Charter 2022

Global Security Database Working Group Charter

© Copyright 2022, Cloud Security Alliance. All rights reserved.
Table of Contents

Executive Overview.............................................................................................................................4
Scope and Responsibilities..................................................................................................................4
Research Initiatives ............................................................................................................................5
Working Group Membership .............................................................................................................5
Alignments with Outside Groups.......................................................................................................6
Operations..........................................................................................................................................6
Communications Methods..................................................................................................................6
Decision-making Procedures .............................................................................................................7
Duration...........................................................................................................................................7
Charter Revision History ...................................................................................................................8
Executive Overview

The Global Security Database (GSD) Working Group within the Cloud Security Alliance (CSA) has been created to guide the creation of an open source and automation compatible vulnerability identification framework. By making it easy to generate and consume vulnerability information, the cybersecurity industry will be better equipped to rapidly respond to emerging threats.

Specific areas of focus will be machine readable formatting of the data, covering a greater variety of vulnerability categories and products/services, thoroughly labeling the data to allow easy filtering and processing, and the ability to easily update and correct vulnerability information, not only for GSD generated data but other identifiers generated by other organizations without being hindered by manual intervention. Previous attempts at finding a solution have proved too work intensive to properly scale to the level needed, don’t cover many vulnerability scenarios, and are difficult to integrate into automated systems.

Scope and Responsibilities

The scope of this project is to identify and understand the problems around vulnerability discovery, reporting, publication, tracking, and classification. Using the same style of open source collaborative techniques that have worked to create the software ecosystem that we have today, the CSA is creating a community-focused working group meant to replicate this success in the vulnerability identifier problem space. The project is not limited to vulnerabilities in the cloud as we are seeing the same problems and increase in attacks across all forms of IT infrastructure. The common design goal is for vulnerability identifiers to be easily discovered, fast to assign, updatable, and publicly available.

The working group aims to:

- Standardize on component identification/mapping frameworks
- Standardize on vulnerability naming/classification frameworks
- Standardize the mappings of vulnerabilities and components in a way that is automated and consistent rather than manual and inconsistent
- Create a quick, reliable, transparent process for requesting security identifiers and publishing them
- Create feedback loops and supporting technology that allow automated systems and people to provide feedback, updates, and corrections to security identifiers
- Create guidelines and supporting technology that allow potential security issues to be flagged for review and handling
- Create tagging and views of the data to provide structured and ad-hoc views, e.g. “all confirmed security vulnerabilities in language X” or “all smart contract reentrancy vulnerabilities”
- Partnering with industry groups and companies in order to improve and evolve security capabilities (e.g. “Request a GSD button” in products)
Out of the working group’s scope:

- Security response process for vendors and projects
- Secure development process for vendors and projects
- Embargoed vs. public security vulnerability handling
- Disclosure process, Responsible vs Coordinated and so on
- Vulnerability severity scoring and rating standards

**Research Initiatives**

Architecting a vulnerability identifier ecosystem that fulfills modern requirements, as well as supporting community over committee. We will either architect or integrate with existing machine readable component mapping, vulnerability naming, and vulnerability to component mapping frameworks. Where possible, rather than reinvent the wheel, we will support and expand upon what the community is already using.

For further information on current working group initiatives: [https://circle.cloudsecurityalliance.org/community-home1?CommunityKey=c4811e28-4a39-4eb0-b003-99408a5a5ec6](https://circle.cloudsecurityalliance.org/community-home1?CommunityKey=c4811e28-4a39-4eb0-b003-99408a5a5ec6)

**Working Group Membership**

The working group is led by the appointed co-chairs and is composed of volunteers. Members of the working group are welcome to invite others to join the working group and attend meetings.

**Working Group Structure**

**Co-Chairs**

The working group will be led by co-chairs in addition to selected leadership. The co-chairs will assist with the leadership responsibility of the working group. The co-chairs may appoint others as necessary to assure the effective execution of the defined research.

**Committees**

The working group may designate and organize subcommittees to aid in research with the initiatives pertaining to the subject matter of the working group.

**Sub-Work Groups**

Ad hoc sub-work groups composed of subject matter experts may be formed to plan or execute any related outreach, awareness, or research opportunities. Such sub-working groups shall report directly to the main working group.
Alignments with Outside Groups

The working group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs, and other activities needed to support the working group’s defined body of work, on-demand basis. The working group will share research and standards-aligned with other CSA Working Groups, advisory groups, and industry partners (i.e., SDOs, gov).

Operations

Advisory

The CSA Working Group will be advised by the CSA Subject Matter Expert Advisory Council, International Standardization Council, and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to the industry and refer to any redundant or replicated works.

Research Lifecycle

The CSA Working Group will follow the development of the CSA Research Lifecycle for all projects and initiatives: https://cloudsecurityalliance.org/research/lifecycle/

Peer Review

We will seek CSA’s help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

Communications Methods

Infrastructure & Resource Requirements

The working group will be composed of CSA volunteers and co-chairs, and/or committee(s). The working group will require typical project management, online workspace, and technical writing assistance.

Work Group Conference Calls and In-person Meetings

The working group will hold conference calls no less than quarterly. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.
Decision-making Procedures

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a “member present and voting” shall be a member voting “for” or “against” a proposal, including proxy representative.
5. Proxy, where authority is delegated through a written statement or non-repudiated email, should be declared and inspected for validity by the working group leadership before voting starts.

B. Abstentions of more than fifty percent

1. When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

C. Voting procedures

1. The voting procedures are as follows:
   a. By one vote per person via email as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote (previously engaged in the discussion), so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority
   b. By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)
2. The Chair(s) shall, before commencing a vote, observe any request as to how the voting shall be conducted and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
3. In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

Duration

The working group will operate until an architecture for the vulnerability identifier ecosystem is identified. At which time, this charter should be renewed with the specific initiatives related to implementing that ecosystem.
## Charter Revision History

<table>
<thead>
<tr>
<th>February 2022</th>
<th>First version</th>
<th>Josh Bressers, Kurt Seifried, and Josh Buker</th>
</tr>
</thead>
</table>

© Copyright 2022, Cloud Security Alliance. All rights reserved.