Carnegie Mellon University
Software Engineering Institute

Enhance AppSec maturity and outcomes using DevSecOps Metrics

Sep 15, 2021

Suresh Chandra Bose Ganesh Bose

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Carnegie Mellon University Software Engineering Institute

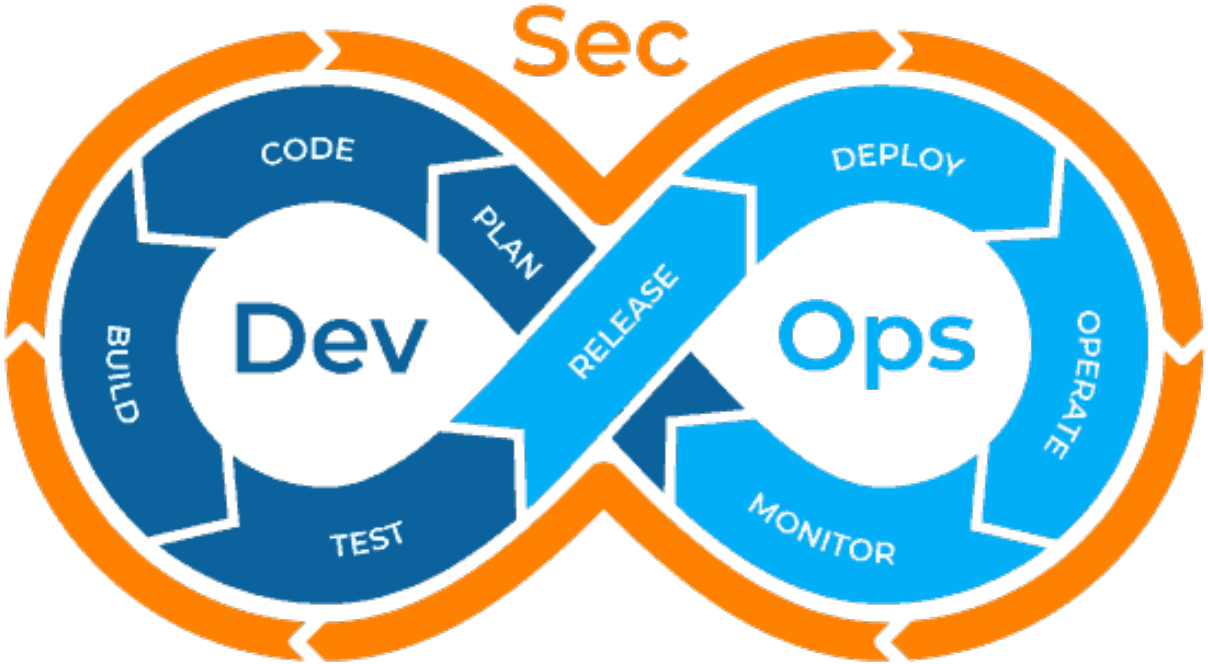
DEV SEC OPS DAYS LOS ANGELES

Biography

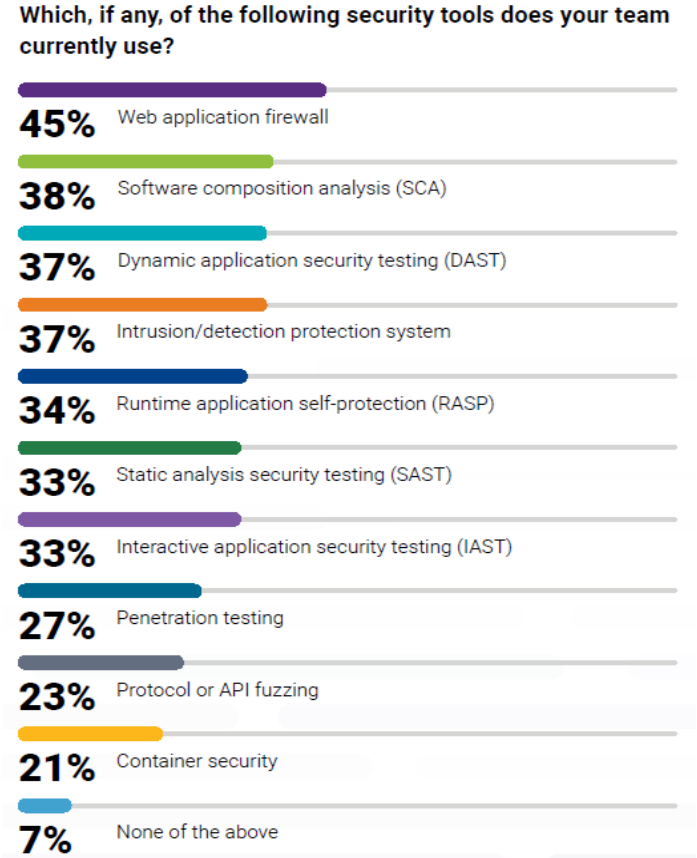
Suresh Chandra Bose, Ganesh Bose *is a Senior Manager – Consulting (Associate Director) at Cognizant Business Consulting practice. Suresh is an accredited Lead Assessor from TMMi Foundation and has been in the IT Industry for more than 23 years with vast consulting experience in various industries. He has executed strategic initiatives for many Fortune 100 companies in the areas of PMO, PPM, Process Consulting, Program Management, TMMi Assessment/ Implementation, Organization Strategy, Test Consulting and CIO/Governance Dashboard/Metrics across the globe.*

