VERACODE

Overcoming the DevSecOps Imposter Syndrome

Life is too short

Michael Man

July 2022

DevSecOps Evangelist

- Founder of “DevSecOps – London Gathering”
- Member of the DevSecCon CFP Review Board
- OpenUK Ambassador
- Offensive Security Certified Professional

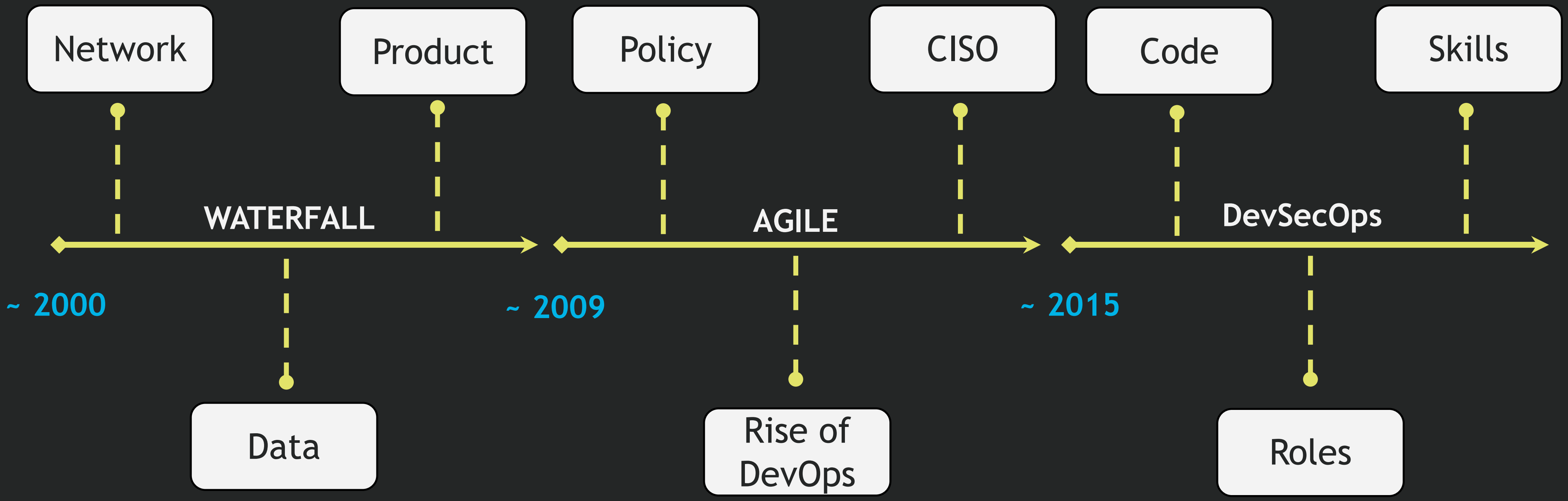
dsotraining.github.io

What is DevSecOps?

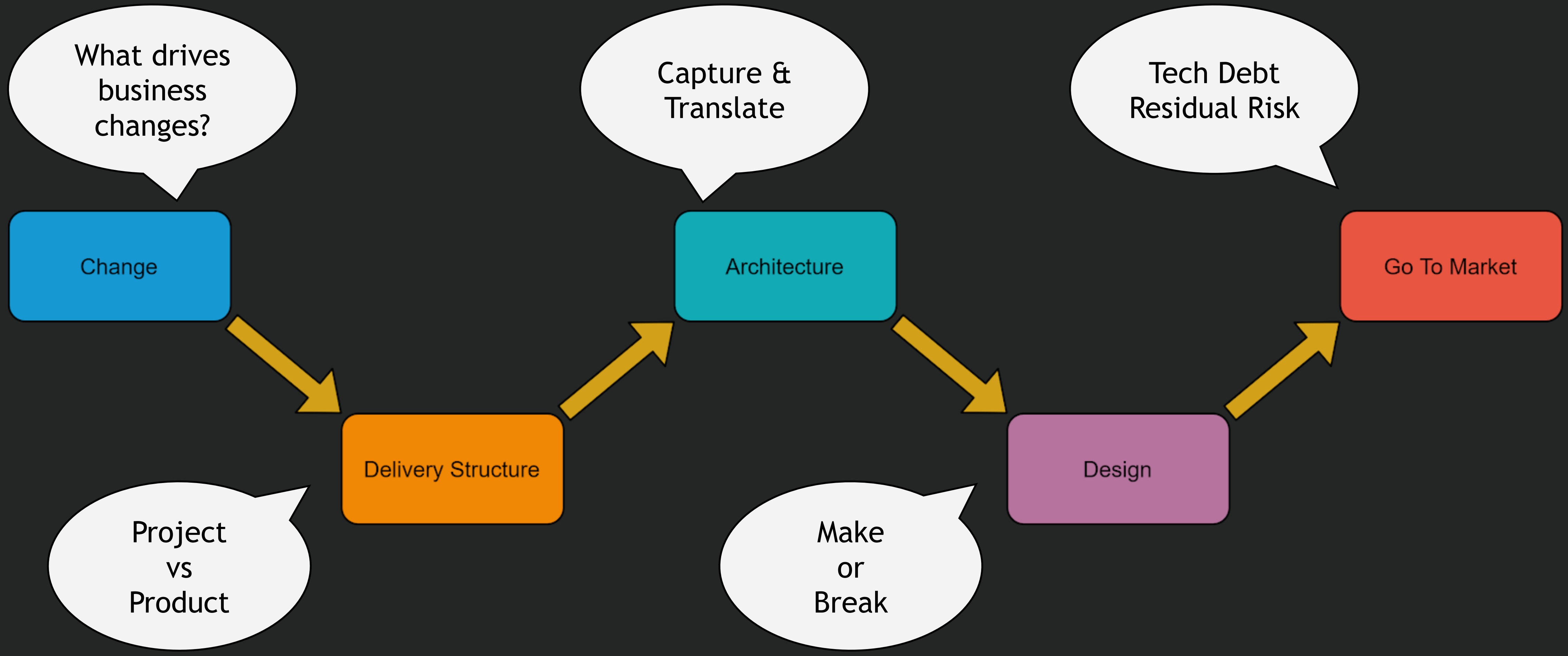
Where do you start?

Who can I talk to?

