ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Shifting the DevSecOps Culture –
Taking Away The Sugar Piece & Giving The Pile To Ants

Vandana Verma Sehgal

ADDO
ALL DAY DEVOPS

Who Am I

- Security Architect
- Application and Cloud Security
- Heading InfoSec Girls
- Co-Founder of OWASP Seasides
- Co-Organizer - BSides Delhi
- Chapter Leader - OWASP Bangalore
- Secretary : WIA OWASP
- Lead: Women of Security WoSec India

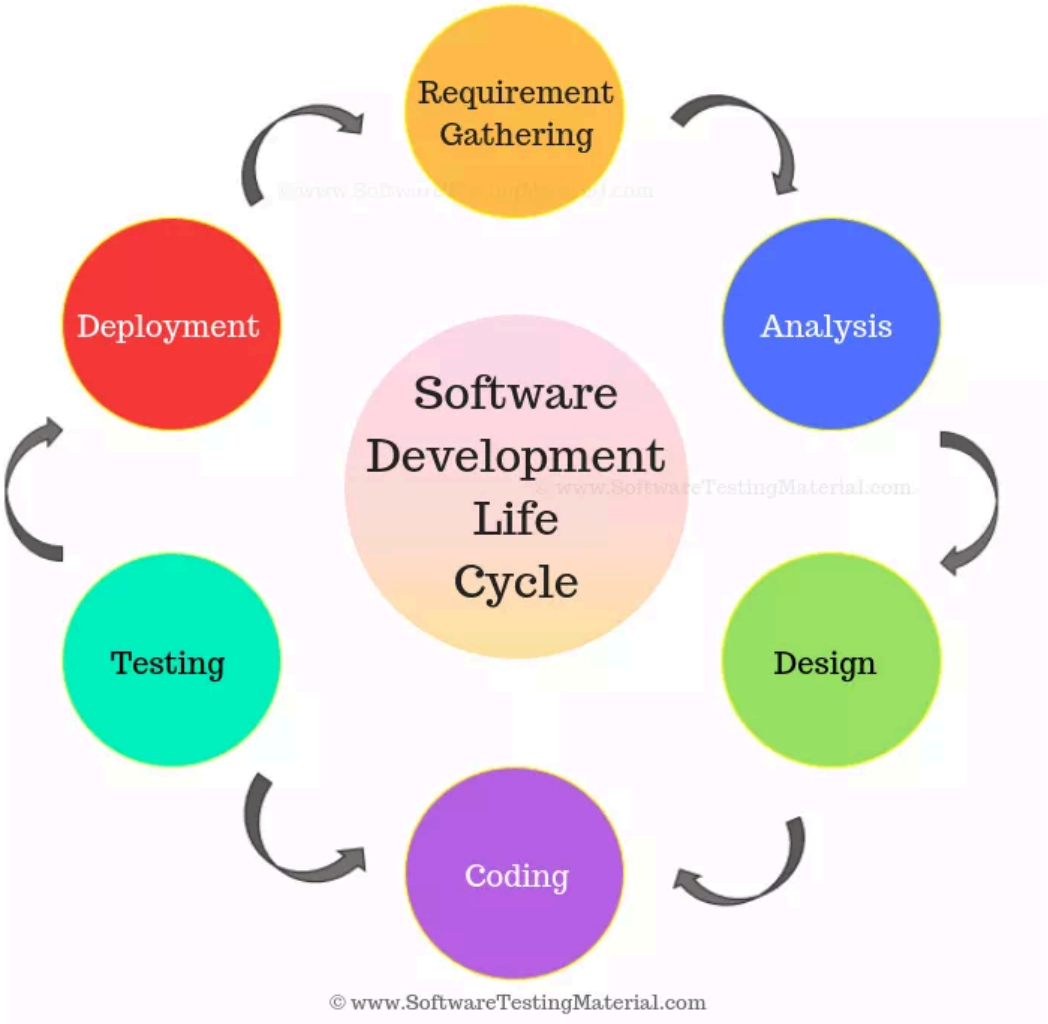
ADDO
ALL DAY DEVOPS

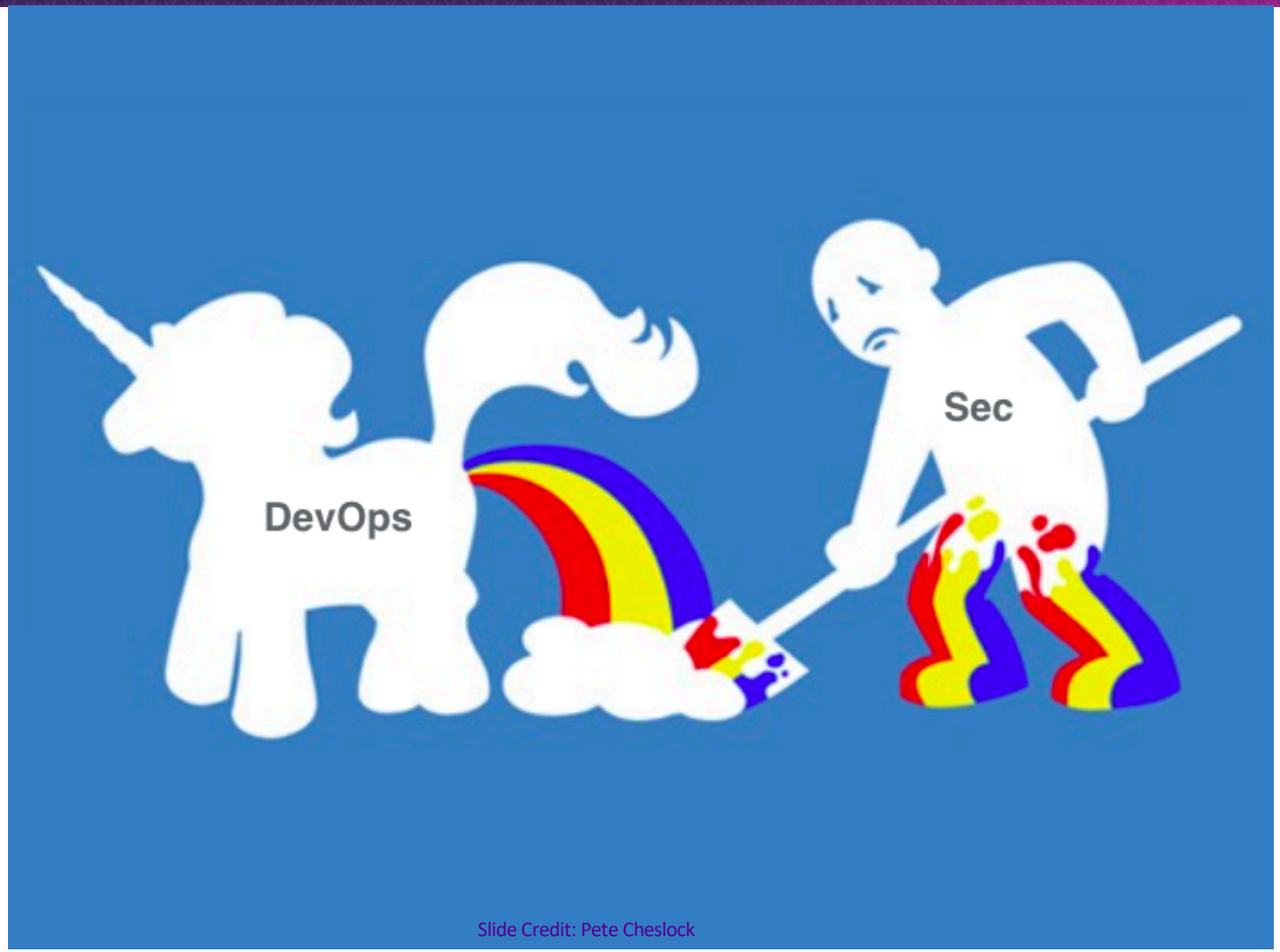
Agenda

- About DevSecOps
- DevSecOps Myths
- Culture Challenges in the Organizations
