Gilbert Choo Zhi Wei

CRISC I CompTIA CySA+ I Cyber Threat Intelligence I Artificial Intelligence

Email: gilbertchoozw@gmail.com - **Mobile:** +65 81804889 – **Web:** https://www.credly.com/users/gilbert-choo

Gilbert operates at a convergence few practitioners can claim—strategic, technical, and creative, drawn from very different backgrounds. As enterprise risk enters a decade of autonomous adversaries, machine-speed attacks, and the slow collapse of today's cryptography, he sits where those forces meet and is building the capabilities organizations will need before most realize they need them.

What sets him apart isn't any single domain but how he connects them. He is a builder by instinct: he has architected Standard Operating Procedures from scratch, help built multiple CTI SME functions, designed a Cyber Incident Management Centre, and shipped internal tools that turned recurring problems into solved ones. That inventiveness traces back to founding his own secure digital solutions company and, before that, a career in real estate marketing—a lineage that gives him a commercial, human-centered perspective most technical specialists lack.

His toolkit is deliberately forward-leaning. Alongside CRISC and CompTIA CySA+, he holds a certificate in Quantum Computing in Cybersecurity and formal training in AI and prompt engineering—letting him reason fluently about threats that have no playbook yet. He works across MITRE ATT&CK and the Cyber Kill Chain, understands the cloud, and is fluent across the major intelligence platforms—Recorded Future, Intel 471, Flashpoint, Anomali, and Cybersixgill—and is bilingual in English and Mandarin.

Strategic enough to see around corners, technical enough to build the response, creative enough to imagine what others miss—Gilbert is a problem solver shaping how enterprises will defend themselves through the next decade of risk.

Work Experiences

1. **Associate Director – Cyber Intelligence Centre - UBS AG**
   Feb 2025 – PRESENT

   Member of the Early Warning Cell at UBS Cyber Intelligence Centre with focus on Tactical Cyber Threat Intelligence. As an AI Champion, I help to drive the adoption and integration of (Gen)AI and agentic AI solutions in my group function. Focusing on Tactical Cyber Threat Intelligence, I contribute to the Early Warning Cell within the UBS Cyber Intelligence Centre. Furthermore, as an AI Champion, I am dedicated to accelerating the integration and adoption of (Gen)AI and agentic AI solutions across my group function.

   Business As Usual (BAU) Operations

   - Monitored UBS's global cyber threat landscape proactively to detect and assess emerging threats.
   - Analyzed and responded to priority alerts and tactical escalations, which included vulnerability threat intelligence, third-party vendor breaches, malware-driven cyberattacks, UBS data leakages, DDoS events, and phishing incidents.
   - Collaborated with key global stakeholders to deliver timely, on-demand cyber threat intelligence, strengthening incident management and response strategies.

   Projects & Initiatives

   - Create, develop and implement streamlined workflows, Standard Operating Procedures (SOPs), customize tools and training materials to improve cybersecurity operational efficiency.

2. Senior Security System Engineer – EPAM Systems Singapore

May 2023 – Feb 2025

Contracted to UBS AG Singapore as a Cyber Threat Intelligence Analyst. My work at UBS includes but not limited to:

Revamping the Global Cyber Threat Intelligence Program

- Established and cultivated relationships with global stakeholders to understand intelligence needs, leading to the definition and creation of relevant CTI products and services.
- Developed comprehensive Standard Operating Procedures (SOPs) to ensure operational consistency and efficiency across key areas: Third-Party Vendor Monitoring, Proactive Vulnerability Monitoring, Data Leaked Monitoring, Tactical Monitoring and Escalations, and Alerts Creation/Decommissioning.
- Spearheaded the planning, design, and establishment of the Vulnerability Subject Matter Expert (SME) function, introducing solutions such as the Vulnerability SME Intranet website, the UBS Critical Infrastructure List, and a dedicated Vulnerability Tracker to resolve daily team challenges.
- Enabled effective role execution through comprehensive SOP process and workflow training delivered to the global team.
- Collaborated with engineering teams to develop internal tools and applications, thereby enhancing intelligence gathering and analysis capabilities.

