






Securing Your Digital Future with Penetration Testing

humanlogica.com



 Lot 26-26, 2nd Floor, Setia Raja Commercial Centre,
Jalan Setia Raja, 93350, Kuching, Sarawak

 010 4242 532

 kamree@humanlogica.com

ADVANCED PROTECTION FOR YOUR BUSINESS

We offer a full spectrum of cybersecurity services, from vulnerability assessments and penetration testing to managed security operations and digital forensics.

Our cutting-edge labs and expert team provide proactive protection and rapid response to cyber threats.

Cybersecurity services

Vulnerability Assessment
Penetration Testing
Compromise Assessment
Source Code Review
System Hardening
Advisory (SOP/Policy)

Cybersecurity labs and SOC

Threat Intelligence Lab
Digital Forensics Lab
Managed Services SOC



Why Penetration Testing Matters



Proactive Defense

Penetration testing uncovers vulnerabilities before attackers do. It identifies weaknesses in your systems.



Compliance

Many regulations require regular security assessments. We can help you meet these requirements.



Risk Reduction

Penetration testing can lower the risk of data breaches. Protect your reputation and finances.

CYBER SECURITY ACT 2024 (ACT 854)

The Cyber Security Act 2024 has been officially gazetted by the Attorney General's Chambers on 26 June 2024. This legislation is a major milestone in strengthening Malaysia's cyber defenses and enhancing our resilience against emerging threats.

Under Malaysia's Cyber Security Act 2024 (Act 854), penalties for non-compliance can include **fines up to RM500,000** (Malaysian Ringgit) and **imprisonment for up to 10 years, or both**, particularly for failing to report critical cybersecurity incidents or not adhering to required security measures for National Critical Information Infrastructure (NCII) entities.



Threat Hunting

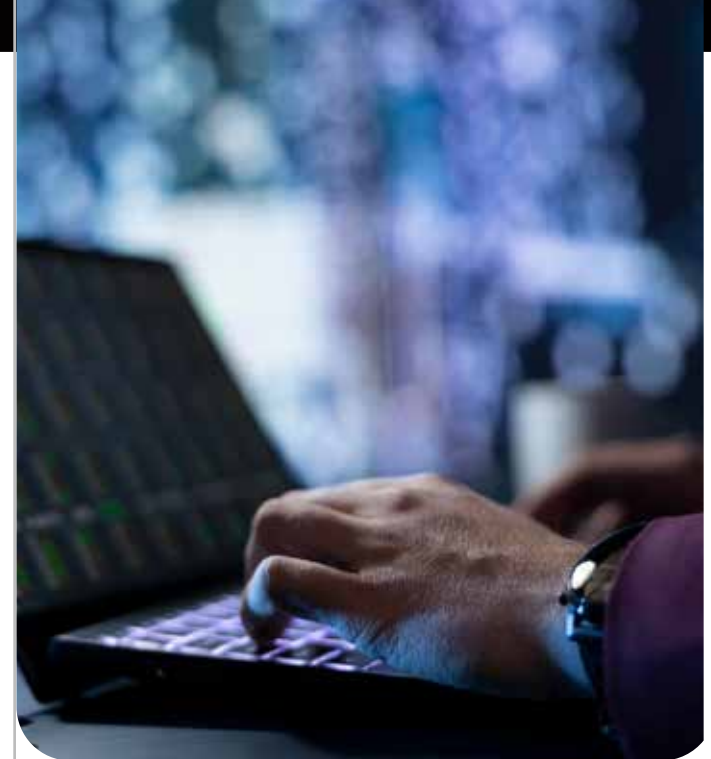
- We provide rapid threat hunting services to identify and gather bad actor digital footprints.

OUR USP

Unique Selling Proposition

Takedown Services

- Identify illegal websites or known malicious websites for immediate takedown.



Forensics Expertise

- Build telemetry between mobile and computer devices to detect root cause of crimes committed within the network.
- Digital forensics to ensure that evidence integrity and data recovery in cybercrime investigations are met with the highest expectation



INDUSTRIES WE SERVE

We proudly serve a diverse range of industries, providing tailored security solutions to meet their unique needs. Our expertise spans the following **National Critical Information Infrastructure (NCII)**:

1. Government
2. Banking and finance
3. Transportation
4. Defence and national security
5. Information, communication and digital
6. Healthcare services
7. Water, sewerage and waste management
8. Energy
9. Agriculture and plantation
10. Trade, industry and economy
11. Science, technology and innovation



Types of Penetration Testing

Network Penetration Testing

Assess network infrastructure security.

