GIC Meeting Minutes
Friday March 3, 2011 (17:00 -18:00 GMT)

Present:
Joe Bernik (Chair), Sarah Baso (Secretary), Colin Watson, Kate Hartmann, Mauro Flores, Tony UcedaVelez, Alexander Fry, Rex Booth, David Campbell, Nishi Kumar (joined at 17:45), Lorna Alamri (joined at 17:45)

Regrets (or no response):
Eoin Keary, George Hess, Sherif Koussa, Jerry Hoff, Michael Scovetta, Mateo Martinez,

Discussion, Action, Results

Budget

- SB and JB prepared high level GIC budget for 2011 – SB emailed to committee last night. Would like committee members to comment no later than Monday so we can submit proposed budget to Board for Tuesday (3/8/2011) meeting.
- Comment – SB' administrative costs not included in budget. This should include $5,000 already approved by board for 2011 and administrative costs for 2012. All agreed that Sarah should continue in administrative support role for this year and into next year.
- Action item: JB and SB to revise budget and email committee by EOD so that they can comment before submission to board on Tuesday morning.

2011 AppSec Conferences: AppSec EU, AppSec USA, and AppSec SA

- There has been discussion about using the App Sec conferences as a venue for Industry working groups and discussions with verticals – what is our plan for this?
- JB – This should be a two tiered approach:
  1) GIC contacts conference coordinators to find out their plan for working with local industries (who may or may not attend local OWASP meetings). GIC asks for support from conference coordinators in working with verticals to be targeted for attendance at conference.
  2) Based on verticals targeted (as decided in #1), GIC sends invitations asks individuals to attend who should be part of the discussion/working group.
- RB – Will focus on Government vertical. Important to approach and strategy for verticals separate. What works for Government, may not be the right strategy for the Financial industry.
- JB – We will keep the plan for industry outreach general for now, but as we gain momentum within the committee we will work towards more specific plans. At the conferences, we should organize a single industry session with breakouts (as applicable) for specific verticals
- MF – in contact with organizers for AppSec SA and will work on establishing which verticals GIC should target at this conference.
- Comment – 2011 AppSec Asia (in China) missing from AppSec list – needs to be included in outreach activities and budget (above) planning.

List of Industry Verticals

- List prepared by SB with input from CW and emailed to committee earlier in the week. Comments? Suggestions?
- DC - need to condense list to 6-7 areas to focus on. As list currently exists, too many areas.

- SB – concern as noted by Tom Brennan that we try to keep industry verticals listed (terminology) as they appear in common sources.
- AF – Technology should be listed as Information Technology
- RB – OWASP (not just GIC) also needs to define horizontals…
- Action item: SB to revise list, condense to 6-7 areas and email list next week week for comment

Discuss "Rules of Engagement" for GIC Outreach

- Discussion started at Summit in relation to whether the GIC /OWASP should have a NDA with companies it engages with. It was decided that GIC/OWASP will NOT engage in any NDAs as it goes against OWASP's founding principal of openness.
- John Stevens raised the possibility of setting up "rules of engagement"…

  "Since the first summit, we've all heard several well-respected members of the OWASP community--who are not vendors--lament how difficult it is for them to contribute. The situation faced remains what it was and is simply:

  There is no formal conduit through which the participation of commercial entities and their employees feel comfortable contributing while protecting their organization's privacy, intellectual property, and employment.

  Some organizations and their employees can participate without such a formal conduit, and that's great. Others will not be able to. I imagine we want to actively include those who are currently precluded, even in a first such attempt at outreach for greater involvement. Something Joe, Tom, and other representatives from commercial entities and I have talked about is establishing some 'ground rules' for working with these reluctant organizations. Ground rules would need to address the issues I described in the breakout above."
- TUV – Issue is how to get around signing an NDA (meeting the OWASP objectives of openness) but also protecting corporate interests
- JB – will reach out to FS-ISAC regarding their membership agreement, which he thinks has terms or is a bilateral agreement regarding the protection of corporate interests.
- JB – Right now in OWASP we have a $5k Corporate Membership and a $50 individual membership. Maybe we should have something in the middle, for example: a $500 corporate employee membership - where there is an open disclosure but still a protection of their interests in their membership agreement. These corporate members would have access to vertical driven content, and the ability to interact with peers with similar appsec issues.
- RB – this still sounds too "NDA"ish. Although it isn't called an NDA, it sounds like an NDA.
- JB –we could focus on collecting data from the corporate verticals regarding the most common vulnerabilities for that vertical. They we can sanitize the data and report metrics.
- MF – Not fond of an NDA; we need to to protect sources, but not the information itself
- SB – It sounds like we would like to do something similar to the media who want to protect their sources, but still report on the information…
- JB – In agreement with MF and SB, we will represent the data through sanitized metrics but not disclose the source.

- RB – to email out annual survey results from Grant Thornton, which we may want to use as a model or starting point.

GIC Mailing List

- Who wants to be a list moderator?
- No one volunteered to moderate list, so SB will be list administrator and moderator for now
- DC requested to be taken off list as moderator
- JB – proposed to have the public mailing list (as it currently exists) and also private list for just committee discussion and private list for each vertical. Then the private lists will post to public list when they have decided on what information they should make publically available.
- Discussion re: public vs. private lists. Private lists seem to go against owasp "open" principal, but may be necessary in certain cases – i.e. NK wants to discuss private company info
- MF – we should default in posting to public list, but if there are special instances or specific reasons for keeping things private, we can email to committee members only.
- For time being, if want something sent out to committee members only (and don't have addresses), send to SB and she will send out to committee members
- Action items: SB to talk to Larry Casey about 1) no moderation for committee members posting to list and 2) sending a copy of the message to the sender

Update on Revised Mission

- SB sent a copy of the revised mission to the list last night.
- Committee members should look this over by next week and comment so we can vote on new mission statement (if possible) by end of week

Vote on New GIC Members

- SB – NK needs to resign from GEC before she can be an official member of GIC (no one can be an official member of more than one global committee)
- NK – will follow up with GEC re: resignation, including JB and SB
- Committee vote on new members: Mauro Flores, Mateo Martinez, and Nishi Kumar. No opposition. New membership of all three approved/passed.

GIC Task List

- SB set up google spreadsheet to be used in tracking each committee member's deliverables as well as focus areas. There is a link to this document on the GIC wiki page.
- JB – this will not be used to assign tasks without members knowing, only used to track what each member volunteers to do or work on.

Next Meeting

Friday, 18 March 2011 at 17:00 GMT

- +1 877 534 8500 or International +1 513 534 8500
- Passcode 410105 #

Summary

Post-Meeting Deliverables (for JB and SB)

1. Amend GIC Budget to include Administrative Costs (for SB in 2011 and 2012 as well as travel), email to GIC, and submit to Board on Tuesday for vote (unless problems vocalized from GIC)

2. Amend list of industry verticals and condense to 6-7 categories
3. Contact Larry Casey re: GIC mailing list - no member moderation, send msg copy to sender
4. Collect comments on new GIC mission, and submit final draft to GIC for vote

Deliverables for others – for completion by 3/19/2011

1. JB – Reach out to FS-ISAC regarding terms of engagement for membership agreement
2. RB (Vertical – Government) – Email GIC with GT annual survey results (example/model for GIC metrics collection?)