Shifting Security Left

The Innovation of DevSecOps

Tom Stiehm

@ThomasStiehm

About Coveros

Coveros helps organizations accelerate software delivery using agile and DevOps methods

- Services
  - Agile Transformations & Coaching
  - Agile Software Development
  - Agile Testing & Automation
  - DevOps Implementations
  - DevSecOps Integrations

- Agile, DevOps, DevSecOps Security, Testing Training
  - Open Source Products
  - SecureCI – DevSecOps toolchain
  - Selenified – Agile test framework

How DevSecOps builds on DevOps

DevSecOps is a practice that rose from DevOps that includes information technology security as a fundamental aspect in all the stages of software development. -- Wikipedia

DevSecOps builds on DevOps by leveraging collaboration and feedback to address security concerns throughout the software development life cycle.

Shifting Security Left

- Shifting Left is taking a practice or process done late in development and doing it earlier.
- Shifting Security Left is doing security testing, analysis, and remediation during development, iteratively. Usually automating data collection to make it faster and cheaper.
- **The net result is making security practices part of the daily workflow of the development team.**

Why Shift Security Left?

Application Security is hard, error prone, and expensive. It is often made harder by trying to shoehorn it into the end of a release.

Shifting Left allows the teams to deal with security issues early and often:

- Reducing Risk
- Reducing Cost
- Leads to fewer errors
- Results in fewer security compromises

Security before the code is written

Be proactive:

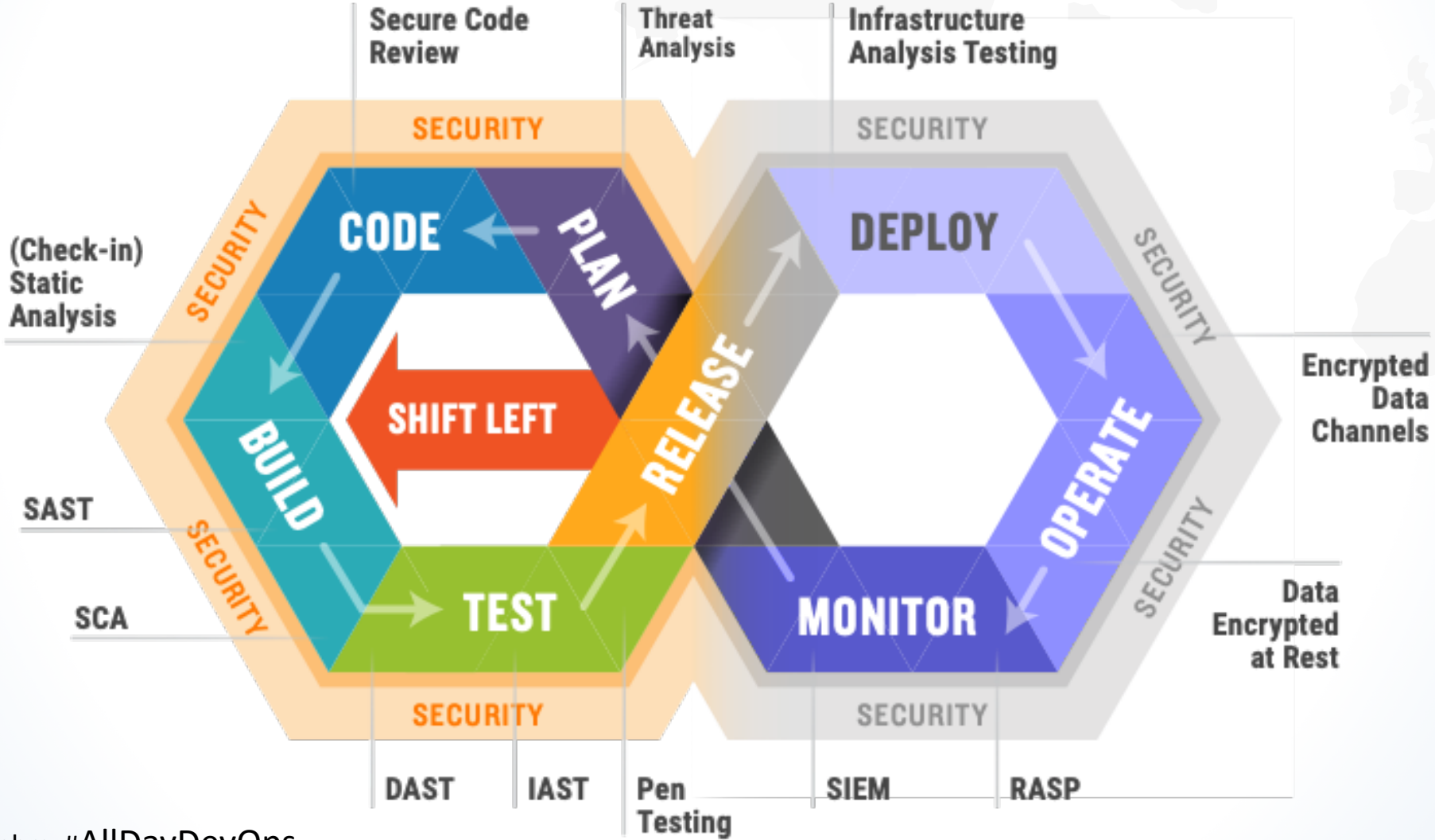
- Architect and design security in from the start based on threat analysis.
- Include security in your pipeline from the start.
- **Take time to analyze and remediate AppSec findings.**

Why?

