

# Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use ([www.sei.cmu.edu/legal/](http://www.sei.cmu.edu/legal/)).

© 2015 Carnegie Mellon University.

# Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

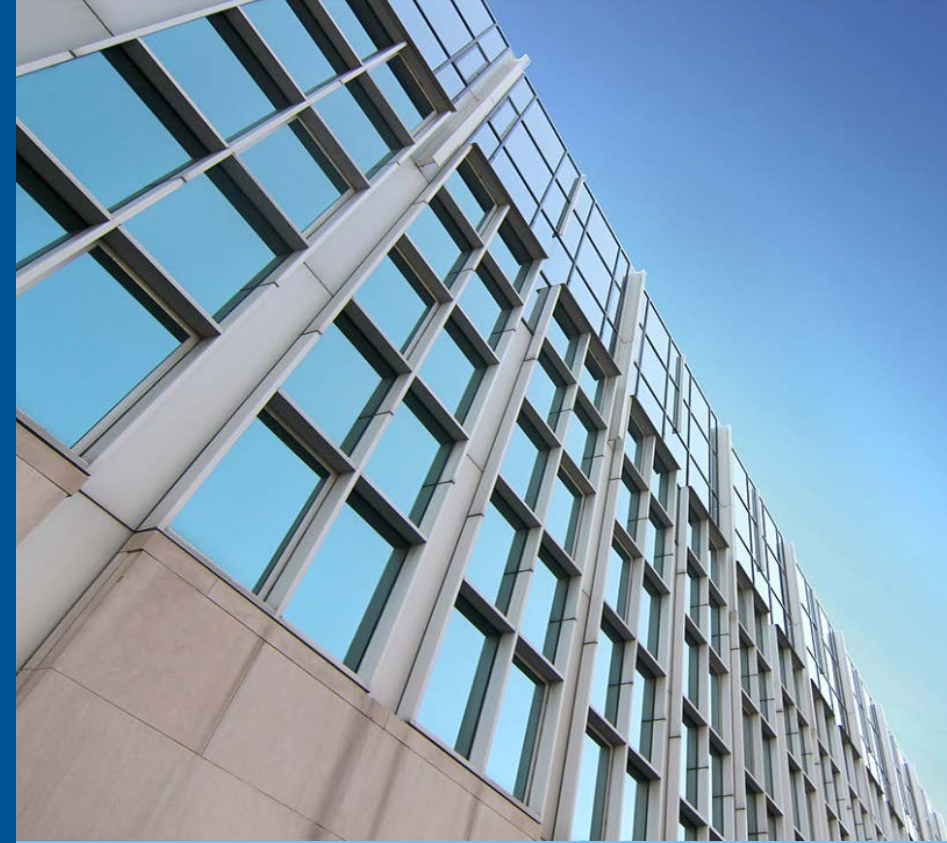
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

