Why Organizations Need DevSecOps Now More Than Ever

Krishna Guru

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Agenda

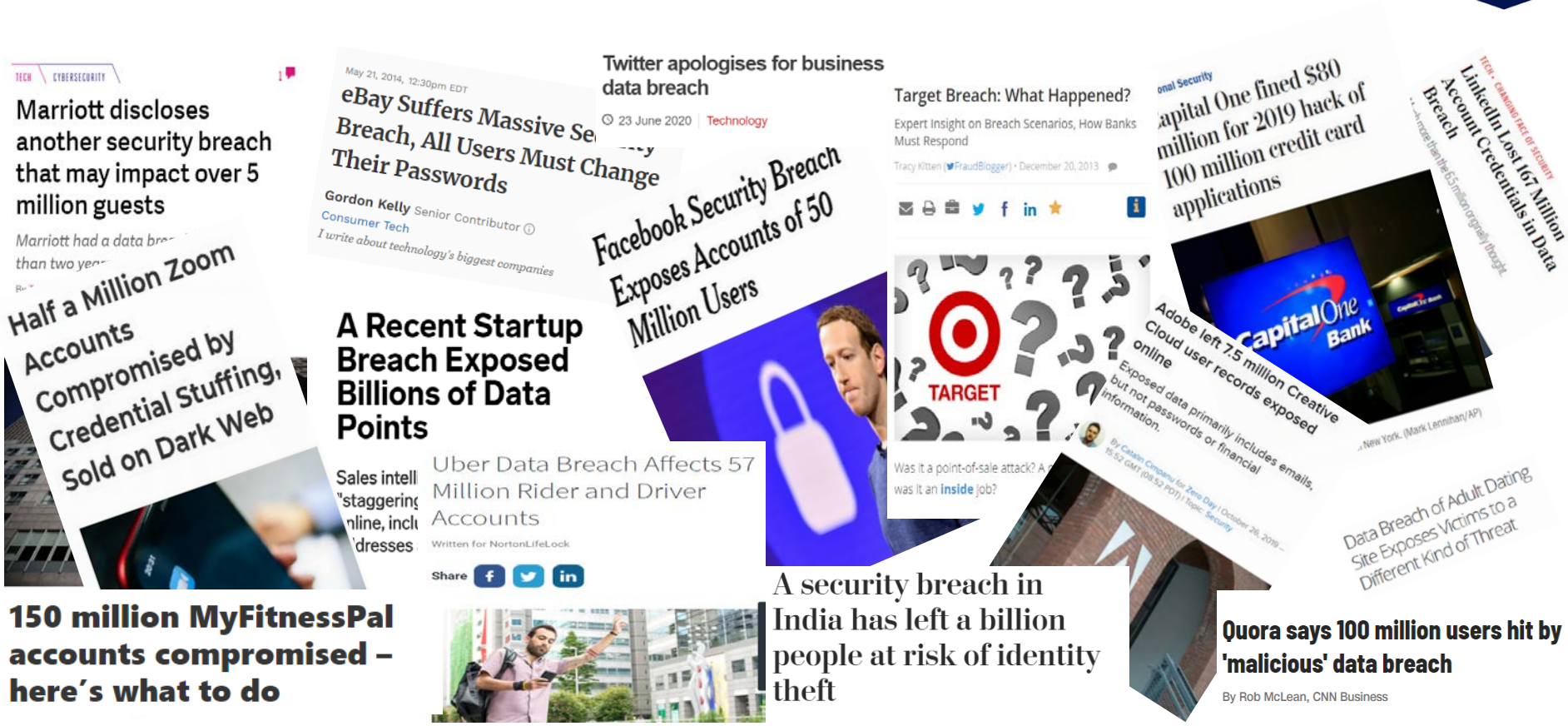
- Data breach
- Open-source software
- DevSecOps
- The current situation
- Transforming from DevOps to DevSecOps
- Q & A

DEV SEC OPS DAYS

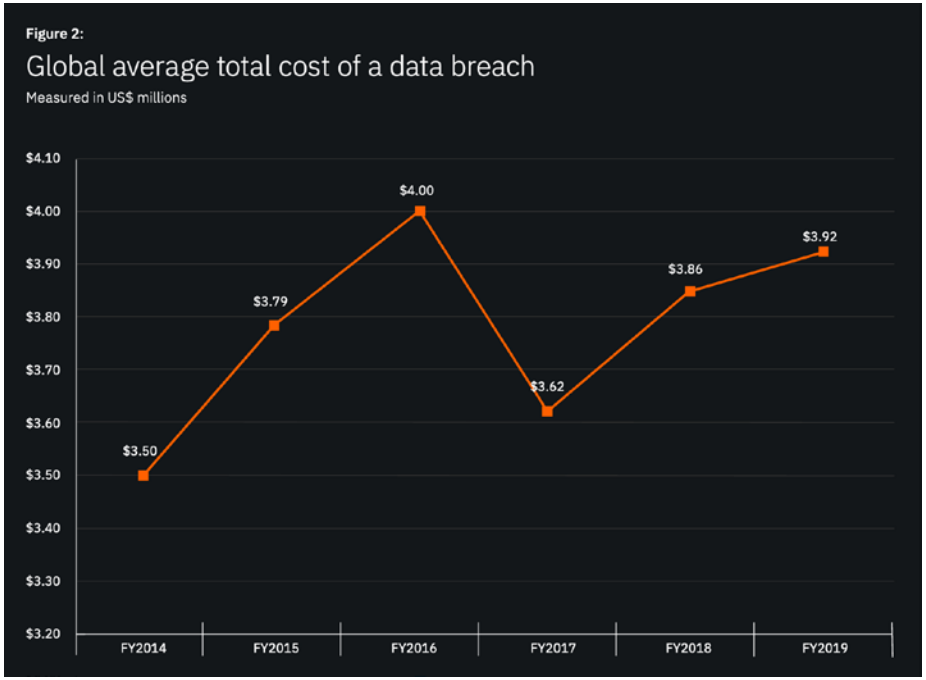
Why Organizations Need DevSecOps Now More Than Ever