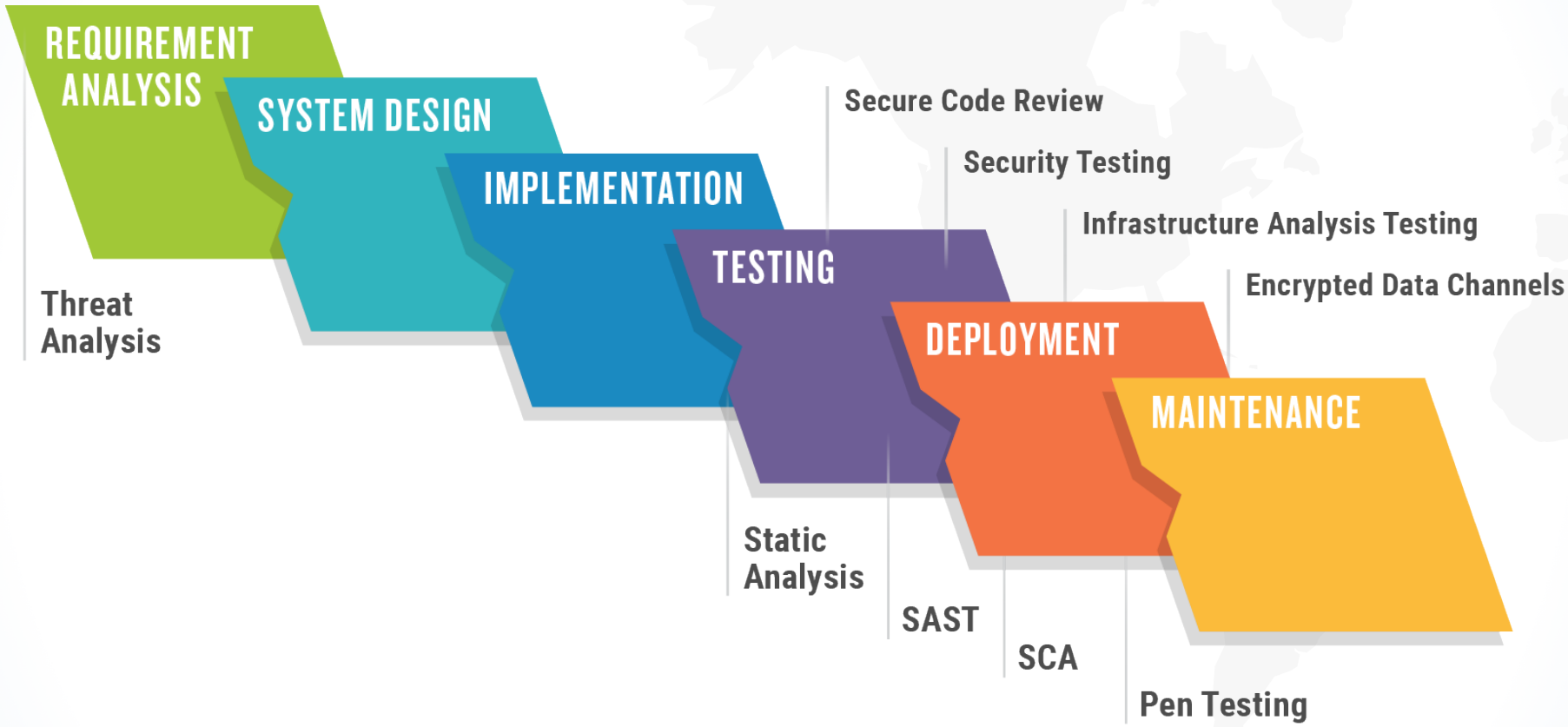
- Your software has security defects in it.
- Testing security into software at the end doesn't work.
- Relying on network and OS security to protect applications doesn't work.
- Ignoring security concerns doesn't work.

Security Practices in DevSecOps

Shifting Left includes reacting to the feedback on a regular basis.

