



DEV  
SEC  
OPS  
DAYS

# Why Organizations Need DevSecOps Now More Than Ever

Krishna Guru

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Agenda



- Data breach
- Open-source software
- DevSecOps
- The current situation
- Transforming from DevOps to DevSecOps
- Q & A

Why Organizations Need DevSecOps Now More Than Ever

# Data breach



# Data Breach

**Marriott discloses another security breach that may impact over 5 million guests**

Marriott had a data breach that impacted more than two years ago.

**Half a Million Zoom Accounts Compromised by Credential Stuffing, Sold on Dark Web**



**150 million MyFitnessPal accounts compromised – here's what to do**

May 21, 2014, 12:30pm EDT  
**eBay Suffers Massive Security Breach, All Users Must Change Their Passwords**

Gordon Kelly Senior Contributor  
Consumer Tech  
I write about technology's biggest companies

**Twitter apologises for business data breach**

© 23 June 2020 | Technology

**Facebook Security Breach Exposes Accounts of 50 Million Users**



**Target Breach: What Happened?**

Expert Insight on Breach Scenarios, How Banks Must Respond

Tracy Kitten (FraudBlogger) • December 20, 2013



Was it a point-of-sale attack? A data breach? Was it an inside job?

**Capital One fined \$80 million for 2019 hack of 100 million credit card applications**



**Adobe left 7.5 million Creative Cloud user records exposed online**

Exposed data primarily includes emails, but not passwords or financial information.

**LinkedIn Lost 167 Million Account Credentials in Data Breach**

LinkedIn says it has 65 million registered users.

**A Recent Startup Breach Exposed Billions of Data Points**

**Sales intelligence startup exposed staggering amount of data online, including addresses**

Written for NortonLifeLock

Share f t i

**Uber Data Breach Affects 57 Million Rider and Driver Accounts**

Written for NortonLifeLock

Share f t i



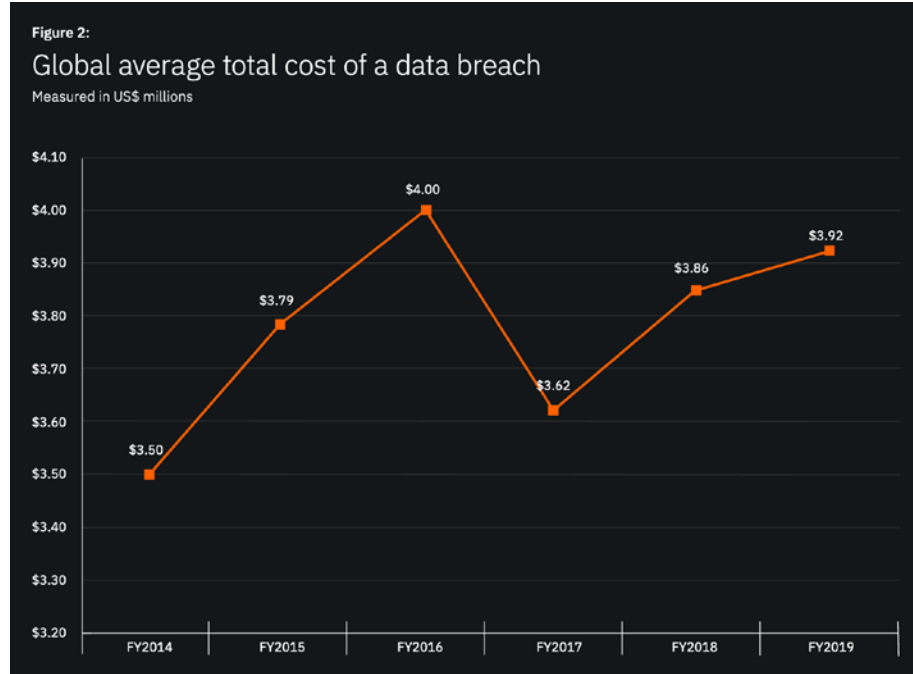
**A security breach in India has left a billion people at risk of identity theft**

**Quora says 100 million users hit by 'malicious' data breach**

By Rob McLean, CNN Business

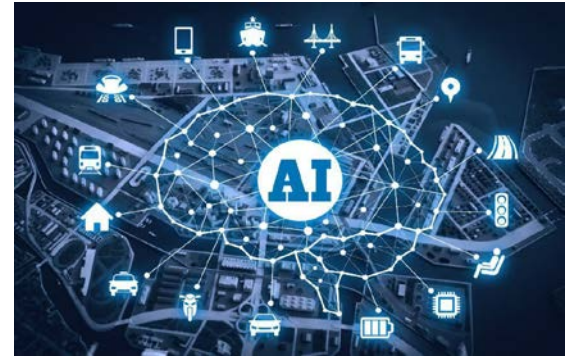
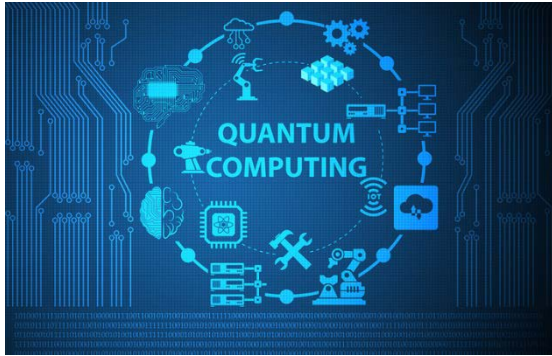
**Data Breach of Adult Dating Site Exposes Victims to a Different Kind of Threat**