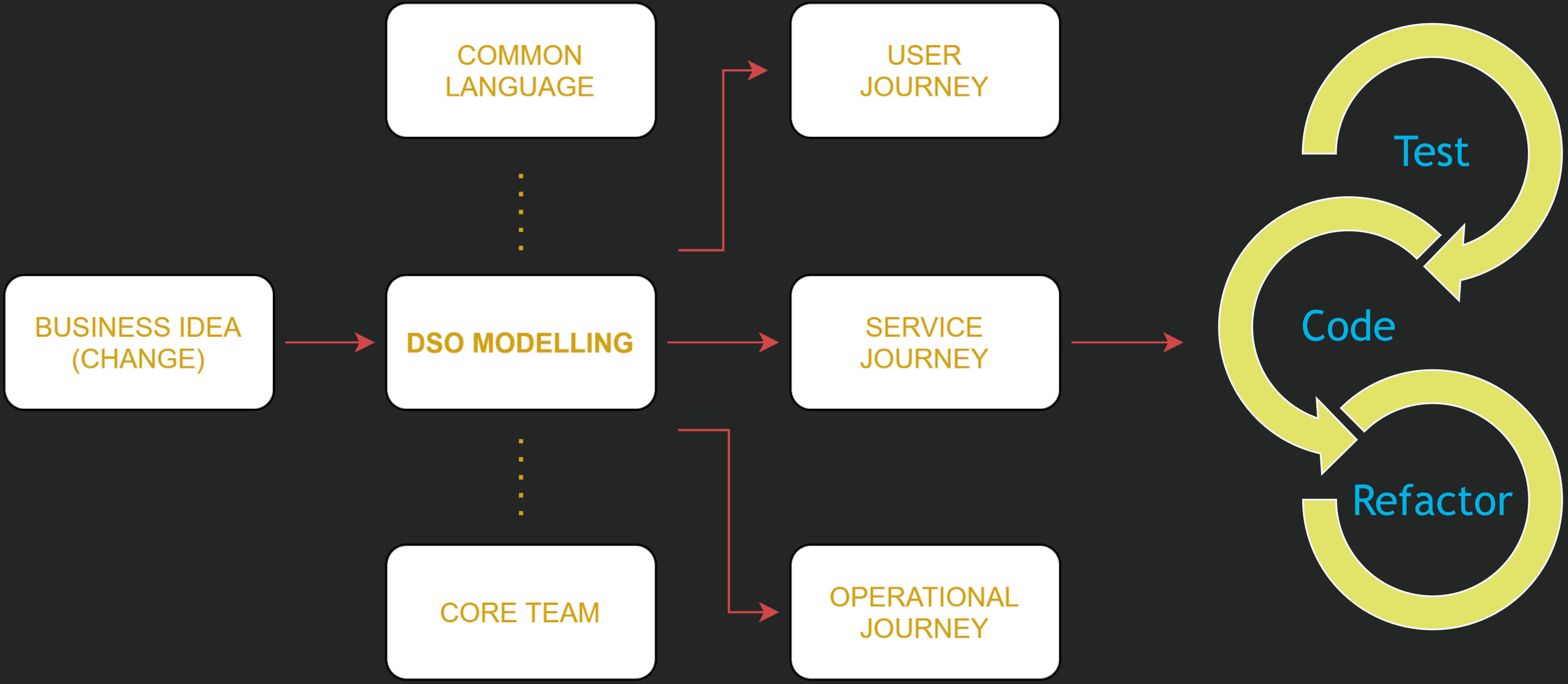
Development & Security Timeline



Delivery Key Stages



DSO Modelling

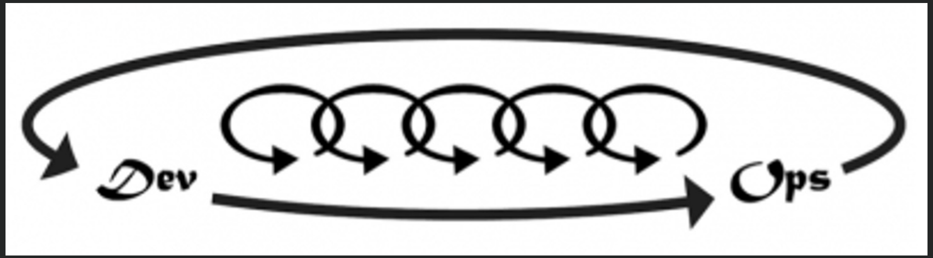


VERACODE

Principles

Lots of Theory

DevOps Principles



https://itrevolution.com/the-three-ways-principles-underpinning-devops/

IT REVOLUTION

The Five Ideals of DevOps

The Unicorn Project by Gene Kim

1 LOCALITY & SIMPLICITY

2 FOCUS, FLOW & JOY

3 IMPROVEMENT OF DAILY WORK

4 PSYCHOLOGICAL SAFETY

5 CUSTOMER FOCUS

https://itrevolution.com/five-ideals-of-devops/

https://itrevolution.com/five-ideals-of-devops/

The Three Ways

- Flow / Systems Thinking
- Amplify Feedback Loops
- Culture of Continual Experimentation & Learning

The Five Ideals

- Locality & Simplicity
- Focus, Flow & Joy
- Improvement of Daily Work
- Psychological Safety
- Customer Focus

Security Principles

CIA

- Confidentiality: Only authorized users and processes should be able to access data
- Integrity: Data should be maintained in a correct state, and nobody should be able to improperly modify it, either accidentally or maliciously
- Availability: Authorized users and processes should be able to access data whenever they need to do so

DIE

- Distributed: preventing dependence on a single system
- Immutable: making assets impossible to change
- Ephemeral: designing assets to have a short and defined lifespan

Three R's

- Rotate datacenter credentials every few minutes or hours.
- Repave every server and application in the datacenter every few hours from a known good state
- Repair vulnerable operating systems and application stacks consistently within hours of patch availability

DSO Principles

- Avoid process handover tasks and manual actions
- Automate environment creation and application deployment activities
- Adopt common SDLC tools
- Adopt lean agile software principles with small, incremental and frequent releases.
- Construct your delivery team to consist of a mixed skill set covering all key disciplines
- Measure and quantify your solution security profile
- Deploy immutable infrastructure

CIA: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

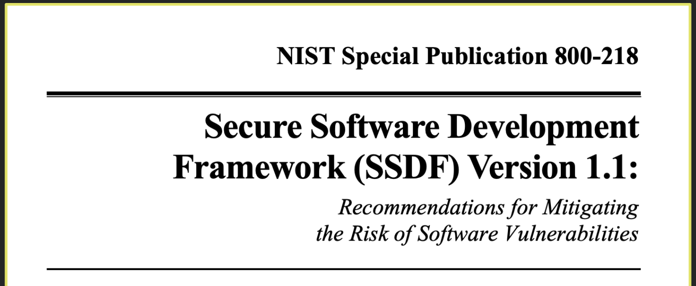
DIE: https://www.fastly.com/blog/the-dept-of-know-live-sounil-yu-on-why-embracing-the-die-security-model-means-faster-innovation

Three Rs: https://tanzu.vmware.com/content/blog/the-three-r-s-of-enterprise-security-rotate-repave-and-repair

DSO Principles: https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

VERACODE

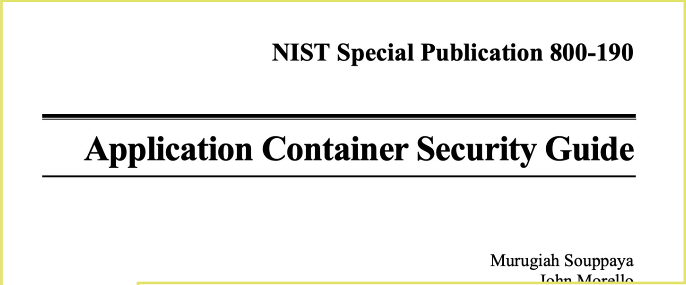
Standards & Benchmarks



NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

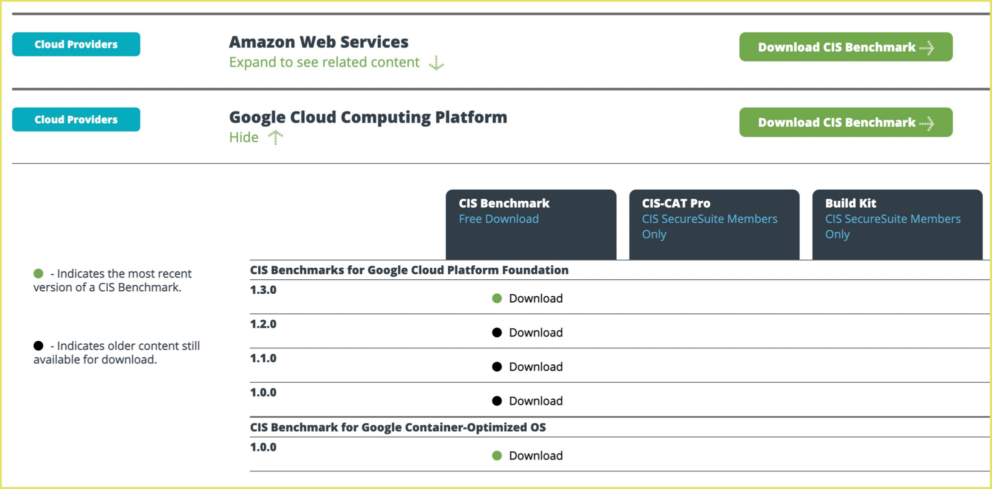
Recommendations for Mitigating the Risk of Software Vulnerabilities



