MANTUA

CYBERSECURITY

COMPANY PROFILE

ABOUT US

Mantua Consulting Pte. Ltd. is a cybersecurity services company with operations in the Philippines and Singapore that helps organizations secure their systems by providing cybersecurity services. We create value for our customers by assisting them to achieve the most cost- effective path to satisfy their cybersecurity requirements.

Mantua Consulting Pte. Ltd. was founded by Jonathan Mantua and Celia Mantua. Together, they built Mantua Cybersecurity from the ground with the network of partners they have worked with and later opened up a Singapore outfit. Since then, the company has provided information security services to a wide range of clients ranging from small businesses to large corporations such as banks, publicly traded companies, multinational companies, and healthcare providers, both in the Philippines and Singapore.

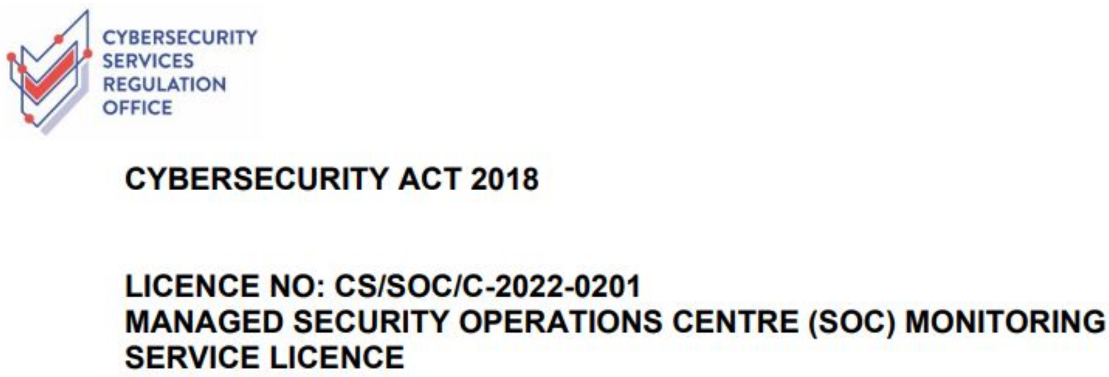
Included in Mantua's portfolio are auditing policies and control, Vulnerability Assessment and Penetration Testing (VAPT), and preparation of recommendations and reports for improvements to overall information of the security posture of their clients. Mantua Cybersecurity is recognized by the Department of Information and Communications Technology (DICT) as a Cybersecurity Assessment & ISMS Provider, and Licensed in Singapore to offer VAPT and Monitoring Services.

Mantua Consulting Pte. Ltd. aims to provide the South East Asia market a world-class quality Security and Data Privacy package and is currently expanding to USA and Australian markets.

ACCREDITATIONS & CERTIFICATIONS:

Singapore:

- Managed Security Operations Centre (SOC) Monitoring Service License
    - License No: CS/SOC/C-2022-0201

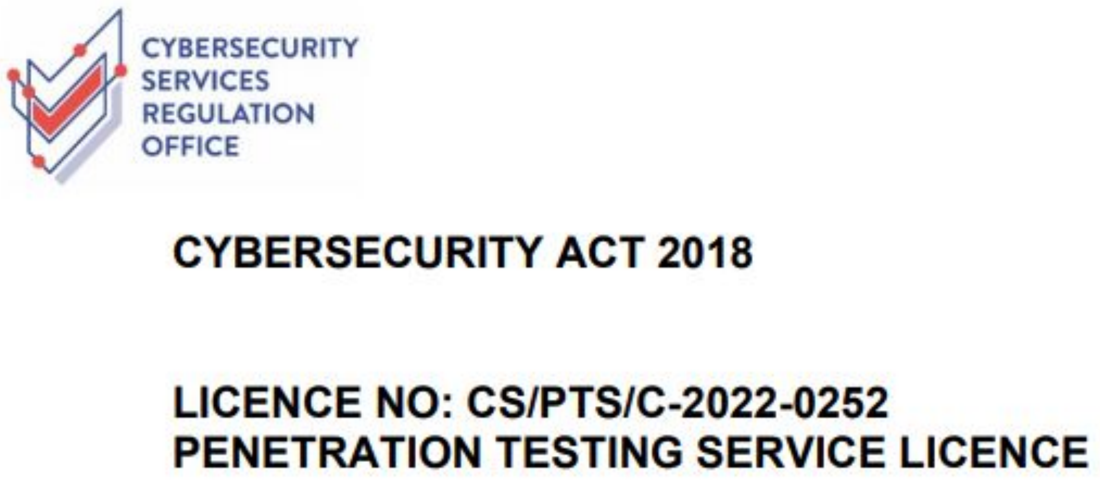


CYBERSECURITY SERVICES REGULATION OFFICE

CYBERSECURITY ACT 2018

LICENCE NO: CS/SOC/C-2022-0201
MANAGED SECURITY OPERATIONS CENTRE (SOC) MONITORING SERVICE LICENCE

- Penetration Testing Service License
    - License No: CS/PTS/C-2022-0252



CYBERSECURITY SERVICES REGULATION OFFICE

CYBERSECURITY ACT 2018

LICENCE NO: CS/PTS/C-2022-0252
PENETRATION TESTING SERVICE LICENCE

SERVICES OFFERED

SECURITY TESTING SERVICES

Vulnerability Assessment and Penetration Testing

Evaluate the current security state of your network infrastructure, servers, web, and mobile applications by conducting Vulnerability Assessment and Penetration Testing (VAPT). Try attacks and exploits on your system before real malicious actors do. Know where to better invest in cybersecurity by knowing your weaknesses and vulnerabilities.