# Cost of a breach

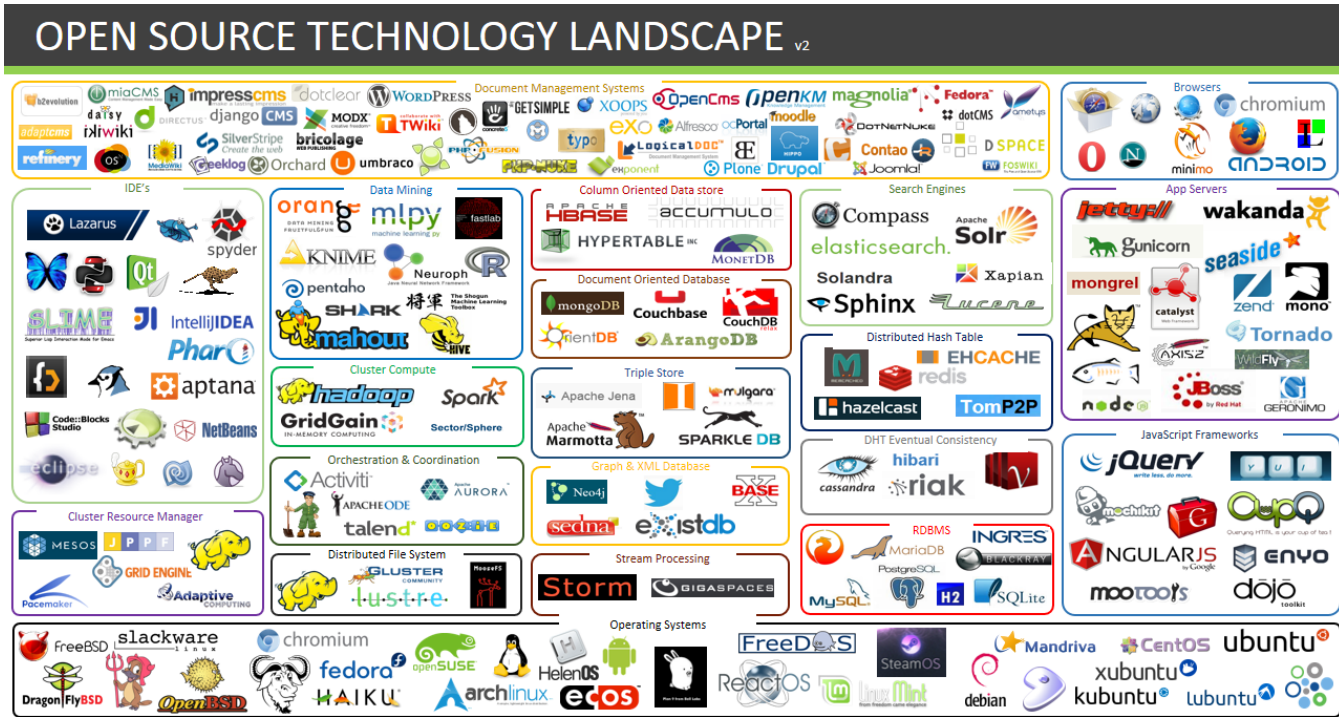


Source - IBM and the Ponemon Institute's annual Cost of a Data Breach\_report

# Threat to emerging technologies



# Open-source software

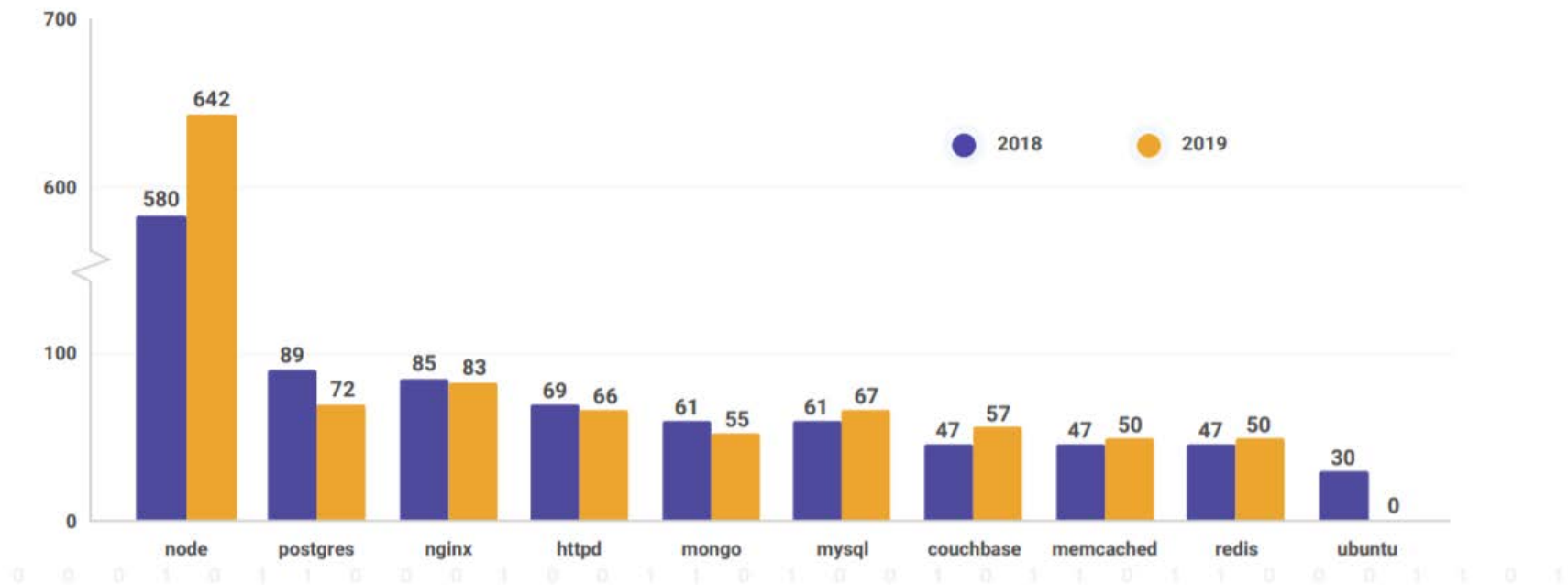


© lanfe.blogspot.com 2014