- Culture Shift Approaches - DevSecOps
- Security Team Responsibilities
- Use Cases
- key takeaways
- Resources

ADDO
ALL DAY DEVOPS

The Traditional Way





Slide Credit: Pete Cheslock

ADDO
ALL DAY DEVOPS

Blame Game

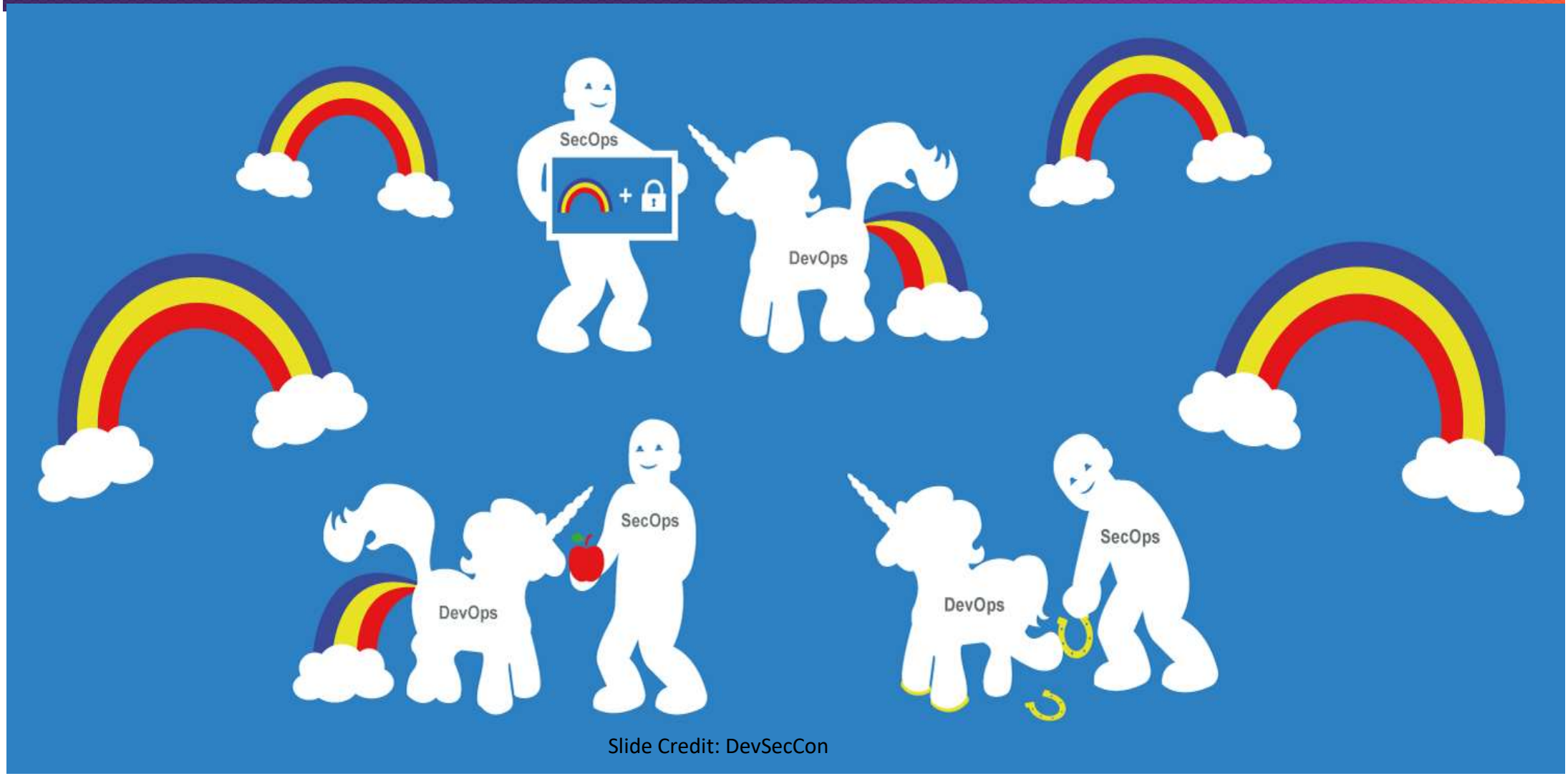
Dev

Ops

Security

https://www.deviantart.com/mibu-no-ookami/art/ACC-It-s-your-fault-328942263

ADDO
ALL DAY DEVOPS



Slide Credit: DevSecCon

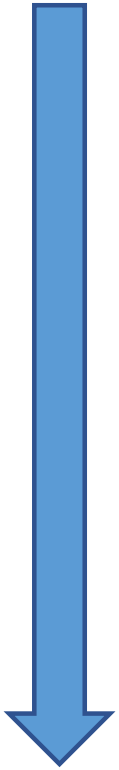
ADDO
ALL DAY DEVOPS

What is DevSecOps?

Integrating security practices within the DevOps process.

DevSecOps fosters a blameless culture and focused on secure delivery of software.