Data breach

Data Breach

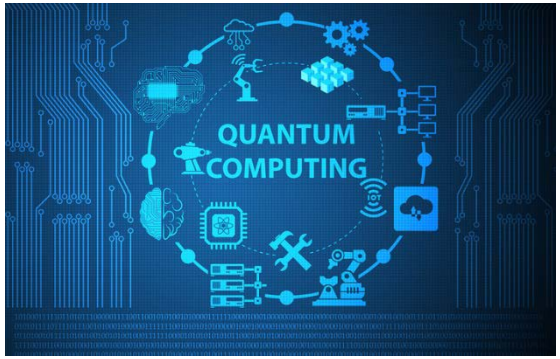


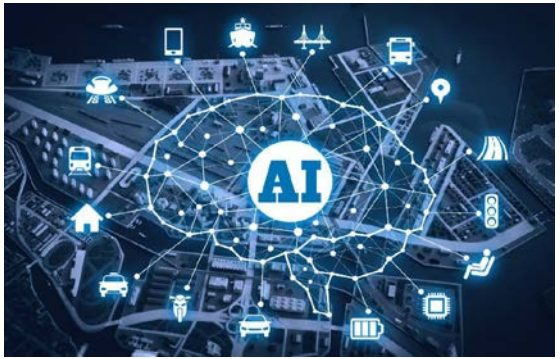
Cost of a breach



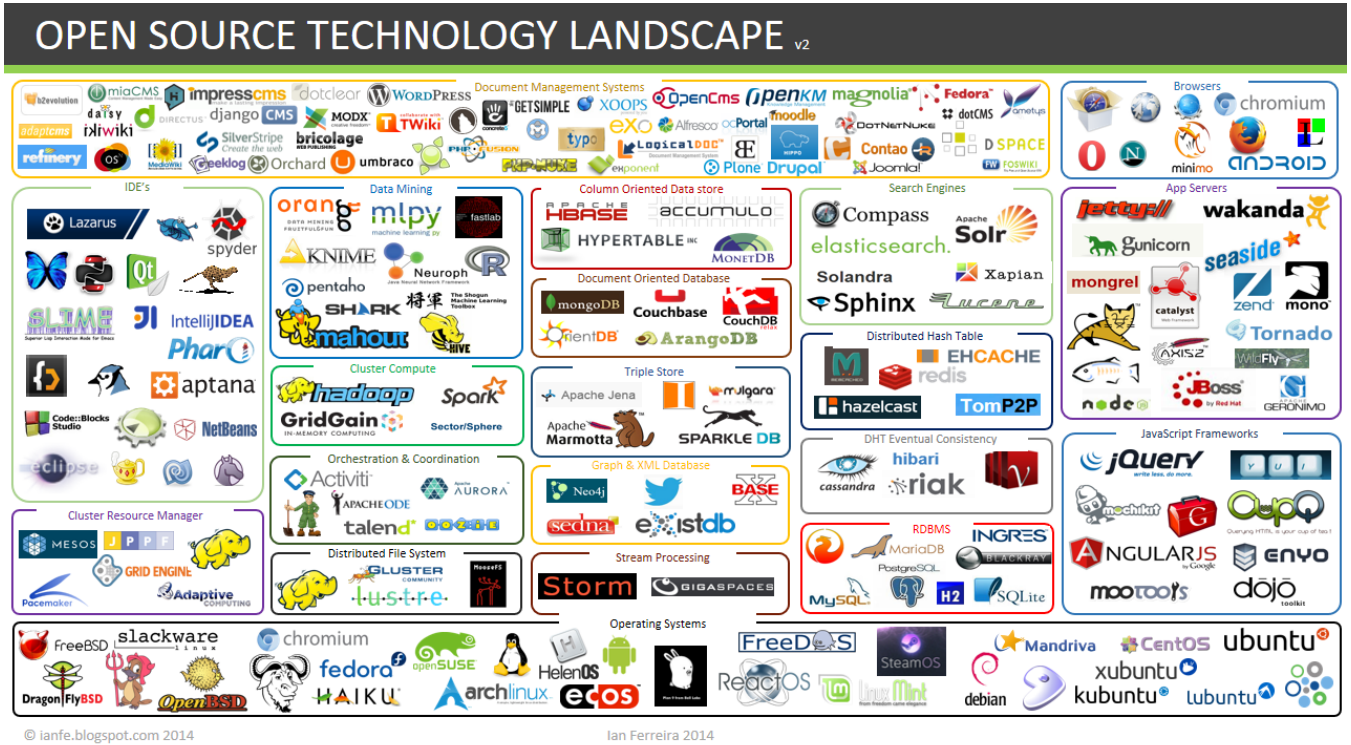
Source - IBM and the Ponemon Institute's annual Cost of a Data Breach report