Ian Ferreira 2014

# Threats in Open-source software

## Vulnerabilities in official container images



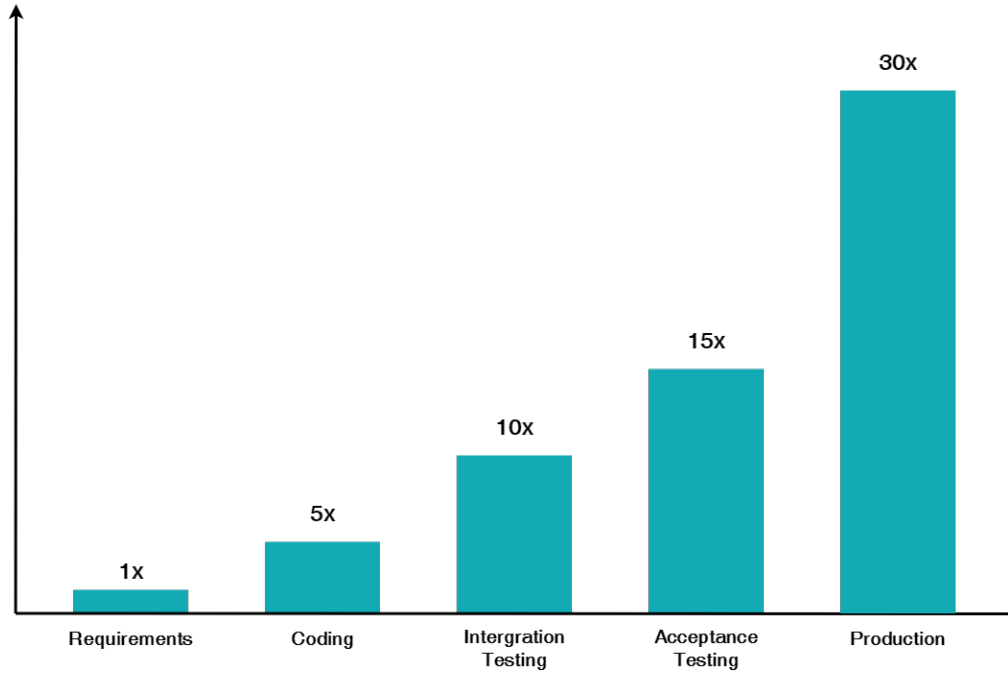


Why Organizations Need DevSecOps Now More Than Ever

# DevSecOps

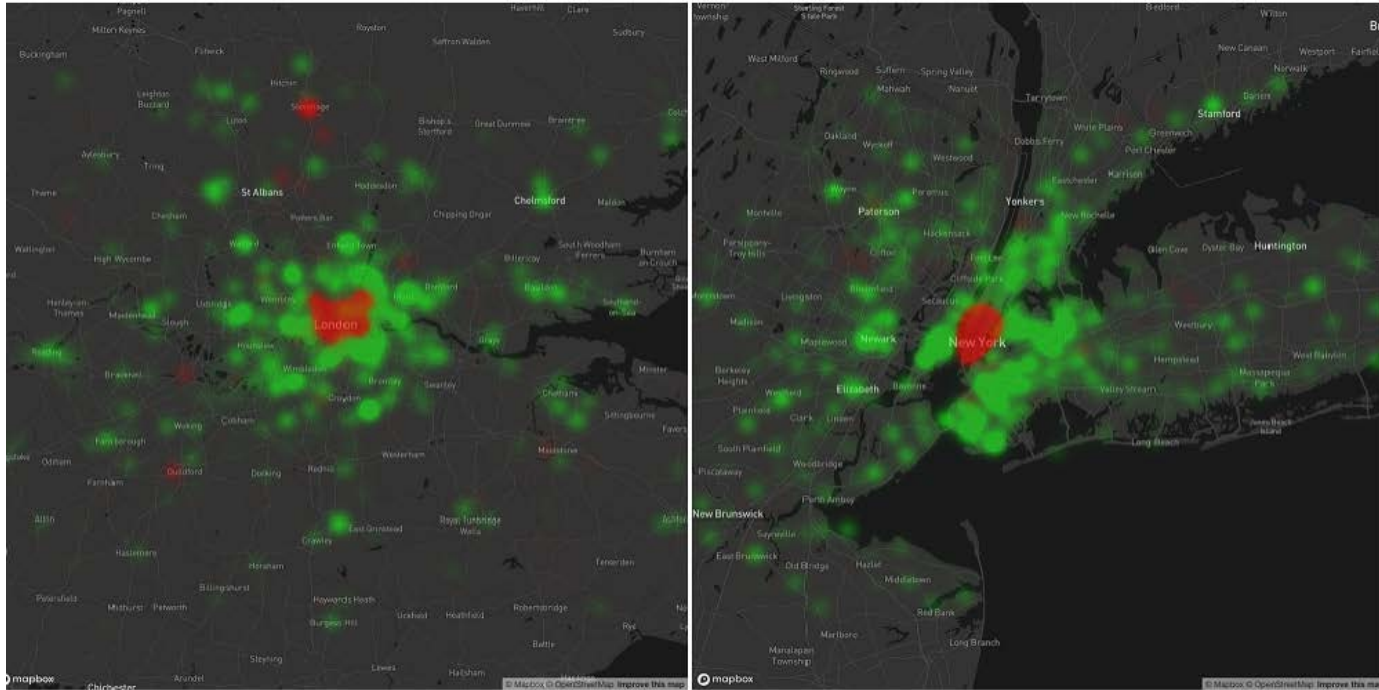


