OWASP Summit 2017 Debrief
The #OWASPSummit has spoiled me for other cons: 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

Retweets Likes
7 6

10:00 AM - 19 Jun 2017

https://www.continuumsecurity.net/owasp-summit-exceeded-expectations/
Welcome to OWASP Summit 2017!

12-16 June 2017
Woburn Forest Center Parcs

#OWASPSummit
Let’s start with a question
Who are we?
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
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
JOIN THE CONVERSATION
#OWASPSummit

SPONSORED BY
- OWASP Foundation
- OWASPSAMM project
- OWASP London Chapter
- OWASP Denver Chapter
- OWASP Belgium Chapter
- OWASP Netherlands Chapter
- OWASP German Chapter
- OWASP Luxembourg Chapter
- DevSecCon
- TOREON
- Barracuda
- CapitalOne
- photobox
- VERACODE
- Xebia Security
- OWASP Foundation
- New York City Chapter
### Monday’s Schedule

<table>
<thead>
<tr>
<th>Location</th>
<th>AM 1 (10:30 to 12:30)</th>
<th>PM 1 (13:30 to 15:00)</th>
<th>PM 2 (15:30 to 16:40)</th>
<th>PM 3 (16:30 to 17:30)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kings</td>
<td>TLS for Local IoT</td>
<td>Security Guild vs Security Champions</td>
<td>OWASP Internet of Things Project</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DevSecOps</td>
<td>DevSecOps</td>
<td>Owasp Projects</td>
<td></td>
</tr>
<tr>
<td>Portland</td>
<td>Top 10 2017 - Process Discussion</td>
<td>Top 10 2017 - Call for Data and Weightings Discussion</td>
<td>Juice Shop Brainstorming</td>
<td>Mobilising Business Lines for Security</td>
</tr>
<tr>
<td>Room 2</td>
<td>Owasp Top 10 2017</td>
<td>Owasp Top 10 2017</td>
<td>Juice Shop</td>
<td>CISO</td>
</tr>
<tr>
<td>Larch</td>
<td>SAMM - Kick Off</td>
<td>SAMM - V2 Ground Rules</td>
<td>SAMM - Conducting Assessments</td>
<td>SAMM - Core Model Update 1 - Intro</td>
</tr>
<tr>
<td>Room 3</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
</tr>
<tr>
<td>Room 4</td>
<td>Mobile Security</td>
<td>Mobile Security</td>
<td>Mobile Security</td>
<td>Mobile Security</td>
</tr>
<tr>
<td>Maulden</td>
<td>Playbooks Common Format</td>
<td>Security Playbooks Diagrams</td>
<td>Security Playbooks Diagrams</td>
<td>Security Playbooks Diagrams</td>
</tr>
<tr>
<td>Room 5</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
</tr>
<tr>
<td>Pedley</td>
<td>GDPR and DPO AppSec implications</td>
<td>Threat Modeling Tools</td>
<td>Threat Modeling Diagramming Techniques</td>
<td>Threat Modeling Diagramming Techniques</td>
</tr>
<tr>
<td>Room 6</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
<td>OwaspSAMM</td>
</tr>
</tbody>
</table>
Outcomes online

• DRAFT started at https://owaspsummit.org/Outcomes/
Full agenda

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 a 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

- Debugging functions on Android
- Finalising JWT Test Case
- Intercepting Google Cloud Messages
- Cryptographic best practices, algorithms & key strength
- Recommends “The Code Book” – Simon Singh for a fun read
- OAuth2 Best Practice for native apps
- IOS Reverse Engineering
- Android file integrity and data integrity
- Static & Dynamic Analysis Verifying Strict Mode
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.
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

