

OWASP Summit 2017 Debrief



 **Stephen de Vries**
@stephendv Following

The #OWASPSummit has spoiled me for other cons: [continuumsecurity.net/owasp-summit-e ...](https://www.continuumsecurity.net/owasp-summit-e...)
many thanks to @sebadele, @devseccon and @DinisCruz for organising

 **The OWASP Summit exceeded all expectations - Continuum..**
I attended my first OWASP Summit last week and it has spoiled most other conferences for me. The summit is not a traditional conference where an "expert" is selected by the CFP panel a...
[continuumsecurity.net](https://www.continuumsecurity.net)

Retweets **7** Likes **6**

10:00 AM - 19 Jun 2017

THE OWASP SUMMIT EXCEEDED ALL EXPECTATIONS

Home » THE OWASP SUMMIT EXCEEDED ALL EXPECTATIONS

The OWASP Summit exceeded all expectations

By Stephen De Vries | 19 June 2017 | Conferences, SecDevOps

I attended my first OWASP Summit last week and it has spoiled most other conferences for me. The summit **is not a traditional conference** where an "expert" is selected by the CFP panel and has 40 minutes to expound The Truth from a podium, while everyone else takes notes. I'd call this a "top down" style of conference, and most in the security and appsec space follow this format.

What made the OWASP Summit unique was that it was a "bottom up" conference. A large number of topics were selected months ago, thrown up onto a github page where anyone interested could sign up as an organiser or participant (no speakers). Participants could then suggest an outcome for the session, push some initial content and get the conversation going. If no-one registered for a given topic, then it was removed. Initially, I thought this system was chaotic and would result in 20 strangers sitting in a room waiting for someone to lead. The exact opposite happened.

Everyone participating in a session had a real interest in being there and contributing or listening and the participants spanned the range from security consultants, to architects to CISOs. The result was engaging and informative discussion about key appsec topics where we could all challenge established ideas and dig deeper into the How and the Why of many practices.

Another key to the success was the calibre of the participants. I bumped into participants from Oracle, Microsoft, AXA, Adobe and Capital One. Participants who are actually implementing the practices contributed to the quality of the discussions during each session.

The premise was that each session should result in an outcome, something that can be published or used as a starting point for more material. While I don't think many of the sessions achieved that goal, the real value was in the mental work and discussions during the sessions. In short, I'll be attending every summit from now on and would love to see it becoming an annual event.

Many thanks to Sebastien Deleersnyder, Francois Raynaud and Dinis Cruz for organising the event as well as the many individual session organisers who made this event such a success. See you next year!

RECENT POSTS

- The OWASP Summit exceeded all expectations
- OWASP Summit 2017
- First International Workshop on Gender and Cybersecurity
- Continuum Security at the Digital Enterprise Show 2017
- Security workflows for DevOps teams with IriusRisk

TAGS

- Community Edition,
- Devops Security, Events, Jira Risk,
- News, Programming,
- Threat Modeling,

ARCHIVES

- June 2017
- May 2017
- April 2017
- February 2017
- January 2017



12-16 JUNE 2017
WOBURN FOREST CENTER PARCS

Welcome
to OWASP
Summit 2017!



Let's start with
a question



Who are **we**?



Full screen



0:01 / 1:01



See video at
<https://youtu.be/RlyPSY0KS2k>



We are the
crazy ones

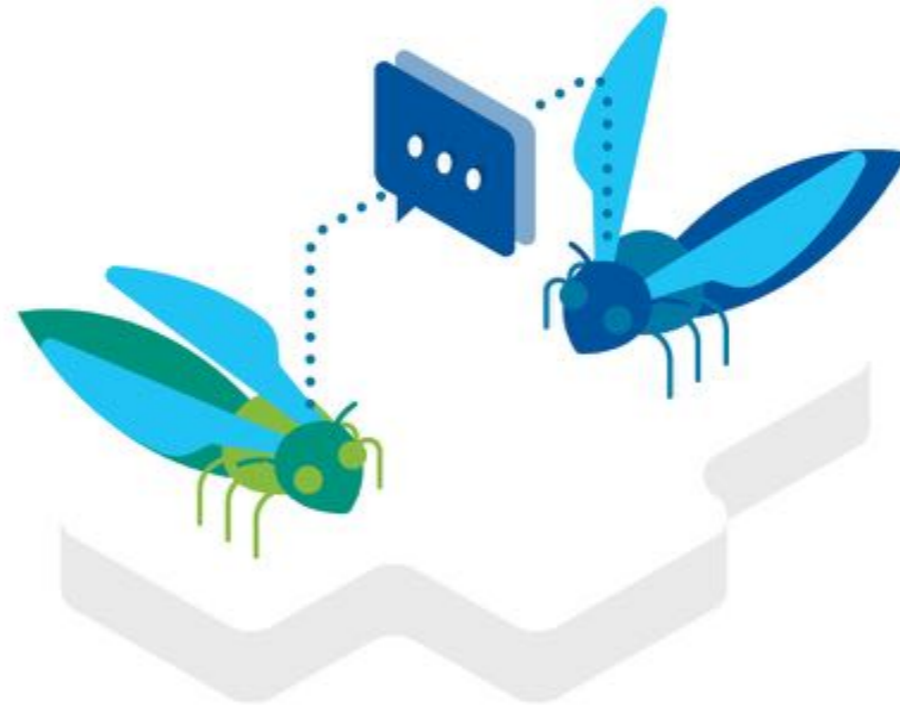
Who think we can
change the world

And who will
change the world

This **Summit** is our
opportunity to create
something amazing

The slide features several stylized dragonflies in shades of blue and green, scattered across the background. Some are positioned in the top left, some in the bottom right, and others in the middle left and right areas, creating a decorative border around the central text.

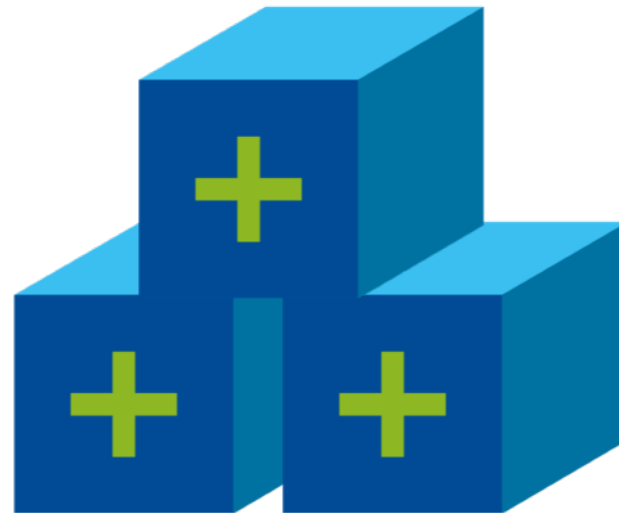
Look around
this room



Everybody is here to
collaborate and share
their knowledge

This is
unique and
very special

We have
the opportunity to
create amazing
outcomes



Use this opportunity
to **learn** and to **solve**
hard problems

In the next 5 days
our actions will
create a **lasting legacy**

But for that
to become *real*

We need to focus 100%
on the outcomes of
your **Working Sessions**



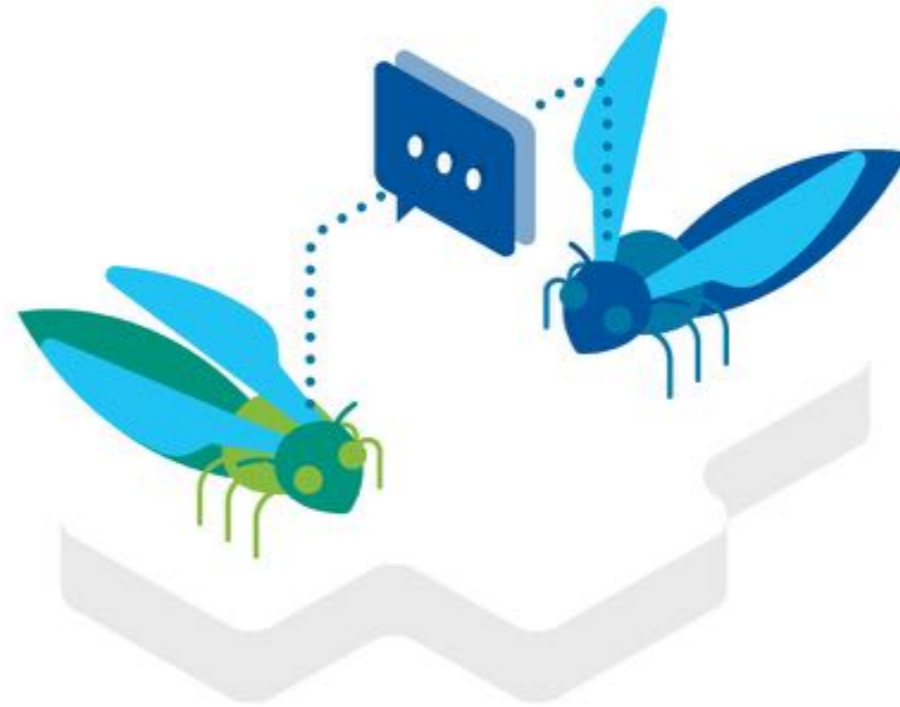
Each Working Session
has to create a
tangible outcome

