Yen-Ming (Kevin) Chiu

kevinchiu923@gmail.com | (+886)975-033-920 | linkedin.com/in/yen-ming-kevin-chiu

PROFESSIONAL SUMMARY

- Cybersecurity leader with proven expertise in group-level security governance and major incident command, bringing 8+ years of experience across digital forensics and incident response (DFIR), threat intelligence, security engineering, and enterprise security governance.
- Served in a group-level security governance management role at a publicly listed enterprise, directing cybersecurity strategy and compliance across 40+ subsidiaries, overseeing SOC operations and security monitoring across 2,500+ endpoints, and driving ISO 27001 ISMS certification preparation.
- Experienced in bridging deep technical expertise in DFIR, threat hunting, and security architecture with enterprise-level governance, risk management, and C-level stakeholder communication.
- Skilled at introducing AI and automation into security operations—reduced threat intelligence report production time by over 80% while lowering error rates on highly confidential deliverables, enabling a small team to deliver outsized governance capacity.
- Continuously engaged in self-directed learning and personal research, with a recent focus on practical AI adoption, automated workflows, and regulatory and compliance studies.

PROFESSIONAL EXPERIENCE

TOPCO SCIENTIFIC CO., LTD. Aug 2025 – Feb 2026

ASSISTANT MANAGER — INFORMATION SECURITY OFFICE (CYBERSECURITY LEAD)

- Spearheaded group-wide cybersecurity governance and third-party risk management across 40+ subsidiaries, establishing unified security policies and compliance standards for data protection.
- Defined and executed the enterprise cybersecurity roadmap in alignment with business objectives, presenting security posture updates and risk assessments to C-level executives on a regular basis.
- Led ISO 27001 ISMS implementation and certification preparation, building structured risk assessment frameworks and internal audit procedures across the organization.
- Built and managed outsourced SOC operations integrating SIEM and EDR platforms, achieving 24/7 centralized security monitoring and threat visibility across 2,500+ endpoints.
- Planned and oversaw enterprise-wide deployment of security platforms (EDR, SIEM, NAC, PAM, DLP), strengthening threat detection, privileged access control, and data loss prevention capabilities.
- Managed vendor relationships with security service providers, overseeing SLA compliance, performance reviews, and cross-functional coordination between IT operations and security teams.
- Led investigation and response for major group-level security incidents, reporting to the CIO and Board of Directors, and coordinated client-side security audit responses—successfully passed the highest-standard audit of a leading domestic semiconductor client, lifted supply restrictions, and safeguarded the group's order eligibility and client trust.
-

CYCRAFT TECHNOLOGY Aug 2023 – Aug 2025

DETECTION & RESPONSE ANALYST

- Managed end-to-end cybersecurity service delivery — including DFIR, EASM, and threat intelligence — for enterprise clients across semiconductor, financial services, and manufacturing sectors, serving as the primary technical point of contact.
- Led high-impact Digital Forensics and Incident Response (DFIR) investigations involving advanced persistent threats, delivering root cause analysis and remediation recommendations to C-level stakeholders at affected organizations.
- Conducted External Attack Surface Management (EASM) assessments, identifying exposed assets and actionable threat intelligence to reduce clients' external risk exposure.
- Engineered an automated EASM threat intelligence reporting system, reducing monthly report production time from 12 hours to 2 hours (~83% reduction) while significantly lowering data transcription errors in highly sensitive client deliverables.

- Developed a semi-automated weekly threat intelligence reporting pipeline for submissions to Taiwan's Financial Supervisory Commission (FSC), cutting production time from 10 hours to 1 hour (~90% reduction) and eliminating repetitive manual workflows.
- Collaborated cross-functionally with product, R&D, and customer success teams to align detection capabilities with evolving client threat landscapes.

GORILLA TECHNOLOGY GROUP Oct 2018 – May 2023
SECURITY ENGINEER

- Served as the core engineer for the company's Endpoint Detection and Response (EDR) product, architecting and developing the solution from initial concept through to successful commercial launch and client deployment.
- Participated in ISO 27001 and ISO 17025 internal audits and coordinated external certification preparation, ensuring compliance readiness across security management and laboratory accreditation standards.
- Delivered security consulting engagements—including vulnerability assessments, compliance advisory, and risk management—for multi-site enterprise environments.
- Supported digital forensics and incident response (DFIR) engagements for government agencies and law enforcement authorities, performing network traffic analysis, malware analysis, and threat research to provide technical analysis and evidentiary support for criminal investigations.
- Contributed to the research and development of multiple commercial security products, including ICS/OT security solutions, network traffic analysis engines, and security detection modules.

ONWARD SECURITY Jul 2017 – Aug 2018
SECURITY ENGINEER (INDUSTRY-ACADEMIA COLLABORATION)

- Researched and developed fuzz-testing modules for industrial control system protocol implementations (IEC 60870-5-104), applied to smart grid and power facility environments to identify potential vulnerabilities in ICS systems.
- Managed a high-speed networking laboratory, coordinating research activities and equipment resources.

EDUCATION

MING CHUAN UNIVERSITY 2016 – 2018
Master of Computer Science, Network Security & IPv6 Research

MING CHUAN UNIVERSITY 2012 – 2016
Bachelor of Computer Science, Computer Networking

Languages

Mandarin (Native) | Taiwanese (Native) | English (Professional Working)

LICENSES & CERTIFICATIONS

- Computer Hacking Forensic Investigator (CHFI)
- BULATS (Cambridge Business Language Testing Service) – Advantage Level

HONORS & AWARDS

- HackTKU Hackathon (Tamkang University) — Most Creative Award
- 2014 World Robot Olympiad (WRO) — 2nd Place, College Division
- 2014 Asian Intelligent Robot Contest (AREC) — 9th Place