KUA HAO REN

Mobile: +65 92358224 | ivankuaahr@gmail.com | LinkedIn: https://www.linkedin.com/in/hao-ren-kua-37b391146/

PROFESSIONAL SUMMARY

Versatile and motivated technology professional with practical enterprise experience in cloud environments and a strong interest in emerging technologies. Skilled in programming automation, cloud platforms (AWS), data analysis, and a range of technical and business tools. A self-driven and proactive learner in the cybersecurity space who continuously builds hands-on expertise in areas such as malware reverse engineering, threat intelligence and AI security. Passionate about bridging technology and business by understanding user needs, system trade-offs, and product impact, and applying technical expertise across cybersecurity, cloud, and product-focused roles to deliver secure, scalable, and customer-centric solutions.

EDUCATION

Nanyang Technological University, Full-time **2020 – 2024**

- Bachelor's Degree in Computer Engineering (with a specialization in Cybersecurity)
  - Final-Year Project – *History Analysis of Decentralized Applications*
    - Analyzed adoption patterns, usage trends, and technical architecture of DApps across major blockchain networks (e.g. Ethereum)
    - Evaluated smart contracts and transaction data using tools like Etherscan, with a focus on token standards (e.g. ERC-20, ERC-721) as implemented through OpenZeppelin's secure and industry-standard libraries to ensure best practices in contract design and interoperability
  - Relevant Modules – Concepts and Techniques of Malware Analysis, Cyber Threat Intelligence, Cyber Physical System Security, Security Management

SKILLS & OTHER

- **Languages:** English, Chinese, Hokkien and Thai (Basic)
- **Interests:** Sports (Basketball & Badminton), Travel, Web3 Innovations (Blockchain, Cryptocurrencies and NFTs), Exploring Emerging Technologies
- **Platforms:** Continuous Learning, CTFs (e.g. HackTheBox), Blockchain Security (e.g. Cyfrin Updraft)
- **Certificates:** $(ISC)^2$ Cybersecurity, IBM Cybersecurity Analyst, Fundamentals of Technology Sales, Excel Skills for Business, AWS Certified Solutions Architect Associate, AWS Certified Security Specialty, CISSP (in progress)
- **Technical Skills:**
  - **Programming & Automation:** Python, Java, C, Solidity, UiPath
  - **Cloud Platforms:** AWS
  - **Containerization & Orchestration:** Docker, Kubernetes
  - **Identity & Access Management:** Active Directory, LDAP, CyberArk
  - **Firewalls & Network Security:** Check Point, Palo Alto, Imperva (WAF/DAM), Cisco ESA
  - **Endpoint & Threat Management:** TrendMicro EPP/EDR, SentinelOne, Rapid7
  - **SIEM & Log Management:** IBM QRadar, Splunk, Wazuh
  - **Security & Analysis Tools:** Wireshark, IDA, Burp Suite, Etherscan
  - **Cybersecurity Domains:** Reverse Engineering, Malware Analysis, Threat Modelling (MITRE ATT&CK, MITRE ATLAS, STRIDE), Risk Management, Vulnerability Management
  - **Operating Systems:** Windows, Linux (RHEL)
  - **Business & Management Tools:** Project Management, Security Governance, Information Security, ITSM (Jira), Tableau, Salesforce, Microsoft Office Suite (Excel, PowerPoint, Word, Outlook), Notion

PROFESSIONAL EXPERIENCE

Security Engineer (Cloud) **Nov 2024 – Present**

ST Engineering Cloud and Data Centre Solutions

- Identity & Access Management
  - Administered Active Directory and LDAP for domain account lifecycle management, including provisioning and de-provisioning across management console applications.
  - Enforced least-privilege access to privileged accounts by designing CyberArk PAM users, user groups and safe mappings, scoping access strictly to authorized personnel in line with zero-trust principles.
  - Implemented zero-trust, least-privilege network controls across Palo Alto and Check Point firewall policies, Linux firewalld rules, AWS Security Groups and IAM policies.
- Threat Detection & Incident Response
  - Analysed threat actor TTPs mapped to MITRE ATT&CK to refine detection logic and incident response playbooks.
  - Correlated security logs in Splunk, IBM QRadar and TrendMicro across endpoint and network layers to detect IOCs, investigate anomalies and escalate potential intrusions.
  - Deployed and maintained Trend Micro Deep Security Agents across RHEL and Windows server fleets, resolving agent issues and triaging warning and critical alerts in Vision One XDR.
  - Investigated and supported response to a cybersecurity incident, covering real-time log and threat analysis, containment and remediation. Worked with internal teams to identify root causes and improve detection controls.
- Security Architecture & Risk Assessment
  - Administered Cisco ESA email security policies, including PDPA and PCI DSS-aligned content filtering, to reduce exposure to phishing and malicious mail.
  - Conducted risk assessments using risk matrices, data flow diagrams and attack path analysis, and threat-modelled with MITRE ATT&CK and STRIDE to tailor controls to client requirements.
  - Configured security policies and hardened enterprise security platforms, including WAF, DAM, PAM and endpoint security.