That is how
we will measure the
success of this Summit

We have an
amazing Summit
team that is focused
in making you productive

Please
help them as
much as possible

Thank you for
being here and for
believing in the Summit



Now is the
time to deliver



Now it's **your** turn



12-16 JUNE 2017
WOBURN FOREST CENTER PARCS

JOIN THE CONVERSATION



SPONSORED BY

OWASP Foundation
OWASPSAMM project
OWASP London Chapter
OWASP Denver Chapter

OWASP Belgium Chapter
OWASP Netherlands Chapter
OWASP German Chapter
OWASP Luxembourg Chapter



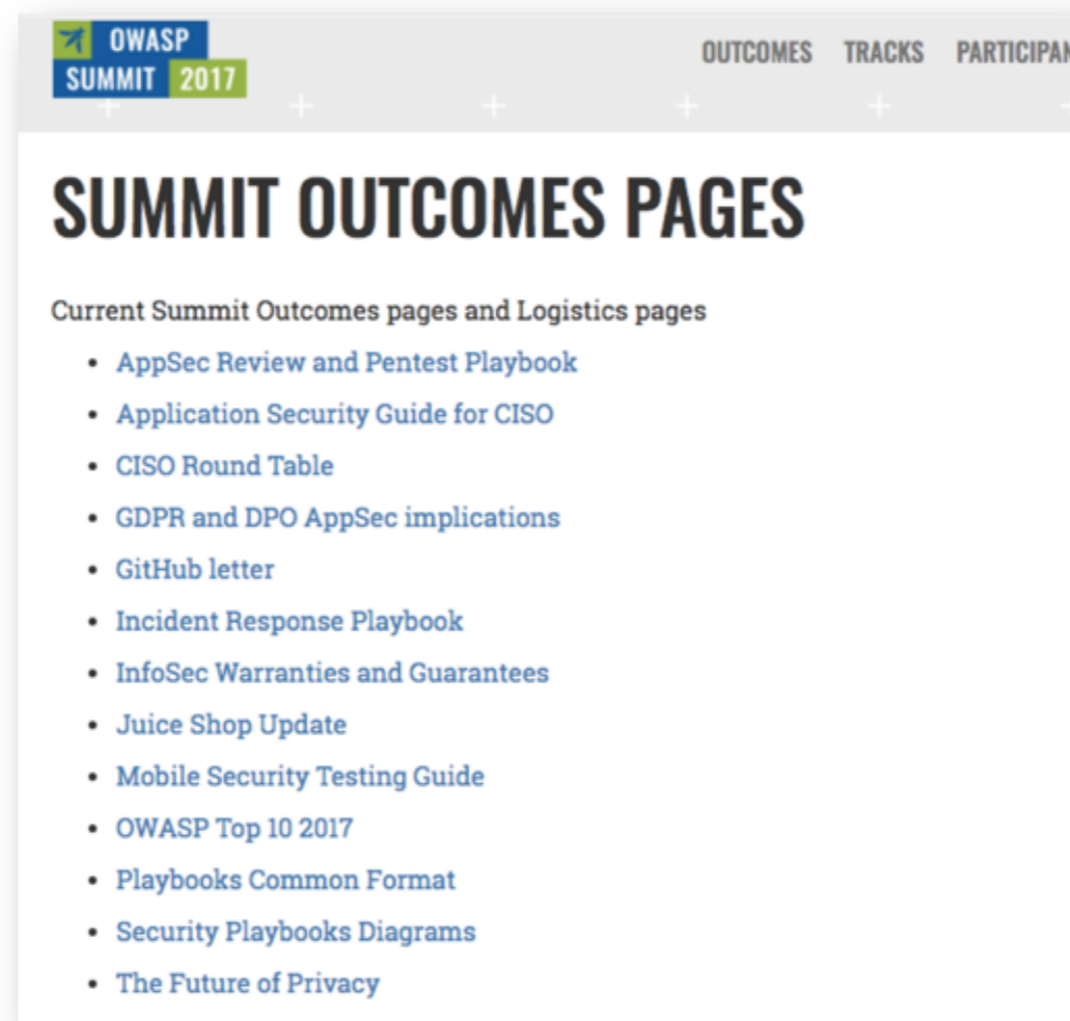
Monday's Schedule



location	AM 1 10:30 to 12:30 (2h)	PM 1 13:30 to 15:00 (1.5h)	PM 2 15:30 to 16:40 (1h)	PM 3 16:30 to 17:30 (1h)
Kings Room-1		TLS for Local IoT DevSecOps	Security Guild vs Security Champions DevSecOps	OWASP Internet of Things Project Owasp-Projects
Portland Room-2	Top 10 2017 - Process Discussion Owasp Top 10 2017	Top 10 2017 - Call for Data and Weightings Discussion Owasp Top 10 2017	Juice Shop Brainstorming Juice Shop	Mobilising Business Lines for Security CSO
Larch Room-3	SAMM - Kick Off OwaspSAMM	SAMM - V2 Ground Rules OwaspSAMM	SAMM - Conducting Assessments OwaspSAMM	SAMM - Core Model Update 1 - Intro OwaspSAMM
Montague Room-4	MSTG Book Sprint - Mobile Operating Systems Mobile Security	MSTG Book Sprint - Mobile Operating Systems Mobile Security	MSTG Book Sprint - Mobile Operating Systems Mobile Security	MSTG Book Sprint - Mobile Operating Systems Mobile Security
Maulden Room-5		Playbooks Common Format Security Playbooks	Security Playbooks Diagrams Security Playbooks	Playbooks vs Handbooks Security Playbooks
Pedley Room-6		GDPR and DPO AppSec implications CSO	Threat Modeling Tools Threat Model	Threat Modeling Diagramming Techniques Threat Model