Strategic, Tactical, and Operational Cyber Threat Intelligence

- Regularly identify, discover, and report critical global cyber threats and risks, providing analysis that informs both operational and tactical decision-making.
- Produce strategic intelligence reports that analyze industry-wide cybersecurity threats, events, and their business impact, guiding proactive strategies.
- Contribute to the development and distribution of tactical and operational threat intelligence products, including alerts, assessments, and briefings, to deliver actionable insights to stakeholders.
- Conduct in-depth research and analysis of cyber threat actors and groups, focusing on their Tactics, Techniques, and Procedures (TTPs), behaviors, motivations, sponsorship, and influencing factors.
- Continuously assess threats and risks posed by emerging technologies to the business, enabling timely mitigation efforts.
- Evaluate cyber threat intelligence sources on an ongoing basis to improve the timeliness and effectiveness of threat assessments and enhance the quality of information from cybersecurity vendors.

3. Lead of Cyber Engagement – Protos Labs Singapore

May 2022 – Jan 2023

Cyber Threat Intelligence (CTI) & Analysis

- **Proactive Risk Mitigation:** Conduct in-depth analysis of emerging cyber threats and dark web intelligence from proprietary and open sources to enable clients to proactively address evolving risks.
- **Customized Threat Landscape Understanding:** Deliver tailored intelligence to help clients understand their specific threat landscape, empowering well-informed decision-making.
- **Structured Threat Detection & Response:** Develop threat scenarios and map Tactics, Techniques, and Procedures (TTPs) to the MITRE ATT&CK framework, establishing a structured methodology to improve threat detection and response capabilities.

- **Deep Insight into Threat Actor Behavior:** Utilize the Diamond Model and Cyber Kill Chain to gain deeper insights into threat actors' motivations and behaviors.
- **Regional Focus:** Conduct research with a specific focus on the Malaysian digital landscape, particularly addressing cyberbullying and scams.

Scams Incident Response & Operational Enablement

- **Threat-Based Cyber Incident Management Centre (CIMC) Leadership:** Led the design and establishment of the CIMC, providing essential services including Cyber Incident Triage Management Support, Cybersecurity Claims Advisory, and Dark Web Intelligence.
- **Policy and Operational Alignment:** Developed a new framework to align insurance policies with cybersecurity operational requirements.
- **Essential Documentation:** Created essential documentation, including Business Continuity Plans (BCP), policies, Standard Operating Procedures (SOPs), playbooks, and consumer scam advisory content and marketing materials.
- **Cloud Platform Management:** Oversaw the installation, maintenance, and hardening of Protos Labs' cloud-based database platform on Alibaba Cloud.
- **Training and Collaboration:** Provided training to incident responders and managed projects in close collaboration with clients and third-party service providers.

Cyber Advisory & Risk Management Consulting

- **Strategic Client Partnership:** Offered strategic cybersecurity advice to SME clients, fostering robust business relationships, and acting as a trusted advisor to drive positive change.
- **Solution Execution:** Executed solutions encompassing third-party cyber products, dark web intelligence analysis, and service support.
- **Awareness Enhancement:** Designed and implemented simulated attack exercises (e.g., phishing simulations) to enhance cybersecurity awareness within client organizations.
- **Regulatory Compliance:** Oversaw and implemented regulatory changes, identifying compliance gaps and driving necessary adjustments.

UX Design and Platform Management (Nexus)

- **Industry Standard Alignment:** Mapped standards such as ISO 27001:2022 to the Nexus backend system to ensure alignment with industry best practices.
- **User Experience (UX) Enhancement:** Collaborated closely with software engineers to enhance the user experience (UX) design for the Nexus risk management platform.
- **Project Delivery Management:** Project managed efforts, involving close collaboration with clients, to ensure successful platform implementation and delivery.