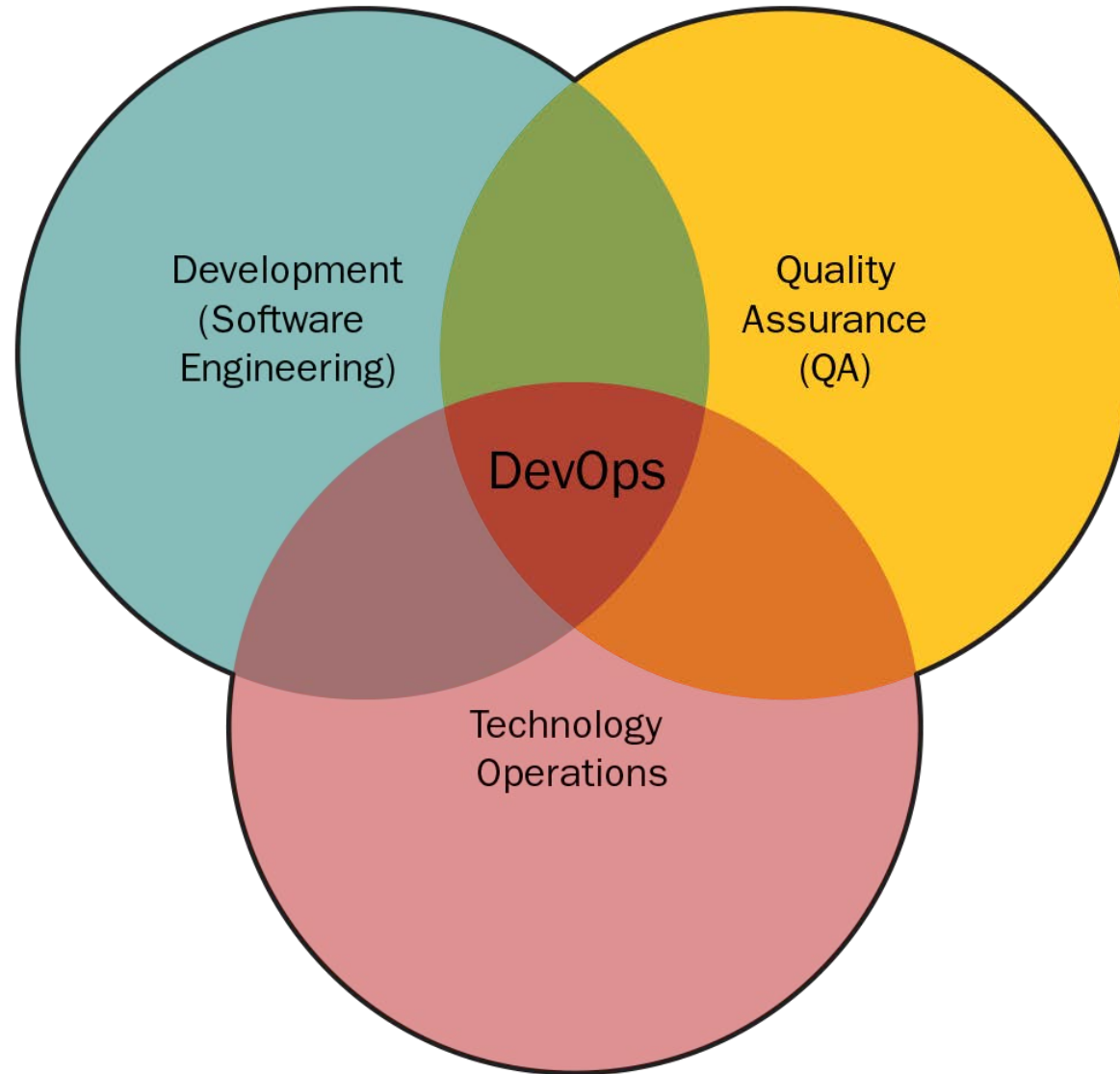
DM-0002664

# 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>
- <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

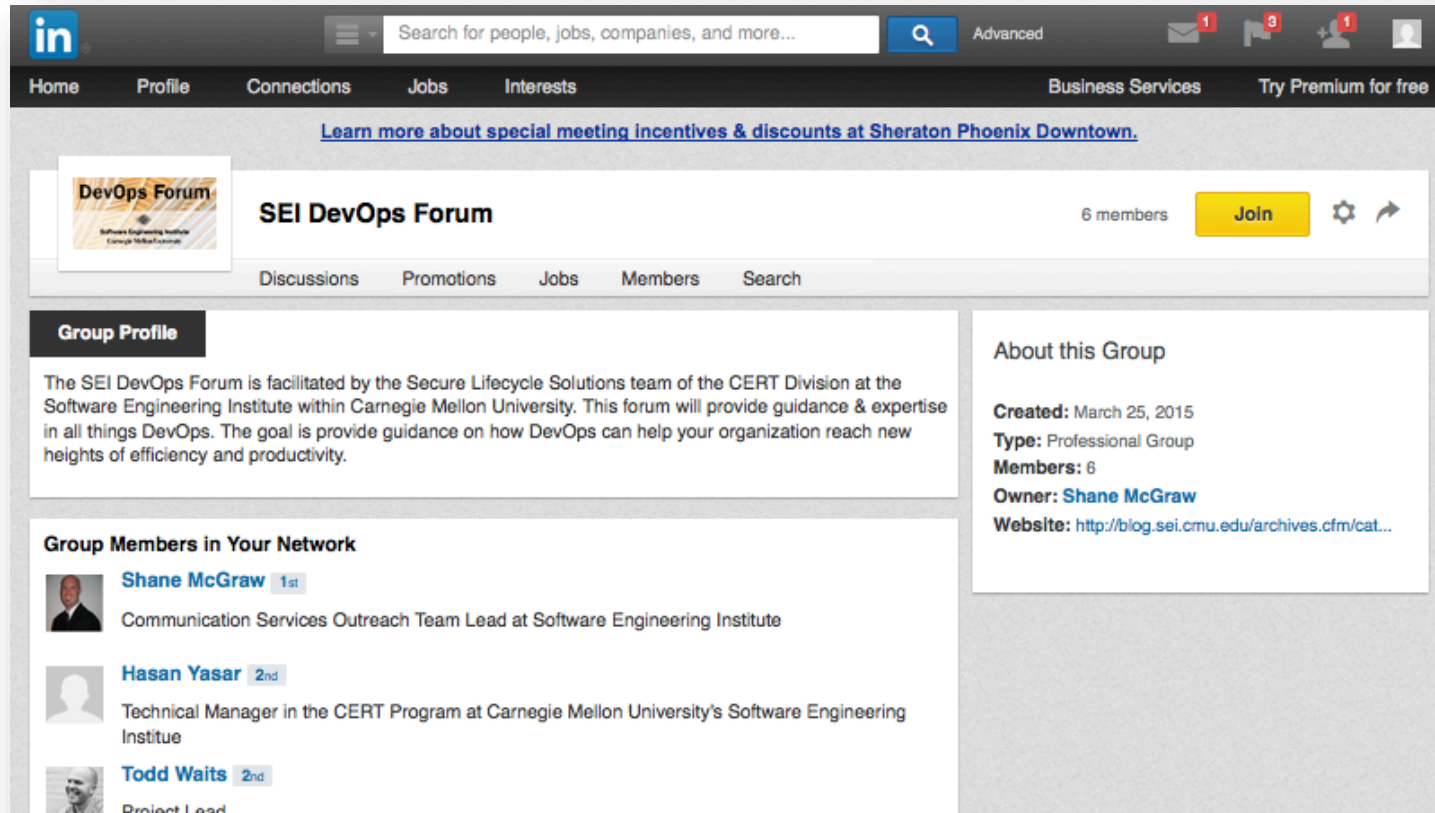
Interaction with customers to identify their goals is necessary to determine what is important to them in terms of x.

- 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



# Q&A

## Join the new SEI DevOps Forum on LinkedIn



The screenshot shows the LinkedIn profile for the SEI DevOps Forum. At the top, there is a search bar and navigation links for Home, Profile, Connections, Jobs, and Interests. Below the navigation is a banner for a special meeting at Sheraton Phoenix Downtown. The main header for the group includes the group name "SEI DevOps Forum", a "Join" button, and a "6 members" indicator. Below the header are tabs for Discussions, Promotions, Jobs, Members, and Search. The "Group Profile" section contains a description: "The SEI DevOps Forum is facilitated by the Secure Lifecycle Solutions team of the CERT Division at the Software Engineering Institute within Carnegie Mellon University. This forum will provide guidance & expertise in all things DevOps. The goal is provide guidance on how DevOps can help your organization reach new heights of efficiency and productivity." To the right, the "About this Group" section lists: "Created: March 25, 2015", "Type: Professional Group", "Members: 6", "Owner: Shane McGraw", and "Website: http://blog.sei.cmu.edu/archives.cfm/cat...". The "Group Members in Your Network" section lists three members: Shane McGraw (1st), Hasan Yasar (2nd), and Todd Waits (2nd).