

Designing DevSecOps for Test, Release, and Operate SDLC phases



Richard Harpur

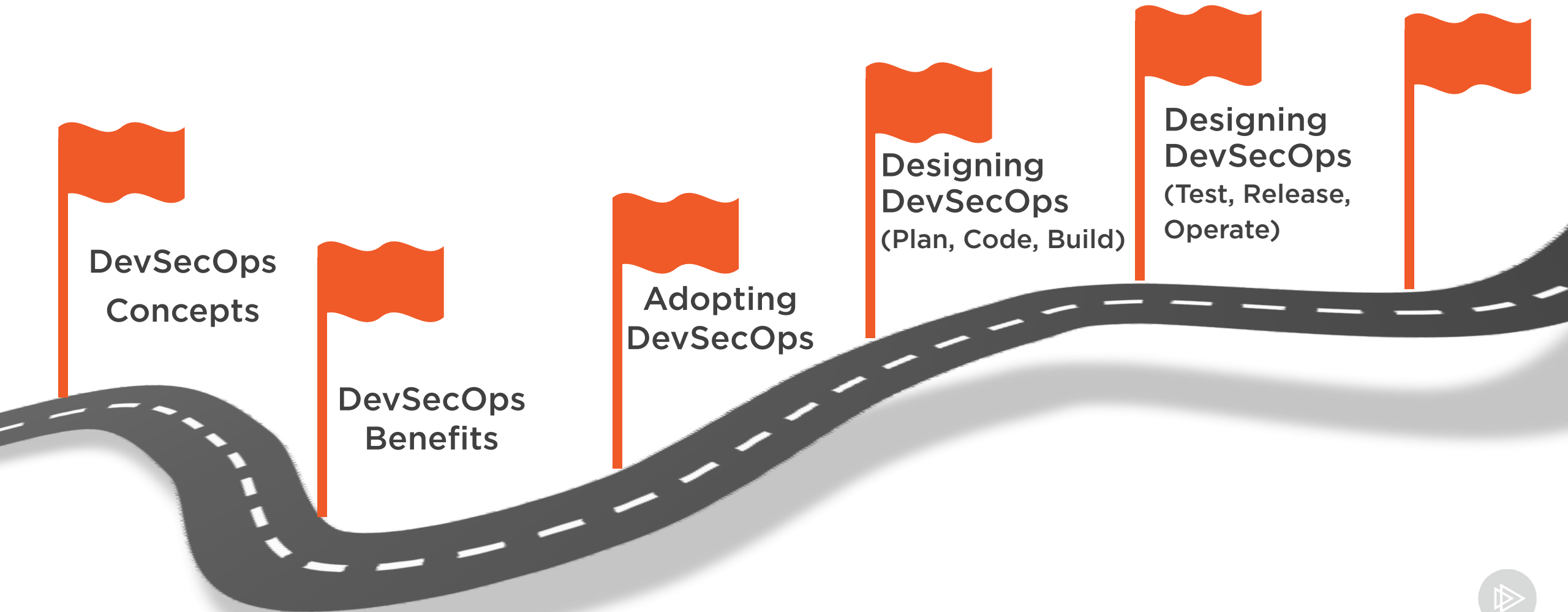
INFORMATION SECURITY PROFESSIONAL, CISM

@rharpur

www.richardharpur.com



Continue Our DevSecOps Journey



Overview

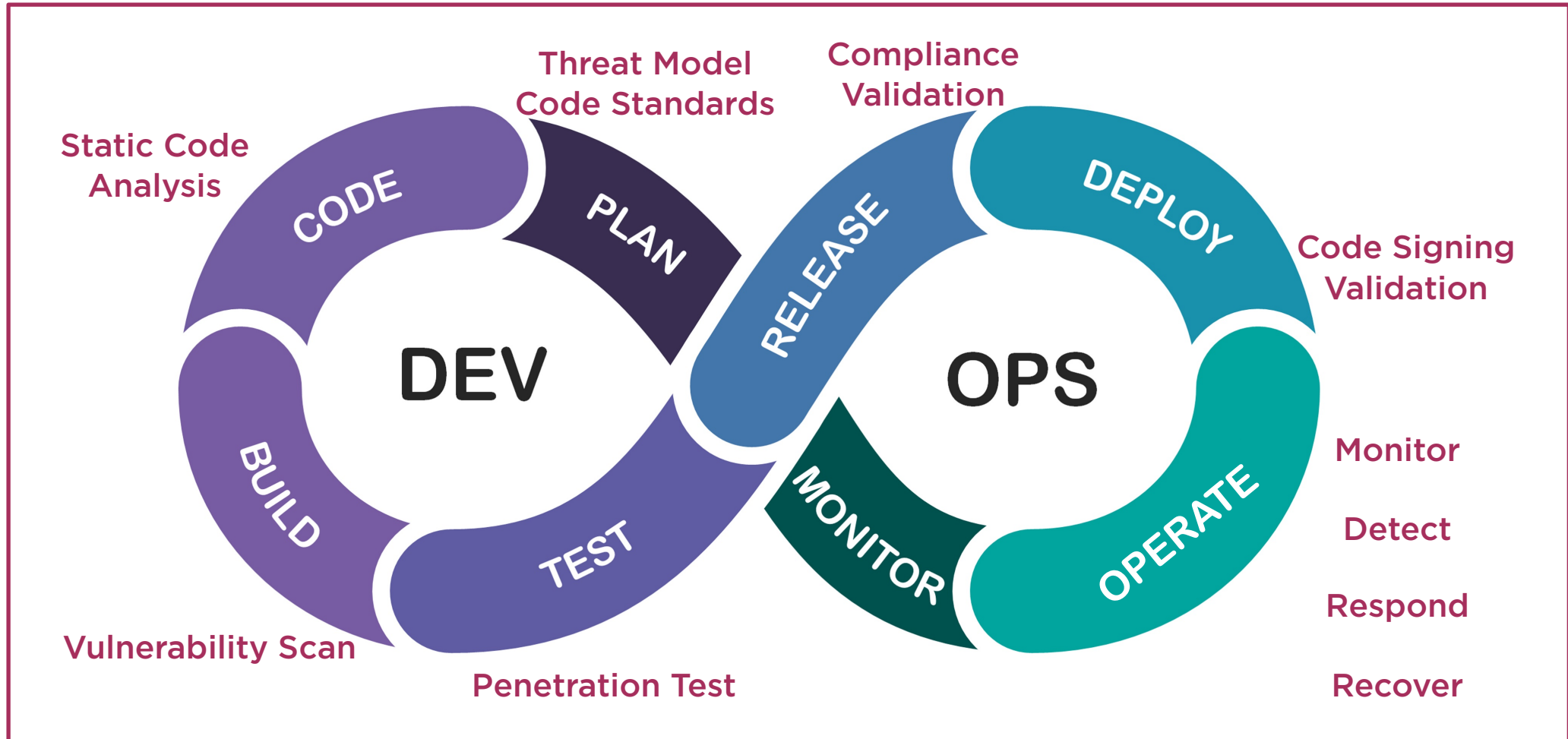


DevSecOps Requirements for:

- Test
- Release
- Operate



Positioning DevSecOps in Your Lifecycle



Security Visibility and Control



Test Phase

Penetration Testing
(Manual)

Load Testing (DDoS) – putting
demand on system and
measuring its response

Fuzzing



Fuzzing

“Fuzzing or fuzz testing is an **automated software testing technique** that involves providing **invalid, unexpected, or random data as inputs** to a computer program. The program is then **monitored for exceptions** such as crashes, failing built-in code assertions, or potential memory leaks. Typically, fuzzers are used to test programs that take structured inputs.”



Test Phase

**Penetration Testing
(Manual)**

**Load Testing (DDoS) – putting
demand on system and
measuring its response**

Fuzzing

**Integration Testing – testing of
combined individual modules**



Deploy Phase

SSL Testing


Ensure all Transport Security
Layer certificates are valid

Application Hardening

Reducing the attack surface
area



SSL Testing



HomeProjectsQualys Free TrialContact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > richardharpur.com

SSL Report: richardharpur.com

[Scan Another >>](#)

	Server	Test time	Grade
1	2606:4700:3036:0:0:0:6818:7307 Ready	Wed, 20 May 2020 00:22:34 UTC Duration: 45.706 sec	A+
2	2606:4700:3035:0:0:0:6818:7207 Ready	Wed, 20 May 2020 00:23:19 UTC Duration: 43.362 sec	A+
3	104.24.115.7 Ready	Wed, 20 May 2020 00:24:03 UTC Duration: 46.161 sec	A+
4	104.24.114.7 Ready	Wed, 20 May 2020 00:24:49 UTC Duration: 45.73 sec	A+

