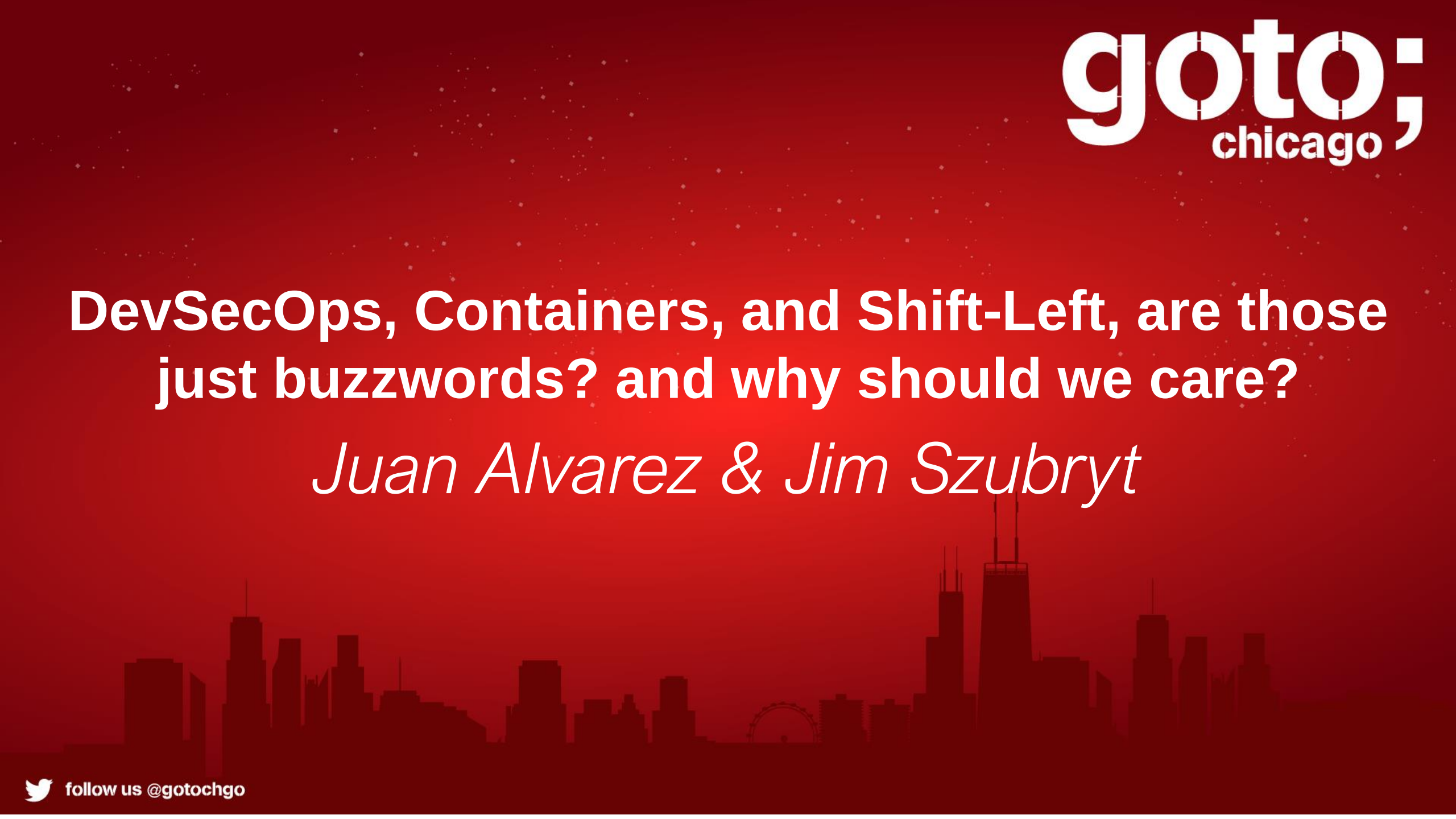