Suresh holds 21 International certifications in IT and speaks at 15+ international conferences, such as American Society for Quality (ASQ) Innovation Conference, American Software Testing Qualifications Board (ASTQB), 8.8 Computer Security Conference, DevSecOps Days, DevOps Days Austin, DevOps Days Medellin, DevOps Days Rio de Janeiro, DevOps Days Tampa Bay, DevOps Days Berlin, Docker Community with JFrog and Pacific Northwest Software Quality Conference (PNSQC). Suresh has been part of the selection and review panel for a leading Software Conference.

What is DevSecOps?



Why DevSecOps?



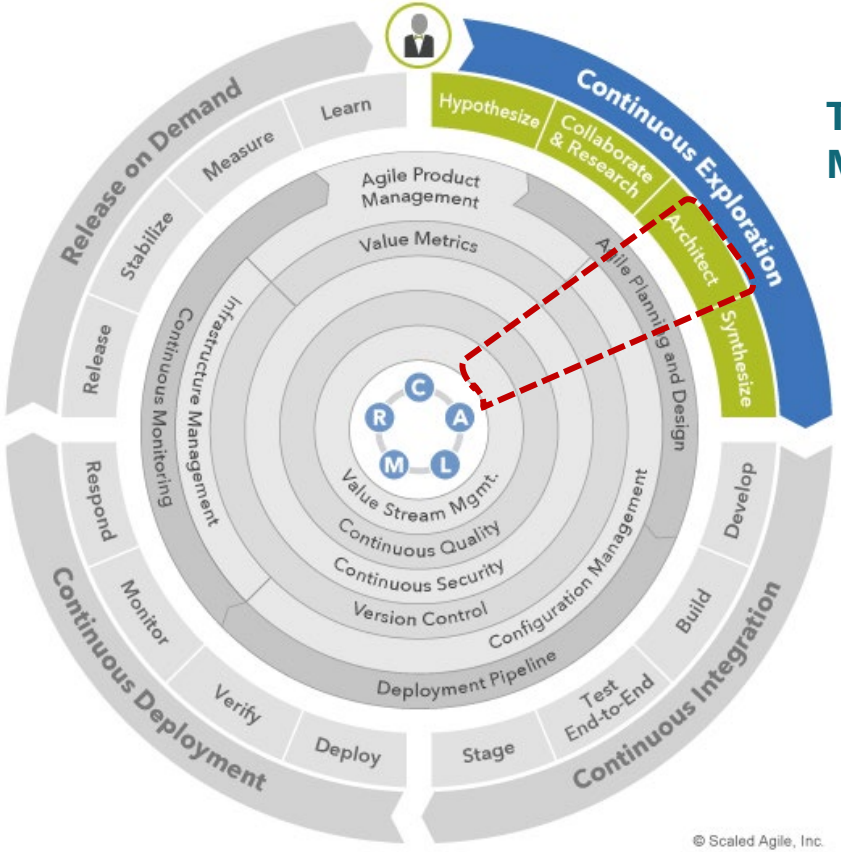
Continuous Delivery Pipeline

The Continuous Delivery Pipeline contains four aspects as per SAFe 5.0 methodology:

- Continuous exploration
- Continuous integration
- Continuous deployment
- Release on demand

Security needs to be strengthened in all these pillars for delivering secured product.