Top Down Approach



ADDO
ALL DAY DEVOPS

Making security as part of the everyday process

ADDO
ALL DAY DEVOPS

Don’t enforce anything and everything

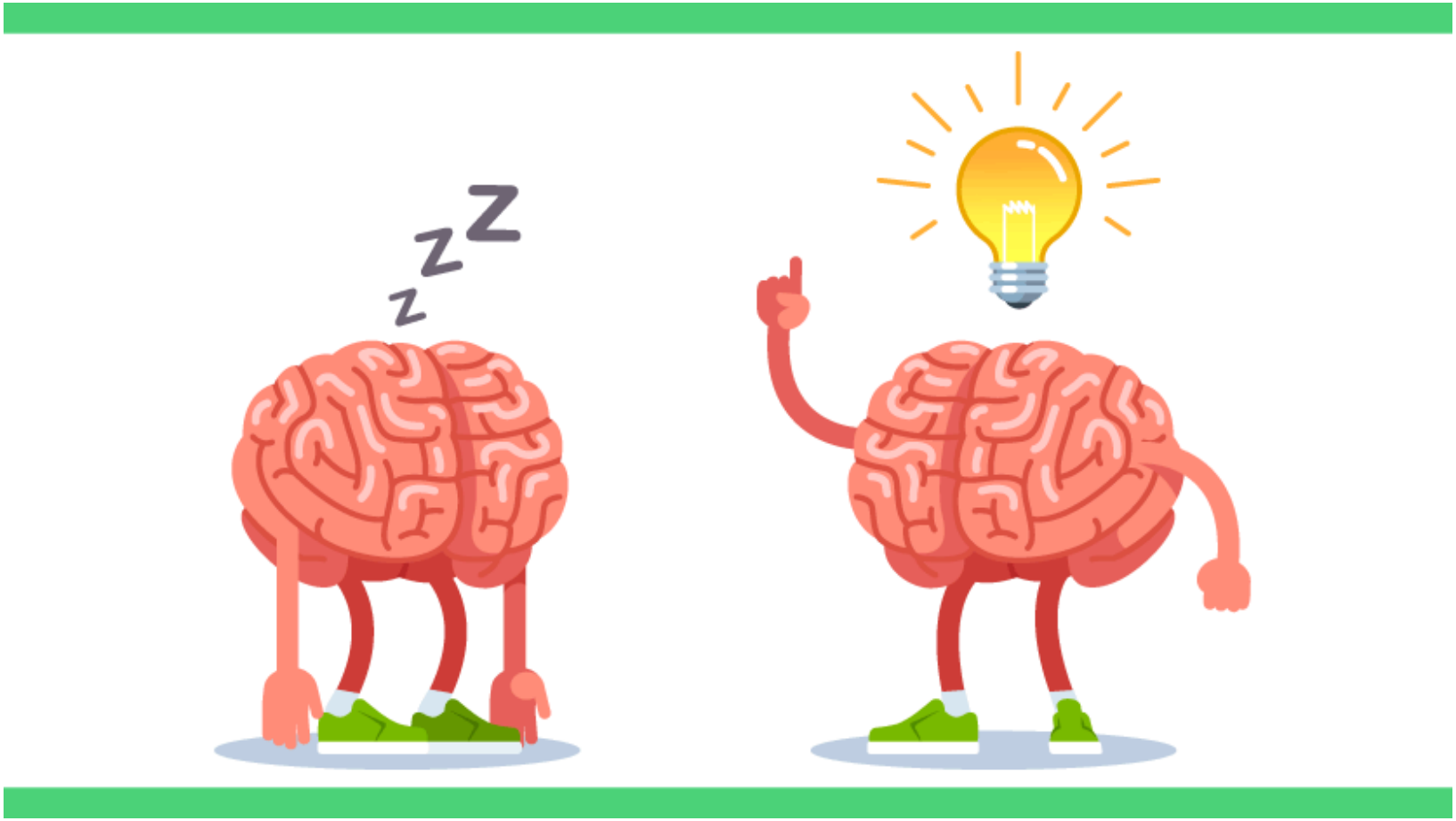
https://si.wsj.net/public/resources/images/BN-QA181_MINDMA_8S_20160927174714.jpg

ADDO
ALL DAY DEVOPS

Build relationships between teams, don’t isolate

ADDO
ALL DAY DEVOPS

Encourage security mindset outside sec team



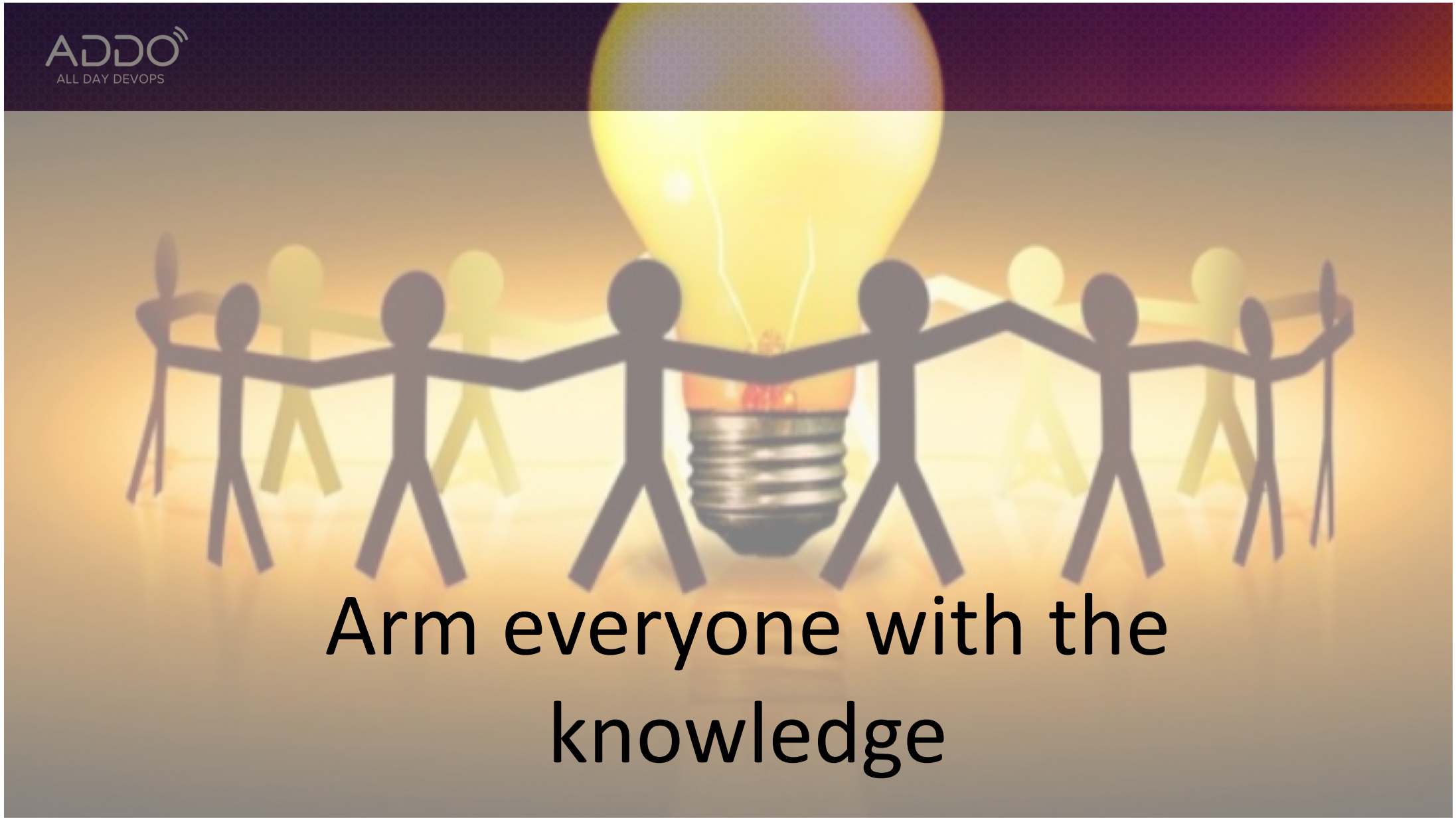
https://capetownguy.co.za/wp-content/uploads/2018/10/skills-shortage-in-South-Africa.jpg

