DEVOPS WORLD by CloudBees

PRACTITIONER

Container pipeline velocity vs security? Why not both?

Eric Smalling

Sr. Developer Advocate
Snyk Inc. | @ericsmalling

Peter McKee

Head of Developer Relations
Docker Inc. | @pmckee

Agenda

- Introductions
- Docker 101
- New Challenges
- How bad could it be?
- Wrap-up / Conclusions
- Q & A

PRACTITIONER

Part 1
Docker 101

DEVOPSWORLD
by CloudBees

Containers

- A container is simply another process on your machine that has been isolated from all other processes on the host machine
  - namespaces
  - cgroups

Container Images

- Containers use an isolated filesystem. This custom filesystem is provided by a container image. Container Images must contain everything needed to run an application.
  - all dependencies
  - configuration
  - scripts
  - binaries

PRACTITIONER

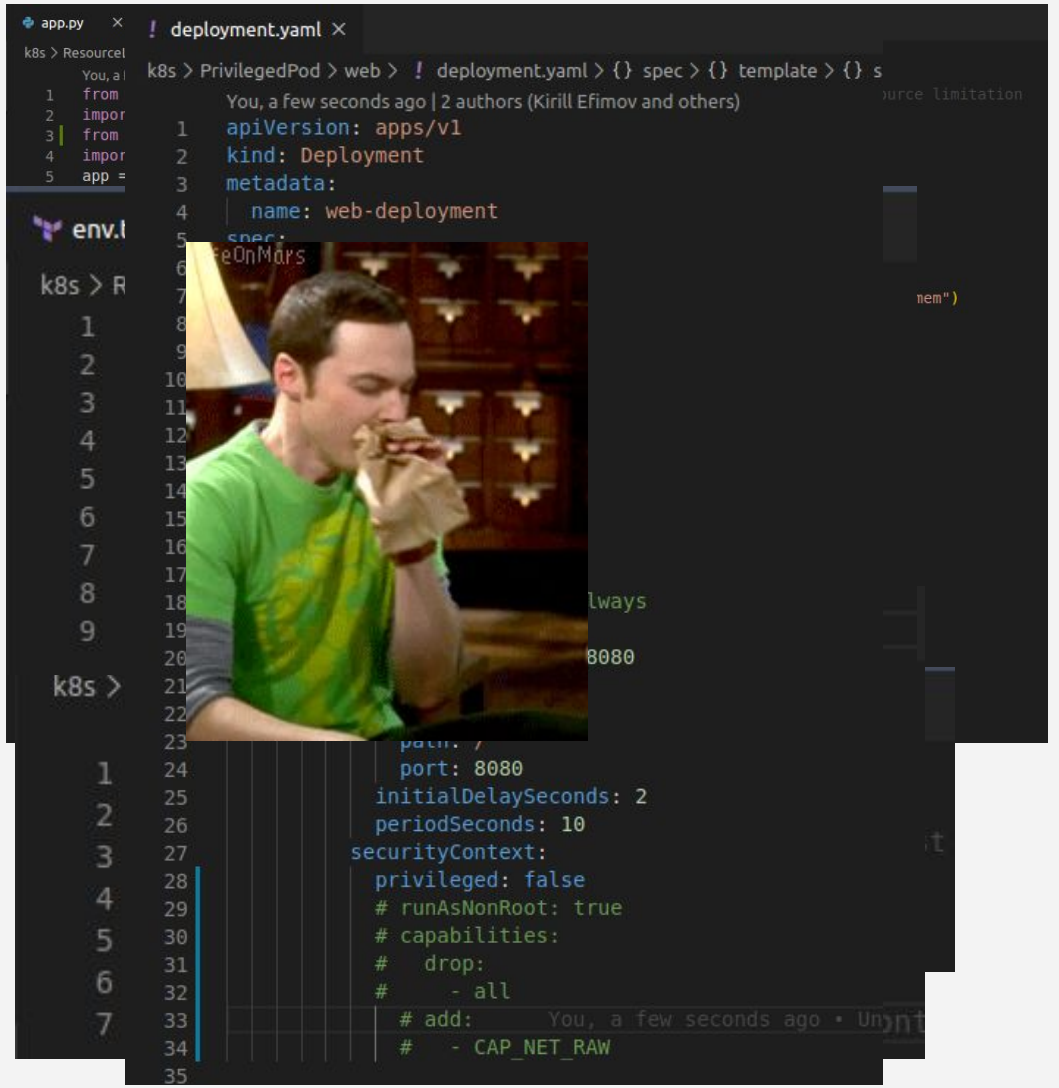
Part 2
New Challenges

Developer, Operations and Security scope changes

