Bank of England

Bank Security

DevSecOps: More than just Shift-left Security

Vince King
January 2023

Who's this talking to me now?

Vincent King

Senior Cyber Analyst
Head of DevSecOps
Bank of England

GIAC CLOUD SECURITY AUTOMATION GCSA

CITP FBCS

CHARTERED FELLOW

bcs The Chartered Institute for IT

Chartered IT Professional citp

(ISC)² CISSP® | Certified Information Systems Security Professional

Reformed Developer
Secure Coding Subject Matter Expert
(ISC)² Certified Information Security Professional
Chartered Fellow of the BCS

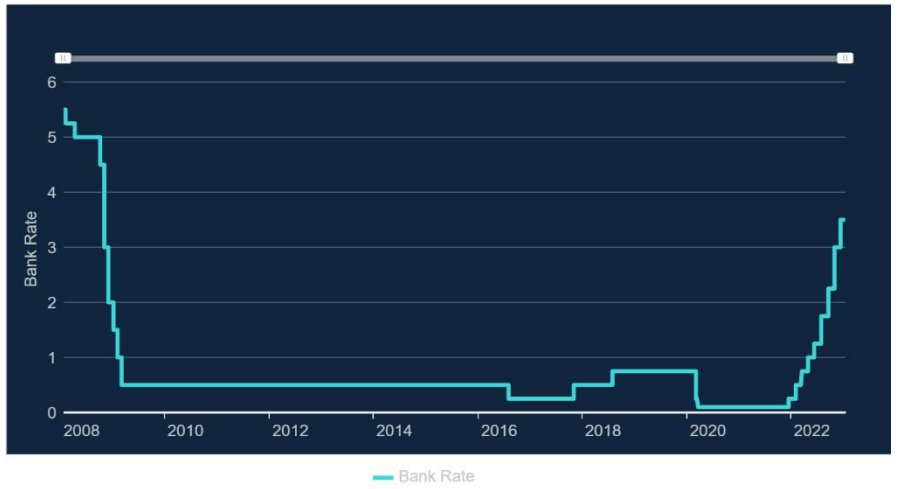
RIT Tech

DevSecOpsVince

Sec Sec Sec Dev Ops Security Everywhere

What does the Bank of England do?

