



SANTIAGO ESPINOSA MOOSER

ABOUT

Hi there 🙋 My name is Santiago, I'm 24 and I've just graduated from the University of Hong Kong. Throughout my university years, I worked part-time in various companies, mostly specializing in cybersecurity, but also including DevSecOps, Penetration Testing, and Software Development. My main focus over the past couple of years has been improving my technical knowledge, and as such, I've experimented with many different technologies, including but not limited to running Arch Linux as my main OS, managing ubuntu-based servers at home, and deploying my own containerized services. I am a team player and love to be the least knowledgeable person in the room, but am also more than happy to help mentor and guide others where needed. I'm currently looking for a job, in any of the diverse fields I'm familiar with. If you're interested in my CV, please feel free to check out my github and/or contact me using my email in the top right ->

WORK EXPERIENCE

Security Research Labs
<https://srlabs.de>
Security Research Labs is a boutique cybersecurity consulting company specializing in telco security testing

Hong Kong
Jun 2022 – Present

Security Specialist (Full-time)
Got head-hunted into the full-time position and I am now working as a security consultant, focusing on vulnerability testing and malware development.

Highlights

Led various vulnerability assessments on internal and external systems of clients
Organized the deployment and provisioning of various internal servers to aid in the vulnerability assessment process
Communicated with clients to understand their needs and provide them with the best possible service

Hex Trust
<https://hextrust.com>
Hex Trust is a fully-licensed and insured provider of bank-grade custody for digital assets with a focus on security and compliance.

Hong Kong
Jun 2022 – May 2023

DevSecOps Engineer (Full-time/part-time)
Got head-hunted into an internship and continued working part-time throughout the last year of my studies. Focused on the 'Build' initiatives and 'Shift Left' approach by delivering several projects within DevSecOps, Application Security, Security Automation and Cyber Defense.

Highlights

Designed, implemented, and maintained the company's first-ever DevSecOps pipeline, preventing vulnerable code, secrets, and dependencies from reaching production using Snyk, tfsec, Clair, and trufflehog, as well as other DAST tools. Also adapted CICD rules based on the company's Git branching strategy.
Personally led the Snyk vulnerability management tool implementation, achieving a 20% reduction in active, potentially exploitable vulnerabilities within the first month. Additionally, also
Deployed and maintained next-gen WAF (Signal Sciences) to protect against OWASP Top-10, various web CVEs, and enumeration attacks. The project led to increased protection as well as visibility into incoming network attacks. The ruleset was managed through Terraform Infrastructure as Code (IAC) for optimized security.
Automated provisioning of company Yubikeys, reducing provisioning time from ~45 minutes to <1 minute. The open-source scripts can be found on my GitHub.
Led the adoption of YubiKey hardware smartcards for company-wide code signing, significantly enhancing security measures across the organization.
Conducted thorough investigations on critical security incidents by analyzing logs and alerts from the company's SIEM and WAF systems, and provided recommendations to the Head of Cybersecurity.
Collaborated with Head of Cybersecurity to evaluate and test next-generation WAF/RASP and automated pentesting tools.

Handshake Networking
<https://handshake.hk>
Handshake Networking is a boutique cybersecurity consultancy company that specializes in penetration testing and application security testing.

Hong Kong
May 2020 – Jan 2022

Pentester, Software Developer, DevOps Engineer (full-time/part-time)
Started as a internship, then deferred a semester to work in various roles (due to the small size of the company): Pentesting, Automation Engineering, Web Development, System Engineering.

Highlights

Designed, developed, and deployed a Python-based Django backend API to automatically scan vessels worldwide using remote scanners, RabbitMQ queues, and asynchronous Celery tasks.
Managed and maintained company servers and VMs, facilitating the deployment and utilization of internal services such as Bookstack, Samba, Elasticsearch, Microsoft Domain Controller, and Microsoft Remote app server.
Compiled an Elasticsearch-based database containing over 4.2 billion records of publicly available leaked credentials to enhance penetration testing quality and increase the success rate of brute-forcing client passwords.
Assisted in the recertification process for the Authorized Scanning Vendor PCI certificate by automating reconnaissance and reporting stages.
Deployed Docker-based internal services, including Bookstack (an internal wiki), GitLab, and an Ubuntu-based Samba server.
Developed various internal automation tools and web applications, such as an ike-scan and nmap multithreaded wrapper (available on GitHub).

