

The Real-World Cyber Threats

Assess Your Organization's Readiness via Red Teaming



Conventional System Penetration Test focuses on identifying the flaws within a system while the Red Team Assessment (Red Teaming), in a nutshell, aims to evaluate the organization's security readiness from all angles - technology, asset, and people towards real-world cyber threats.

Red Teaming provides a broader coverage of an organization's readiness to battle hackers and malicious individuals in real-time, be it through physical, internal, or external access to the organization.

LGMS Red Team consists of ethical and professional individuals with mature security experience, with the mindset and objective to pinpoint the loopholes and entry point weaknesses to an organization's private and valuable assets.

OUR COVERAGE

LGMS can help you to discover security loopholes and entry point weaknesses with followings:

- ▶ Physical & Logical Security
- ▶ Phishing Campaign
- ▶ Social Engineering
- ▶ LAN & Wireless Network Security
- ▶ Privileged & Un-privileged Threats



Red Team Assessment

Red Teaming emulates several actors penetrating the organization's digital and physical infrastructure. An organization's security measures and awareness would be challenged through planned out scenarios by actors masquerading as relevant identities.

LGMS Red Team will carry out rounds of 3-phase activities to complete the Red Teaming cycle within a defined scope and timeline



DELIVERABLES

Red Teaming report shall include all details pertaining to the scenarios attempted, be it successful or failed, which would be useful to map out an organization's real-world security posture. Our client will be provided a report with the following:

- ▶ Executive Summary
- ▶ Information and Observation captured throughout all phases
- ▶ Detailed Progress Timeline on activity conducted
- ▶ Test Cases conducted and detailed outcomes
- ▶ Customized Recommendations per Observation



Securing the Future

LGMS spearheads the cyber security industry by being the first in the country in various areas of specialization. Here are some of LGMS' latest achievements.




The leading cyber security expert in Asia and trusted by multinational corporations around the world, LGMS is a cyber security consulting company focused on delivering specialized cyber security assessments, consultation and advisory services.

Established in 2005, LGMS has since built a reputation for its integrity, values and best practices by providing world-class professional services to local, regional and international clients across various industries and backgrounds.

- 2017 Cyber Security Company of the Year
- First Center for Internet Security (CIS) Member Company
- First Cyber Security Company Certified in ISO/IEC 27001:2013
- First Cyber Security Company Certified in ISO/IEC 9001:2015
- First CREST Certified Penetration Testing Company
- First MILE2 Certified Training & Examination Provider
- First Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
- First PCI Qualified Security Assessor (QSA) Certified with PCI ASV Status
- First PECB Certified Training & Examination Provider
- First TÜV Trust IT Accredited Tester
- 2019 IDC Report: Asia/Pacific Internet of Things Security Landscape and Key Vendors
- Common Criteria EAL2 Certification for LGMS Security Assessment Report Generator (LGMS Reporter) v1.0.0
- Cyber Security Assessor for SWIFT Customer Security Programme (CSP)

Asia Pacific's Leading Cyber Security Specialist

LE GLOBAL SERVICES SDN BHD (700472-M)
CREST • ISO/IEC 17025 • ISO/IEC 27001 • ISO 9001 • PCI ASV
• PCI QSA • COMMON CRITERIA

 www.lgms.global
 +603-8605 0155
 info@lgms.global

LE GLOBAL SERVICES SDN BHD (700472-M)
 A-11-01, Empire Office Tower, Jalan SS 16/1
47500 Subang Jaya, Selangor, Malaysia.