SSL Report v2.1.4

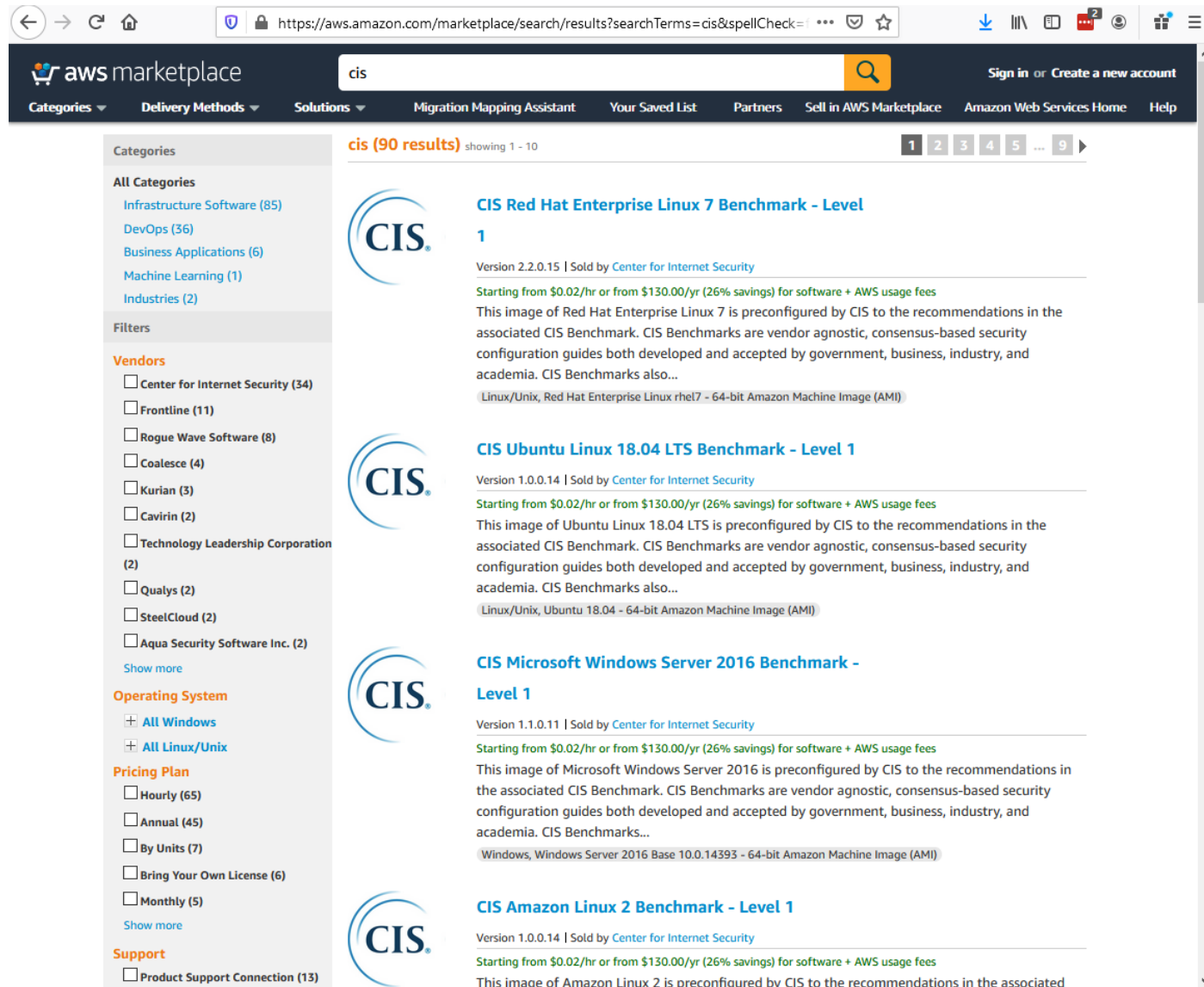
Copyright © 2009-2020 [Qualys, Inc.](#) All Rights Reserved.

[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.

[Terms and Conditions](#)



Run Security Hardened Images



The screenshot shows the AWS Marketplace search results for the term "cis". The interface includes a top navigation bar with the AWS Marketplace logo, a search bar containing "cis", and links for "Sign in" and "Create a new account". Below the navigation bar, there are tabs for "Categories", "Delivery Methods", "Solutions", "Migration Mapping Assistant", "Your Saved List", "Partners", "Sell in AWS Marketplace", "Amazon Web Services Home", and "Help".