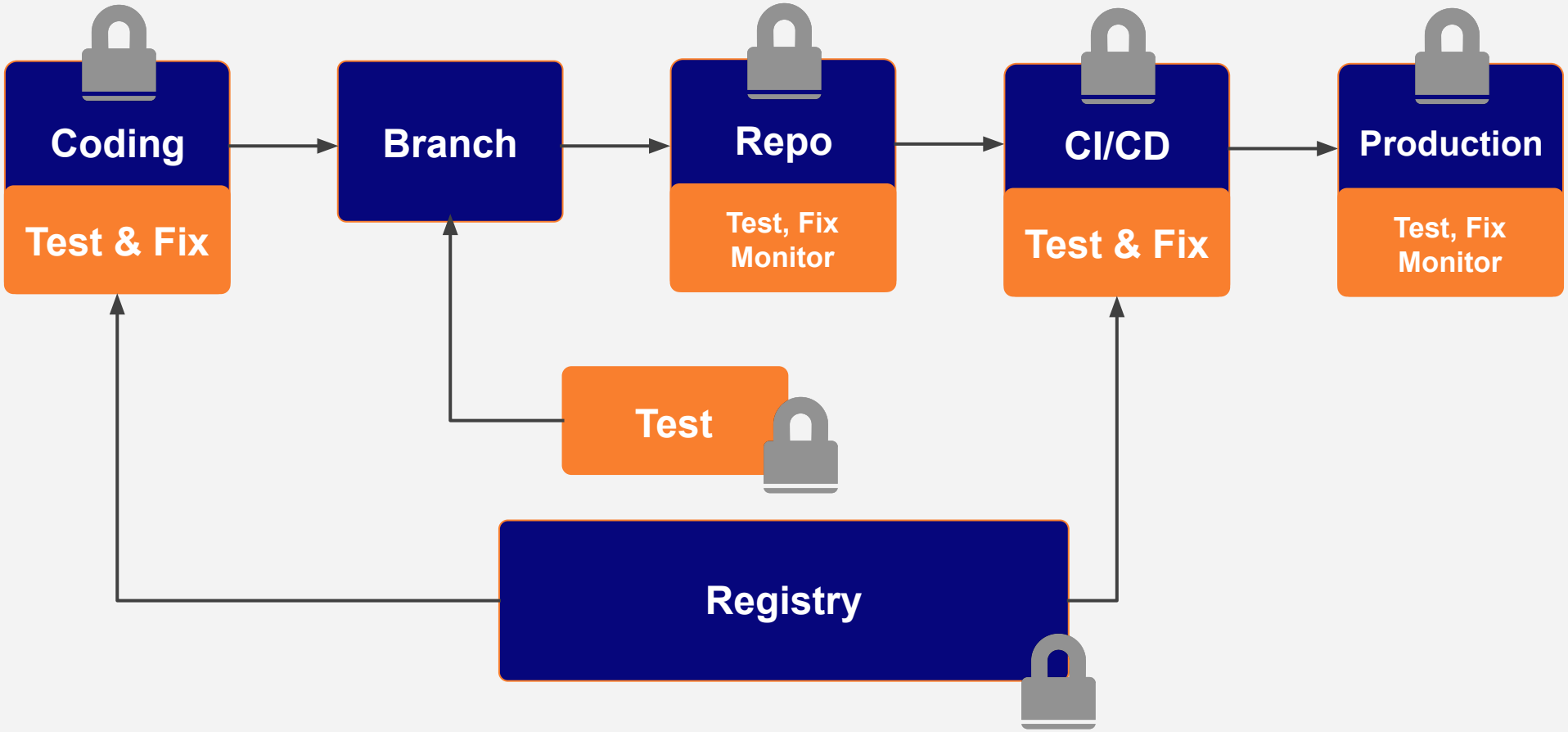
DEVOPSWORLD
by CloudBees

Container Challenges

- Increased scope of responsibility
  - What does my app/service contain?
    - Source code of my app
    - 3rd party dependencies
    - Dockerfile
    - IaC files (eg. Terraform)
    - K8s files
- Lack of expertise
- Maintaining velocity



Shifting Left



PRACTITIONER

Part 3
How bad could it be?

Are container exploits really something to worry about?

Container Security at Scale

Security testing automation drives a culture of security and empowers DevSecOps.

SHIFT-LEFT SECURITY

2x

Companies who automate are twice as likely to implement security testing

CONTAINERS IN PRODUCTION

60%

Containers are dominant mechanism

RAPID FIXES

72%

Fix vulnerabilities in under a week.

36% in under a day!

INCIDENTS

56%

Misconfiguration or known unpatched vulnerability incident in cloud native apps.