# The cost of fixing defects





# The situation now



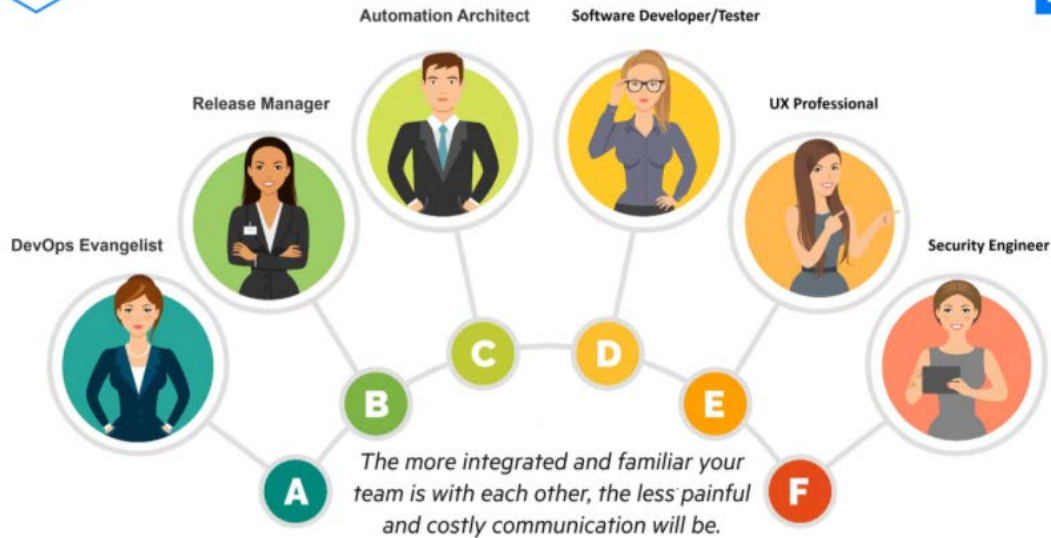
Change in internet use in London (left) and New York (right) between Wednesday 19 February and Wednesday 18 March. Red shows a decrease in traffic, green shows an increase. (Cloudflare)