The search results are displayed in a list format. The left sidebar contains filters for "Categories", "Vendors", "Operating System", "Pricing Plan", and "Support". The main content area shows the search results for "cis (90 results)", with a pagination bar indicating "showing 1 - 10".

The first four results are:

- CIS Red Hat Enterprise Linux 7 Benchmark - Level 1**
Version 2.2.0.15 | Sold by Center for Internet Security
Starting from \$0.02/hr or from \$130.00/yr (26% savings) for software + AWS usage fees
This image of Red Hat Enterprise Linux 7 is preconfigured by CIS to the recommendations in the associated CIS Benchmark. CIS Benchmarks are vendor agnostic, consensus-based security configuration guides both developed and accepted by government, business, industry, and academia. CIS Benchmarks also...
Linux/Unix, Red Hat Enterprise Linux rhel7 - 64-bit Amazon Machine Image (AMI)
- CIS Ubuntu Linux 18.04 LTS Benchmark - Level 1**
Version 1.0.0.14 | Sold by Center for Internet Security
Starting from \$0.02/hr or from \$130.00/yr (26% savings) for software + AWS usage fees
This image of Ubuntu Linux 18.04 LTS is preconfigured by CIS to the recommendations in the associated CIS Benchmark. CIS Benchmarks are vendor agnostic, consensus-based security configuration guides both developed and accepted by government, business, industry, and academia. CIS Benchmarks also...
Linux/Unix, Ubuntu 18.04 - 64-bit Amazon Machine Image (AMI)
- CIS Microsoft Windows Server 2016 Benchmark - Level 1**
Version 1.1.0.11 | Sold by Center for Internet Security
Starting from \$0.02/hr or from \$130.00/yr (26% savings) for software + AWS usage fees
This image of Microsoft Windows Server 2016 is preconfigured by CIS to the recommendations in the associated CIS Benchmark. CIS Benchmarks are vendor agnostic, consensus-based security configuration guides both developed and accepted by government, business, industry, and academia. CIS Benchmarks...
Windows, Windows Server 2016 Base 10.0.14393 - 64-bit Amazon Machine Image (AMI)
- CIS Amazon Linux 2 Benchmark - Level 1**
Version 1.0.0.14 | Sold by Center for Internet Security
Starting from \$0.02/hr or from \$130.00/yr (26% savings) for software + AWS usage fees
This image of Amazon Linux 2 is preconfigured by CIS to the recommendations in the associated

Operate Phase

Compliance as code

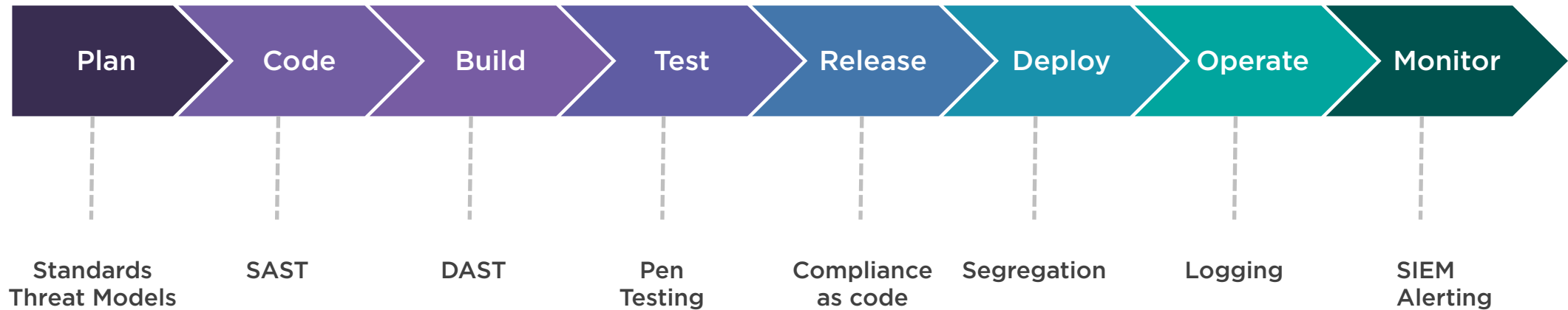
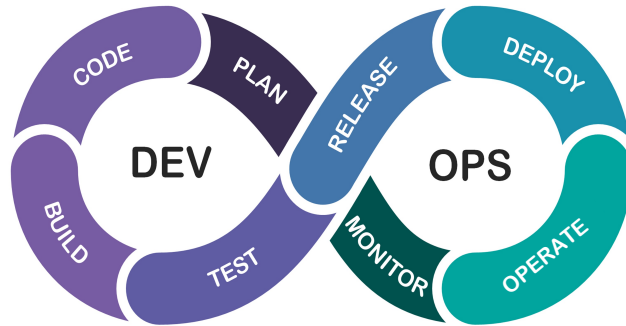
Check against approved baseline, eliminate any deviation from baseline