Source: Snyk 2021 State of Cloud Native Application Security Report

Demo: Setting the scene

- Legacy JEE webapp
  - Apache Tomcat 8
  - OpenJDK 8
- Lift & shifted into container at same TC version: 8.5.21
- Dockerfile:

```
FROM maven:3-jdk-8-slim as build

RUN mkdir /usr/src/goof
COPY . /usr/src/goof
WORKDIR /usr/src/goof
RUN --mount=target=$HOME/.m2,type=cache mvn install

FROM tomcat:8.5.21

RUN mkdir /tmp/extracted_files
COPY --chown=tomcat:tomcat web.xml /usr/local/tomcat/conf/web.xml
COPY --from=build /usr/src/goof/todolist-web-struts/target/todolist.war /usr/local/tomcat/webapps/todolist.war
```

Demo

Other topics

- Minimal image layers
  - Only the minimal filesystem for running and maintaining your application
  - Anything you add can potentially be leveraged by an intruder
  - Deleting files in a layer does not remove them from the host filesystem
- Immutability aids in hardening
  - Read-Only root filesystem on containers
  - Use external log aggregators / collectors
  - Beware overly permissive volume permissions
  - Don’t bind-mount host volumes

Other topics

- Don’t run as root
  - UID 0 in a container can still do malicious things
    - Install software
    - Erase logs
    - Change configurations
    - Full access to mounted filesystems
  - Use UID/GID in Dockerfile “USER” line instead of user/group name
    - K8s **`securityContext:runAsNonRoot:true`** requires this.

- K8s pod/container Security Context
  - Much of the above (and more) can be controlled via securityContext
  - SecurityContext Top 10 Cheat-Sheet

Other topics

- Network Policies
  - Zero-Trust pattern
    - Deny all traffic by default
    - Allow only specific ingress / egress
    - Don’t forget to allow critical services (ie DNS)
- Secrets management
  - NEVER populate a credential in your image or configuration files
  - Ensure K8s secrets are encrypted (they aren’t by default)
  - Consider external secrets store (ie Hashicorp Vault)
- Enforcement via admission control
  - Open Policy Agent (OPA)
  - Kyverno

PRACTITIONER

Conclusions

Key Takeaways

- OS and middleware level security concerns are a new concept for most developers
  - Leverage tools and policies that empower developers to be proactive with actionable feedback
- Pipeline velocity is critical, but not at the expense of quality
  - Fast feedback is critical
  - Don’t kick the can down the road / Throw the code over the wall / [insert your favorite metaphor]
- Defence in depth
  - Understand image construction and minimize footprint
  - Utilize container engine and orchestrator configurations that lock the environments down
  - Don’t forget externals like networks, secrets, etc
  - K8s cluster operators: enforce rules with admission controllers

DEVOPS WORLD by CloudBees

Thank you!

Eric Smalling

Sr. Developer Advocate
Snyk Inc. | @ericsmalling

Peter McKee

Head of Developer Relations
Docker Inc. | @pmckee

Title and Content Layout: Arial 32pt

- First level bullet text, Arial 24pt
- Line spacing 0.95, before paragraph 12pt
- Left justified
- Sentence case
- First level bullet color is accent 1
  - Second level bullet Arial 18pt
  - Line spacing 0.95, before paragraph 6pt