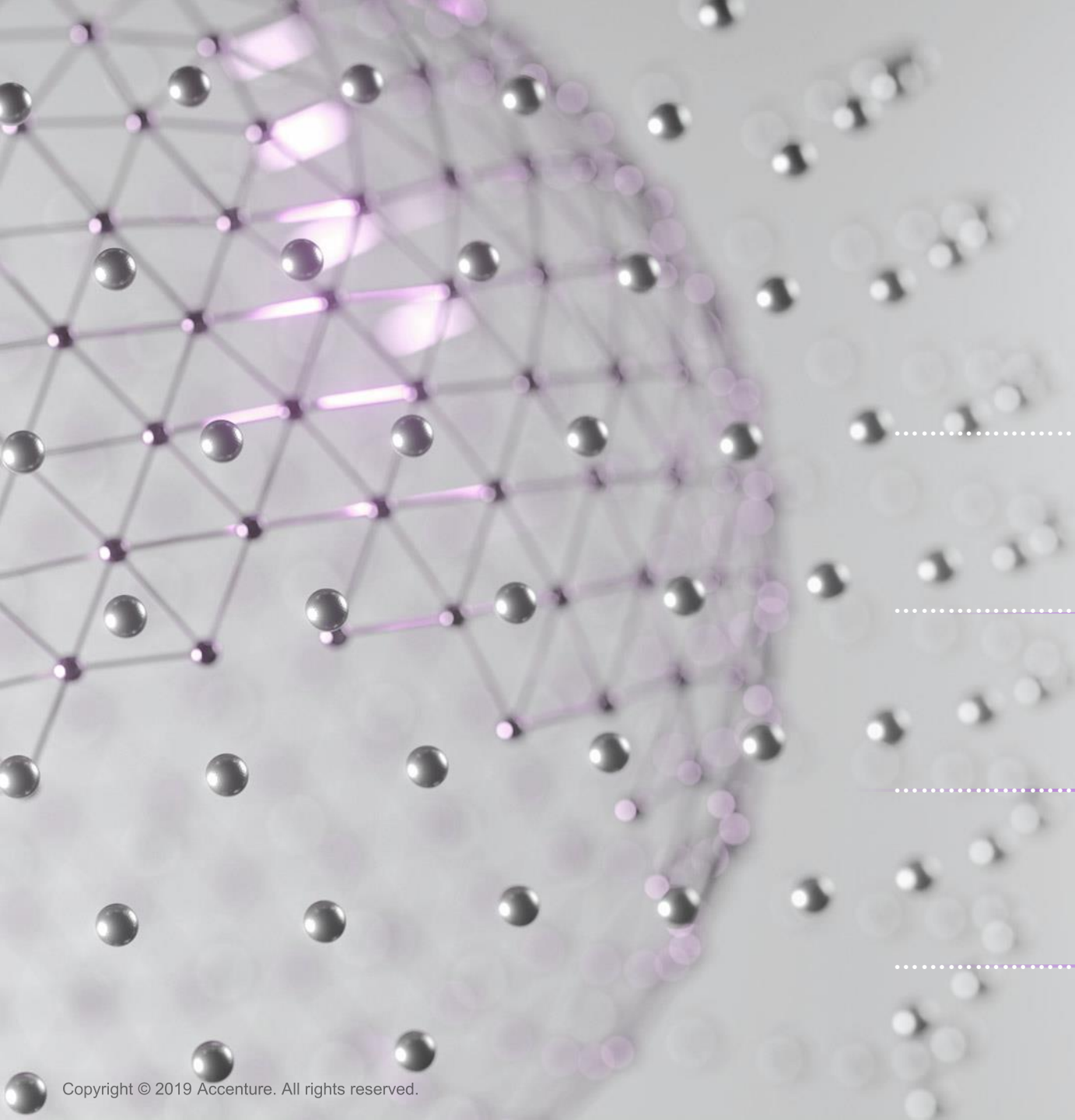