NIST Special Publication 800-190

Application Container Security Guide

Murugiah Souppaya
John Morello



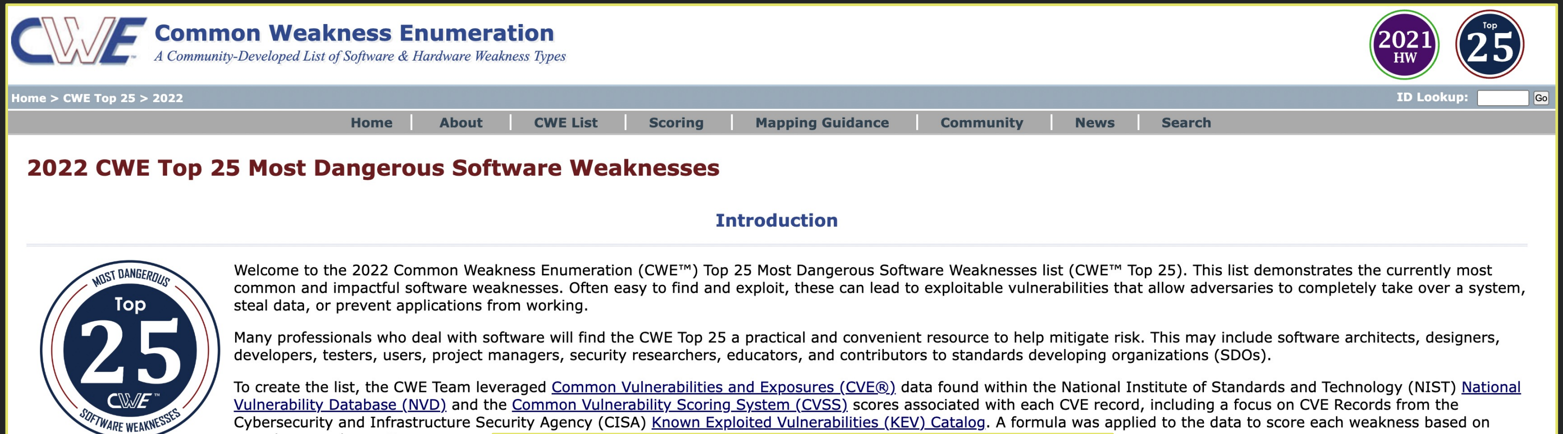
Cloud Providers — **Amazon Web Services** — Expand to see related content — Download CIS Benchmark

Cloud Providers — **Google Cloud Computing Platform** — Hide — Download CIS Benchmark

	CIS Benchmark Free Download	CIS-CAT Pro CIS SecureSuite Members Only	Build Kit CIS SecureSuite Members Only
CIS Benchmarks for Google Cloud Platform Foundation			
1.3.0	● Download		
1.2.0	● Download		
1.1.0	● Download		
1.0.0	● Download		
CIS Benchmark for Google Container-Optimized OS			
1.0.0	● Download		

● - Indicates the most recent version of a CIS Benchmark.

● - Indicates older content still available for download.



Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home > CWE Top 25 > 2022 — ID Lookup: Go

Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

2022 CWE Top 25 Most Dangerous Software Weaknesses

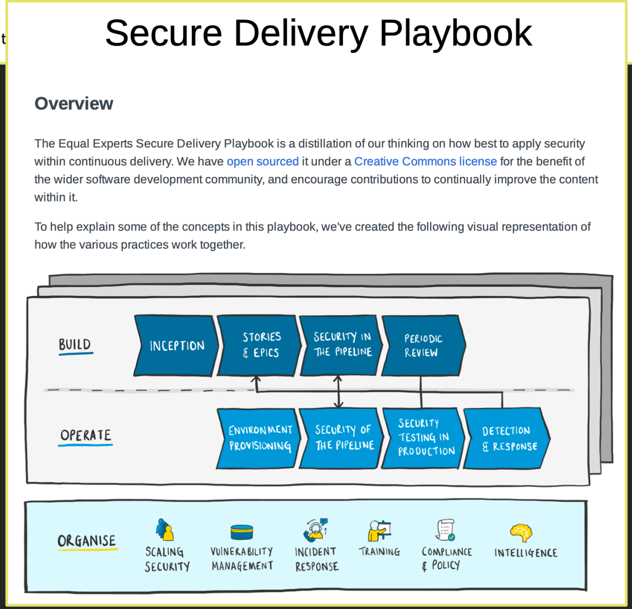
Introduction

Welcome to the 2022 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses list (CWE™ Top 25). This list demonstrates the currently most common and impactful software weaknesses. Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

Many professionals who deal with software will find the CWE Top 25 a practical and convenient resource to help mitigate risk. This may include software architects, designers, developers, testers, users, project managers, security researchers, educators, and contributors to standards developing organizations (SDOs).

To create the list, the CWE Team leveraged Common Vulnerabilities and Exposures (CVE®) data found within the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS) scores associated with each CVE record, including a focus on CVE Records from the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog. A formula was applied to the data to score each weakness based on prevalence and severity.

The dataset analyzed to calculate the 2022 Top 25 contained a t



Secure Delivery Playbook

Overview

The Equal Experts Secure Delivery Playbook is a distillation of our thinking on how best to apply security within continuous delivery. We have open sourced it under a Creative Commons license for the benefit of the wider software development community, and encourage contributions to continually improve the content within it.

To help explain some of the concepts in this playbook, we've created the following visual representation of how the various practices work together.