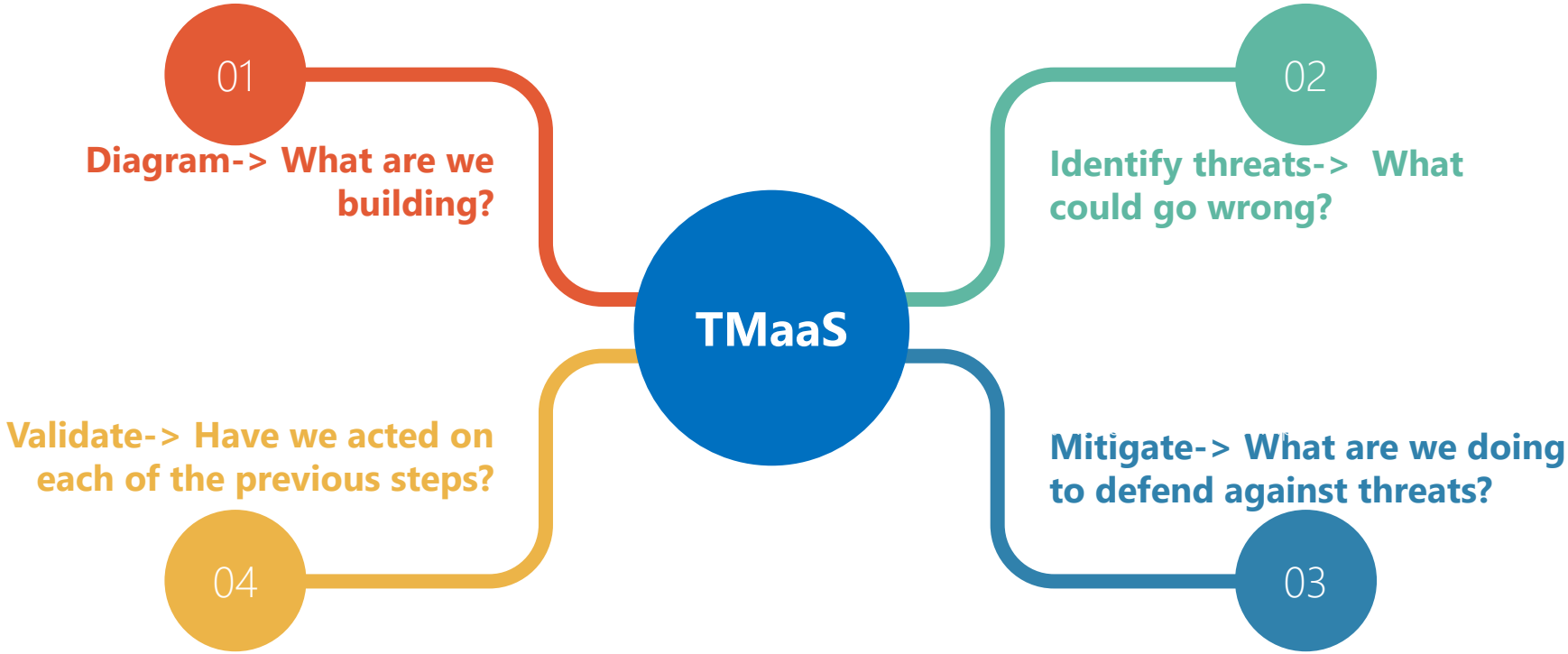
Security in Continuous Exploration



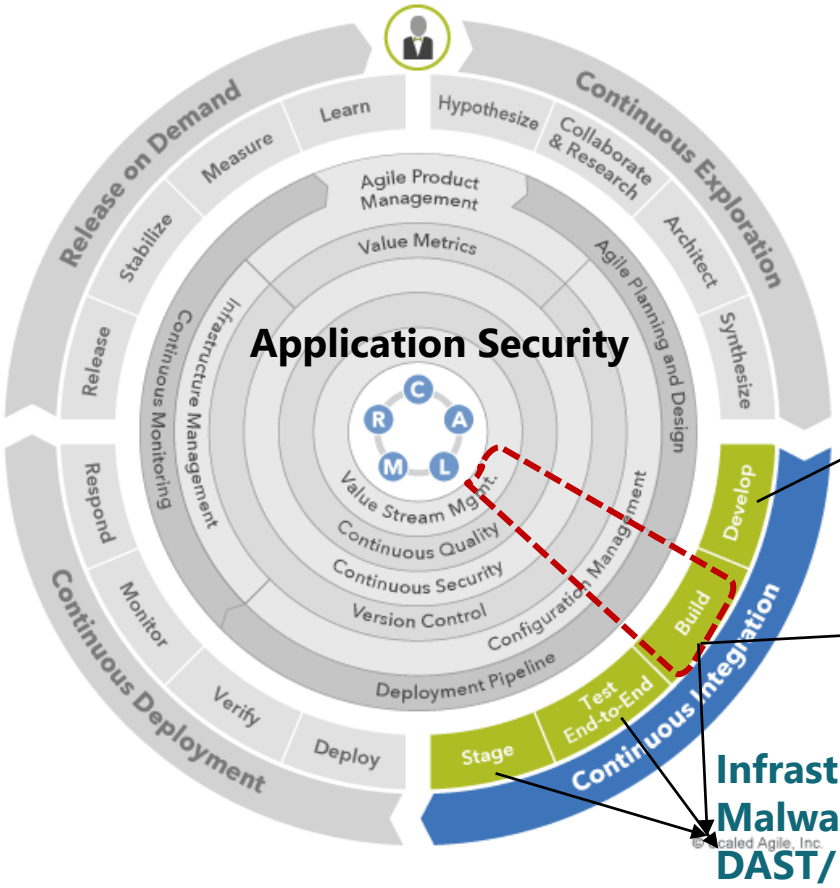
Threat Modeling

Enhance AppSec maturity and outcomes using DevSecOps Metrics