ADDO
ALL DAY DEVOPS

Establish a training program

Ongoing education and training for software developers and Operations Team

https://www.ravepubs.com/wp-content/uploads/2015/05/ongoingtraining.png


ADDO
ALL DAY DEVOPS
Arm everyone with the knowledge

ADDO
ALL DAY DEVOPS

Improve the Skills with Secure code training

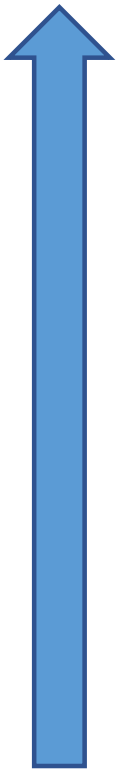
https://cdn1.iconfinder.com/data/icons/internet-12/256/14-512.png

ADDO
ALL DAY DEVOPS

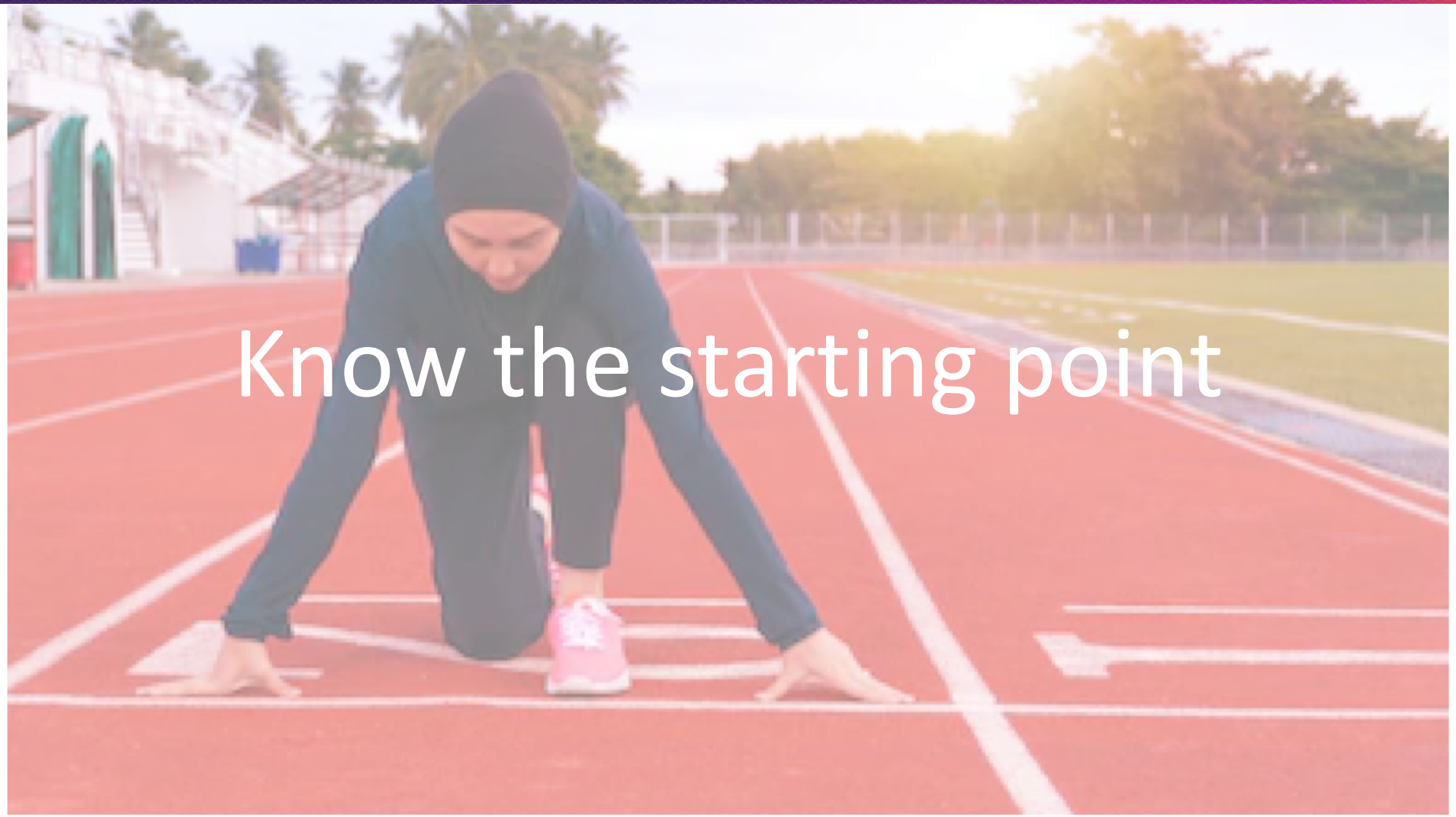
Launch Internal Bug Bounty Program

https://hackernoon.com/hn-images/1*re1GLQjhU86ji8l-5p5yCA.png

Bottom Up Approach



ADDO
ALL DAY DEVOPS

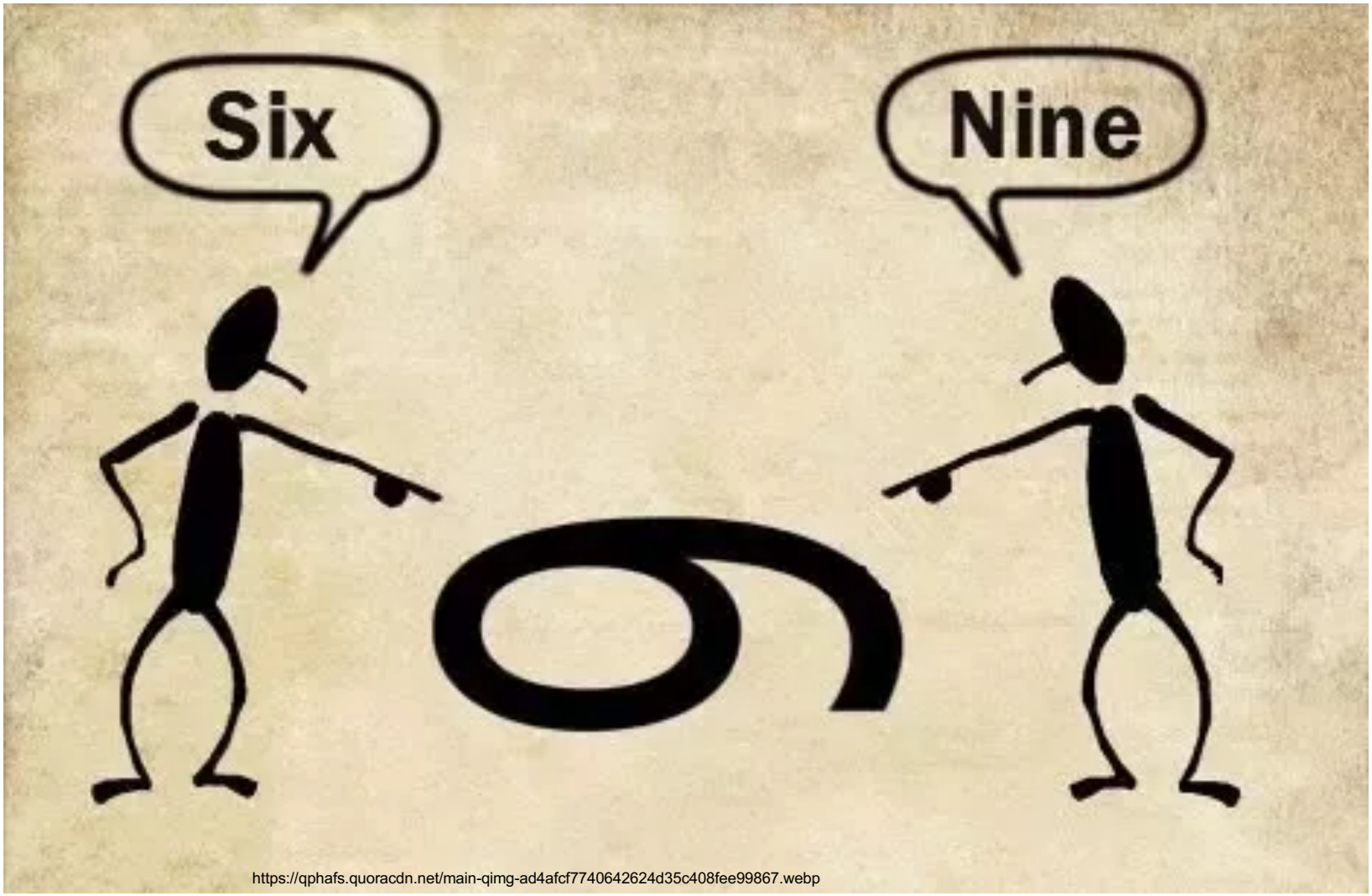


ADDO
ALL DAY DEVOPS

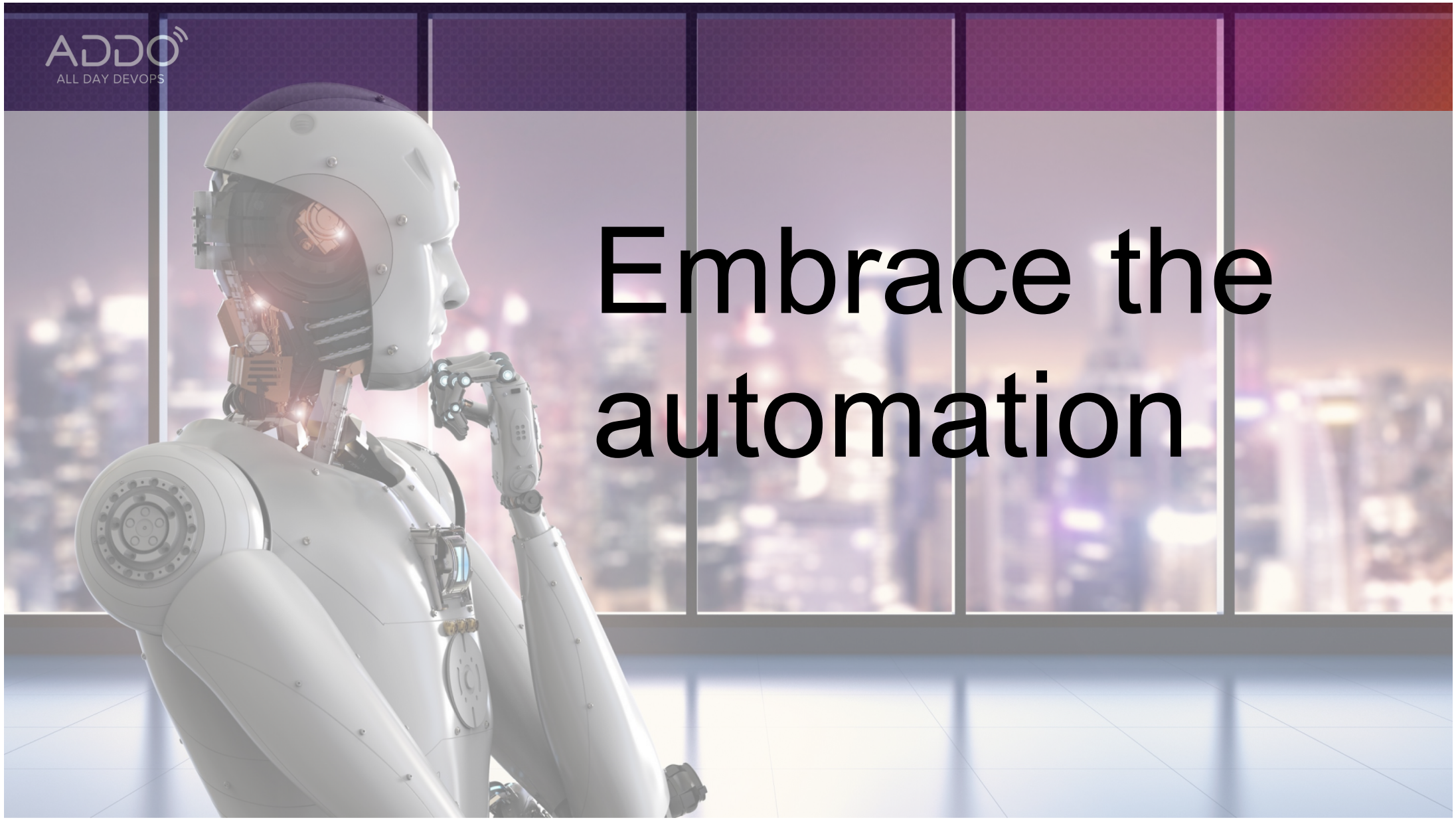
Interacts with multiple departments, assets, and resources