Why Organizations Need DevSecOps Now More Than Ever

# DevOps to DevSecOps



# It starts with culture



Realize the importance of collaboration



Be transparent and lean

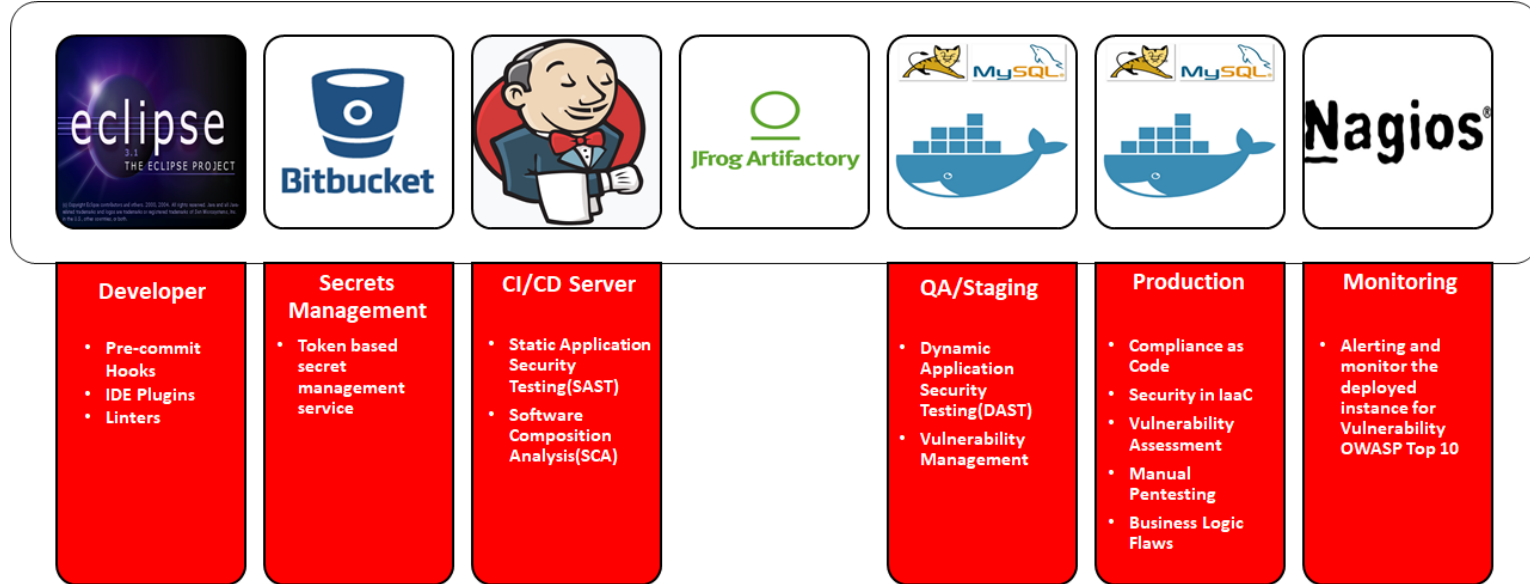


Invest time in innovation

# Creating a DevSecOps pipeline



Source: NotSoSecure

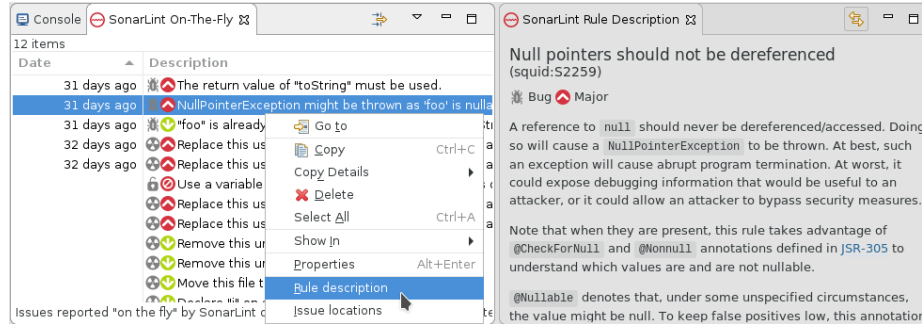


Source : NotSoSecure

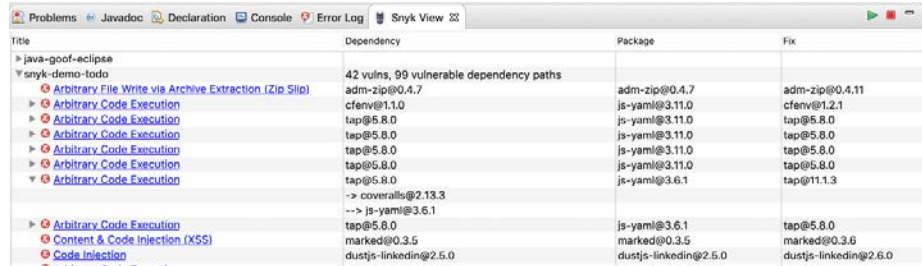


# Security plugins in IDE

## SonarLint



## Snyk Vuln Scanner



# Pre commit hooks

```
→ NoteTaker git:(chapter/6/6.2) ✗ git push origin chapter/6/6.2  
husky > npm run -s prepush (node v8.1.3)
```

```
/Users/rahulgaba/workspace/mywork/NoteTaker/app/index.js
```

```
17:12 error 'clickHandler' is assigned a value but never used no-unused-vars  
17:12 error 'clickHandler' is missing in props validation react/prop-types
```

```
✗ 2 problems (2 errors, 0 warnings)
```

```
husky > pre-push hook failed (add --no-verify to bypass)  
error: failed to push some refs to 'https://github.com/master-atul/react-native-plus-plus-code.git'
```