goto;
chicago
DevSecOps, Containers, and Shift-Left, are those just buzzwords? and why should we care?
Juan Alvarez & Jim Szubryt
follow us @gotochgo

goto; chicago

Click ‘Rate Session’
to rate session
and ask questions.

follow us @gotochgo



ACCENTURE TODAY

469,000
Employees

200
Cities in 52 Countries

$41.0B
(US) Revenues

6,000+
Clients in 120+ Countries

QUICK FACTS

DIGITAL WORKER

Devices

462K
Workstations deployed

Windows 10

436K
Migrated devices

Mobile

140K
Smartphones/ tablets/PCs enrolled in mobile device management

Teams

110K
Teams

287K
Active users

14.2M
Chat messages/ month

Skype

328M
Audio minutes/ month

17M
Video minutes/ month

Accessibility

53%
of interactions with CIO software are accessible

75%
FY19 target of interactions with CIO software to be accessible

Collaboration

1.4M
Searches executed/month

307K
Documents downloaded from knowledge repository/month

Broadcast

294
Events produced/month

2.2M
Minutes of streamed videos/month

O365

1.8B
Files stored in OneDrive for Business

5.3PB
of data in OneDrive for Business

514K
Mailboxes

14.4K
SharePoint sites

43K
Power BI users

QUICK FACTS

PLATFORM

>93% of Accenture applications are supported by the platform economy

Microsoft Azure
amazon web services™
Office 365
salesforce
SAP HANA
servicenow
SAP SuccessFactors
SAP Ariba

Virtual Machines

10.2K
Operating system instances in the public cloud

2.2K
Servers managed in Accenture's private cloud

BEHIND THE SCENES

Digital | Fortified | Secure

Network

881GB
of network capacity

14K
Wireless access points

Analytics

148TB
of enterprise data

171
Digital products

22 AI Models
75 Predictive Models

Cloud Footprint

>93% Today

INTRO

Juan Alvarez an Enterprise Architect in Accenture's Internal IT organization

Juan is an Enterprise Architect in Accenture and has over 2 decades worth of experience working in a variety of roles in IT. Currently, Juan is focusing on using DevOps principles and Cloud-Native technologies to transform the way Accenture Delivers software. He is a member of the Google Cloud DevOps Technical Advisory Council. He also is the Accenture Chicago Hispanic American ERG Lead and passionate about inclusion and diversity in technology. He currently lives in Chicago and is a graduate of the University of Wisconsin – Madison with a B.S. degree in Mathematics.

Jim Szubryt an Enterprise Architect in Accenture's Internal IT organization

Leading container platform including standardizing, deploying, securing & monitoring all of the components it takes to run an enterprise container platform

Past roles include running TFS, adoption of automated deployments, adoption of automated testing, cloud architecture and Disaster Recovery

Speaker at Microsoft Build on containers, Microsoft Ignite on DR, multiple VS Lives on ALM/DevOps and many of the Chicago user groups

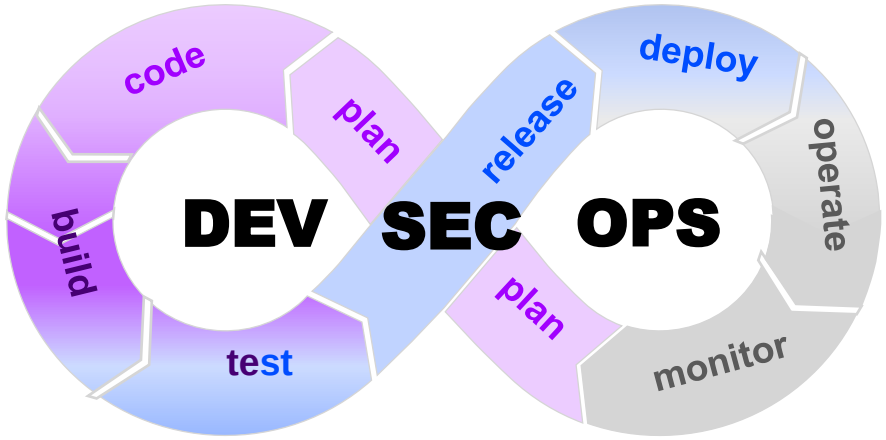
Microsoft ALM Ranger since 2011 and was a Microsoft ALM MVP from 2013 through 2018