3.1 Cyber Threat Intelligence Analyst

May 2022 – May 2022

- **Analyzed** and tracked emerging cyber threats using proprietary and open-source intelligence.
- **Mapped** Tactics, Techniques, and Procedures (TTPs) of significant cyber threats to our backend systems, leveraging the MITRE ATT&CK framework.
- **Developed** and presented recommendations for CVE remediation and mitigation strategies to clients.
- **Designed** and produced the Protos Labs Intelligence Report.

4. **Cyber Security and Blockchain Practitioner - IBM**
   September 2021 – March 2022

   A government sponsored apprenticeship program related to cybersecurity, blockchain and cloud computing.

5. **Founder – Master of Digital**
   January 2014 – May 2022 – 8 Years+

   My expertise lies in the design, planning, coordination, and maintenance of secure web and digital solutions. This role requires extensive collaboration with cross-functional and regional teams, as well as contractors, across diverse locations including Thailand, Indonesia, Vietnam, India, the United States, the United Kingdom, and Australia.

6. **Marketing Director – ERA Realty Network Pte Ltd**
   A Public Listed Real Estate Company – 2009 – 2014 – 5 Years

   - Managed a real estate portfolio in Singapore, valued at $60 million.
   - Founded EstatesTrends.com, an educational platform focused on guiding and protecting individuals through the real estate buying, selling, and investment process.
   - Oversaw and guided teams, consistently exceeding sales quotas through comprehensive training programs for both new and established agents.
   - **Awards:** Top Achiever (2010); Top Achiever 1st Runner-up (2009).

7. **Singapore Police Force - National Service**
   2009 – 2007 - 2 years

   - Deployed to the Crime Prevention Unit of Foxtrot Division.

Competencies, Skills and Tools

- Google Threat Intelligence
- Intel471 Titan
- Flashpoint Ignite
- Group IB Threat Intelligence Platform
- Recorded Future
- RiskRecon
- Feedly Cyber Threat Intelligence Platform
- Anomali Threatstream
- IBM Resilient
- DevOps Microservices Practices
- Hyperledger Fabric Blockchain Platform
- Agile Methodology
- Cybersixgill: Real-Time Cyber Threat Intelligence
- Flare Systems– Dark Web Intelligence Tool
- IBM Security QRadar XDR (SIEM),
- IBM X-Force Exchange
- Kali Linux, Parrot OS
- Wireshark, ZenMap, NMap, Burp Suite, Metasploit
- AWS, IBM Cloud, Alibaba Cloud, Digital Ocean
- Enterprise Design Thinking
- No Code Web Development
- Windows, Mac & Linux OS

Professional Certificates [Click To View All Certificates At Credly]

- Advanced Cyber Threat Intelligence - Arcx Intelligence
- Cyber Threat Intelligence Practitioner - Arcx Intelligence
- Certified In Risk and Information Systems Control (CRISC)
- CompTIA CySA+
- Professional Certificate in Quantum Computing in
- AttackIQ Uniting Threat and Risk Management with NIST 800-53 and MITRE ATT&CK
- AttackIQ Top ATT&CK Techniques
- AttackIQ MITRE ATT&CK Security Stack Mappings: Azure & AWS
- AttackIQ Extending ATT&CK with ATT&CK Workbench
- AttackIQ Introduction to FIN6 Emulation Plans

Cybersecurity - LSBA
- Prompt Engineering - Vanderbilt University
- AI For Everyone - DeepLearning Ai
- ChatGPT Advanced Data Analysis - Vanderbilt University
- Recorded Future Certified Analyst
- EPAM Prompt Engineering Foundations
- EPAM CloudX Professional
- IBM Data Science Orientation
- AttackIQ MITRE ATT&CK To CVE Impact
- AttackIQ Foundations of Operationalizing MITRE ATT&CK
- IBM Cybersecurity Practitioner
- IBM Blockchain Practitioner
- IBM Cloud Computing Practitioner
- IBM Enterprise Design Thinking

Highest Qualification

Diploma in Business Computing, Republic Polytechnic, 2007

Languages Proficiency

- Fluent in reading, writing and speaking English
- Fluent in reading, writing, and speaking Mandarin Chinese