Official Bank Rate



RTGS

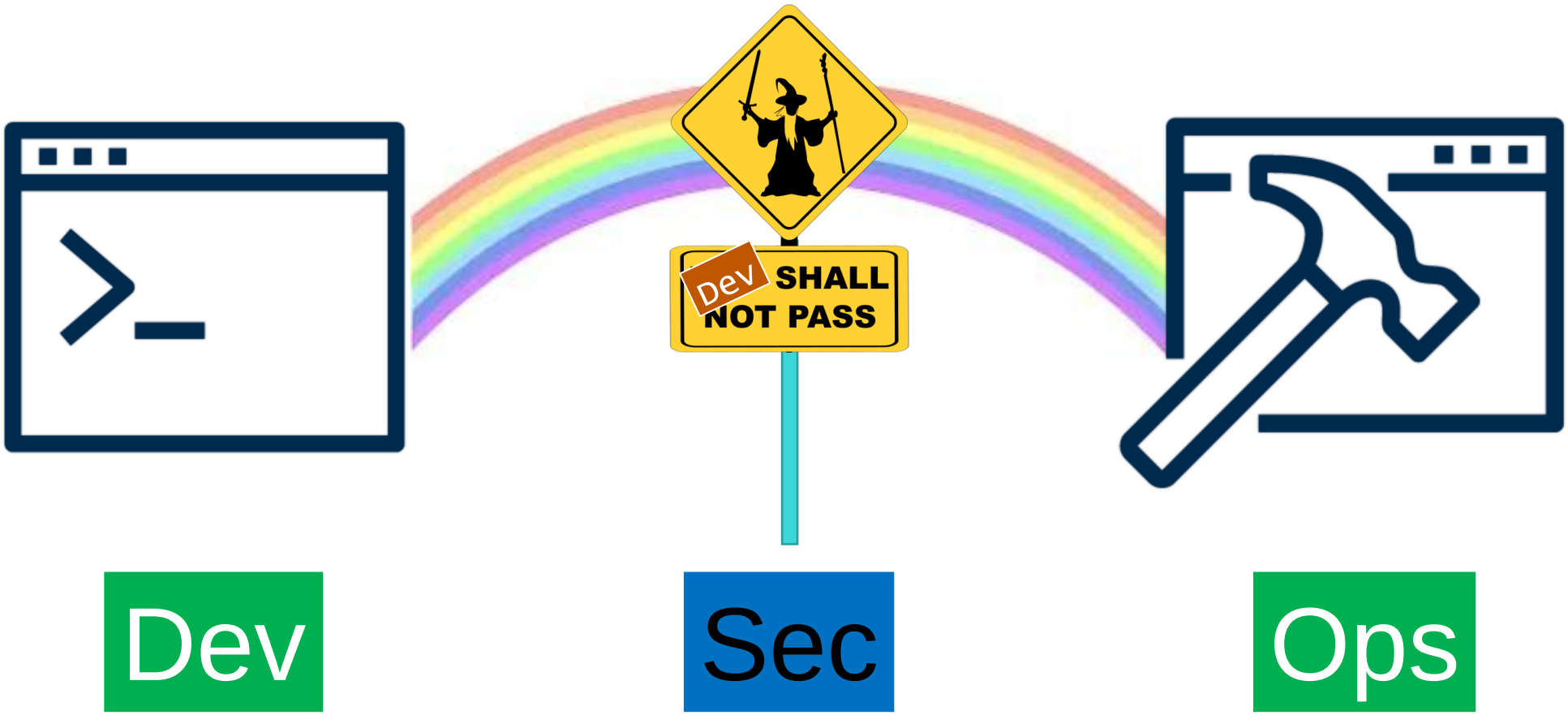
Real-Time Gross Settlement

Settled an average of over **£720 billion** each working day

CHAPS | CREST | BACS | Image Clearing System for cheques | Faster Payments

LINK | Mastercard Europe | Visa Europe | PEXA

DevOps vs Security – The Perception

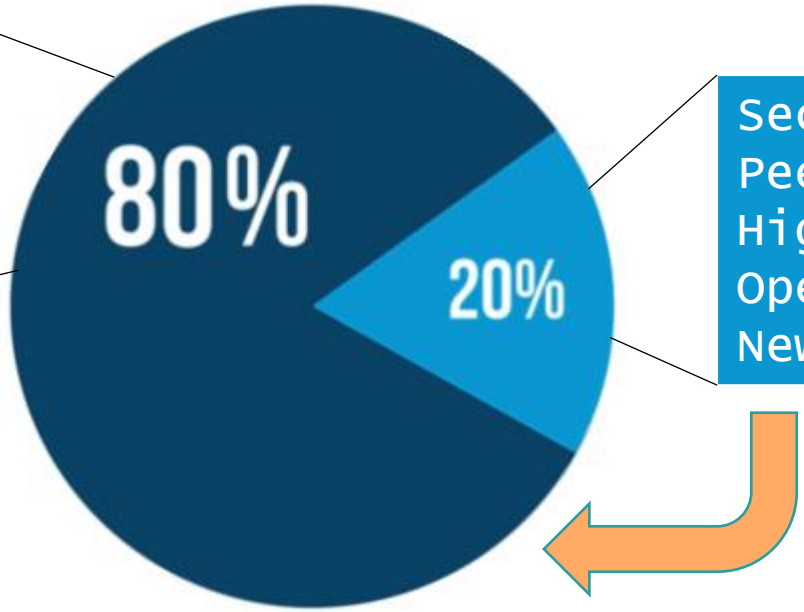


Where should Sec live?