MODERN APPLICATION DELIVERY CONCEPTUAL DELIVERY PIPELINE

Source Control Management

Application | Policy | Data Infrastructure | Configuration

Heart of the Delivery Pipeline using:
- Branching Strategy
- Check-in Policies
- Self Documenting
- ETE Traceability



Continuous Integration

Quality Scans| Security Scans Builds | Unit Testing | Package

Create and package a release.
Perform initial testing and compliance checks of a build

Continuous Delivery

Release Management | Deploy Continuous Testing | Compliance

Deploy to pre-prod and prod environments:
- Zero downtime | Blue/Green | Canary

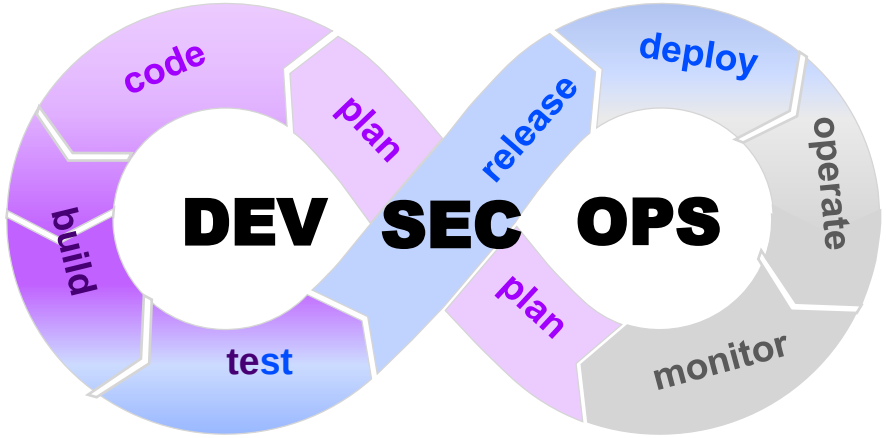
Functional, performance, security testing
Quality Gates

Automated Operations

Monitoring | Logging | Insights Self Healing | Auto Scaling

Ensuring uptime.
Mechanism for Continuous Improvement feedback into the Delivery Pipeline.

DEV <*> OPS



Why DevSecOps?

Everything is Versioned

Traceability is an enabler. It ties changes to events all along the pipeline.

Integrate * with the Delivery Pipeline

Security is built into how we deliver our services

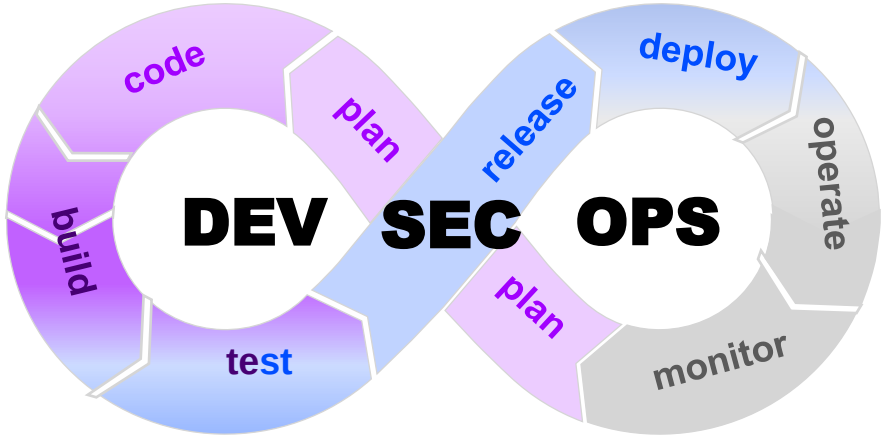
Test * earlier and always

Test continuously to catch vulnerabilities along each step of the way.