Outcomes online

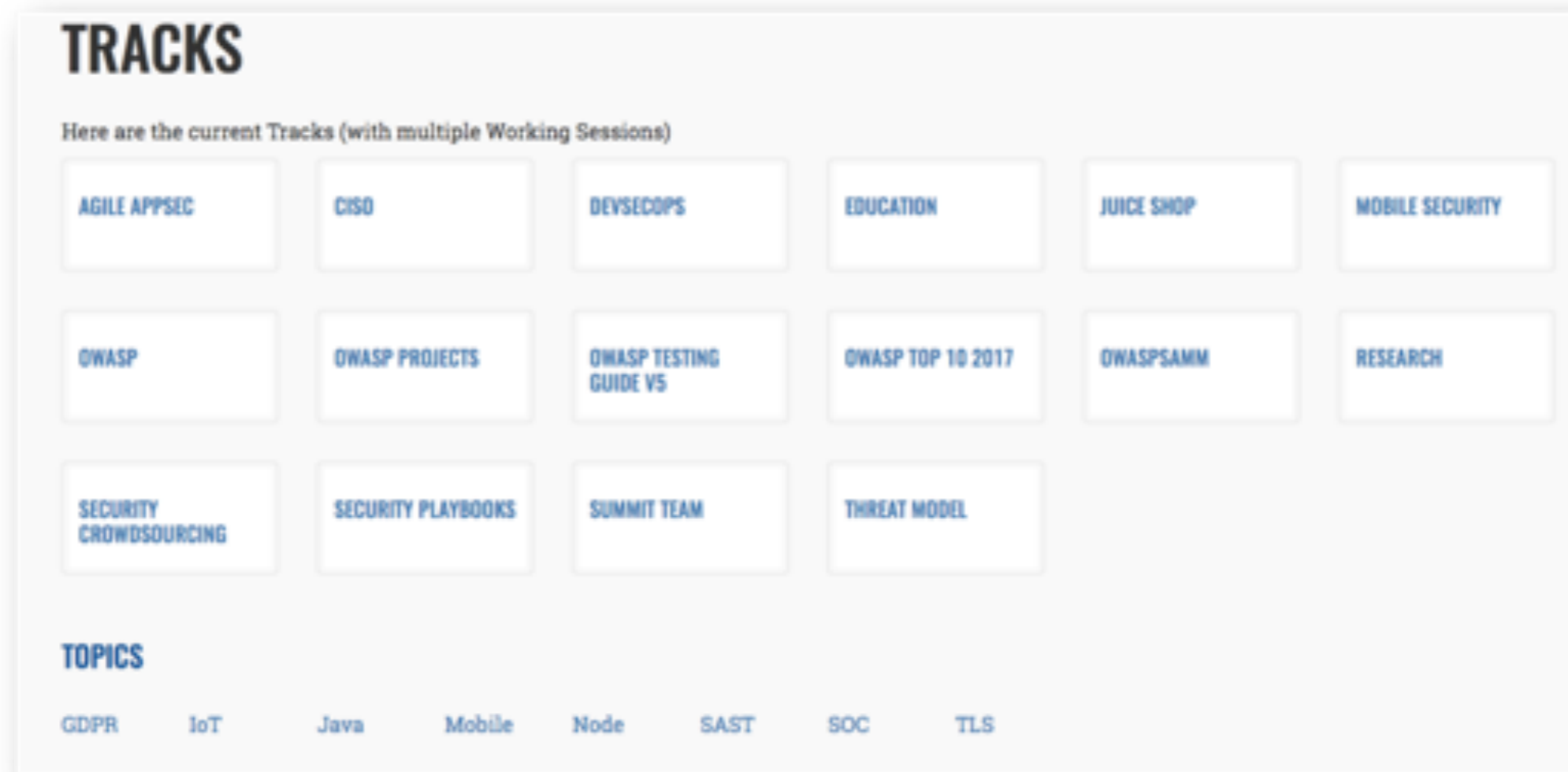
- DRAFT started at <https://owaspsummit.org/Outcomes/>



The screenshot shows a web page titled "SUMMIT OUTCOMES PAGES" with a navigation bar at the top containing "OWASP SUMMIT 2017" and "OUTCOMES TRACKS PARTICIPANT". Below the title, there is a list of "Current Summit Outcomes pages and Logistics pages" including:

- AppSec Review and Pentest Playbook
- Application Security Guide for CISO
- CISO Round Table
- GDPR and DPO AppSec implications
- GitHub letter
- Incident Response Playbook
- InfoSec Warranties and Guarantees
- Juice Shop Update
- Mobile Security Testing Guide
- OWASP Top 10 2017
- Playbooks Common Format
- Security Playbooks Diagrams
- The Future of Privacy

Full agenda

A screenshot of the OWASP Summit 2017 agenda website. The page is titled "TRACKS" and includes a sub-header "Here are the current Tracks (with multiple Working Sessions)". Below this, there are 22 track buttons arranged in three rows. The first row contains: AGILE APPSEC, CISO, DEVSECOPS, EDUCATION, JUICE SHOP, and MOBILE SECURITY. The second row contains: OWASP, OWASP PROJECTS, OWASP TESTING GUIDE V5, OWASP TOP 10 2017, OWASPSAMM, and RESEARCH. The third row contains: SECURITY CROWDSOURCING, SECURITY PLAYBOOKS, SUMMIT TEAM, and THREAT MODEL. At the bottom of the screenshot, there is a "TOPICS" section with buttons for: GDPR, IoT, Java, Mobile, Node, SAST, SOC, and TLS.

173 working sessions in 6 meeting rooms and 10+ villas
208 participants (153 on-site & 55 remote)

“small” selection of outcomes
(in no particular order)

Top 10 2017 – Process Discussion

The history of the Top 10 was covered briefly:

- 2004, no data backing the standard
- 2007, CVE data only was used for analysis; we used our judgement to fit in CSRF as an issue
- 2010 and 2013, the forward-looking issue was out of date components, which on one analysis of the OWASP Top 10 to breach data represents a full 24% of all data breaches.
- Moving forward, it was agreed there should always be room for forward-looking inclusions.

Key takeaways

- Our audience is everyone in AppSec, not just developers
- The basis for the OWASP Top 10 is "risks"
- We will document the rationale for the OWASP Top 10; for 2017, 2020, and 2023
- The Board will be asked to change the Project Leader Handbook, where Flagship projects will have a six-month grace period to obtain at least two leaders from two different firms to avoid perceptions of vendor lock-in, either real or perceived.
- There will be a transparent and documented decision to ensure that up to 2 of the OWASP Top 10 issues will be forward-looking, and that the community should drive the consensus for what they will be.

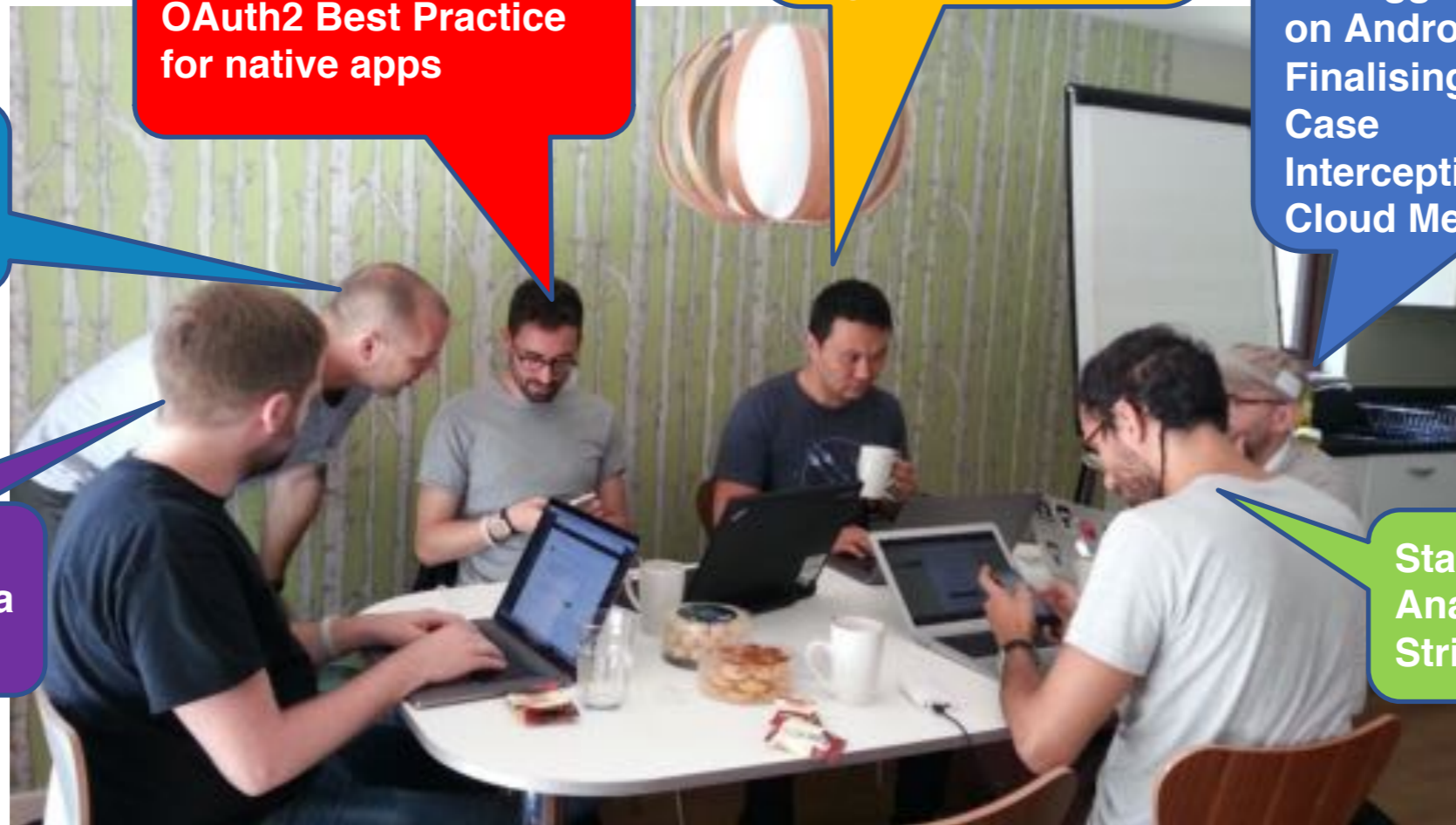
Top 10 2017 – Call for Data and Weightings Discussion