Scary Slide No.1

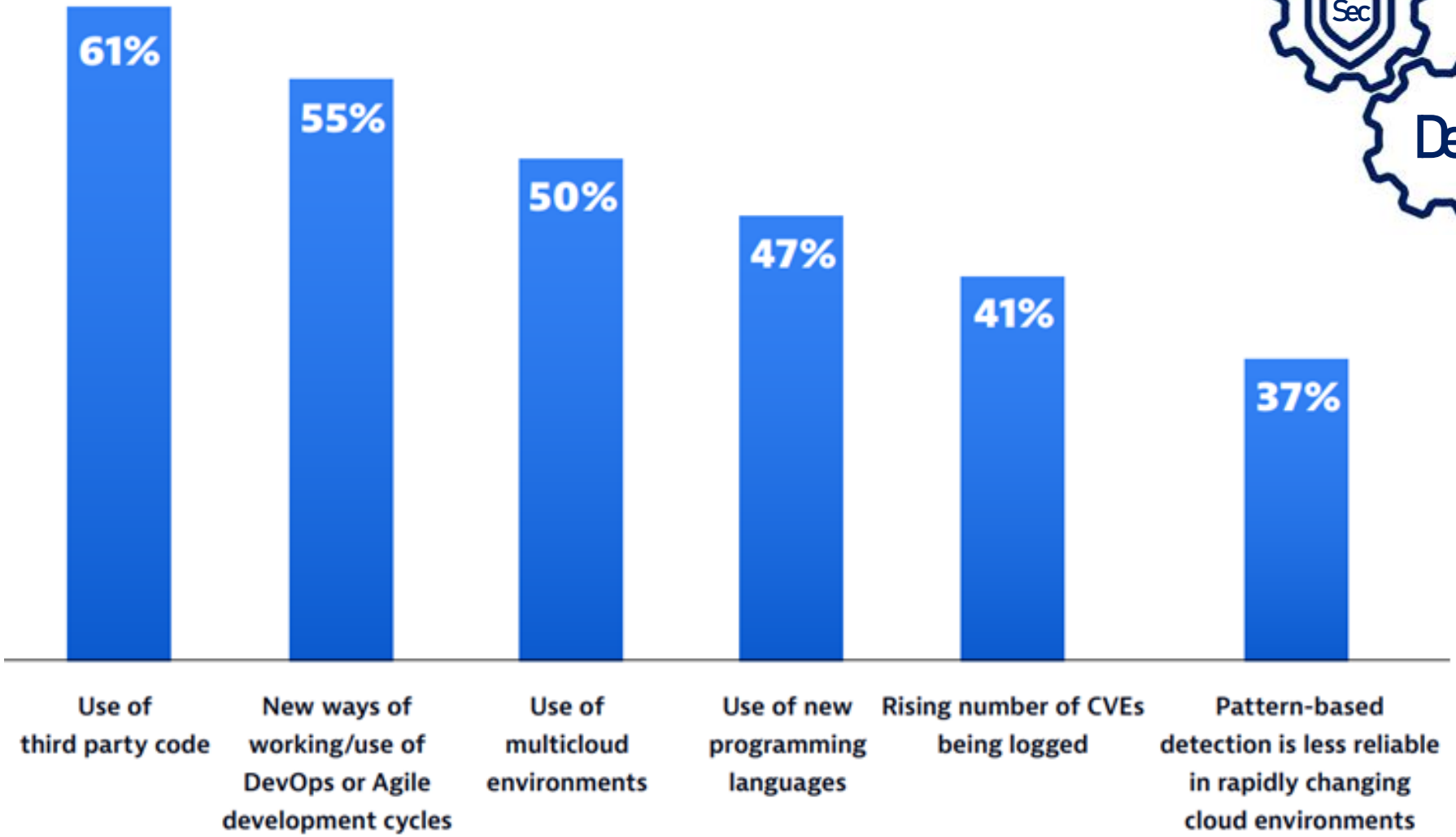
Where should Sec live?