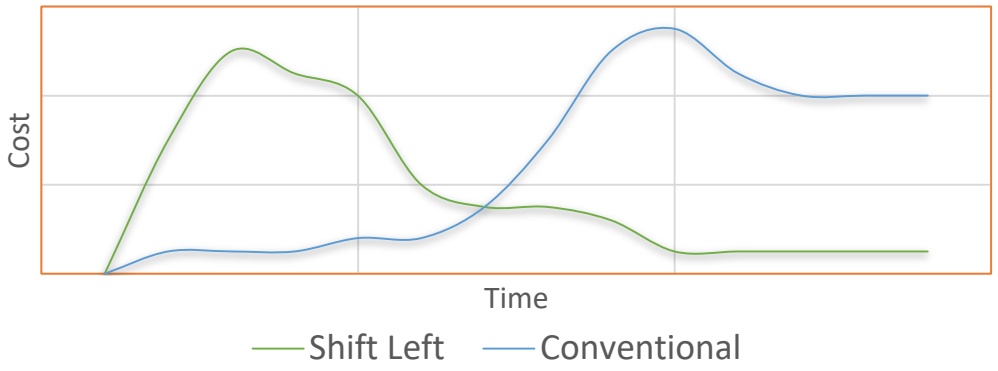
Bring * in front of Developers

Bring the visibility to our development teams – learn about how to develop securely.

SHIFT LEFT



Security Issue
Detection Differentiation



Moving Quality, Security, Compliance earlier in the Delivery Pipeline

Source Control Management

- Application
- Policy
- Data Base
- Infrastructure
- Configuration

Continuous Integration

- Quality Scans
- Security Scans
- Builds
- Unit Testing
- Package

Continuous Delivery

- Release Management
- Deploy
- Sec |Func | Perf Test
- Compliance

Automated Operations

- Monitoring
- Logging
- Insights
- Self Healing
- Auto Scaling

The idea is simple… the earlier in the development process (Delivery Pipeline), the less work and effort (i.e. cost) required to fix a quality or security problem and enforce compliance

CONTAINER ENGINEERING IN ACCENTURE CIO

Our Goal

- Enable legacy .NET apps to move to Windows Containers running on Azure Service Fabric
- Meet Info Sec requirements for a secure platform
- Minimize hosting spend
- Significantly reduce effort patching and managing vulnerabilities

Our approach

- Build core team of Container Engineers
- Create reusable assets that teams can use to easily move to containers
- Enable application modernization

