synopsys®

Webinar

# DevSecOps Explained

# What is DevSecOps?

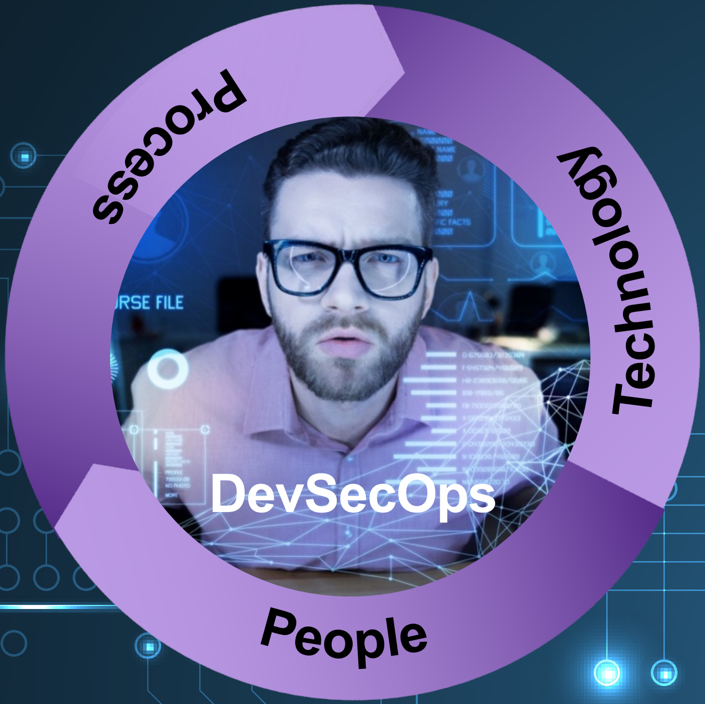
# Gartner definitions

**DevOps**—a change in IT culture focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach.

**DevSecOps**—information security architects integrating security at multiple points into DevOps workflows in a collaborative way that is largely transparent to developers, and preserving the teamwork, agility, and speed of DevOps and agile development environments.

Security activities must be an integral part of DevSecOps, and DevOps teams must own security in the same way they own development and operations.

# DevSecOps: A shift in culture



## CALMS

**Collaboration, Continuous feedback**

**Automation** sets up a converged software supply chain that is both reliable and repeatable

**Lean, Learning** from broken integrations, unacceptable metrics, and critical security issues

**Measurement**

**Sharing** goes hand-in-hand with the basic definition of DevSecOps

# The DevSecOps market problem

- Lack of awareness
- Organizational silos
- Complexity of modern applications
- Resource constraints
- Cultural change across organization

