OWASP 2022 GLOBAL AppSec™

SAN FRANCISCO
NOV 14-18

Paul McCarty

DevSecOps Playbook: A step-by-step guide to implementing a DevSecOps program

SecureStack

SecureStack CEO

STARTUPS | DEVSECOPS | SNOWBOARDING

BOEING

NASA JPL

JOHN DEERE

Queensland Government

Regence

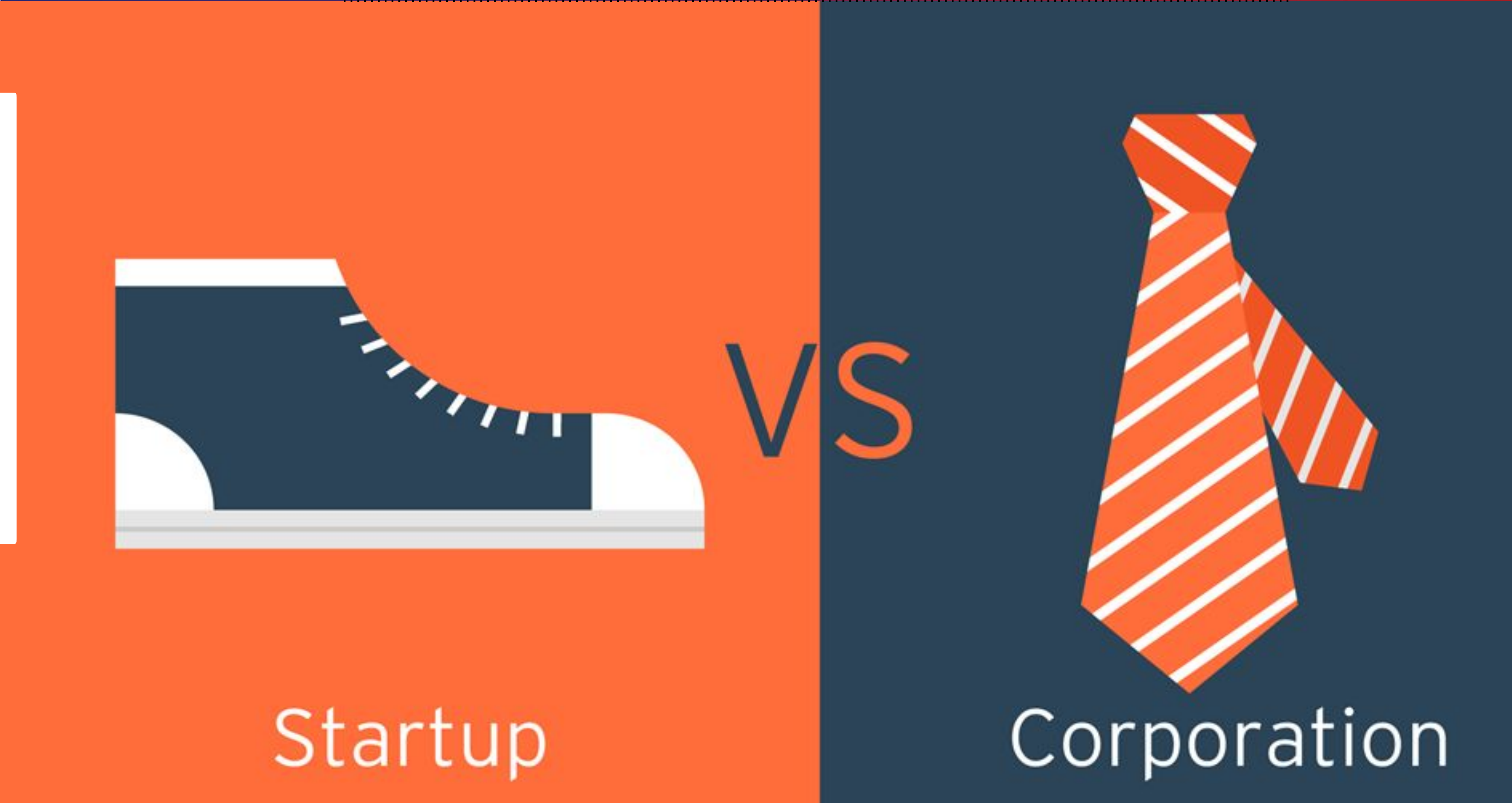
U.S.ARMY

The DevSecOps Playbook

What it is and why I wrote it

The Problem

Teams are not working together cohesively, so security & speed are still mutually exclusive