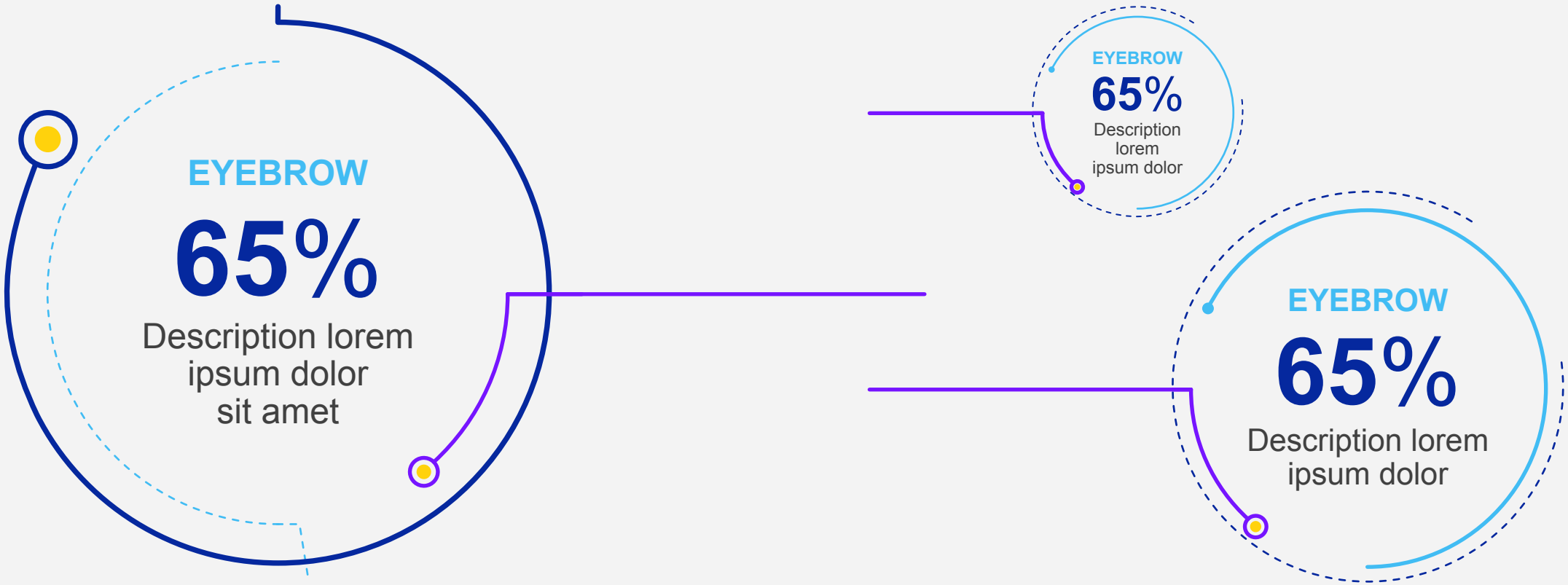
Two Content Layout

- First level bullet, Arial 24pt
- Line spacing 0.95, before paragraph 12pt
- Left justified
- Sentence case
- First level bullet color is accent 1
  - Second level Arial 18pt
  - Line spacing 0.95, before paragraph 6pt

- First level bullet, Arial 24pt
- Line spacing 0.95, before paragraph 12pt
- Left justified
- Sentence case
- First level bullet color is accent 1
  - Second level Arial 18pt
  - Line spacing 0.95, before paragraph 6pt

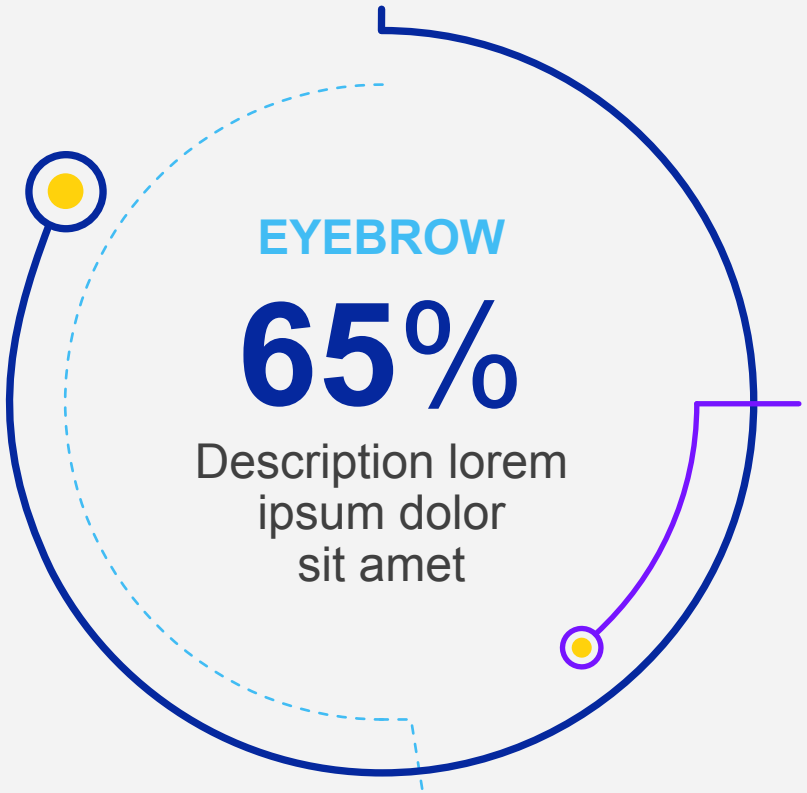
Stat Layouts with Subhead and Callouts

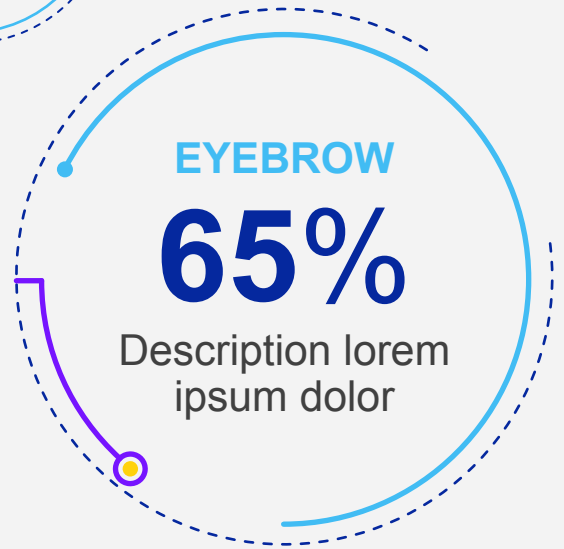
Subhead content style



Stat Layouts with Subhead

Subhead content style





Theme Colors

White
#FFFFFF

Black
#000000

Light 2 –Background
#F4F4F4

Dark 2
#404040

Accent 1
#05299E

Accent 2
#7614FF

Accent 3
#42BCF4

Accent 4
#F97F2E

Accent 5
#99E45C

Accent 6
#FFD20C

CHARTS WARNING: If you have both Office 2003 and 2007 installed on your system there may be a bug in chart colors. To ensure that accent colors 1-6 are used we recommend opening Excel 2007 prior to working with charts. We have discovered that if Excel 2007 is not open:

