



## Open Security Community Meeting - March 13

### Attendees:

Mr. B. (Bart)  
Evan Powell  
Brennan Lodge

### Meeting Summary:

The mission of the Open Security Community is to foster dialogue about open security and software, and to share data that aids the development of open security solutions. The community aims to be a "town square" where open-source security enthusiasts and software practitioners can share their work and discuss open security approaches without the pressure of vendor pitches.

### Key Approaches and Offerings:

- Focus on open-source security companies and related government initiatives like those by CISA.
- The community serves as a platform for technical show-and-tell, allowing builders to present their work.
- Discussions on security data in Kubernetes and open-source project contributions are encouraged.
- Highlighting deep learning and AI for MITRE mapping to garner the attention deserved by open-source projects.
- Objectives:
  - To build a community driven by passion, with strong bonds and a common project focus, enabling it to thrive and stand out.
  - To collaborate on projects that benefit the community and highlight unique spaces within open security.



### Upcoming Initiatives:

- Evan is arranging a collaboration with the OSSSF to strengthen community outreach.
- Plans to organize a YouTube event or similar platform to showcase speakers and their work within the next two weeks.
- Engaging with the OSSSF community for feedback and securing the first speaker for the event.
- Establishing a structured format that includes talks and forums flexible enough to adapt to community feedback.

### Event Structure Suggestions:

- Considering formats like fireside chats or lightning talks with a preference for brevity (e.g., 20-minute talks followed by 10-minute Q&A).
- Curating themes for discussion, starting with questions that spark interest, such as recommended tools for Kubernetes clusters or general advice for the community.
- Content and Persona Focus:
  - Catering to Response and Detection Engineering personas and those interested in building their own SIEM solutions.
  - Attracting data scientists interested in security applications and leveraging the energy of community members with frontline cybersecurity experience.
  - Identifying common themes within the Data <> Cybersecurity community to guide the community's direction and content.

### Community Engagement and Logistics:

- "Bart" emphasized the importance of creating an engaging town square vibe without vendor influence.
- Distributing a Google document for collaborative preparation and collecting questions in advance to guide the event.



- Encouraging speakers to focus on presenting problems and solutions in an open format, with optional use of slides or code demos.

Suggesting the creation of a briefing book to provide structure while maintaining an informal atmosphere.

### Action Items:

- Utilize GitHub for community issue tracking and transparent speaker invitations.
- Invite speakers publicly and directly, aiming for a target group of 6-8 individuals.
- Bart to be out until April 6, with tasks delegated accordingly.
- The meeting closed with a reaffirmation of the goal to create institutional success within the community, including engaging with organizations like CISA and MITRE to ensure a safe space for building open-source security products.
- The big next step is - get a cool speaker and rally 10-15 folks to join them. We are thinking MITRE themselves and/or others might want to speak, let's see. I'll be directly pinging as will others.
- If you are someone like @Loris Degioanni who wanted to help prime the pump by sharing your story and maybe some code, that would of course be amazing OR if you have suggestions as to folks who might be able to speak about their use of open source security, what problems they addressed, and how they see their particular area evolving that would be amazing.

### Notes from Brennan

#### Attendees

Mr B.- Bart

Evan Powell

Brennan Lodge



### Meeting Minutes

Mission: A community to discuss open security and software related approaches with data that supports the creation of open security

Overall approach:

- open source security companies
  - sys dig
- open source related security
- CISA (government related)
- where do we fit?
  - town square (in the positive sense)
    - offerings:
      - technical work show-and-tell
      - get other builders and practitioner in the town square to talk about it
      - data on security in k8
      - open source project
      - deep learning and AI of MITRE mapping
    - get the attention they deserve on open source building
    - Bart - it resonates to create a town square vibe and not be showered with vendor pitched
    - objectives
      - there is passion behind it
      - have a common project to work on
    - for a community to thrive with strong bonds for a strong community
    - work on a project together
    - great way to stand out as a different space
- Even trying to schedule time with the OSSSF to join forces and build out the community
- approach:
  - in 2 weeks we will have (forcing function) will have a YouTube or event to denote speakers for show-and-tell



- OSSSF - Bart knows the community
- get their feedback
- get 1st speaker
- helpful to have a structure for the audience to know
- what are the best talks to think of good content and forum (be flexible)?
- see code?
- demo?
- Structure:
  - fireside chat?
  - time based (20 min talk with 10 min Q&A)
    - shorter the better
    - lighting talks
  - themes for what will be talked about
- start by asking
  - what 3 tools would you first install on K8 cluster
  - what piece of advice
  - ask the community a question about what will want to be solved
  - Evan - security itself and data to help do security
- Response and Detection Engineering personas
- build of your own SIEM
- appeal to the data scientist that want to do security
- energy from folks that did the fighting
- build van diagram of personas in this Data <> Cybersecurity community to identify common themes for the community
- 
- thus spoked "Bart"
- send out google document
- get questions ahead of time
- if asking to show code or deck (could be good)
- deck optional?



- start with problem
- solutions
- prove your solutions
- have a briefing book
- helps structure but encourage free style and makes it more comfortable
- don't ask something that may be uncomfortable of divulging too much information
- success comes from becoming institutional
- talk to CISA and MITRE for a safe space to build these open source products
- action items:
- issues in Github
- go ahead and invite speakers and do it publicly and directly to 6-8 folks
- Bart out to April 6