Secure Code Review

Ensure that your applications are secure by having them reviewed for security, design flaws, and conformity to programming language-specific best practices. Code review also ensures that the Open Web Application Security Project (OWASP) recommended best practices are followed, ensuring that the code you deploy is secured.

Vulnerability Management

Vulnerability management is a continuous and proactive process which aims to reduce the organization's overall risk exposure through mitigating vulnerabilities.

An inventory of all assets must be created, these assets must undergo Vulnerability Assessment and Penetration testing to identify security issues. Tools such as network scanners may be used in order to identify the assets within the organization. This list must constantly be updated once new assets are added or discovered.

SERVICES OFFERED

SECURITY TESTING SERVICES

Red Teaming Exercise

Check your company's Blue Team capabilities by performing Red Teaming Exercises. This campaign is composed of different scenarios that can happen in real life but conducted in a controlled environment and coordinated with the client. Some of the methods include but are not limited to Ransomware Infection, Rogue Access Point, and Malicious USB drops.

Load and Performance Testing

Determine failures and slowdown of software systems. This service can also profile the maximum threshold of simultaneous users and transactions being executed. Identify and verify the system's bottlenecks, and potential scalability problems early on so organizations are better advised in potential future investments to grow their user-base and operations.

Smart Contract Audit

Smart contract auditing is a thorough analysis of blockchain applications' smart contracts to correct design issues, errors in the code, and security vulnerabilities.

This is usually done side-by-side with the review of a project's white paper to give potential investors and users peace of mind.

SERVICES OFFERED

MONITORING SERVICES

Security Operations Centre as a Service (SOCaaS)

We provide trained cybersecurity engineers with vast experience in running SOC operations and SIEM tools to help you with monitoring the logs of your system. This is to to ensure that threats are detected and remediated as soon as possible. Our team will work 24 x 7 with our proprietary in-house built monitoring systems to monitor any type of logs you send our way.

Web Defacement Monitoring

Web defacement refers to unauthorized access in which malicious parties penetrate a website and inserts malicious codes, images, and contents that can severely damage your organization's image and reputation. Web and security defacement monitoring can monitor and detect these hacking activities before these affect your website and customers.

Application Monitoring

Keep your systems and customer data safe by identifying and monitoring suspicious activities. Our cybersecurity engineers can detect malicious patterns based on user behavior, data, and transactions.

Information Security Consulting

Meet your demands for enterprise information security management when you lack the internal resources to do so. We will help you develop a cyber security strategy to ensure that sensitive information and your IT infrastructure are protected from ever evolving threats.

SERVICES OFFERED

MONITORING SERVICES

Threat Hunting

Organizations rarely know that they have already been compromised or that a threat is already lurking within their midsts. The common trend seen in compromised organizations is from the moment exploitation is noticed, the prolonged period prior to detection grants attackers the privilege to discover, acquire, exfiltrate, and extort critical business data. In essence, threat hunting is a proactive approach in preventing a compromise.

Threat Intelligence

Threat intelligence is the process of identifying and analysing cyber threats. The term 'threat intelligence' can refer to the data collected on a potential threat or the process of gathering, processing and analysing that data to better understand threats. Threat intelligence involves sifting through data, examining it contextually to spot problems and deploying solutions specific to the problem found.

Compromise breach Assessment

Compromise breach assessment is a type of investigation wherein a team of security analysts combs through log sources and utilizes tools in order to answer the question "Have I been breached?".

This involves analysis of network logs and system logs to determine whether a system has been compromised. A security analyst will be looking for indicators of compromise (IoC) or malicious software. Organizations typically do not know that they have already been compromised and that their data is being sold on the dark web. It is possible to identify if a threat actor is dwelling on an organization's network or system through a compromise breach assessment which can provide insight on future improvements and security gaps.

SERVICES OFFERED

CONSULTING SERVICES

IT and Data Privacy Audit

Assess and evaluate your organization's IT infrastructure, policies, and operations to determine whether controls are in place to ensure protection of information, IT assets, and compliance with known legislations, regulations, and industry standards such as Data Privacy Act, Payment Card Industry Data Security Standard (PCI-DSS), General Data Protection Regulation (GDPR), and so on. By performing a comprehensive IT audit in your organization, risks are addressed and managed in an effective, and cost-effective manner.

IT Forensics

Comprises of recovery and investigation of material found in digital devices, often in the event of a computer crime, like ransomware attacks or digital theft. Our security engineers follow the digital forensic investigation process for acquisition of imaging of devices, analysis, and reporting. IT Forensics likewise ensures that the integrity and authenticity of the digital evidence are maintained and admissible for legal purposes.

MANTUA

o-CYBERSECURITY--o

CEL MANTUA

CHIEF OPERATING OFFICER
cel@mantuaservices.com
(+63) 917-875-1110

SALES TEAM

sales@mantuaservices.com