THE DEPARTMENT OF
COMPUTER SCIENCE
& ENGINEERING
計算機科學及工程學系

SCCCE: Cloud Security Audit & Log Collection

YEUNG, Jasmine Yat Yau

Supervised by Dr. Ricci IEONG & Dr. Brian MAK

Introduction

The Industry Problem

Cloud security auditing involves extensive manual work through CSP portals, leading to:

- Time-consuming processes
- Higher risk of human error

The Solution: SCCCE

- Entering the 6th year of development
- Automated security data collection
- Streamlined auditing process
- Yet, not used in production. Why?

Objectives

The main goal of this project is to **polish SCCCE to be used for real-world cloud configuration reviews**.

1. **Understand and get familiarized with** SCCCEv5 including technologies used and expected functionalities.
2. **Debug, test and fix** identified bugs and possible vulnerabilities.
3. **Ensure code quality** for product stability and future expansion
4. **Experience with** the existing cloud security auditing workflow
5. **Develop** functionalities tailor-made for security auditing use cases

Technologies

Frontend: VueJS + TypeScript

Backend: Golang

Database: MongoDB + Redis + Elasticsearch (For logs) + IndexedDB

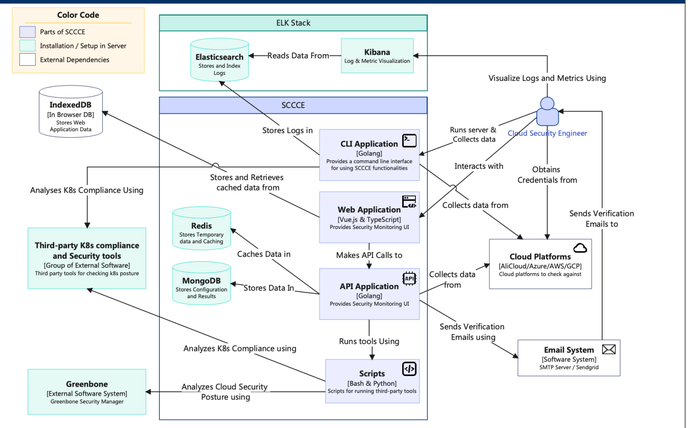
Visualization: Kibana (For Logs & Metrics)

Testing: Vitest + go test

CSPs AWS + Azure + GCP + Alibaba Cloud

Third-party Tools: Kube-linter + Kube-bench + Kube-hunter + Kube-score + Greenbone + Prowler

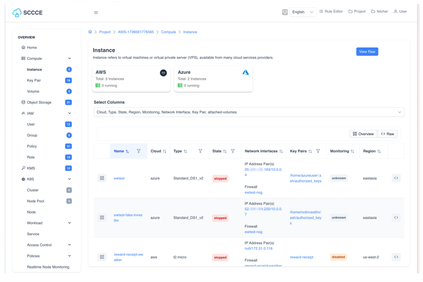
Architecture Diagram



Product Features Highlight

New CLI Application

- ✓ Decoupled Data Fetching
- ✓ Scoped Data Fetching
- ✓ Start Server with Web + Docs
- ✓ Concurrent Data Fetching
- ✓ Ability to Collect Logs
- ✓ Logging and Error Handling



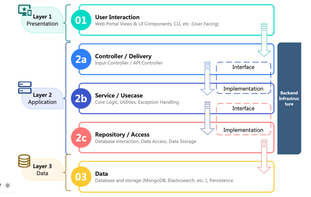
Data Visualization

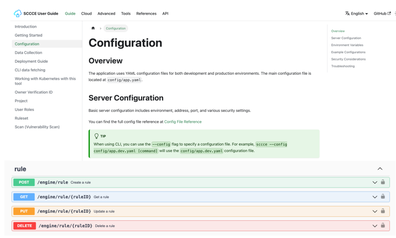
- ✓ Filter and Search
- ✓ Raw Data + Overview
- ✓ Navigation Links to see relationships
- ✓ Network Graphs
- ✓ Multi-CSP support

Development Improvements Highlight

Architectural Improvements

- ✓ Layered Backend Design
- ✓ Dependency Injection
- ✓ Inheritance + Abstraction + Polymorphism
- ✓ Strict Data Typing (Golang + TS)



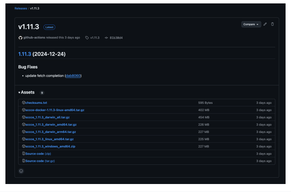


Comments + Docs

- ✓ Commenting Standards: JSDoc + godoc
- ✓ Auto Generate API Docs
- ✓ User Guide available online on GH Pages
- ✓ User Guide i18n Support

Test + CI/CD

- ✓ Wrote tests for existing code
- ✓ New CI/CD + Release pipeline
  - ✓ Run Tests + Generate Coverage
  - ✓ Build → Release → Publish
  - ✓ Deploy Docs to GH Pages
  - ✓ Scan for Committed Secrets
  - ✓ Auto Generate Changelog
  - ✓ Release for different OS
  - ✓ Calculate Version number from commit messages



Conclusion

In conclusion, this project is a successful update to the previous version, with improvements in both user and developer's experience, creating a more user-friendly and efficient tool for cloud security auditing, while enabling better maintainability and scalability.