- We want to drive a release, but RC2 will not come out this week, so we will work on collecting more data.

Key takeaways

- Data collection process and timeline will be published on the wiki to ensure sure everyone knows how data is collected and analysed.
- Andrew van der Stock will work on a process with Foundation staff to ensure that we can maximise publicity for the next data call round in 2019.
- A data call extension will be pushed out for interested parties.
- Dave Wichers will reach out to Brian Glas for feedback for tomorrow morning's data weighting session.
- For 2020, we will try to find data scientists to help us to improve our data methodology and analysis.
- Ordering will never be strictly data order; to provide continuity, there is a decision (which will now be documented) that if A1 ... A3 in 2010 are the same in 2017 but in a slightly different order, those will retain a previous order.
- Feedback obtained from the OWASP Top 10 mail list will end up in Git Hub tomorrow as issues.

work in progress



IOS Reverse Engineering

OAuth2 Best Practice for native apps

Cryptographic best practices, algorithms & key strength
Recommends "The Code Book" – Simon Singh for a fun read

Debugging functions on Android
Finalising JWT Test Case
Intercepting Google Cloud Messages

Android file integrity and data integrity

Static & Dynamic Analysis
Verifying Strict Mode

OWASP MOBILE SECURITY TESTING GUIDE UPDATE



- The OWASP Mobile Security Testing Guide (MSTG) was updated at the OWASP Summit 2017.
- The MSTG is a comprehensive manual for mobile app security testing and reverse engineering.
- It describes technical processes for verifying the controls listed in the OWASP Mobile Application Verification Standard (MASVS).
- The current master branch can also be read on Gitbook, as well as leanpub.

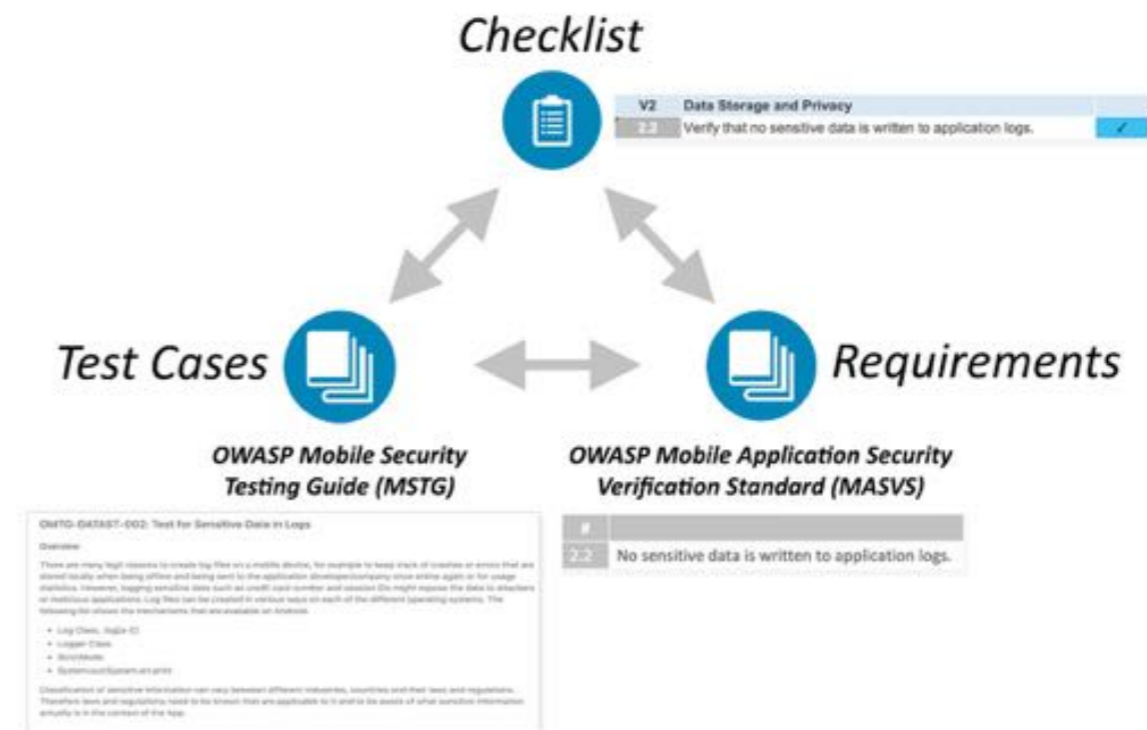
<https://leanpub.com/mobile-security-testing-guide-preview>

Aim of the MST Guide

To produce a comprehensive testing guide to be used during a mobile app security test that enables testers to deliver consistent and complete results.

To include:

- Processes
- Techniques
- Tools
- Exhaustive set of test cases



Content created

Authentication

- Creating best practices for OAUTH2
- JWT – JSON web token authentication for mobile apps
- Having device binding in IOS
- Up to date biometric authentication for android

Cryptography

- Reviewing general cryptography principles
- General & platform specific
- Issues around password storage

General Editing

- Removing any duplications and surplus information
- Writing in easy-to-read English

Define Agile Security Practices

Participants redefined the session goals to discuss security practices for agile development teams, rather than agile practices for security teams.

We noted the following point on the original scope:

- The security team should be a friend that provides help and resources to the dev teams, rather than source of work, blame, and stress.
- For more information, and there is a lot, please see the what we uploaded to GitHub

Agile Practices for Security Teams

We discussed the key activities of an Agile Security Team and agreed on this list



- Education
- Communication
- Standardization and Compliance
- Support
- Governance and control
- Engineering
- Practices

SAMM V2

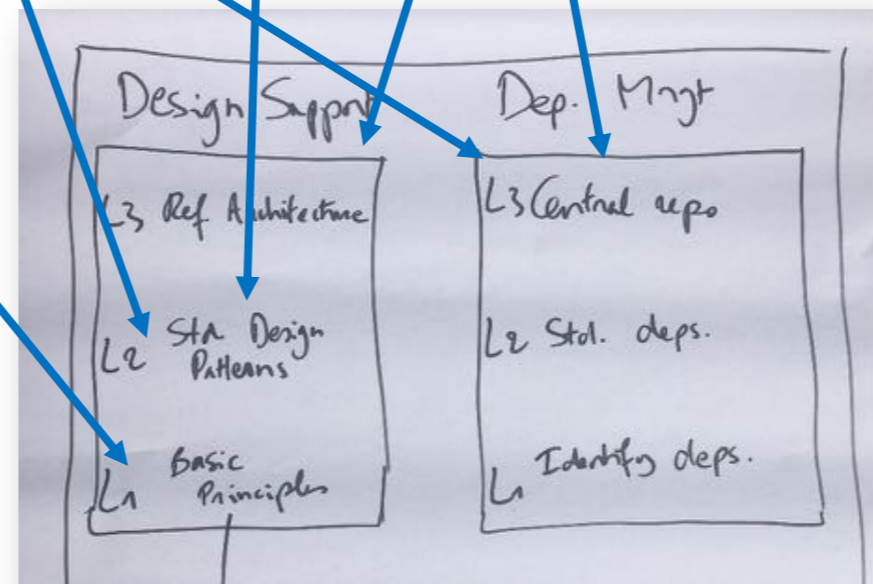
- One Model
- Evolution
- Scope = software
- Experiment with tagging to cover various viewpoints
- Extra working sessions with DevSecOps maturity model
- Keep it simple! Balanced model (desirable)