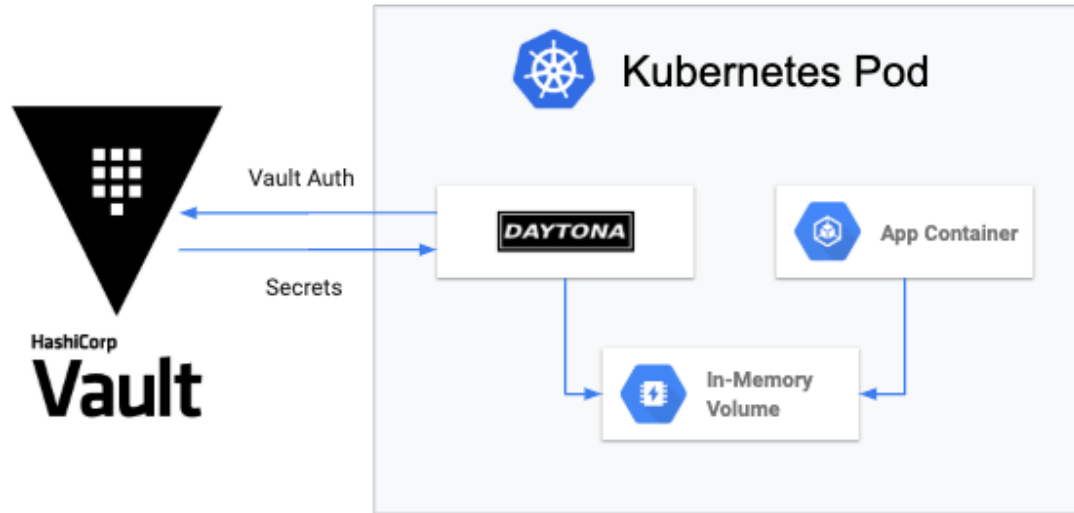
Talisman



Git hooks



# Secrets Management



AWS Secrets manager



# Software composition analysis

The screenshot shows the Snyk web interface. At the top, there's a navigation bar with 'snyk' logo, a dropdown menu for 'sjmaple', and links for 'Vulnerability DB', 'Docs', and 'My account'. Below the navigation bar, there are tabs for 'Dashboard', 'Reports', 'Projects', 'Integrations', and 'Settings'. A search bar is present with the text 'Search repositories' and a 'Search' button. To the right of the search bar, there's a status indicator 'Importing projects. View log' and an 'Add projects' button. The main content area displays a list of projects under the 'GitHub' filter. Each project entry includes the project name, a list of dependencies, a vulnerability status bar (e.g., 12 H, 13 M, 8 L), a 'View report and fix' link, a 'Test daily' dropdown, and a 'Tested an hour ago' timestamp. The projects listed are: sjmaple/goof (package.json), sjmaple/java-goof (pom.xml, todolist-core-common/pom.xml, todolist-web-common/pom.xml, todolist-web-struts/pom.xml), sjmaple/jdk9-jigsaw (session-3-jshell/Shell-Examples/pom.xml, session-3-jshell/shellFX/pom.xml, session-3-jshell/teamshell/pom.xml), sjmaple/shallow-goof (package.json), and sjmaple/spring-goof (pom.xml).