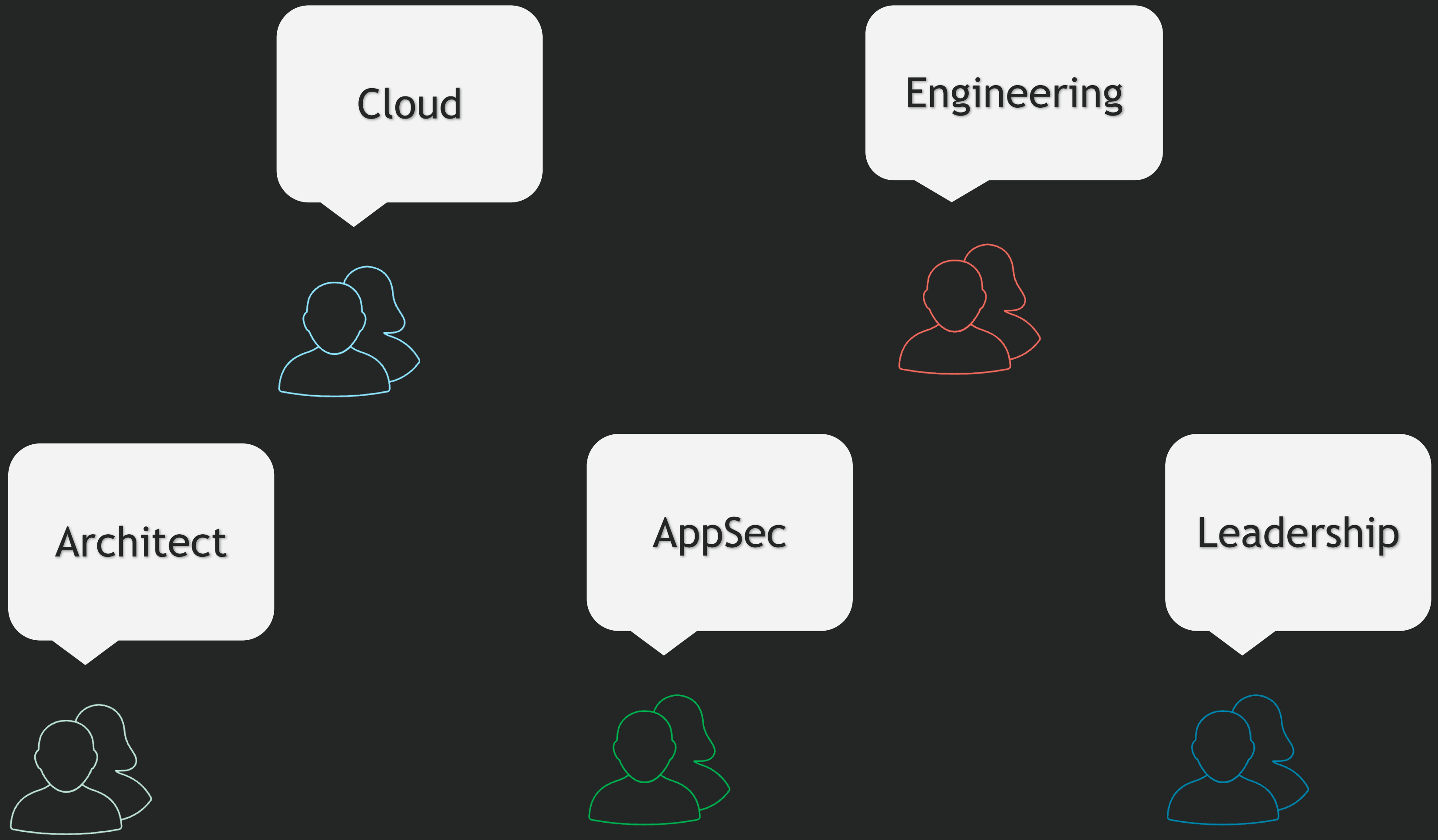
https://secure-delivery.playbook.ee/

VERACODE

Roles

Who Do I Want To Be?

