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

Reformed Developer
Secure Coding Subject Matter Expert
(ISC)² Certified Information Security Professional
Chartered Fellow of the BCS
What does the Bank of England do?

**Official Bank Rate**

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

You are the key
to better Bank security

Document classification: Green
DevOps vs Security – The Perception

Dev

Sec

Ops
Where should Sec live?

Security Everywhere
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

You are the key
to better Bank security
You are the key to better Bank security.

Scary Slide No.2

61% of apps had a security flaw that fell into the OWASP Top 10

- 61% Use of third party code
- 55% New ways of working/use of DevOps or Agile development cycles
- 50% Use of multicloud environments
- 47% Use of new programming languages
- 41% Rising number of CVEs being logged
- 37% Pattern-based detection is less reliable in rapidly changing cloud environments

68%
Where should Sec live?

- CI/CD pipelines
- Don’t break every build
- Gold container images
- Challenge non-standard architecture
- Infrastructure as code
- Trust, but verify

Security Everywhere
You are the key to better Bank security

Scary Slide No.3

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

<table>
<thead>
<tr>
<th>CVSS Score Ranges</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>11982</td>
</tr>
<tr>
<td>1-2</td>
<td>3446</td>
</tr>
<tr>
<td>2-3</td>
<td>60</td>
</tr>
<tr>
<td>3-4</td>
<td>864</td>
</tr>
<tr>
<td>4-5</td>
<td>1217</td>
</tr>
<tr>
<td>5-6</td>
<td>2198</td>
</tr>
<tr>
<td>6-7</td>
<td>2395</td>
</tr>
<tr>
<td>7-8</td>
<td>2325</td>
</tr>
<tr>
<td>8-9</td>
<td>79</td>
</tr>
<tr>
<td>9-10</td>
<td>80</td>
</tr>
</tbody>
</table>

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.

Document classification: GREEN
Where should Sec live?

- Policy compliance
- Proactive patching
- Posture management reporting
- Destroy & rebuild
- Continuous monitoring
- Vulnerability Management

You are the key
to better Bank security

Document classification: GREEN
#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

**DevSecOps Process Chain (abridged!)**

**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!

You are the key to better Bank security
#DevSecOpsHow

## Culture
- Code Warrior
- Pluralsight
- OWASP Top 10
- 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 Morgan
- Orca Security
- HackerOne
- graphite
- Wiz.io

## Operations
- BMC Remedy
- ServiceNow
- 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.

## Developer Tooling
- NPM
- NodeJS
- SonarLint
- DeepSource
- SonarQube
- JetBrains
- GitLab
- Github
- BitBucket
- Azure DevOps
- Github Actions
- JIRA
- Artifactory
- ReSharper
- 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

## Infrastructure
- Azure Virtual Machines
- Amazon Machine Images
- GCP Compute Engine
- Docker
- ECR
- Terraform
- YAML
- Ansible

## Deployment
- JIRA
- Artifactory
- ReSharper
- VSCode

## Operations
- BMC Remedy
- ServiceNow
- 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.

## Developer Tooling
- NPM
- NodeJS
- SonarLint
- DeepSource
- SonarQube
- JetBrains
- GitLab
- Github
- BitBucket
- Azure DevOps
- Github Actions
- JIRA
- Artifactory
- ReSharper
- 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

You are the key to better Bank security

Document Classification: Green
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