VS
Startup
Corporation

Evidence of the problem

1. Cloud sprawl: engineers have unfettered access to cloud
2. We are deploying at an increasing rate & engineers often use speed as a reason to not implement security controls
3. Mindset that short lived things don’t need securing

DevSecOps has never been as critical as it is now

70% Of developers admit to skipping security due to delivery timeframes

81% Of devs admit to pushing code with known vulnerabilities

96% Of cloud breaches are self-inflicted

Source: Osterman Research

Software Development Priorities

Features ✓

Speed ✓

Security ✗

Features ✓

Speed ✓

Security ✗

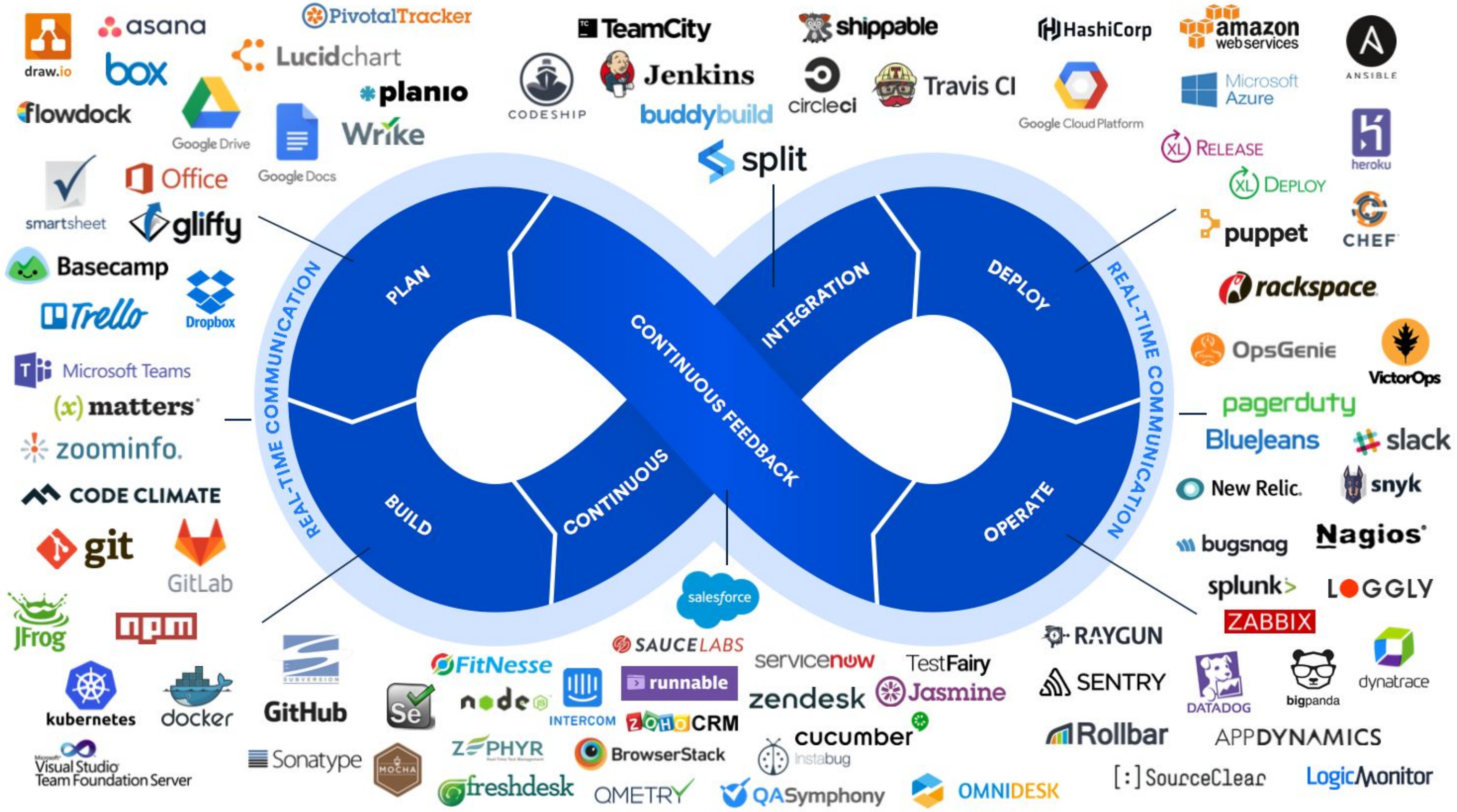
InfoSec hasn’t moved towards the center like ops and devs did during the “DevOps Revolution”