Roles: DevSecOps Knowledge Domain



Cloud

Engineering

Architect

AppSec

Leadership

Tools & Testing

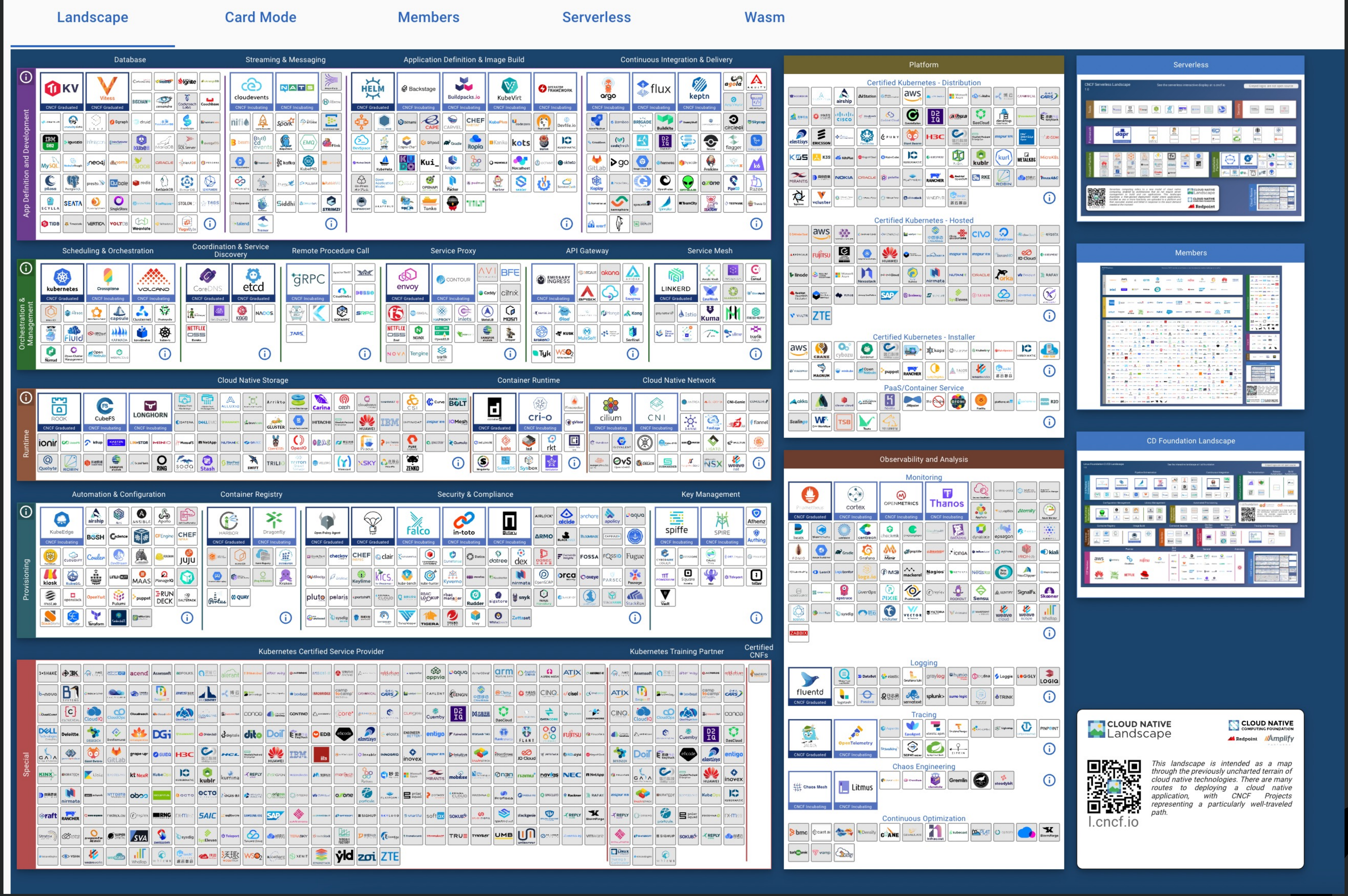
Everybody likes to play

Cloud Native

Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

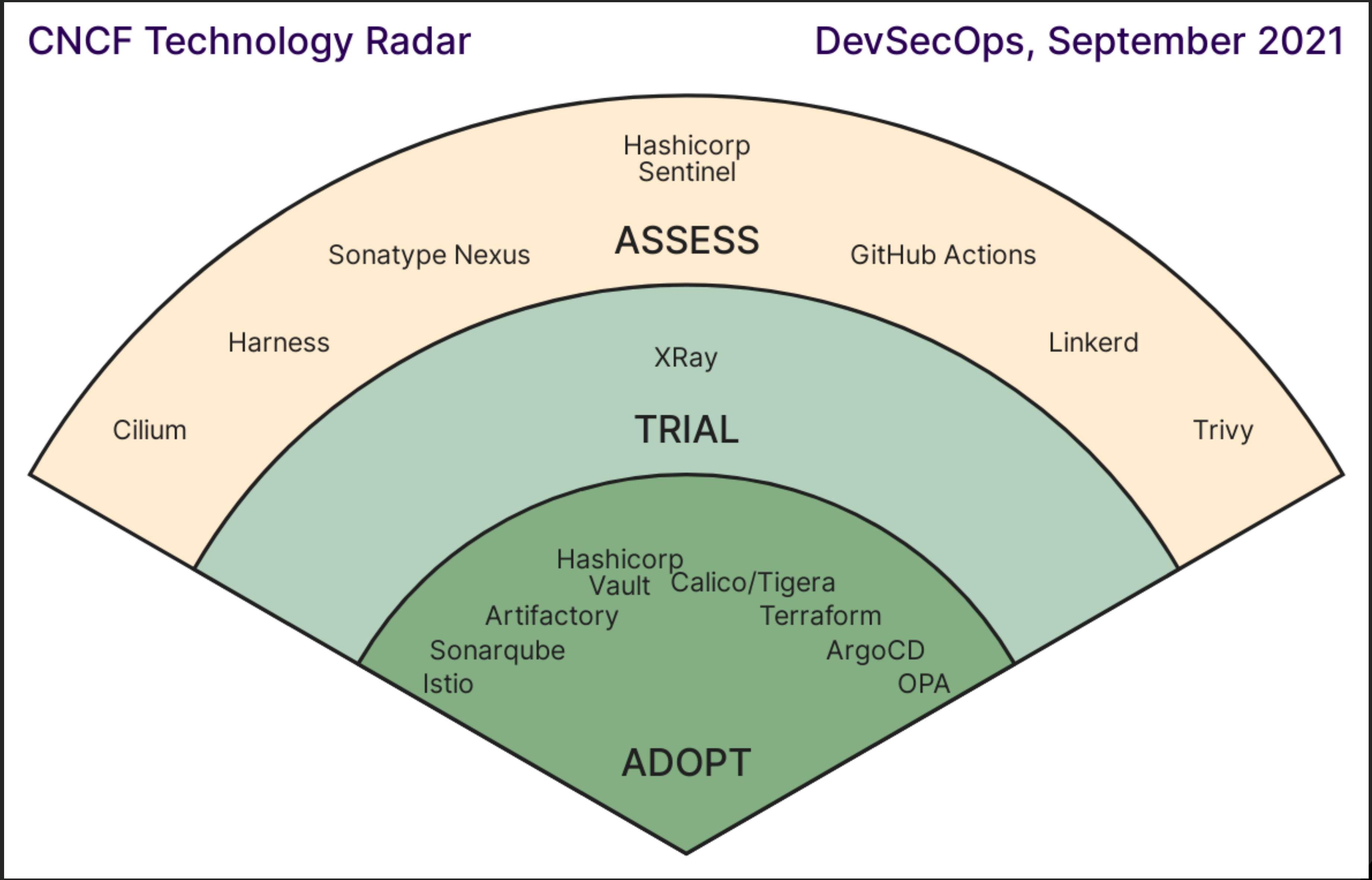
These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

https://github.com/cncf/toc/blob/main/DEFINITION.md https://landscape.cncf.io/



This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

https://radar.cncf.io/



CNCF Technology Radar

DevSecOps, September 2021

Application Security

SAST

- What you write or copy
- First Party Code
- Framework
- Inside Out

SCA

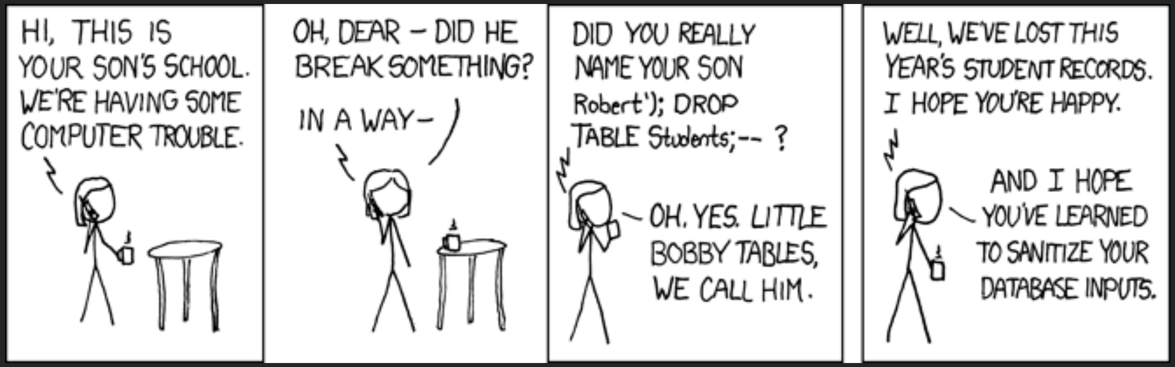
- What you borrow to use
- Third Party Code
- Second Party Code
- Direct / Transitive