Threat Modeling as a service (TMaaS)



Security in Continuous Integration



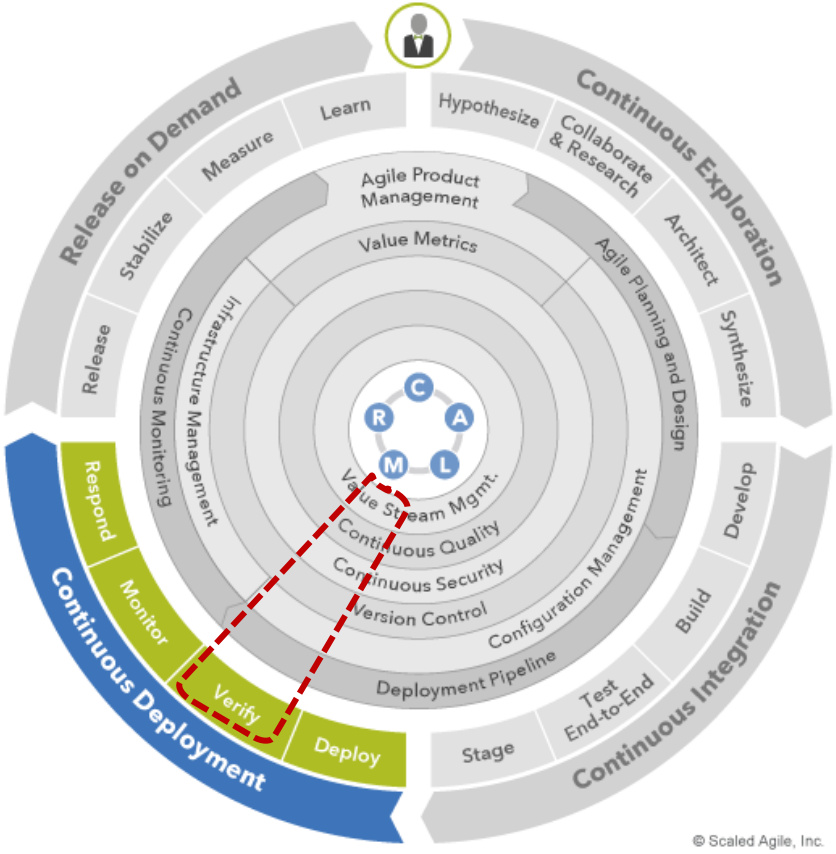
Security IDE Plug-ins
Code reviews/ Pair work