Evidence of the problem

1. Many InfoSec teams still focused on questionnaires
2. Still focused on the edge - not aligned w/cloud strategy
3. Security tooling is often siloed. My precioussssss!
4. As a result, companies have “right sized” infosec teams
5. DevSecOps is opportunity to bring InfoSec into our world

Operations has been devalued in the "cloud-native" world, which leads to the mess we're in

DevSecOps Playbook: A step-by-step guide to implementing a DevSecOps program



The Solution

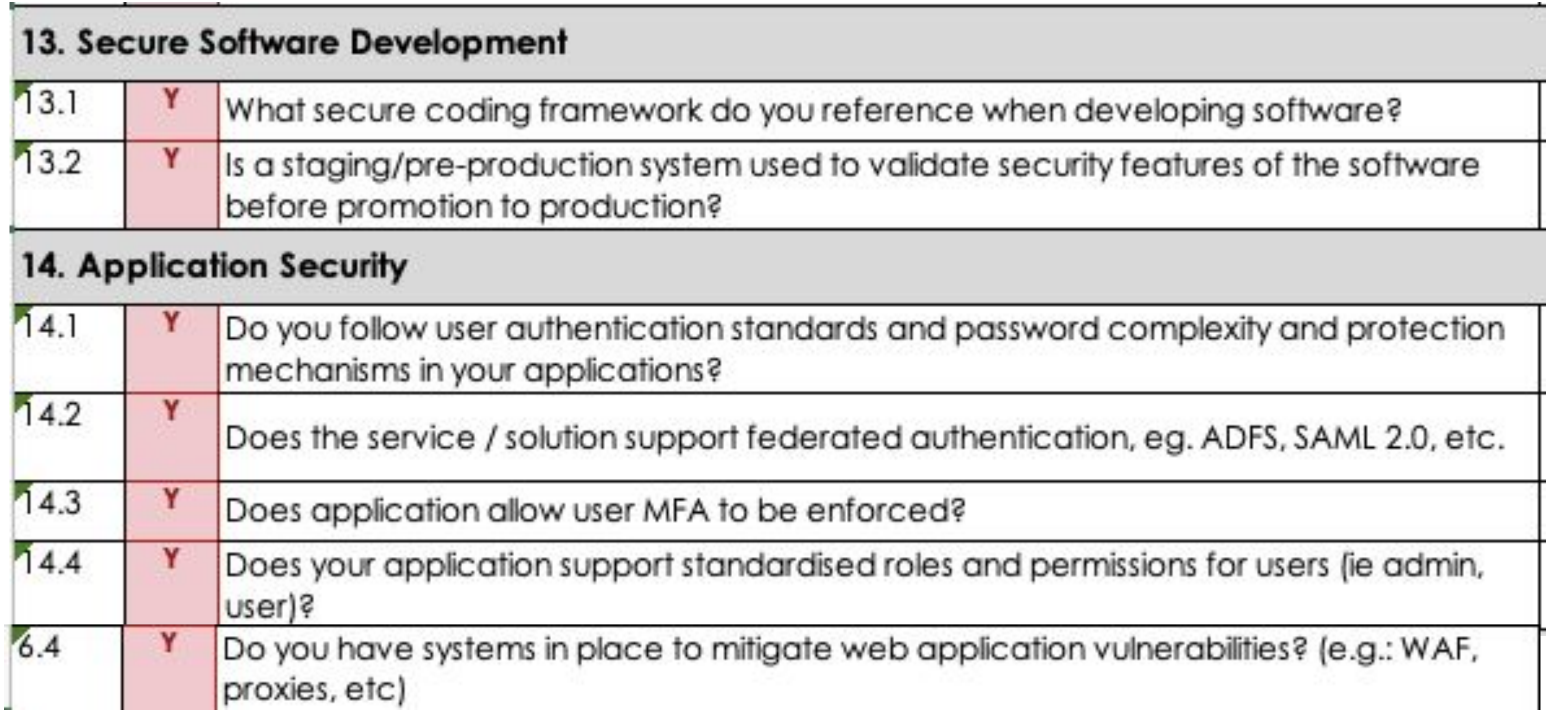
An easy, step-by-step implementation guide with individual tasks for any role, at any organization, prioritized by value & sorted by difficulty