(when)	Monday	Tuesday	Wednesday	Thursday	Friday
AM-1	SAMM - Kick Off <i>Room-3</i>	SAMM - Introduction to Generic DevOps Security Maturity Model <i>Villa-1</i>	SAMM - Dataset Project <i>Villa-1</i>	SAMM - Core Metrics <i>Villa-1</i>	SAMM - Maturity Models tool <i>Main-Room</i>
PM-1	SAMM - V2 Ground Rules <i>Room-3</i>	SAMM - Core Model Update 2 - Dev Methods <i>Villa-1</i>	SAMM - Core Model Update 3 - Implementation <i>Villa-1</i>		SAMM - After Action Report <i>Room-4</i>
PM-2	SAMM - Conducting Assessments <i>Room-3</i>	SAMM - OWASP Project alignment <i>Villa-1</i>	SAMM - Outreach and Marketing <i>Villa-1</i>		
PM-3	SAMM - Core Model Update 1 - Intro <i>Room-3</i>	SAMM - Stories and Templates <i>Villa-1</i>	SAMM - Standards and Compliance Mapping <i>Villa-1</i>		
Eve		SAMM - Mapping DevOps Maturity Model <i>Villa-1</i>	SAMM - core model placeholder <i>Villa-1</i>		

SAMM Sessions – Core Model Update - Developer Methodology

- Restructure SAMM activities with an increasing maturity of implementation
- Apply this restructure exercise to all SAMM practises and activities (high level).
- Create one or more detailed descriptions with implementation guidance.

Secure Architecture ...more on page 44			
	SA 1	SA 2	SA 3
OBJECTIVE	Invert consideration of proactive security guidance into the software design process.	Direct the software design process toward known-secure services and secure-by-default designs.	Formally control the software design process and validate utilization of secure components.
ACTIVITIES	A. Maintain list of recommended software frameworks B. Explicitly apply security principles to design	A. Identify and promote security services and infrastructure B. Identify security design patterns from architecture	 A. Establish formal reference architectures and platforms B. Validate usage of frameworks, patterns, and platforms



Implementation Review

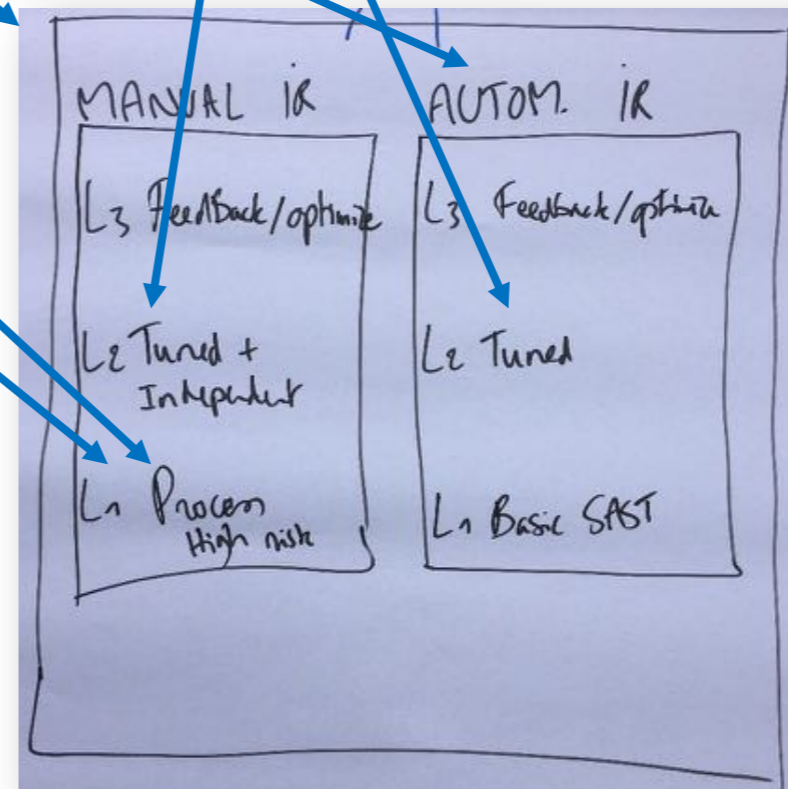
...more on page 12

✓ IR 1

✓ IR 2

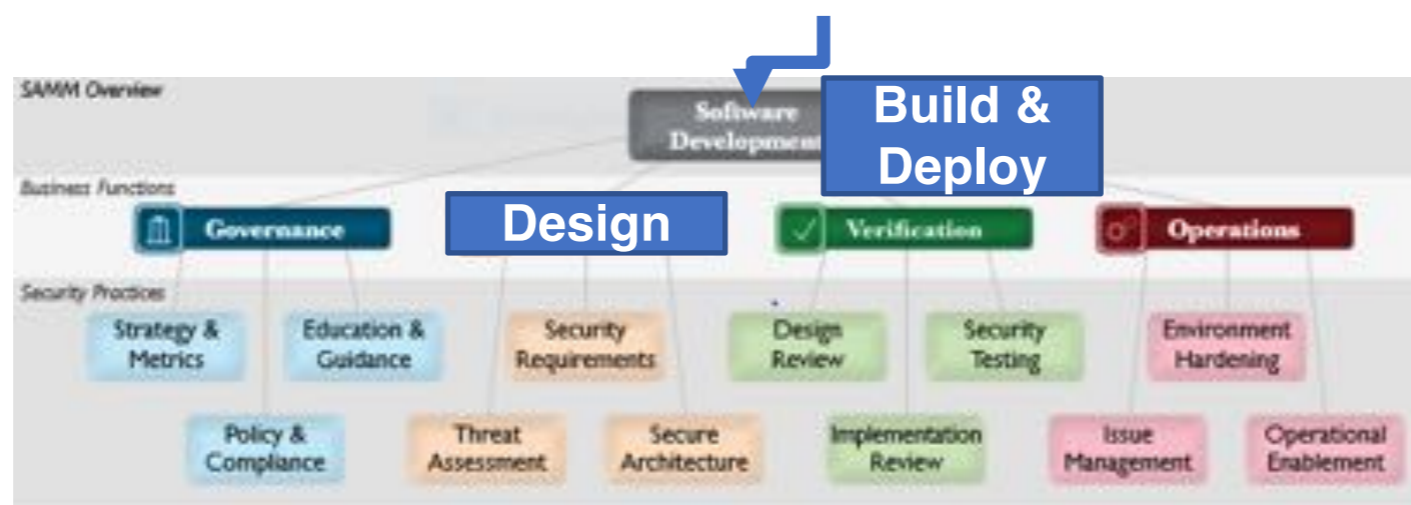
✓ IR 3

	IR 1	IR 2	IR 3
OBJECTIVE	Opportunistically find basic code-level vulnerabilities and other high-risk security issues.	Make implementation review during development more accurate and efficient through automation.	Mandate comprehensive implementation review process to discover language-level and application-specific risks.
ACTIVITIES	A. Create review checklists from known security requirements B. Perform point-review of high-risk code	A. Utilize automated code analysis tools B. Integrate code analysis into development process	A. Customize code analysis for application-specific concerns B. Establish release gates for code review



SAMM Sessions – Core Model Implementation

- Explore adding a fifth business function to the SAMM Model
 - Missing activities for secure build
 - Operations does not cater for deployment
 - Issue management is not covering defect management



SAMM Sessions – Defect management

Defect Tracking

L3: Full integration with risk management + feedback loop to other activities

L2: Integrate with existing defect tracking system + SLA

L1: Triage Defects

Confirm, severity, priority, assignments

Vulnerability Tracking

L3: Integrate with SOC + self-protection

L2: Disclosure process + integration with tracking system + SLA

L1: Vulnerability tracking + response plan

Recruiting AppSec Talent

- We discussed the gap between companies' needs to recruit talented AppSec people, and attracting the best AppSec people to come work at their company.
- The Joel Test is a quick indicator of Development culture: an irresponsible, sloppy test to rate the quality of a software team.
- We have adapted the Joel Test to quickly indicate a company's AppSec culture.
- The test's purpose is to help companies attract the right talent and help talent to find the right company



First draft of the AppSec Joel Test (in no specific order):

1. Does the company fund ongoing education for AppSec hires?
2. Do developers undergo periodic AppSec training?
3. Do AppSec people have quiet working environment?
4. Are there both offense and defense teams, and do they work together?
5. Can the AppSec team delay release (or fix) a new version or product?
6. Is the AppSec team involved throughout the development lifecycle process?
7. Can I access developers directly?
8. Are security bugs treated like functional bugs?
9. Is there some form of SDL / Maturity model / or other process in place?
10. Can AppSec people choose their own tools (paid for by the company)?
11. Is there a dedicated Incident Response team?
12. Does the company contribute to Open Source and community efforts (or support personal contributions)?