DAST / IAST

- Profiling
- Configuration
- Business Logic
- Outside In

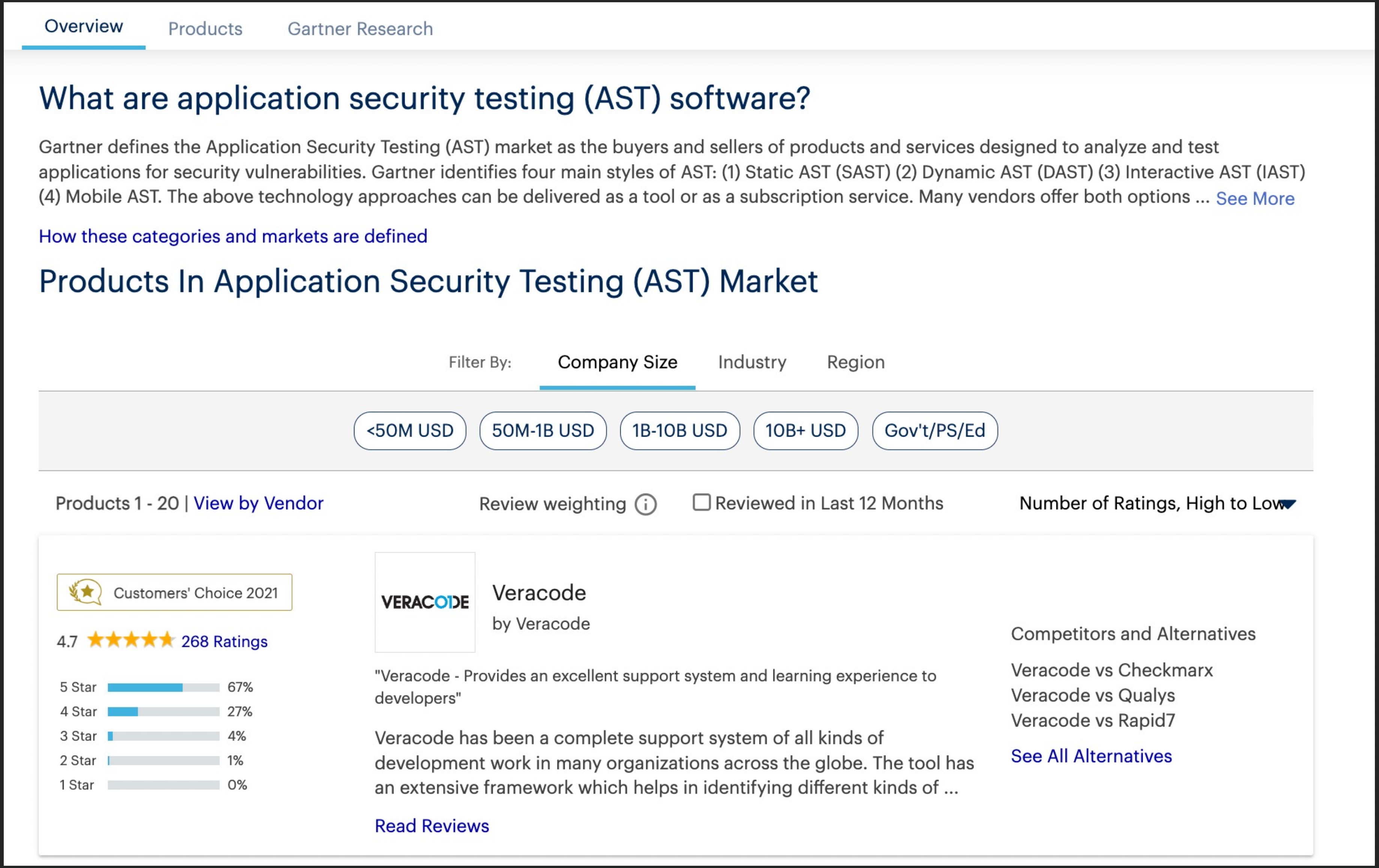
Infrastructure

- Cloud
- Virtual Machines
- Containers
- Kubernetes


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

https://xkcd.com/327/

https://www.gartner.com/reviews/market/application-security-testing



What are application security testing (AST) software?

Gartner defines the Application Security Testing (AST) market as the buyers and sellers of products and services designed to analyze and test applications for security vulnerabilities. Gartner identifies four main styles of AST: (1) Static AST (SAST) (2) Dynamic AST (DAST) (3) Interactive AST (IAST) (4) Mobile AST. The above technology approaches can be delivered as a tool or as a subscription service. Many vendors offer both options ... See More

How these categories and markets are defined

Products In Application Security Testing (AST) Market

Products 1 - 20 | View by Vendor

Review weighting ⓘ

□ Reviewed in Last 12 Months

Number of Ratings, High to Low

Customers' Choice 2021

4.7 ★★★★★ 268 Ratings

5 Star	67%
4 Star	27%
3 Star	4%
2 Star	1%
1 Star	0%

Veracode
by Veracode

"Veracode - Provides an excellent support system and learning experience to developers"

Veracode has been a complete support system of all kinds of development work in many organizations across the globe. The tool has an extensive framework which helps in identifying different kinds of ...

