

# Curriculum Vitae

zhaohongri's Curriculum Vitae

## Zhao Hongri (Leo Zhao)

### Cloud Security Solutions Architect

 [flashoop@gmail.com](mailto:flashoop@gmail.com) |  +60 17 203 2066 / +86 158 1127 0428

 Kuala Lumpur, Malaysia |  B.S. Computer Science |  18 Years Experience

 [LinkedIn](#)

 [OffSec Profile](#)

---

## Professional Summary

Accomplished Cloud Security Solutions Architect with over 18 years of IT experience and 10+ years specializing in cloud security across AWS, Azure, and GCP platforms. Proven track record managing cloud security products at Alibaba Cloud and Huawei Cloud, with expertise in Anti-DDoS defense, Identity and Access Management (IAM), penetration testing, and regulatory compliance (GDPR, PCI-DSS, R155).

Successfully delivered \$25M+ in security solutions revenue for enterprise clients across APAC, Middle East, and LATAM regions, including financial services, Web3, and automotive sectors. Holder of multiple elite certifications including CISSP, CCSP, OSCP, OSEP, GCPN, and AWS certifications.

---

## Core Competencies

**Cloud Security:** AWS Security Specialist | Azure & GCP Security | Anti-DDoS Defense Architecture | IAM Design & Implementation

**Cybersecurity:** Penetration Testing (OSCP, OSEP, GCPN) | Vulnerability Assessment | Security Architecture | Threat Detection & Response

**Technical Skills:** Cloud Native Security | Network Security | Application Security | DevSecOps | Security Automation

---

## Professional Experience

### Cloud Security Solutions Architect | Huawei Technologies Malaysia

Huawei Cloud Computing Technology Co., Ltd. | December 2016 - Present

#### Global Sales Solutions Department (Malaysia) | Current Role

- Architected and delivered comprehensive cloud security solutions for customers across Asia Pacific, Middle East, Africa, and Latin America, generating over **\$25M USD in security revenue**
- Spearheaded security and compliance solutions for Fintech, Web3, and automotive sectors, serving high-profile clients including:
- **Financial Services:** Green Link Bank (Singapore), Asia Pacific Exchange APEX (Singapore)
- **Cryptocurrency Exchanges:** Gate.io (Middle East), BitMar (Middle East)
- **Enterprise:** Astro (Malaysia), Sunway (Malaysia)
- Led compliance consulting engagements for **GDPR, PDPA, PCI-DSS, and R155** standards
- Designed and implemented Internet of Vehicles (IoV) security solutions for Chinese automotive manufacturers expanding globally, including **Great Wall Motors, BAIC Foton, and GreatWall Automobile**
- Developed IoV KPI monitoring solutions and Vehicle Security Operations Center (VSOC) architectures

#### Cloud Security R&D Department (Beijing) | Previous Role

**Anti-DDoS Product Management:**

- Led the DDoS Defense Design Team for Huawei Cloud Anti-DDoS Service, defining product strategy and technical architecture
- Designed public cloud network defense platform solutions and BGP proxy broadcast infrastructure for DDoS mitigation
- Architected enhanced DDoS attack detection and defense solutions for Huawei Cloud Internet egress networks
- Built Advanced Anti-DDoS solutions for overseas edge security deployments

#### **Identity and Access Management (IAM) Product Management:**

- Managed IAM service product development, delivering critical features including:
- Fine-grained authorization and access control
- Global cloud IAM architecture
- Enterprise project management capabilities
- GDPR compliance features and privacy controls

---

## **Cloud Security Product Manager | Alibaba Cloud Computing Technology Co., Ltd.**

**Cloud Security Product Management Department | February 2013 - December 2016 | Hangzhou, China**

- Product Manager for Alibaba Cloud's Advanced Anti-DDoS service, the company's flagship cloud security offering
- Drove product strategy for Advanced Anti-DDoS, which generated **over 60% of total cloud security service revenue**
- Defined product roadmap, feature prioritization, and go-to-market strategies for enterprise DDoS protection

- Collaborated with engineering teams to deliver industry-leading DDoS mitigation capabilities
  - Conducted competitive analysis and positioned Alibaba Cloud as a leader in cloud security market
- 

## Product Manager, Enterprise Security | Qihu 360 Enterprise Security

Enterprise Security Product Division | September 2006 - December 2013 | Beijing, China

- Product Manager at China's largest security company, responsible for enterprise security product portfolio
  - Founded and led **360 Website Guard**, one of China's pioneering cloud security protection services competing with CloudFlare
  - Managed cross-functional team of **10+ members**, delivering security services to **100,000+ customers**
  - Drove product innovation in web application firewall (WAF) and DDoS protection technologies
  - Established early-stage cloud security product-market fit in the Chinese enterprise market
- 

## Key Projects & Achievements

### Enterprise Client Projects

#### Gaming Sector Specialist:

Lead security architect for top-tier gaming clients including **Tencent Games (LATAM)**, **Lilith Games**, and **37 Interactive Entertainment (三七互娱)**.