Threat to emerging technologies

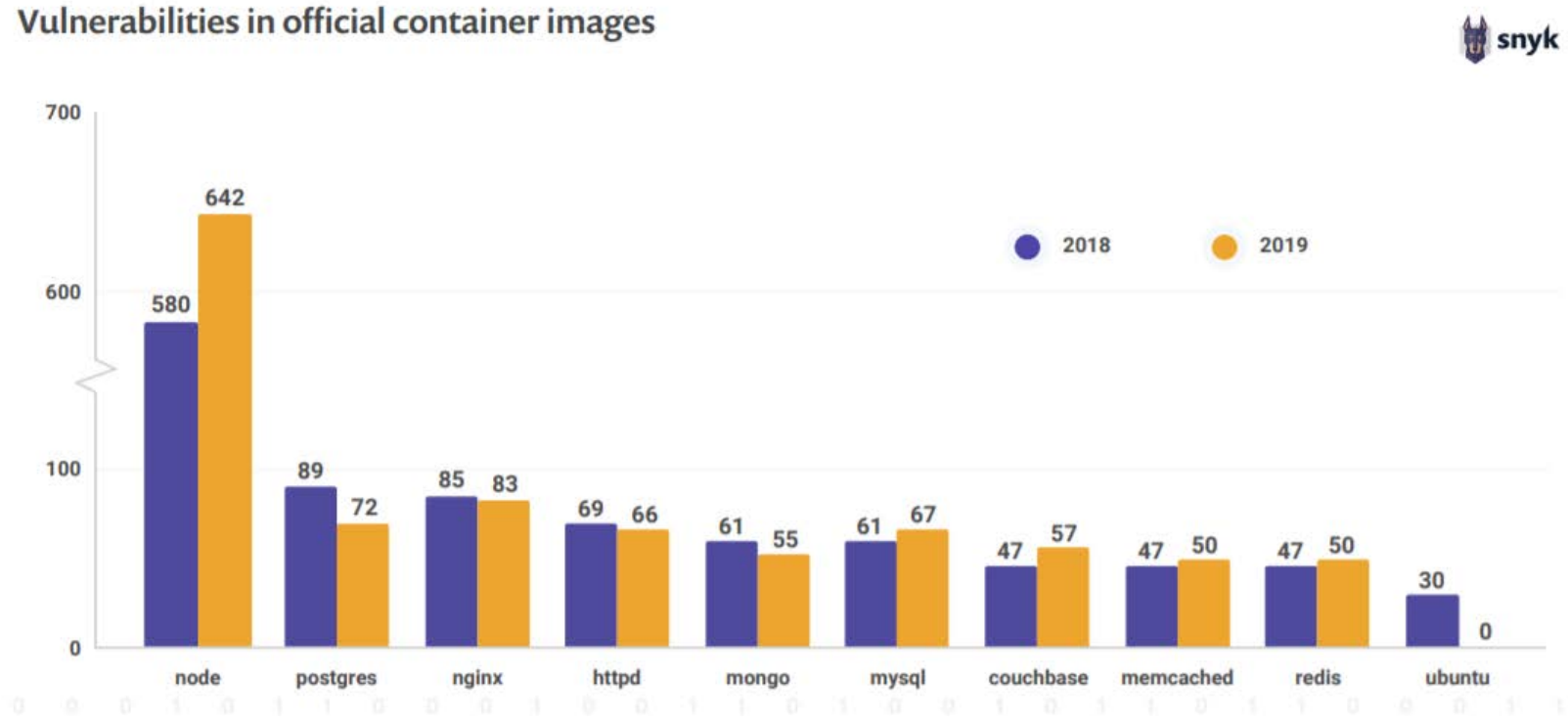




Open-source software



Threats in Open-source software

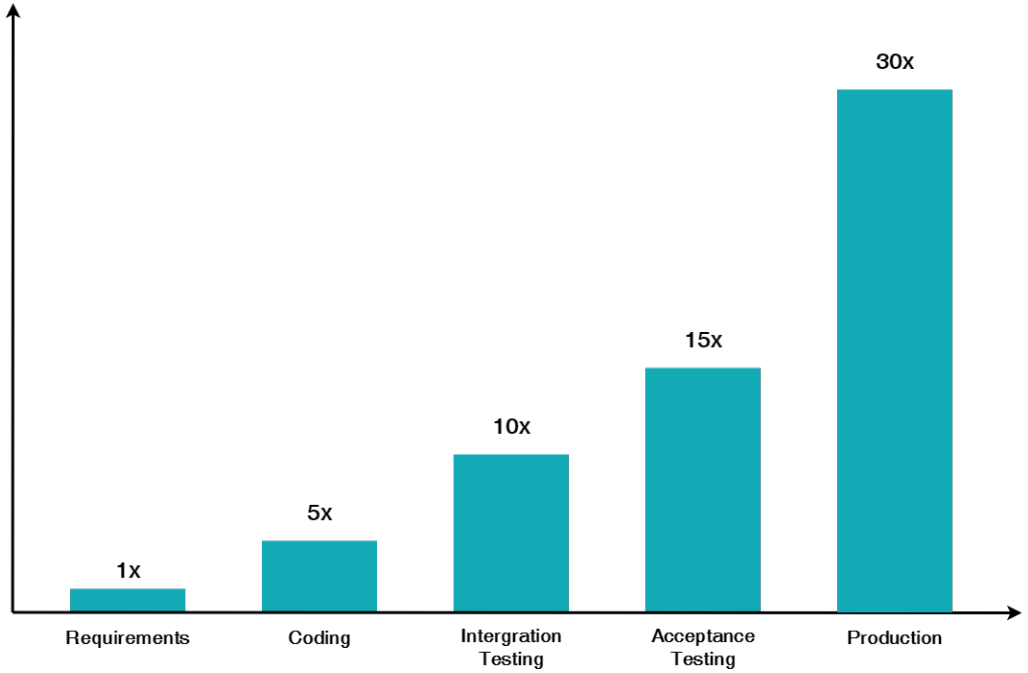


DEV SEC OPS DAYS

Why Organizations Need DevSecOps Now More Than Ever

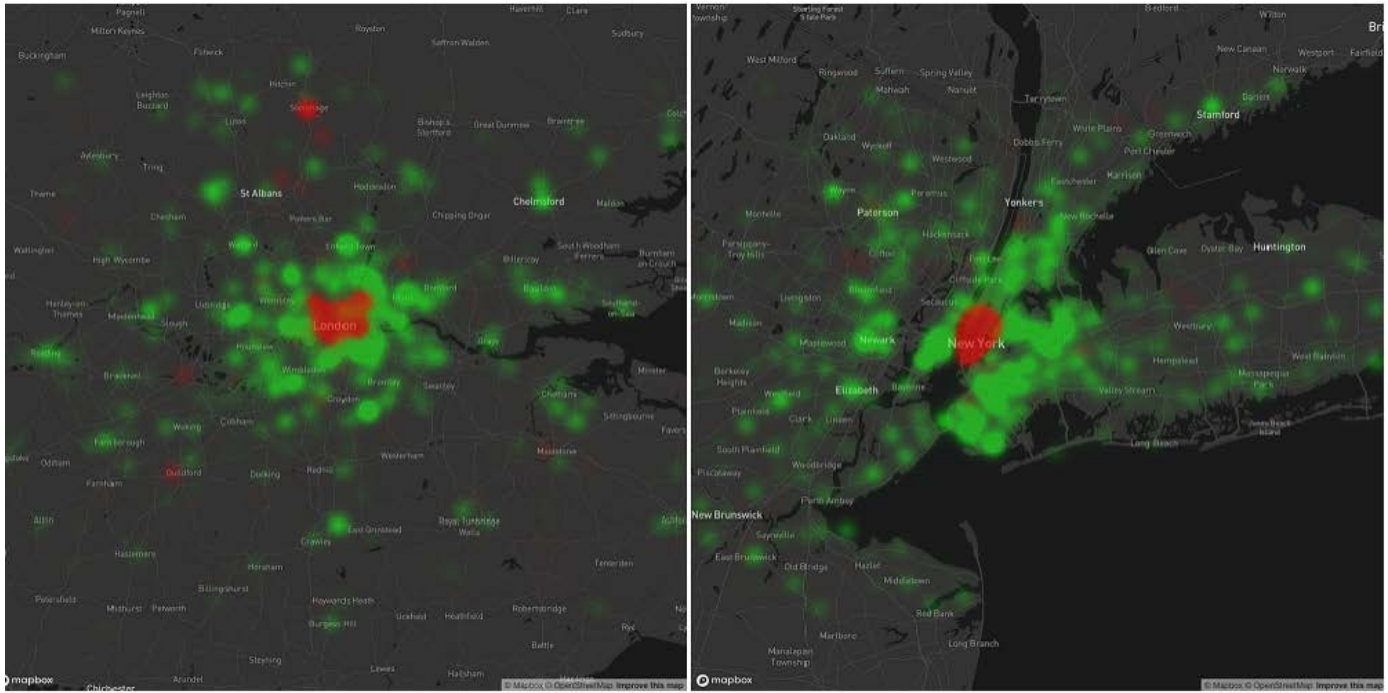
DevSecOps

The cost of fixing defects



DevSecOps

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. (Cloudfare)

DEV SEC OPS DAYS

Why Organizations Need DevSecOps Now More Than Ever

DevOps to DevSecOps

It starts with culture

Creating a DevSecOps pipeline

Source: NotSoSecure

Developer

- Pre-commit Hooks
- IDE Plugins
- Linters

Secrets Management

- Token based secret management service

CI/CD Server

- Static Application Security Testing(SAST)
- Software Composition Analysis(SCA)

QA/Staging

- Dynamic Application Security Testing(DAST)
- Vulnerability Management

Production

- Compliance as Code
- Security in IaaC
- Vulnerability Assessment
- Manual Pentesting
- Business Logic Flaws