Verification and monitoring

Continuous checking that everything is operating “normally”



CI/CD Pipeline



PERIODIC TABLE OF DEVOPS TOOLS (v3)																		EMBED	
<div><div><div>Os</div><div>Fr</div><div>Fm</div><div>Pd</div><div>En</div></div><div>Open Source</div><div>Free</div><div>Freemium</div><div>Paid</div><div>Enterprise</div></div> <div><div></div><div></div><div></div><div></div><div></div></div> <div>Source Control Mgmt.</div> <div>Database Automation</div> <div>Continuous Integration</div> <div>Testing</div> <div>Configuration</div> <div><div></div><div></div><div></div><div></div><div></div></div> <div>Deployment</div> <div>Containers</div> <div>Release Orchestration</div> <div>Cloud</div> <div>AI/Ops</div> <div><div></div><div></div><div></div><div></div><div></div></div> <div>Analytics</div> <div>Monitoring</div> <div>Security</div> <div>Collaboration</div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Sp</div> <div>Splunk</div>	
<div><div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div><div>Gh</div><div>GitHub</div></div> <div><div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div><div>Dt</div><div>Datical</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Sl</div> <div>Sumo Logic</div>	
<div><div><div>Os</div><div>En</div><div>En</div><div>En</div><div>En</div></div><div>Sv</div><div>Subversion</div></div> <div><div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div><div>Db</div><div>DBMaestro</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	
<div><div><div>En</div><div>En</div><div>Os</div><div>Fm</div><div>Os</div><div>Fr</div><div>Fr</div><div>Fm</div><div>En</div><div>En</div><div>En</div><div>En</div><div>Os</div><div>Fm</div><div>En</div><div>En</div><div>Os</div><div>En</div></div><div>Cw</div><div>ISPW</div><div>Dp</div><div>Delphix</div><div>Jn</div><div>Jenkins</div><div>Cs</div><div>Codeship</div><div>Fn</div><div>FitNesse</div><div>Ju</div><div>JUnit</div><div>Ka</div><div>Karma</div><div>Su</div><div>SoapUI</div><div>Ch</div><div>Chef</div><div>Tf</div><div>Terraform</div><div>Xld</div><div>XebiaLabs XL Release</div><div>Ud</div><div>UrbanCode Deploy</div><div>Ku</div><div>Kubernetes</div><div>Cc</div><div>CA CD Director</div><div>Pr</div><div>Plutora Release</div><div>Al</div><div>Alibaba Cloud</div><div>Os</div><div>OpenStack</div><div>Ps</div><div>Prometheus</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	
<div><div><div>Os</div><div>En</div><div>Pd</div><div>Fm</div><div>Fr</div><div>Fr</div><div>Os</div><div>Pd</div><div>Os</div><div>Os</div><div>En</div><div>Os</div><div>Os</div><div>Os</div><div>Os</div><div>Pd</div><div>Os</div><div>En</div></div><div>At</div><div>Artifactory</div><div>Rg</div><div>Redgate</div><div>Ba</div><div>Bamboo</div><div>Vs</div><div>VSTS</div><div>Se</div><div>Selenium</div><div>Jm</div><div>JMeter</div><div>Ja</div><div>Jasmine</div><div>Sl</div><div>Sauce Labs</div><div>An</div><div>Ansible</div><div>Ru</div><div>Rudder</div><div>Oc</div><div>Octopus Deploy</div><div>Go</div><div>GoCD</div><div>Ms</div><div>Mesos</div><div>Gke</div><div>GKE</div><div>Om</div><div>OpenMake</div><div>Cp</div><div>AWS CodePipeline</div><div>Cy</div><div>Cloud Foundry</div><div>It</div><div>ITRS</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	