ADDO
ALL DAY DEVOPS

Respect others expertise and opinion

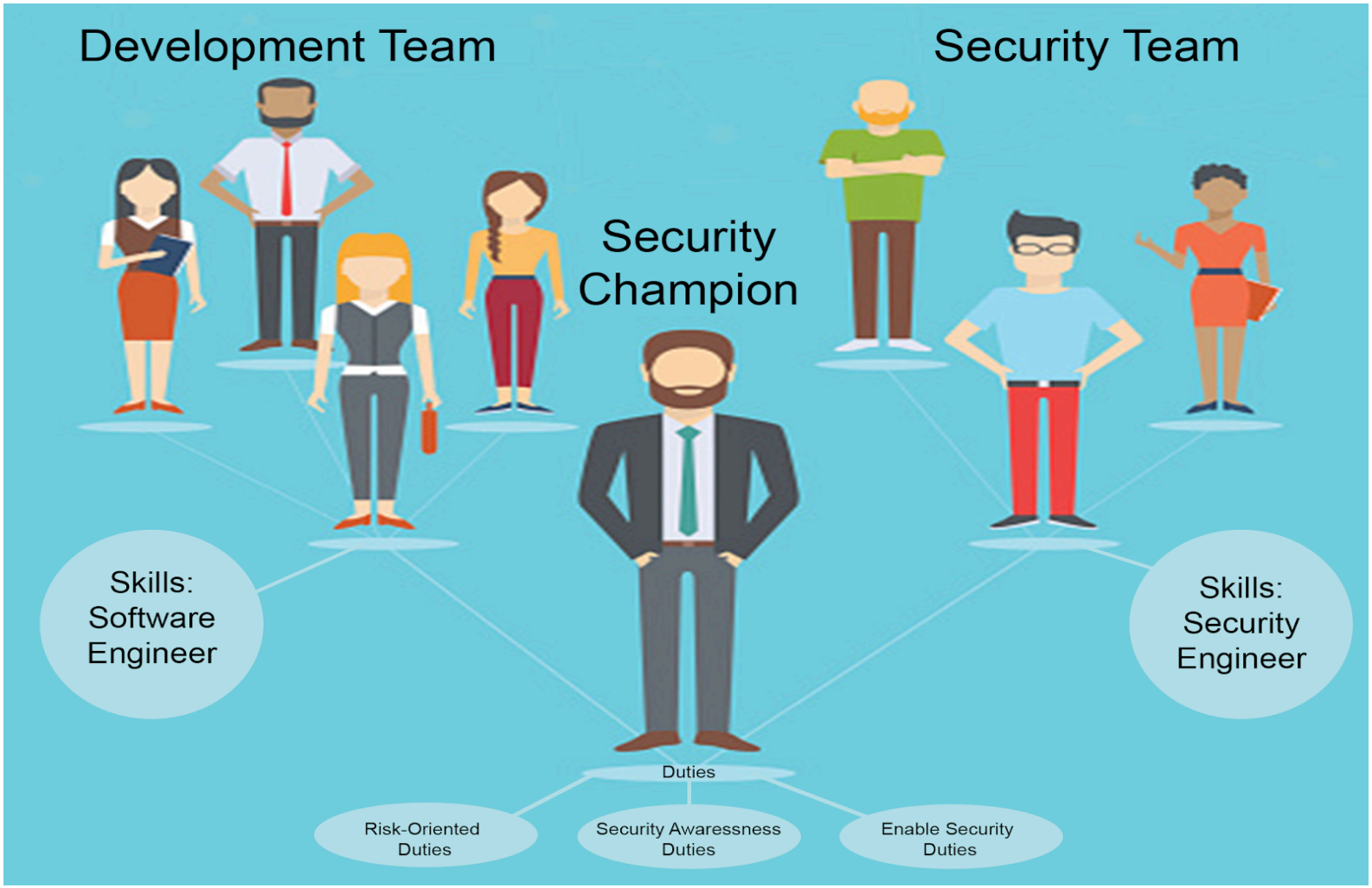


https://qphafs.quoracdn.net/main-qimg-ad4afcf7740642624d35c408fee99867.webp


ADDO
ALL DAY DEVOPS
Embrace the automation

ADDO
ALL DAY DEVOPS

Create more Security Champions



Ref:- https://safecode.org/wp-content/uploads/2019/01/champs-pic-768x549.png

ADDO
ALL DAY DEVOPS

Cross Skilling

https://www.accuprosys.com/wp-content/uploads/2014/09/42.jpg

ADDO
ALL DAY DEVOPS

Empower Dev /Ops to deliver better and faster and secure, instead of blocking.

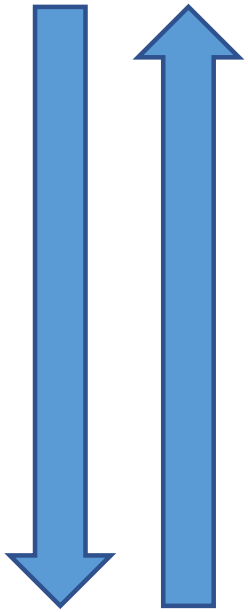
ADDO
ALL DAY DEVOPS

Inviting Dev and Ops to participate in Security Activities

ADDO
ALL DAY DEVOPS

Top Down Approach

- Let developers lead the way
- Organizational transparency
- Breaking Down Barriers and Silos

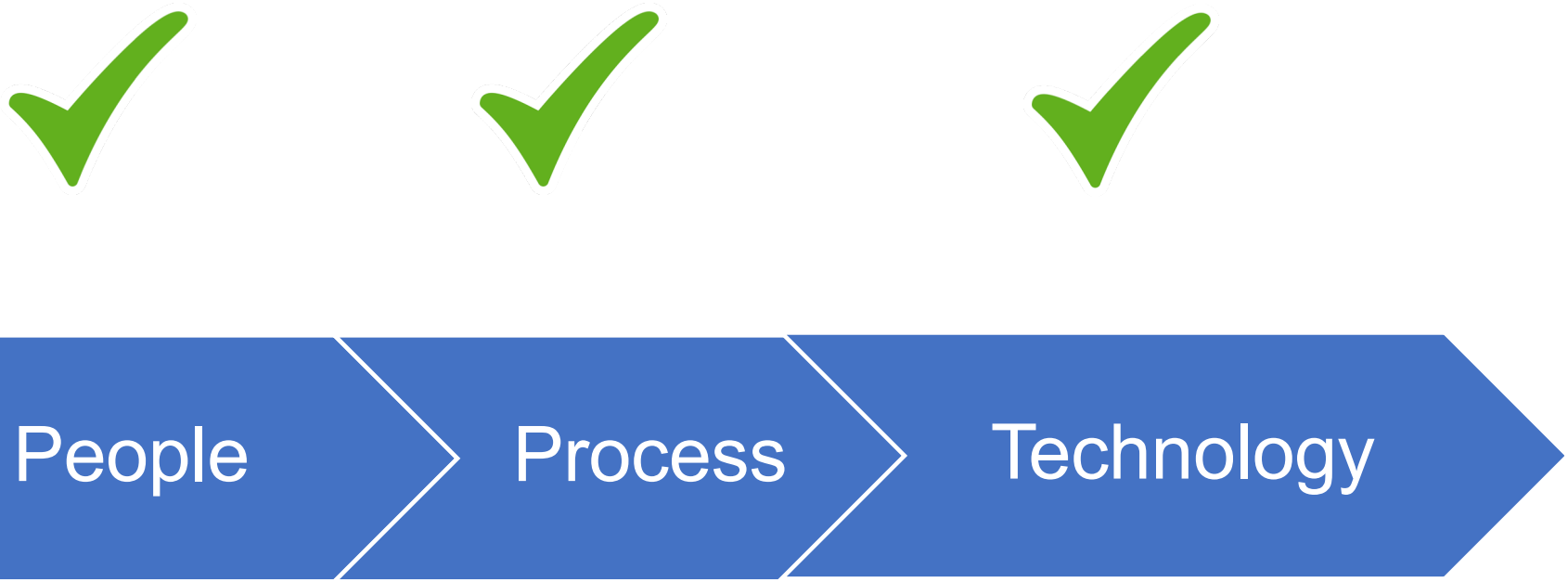


- Teams collaboration and inclusive culture
- Build Champions and collaborate them
- Speak in executives speak!