SAST/ Static Code Analysis
3rd Party scans
Fuzz Testing
Code signing

Infrastructure scans/
Malware scans
DAST/ Dynamic scans

Enhance AppSec maturity and outcomes using DevSecOps Metrics

Security in Continuous Deployment



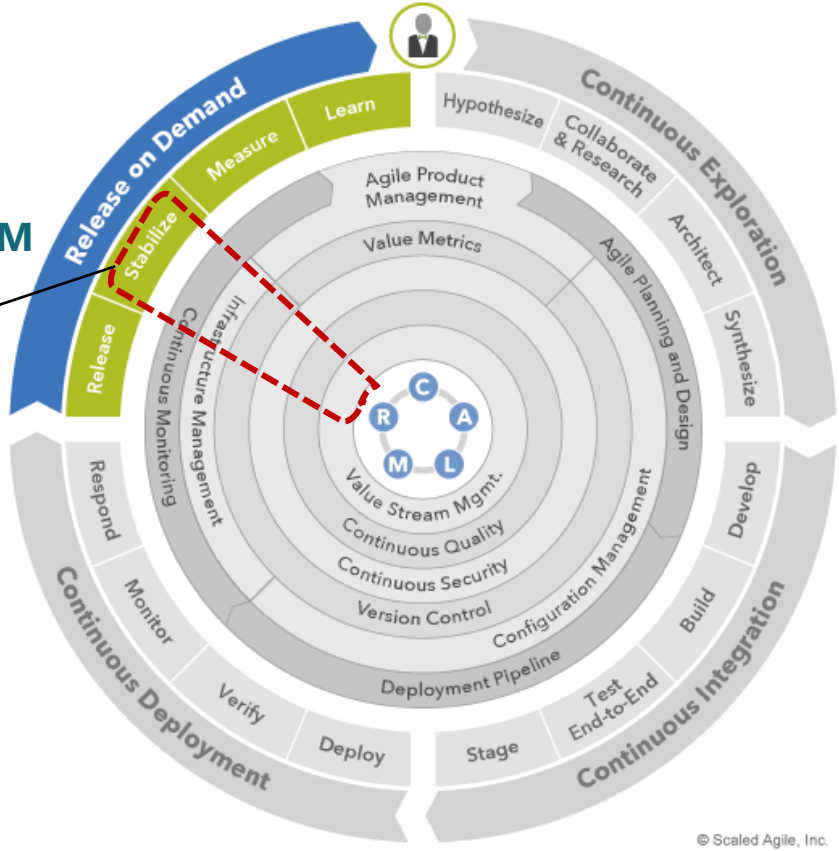
Penetration Testing

Enhance AppSec maturity and outcomes using DevSecOps Metrics

Security in Release on Demand

Continuous Security Monitoring using SIEM

Security Response Team
Incident Response
Security bulletins
Security Mailboxes

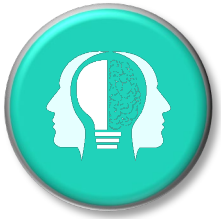


Enhance AppSec maturity and outcomes using DevSecOps Metrics

Key Best practices from Gartner and others leading experts

Automation is good

Shift Left for efficiency