Creating AppSec Talent (next 100K Professionals)

Goal: Bridge the hiring gap in AppSec focusing on

- Bringing in new entrants, and those in the mid-career phase

Main Outcomes

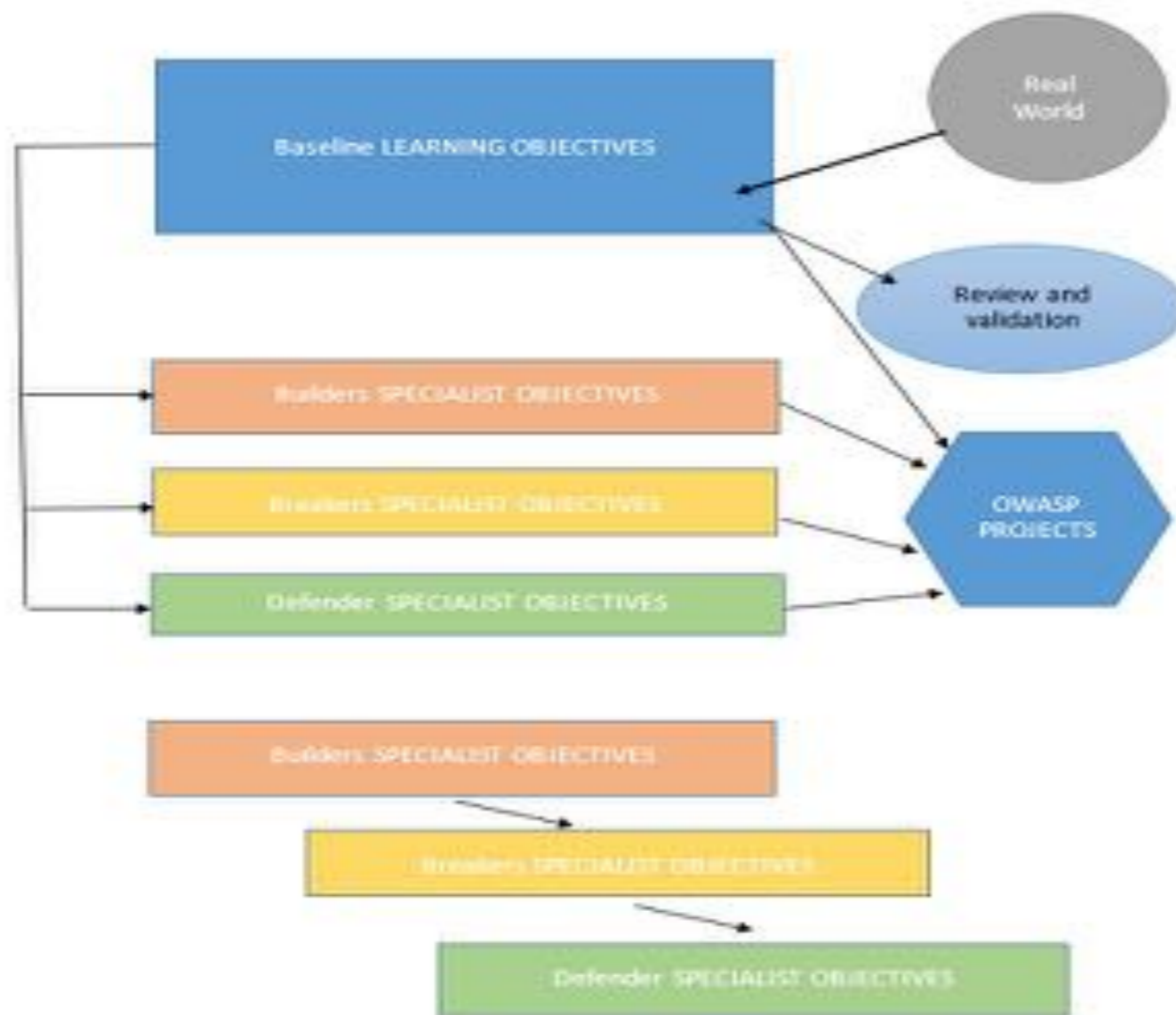
- Education as a Path
- Educate Managers & Directors (Board Level)
- Develop the Security Culture
 - Make reciprocal agreements with other professional bodies (piggy back joint ventures)
 - Use industrial regulator or other standards
 - Market these resources aggressively
- Diversify Language
 - Git Plugin for Internationalisation
- Design Targeted Accessible Resource Sheets (Reference “A Quick Developers Guide for OWASP Projects” Infographic)
 - How to get Management on Board?
 - AppSec for Developers
 - Resource Menu for Educator’s (Primary -> Tertiary)
 - How to transition from other careers

Application Security BSc/Masters Curriculum Design

Outcomes

- A wider Strategy than BSC/MSc, that Combines OWASP strategic strengths
- Agreement that there is not enough APPSEC, in educational curriculums
- Prioritise/Rank learning objectives.
- Creation of an Educational Diagram
- Completion of an exit survey

Application Security BSc/Masters Curriculum Design (Diagrams)



Application Security Guide for CISO 1/3

Outcome 1 (unranked) – What topics would you like covered in the new CISO guide?

- **Incorporate reference to outcomes of 2017 Summit CISO track**
- **Expand to include new tools/technologies**
- **Expand to include compliance with GDPR**
- **Expand on new emerging technology risks** and provide risk Mitigation Guidance (e.g. APIs, proliferation, and Micro-services/interoperability, Biometrics, Cloud (internal and external), strategies for managing risk in Cloud environments)
- **Expand on Risk Management Strategies** For Vendors, Provisioning, Supply-Chain Risks
- **Expand on new evolving threats facing web Applications** (e.g. 0-day exploits)
- **Add reference to handbooks and playbooks** for CISO's managed process
- **Where to provide guidance** or where to put a focus, e.g., 5,000 applications in different countries, where to allocate security resources in such a situation
- **How to get visibility across the organisation** – who is doing what. As CISO you need to know what changes are being made, and where

Application Security Guide for CISO 2/3

Outcome 1 (unranked) – What topics would you like covered in the new CISO guide?

- **Corporate culture:** how can a CISO be an agent of change and overcome cultural challenges? Knowing the corporate culture to enable CISO to function properly; trust is crucial to success
 - **Success stories** as examples of how to win – people can refer to these as a value-add – how can the CISO provide value to the business
 - **Knowing the right questions** to ask triggers the appropriate response and action
 - **A proactive**, strategic CISO is better than a reactive one: knowing to shift focus from fighting fires to ensuring the fires do not get out of control
- **After an incident**, think about how to promote change; train people to think holistically not just about the incident, but about the impact of the incident
 - **Involvement** CISO should be involved in road mapping for future deployment and included in business development meeting so CISO can plan ahead
 - **Format:** It was agreed that a handbook would have more value than a playbook given threat variables between company requirements

Application Security Guide for CISO 3/3

Outcome 2 (unranked) – What type of question would you like included in the new CISO guide?