My Requirements

1. Needed simple “checklist” style document
2. Focus on DevSecOps and collaboration
3. Multiple future compliance requirements, so needed a “matrix” of compliance mappings
4. Way to “pull” InfoSec and Ops to the Playbook

Objectives

1. I want to bring InfoSec teams in
2. Make AppSec a first class citizen for InfoSec
3. Address security questionnaires ahead of time
4. Increase CI/CD and automation maturity
5. Create a document that engineers, security and engineer teams feel they could make submissions to



13. Secure Software Development		
13.1	Y	What secure coding framework do you reference when developing software?
13.2	Y	Is a staging/pre-production system used to validate security features of the software before promotion to production?
14. Application Security		
14.1	Y	Do you follow user authentication standards and password complexity and protection mechanisms in your applications?
14.2	Y	Does the service / solution support federated authentication, eg. ADFS, SAML 2.0, etc.
14.3	Y	Does application allow user MFA to be enforced?
14.4	Y	Does your application support standardised roles and permissions for users (ie admin, user)?
6.4	Y	Do you have systems in place to mitigate web application vulnerabilities? (e.g.: WAF, proxies, etc)

Existing documents were inspiration for the Playbook

Minimal Viable Secure Product

MVSP

Secure Software Development Framework

NIST

Application Security Verification Standard

OWASP®

DevSecOps Maturity Model

DSOMM

Source: Osterman Research

What is Application Security?

Definition:

“Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification and abuse”

Application Security Primitives

1. **TEAM:** AppSec teams tend to be staffed primarily by software engineers, not sysadmin or secops
2. **PERSPECTIVE:** Concentration on software testing and secure coding practices
3. **SCOPE:** Appsec programs tend to concentrate more on securing the application than the whole environment
4. **TOOLS:** Git and IDE security integration, secure coding, risk analysis, security tooling (SCA, SAST & DAST)

OWASP has a great document about how to start your appsec program:

https://owasp.org/www-pdf-archive/OWASP_Quick_Start_Guide.pdf

What is DevSecOps?

Definition:

"DevSecOps automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery."

DevSecOps is a “portmanteau” of developers, security and operations. And that’s exactly what it should be: a collaboration of different teams working together to build better systems

DevSecOps Primitives

1. **TEAM:** Includes team members with more diverse (ops, security, qa, sre, dba, cloudops, appsec) backgrounds
2. **PERSPECTIVE:** Whole of SDLC automation: testing, delivery, deployment and cloud
3. **SCOPE:** DevSecOps focuses on the whole of the SDLC rather than the far left. App environment vs app.
4. **TOOLS:** CI/CD & deployment focus, security tools are automated at multiple levels, integration, monitoring

What DevSecOps is NOT

1. **CI/CD:** DevSecOps is more than a little bit of security testing in your CI/CD pipelines
2. **GARTNER:** Vendors and Gartner don't get to define what DevSecOps is.
3. **PRs:** DevSecOps does not all happen in PRs
4. **INFOSEC ONLY:** It's not about spying on devs
5. **OPS:** If your plan doesn't include Ops, then what is it?

DevSecOps Success Outcomes

Team members who are subject matter experts in a principal aspect of the application environment, but understands other aspects and can perform other functions across the team responsibilities.

A reminder...

