steampipe check list  
 steampipe mod install github.com/turbot/steampipe-mod-aws-compliance

ls #you should look for mod.sp  
 git clone <https://github.com/turbot/steampipe-mod-aws-compliance> cd steampipe-mod-aws-compliance

steampipe query --var=instance\_state="running"  
 steampipe check all --output=brief

powerpipe benchmark run aws\_compliance.benchmark.soc\_2

steampipe check benchmark.cis\_v130 --tag cis\_level=1 --dry-run  
 steampipe check all --where "severity in ('critical', 'high') and tags ->> 'pci' = 'true'" #can use tag given in document so get detailed report  
 steampipe check all --where "severity in ('critical', 'high')   
 steampipe check all --where "severity in ('critical', 'high')" --output=html #to get output in html formate  
 steampipe check all --where "severity in ('critical', 'high')" --export=html #to download output in html formate

steampipe check all --where "severity in ('critical', 'high','midium')" #this command only work if there's "mod.sp"

**Detailed**  
  
Here's a document summarizing the Steampipe and Powerpipe commands and operations , along with some explanations for better understanding:

---

Steampipe and Powerpipe Commands

Steampipe Commands

1. Install AWS Compliance Module

```bash

steampipe mod install github.com/turbot/steampipe-mod-aws-compliance

```

- Installs the AWS Compliance module to check against AWS compliance standards.

2. List Installed Modules

```bash

ls

```

- Look for `mod.sp` to verify if the module has been installed correctly.

3. Clone AWS Compliance Module Repository

```bash

git clone https://github.com/turbot/steampipe-mod-aws-compliance

cd steampipe-mod-aws-compliance

```

- Clones the module repository and navigates into the directory.

4. Run Query with Variable

```bash

steampipe query --var=instance\_state="running"

```

- Runs a Steampipe query where `instance\_state` is set to "running".

5. Check Compliance

```bash

steampipe check all --output=brief

```

- Runs compliance checks and provides a brief output summary.

6. Run Benchmark Test

```bash

powerpipe benchmark run aws\_compliance.benchmark.soc\_2

```

- Runs a benchmark test for AWS compliance related to SOC 2.

7. Dry-Run Benchmark Check

```bash

steampipe check benchmark.cis\_v130 --tag cis\_level=1 --dry-run

```

- Performs a dry-run of a benchmark check for CIS version 1.30 with a specific tag.

8. Filter and Output Compliance Checks

- Detailed Report with Tags

```bash

steampipe check all --where "severity in ('critical', 'high') and tags ->> 'pci' = 'true'"

```

- Filter by Severity Levels

```bash

steampipe check all --where "severity in ('critical', 'high')"

```

- HTML Output

```bash

steampipe check all --where "severity in ('critical', 'high')" --output=html

```

- Export HTML

```bash

steampipe check all --where "severity in ('critical', 'high')" --export=html

```

- Additional Severity Levels

```bash

steampipe check all --where "severity in ('critical', 'high','medium')"

```

Explanation

- `steampipe mod install`: Installs the required modules from a given repository.

- `steampipe query`: Executes a query with specific parameters.

- `steampipe check`: Performs compliance checks on your infrastructure. The `--where` flag allows you to filter the results based on conditions such as severity and tags. The `--output` and `--export` flags define the output format (e.g., brief, html).

- `powerpipe benchmark run`: Executes a benchmark test to measure compliance or performance.

Documentation

For a deeper understanding, you may refer to the official Steampipe and Powerpipe documentation:

- [Steampipe Documentation](https://steampipe.io/docs)

- [Powerpipe Documentation](https://docs.turbot.com/powerpipe)