Designed robust architectures to defend against Tbps-level DDoS attacks while maintaining ultra-low latency (<50ms) for global players.

#### Financial Services & Web3 Security

- Architected cloud security infrastructure for Singapore's Green Link Bank and APEX Exchange
- Designed high-availability, DDoS-resistant architectures for cryptocurrency exchanges serving Middle East markets
- Implemented PCI-DSS compliant cloud environments for payment processing systems

## Automotive IoV Compliance Solutions

- Delivered R155 compliance architecture for multiple Chinese automotive manufacturers expanding to international markets
  - Designed Vehicle Security Operations Center (VSOC) for real-time threat monitoring and incident response
  - Implemented security KPI frameworks aligned with automotive cybersecurity regulations
- 

## Personal Projects & Open Source

### CyberDiagram - Security Audit Specialist Agent

[cyberdiagram.com](https://cyberdiagram.com)

AI-driven automated security audit platform integrating professional penetration testing tools with intelligent decision-making capabilities using Claude AI and Model Context Protocol (MCP).

#### Key Features:

- **Automated Reconnaissance:** Network scanning, port discovery, service enumeration via Nmap integration
- **Vulnerability Research:** Exploit-DB and Metasploit framework integration
- **AI-Driven Analysis:** Intelligent workflow orchestration and vulnerability prioritization
- **Compliance Logging:** SOC 2 and ISO 27001 compliant audit trails

- **Professional Reporting:** Automated Markdown-based security assessment reports
- **Security Controls:** Authorization validation, rate limiting, comprehensive audit logging
- **Architecture:** Hybrid Brain + Executor model separating cognitive planning from operational execution

**Technology Stack:** Claude AI, Model Context Protocol, Nmap, Metasploit, Exploit-DB

 agent · Private

main · 1 Branch · 0 Tags

Go to file · Add file · Code

**About**

AI Penetration Testing for SMBs. At 1/10th the cost of a consultant.

 cyberdiagram.com

ai-penetration-testing

Readme · Activity · Custom properties · 0 stars · 0 watching · 0 forks · Audit log

**Commits**

Author	Message	Time Ago
Auto Commit	add architecture	b597b2f · 2 days ago
agent	add files and structure	5 days ago
dashboard	add rag and cloud deployment docs	3 days ago
docs	add architecture	2 days ago
reports	chore(phase4): add Phase 4 implementation, docs, and M...	4 days ago
scripts	chore(phase4): add Phase 4 implementation, docs, and M...	4 days ago
src	modify brain and executor	2 days ago
templates	chore(phase4): add Phase 4 implementation, docs, and M...	4 days ago
writeup	add rag file	3 days ago
.claudeignore	chore: add .github/copilot-instructions.md (AI guidance) ...	4 days ago
.dockerignore	add rag and cloud deployment docs	3 days ago
.env.example	modify brain and executor	2 days ago
.gitignore	chore(phase4): add Phase 4 implementation, docs, and M...	4 days ago
CLAUDE.md	chore(phase4): add Phase 4 implementation, docs, and M...	4 days ago
Dockerfile	add rag and cloud deployment docs	3 days ago
Dockerfile.slim	add rag and cloud deployment docs	3 days ago
GEMINI.md	chore: update agent files (exclude venv)	4 days ago
QUICKSTART.md	Implement comprehensive monitoring system for security...	5 days ago
README.md	modify brain and executor	2 days ago
docker-compose.yml	add rag and cloud deployment docs	3 days ago
install.sh	modify the nvm	5 days ago
package.json	modify brain and executor	2 days ago
tsconfig.json	add files and structure	5 days ago

**Releases**

No releases published

[Create a new release](#)

**Packages**

No packages published

[Publish your first package](#)

**Languages**

TypeScript 94.8% · CSS 2.1% · JavaScript 2.0% · Dockerfile 0.5% · Shell 0.3% · Slim 0.3%