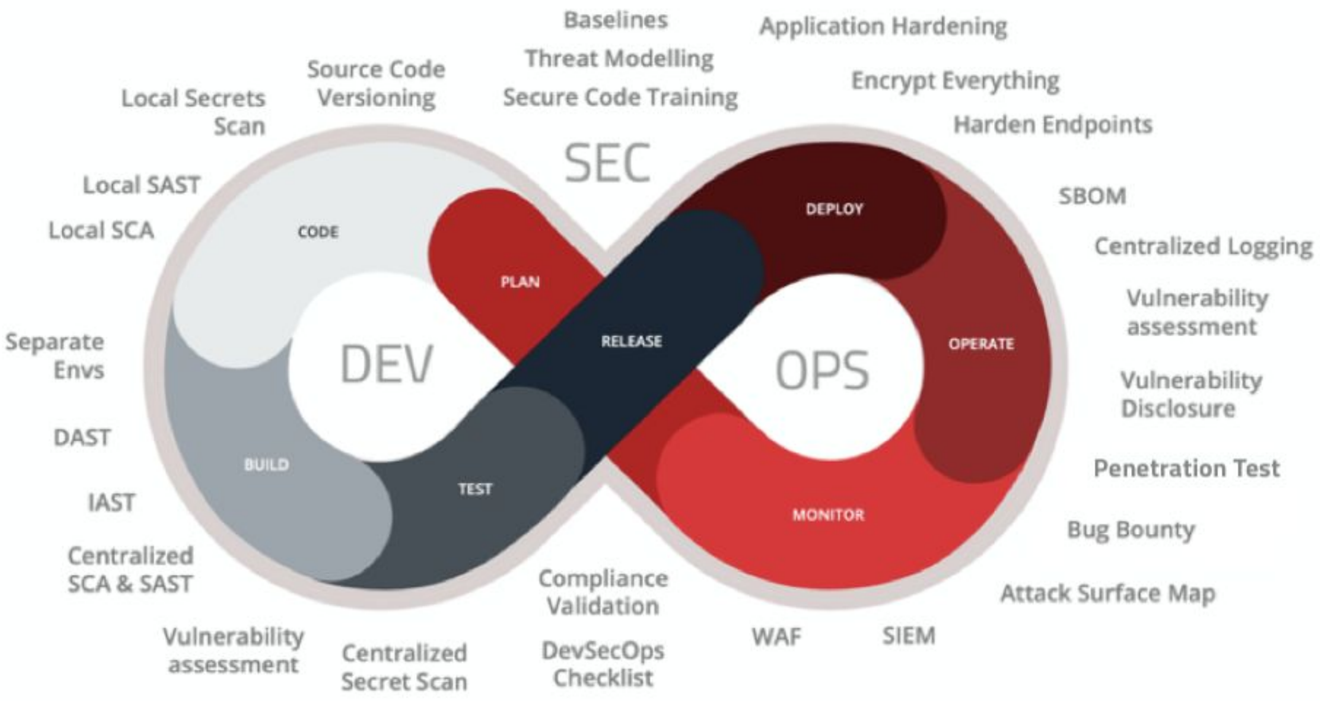
I am trying to help my teams working more collaboratively. I am not trying to build an AppSec team

How to start a DevSecOps program?

1. **ASSESS:** Spend a month or two to identify your assets, applications, teams and resources and then devise a game plan & identify your entry points. Choose your LZ carefully & execute
2. **CHAMPIONS:** Who are the natural champions and who will lead the charge? Doers will do and followers will follow
3. **PRIORITIZE:** Make it a priority at your company to improve application security and deployment. Get management involved on a weekly or monthly basis. Evangelize DevSecOps everywhere
4. **COLLABORATION:** Identify the relevant teams you need to interact with and empower them to be a part of the process. Enable other teams to join the process as well. Onboarding, playbooks and templates are key
5. **QUANTIFY:** Learn how to quantify success as it's a long slow journey so make sure you are celebrating it. KPIs that don't suck