Secure coding training
Code reviews
SAST
Secure code reuse
Strict policies



Secure code champions
Peer oversight
High trust team
Open Source code use
Newer container images

Scary Slide No.2



68%

of apps had a security flaw that fell into the OWASP Top 10

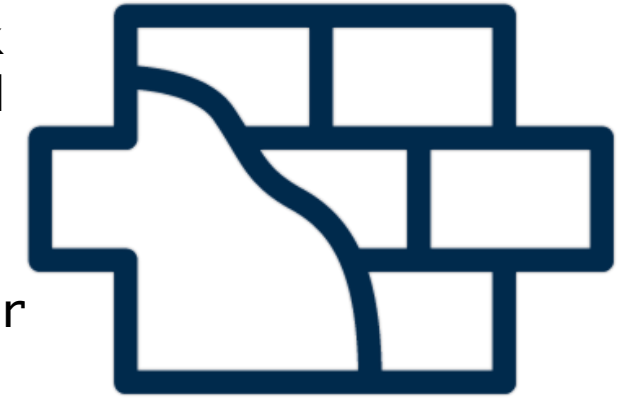
You are the key
to better Bank security

Where should Sec live?

CI/CD pipelines

Don't break every build

Trust, but verify



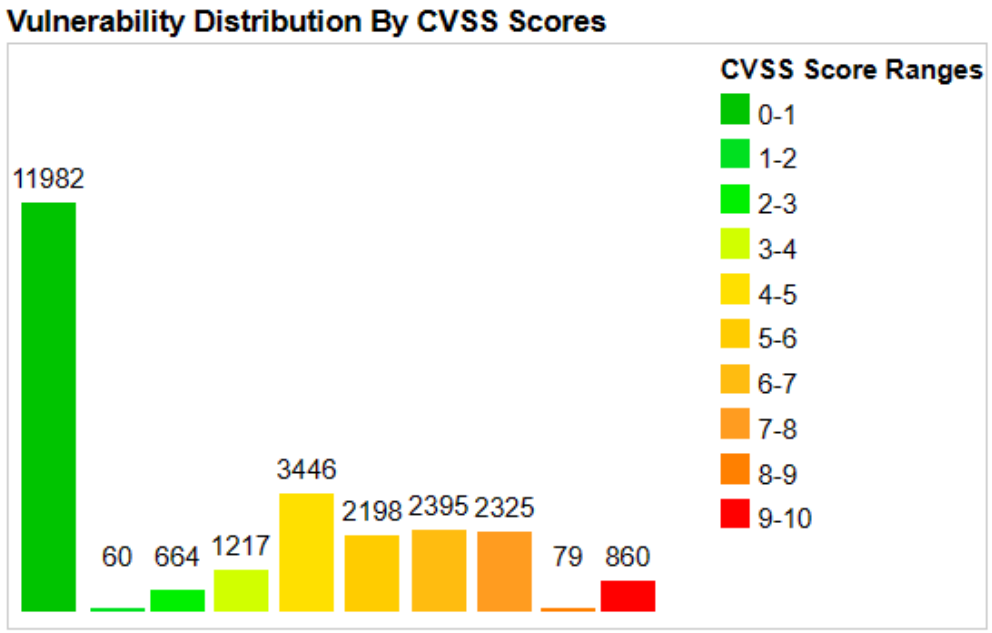
Gold container images

Infrastructure as code

Challenge non-standard architecture

Scary Slide No.3

25,226 Common Vulnerabilities and Exposures (CVEs) were published last year alone.



57% report that their breaches could have been prevented by installing an available patch

34% victims knew of the vulnerability, but hadn't taken action

Where should Sec live?