1. the charting could default back to MS graph app.
2. An error box may appear asking user to close excel dialog boxes

Default Settings

Theme Fonts:

Arial (heading)

Arial (body)

Text Box:

Default: Arial Bold 20pt

Center

Blue, Accent 1

Line spacing [.9]

Space before [12pt]

For Alt Text Styles only – use layout placeholders for bulleted lists

Drawing Style:

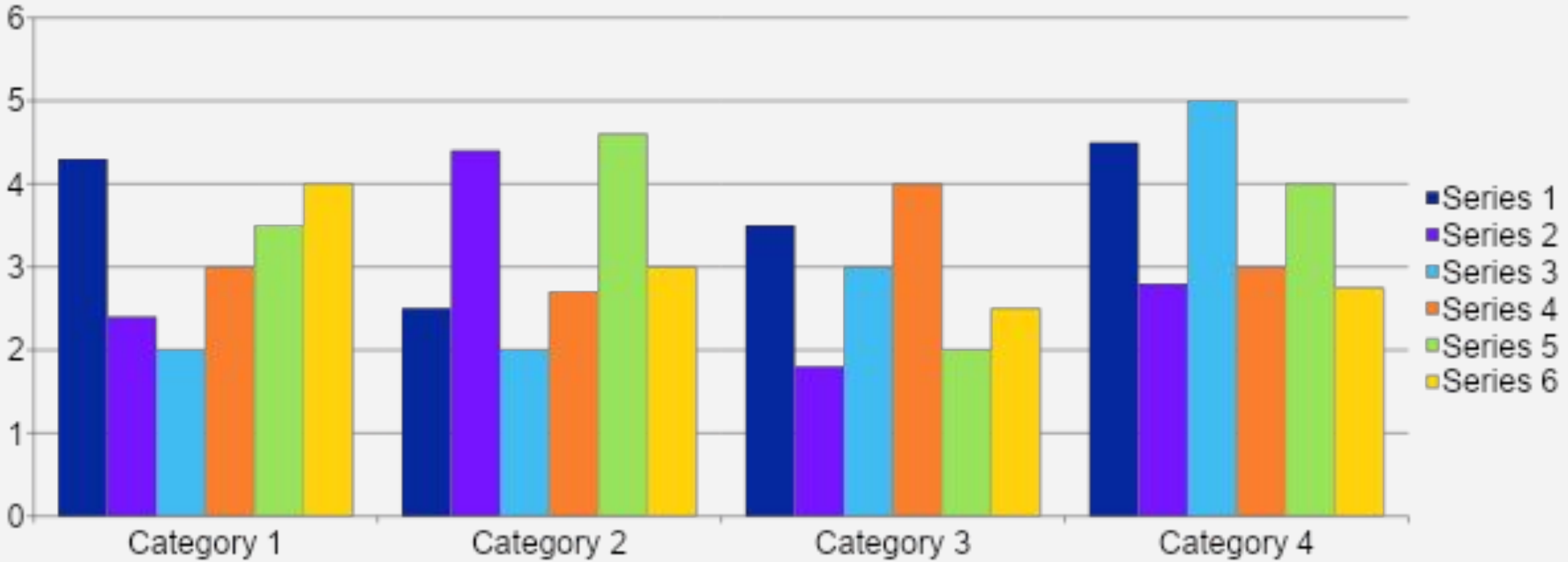
Line Style:

