to work can break without security
  - Build value for them based on this relationship between what they need and the security you can provide
Join the new SEI DevOps Forum on LinkedIn