PWC New Ventures
www.pwchk.com/en/services/new-ventures.html
PWC New Ventures builds software solutions for PWC's client base.

Hong Kong
May 2019 – Dec 2019

DevOps Intern (Full-time), DevOps Engineer Apprentice (Part-time)
Started as an internship, then worked part-time during uni semester within the DevOps team to automate the provisioning of company servers and services.

Highlights

Collaborated with the Head of DevOps to automate server deployments and provisioning using Ansible and Terraform, reducing deployment and provisioning time from 3-5 business days to 30-45 minutes.
Developed and maintained Ansible-based playbook for deploying internal communication tool instances (Mattermost) using Docker-compose and Bash.
Troubleshoot certificate issues on Docker-based deployments utilizing tools such as Docker-compose, Lazydocker, and Certbot.

PROJECTS

DevSecOps pipeline:
Implemented DAST, SAST, and secure stages for NodeJS projects to enhance early detection of security vulnerabilities. Adapted each environment pipeline to its corresponding development environment, using tools such as Snyk, Zap Scanner, tfsec, Hadolint, JSLint, Sonarqube, and Sigstore.

Ansible-based automation for server provisioning:
Developed Ansible playbooks for provisioning PWC's servers using Ansible, Jinja2, and Bash scripting, reducing provisioning time from 4-5 business days to 30-45 minutes.

Django-based network scanner API:
Designed, developed, and deployed a Django-based API for scanning vessels connected to satellite and 4G networks using asynchronous, pluggable 'scan engines' that communicate via RabbitMQ queues.

Django-based covid tracker dashboard:
Created a Django-based dashboard for displaying Covid-19 statistics as part of a software engineering course at HKU, utilizing Jira and GitHub in an Agile development process.

Haskell-based interpreter:
Developed a custom programming language interpreter using Haskell for a Principles of Programming Languages Course, incorporating features like First-class Functions, Variable Scoping, Monads, and Mutable States. See <https://github.com/santiago-mooser/haskell-based-interpreter.git>

Computer Science Association Virtual Career Week 2022:
Organized and led the 2022 virtual career week event for the Computer Science Association, hosting six speakers from various roles and serving as a host for three fireside talks

Unraid Self-hosted Media Server:
Deployed an Unraid-based server for personal media and data backup, hosting various Docker-based services such as PhotoPrism and Syncthing, and experimenting with new tools like Syncthing, nextdns.io, rclone, and Syncthing.

CONTACT

Hong Kong

contact@santiago-mooser.com

[santiago-mooser](https://github.com/santiago-mooser)

[santiago-mooser](https://www.linkedin.com/in/santiago-mooser)

[santiagooespinosa](https://keybase.io/santiagooespinosa)

CV
[Download this as PDF](#)

EDUCATION

University of Hong Kong
<https://hku.hk/>
Bachelor
Computer Science
2018 - 2023

Courses

Cryptography
Design And Analysis of Algorithms
Algorithmic Game Theory
Principles of Operating Systems

SKILLS

Scripting / Automation

Bash

Python

Linux shell

DevSecOps & SRE

Kubernetes

Helm

DAST

SAST

Ansible

Terraform

Docker

CIS

Snyk

tfsec

kube-bench

Linux/Unix systems

Ubuntu

Arch

Bash

Systemd

Troubleshooting

System Administration

XCP-ng

Ansible

Azure

AWS

Linode

Digital Ocean

Pentesting

reconnaissance

Network scanning

nmap

ike-scan

Burp suite

Zap scan

Web development

Django

API

RabbitMQ

Celery

Queues

MySQL

LANGUAGES

English	Native
Spanish	Native
German	Proficient
Cantonese	Rudimentary

INTERESTS

- Playing the Bass
- Muay Thai, MMA and Running
- Co-op Videogames
- Cybersecurity and Ethical Hacking
- Privacy
- Self-hosting

REFERENCES

Santiago's rich experience in DevOps and Information Security allowed us to complete the design and implementation of our DevSecOps pipeline in a matter of weeks rather than months.
— [Shane Read](#) - Chief Information Security Officer at HexTrust

Santiago was always willing to offer his assistance and had excellent technical skills on working software products.
— [Kit Ho](#) - Head of DevOps at PWC New Ventures

— [Richard Staggs](#) - Director and Managing Consultant at Handshake Networking