DEVOPSWORLD by CloudBees

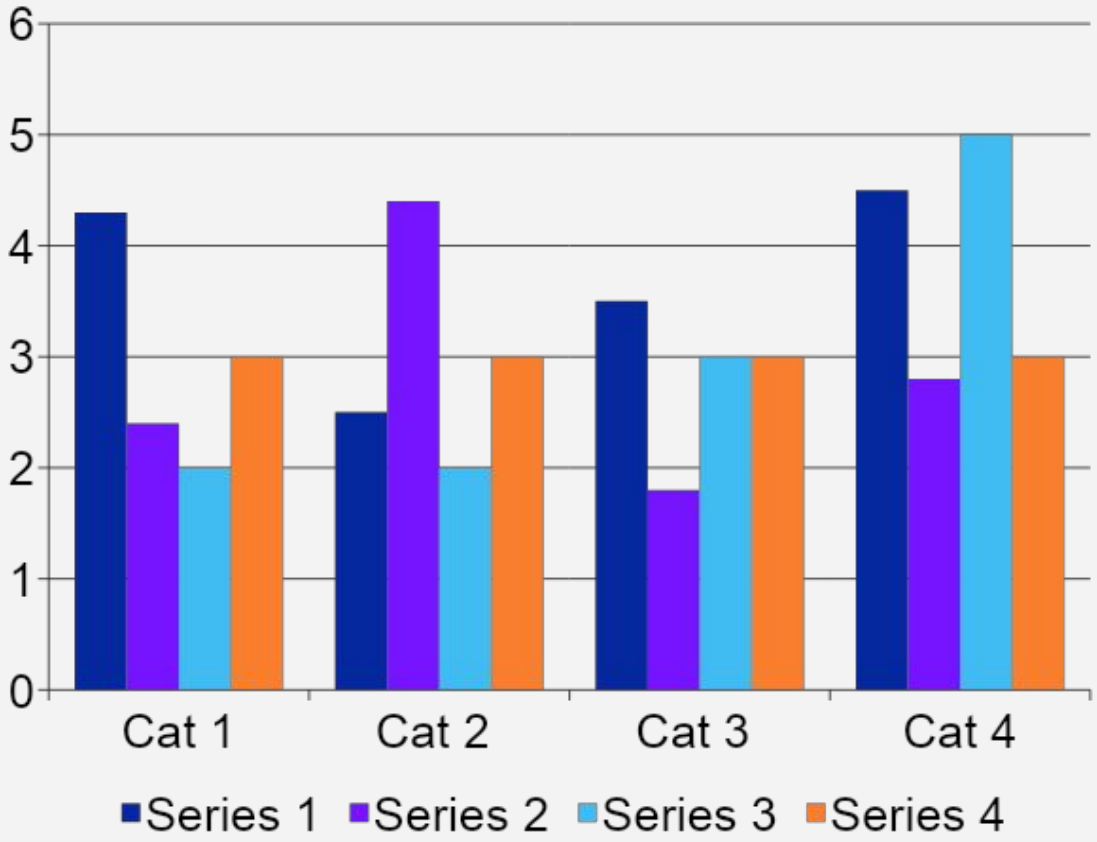
Default Table Style

Heading 1	Heading 2	Heading 3	Heading 4	Heading 5
Content	Content	Content	Content	Content
Content	Content	Content	Content	Content
Content	Content	Content	Content	Content
Content	Content	Content	Content	Content