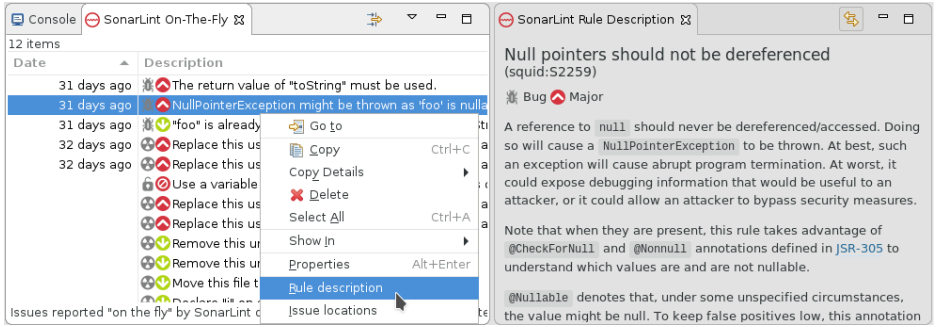
Monitoring

- Alerting and monitor the deployed instance for Vulnerability OWASP Top 10

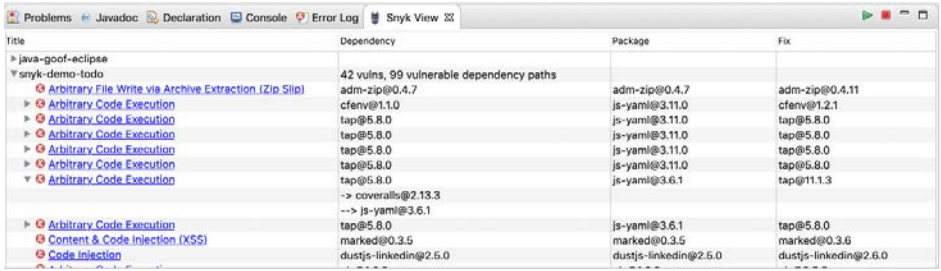
Source : NotSoSecure

Security plugins in IDE

SonarLint



Snyk Vuln Scanner



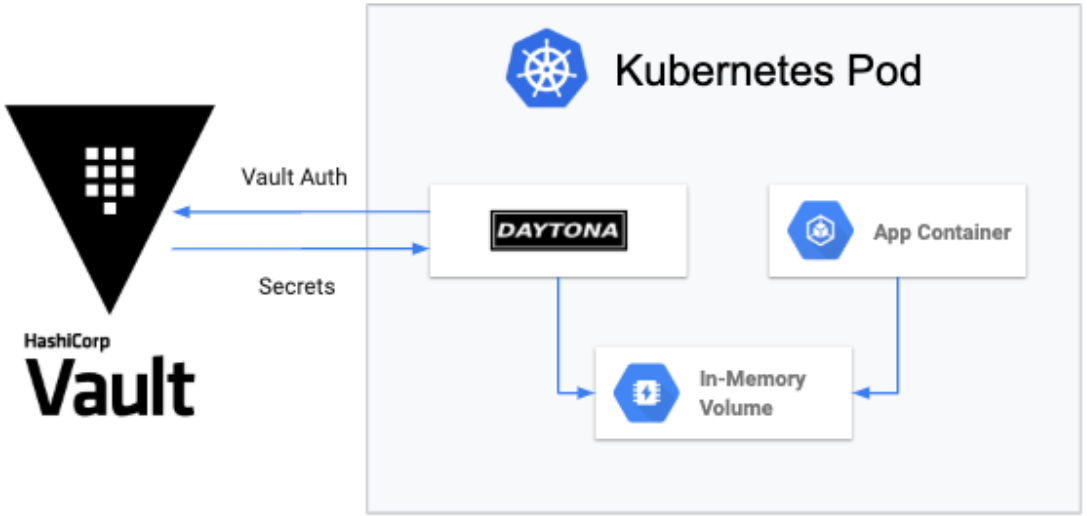
Pre commit hooks

```
➜  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

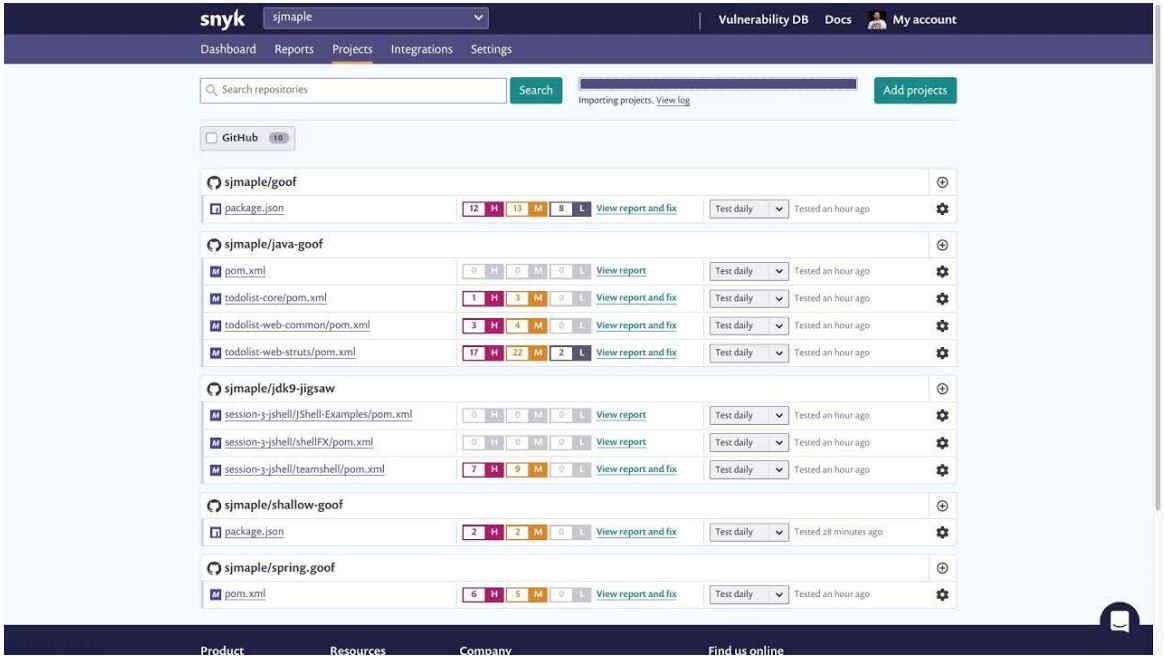
Git hooks

Secrets Management



AWS Secrets manager

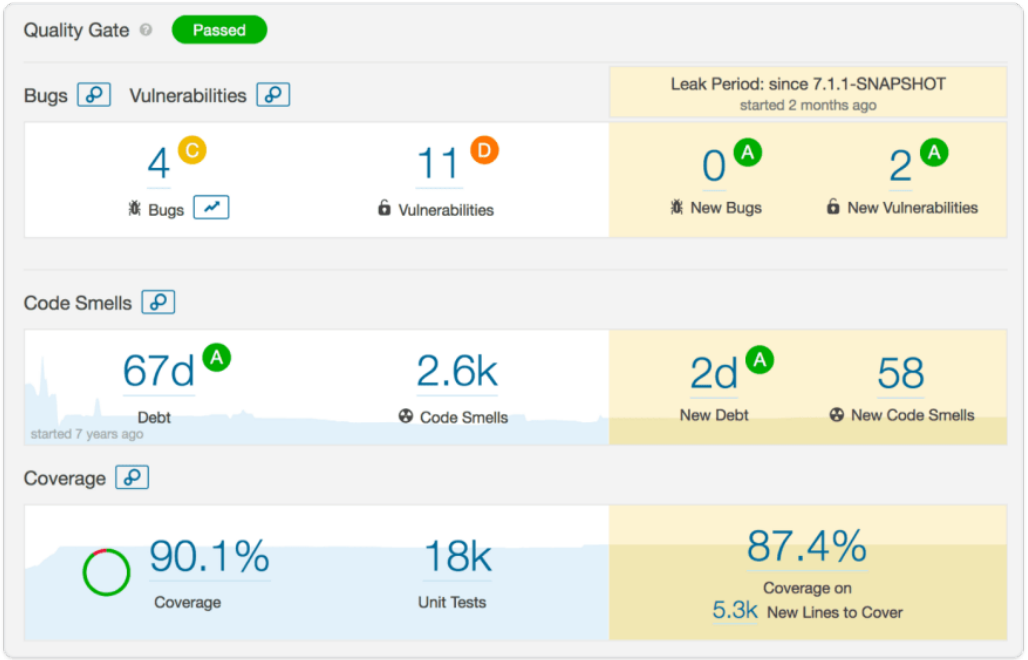