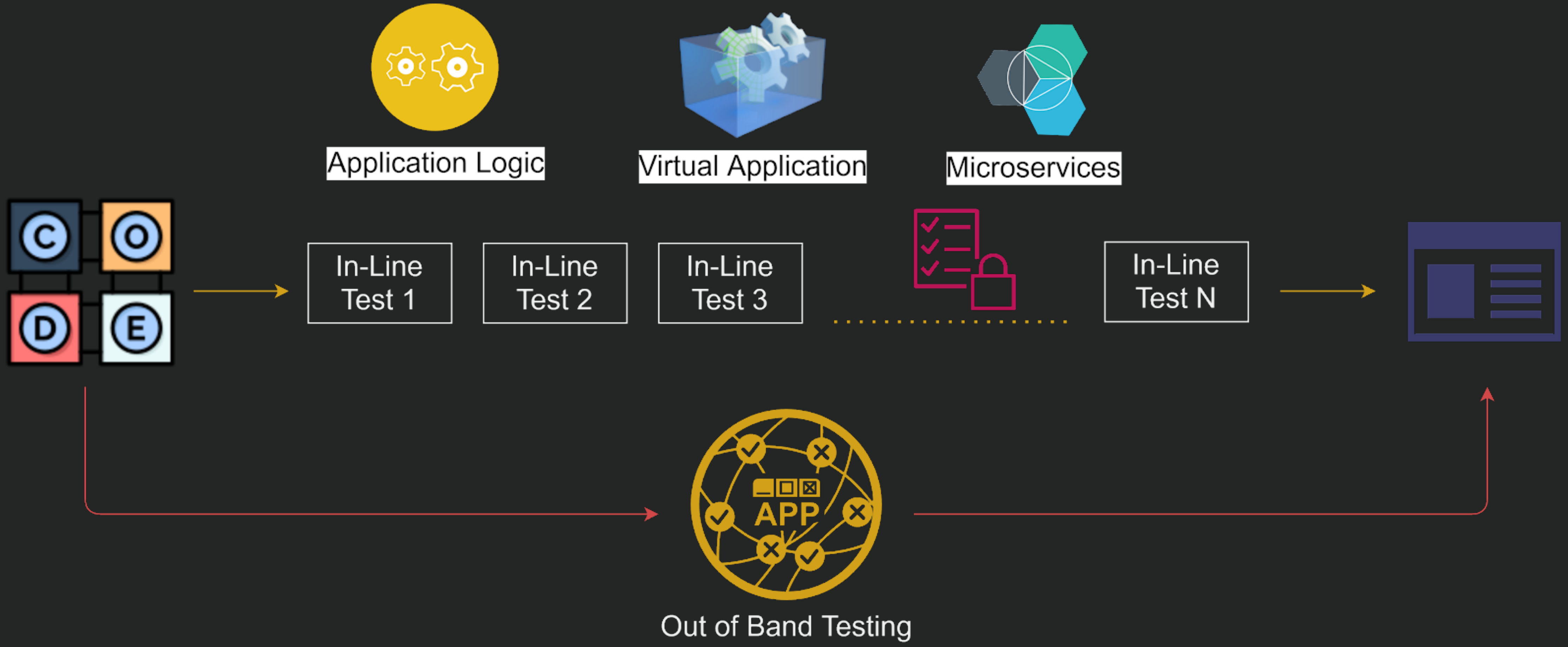
Read Reviews

Competitors and Alternatives

Veracode vs Checkmarx
Veracode vs Qualys
Veracode vs Rapid7

See All Alternatives

Do The Right Tests



Application Logic

Virtual Application

Microservices

In-Line Test 1

In-Line Test 2

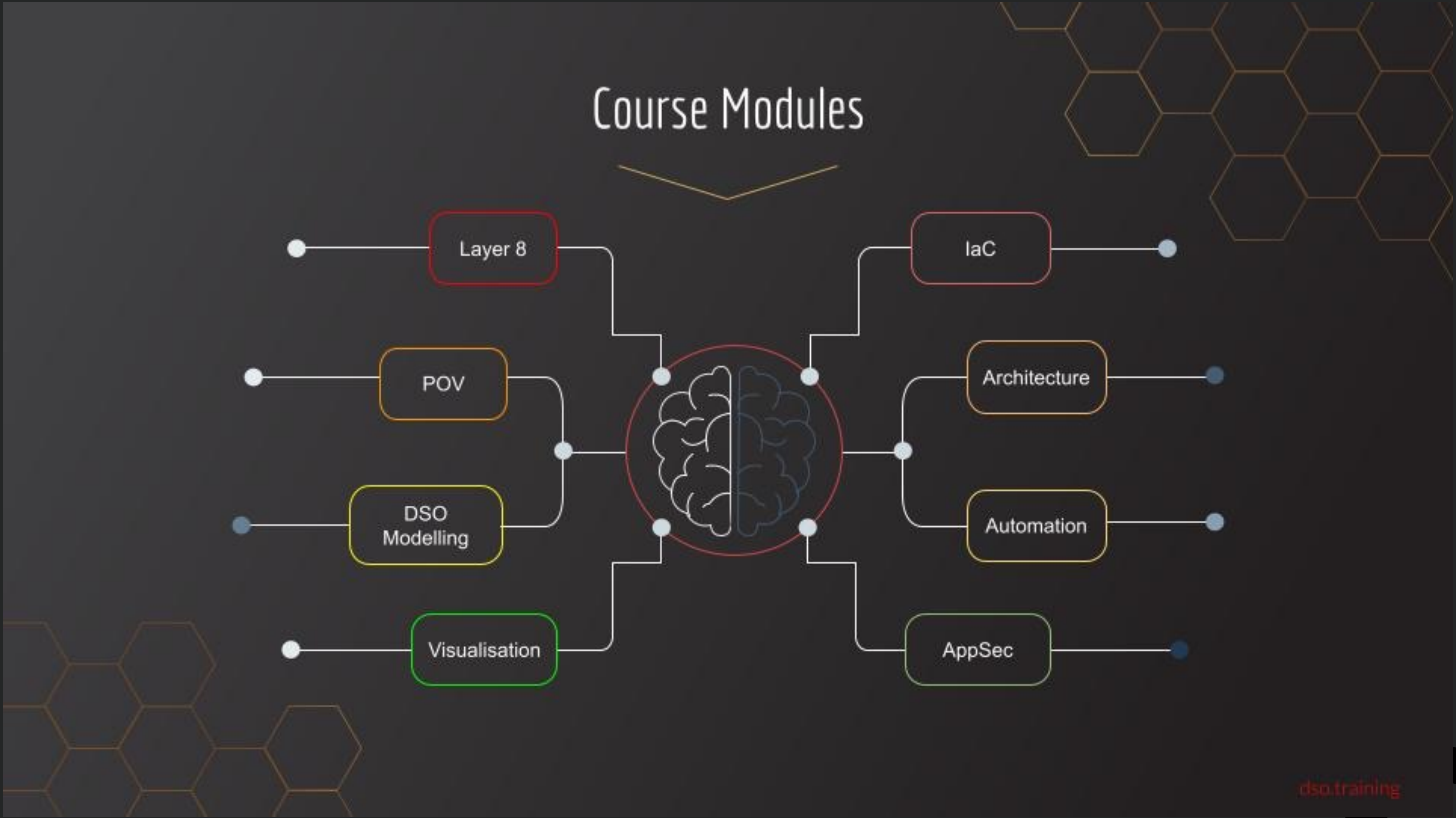
In-Line Test 3

In-Line Test N

Out of Band Testing

My Tips

Subject To Change



Course Modules

Layer 8

POV

DSO Modelling

Visualisation

IaC

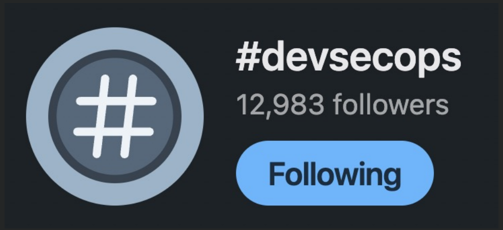
Architecture

Automation

AppSec

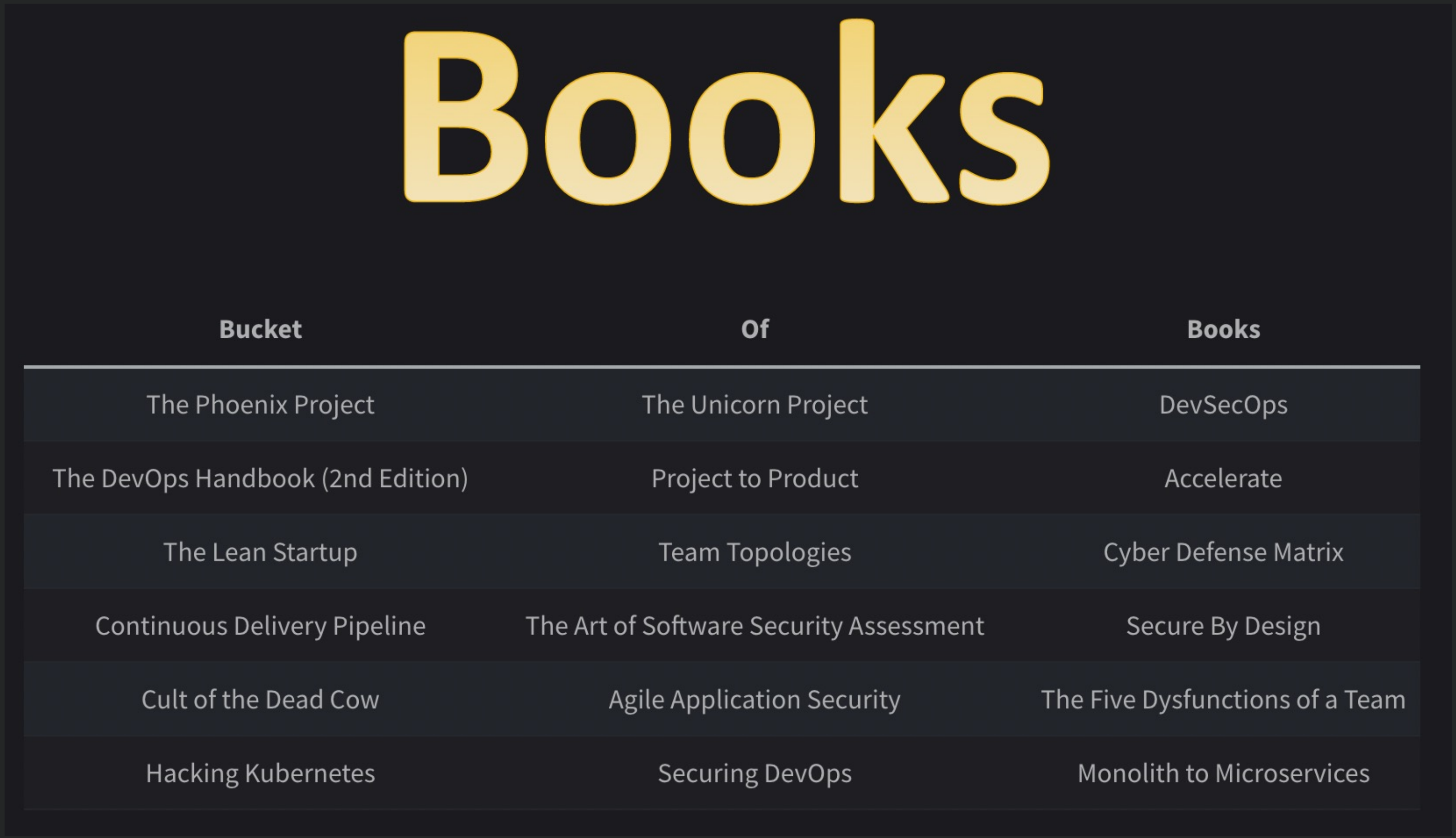
dso.training

Data Sources


#devsecops
12,983 followers

- Read multiple books at the same time
- Social feeds: LinkedIn, sometimes Twitter
- Video news
- Digest the info by summarizing it or discuss it with others