Adopt a Security Champion

Training developers on security

Carry out threat modeling

Implement Strong Version Control

Focus on Known Open-Source Vulnerabilities

WhiteSource

DevSecOps Metrics

Reduced Total Security Tickets Opened

Reduced Time-to-Deploy

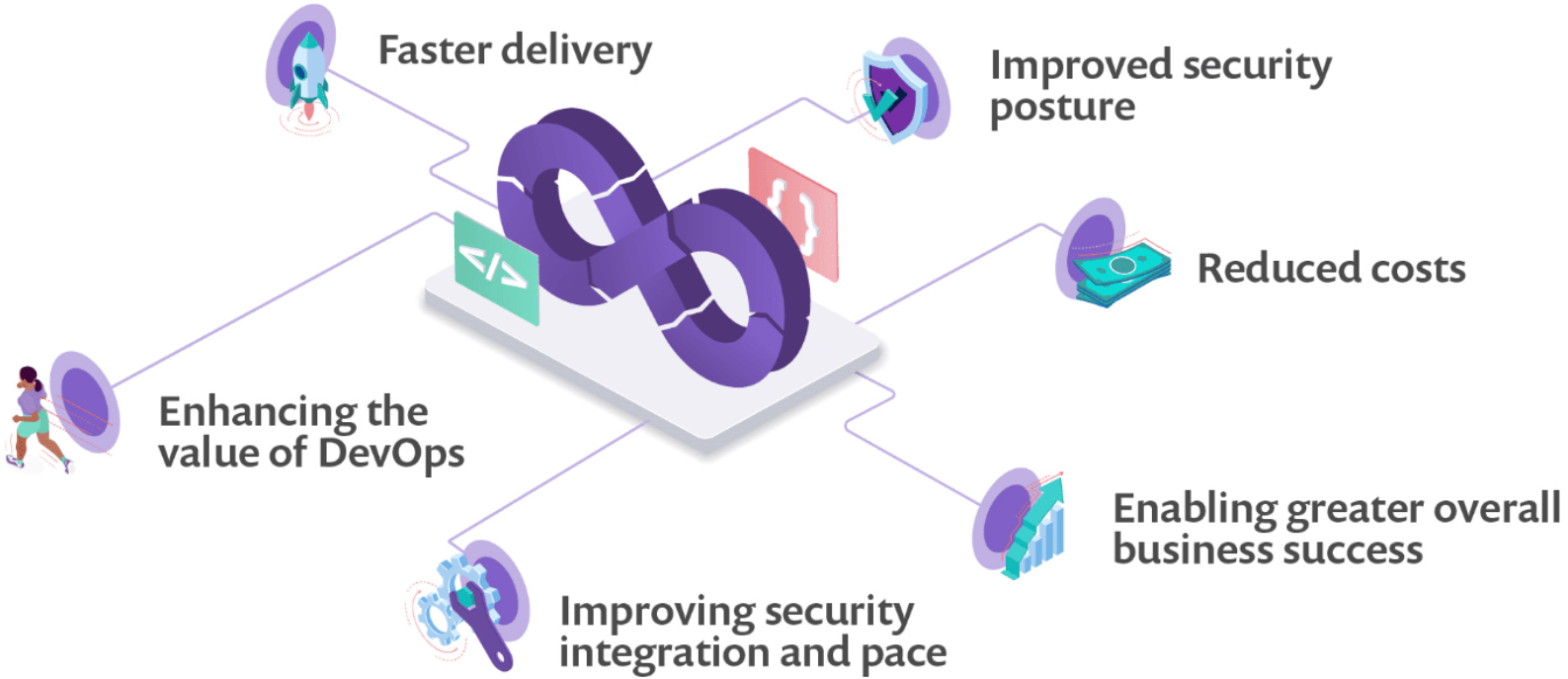
Discovery of Preproduction Vulnerabilities

Reduced Time-to-Remediate

Percentage of Security Audits Passed

Reducing Failed Security Tests

Meeting Business outcomes



Contact me @

Suresh Chandra Bose Ganesh Bose

SureshChandra.GaneshBose@cognizant.com

www.linkedin.com/in/gsubose/

https://twitter.com/gsubose

Thank you

Suresh Chandra Ganesh Bose SureshChandra.GaneshBose@Cognizant.com