Aiden Chan Kai Ming

Email GitHub LinkedIn

Work Experience

VM & Security Engineering Intern @ Grab
July 2025 — December 2025 On Site

- Architected and deployed a Breach and Attack Simulation (BAS) platform to facilitate collaborative Purple Team exercises, utilizing Terraform and Kubernetes (EKS) to build a scalable, automated environment for threat validation.
- Engineered an automated ETL pipeline using Python and GitLab CI to ingest security telemetry into an AWS S3 data lake, centralizing critical data for enterprise-wide visibility.
- Developed a centralized Vulnerability Management (VM) Governance dashboard, utilizing complex SQL to aggregate risk metrics and provide stakeholders with actionable insights into the organization's security posture.
- Led the end-to-end evaluation and implementation of new security infrastructure, bridging the gap between Red and Blue teams by automating attack scenarios and defensive control testing.

Education

Bachelor in Computer Science (Hons. Cybersecurity)
Multimedia University, Cyberjaya
Aug 2023 — July 2026 Cyberjaya, MY | CGPA: 3.76

Leadership Experience

Co-President
Hackerspace MMU **May 2025 — Present**
Achieved approx. 195 registrations, provision semesterly hackathon, setup venue every tuesday for Hackerspace session, work on side-projects.

President
MMU Esports Club **April 2023 — July 2025**
MoU signing between MMU and UniPin, secured partnership with UniPin and CRIT Esports, restructured organisation, organised university-level tournament, led 40 committee members, broadcasting team in MPLSG Season 9

Languages

- Professional: English
- Conversational: Chinese, Malay

Participations

San Diego CTF, Rentas CTF, SD CTF 2024, and L3akCTF 2024, Great Malaysia AI Hackathon by AWS

Technical Skills

Language	Python · Javascript · TypeScript · Bash
AWS	Lambda · CloudWatch · EC2 · S3 · VPC · EKS
CI/CD	GitHub Actions · GitLab CI/CD
Tools	Docker · Kubernetes · Terraform
Databases	MySQL · PostgreSQL

Projects

Schedulr - Timetable management system (Website)
- Open-source cross-browser extension for MMU students and lecturers to automate the process of transferring timetables from university portal to digital calendars
- Eliminates manual data entry, turning time-consuming hour-long task into a few-second process. Has fixes for common data inconsistency in the university portal
- Setup proper environment (dev/stg/prd) and github action to streamline development process, monitor project with sentry and report issues to slack channel with webhook
- Tech: JavaScript, HTML, CSS, Google Calendar API, OAuth 2.0, Cloudflare Workers, Supabase, Rollup, GitHub Actions
- Skills: GCP Deployment, CI/CD, Secrets Management, REST API, Environment Management, Monitoring/Alerting

DevSecOps CI/CD Pipeline
- Built a 5-stage pipeline featuring Gitleaks secret detection, Semgrep SAST, and Trivy SCA; integrated Kyverno CLI to block non-compliant manifests pre-deployment.
- Secured container builds using CycloneDX SBOM generation and Cosign cryptographic image signing for end-to-end supply chain trust.
- Centralized vulnerability management via DefectDojo, aggregating and deduplicating SAST, SCA, container, and OWASP ZAP DAST scan results.
- Tech: GitHub Actions, Trivy, Semgrep, Gitleaks, Cosign, CycloneDX, OWASP ZAP, DefectDojo

Cloud-Native Security on AWS EKS
- Provisioned an isolated, private AWS EKS cluster via Terraform (VPC, IAM, ECR, KMS) using AWS SSM Session Manager for secure administrative access—eliminating bastion hosts and public endpoints.
- Enforced cluster-wide Policy-as-Code by deploying Kyverno with 6 core policies targeting security hardening (non-root execution, dropped capabilities, read-only rootfs) and operational guardrails.
- Architected a continuous delivery workflow using the ArgoCD App-of-Apps pattern paired with a Prometheus, Grafana, and Alertmanager stack for cluster observability and real-time alerting.
- Tech: AWS EKS, Terraform, Kyverno, ArgoCD, Prometheus, Grafana, AWS SSM

Homelab
- Orchestrated a containerized environment on Debian using Docker Compose to enforce IaC principles, ensuring repeatable deployment and management of services.
- Deployed a secure, encrypted remote-access layer via Tailscale SSH and a unified observability stack for real-time monitoring of system and container health.
- Tech: Docker (Compose), Tailscale, Prometheus, Grafana, cAdvisor, Node Exporter.
- Key: SysAdmin, Network Security, Observability & Monitoring, IaC, Linux.

Referee

Roy Chiu, Security Automation and Detection Team Manager @ Grab manshan.chiu@grabtaxi.com