Reading



Books

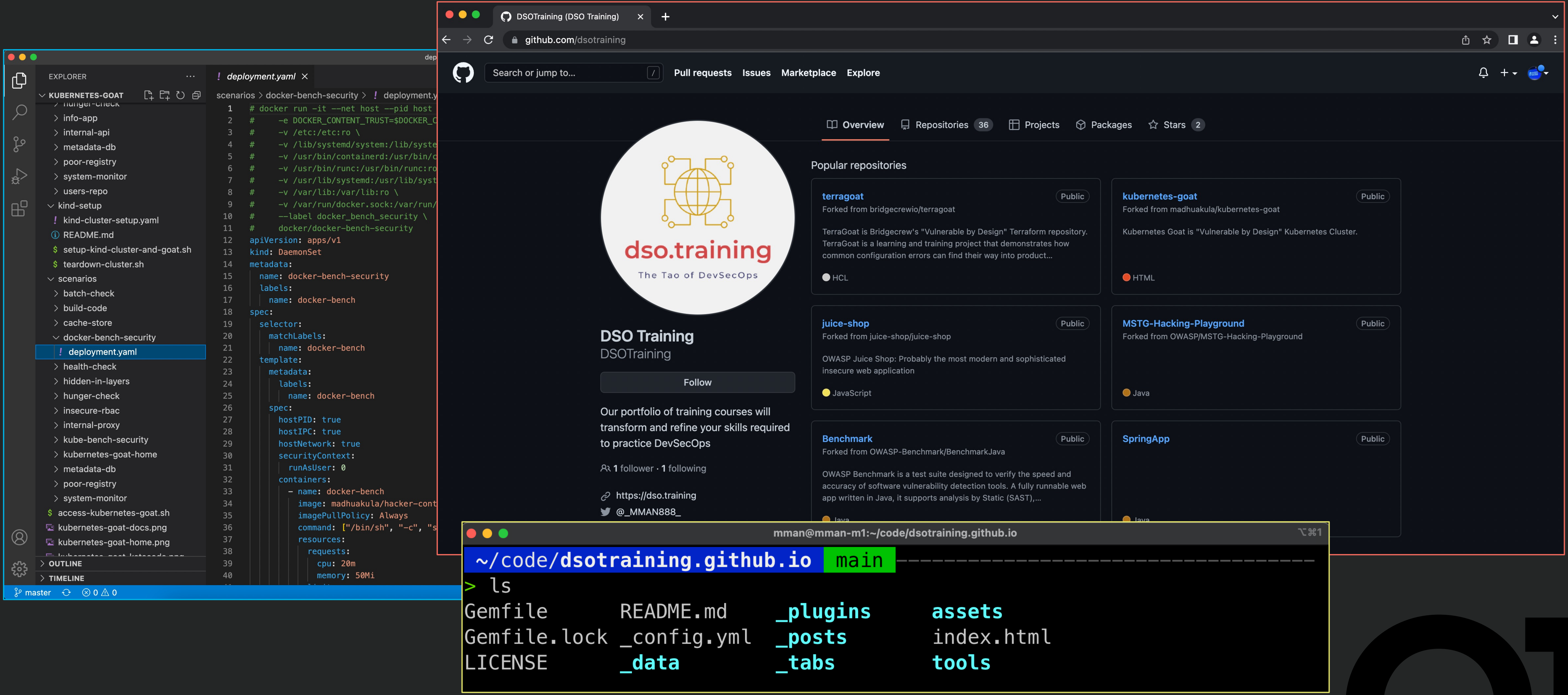
Bucket	Of	Books
The Phoenix Project	The Unicorn Project	DevSecOps
The DevOps Handbook (2nd Edition)	Project to Product	Accelerate
The Lean Startup	Team Topologies	Cyber Defense Matrix
Continuous Delivery Pipeline	The Art of Software Security Assessment	Secure By Design
Cult of the Dead Cow	Agile Application Security	The Five Dysfunctions of a Team
Hacking Kubernetes	Securing DevOps	Monolith to Microservices

https://dsotraining.github.io/posts/Continuous-Learning/

Interactions

- Community Meet-Ups
- Conferences
- Lunch dates
- Volunteer and help out

Try Things and Ask



```
hunger-check
> info-app
> internal-api
> metadata-db
> poor-registry
> system-monitor
> users-repo
v kind-setup
  ! kind-cluster-setup.yaml
  README.md
  $ setup-kind-cluster-and-goat.sh
  $ teardown-cluster.sh
v scenarios
  > batch-check
  > build-code
  > cache-store
  v docker-bench-security
    ! deployment.yaml
  > health-check
  > hidden-in-layers
  > hunger-check
  > insecure-rbac
  > internal-proxy
  > kube-bench-security
  > kubernetes-goat-home
  > metadata-db
  > poor-registry
  > system-monitor
$ access-kubernetes-goat.sh
kubernetes-goat-docs.png
kubernetes-goat-home.png
```

```yaml
# docker run -it --net host --pid host
#     -e DOCKER_CONTENT_TRUST=$DOCKER_C
#     -v /etc:/etc:ro \
#     -v /lib/systemd/system:/lib/syste
#     -v /usr/bin/containerd:/usr/bin/c
#     -v /usr/bin/runc:/usr/bin/runc:ro
#     -v /usr/lib/systemd:/usr/lib/syst
#     -v /var/lib:/var/lib:ro \
#     -v /var/run/docker.sock:/var/run/
#     --label docker_bench_security \
#     docker/docker-bench-security
apiVersion: apps/v1
kind: DaemonSet
metadata:
  name: docker-bench-security
  labels:
    name: docker-bench
spec:
  selector:
    matchLabels:
      name: docker-bench
  template:
    metadata:
      labels:
        name: docker-bench
    spec:
      hostPID: true
      hostIPC: true
      hostNetwork: true
      securityContext:
        runAsUser: 0
      containers:
        - name: docker-bench
          image: madhuakula/hacker-cont
          imagePullPolicy: Always
          command: ["/bin/sh", "-c", "s
          resources:
            requests:
              cpu: 20m
              memory: 50Mi
```

DSO Training
DSOTraining

Our portfolio of training courses will transform and refine your skills required to practice DevSecOps

1 follower · 1 following

https://dso.training

@_MMAN888_

Popular repositories

terragoat Public
Forked from bridgecrewio/terragoat
TerraGoat is Bridgecrew's "Vulnerable by Design" Terraform repository. TerraGoat is a learning and training project that demonstrates how common configuration errors can find their way into product...
HCL

kubernetes-goat Public
Forked from madhuakula/kubernetes-goat
Kubernetes Goat is "Vulnerable by Design" Kubernetes Cluster.
HTML

juice-shop Public
Forked from juice-shop/juice-shop
OWASP Juice Shop: Probably the most modern and sophisticated insecure web application
JavaScript

MSTG-Hacking-Playground Public
Forked from OWASP/MSTG-Hacking-Playground
Java

Benchmark Public
Forked from OWASP-Benchmark/BenchmarkJava
OWASP Benchmark is a test suite designed to verify the speed and accuracy of software vulnerability detection tools. A fully runnable web app written in Java, it supports analysis by Static (SAST),...
Java

SpringApp Public
Java

```
mman@mman-m1:~/code/dsotraining.github.io
~/code/dsotraining.github.io  main
> ls
Gemfile       README.md     _plugins     assets
Gemfile.lock  _config.yml   _posts       index.html
LICENSE       _data         _tabs        tools
```

VERACODE

Take Away

What 20% will you remember?

Keep Asking

dsotraining.github.io

VERACODE

Thank you for today

Michael Man

mman@Veracode.com