**Suggested workflows**

Based on your tech stack

 **Webpack** [Configure](#)  
Build a NodeJS project with npm and webpack.

 **SLSA Generic generator** [Configure](#)

## HYBRID MODEL AGENT: BRAIN + EXECUTOR FLOW

### Phase 1-2: 🧠 BRAIN – Reconnaissance & Intelligence Gathering

- Reconnaissance (port scan, service detection)
- Target Profiling (classify target, assess security posture)
- Tool Strategy (select optimal tools)
- Vulnerability Research (CVE lookup, PoC search)
- Attack Vector Planning (prioritize approaches)

▼ 📦 BRAIN→EXECUTOR Handoff  
(BrainIntelligence package)

### Phase 3: ⚙ EXECUTOR – Assemble Attack Plans

- Receive BrainIntelligence from Brain
- Transform attack vectors into executable plans
- Map Brain's priorities to execution order
- Perform operational risk assessment

[HITL MODE CHECK] —> If mode='plan\_only': STOP HERE

### Phase 4: ⚙ EXECUTOR – Exploit Execution

- Execute exploits in priority order
- Manage fallback chain for each target
- Track attempt results and success metrics

Multiple Failures?

YES

### Phase 4b: 📦 EXECUTOR→BRAIN Handback – Custom Exploit

- Brain attempts creative exploitation (AI-driven)
- Context from failed attempts informs approach
- If still fails: TERMINATE exploitation

### Phase 5: 🧠 BRAIN – Post-Exploitation Analysis

- Shell verification
- Privilege escalation
- Flag capture
- System enumeration

Data visualization platform for simplified asset management and compliance reporting. Enables online management of network assets through interactive topology visualization.

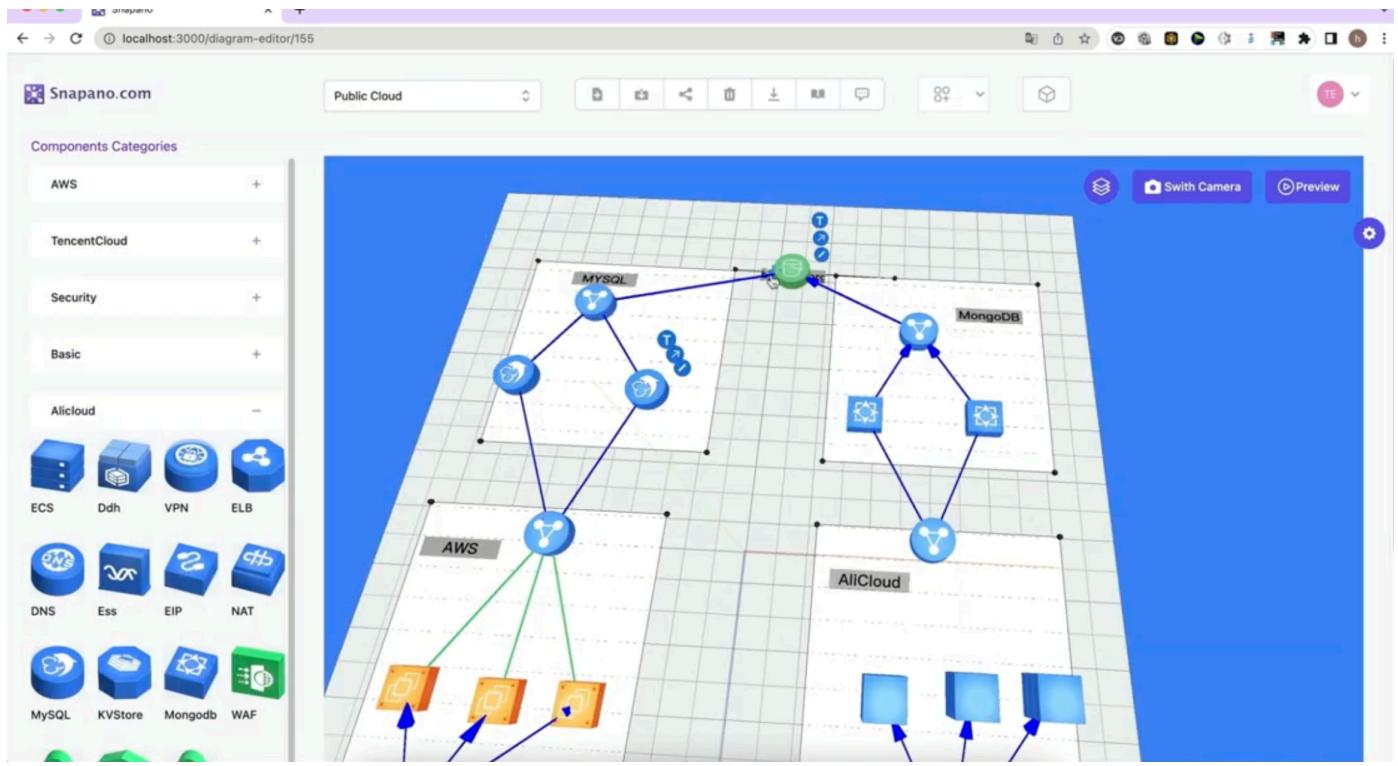
- **Technology Stack:** React, Three.js, WebGL