Web Application Testing

Find vulnerabilities in web apps.

Mobile Application Testing

Secure mobile applications.

Cloud Penetration Testing

Identifies misconfigurations, privilege escalations, and API security flaws.

Wireless Penetration Testing

Targets Wi-Fi networks to identify weak encryption, rogue access points, and unauthorized devices.

Website Pentest

Reputation management.

SCADA / IOT Penetration Test

Factories, Agriculture, Utilities, and more industries with sparse locations.

SYSTEM SCOPING

Survey of a network, servers & endpoints to discover:

- Unknown vulnerabilities
- Hidden or missing assets
- Security breaches
- Malware
- Unidentified access
- Indicators of compromise (IOC)
- Threat level benchmark

PROJECT KICKOFF

- Period of testing
- Disruption list identification

PENTEST SCOPING

- Identify constraints of Pentest
- Identify type of pentest
- Network tapping for packet capture
- White or Black penetration (credentials based)
- Covert external
- Internal Beaconing

BUDGETARY CONSULTANCY

- Provide budgetary justification for complete remediation

PENTEST FINDINGS REPORT

- Assessment report
- Vulnerability assessment
- Remediation recommendation

NACSA COMPLIANCE REMEDIATION

- Specific threat repeat pentest for Nacsa compliance
- Post remediation by organisation

Process Overview

Partner Certification



Our Commitment to Compliance and Industry Best Practices

Your security is our priority. We demonstrate our commitment through rigorous adherence to industry best practices and compliance with all relevant regulations, providing you with peace of mind and a secure foundation for your business.

Compliance and Certifications



Certifications



Cloud CyberSecurity Services



Approval Letter for Penetration Testing Service Licence

PERKHIDMATAN PENGUJIAN PENEMBUSAN

Dengan ini diperakukan bahawa syarikat yang dinyatakan di bawah ini telah dilesenkan oleh Agensi Keselamatan Siber Negara mengikut Akta Keselamatan Siber 2024 [Akta 854]. Lesen ini tertakluk kepada syarat-syarat yang telah dinyatakan di dalam Akta 854 dan Peraturan-Peraturan Keselamatan Siber (Pelesenan Pemberi Perkhidmatan Keselamatan Siber) 2024 [P.U. (A) 221/2024].

Nama : HUMANLOGICA TECHNOLOGIES SDN BHD
Nombor Pendaftaran Syarikat : 1515282-P
Alamat : LOT 26-27, 2ND FLOOR, SETIA RAJA
COMMERCIAL CENTRE, JALAN SETIA RAJA,
93350, KUCHING, SARAWAK
Nombor Lesen : 20065-02
Tarikh Mula : 9 DISEMBER 2024
Tarikh Luput : 8 DISEMBER 2025

Nota: Pembaharuan lesen ini hendaklah dibuat sekurang-kurangnya 30 hari sebelum tarikh luput lesen.

(Ir. Dr. MEGAT ZUHAIRY BIN MEGAT TAJUDDIN)

Ketua Eksekutif
Agensi Keselamatan Siber Negara
Majlis Keselamatan Negara
Jabatan Perdana Menteri
Tarikh: 9 December 2024



Our Penetration Testing Workflow

Our comprehensive penetration testing workflow is designed to ensure a thorough and effective assessment of your security posture. Each step is crucial in identifying vulnerabilities and providing actionable insights. Here's a clear breakdown of our process:

01

Initial Consultation

We discuss your needs and concerns to tailor our approach.



02

Scope Definition

We outline what systems and areas will be tested to ensure comprehensive coverage.



03

Testing & Exploitation

Our team conducts tests to find vulnerabilities by simulating real attacks.



04

Reporting & Recommendations

We provide a clear report of our findings and actionable steps to improve your security.





Cybersecurity Ecosystem Services

NACSA COMPLIANCE +
ISO 27001 CERTIFICATION

CYBERAWARENESS +
TABLETOP EXERCISE

PENTEST+
CLOUD SERVER HARDENING +
CYBER ADVISORY

MANAGED SERVICES+
BLOCKCHAIN AUTHENTICATION