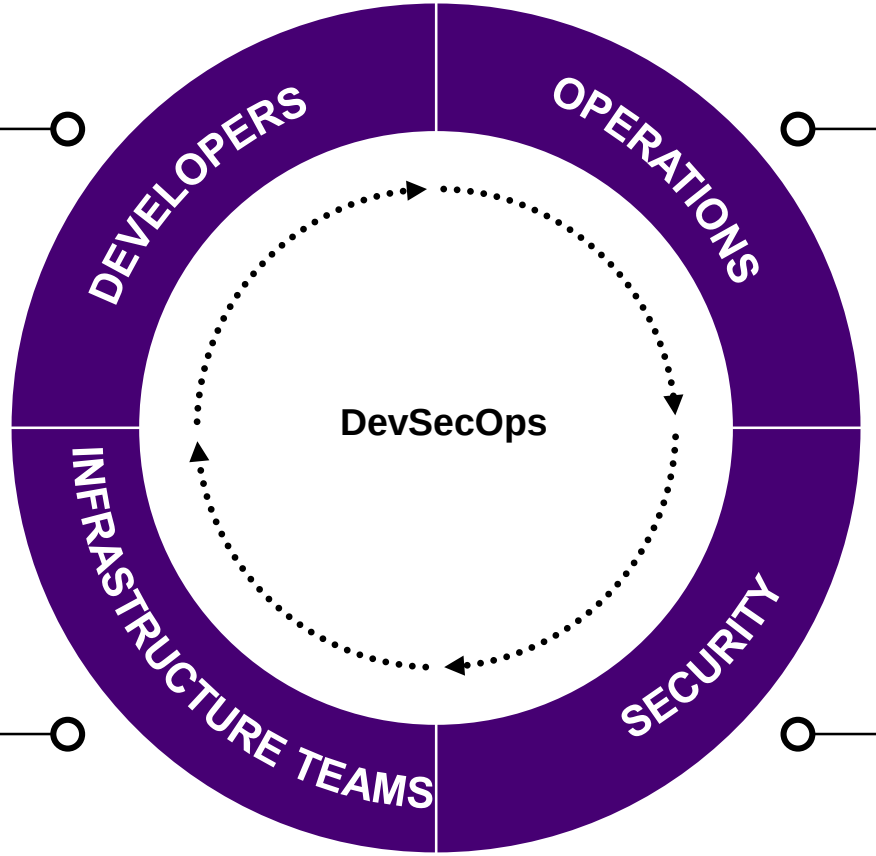
WHAT DO CONTAINERS MEAN FOR US

DEVELOPERS

- No longer need to concern themselves with underlying servers; ability to run anywhere
- Repeatable environment deployments; no surprises due to standardization
- Rapid deployment; getting a new PoC environment is minimal
- Accelerated delivery of app features to business

INFRASTRUCTURE TEAMS

- No more provisioning of servers; can focus on more value-added tasks
- Infrastructure as code; scripted, versioned and testable



OPERATIONS

- Automated rollouts and rollbacks across multiple upgrade/fault domains
- Service health monitoring
- Automatic scaling of services
- Ability to deploy anywhere, including hybrid cloud environments
- Centralized logging (performance, web and custom)

SECURITY

- Ability to identify security vulnerabilities as part of the dev process (DevSecOps)

SECURE DEVELOPMENT LIFECYCLE PATTERN

Developers
- Create Docker file
- Create containers build
- Configure for deployment
- Check in to trigger build and deploy