- **GitHub Repositories:**

- [three-editor-React-Alpha](#)

- [diagram-front-end](#)

- **Demo:** [YouTube Video](#)



## Professional Certifications

### Security Certifications

- CISSP - Certified Information Systems Security Professional



- CCSP - Certified Cloud Security Professional



# International Information System Security Certification Consortium

The ISC2 Board of Directors hereby awards

**hongri zhao**

the credential of

## Certified Cloud Security Professional

Having met all of the certification requirements, adoption of the ISC2 Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the ISC2 Bylaws.

James Packer - Chairperson

Guy Hermann Ngambeket  
Ndiandukue - Secretary



764680

Certification Number

Aug 1, 2026 - Jul 31, 2029

Certification Cycle

Certified Since: 2023

- **OSCP** - OffSec Certified Professional (Penetration Testing)

- **OSEP** - OffSec Experienced Penetration Tester (Advanced Exploitation)

Congratulations!  
**hongri zhao**

You earned the following certifications:

Earned 3 out of 16

	Penetration Testing with Kali Linux - OSCP		Wireless Attacks - OSWP
	Evasion Techniques and Breaching Defenses - OSEP		

- **GCPN** - GIAC Cloud Penetration Tester

This badge was issued to [Hongri Zhao](#) | [View celebrations](#)

Date issued: April 26, 2025 | Expires: April 30, 2029

[Share](#) [...](#)



## GIAC Cloud Penetration Tester (GCPN)

Issued by [Global Information Assurance Certification \(GIAC\)](#)

The GIAC Cloud Penetration Tester (GCPN) certification validates a practitioner's ability to conduct cloud-focused penetration testing and assess the security of systems, networks, architecture, and cloud technologies.

[Learn more](#)

Certification Advanced Paid

### Skills

Authentication AWS Azure Cloud Environments cloud native applications  
 Containers Continuous Integration Continuous Delivery Environment Mapping  
 Information Security Microservices Architecture Penetration Testing Reconnaissance  
 Red Team Service Discovery

## Cloud Certifications

- AWS Certified Solutions Architect - Professional
- AWS Certified Security - Specialty
- AWS Certified Advanced Networking - Specialty

## Privacy & Compliance

- CIPP/E - Certified Information Privacy Professional/Europe (GDPR)



## Education

### Bachelor of Science in Computer Science

University Name | Graduation Year

# Languages

**English:** Upper Intermediate (B2) - Professional Working Proficiency

- TOEIC Listening & Reading: 780
- TOEIC Speaking: 130
- Proficient in technical documentation and business communication

**Mandarin Chinese:** Native Proficiency

---

## Career Objectives

**Target Positions:**

- Cloud Security Solutions Architect
- Cloud Infrastructure Security Engineer
- Cloud Penetration Tester
- Security Architecture Lead

**Preferred Locations:**

- Asia Pacific Region
  - Other International Markets
- 

## Technical Proficiencies

**Cloud Platforms:** AWS, Azure, Google Cloud Platform (GCP), Huawei Cloud, Alibaba Cloud

**Security Tools:** Metasploit, Nmap, Burp Suite, Wireshark, Exploit-DB, DirBuster

**Programming/Scripting:** Python, JavaScript/TypeScript, React, Node.js, Shell Scripting

**Security Frameworks:** NIST, ISO 27001, SOC 2, CIS Controls, OWASP Top 10

**Networking:** BGP, TCP/IP, DNS, Load Balancing, CDN, DDoS Mitigation

**DevSecOps:** CI/CD Security, Container Security, Infrastructure as Code (IaC)

---

*References available upon request*