Destroy & rebuild

Policy compliance

Continuous monitoring

Proactive patching

Vulnerability Management

Posture management reporting

#DevSecOpsHow

Culture

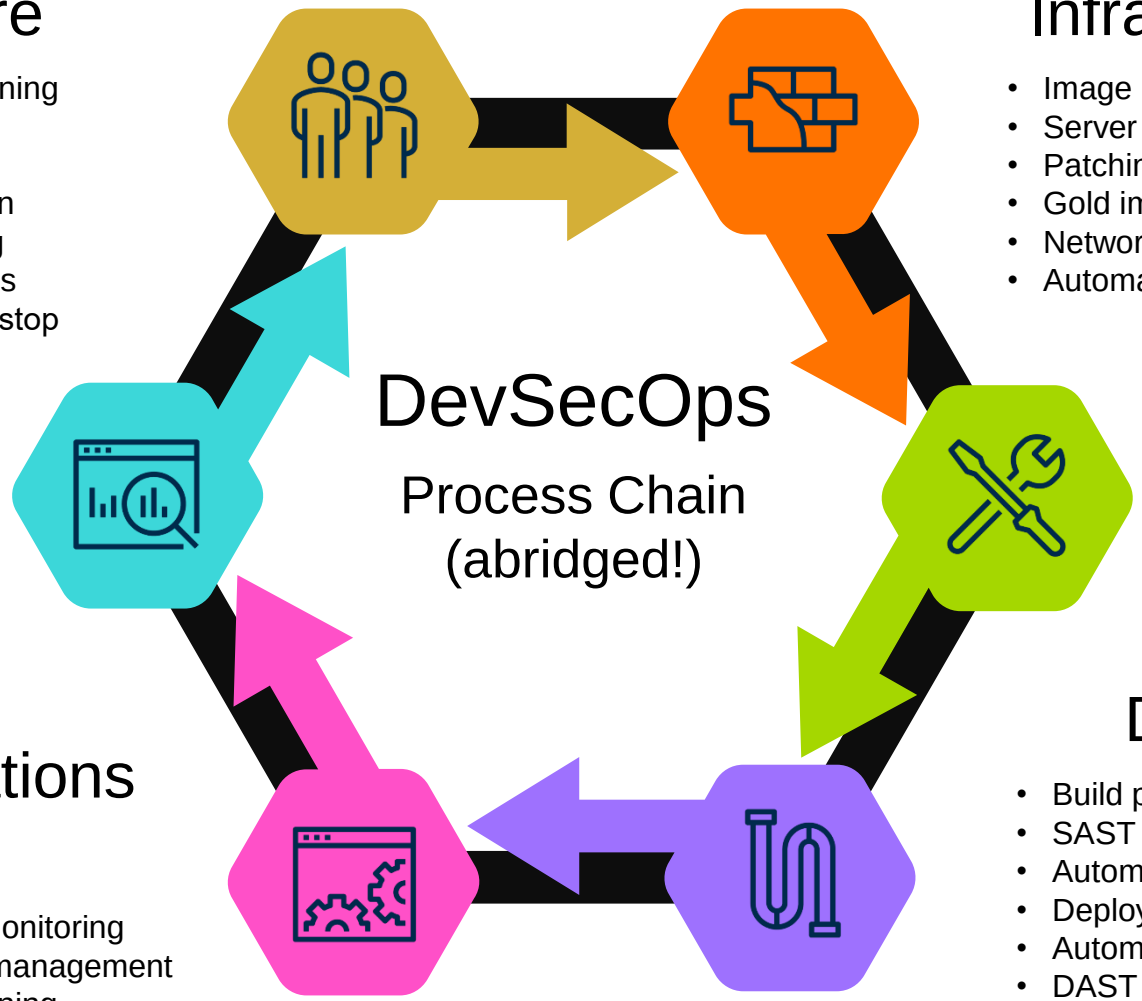
- Secure code training
- Peer reviews
- Unit testing
- Coding champion
- Threat modelling
- Coding standards
- First warning … stop reading!

Monitoring

- Logging
- Metrics
- Analysis
- Reporting
- Threat intelligence
- Evidence as policy
- Slide isn't meant to be read

Operations

- Support
- Service desk
- Continuous monitoring
- Vulnerability management
- Security scanning
- Policy enforcement



Infrastructure

- Image library source
- Server hardening
- Patching
- Gold image curation
- Networks and firewalls
- Automatic provisioning

Developer Tooling

- IDE
- Package Management
- Application Lifecycle Management
- Ticketing system
- DAST tooling
- Source control

Deployment

- Build pipelines
- SAST tooling
- Automated testing
- Deployment environments
- Automatic fault reporting
- DAST tooling
- Secrets management
- Stop reading this slide!