DevSecOps Playbook: A step-by-step guide to implementing a DevSecOps program

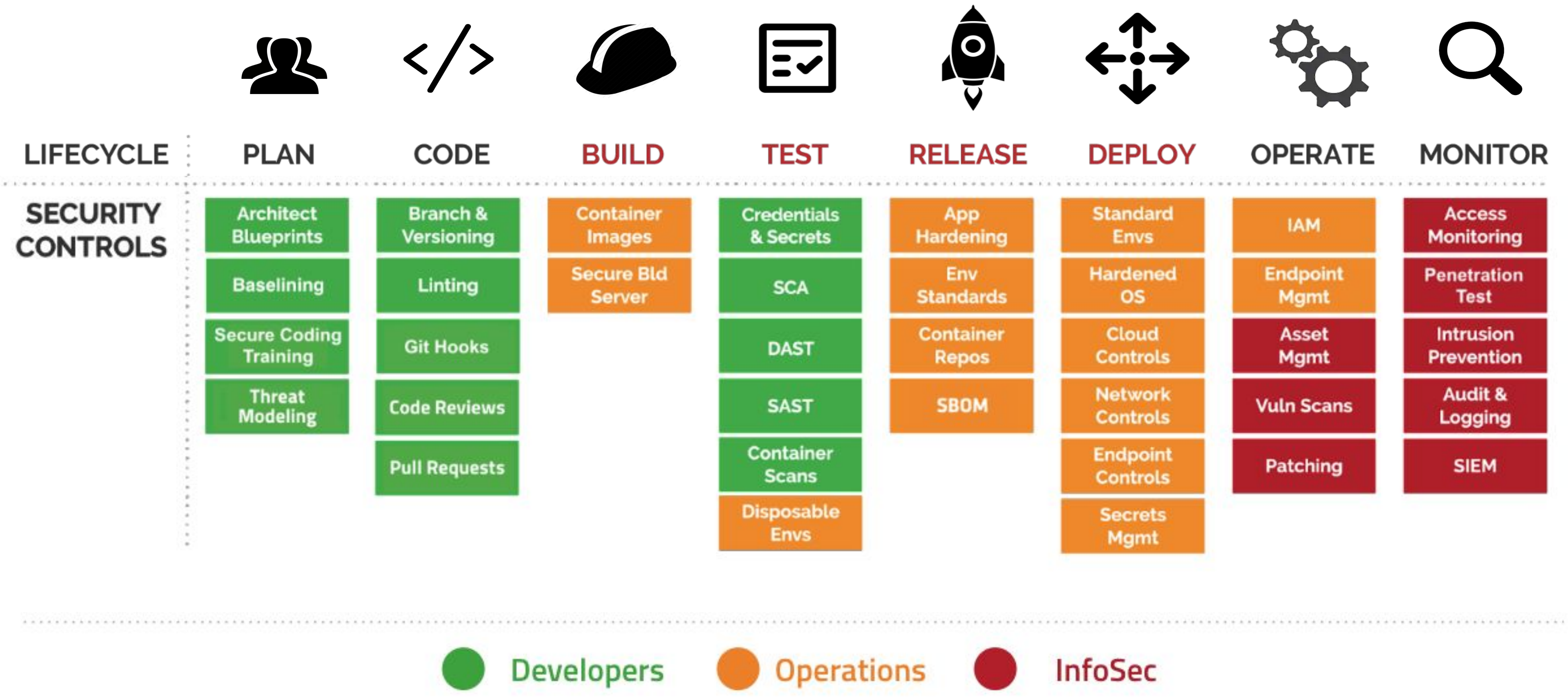
DevSecOps Playbook



LIFECYCLE	PLAN	CODE	BUILD	TEST	