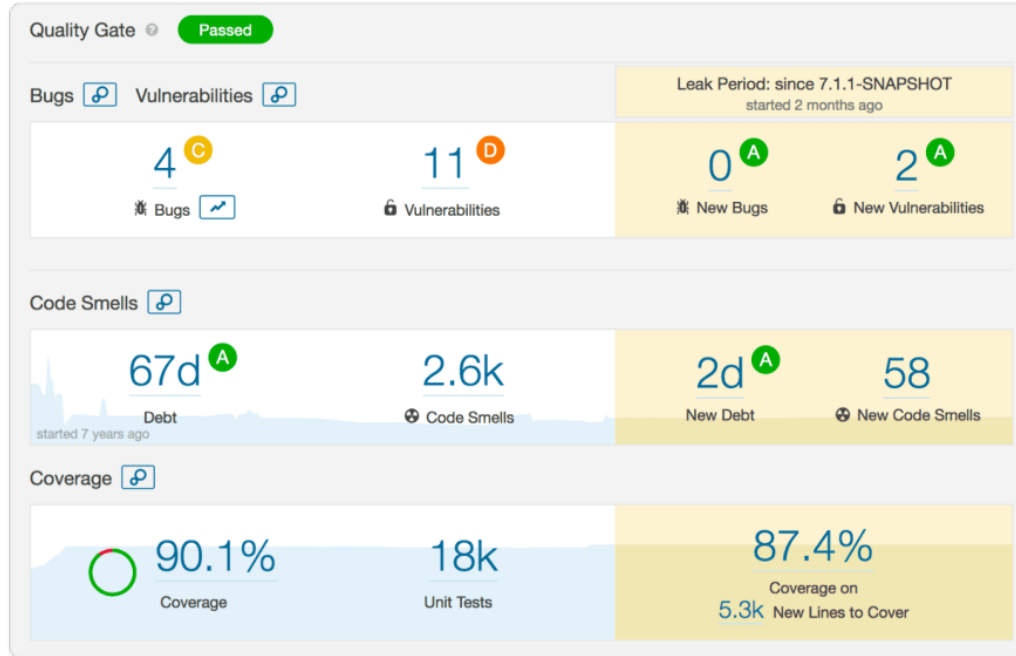
Owasp dependency check



Sonatype

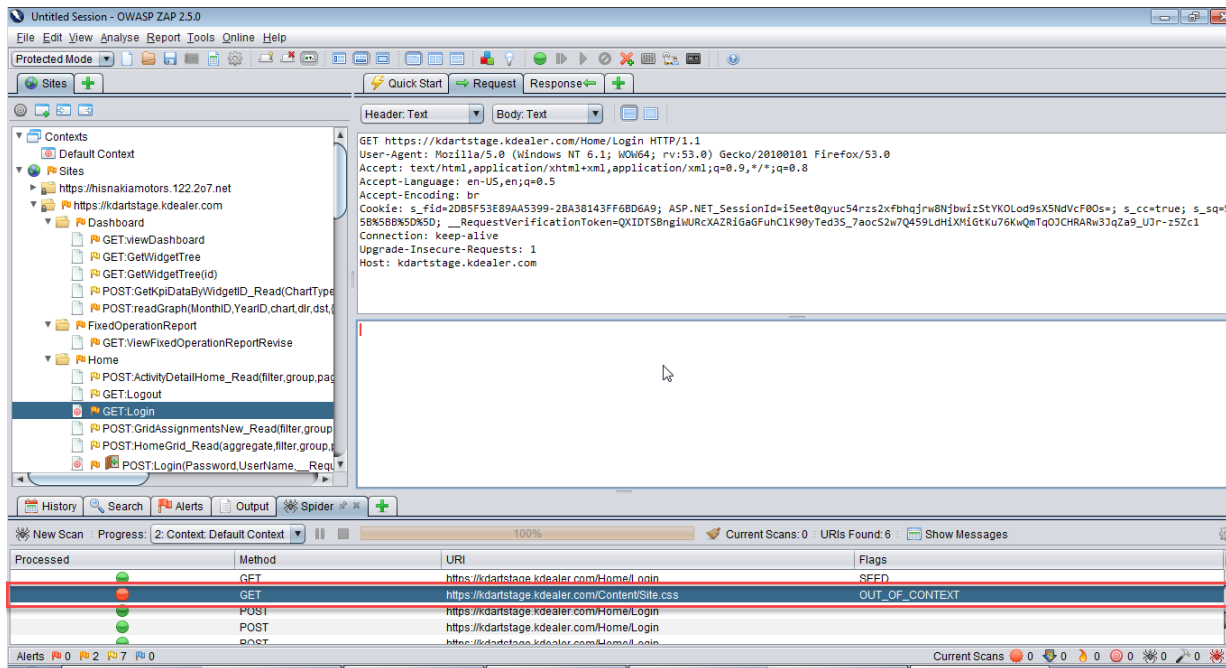


# Static Analysis



Tools that can be used – SonarQube, Bandit

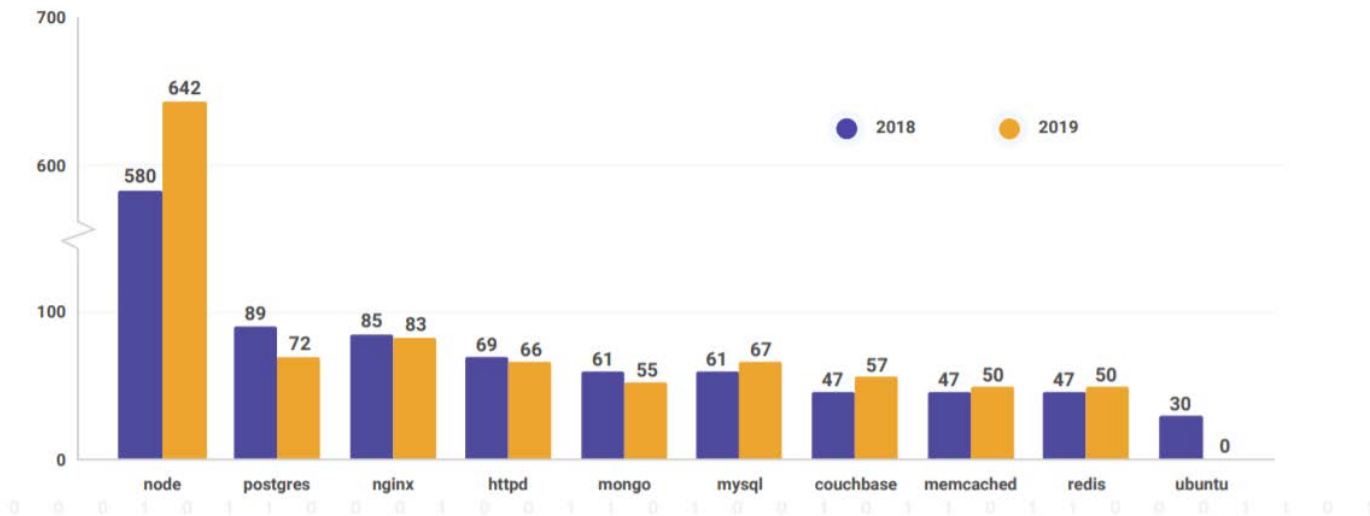
# Dynamic Analysis



Tools that can be used – OWASP ZAP, Nikto

# Embedding security into IaaS

## Vulnerabilities in official container images



Tools that can be used – Snyk, Docksan

# Compliance as Code

✓ **tls-compliance** < 4 Pipeline Changes Tests Artifacts Login X

Branch: master 1m 3s No changes  
Commit: e5fa399 3 minutes ago Push event to branch master