- **Which among the organization IT assets, networks or applications are considered more at risk of cyber-attacks ?**
- **Does your organization have a cyber-threat intelligence program and attack monitoring/alert process ?**
- **Does your organization has adopted S-SDLC? If yes which one. Does it include threat modeling ?**
- **Is application security seen as an investment or as a cost by your organization ?**
- **Does your planning of application security follow a long term strategy (at least two years) ?**
- **Need to ask questions** about how to map the scope, application, and business process perspectives
- **How to manage risk** from third parties, private vs. public premise
- **How do you manage the risk** for developing technologies, such as the Cloud?

Securing GitHub Integration

Roles

- Users (repo owners): want to **allow** access only to what's necessary, not full access
- Integrators (Oauth apps): only want to **ask** for access to necessary resources, not full access
- Administrators: want a rich audit trail

What's needed

- A more granular access control:
 - Be able to select what repositories can be accessed (currently it's all or nothing)
 - Allow read-only access to a repo (currently it's read/write or nothing)
 - Setup `commit status webhook` without asking for `write` access to the repo
- Better Audit trail:
 - Organization wide audit trail (Github Online)
 - Better visibility into the activity of users (Github Enterprise)



Outcome

- We drafted a letter so we can reach out to GitHub with a request for comment, and to start a dialogue

Threat Modelling sessions

- Series of Hands on Threat Modelling Juice Shop :
 - Architecture, Deployment & Operation, New features, Purchase workflow
 - Attacking & Fixing
- Threat Modeling OWASP Pages revamp
- Threat Modeling Templates
- Threat Modeling IoT Devices
- Threat Modeling Diagramming Techniques
- New slogan: **The Sooner The Better, Never Too Late!**

Threat Modelling Cheat Sheet & Lightweight Threat Modelling

- The process has three activities
 - Ascertain
 - Threats
 - Mitigations
- Ascertain – Define the underlying structure using Agile User Stories.
- Threats – Apply OWASP Threat Templates to the structure.
- Mitigations – Apply OWASP Countermeasures to relevant threats.

WebGoat – 1/2

- **Add lessons not found in other Goat like applications e.g. SSRF**
- **Discussion about sharing content between Goat like applications such as WebGoat, NodeGoat, etc.**
- **Flexibility when presenting in lessons**
- **Language support discussion and agreed on supporting one language and focus on other features first**
- **How to integrate automated vulnerability checking into WebGoat**
- **Fixing a lesson should be added so developers can fix as well as break**

WebGoat – 2/2

New lesson ideas

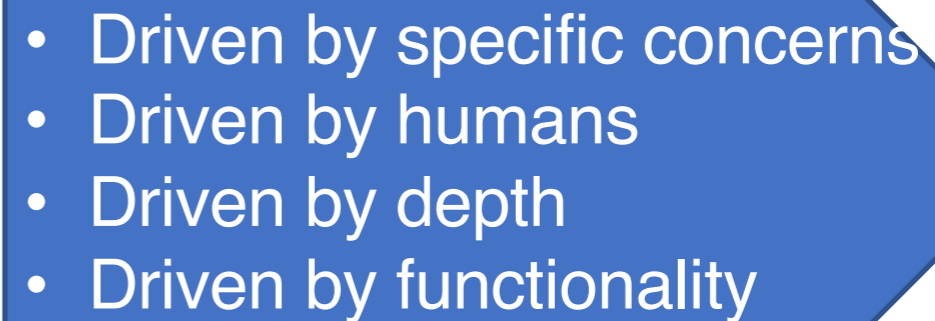
- **Upload functionality**
- **Path traversal with shell upload**
- **Crypto**
- **Focus on HTML5**
- **JSON Injection**
- **Business logic**
 - **For example, after payment of an order repeat the request and keep ordering the TVs without paying.**

OWASP Playbooks Series

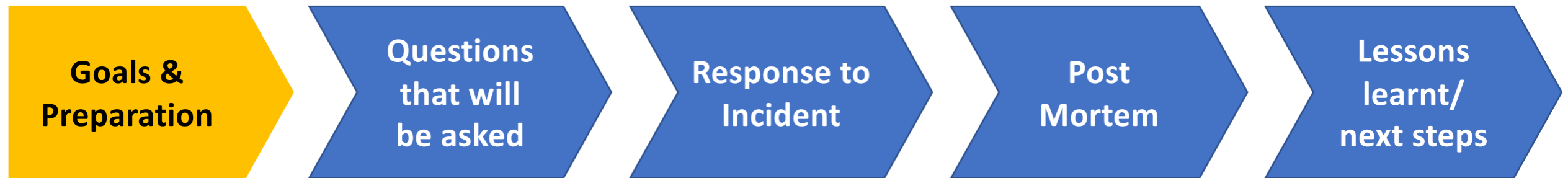
- actionable, consistent process for getting started with various application security scenarios
- Templates creates
- First series started
 - AppSec Review and Pentest Playbook
 - Bug Bounty Playbook
 - Playbooks Common Format
 - Incident Response Playbook
 - DoS Playbook
 - Security Playbooks Diagrams
 - Media Handling Playbook
 - Due Diligence Playbook
 - Ransomware Playbook
 - Playbooks vs Handbooks
 - Security Monitoring Playbooks

AppSec Review and Pentest Playbook Outcomes

- ❑ Eleven participants collaborated on what defines an Application Security Pen Test:
- ❑ Created outline for a AppSec Pen Test Playbook
 - ✓ Initial draft of outline sent to participants for consensus

- 
- Driven by specific concerns
 - Driven by humans
 - Driven by depth
 - Driven by functionality

Incident Response Playbook



Goals & Preparation

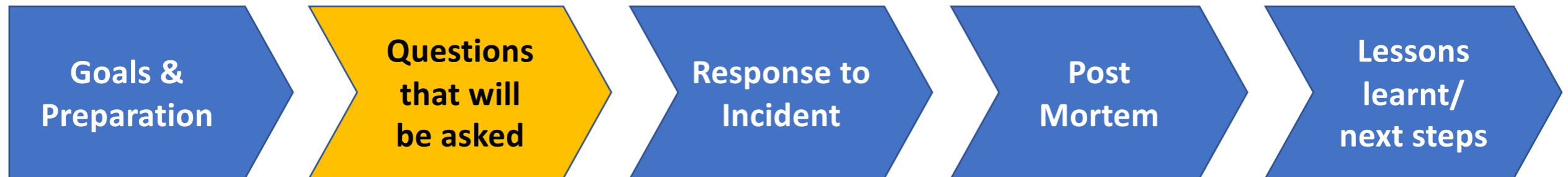
Goals

- IR from a developer's perspective
- Don't cover entire IR field, just developer's roles and responsibilities
- Reinforce how other best practices, such as threat models, support the IR process.

Preparation

- Conduct fire drill – consider tabletop exercises
- Assign points of contact (e.g. Security Champions)
- Rapid deployment plan
- Logging

Incident Response Playbook



- Is it our data?
- Is it a breach?
- What app/service provides the data?
- Where did data come from?
- Can the data be time stamped?
- What does it mean?
- Does it have value?
- Can we roll back to last known 'good' state?