Content Layout: Column Chart Sample

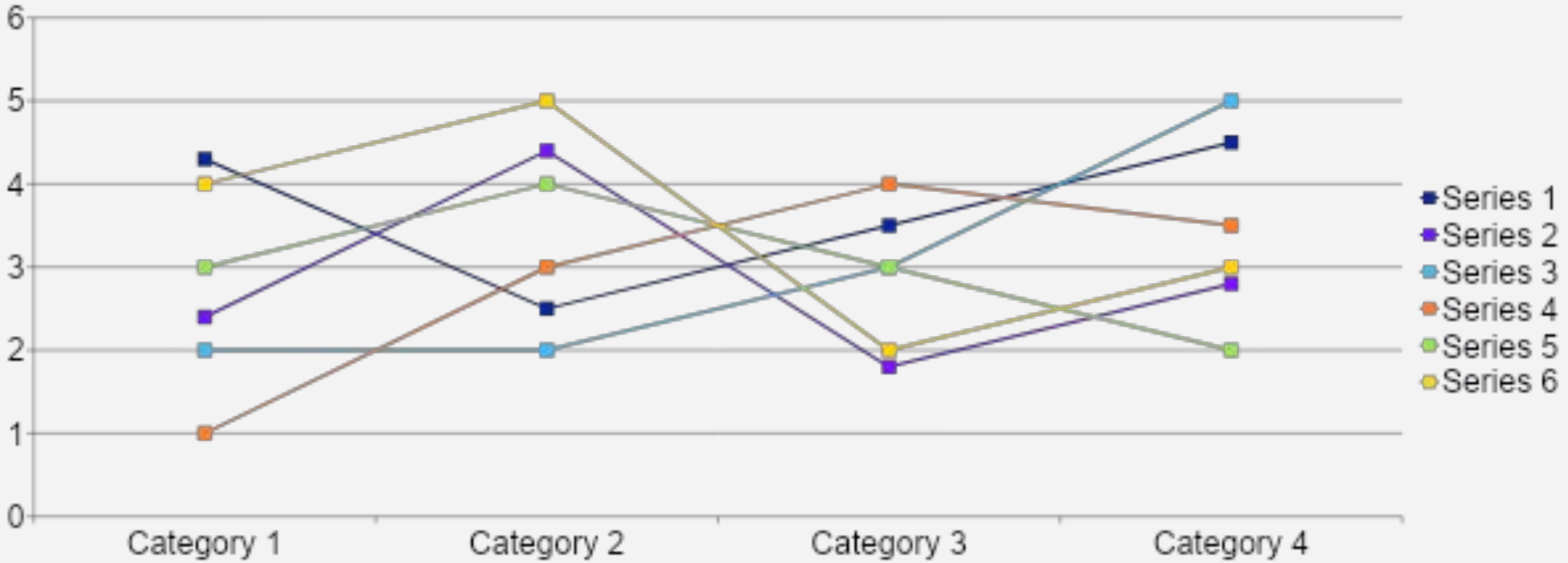


Two Content Layout: Column Chart Sample

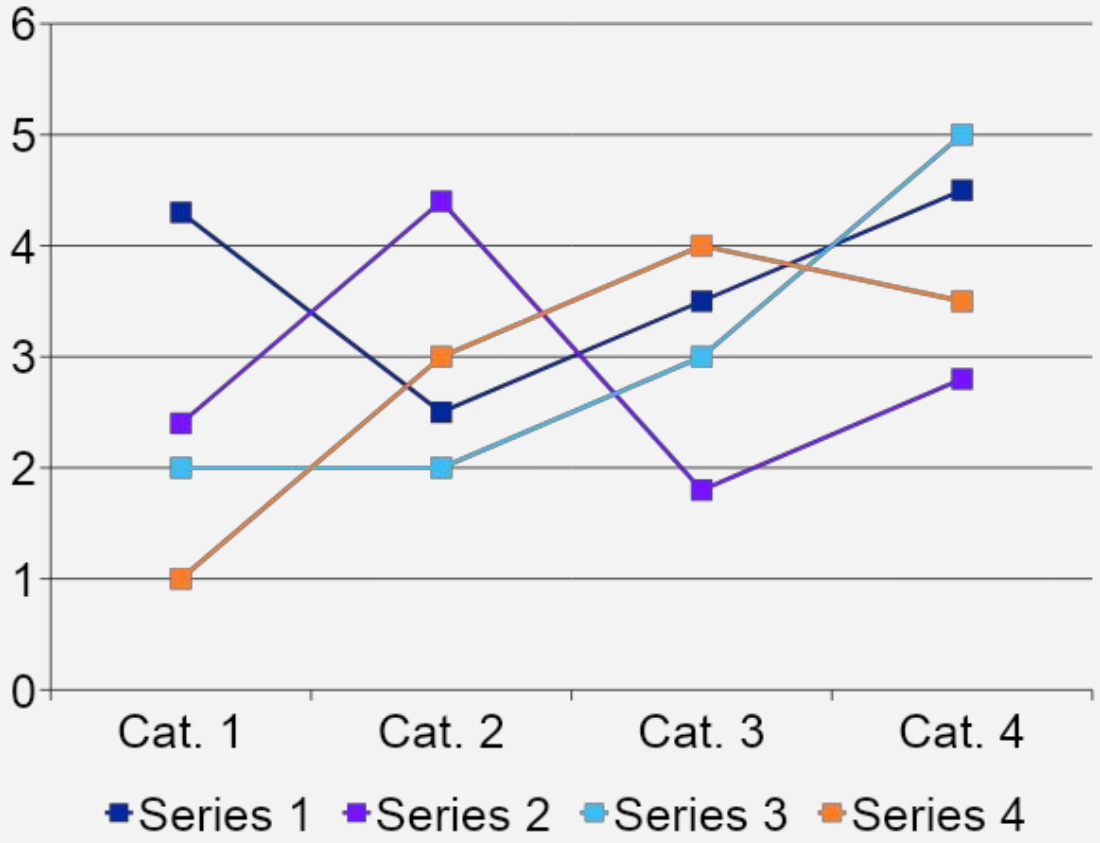


- First level bullet text
- Line spacing 0.95, before paragraph 12pt
- Left justified
- Sentence case
- First level bullet
  - Second bullet level
  - Second bullet level