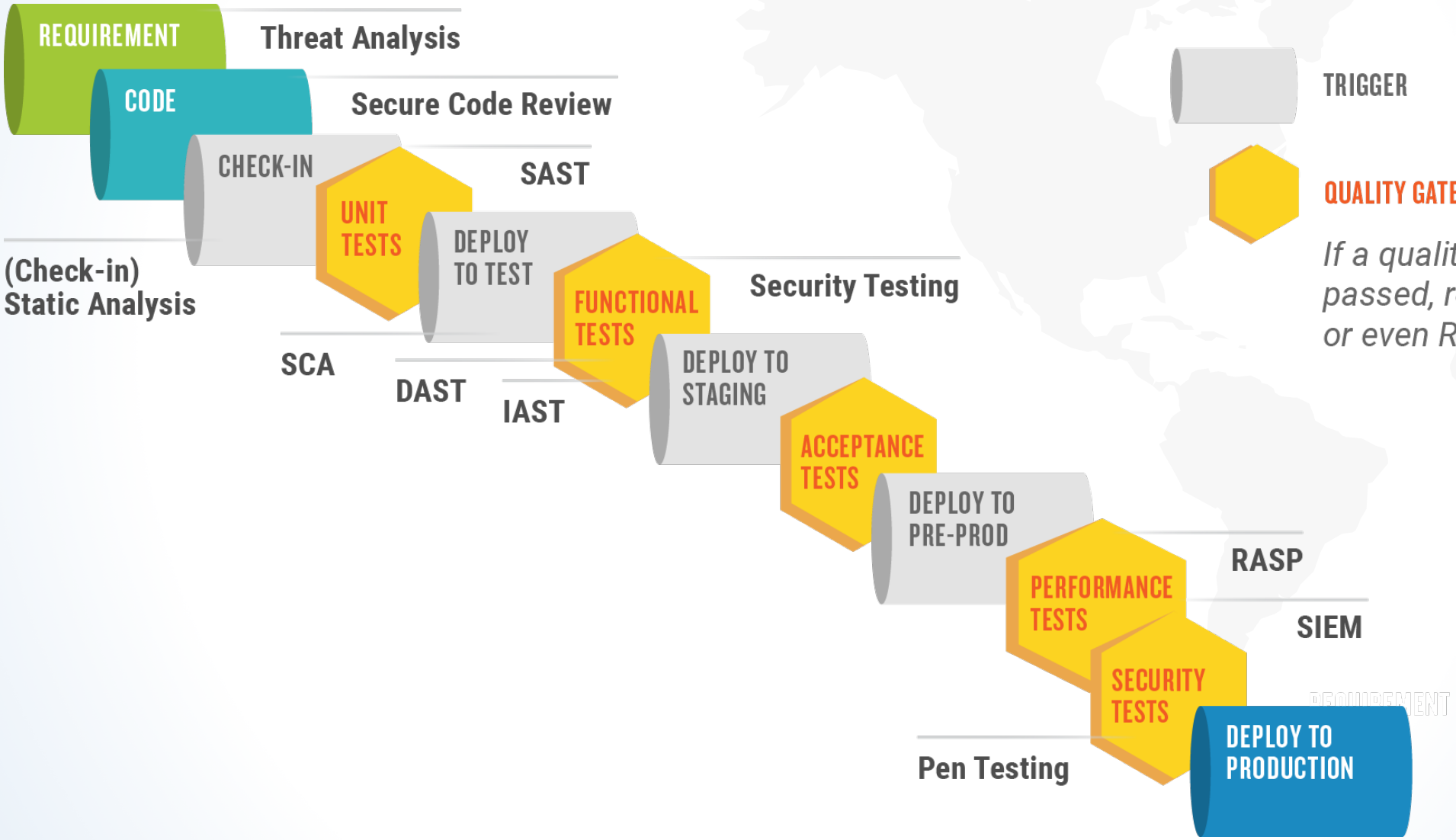


Legacy Security Practices



The Focus is on testing at the end.

Secure practices in a pipeline



Where to Start

- SCA - Install Software Composition Analysis
  - Expand existing CI/CD processes to scan your application dependencies
- SAST - Start with Static Application Security Testing
  - Quick to integration into a build pipeline
  - Leverages existing CI/CD assets
- DAST - Next integrate Dynamic Application Security Testing
  - Could be as simple as adding a DAST proxy to your existing automated or manual testing environment
  - Expand into using the automated aspects of DAST tools

Culture Shift

Goal Mindset: “Everyone is responsible for security.”

Three things to try when changing culture:

1. Build a Knowledge base
2. Promote Openness
3. Create Cybersecurity Champions

Need to experiment to find what works for your specific organization.

Wrap UP

#Coveros5

- Starting to Shift Left is more important then what practices you start with
- Greenfield start with Threat Analysis and build security in
- Legacy or brownfield start with SAST (or SCA or DAST)
- Iteratively add more security practices into your process
- Iteratively add more security to your build pipeline

Questions?
@thomasstiehm

- **Join me on Slack**
- **https://alldaydevops.slack.com/**
- **#2019addo-devsecops**