#DevSecOpsHow

Culture

- Code Warrior
- Pluralsight
- OWASP Top 10
- LinkedIn Learning
- Udemy
- Evil user stories
- CERT Secure Coding Standards
- Game day exercises
- Gerrit
- Github pull requests
- Review board
- JUnit
- xUnit
- Evil user stories
- OWASP Threat Dragon
- CERT Secure Coding Standards

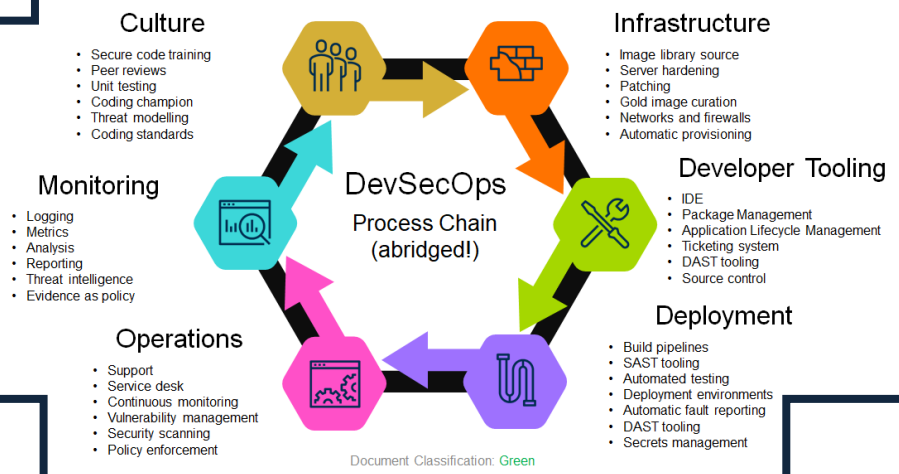
Monitoring

- Azure Defender for Cloud
- Azure Sentinel
- Splunk
- SolarWinds
- RSA NetWitness
- Archer
- ThreatConnect
- OWASP Threat Dragon
- Chef
- HashiCorp Sentinel
- nmap
- Etsy Morgue
- Orca Security
- HackerOne
- graphite
- Wiz.io

Operations

- BMC Remedy
- ServiceNow
- LinkedIn Learning
- Udemy
- Evil user stories
- OWASP Threat Dragon
- CERT Secure Coding Standards
- Qualys
- Tenable
- Spiceworks
- BeyondTrust
- AWS CloudTrail
- Nessus
- Seriously … stop reading! You will hurt your eyes.

The DevSecOps Toolchain



(VERY abridged!)

Infrastructure

- Azure Virtual Machines
- Amazon Machine Images
- GCP Compute Engine
- Docker
- ECR
- Terraform
- YAML
- Ansible
- Chef
- SaltStack
- AWS CloudFormation
- Azure Resource Manager
- CIS Benchmarks
- SCCM
- Qualys Patch Management
- Automatic Updates

Developer Tooling

- NPM
- NodeJS
- SonarLint
- DeepSource
- SonarQube
- JetBrains
- Github
- GitLab
- BitBucket
- Azure DevOps
- Github Actions
- JIRA
- Artifactory
- ReSharper
- Final warning! Stop it!
- VSCode

Deployment

- Jenkins
- Azure DevOps
- AWS Deploy
- VeraCode
- Fortify
- Selenium
- TestComplete
- Azure Key Vault
- AWS KMS
- Atlassian Bamboo
- TeamCity
- YAML
- PowerShell
- SARIF SAST Tools
- Yarn
- Test Management

Vince's Five Rules of DevSecOps in the Cloud

1 

Use the benefits cloud platforms gives you

2 

Automate everything; where you can't automate, secure the manual process

3 

Set policies and controls and enforce them through automation

4 

Report on compliance and make the data available to all teams

5 

Tooling cannot fix all your problems, invest in people and processes

Questions?

Vincent King
Head of DevSecOps for Cloud Transformation

DevSecOpsVince.com