Content Layout: Line Chart Sample

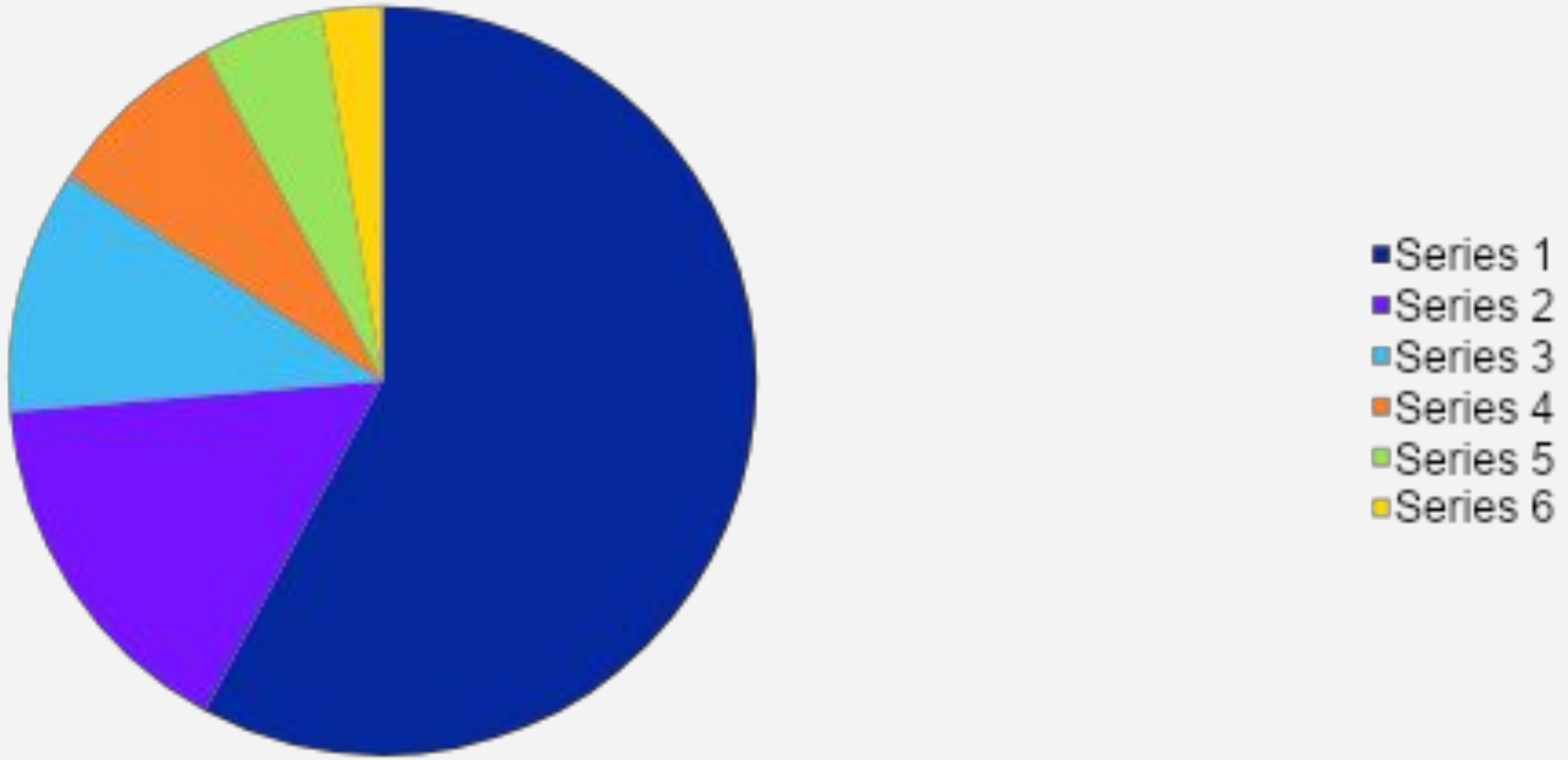


Two Content Layout: Line Chart Sample

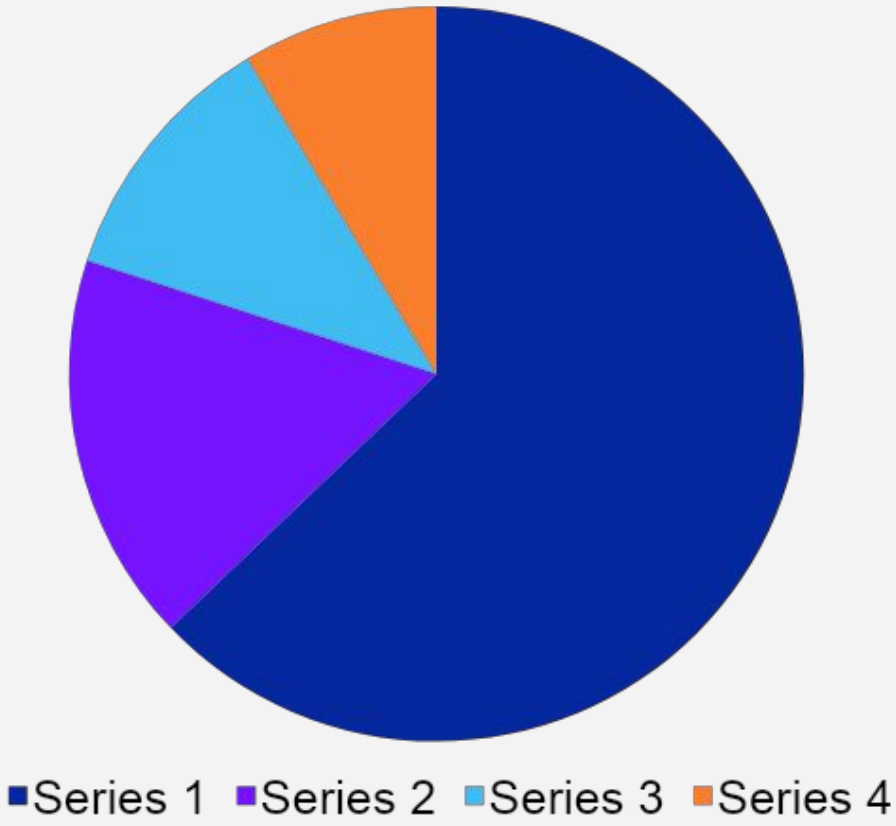


- First level bullet text
- Line spacing 0.95, before paragraph 12pt
- Left justified
- Sentence case
- First level bullet
  - Second bullet level
  - Second bullet level

Content Layout: Pie Chart Sample



Two Content Layout: Pie Chart Sample



- First level bullet text
- Line spacing 0.95, before paragraph 12pt
- Left justified
- Sentence case
- First level bullet
  - Second bullet level
  - Second bullet level

Custom Column Chart