Software composition analysis



Owasp dependency check

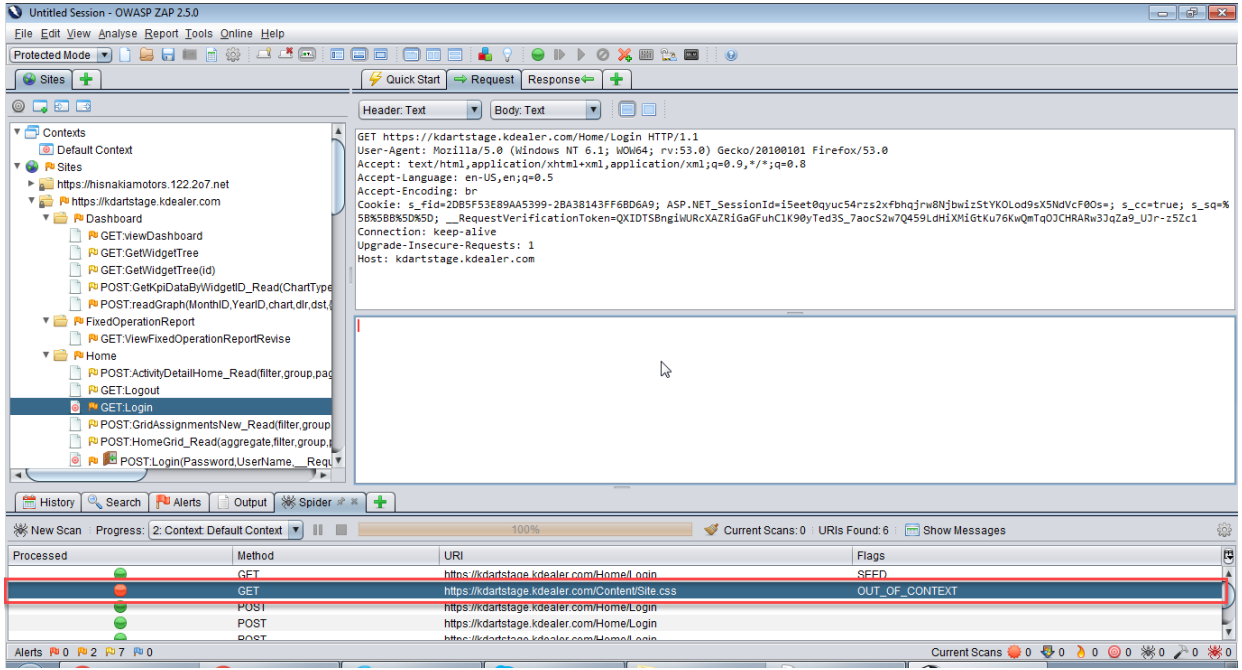
Sonatype

Static Analysis



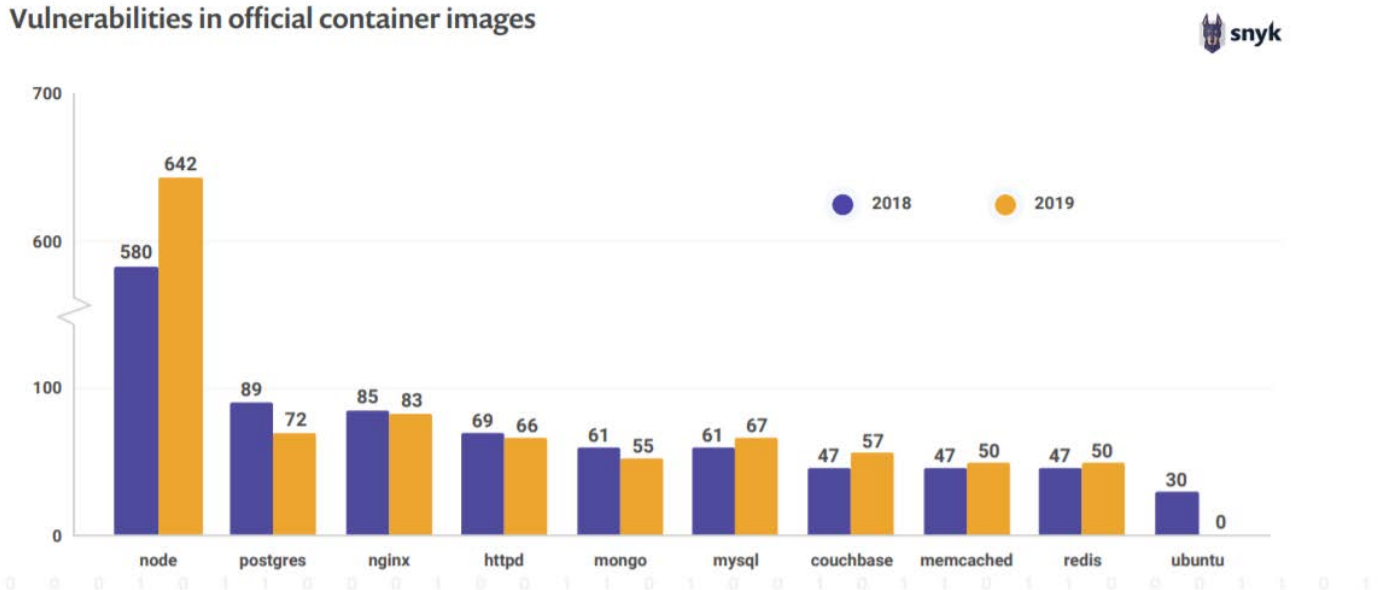
Tools that can be used – SonarQube, Bandit

Dynamic Analysis



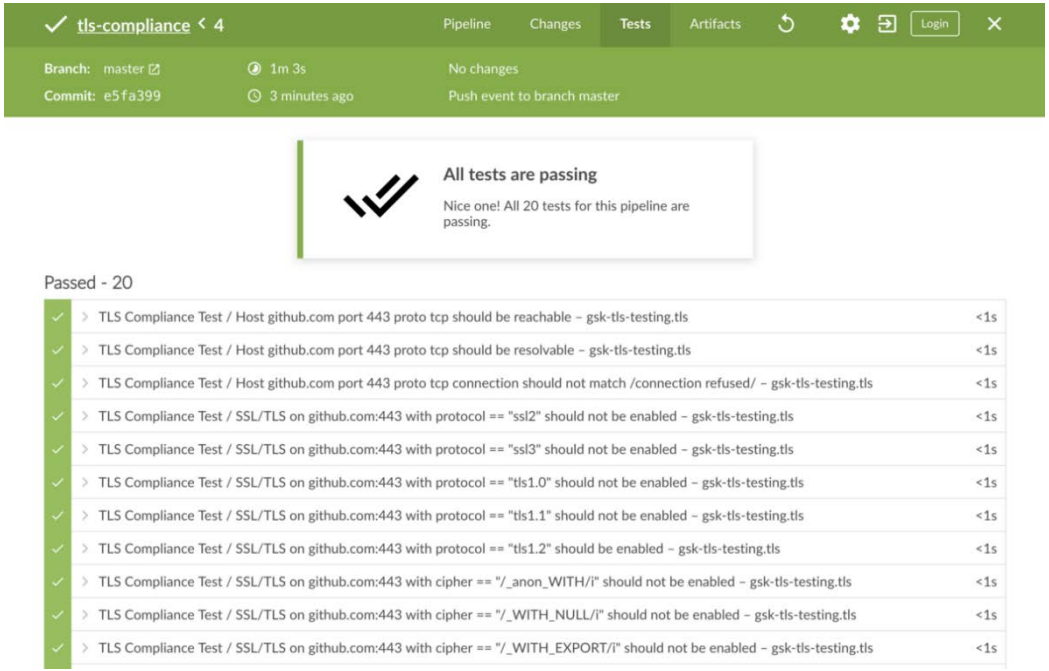
Tools that can be used – OWASP ZAP, Nikto

Embedding security into IaaS



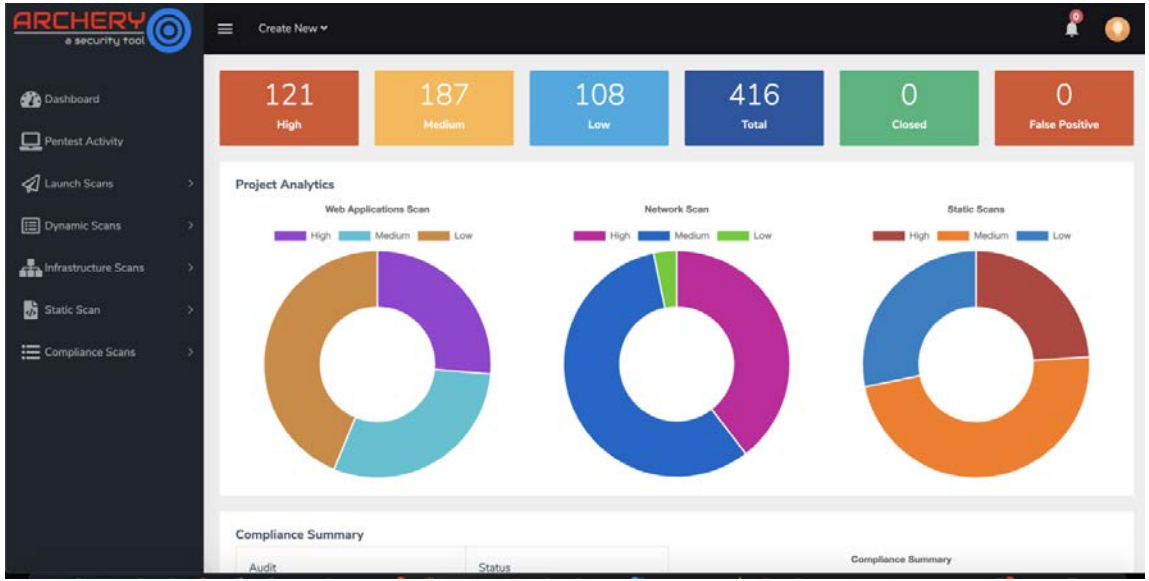
Tools that can be used – Snyk, Docksan

Compliance as Code



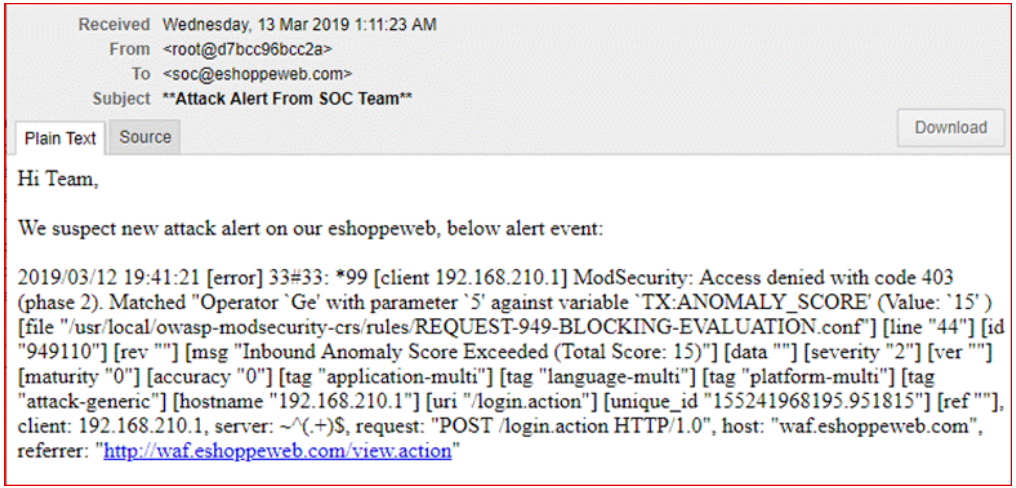
Tools that can be used – Inspec, Kitchen CI

Vulnerability Dashboard



Tools that can be used – ArcherySec, DefectDojo

Alerts and Monitoring



Received Wednesday, 13 Mar 2019 1:11:23 AM
From <root@d7bcc96bcc2a>
To <soc@eshoppeweb.com>
Subject **Attack Alert From SOC Team**

Plain Text | Source | Download

Hi Team,

We suspect new attack alert on our eshoppeweb, below alert event:

2019/03/12 19:41:21 [error] 33#33: *99 [client 192.168.210.1] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15') [file "/usr/local/owasp-modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "44"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [data ""] [severity "2"] [ver ""] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "192.168.210.1"] [uri "/login.action"] [unique_id "155241968195.951815"] [ref ""], client: 192.168.210.1, server: ~^(.+)$, request: "POST /login.action HTTP/1.0", host: "waf.eshoppeweb.com", referrer: "http://waf.eshoppeweb.com/view.action"

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