Bottom Up Approach

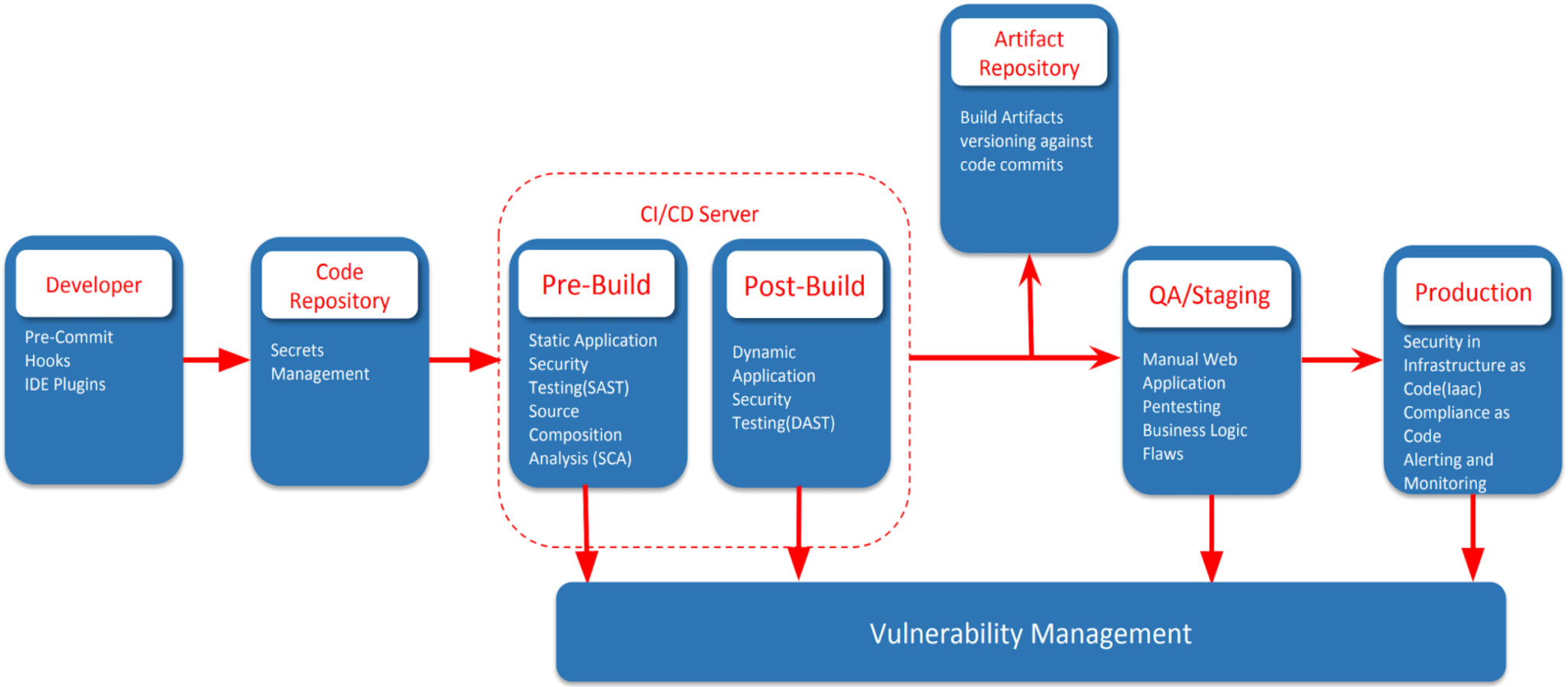
ADDO
ALL DAY DEVOPS

For DevSecOps to succeed



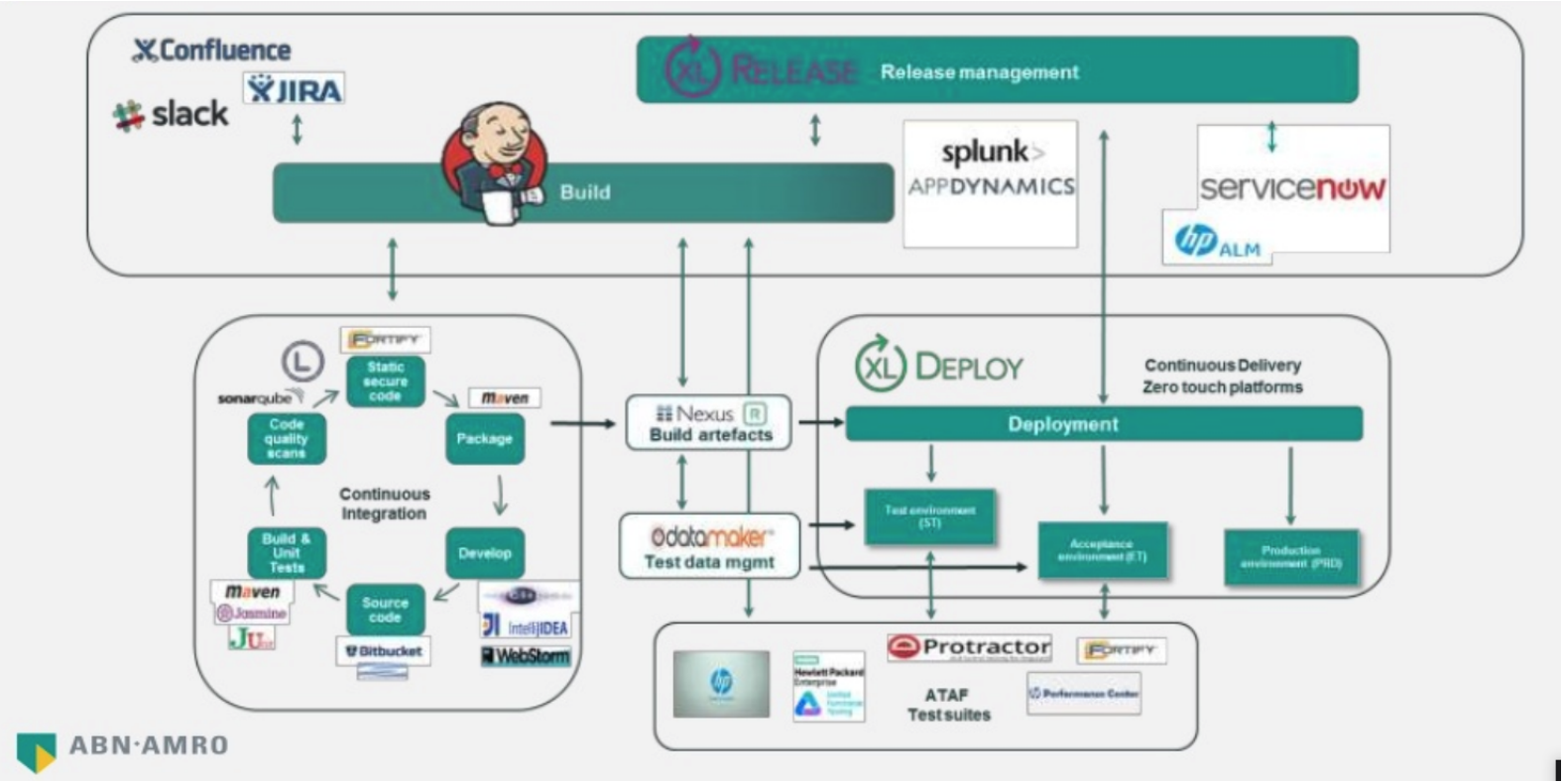
ADDO
ALL DAY DEVOPS

Sample DevSecOps Architecture



ADDO
ALL DAY DEVOPS

Case Studies – ABN Amro



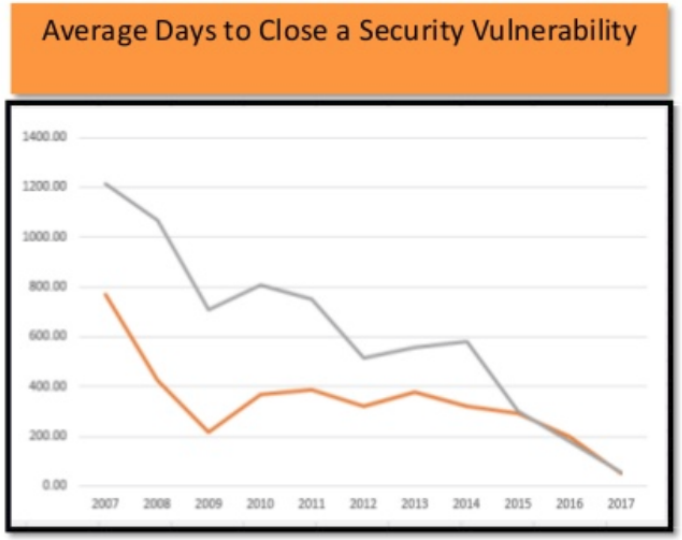
https://www.slideshare.net/derweeksglobal/abn-amro-devsecops-journey

Case Studies – Fannie Mae

DevSecOps @ Fannie Mae – The Results

Delivering the Promise

- Average days to close a vulnerability improved by 74%
- Automated code quality scanning shows overall security code scores has increased by 10%
- More than 60% of application teams are performing security tests before release
- Critically vulnerable open source components (CVE 7.5+) downloaded has decreased from 18% to 6.25%
- ~ 55% of technical debt and security defects identified as a result of periodic testing have been dispositioned
- ~ 77% of older technical debt and security defects have been remediated, have a remediation plan in place, or have been addressed through managed retirements of assets



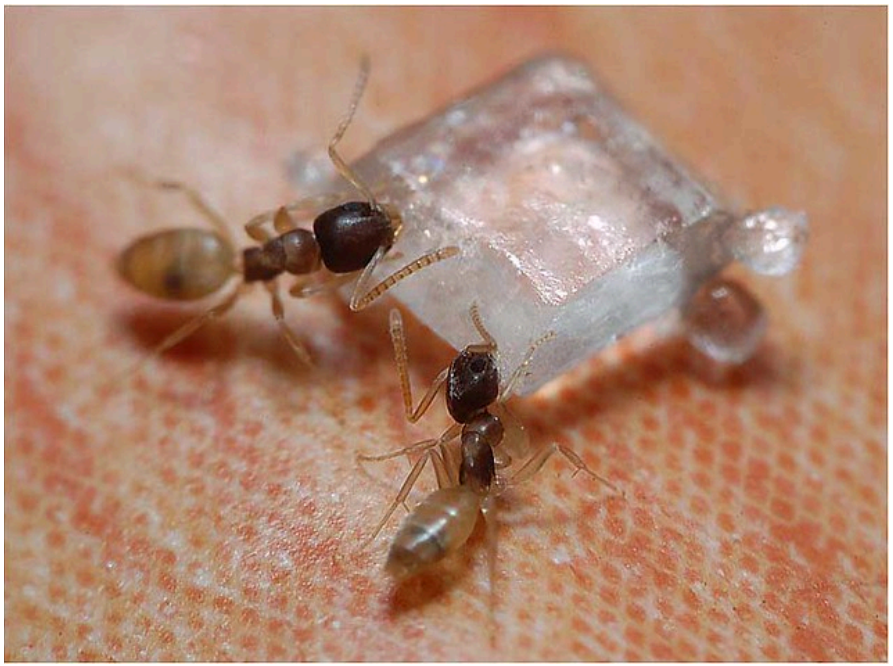
https://www.slideshare.net/derweeksglobal/abn-amro-devsecops-journey

Key takeaways

- Prepare your Umbrella Before it Rains (Early AppSec in Pipeline)
