Achieving Secure Continuous Delivery (cont..)
--lightning talk--

Nikos / Jesus / Lucian
April 2018
Typical discussions...

FORTIFY FOUND 1356 VULNS AND WE FIXED THEM ALL... [COOL]

WE STILL RUN ALL SECURITY TESTS MANUALLY, PEOPLE LEAVING OUR TEAM... [NOT COOL]

WE RAN CHECKMARX YESTERDAY AND FOUND ANOTHER 459!

DON'T WORRY, YOU'LL GET THERE, I HAVE A TOOL IN MIND FOR YOU...
Pain points

- Same problem in 2018!
- Difficult access to (uncorrelated) vulnerability data
- No clear view on the security risk of a specific build or release
- No real agreed security gate (no trigger threshold)
- Short memory! Tools get easily forgotten or abandoned...
- Product has a Roadmap and Security is (always) not (always) part of it
- Security requirements appear (dark magic!) when project is almost finished
- Security sign-off is a bottleneck [choke]
- Security testing tools! Lots of tools!! And reports!!!
- When am I finally secure enough? Never! says Mordac.
Tools!!

SAST list [HERE]

DAST list [HERE]

Dependency Checking Tools list [HERE]

Container Security tools [HERE]

Google list [HERE]

Others [HERE]
The Want

- Automation & centralisation of application security testing
- Risk based approach to application delivery & deployment
- Security Champions process and responsibilities
Existing initiatives

Lots!!!

OWASP AppSec Pipeline  OWASP OWTF  OWASP Defect Dojo

Others talking about this

OWASP Israel

Christian Schneider

SAMPLE

OWASP AppSec Pipeline
Where we are now

- Jenkins
- GitLab
- GitHub
- TFS
- Fortify
- Checkmarx
- OWASP
- Dependency-Check
- Qualys WAS
- OWASP
- Node Security Project
- Ready! API
- Zed Attack Proxy
- Cloudflare
- iMPERVA
- JIRA
- TFS
- X-Force
- Waratek
- OWASP
- Open Web Application Security Project
Developer Jenkins

#912 triggered by remote trigger changes by Nikos Savvidis started 5 days ago

Total build time: 10 min 52 sec

Changes:
1698e456796d8be2e1e43f0dedae6463358e19df Nikos Savvidis Turning onboarding creditor verification flow off again.

BUILD
build
5 days ago 5 min 22 sec

Test Result
Total Failures Skipped
740 0 3

QA
deploy
deploy
test
DDM Security Testing
DDM Threadfix Security Policy Check

OWASP
Open Web Application Security Project
Security Jenkins

1. How does Jenkins run tools

2. How does Threadfix receive results

3. Check my policy

4. How we inform
Threadfix policies

The image shows the Threadfix interface with the policies status set to "PASSING". The table lists various policies such as CHLM, XSS, CHLW, CSRF, SQL Injection, Injection, CH, etc., each with a corresponding filter name (CHLM, XSS-filter, CHLW, CSRF, SQL Injection, Injection, CH) and status (PASS). The URL in the browser is `/threadfix/rest/applications/15/policyStatuses?apiKey`.
Fixing the stuff

GO FIX IT!
**Next?**

<table>
<thead>
<tr>
<th>What is best for you and your businesses’ appetite?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get a DevSecOps team to build and maintain toolz&amp;stuff for you £££</td>
</tr>
<tr>
<td>OWASP project (Pipelines?) to support all free tool inputs into one central repo</td>
</tr>
<tr>
<td>(Somehow) work with commercial tool providers to support that</td>
</tr>
</tbody>
</table>

Inspire and empower your Security Champions
Q/A

AUTOMATION
DON'T KILL BUGS,
PEOPLE* DO

HA, HA,
HA!

☆ DEVELOPERS MAINLY - SINCE THEY WERE THE ONES WHO CREATED THE BUGS IN THE FIRST PLACE

AG