# Why DevSecOps is important

Security

Cost-effective

Faster time-to-market

Compliance

Improved collaboration

# Steps involved

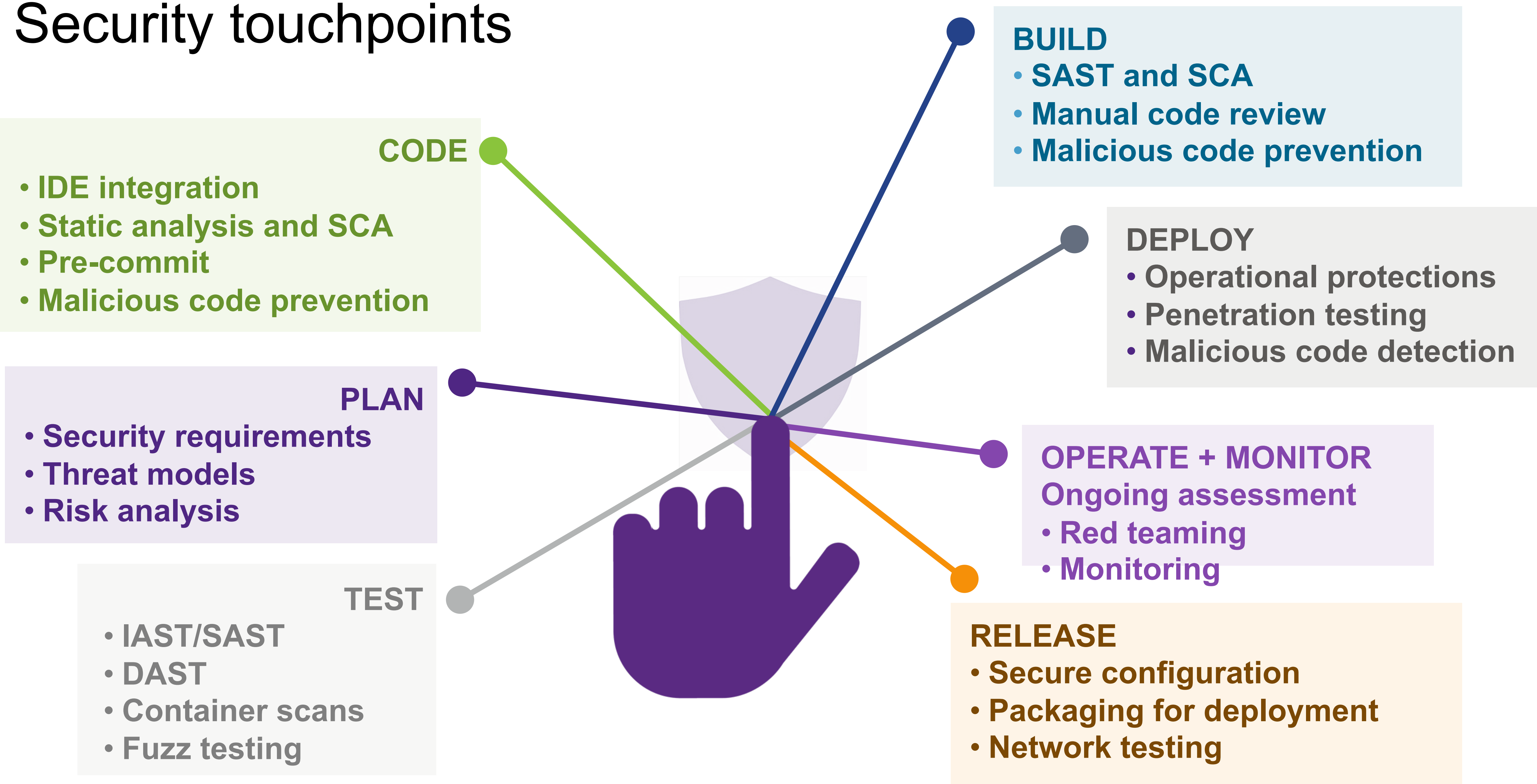
Planning

Development

Continuous integration and Continuous deployment (CI/CD)

Operations and maintenance

# Security touchpoints



**PLAN**
- Security requirements
- Threat models
- Risk analysis

**CODE**
- IDE integration
- Static analysis and SCA
- Pre-commit
- Malicious code prevention

**BUILD**
- SAST and SCA
- Manual code review
- Malicious code prevention

**TEST**
- IAST/SAST
- DAST
- Container scans
- Fuzz testing

**RELEASE**
- Secure configuration
- Packaging for deployment
- Network testing

**DEPLOY**
- Operational protections
- Penetration testing
- Malicious code detection

**OPERATE + MONITOR**
Ongoing assessment
- Red teaming
- Monitoring

# Recommended best practices

- Start with a clear plan
- Emphasize collaboration
- Prioritize automation
- Integrate security at every stage
- Make security a shared responsibility
- Monitor and assess risks continuously
- Stay up-to-date
- Foster a culture of security

# Key takeaways

- Adopting DevSecOps means shifting organization’s culture towards **CALMS**
  - Culture, Automation, Lean, Learning, Measurement, and Sharing
- Achieving successful DevSecOps is dependent on all three pillars
  - **people, process, and technology**
- Stakeholder enablement and **continuous collaboration** are key factors in building the people pillar of DevSecOps
- **Automation of tools and processes**, along with appropriate security checkpoints in CI/CD pipeline, mark the way forward for successful DevSecOps
- **Process pillar** of DevSecOps focuses on using technology to implement workflows such as breaking builds, approving artifacts, or conducting out-of-band activities
- **Defect management and metrics** dashboards can be used as a communication mechanism for all stakeholders to view project status and make go/no-go decisions

# Questions?

SYNOPSYS®
Silicon to Software™

# Thank You