- Security is everyone’s responsibilities
- DevSecOps won’t replace your pentesting activity
- Create a Parallel security pipeline for more in-depth testing
- Don’t take on risk to generate business value

ADDO
ALL DAY DEVOPS

End Goal



ADDO
ALL DAY DEVOPS

References:-

- https://dzone.com/articles/shifting-left-devsecops
- https://enterprisersproject.com/article/2018/6/how-build-strong-devsecops-culture-5-tips
- https://techbeacon.com/security/how-build-devsecops-grow-culture-ground
- https://www.beyondtrust.com/blog/entry/devsecops-culture-shift-expect-adapt
- https://i.blackhat.com/asia-19/Thu-March-28/bh-asia-Shrivastava-DevSecOps.pdf
- https://businessinsights.bitdefender.com/building-devsecops-culture
- https://www.devseccon.com/wp-content/uploads/2017/07/DevSecOps-whitepaper.pdf
- https://www.contino.io/insights/introduction-to-devsecops-best-practices-people-part-1-of-3
- https://dzone.com/articles/devsecops-keys-to-success
- https://techbeacon.com/security/6-devsecops-best-practices-automate-early-often

Reach Me!

Twitter: @InfosecVandana

LinkedIn: vandana-verma

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs

cloudbees

Carnegie Mellon University Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire

ADDO
ALL DAY DEVOPS

SUPPORTERS

Thank you!