<table>
<thead>
<tr>
<th><strong>Authentication</strong></th>
<th><strong>Cryptography</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creating best practices for OAUTH2</td>
<td>• Reviewing general cryptography principles</td>
</tr>
<tr>
<td>• JWT – JSON web token authentication for mobile apps</td>
<td>• General &amp; platform specific</td>
</tr>
<tr>
<td>• Having device binding in IOS</td>
<td>• Issues around password storage</td>
</tr>
<tr>
<td>• Up to date biometric authentication for android</td>
<td></td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th>AM-1</th>
<th>SAMM - Kick Off</th>
<th>SAMM - Introduction to Generic DevOps Security</th>
<th>SAMM - Dataset Project</th>
<th>SAMM - Maturity Models tool</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Room-3</td>
<td>Maturity Model</td>
<td>Villa-I</td>
<td>Main-Room</td>
</tr>
<tr>
<td>PM-1</td>
<td>SAMM - V2 Ground Rules</td>
<td>SAMM - Core Model Update 2 - Dev Methods</td>
<td>SAMM - Core Model Update 3 - Implementation</td>
<td>SAMM - After Action Report</td>
</tr>
<tr>
<td></td>
<td>Room-3</td>
<td>Villa-I</td>
<td>Villa-I</td>
<td>Room-4</td>
</tr>
<tr>
<td>PM-2</td>
<td>SAMM - Conducting Assessments</td>
<td>SAMM - OWASP Project alignment</td>
<td>SAMM - Outreach and Marketing</td>
<td>Villa-I</td>
</tr>
<tr>
<td></td>
<td>Room-3</td>
<td>Villa-I</td>
<td>Villa-I</td>
<td></td>
</tr>
<tr>
<td>PM-3</td>
<td>SAMM - Core Model Update 1 - Intro</td>
<td>SAMM - Stories and Templates</td>
<td>SAMM - Standards and Compliance Mapping</td>
<td>Villa-I</td>
</tr>
<tr>
<td></td>
<td>Room-3</td>
<td>Villa-I</td>
<td>Villa-I</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>SAMM - Mapping DevOps Maturity Model</td>
<td>Villa-I</td>
<td>SAMM - core model placeholder</td>
<td>Villa-I</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Objective</th>
<th>SA 1</th>
<th>SA 2</th>
<th>SA 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert consideration of proactive security guidance into the software design process.</td>
<td>Direct the software development process toward known-secure services and secure-by-default design.</td>
<td>Formally control the software development process and validate utilization of secure components.</td>
<td></td>
</tr>
</tbody>
</table>

### Activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>SA 1</th>
<th>SA 2</th>
<th>SA 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Maintain list of recommended software frameworks</td>
<td>A. Identify and promote security services and infrastructure</td>
<td>A. Establish formal reference architectures and platforms</td>
<td></td>
</tr>
<tr>
<td>B. Explicitly apply security principles to design</td>
<td>B. Identify security design patterns from architecture</td>
<td>B. Validate design of frameworks, patterns, and platforms</td>
<td></td>
</tr>
</tbody>
</table>

---

### Design Support

- L3: Ref. Architecture
- L2: STA Design Patterns
- L1: Basic Principles

### Dev. Mgmt

- L3: Central WOP
- L2: Std. dep.:
- L1: Identify dep.
<table>
<thead>
<tr>
<th>Objective</th>
<th>IR 1</th>
<th>IR 2</th>
<th>IR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunistically find basic code-level vulnerabilities and other high-risk security issues.</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Make implementation review during development more accurate and efficient through automation.</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Mandate comprehensive implementation review process to discover language-level and application-specific risks.</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activities</th>
<th>IR 1</th>
<th>IR 2</th>
<th>IR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Create review checklists from known security requirements</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Perform point-review of high-risk code</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>A. Utilize automated code analysis tools</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>B. Integrate code analysis into development process</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>A. Customize code analysis for application-specific concerns</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Establish policies for use</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MANUAL IR**
- L5 Feedback/optimization
- L3 Tuned + Independed
- L2 Process High risk

**AUTOM IR**
- L5 Feedback/optimization
- L3 Tuned
- L2 Basic SAST
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

L1: Triage Defects
Confirm, severity, priority, assignments

L2: Integrate with existing defect tracking system + SLA

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

Vulnerability Tracking

L1: Vulnerability tracking + response plan

L2: Disclosure process + integration with tracking system + SLA

L3: Integrate with SOC + self-protection
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 Microservices/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
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
• 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

Goals & Preparation

Questions that will be asked

- 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?

Response to Incident

Post Mortem

Lessons learnt/next steps
Incident Response Playbook

Goals & Preparation

Questions that will be asked

Response to Incident

Post Mortem

Lessons learnt/next steps

- 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.
Tasks completed

• Brainstorming regarding the new activities to perform to improve the guide
• 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?
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) add Client Side SQLi
Review of 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

https://github.com/wurstbrot/docker-security-workshop
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)
Numerous project reboots / started

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

Join us again next year!!!!

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

Same venue, same team, more focus, better preparation

https://owaspsummit.org/

@OWASPSummit