<div><div><div>Os</div><div>Os</div><div>Os</div><div>Fm</div><div>Os</div><div>Fr</div><div>Fm</div><div>Pd</div><div>En</div><div>Os</div><div>Fm</div><div>En</div><div>En</div><div>Os</div><div>Pd</div><div>Os</div><div>Os</div><div>Pd</div></div><div>Nx</div><div>Nexus</div><div>Fw</div><div>Flyway</div><div>Tr</div><div>Travis CI</div><div>Tc</div><div>TeamCity</div><div>Ga</div><div>Gatling</div><div>Tn</div><div>TestNG</div><div>Tt</div><div>Tricentis Tosca</div><div>Pe</div><div>Perfecto</div><div>Pu</div><div>Puppet</div><div>Pa</div><div>Packer</div><div>Cd</div><div>AWS CodeDeploy</div><div>Ec</div><div>ElectricCloud</div><div>Ra</div><div>Rancher</div><div>Aks</div><div>AKS</div><div>Rk</div><div>Rkt</div><div>Sp</div><div>Spinnaker</div><div>Ir</div><div>Iron.io</div><div>Mg</div><div>Moogsoft</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	
<div><div><div>Fm</div><div>En</div><div>Fm</div><div>Pd</div><div>Fr</div><div>Os</div><div>Os</div><div>En</div><div>Os</div><div>Os</div><div>Os</div><div>En</div><div>En</div><div>En</div><div>Pd</div><div>En</div><div>Os</div><div>En</div></div><div>Bb</div><div>BitBucket</div><div>Pf</div><div>Perforce HelixCore</div><div>Cr</div><div>Circle CI</div><div>Cb</div><div>AWS CodeBuild</div><div>Cu</div><div>Cucumber</div><div>Mc</div><div>Mocha</div><div>Lo</div><div>Locust.io</div><div>Mf</div><div>Micro Focus UFT</div><div>Sl</div><div>Salt</div><div>Ce</div><div>CFEngine</div><div>Eb</div><div>ElasticBox</div><div>Ca</div><div>CA Automate</div><div>De</div><div>Docker Enterprise</div><div>Ae</div><div>AWS ECS</div><div>Cf</div><div>Codefresh</div><div>Hm</div><div>Helm</div><div>Aw</div><div>Apache OpenWhisk</div><div>Ls</div><div>Logstash</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	
<div><div><div>En</div><div>Os</div><div>Fm</div><div>En</div><div>En</div><div>Fm</div><div>Os</div><div>Os</div><div>Os</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div><div>Xli</div><div>XebiaLabs XL Impact</div><div>Ki</div><div>Kibana</div><div>Nr</div><div>New Relic</div><div>Dt</div><div>Dynatrace</div><div>Dd</div><div>Datadog</div><div>Ad</div><div>AppDynamics</div><div>El</div><div>ElasticSearch</div><div>Ni</div><div>Nagios</div><div>Zb</div><div>Zabbix</div><div>Zn</div><div>Zenoss</div><div>Cx</div><div>Checkmarx SAST</div><div>Sg</div><div>Signal Sciences</div><div>Bd</div><div>BlackDuck</div><div>Sr</div><div>SonarQube</div><div>Hv</div><div>HashiCorp Vault</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	
<div><div><div>En</div><div>Pd</div><div>Fm</div><div>Fm</div><div>Fm</div><div>En</div><div>En</div><div>En</div><div>Pd</div><div>Pd</div><div>Os</div><div>Os</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div><div>Sw</div><div>ServiceNow</div><div>Jr</div><div>Jira</div><div>Ti</div><div>Trello</div><div>Sl</div><div>Slack</div><div>St</div><div>Stride</div><div>Cn</div><div>CollabNet VersionOne</div><div>Ry</div><div>Remedy</div><div>Ac</div><div>Agile Central</div><div>Og</div><div>OpsGenie</div><div>Pd</div><div>Pagerduty</div><div>Sn</div><div>Snort</div><div>Tw</div><div>Tripwire</div><div>Ck</div><div>CyberArk Conjur</div><div>Vc</div><div>Veracode</div><div>Ff</div><div>Fortify SCA</div></div>																		<div><div>En</div><div>En</div><div>En</div><div>En</div><div>En</div></div> <div>Fd</div> <div>Fluentd</div>	

XebiaLabs

Enterprise DevOps

Follow @xebialabs

Publication Guidelines



Summary



Focus on automated checks

Reduce feedback time lag

Use appropriate tooling at each phase

Up Next

- Debunking DevSecOps Myths

