Responding to a Data Breach

Getting a professional team to handle a cyber incident.

Data breaches cost direct and indirect financial consequences to organizations in both the short and long term. Organizations that are able to respond effectively to a data breach with a well-rehearsed incident response plan can limit the impact of the breach.
Hence, what is done after a cyber incident will make a difference in the impact and cost.

LGMS cyber incident response team aims to help organizations resolve cyber incidents with industry-leading expertise by combining investigative services and remediation advisory. Our goal is to assist organizations to manage the cyber incidents in such a way to limit damage, address the cause of cyber incident, and provide necessary
advisory to reduce the long-term risk of the data breach.

LGMS extensive experience in penetration testing allows better understanding of cases from the attacker's perspective when performing digital forensics. LGMS cyber incident response team works collaboratively with organizations in responding to security incidents, and to strategize improvements in their security posture and compliance program moving forward.

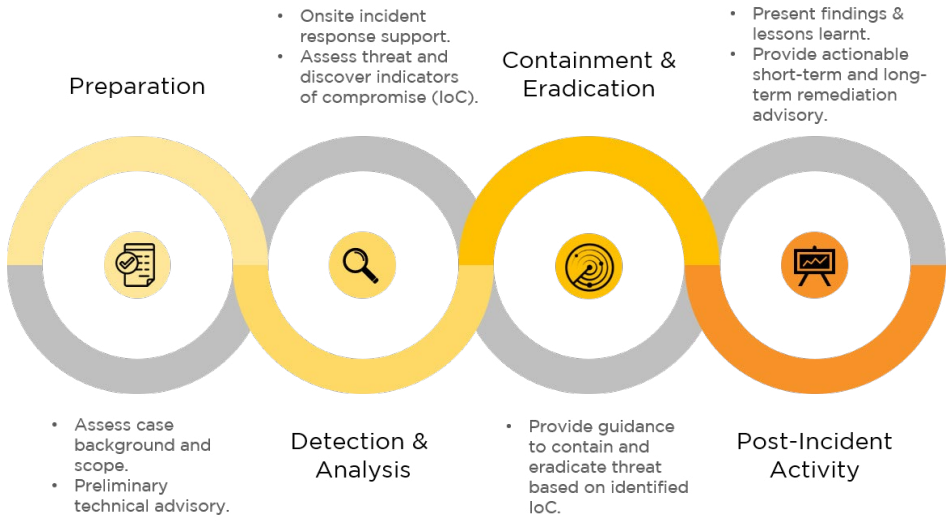
OUR COVERAGE

LGMS provide incident handling, support, and root cause analysis for the following:

- Service Interruption
  - Denial-of-Service Attack (DoS)
  - Ransomware Attack
- Unauthorized Access
  - Web Defacement
  - Remote Compromise
  - Brute Force Attack
  - Data Leak
- Malicious Code
  - Attack Scripts
  - Virus
  - Worm
  - Trojan

Cyber Incident Response Service

LGMS incorporates standard incident response workflow to ensure a systematic approach to incident handling. Indicators of compromise (IoC) identified during the investigative phase will be shared with our clients so that action can be taken to discover and eliminate them vulnerabilities the organization's network.



DELIVERABLES

LGMS will present an investigation report with the following:

- Executive Summary
- Timeline of Events
- Finding Details
- Other Observations
- Recommendation
- Indicators of Compromise

LGMS

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.