Tim Chu

LinkedIn: https://www.linkedin.com/in/qiusheng-chu-895549129/
Mobile: 0481973240
Email: timc19911012@gmail.com

About Me:

Senior cybersecurity engineer with deep expertise in application and infrastructure security, DevSecOps, cloud security, and penetration testing. With a strong full-stack and automation background, I design scalable security architectures, harden CI/CD and API ecosystems, and drive secure development across teams. I also specialize in AI-driven security engineering — building functional AI agents, fine-tuning LLMs for secure code analysis, and integrating intelligent workflows to enhance detection, analysis, and developer productivity.

Experience:

Senior Manager – Application Security Design Engineer

Macquarie Group - Banking and Financial Service 2023 June to Now

- Designed Noname API security integration architecture with compliance requirement and Developing automation for automatic instance redeployment and failover. Designing Role based access control for access management via SAML.
- Executed targeted penetration testing on newly released applications and features to uncover potential security gaps, while also delivering software development deep dive sessions to demonstrate coding security issues and prioritize enhancements.
- Developed security coding templates and fortifying CI/CD pipelines to ensure adherence to best practices and mitigate risks associated with continuous integration and deployment.
- Designed and implemented API security solutions in Apigee API gateway according application requirement with internal authentication and authorization pattern and analyzing the gap between old implementation and current standard.
- Built robust Apigee gateway proxies for banking and employee applications, implementing OAuth 2.0 for enhanced authentication and authorization mechanisms, and reviewing existing authentication and authorization flows to strengthen security posture.
- Engineered and built a fast docker vulnerability data contextualizer to streamline the process of managing and visualizing vulnerabilities for thousands of docker images and automate the audit process.
- Engineered the implementation of GitHub Advance Security for organization code repositories and modulized github workflows and customizing the scanning processes and providing scanning governance and guidelines for adoption.
- For AppSec leftshift, supervised fine tune (SFTed) with QWen-2B and QLoar Llama2-7B

with customized CodeQL rulesets and aligning model response via direct preference optimization (DPO) for making specialized CodeQL query writers.

Full-Stack Developer - Side Project 2023 June to Now

- Crafted and implemented the backend infrastructure for the Information web application using Node.js Express for business feature development.
- Developed a responsive frontend interface for the web application using React.js, coupled with the creation of Docker images to streamline deployment and scalability.
- Built and secured CI/CD pipeline through GitHub workflows to automate the deployment process and ensure code quality and security measures are upheld.
- Integrated authentication and authorization with 3rd identity provider via OAuth2.0 and building multi-factor authentication for user account security uplift.
- Developed a variety of data pipelines and web crawler for data searching, collection, parsing and normalization according to functional requirements for application data foundation.
- Developed functional AI agents using Python FastAPI, enabling advanced response synthesis, data correlation, intelligent filtering and fulltext search in mongodb for enhanced efficiency and accuracy.
- Identified and resolved AI-generated response inconsistency issues by designing and implementing effective solutions to enhance accuracy and reliability.
- Designed and developed intuitive user interfaces using React.js and Material-UI, ensuring seamless user experiences and modern aesthetics.
- Engineered prompts and deployed multi-agent workflow for synthesising correct and related response of user's prompt.
- Contextualized the prompt with enriched data source via external API and retrieving document via RAG for better responses.
- Built deep search AI agent via LangChain and LangGraph with async event generators, real-time user prompt correction.

Lead Cyber Security Consultant

Wipro Shelde 2022 May to 2023 May

- Lead initiatives for migrating projects to AWS RDS and automating infrastructure and security baselines using CloudFormation, Terraform, and Jenkins pipeline jobs to streamline deployment and ensure consistent security posture.
- Designed and conducted proof of concept (POC) for integrating CyberArk Export Vault Data utility with AWS EC2, Microsoft SQL, Splunk, and other AWS services, enhancing security and compliance across the infrastructure.
- Provided support for EY tech audits by demonstrating evidence of security controls and reviewing security implementation designs to ensure alignment with industry standards and best practices.
- Developed plugins for CyberArk Privileged Session Manager (PSM) and Central Policy Manager (CPM) to automate privileged access management tasks and enhance security governance.

- Designed and implemented Qualys vulnerability scanning solutions and processing report data using AWS Lambda functions, enabling proactive identification and remediation of security vulnerabilities.
- Mentored junior team members to cultivate their skills in automation tools, and security best practices to foster a culture of continuous improvement and team collaboration.

Cloud Security Engineer

Pronto Software **2018 Nov to 2022 April**

- Integrated and maintained Nagios as a cloud monitoring solution, with a specific emphasis on application-level checks, system upgrades, and fine-tuning to ensure robust security and system telemetry monitoring capabilities.
- Orchestrated responses to malicious security incidents, conducting thorough incident investigations, implementing remediation measures, and overseeing resolution efforts to mitigate risks and safeguard critical assets.
- Integrated VMWare LogInsight with AlienVault to automate the detection and alerting of security events, enhancing the organization's ability to detect and respond to potential threats in real-time.
- Managed patch solutions for both Windows and RedHat environments using tools like BatchPatch and RedHat Satellite, ensuring timely patching of vulnerabilities to maintain a secure infrastructure.
- Introduced Palo Alto Next-Generation Firewalls (NGFW) into the cloud infrastructure, focused on troubleshooting network layer routing issues and optimizing security configurations to protect against advanced threats.
- Defined and fine-tuning Palo Alto Intrusion Prevention System (IPS) detection policies, as well as scripting automated remediations for malicious events to enhance the organization's proactive security posture.
- Utilized containerization expertise to secure pronto ERP applications within Kubernetes clusters, designing and implementing robust security controls to protect against container-based threats.
- Conducted penetration testing for newly released web applications, providing detailed reports to management boards.
- Managed vulnerability detection solutions and oversaw the remediation process for identified vulnerabilities, ensuring continuous improvement of the organization's security posture.
- Designed and configured CyberArk Privileged Access Management (PAM) solutions, including building Privileged Session Manager (PSM) plugins for various applications to enforce least privilege principles and protect against insider threats.
- Collaborated with DevOps engineers to manage configuration management using Puppet modules, ensuring secure and compliant configurations across the organization's infrastructure and application stack.

Education:

- University of Wollongong
  Information and network Security — Master 2016-2018
- Shanghai Business School
  Computer Science — Bachelor 2010-2014

Programming:

- Python, Typescript, Fullstack, Bash

Certificate:

- Certified Ethical Hacker V10
- AWS Certified Security Specialty
- Cisco Certified Internet Expert – Routing and Switching CCIE #41400
- RedHat Certified Architect - RHCA ID 140-048-935