    - Remediated findings from compliance scans (HCR), network VAPT and penetration tests across Windows and Linux environments.
- Monitoring & Operations Engineering
    - Administered RHEL servers, troubleshooting OS and service issues and integrating hosts with security and monitoring platforms.
    - Automated Day-2 operations with custom scripts, reducing manual operational workload by 40%.
    - Designed and maintained monitoring and alerting across hundreds of servers in enterprise and government (GCC) environments, cutting MTTR from hours to minutes and sustaining 99.9% system reliability.
    - Executed Day-1 and Day-2 operations across multiple enterprise and CII client environments.
- Leadership & Client Engagement
    - Authored SLA documentation, solution design documents, operational playbooks and user guides, and contributed technical input to solution pitches and proposals.
    - Delivered executive-level presentations that translated technical security concepts into business terms.
    - Mentored and supervised interns on daily security operations tasks, providing technical guidance and quality review.
    - Served as technical liaison between engineering teams and clients to keep project delivery aligned.

Group IT Intern **Jan 2023 – Aug 2023**
PSA International Pte Ltd

- Automated UI test cases in Katalon Studio and test APIs with Postman.
- Created detailed documentation to support process implementation and ensure knowledge transfer.
- Developed and deployed UiPath workflow solutions to automate manual clickops tasks, saving 20+ hours of work per week.
- Performed functionality, integration and system testing on the Global Maritime System to ensure web functions worked as intended and that changes did not break existing functions.

PROJECTS

Infrastructure Monitoring & Observability - Prometheus + Grafana (Self-Directed Project)
- Deployed Prometheus for metrics collection and Grafana for visualization to build hands-on observability experience.
- Configured Prometheus exporters and scrape targets to collect host-level metrics (CPU, memory, disk) and build custom Grafana dashboards for real-time visibility.
- Set up threshold-based alerting in Grafana to simulate production incident-detection workflows and reinforce observability fundamentals.

Centralized Security Logging & Automated Threat Response — Wazuh + Suricata (AWS) (Self-Directed Project)
- Architected a segmented two-VPC AWS environment with VPC peering and Traffic Mirroring to route network traffic to a Suricata sensor for real-time intrusion detection.
- Deployed Wazuh as a centralized SIEM to ingest Suricata alerts alongside host-based telemetry, correlating network and endpoint signals into a unified Day-2 threat response pipeline.
- Tuned custom Wazuh detection rules and decoders to triage Suricata alerts, evaluating an open-source alternative to commercial SIEM stacks for automated security operations.

CO-CURRICULAR ACTIVITIES

Financial & Market Interests **2021 – Present**
- Actively follow global commodity flows, financial markets, macroeconomic trends, and digital asset markets to understand supply–demand cycles, pricing dynamics, and emerging financial innovations.
- Explored emerging trends such as blockchain, cryptocurrencies, and NFTs to stay informed on evolving technologies.

NTU SCSE Club **2022 – 2023**
- Assumed the role of Head Programmer, coordinating with multiple teams to plan, organize, and execute activities for incoming undergraduates.
- Facilitated essential logistics and contributed program ideas for Freshmen Orientation Camp.

SG Basketball Player (Club) **2016 – Present**
- Represented team in the Milo Cup and National Basketball League Qualifiers.

Mentoring Club Executive **2015 – 2017**
- Participated in interactive games to instill strong moral values and provide academic help to Primary School students.
- Participated in events and camps for children and mentors with the joint effort of fellow committee members.

AWARDS & ACHIEVEMENTS

Edusave Certificate of Academic Achievement **2011, 2013, 2014, 2017, 2018**
- Awarded for outstanding results achieved (top 15%) during course of study.