Incident Response Playbook



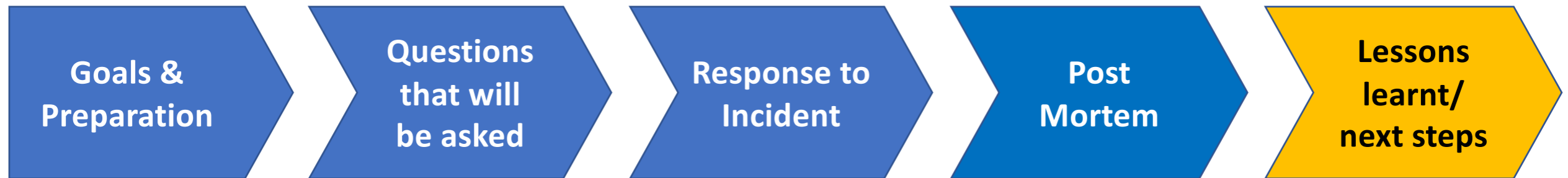
- **Rapid deployment, owners have to know their roles**
- **Communication – keep people updated with minimal publicity**
- **Log what happens, and when, so people coming in as the crisis develops can be brought up to speed quickly**
- **Stagger engineering team so that 24/7 coverage is possible (people need to rest, eat, etc.)**
- **The benefit of a situation dealt with quickly and efficiently outweigh the cost of the remedy and the cost to the business**

Incident Response Playbook



- **Did the threat model cover this?**
- **Bug Bounty the target?**
- **Why it happened?**
- **How did we react?**
- **Was best practice followed?**
- **If not, why not?**
- **Tuning web application firewalls**

Incident Response Playbook



- **How many pre-requisites were satisfied**
- **Was Playbook appropriate?**
- **Variables will cause gaps in PB**
- **What adjustments need to be made**

- **We feel that a Preparation Guide could satisfy needs in this area, perhaps building on Tom Brennan's OWASP Incident Response Project**

OWASP Testing Guide v5

Tasks completed

- Brainstorming regarding the new activities to perform to improve the guide
- Alignment with OWASP guides: Development Guide, Code Review Guide, ASVS, Top10, Testing Checklist, ZAP, Vulnerability list
- Discussion on tools
- Add the list of new tests to the v5



Outcomes

New Tests to Write

- Server-Side Request Forgery (SSRF)
- Server-side Remote Code Execution (RCE)
- XML External Entity Attacks (XXE)
- Self Based DOM XSS
- Authorization bypass horizontal
- Authorization bypass vertical
- Server-Side Template Injection (SSTI)
- Host Header Attack
- SPARQL Injection
- Testing for Deserialization of untrusted data
- API Abuse
- Testing Content Security Policy V2 (CSP)?
- Testing for SSO?

OWASP Testing Guide v5

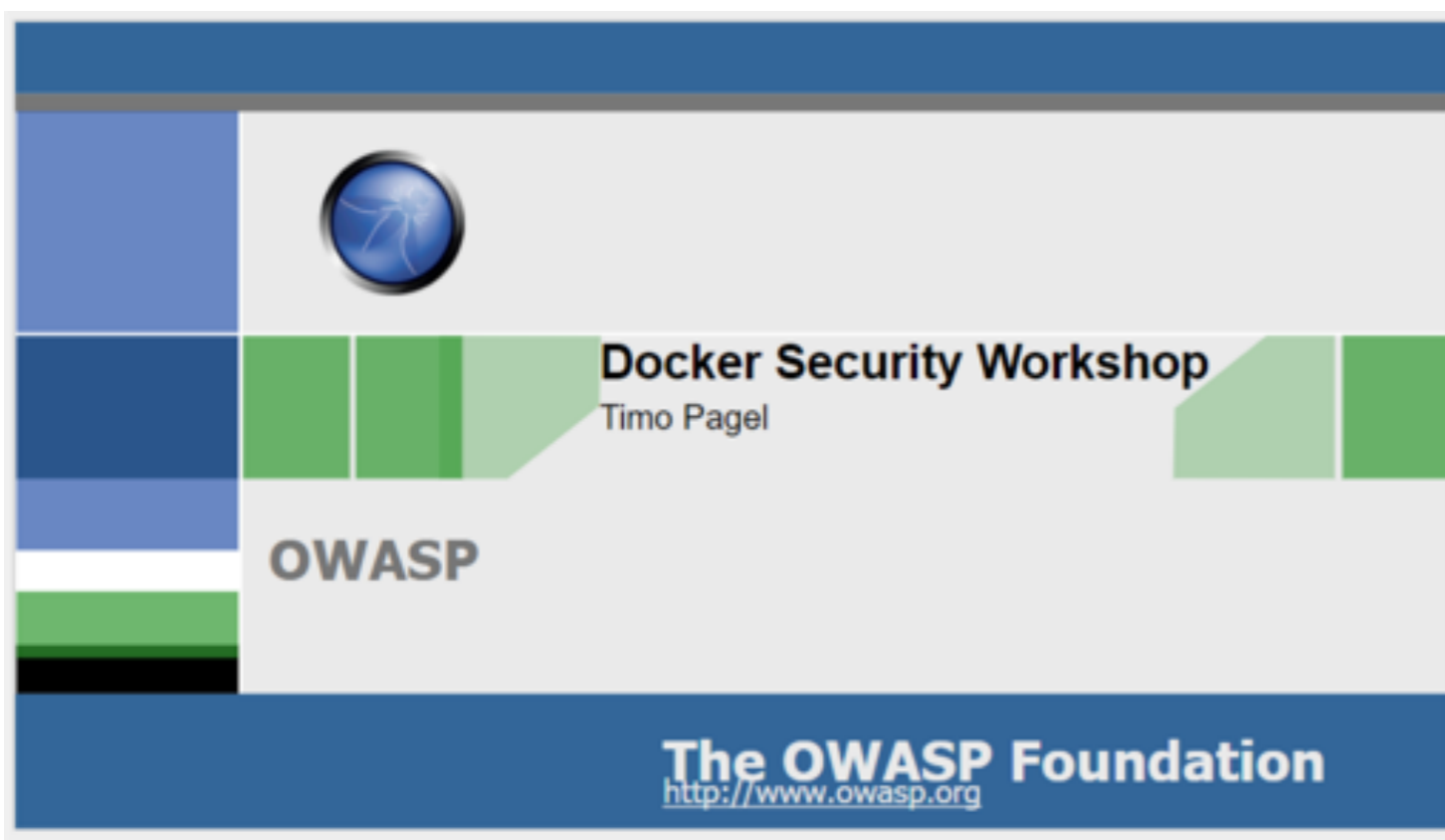
Review

- Client Side Testing
- ORM Injection
- Authorization Testing
- Information and Config management testing
- Authentication Testing: add oauth testing
- Reporting: adding how to create security testing case for devs
- [https://www.owasp.org/index.php/Test_Local_Storage_\(OTG-CLIENT-012\)](https://www.owasp.org/index.php/Test_Local_Storage_(OTG-CLIENT-012)) add Client Side SQLi



The screenshot shows a web browser displaying an article on the OWASP website. The article title is "Test Local Storage (OTG-CLIENT-012)". The page includes a navigation menu on the left with links like Home, About OWASP, and Downloads. The main content area contains a notice that the article is part of the new OWASP Testing Guide v4, with links to the v4 Table of Contents and the OWASP Testing Project. Below this is a table of contents for the article, listing sections like Summary, How to Test, Tools, and References. The article text begins with a definition of Local Storage, also known as Web Storage or Offline Storage, as a mechanism to store data as key/value pairs tied to a domain.

Review of Docker Security Workshop



<https://github.com/wurstbrot/docker-security-workshop>

Outcome

- Audience: Users of Docker
- Modification/Simplifying of slides
- Remove complicated slides
- Correction of (some) translation issues
- Enhancement of documentation
- Outlook:
- Example for Clair to scan local images

OWASP-CDC

- Owasp Collective Defence Cluster
- Triggered for the first time 8-June!!!!
 - Slack Channel Created
 - Connections made help to clarify situation
- Already a success story
- If you happen to need it, please don't hesitate to trigger it (even before formal agreement)



OWASP Collective Defence Cluster

Press Release

On day x, company X was hit by a cyber security incident which severely affected the security of its web platform.

After identifying the scope of the incident, company x realised it lacked the internal resources, defence mechanisms, and expertise to handle the security workload, and this would affect the speed of its response to a sophisticated, malicious attack.

Company X triggered the OWASP Collective Defence Cluster (CDC), which allowed it to access the resources shared by the participating companies.

The on-call Security Champions and SoC (Security Operations Centre) members activated the Collective Incident Response PlayBook, which described the activities and sequence of events of the incident.



Numerous project reboots / started

- Owasp Orizon Reboot (SAST tool for Owasp)
- Threat Modeling
- OWASP CDC
- ...

OWASP Summit 2018



Join us again next year!!!!

Summit dates **23-27 of April 2018**

Same venue, same team, more focus, better preparation

<https://owaspsummit.org/>

[@OWASPSummit](https://twitter.com/OWASPSummit)