OWASP Summit 2011

Industry Committee Working Session

Wednesday 9th February 2011

These notes completed on 22nd February 2011

The top three accomplishments of this working session were:

1. A refocus by the Industry Committee on engaging with different market vertical sectors, to listen, and to make OWASP more relevant
2. Realization that the Industry Committee, not the board nor anyone else, needs to take hold of this targeted approach
3. Pledges from at least four leaders outside the US/EU to become new members of the Industry Committee

Thank you to the working session participants especially representatives from government and businesses, and to Joe Bernik, Tom Brennan, Eoin Keary, and Colin Watson for leading the session.

Industry Committee Working Session Outputs

During the working session

1. Listen to industry

The Industry Committee will undertake greater efforts to listen to industry. In order to solicit information in a suitable environment, the concept of face-to-face industry forums will be progressed.

One such event will be a meeting with a small group of influential leaders from the financial services sector, possibly arranged for during AppSec EU2011 (Dublin) in June.

Other sectors to be targeted are healthcare, and government.

2. Industry survey

The committee will proceed with its efforts to seek feedback from industry more widely (but not security consultants or vendors) using a questionnaire in association with ISC2.

The survey needs final review, building into an online system, testing and then promotion to target groups. It may be useful to have some incentive for completion of the survey.

Immediately subsequent to the summit

3. New committee members

Jerry Hoff, Mauro Flores , Mateo Martinez, Sherif Koussa and Nishi Kumar have submitted fully-complete applications to become members of the Industry Committee.

http://www.owasp.org/index.php/Global_Industry_Committee_-_Application_11

http://www.owasp.org/index.php/Global_Industry_Committee_-_Application_8

http://www.owasp.org/index.php/Global_Industry_Committee_-_Application_9

http://www.owasp.org/index.php/Global_Industry_Committee_-_Application_10

http://www.owasp.org/index.php/Global_Industry_Committee_-_Application_6

These are awaiting final verification by OWASP.

Michael Scovetta and Tony Ucedavelez may also be seeking to become committee members.

4. Appointment of chair

Joe Bernik was appointed chair of the GIC on 18th February 2011, following a unanimous vote by all members of the committee. This has ended uncertainty in the leadership of the committee, and allows it to move forward.

5. Committee restart

The Industry Committee is set for its refocus and reinvigoration under its new chair, with a conference call being held on Friday 25th February at 18:00 GMT – details are shown on the GIC page of the OWASP wiki: http://www.owasp.org/index.php/Global_Industry_Committee

Industry Committee Working Session Notes

Notes were taken at the meeting by Sarah Baso and are attached below.

Meeting Minutes from GIC Working Session

Date/Time: 09 February, 2011 (14:00 – 15:20)

Location: Alentejo Room at Global Summit

Meeting Chairs: Joe Bernik & Eoin Keary

GIC Status Update: Where are we now? (Eoin Keary)

- Goals for GIC – make Industry/OWASP more relevant, set agenda
- Problem – listen to the industry instead of ourselves (OWASP)
- Recently – we have been commenting on white papers and position papers
- Don' t have a chair. Chair (YP) resigned a couple of days ago due to personal reasons.
- Industry survey with ISC2
- Questioning relevance of OWASP tools in industry and appsec in general, how can we be more effective?
- GIC Mission? Listening to industry

Short presentation by Joe Bernik: FS-ISAC Overview for OWASP (slides)

- Financial Services – information sharing and assurances center
- Historically very secretive
- Background on organization
- Membership growth – corporate membership $25-50,000 almost 5000 members (lots of corporate growth). Don't meet very much… not as serious meetings (more social opportunity)
- The Challenge – Online Fraud, under UCC customer is responsible. Cyber Crime Growth at Exponential Rates (10 billion projected loss…)
- Who are the criminals? Ukrainian kids with root kits, members of organized crime
- Account Takeover Attacks – steps for a user
- FCISAC Taskforce – unprecedented bank collaboration! (Can we learn from them?)
- How can we (OWASP) help/participate?
    A. Build a cool fuzzing tool
    B. Review some source code

C. Write an open email to a list

D. Develop an open framework for capturing and analyzing application and session data in order to isolate criminal behaviors.

Ideas/discussion points on proactive strategies and solutions to make GIC more relevant:

- NB Trustwave promo literature has a list of solutions
- Industry "board" or consultations – non OWASP members willing to contribute their thoughts/experience/suggestions
- Bounty for good solutions, $10k for solution to x,y,z
- Training at companies. Company pays for travel (not normal thousands of dollars for salary)
- Need to go in house and promo stuff!
- Industry Forum -- identified people to meet up (maybe not "open") Need to find a way to learn about and address issues of industry in a meaningful way. Some people just won't talk about this in an "open" environment. Possibly could have 3 informal behind closed door sessions (Europe, US, and Asia) – try to listen, and see where we are at!
- Need new members to join GIC, particularly from new areas of the world – now Europe/US heavy
- Question: What is "Industry"? Answer: Industry includes people that run organizations
- Question: What is the difference between OWASP and other groups (like ISSA)? Answer: OWASP makes stuff, ISSA – doesn't do this…. [No conclusion reached by group on this point]
- Problem – companies don't want OWASP software – currently OWASP does not provide support, also don't want open source, volunteer written (there is no place to put the blame if something goes wrong)
- GIC needs to build awareness, reach out to power players – training, not code
- Toastmasters for Security… we need a way to socially engineer these situations. Many companies will be crazy not to at least consider code written by big players at companies like Mozilla, Google, etc.
- So – do we continue to build tools, or do we take a different direction and listen to what the industry needs are?
- Need to set up OWASP for Banks, OWASP for Government, OWASP for healthcare, etc. to address and specifically target the different industries

Discussion of NDA – pros/cons (Tom Brennan)

- Problem - Only 7 people in OWASP can sign NDA
- Too hard to get all people in room to agree to NDA
- Companies/banks will really hesitate to consider working with OWASP without NDA
- OWASP policy: do not sign NDA

Current GIC initiative: Industry Survey (Colin Watson)

- Not for consultants, for people in the industry (done with ISC2)
- Use networking to ask people to fill out survey
- Do we need to provide an incentive for answering?
- Contact Colin Watson with questions

Note – There is an existing presentation on what the industry committee is, contact Colin Watson