


# OpenSSF Meeting Notes Template

: [Repo](#) | [Charter](#) | [Discussions](#)

 **17** : Weekly: Wednesday

 : [10 a.m. PT](#) | [1 p.m. ET](#)

 : [Zoom](#)

 : [OpenSSF\\*](#) (Mailing List)

\* Join the Mailing List to receive the calendar meeting invite.

 : [OpenSSF](#) (Previous Meetings)

Want to join?

- Attend at least 2 meetings and contribute
- Create a PR adding yourself as a member on our GitHub

## Meeting Notes

- Notes are in reverse chronological order. Most recent meeting at the top.

## Future Meetings

Proposed Agenda Items (anyone can propose one here for small-ish items or to discuss with the group when to schedule and we'll add to meetings on-the-fly as time permits)

- TODO

# Planned Meetings

June 17:

Meeting Facilitator(s):

- Emily

Agenda:

- Check point on the doc
- TODO

June 24:

Meeting Facilitator(s):

- Emily

Proposed Agenda:

- TODO

July 1st

Meeting Facilitator(s):

- Cameron

Proposed Agenda Topics (please include POC)

- Sandbox/incubation/graduation updates
- TODO

# 2020-JUL-08 Meeting

Attendance (PLEASE ADD YOURSELF):

- Cameron

Notes (Please anyone feel free to join in shared note-taking):

Topic	Notes: Scribe 1	Notes: Scribe 2
1. Attendance and designating scribes.		Trishank - Datadog
2. General standup and check-ins from partner SIGs and WGs.	NA - Presentation	NA - Presentation OPA is looking to graduate, formally applying for graduation in a few weeks Question on policy management and integration on graphing database
3. Presentations.	<p>Checkov</p> <ul style="list-style-type: none"><li>• Static analysis tool for infra configuration management</li><li>• Python composition for policy construction</li><li>• Runs as test suite in the cicd pipeline and validate config</li><li>• Found misconfiguration issues in Terraform</li><li>• Installation via pip, brew, docker</li><li>• Various output formats like JSON, JUnit etc</li><li>• Can skip tests as well by providing annotations</li><li>• Execution modes: local, pre-commit hook, kube cluster, cicd pipeline</li><li>• Pre-commit hook: can catch issues before pushing to Github for ex.</li><li>• Ci/CD pipeline: Run checkov on every PR</li><li>• Kube cluster: Deploy checkov as another container and it will validate the manifests</li><li>• Roadmap:<ul style="list-style-type: none"><li>◦ Policy sharing - loading policies from github repos</li><li>◦ Deploy as a Kube admission controller</li></ul></li></ul>	<p>Presented by Checkov from Bridgecrew, presented by Barak Schoster Released Dec 2019 under Apache license</p> <ul style="list-style-type: none"><li>• Checkov is static analysis tool for config management</li><li>• Initially wrote 50 checks to validate against code frameworks e.g. Terraform Cloudformation, K8s</li><li>• A check is written in Python for 'checks' against code frameworks</li><li>• Runs like a test suite</li><li>• Validates all infra code against now 300 and growing checks</li><li>• Scanned terraform registry 2,500 checks, 44% were misconfigured e.g. encryption issues, logging issues, iam issues. Some had several millions of downloads<ul style="list-style-type: none"><li>◦ Logging is a common missing piece in terraform config</li></ul></li><li>• Installation via pip on python 3.7+, brew (macos), docker</li><li>• Json, Junit, md table, or color cli rich output format</li><li>• 300 checks for resources are available on <a href="https://checkov.io/2.Scans/resource-scans.html">https://checkov.io/2.Scans/resource-scans.html</a></li></ul>

	<ul style="list-style-type: none"> <li>• 590k downloads, 977 github stars</li> </ul>	<ul style="list-style-type: none"> <li>• Can ignore and skip checks with annotations</li> <li>• Can skip a full category of checks like if you don't want to enforce encryption or add a description to security groups</li> <li>• 4 execution modes: <ul style="list-style-type: none"> <li>◦ Local</li> <li>◦ Pre-commit hook</li> <li>◦ ci/cd pipeline</li> <li>◦ K8s cluster</li> </ul> </li> <li>• Pre-commit hook: checkov can interact as a linter in pre-commit hook and can block you from bad code</li> <li>• ci/cd pipeline: github actions, jenkins, gitlab can run checkov on any PR</li> <li>• K8s cluster: can scan k8s manifests <ul style="list-style-type: none"> <li>◦ Does api calls to k8s api-server and can check if manifests are valid/not valid</li> </ul> </li> <li>• Advantage: Policy as code <ul style="list-style-type: none"> <li>◦ Version controlled</li> <li>◦ Peer reviewed</li> <li>◦ Use inheritance and reuse code</li> <li>◦ Add to SDLC</li> <li>◦ Add to CI</li> </ul> </li> <li>• Roadmap <ul style="list-style-type: none"> <li>◦ Policy sharing via github repos</li> <li>◦ ARM template policies</li> <li>◦ Helm chart</li> <li>◦ Relationship engine</li> <li>◦ Kubectl plugin</li> <li>◦ K8s admission controller</li> </ul> </li> <li>• Project stats: <ul style="list-style-type: none"> <li>◦ Released 6 months</li> <li>◦ 590k downloads</li> <li>◦ 32 contributors</li> <li>◦ 250 PR</li> </ul> </li> <li>• Interested in submitting to CNCF at incubation level <ul style="list-style-type: none"> <li>◦ SIG Security can perform a security assessment</li> </ul> </li> </ul>
3.1. Discussion	Q. Teraform HCL is dynamic. How does checkov handle this ?	QA: <ul style="list-style-type: none"> <li>• Can you use this with an</li> </ul>

	Some use-cases covered by certain special handlers. Still a WIP	<p>admission controller? At-scale have problems with context, with flat rules you're going to hit a wall because it doesn't have context. - In large organizations, teams in AWS, GCP, Salesforce said 80% of issues can be fixed with 'flat rules' - would like to have an engine over relationship rules</p> <ul style="list-style-type: none"> <li>• If I need to update the rules? - always run <code>pip install -u</code> to get commit updates or pull the latest docker image. Add custom rules in Python.</li> <li>• Have you compared this with the ConfTest project? Not aware of ConfTest only aware of OPA and ConfTest is related to OPA? With OPA you need to have plan generated for Terraform for example so OPA can run tests over variables on manifest. Checkov has some logic to run tests on variables on plans. Both ConfTest and OPA require variables or plan files while Checkov does not.</li> </ul>
4. Issues/PRs for discussion.		
4.1.		
4.2. <a href="#">PRs</a> requiring chair approval.		
5. General discussions (open the floor).		