**All tests are passing**  
Nice one! All 20 tests for this pipeline are passing.

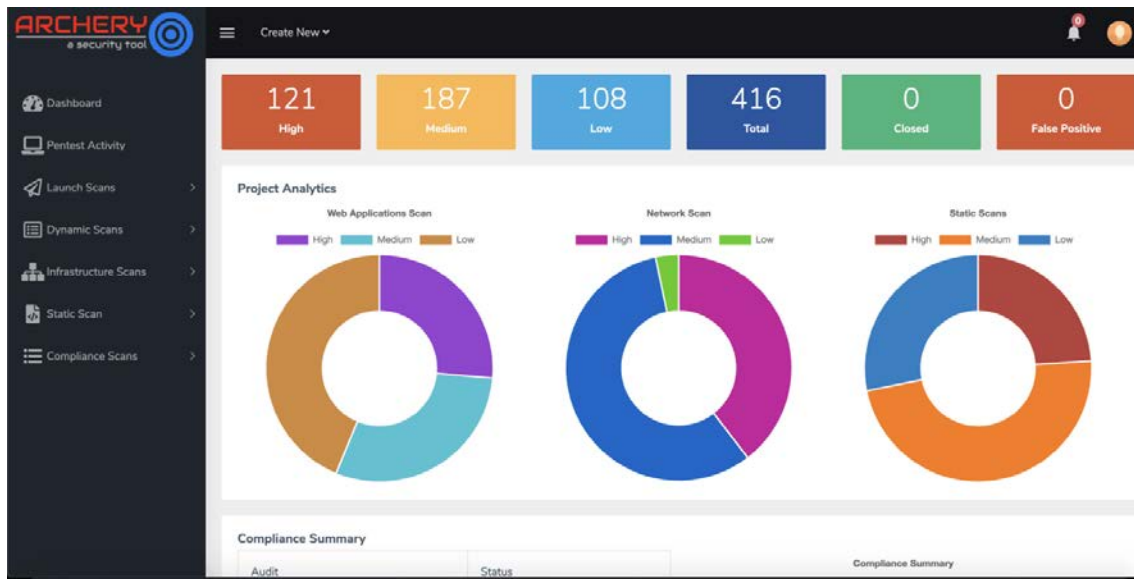
Passed - 20

✓	> TLS Compliance Test / Host github.com port 443 proto tcp should be reachable - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / Host github.com port 443 proto tcp should be resolvable - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / Host github.com port 443 proto tcp connection should not match /connection refused/ - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "ssl2" should not be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "ssl3" should not be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "tls1.0" should not be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "tls1.1" should not be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "tls1.2" should be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with cipher == "/_anon_WITH/!" should not be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with cipher == "/_WITH_NULL/!" should not be enabled - gsk-tls-testing.tls	<1s
✓	> TLS Compliance Test / SSL/TLS on github.com:443 with cipher == "/_WITH_EXPORT/!" should not be enabled - gsk-tls-testing.tls	<1s

Tools that can be used – Inspec, Kitchen CI

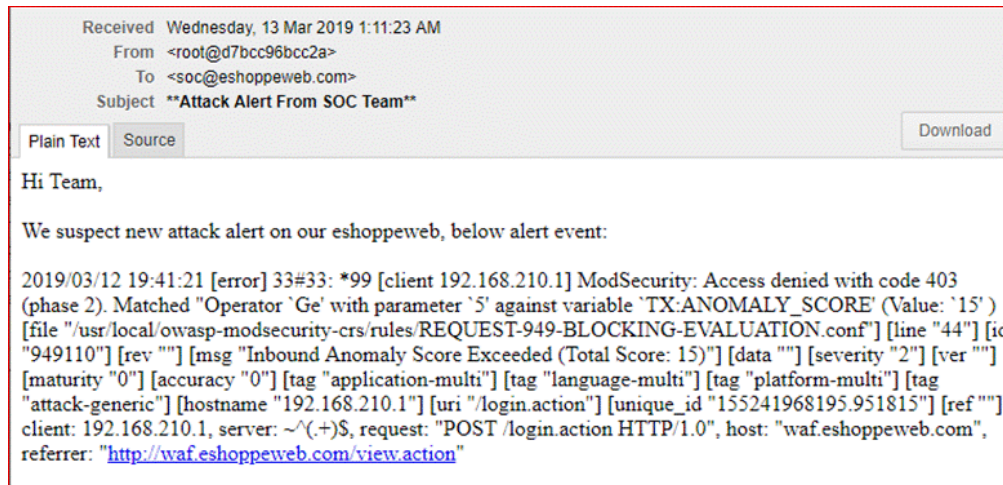


# Vulnerability Dashboard



Tools that can be used – ArcherySec, DefectDojo

# Alerts and Monitoring



Modsecurity notification

# References



<https://www.synopsys.com/blogs/software-security/devsecops-pipeline-checklist/>

<https://notsosecure.com/achieving-devsecops-with-open-source-tools/>

<https://www.slideshare.net/notsosecure/devsecops-what-why-and-how-blackhat-2019>

<https://www.ciodive.com/news/devsecops-security-CIO-infosec/576379/>

<https://www.technologyreview.com/2020/04/07/998552/why-the-coronavirus-lockdown-is-making-the-internet-better-than-ever/>

<https://www.crn.com/news/cloud/refactr-ceo-coronavirus-crisis-is-rapidly-accelerating-shift-to-devsecops?itc=refresh>

## Q and A