RELEASE	DEPLOY	OPERATE	MONITOR

OWASP USA | 2022

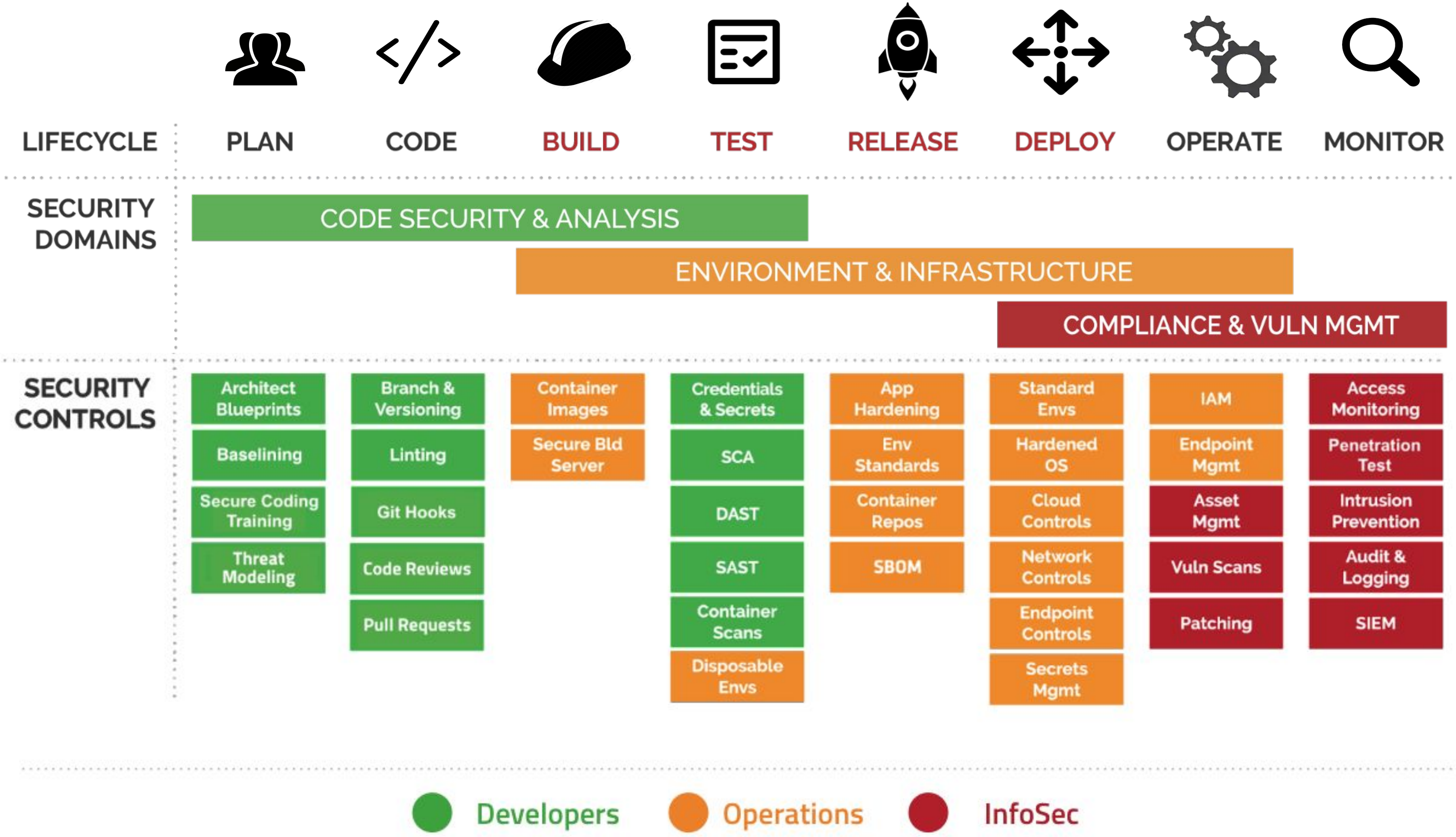
DevSecOps Playbook: A step-by-step guide to implementing a DevSecOps program