Code

Build

Artifact Repository

App Container Registry

Deploy

Environments

Monitoring

1

2

3

Pull image to push to environment

Scan image daily

Base image

Base Image Container Registry

Scan image during build

Security

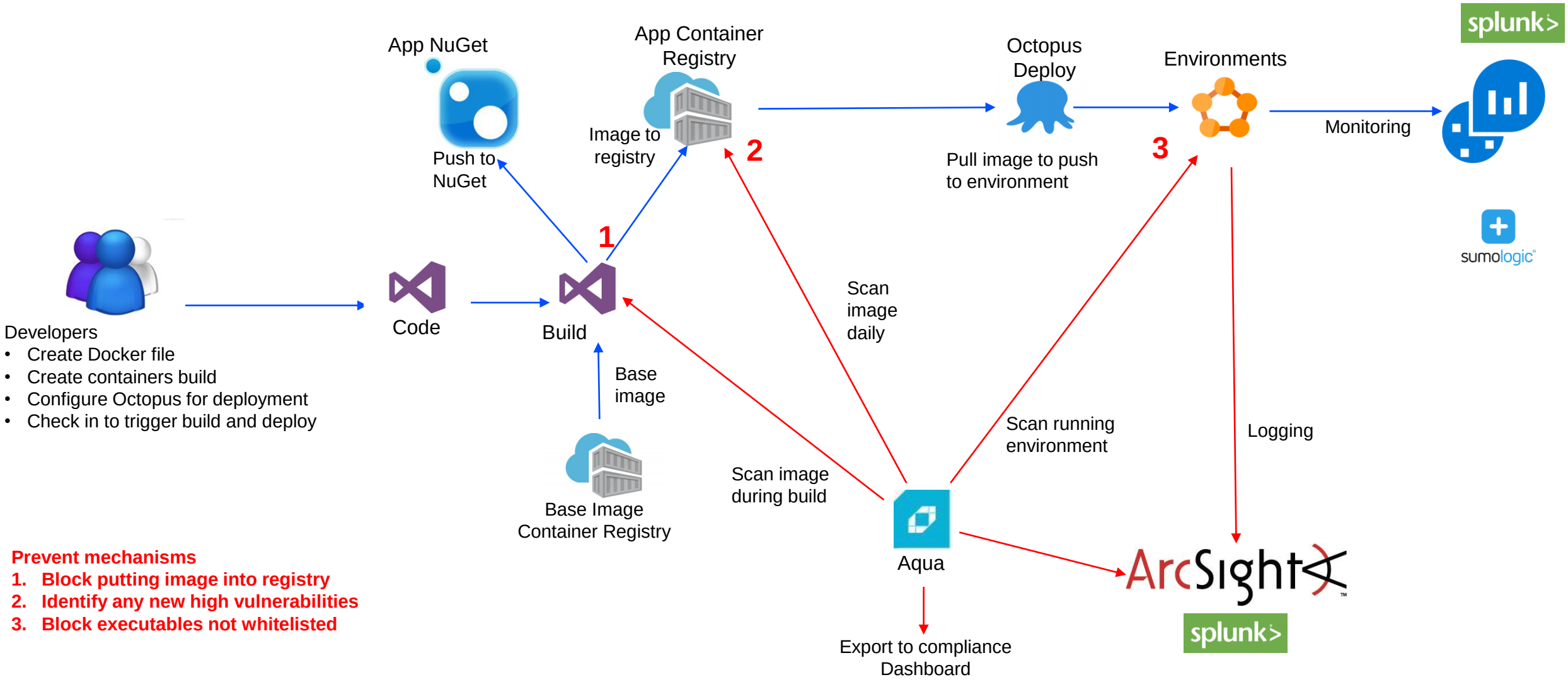
Scan running environment

Logging

Centralized Logging

Prevent mechanisms
1. **Block putting image into registry**
2. **Identify any new high vulnerabilities**
3. **Block executables not whitelisted**

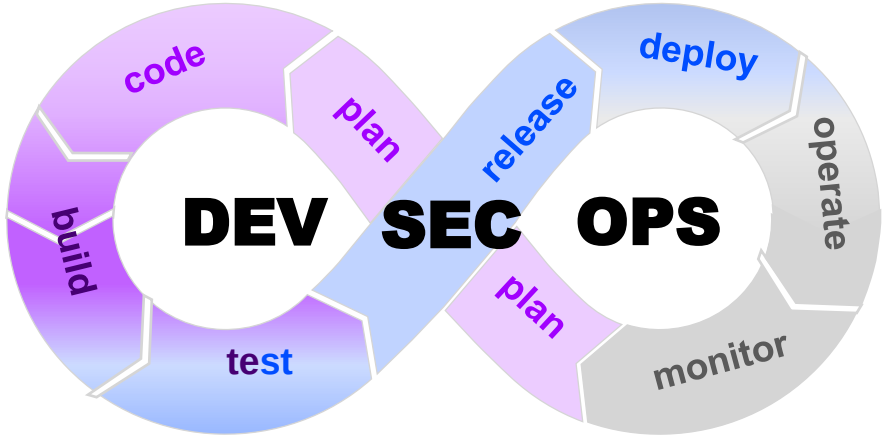
DEVELOPMENT LIFECYCLE FOR SECURITY



Prevent mechanisms

1. **Block putting image into registry**
2. **Identify any new high vulnerabilities**
3. **Block executables not whitelisted**

HOW TO GET STARTED



“So we are kind of doing some DevOps, how can take the right next steps?”