LIFECYCLE	PLAN	CODE	BUILD	TEST	RELEASE	DEPLOY	OPERATE	MONITOR
SECURITY CONTROLS	Architect Blueprints	Branch & Versioning	Container Images	Credentials & Secrets	App Hardening	Standard Envs	IAM	Access Monitoring
	Baselining	Linting	Secure Bld Server	SCA	Env Standards	Hardened OS	Endpoint Mgmt	Penetration Test
	Secure Coding Training	Git Hooks		DAST	Container Repos	Cloud Controls	Asset Mgmt	Intrusion Prevention
	Threat Modeling	Code Reviews		SAST	SBOM	Network Controls	Vuln Scans	Audit & Logging
		Pull Requests		Container Scans		Endpoint Controls	Patching	SIEM
				Disposable Envs		Secrets Mgmt		

● Developers ● Operations ● InfoSec

DevSecOps Playbook: A step-by-step guide to implementing a DevSecOps program



SECURITY DOMAINS

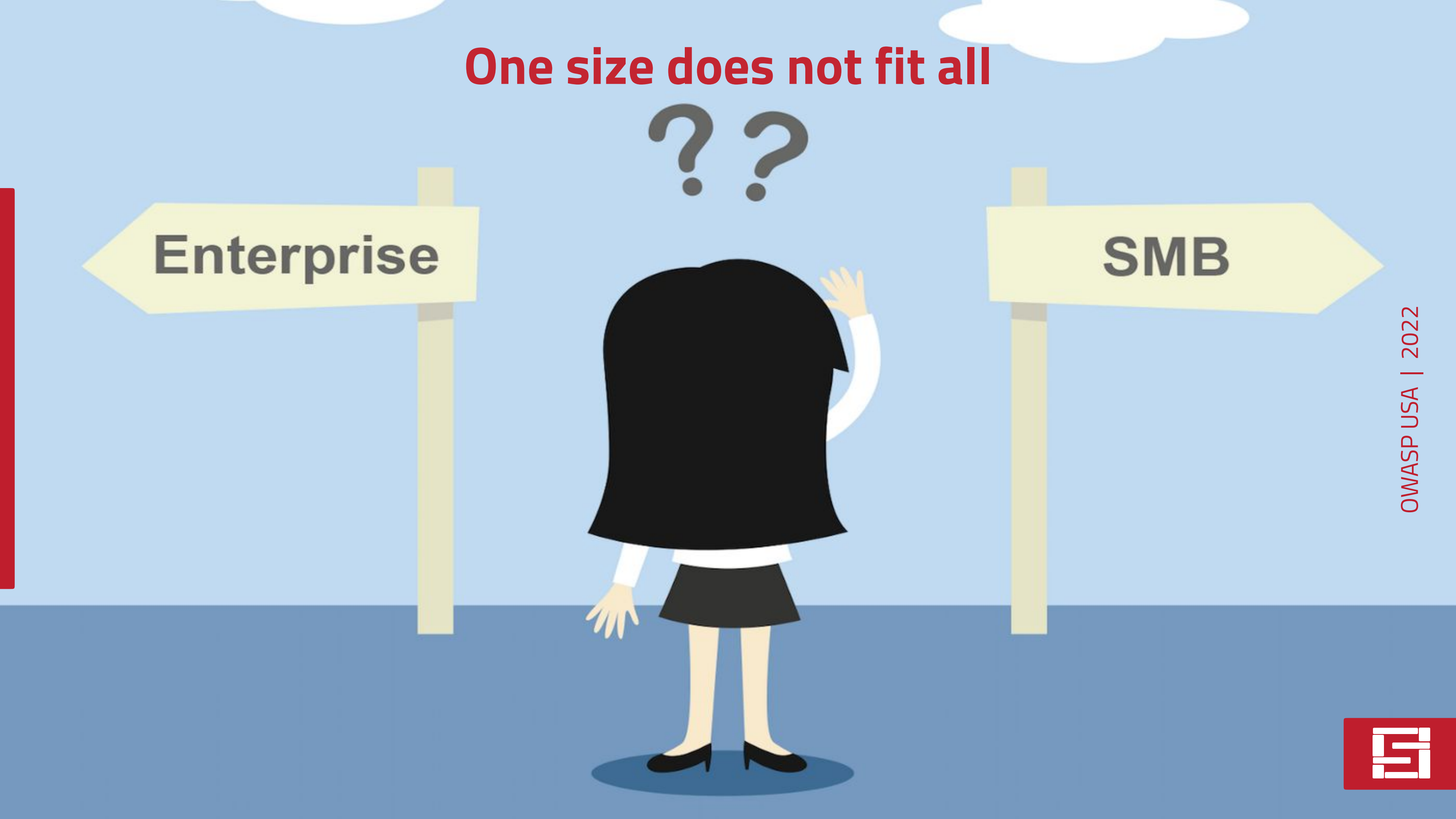
- CODE SECURITY & ANALYSIS (PLAN – TEST)
- ENVIRONMENT & INFRASTRUCTURE (BUILD – OPERATE)
- COMPLIANCE & VULN MGMT (DEPLOY – MONITOR)

SECURITY CONTROLS

LIFECYCLE	PLAN	CODE	BUILD	TEST	RELEASE	DEPLOY	OPERATE	MONITOR
SECURITY CONTROLS	🟩 Architect Blueprints	🟩 Branch & Versioning	🟧 Container Images	🟩 Credentials & Secrets	🟧 App Hardening	🟧 Standard Envs	🟧 IAM	🟥 Access Monitoring
	🟩 Baselining	🟩 Linting	🟧 Secure Bld Server	🟩 SCA	🟧 Env Standards	🟧 Hardened OS	🟧 Endpoint Mgmt	🟥 Penetration Test
	🟩 Secure Coding Training	🟩 Git Hooks		🟩 DAST	🟧 Container Repos	🟧 Cloud Controls	🟥 Asset Mgmt	🟥 Intrusion Prevention
	🟩 Threat Modeling	🟩 Code Reviews		🟩 SAST	🟧 SBOM	🟧 Network Controls	🟥 Vuln Scans	🟥 Audit & Logging
		🟩 Pull Requests		🟩 Container Scans		🟧 Endpoint Controls	🟥 Patching	🟥 SIEM
				🟧 Disposable Envs		🟧 Secrets Mgmt		

🟩 Developers 🟧 Operations 🟥 InfoSec

One size does not fit all



What’s different for startups?

Size and Team, duh!?

- No SMEs, so everybody kinda does everything
- Mostly driven by developers
- Often, no real infrastructure experience at all

What’s different for startups?

Size and Team, duh!?

- No SMEs, so everybody kinda does everything
- Mostly driven by developers
- Often, no real infrastructure experience at all

How do we compensate?

- Break the tasks into “domains” of ownership
- Add a prioritization system - What you should do first
- Define how difficult the task is so the team understands the ROI

Show the bloody repo already!

DEMO

https://github.com/6mile/DevSecOps-Playbook

What does the future hold?

Future work

- Add a second markdown page that will have more in depth detail about each task
- Add *specific* compliance requirements rather than “SSDF1.1” or “CIS8”
- Add more compliance frameworks
- Add the ability to sort by priority and difficulty
- FIND MORE COLLABORATORS

Paul McCarty

@eastside-mccarty

✉ paulm@securestack.com

SECURESTACK