Put everything in SCM

Do:
- Version everything.
- Roadmap to bring in database, infrastructure, etc.
- Start tying commits to User Stories.

Get the Basics

Do:
- Code Quality Scanning
- Unit Testing
- Fail Builds that don’t meet standards – Quality Gating

Look to shift left whenever you can

Do:
- security scans early and often
- Integration and functional testing using containers
- Leverage mock data or service virtualization

Keep a pulse on what is happening

Do:
- Make sure your acting on insights
- Leverage KMS for secrets
- Think about your architecture (threat modeling?)


goto;
chicago
Q&A
follow us @gotochgo

goto; chicago

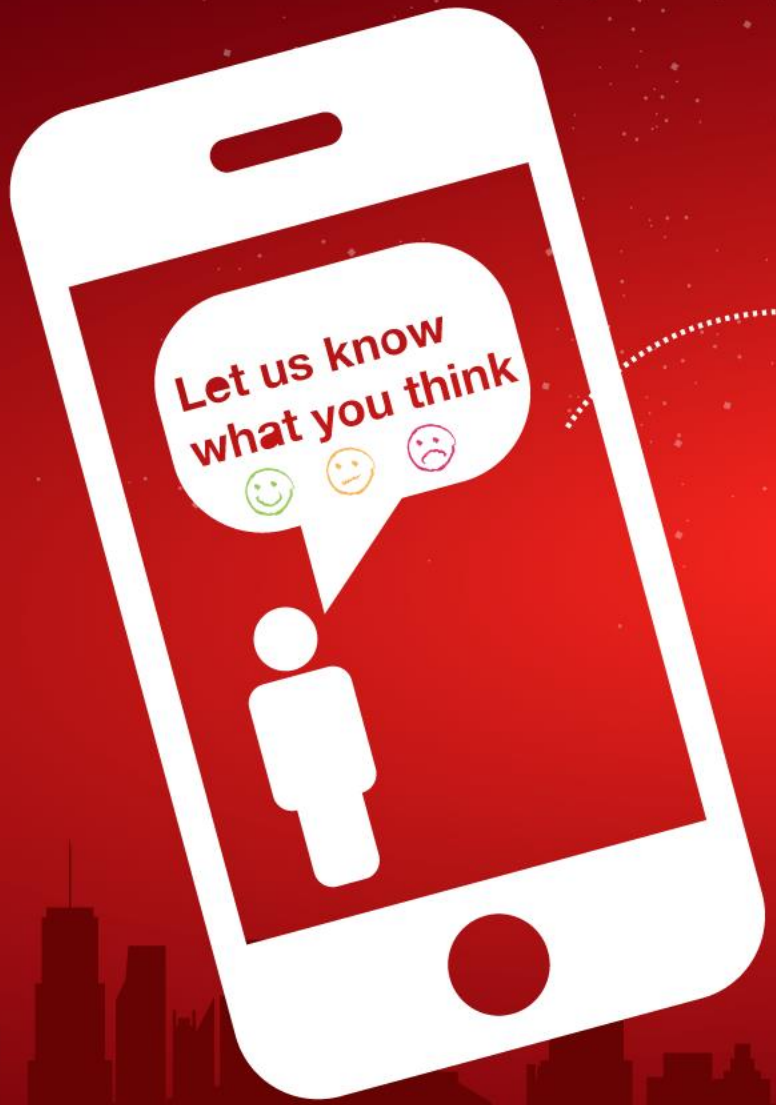
Please

Remember to rate this session

Thank you!

follow us @gotochgo

goto; chicago



Click ‘Rate Session’

Rate **5** sessions to get the supercool GOTO reward

follow us @gotochgo