CyberQuote

Financial Training

Information Technology

PRO

# CYBERSECURITY SERVICES 2024

CyberQuote

Financial Training
Information Technology

# ABOUT US

CyberQuote is an ISO 27001 & CREST certified company specialising in financial training and information security services such as penetration tests, baseline audits, phishing drills, red team drill exercises and more

As an established name with more than 20 years of experience, we pride ourselves in serving the investing public and various industries. Our clientele covers different industries such as Airports, Banking Entities, Insurance Firms, Fin-Tech Firms, Healthcare Firms, Blockchain Firms etc. With a proven reputation for service excellence, we endeavor to build long-term relationships with our customers and business partners.

CQ CyberQuote
Financial Training
Information Technology

# OUR FOOTPRINT

SINGAPORE

MALAYSIA

HONG KONG

TURKEY

INDONESIA

VIETNAM

JAPAN

THAILAND

CyberQuote

Financial Training
Information Technology

# OUR PRODUCTS & SERVICES

**We provide data, information, analytics and cybersecurity services to businesses.**

- Vulnerability Assessment
- Penetration Testing
- Phishing Drill
- Anti-Phishing Awareness Training
- Cyber Security Baseline Audit
- Cyber Security Forensic
- Smart Contract Audit
- Red Team Drill Exercise
- Data Asset Carding

CQ
CyberQuote
Financial Training
Information Technology

# CYBER SECURITY

## Cyber Security Services

CREST Approved Penetration Testing & Vulnerability Assessment

CREST. | VA | PEN TEST

CyberQuote
Financial Training
Information Technology

# VULNERABILITY ASSESSMENT

## INTRODUCTION

Our Penetration Testing services is extremely popular in Singapore & South East Asia. Commercial enterprises that extensively rely on online trading cannot undermine the importance of Cyber Security. Unless you deploy a proven measure to safeguard your sensitive data you can never know when hackers can malign their integrity.

Astonishingly, information and data security issues often remain overlooked and its responsibility is enshrined to the IT department. However, it can prove to be disastrous. Commercial enterprises need to realise that the impact of data security is one of the determining factors of long-term sustainability.

Information security is a niche area and calls for the assistance of specialised consultancy or if the organisation is large it may have a dedicated department for securing its informational resources. our Cyber Security Services can help you protect your mission-critical business data from insider threats and hackers.

## HOW IT WORKS

Our skilled computer experts will perform ethical hacking utilising programming skills to uncover vulnerabilities in your computer system.

In sharp contrast to ethical hackers who are bent on abusing these vulnerabilities for personal gain, ethical hackers can help you uncover them and recommend changes for strengthening the system.

Ethical hacking services provided under the supervision of skilled computer experts can keep your information and the systems involved safe.

### Phase 1 Information Gathering

- *Understanding the business objective*
- *Reviewing the types of system, network, and application*
- *Identifying the services or sensitive technical information*

### Phase 2 Vulnerability Identification

- *Ensure that all components of applications are analysed*
- *Performing manipulative, aggregation and interactive testing*

### Phase 3 Vulnerability Analysis

- *Analysis of vulnerabilities detected to identify the chances of exploitation*

CyberQuote
Financial Training
Information Technology

# PENETRATION TESTING

## INTRODUCTION

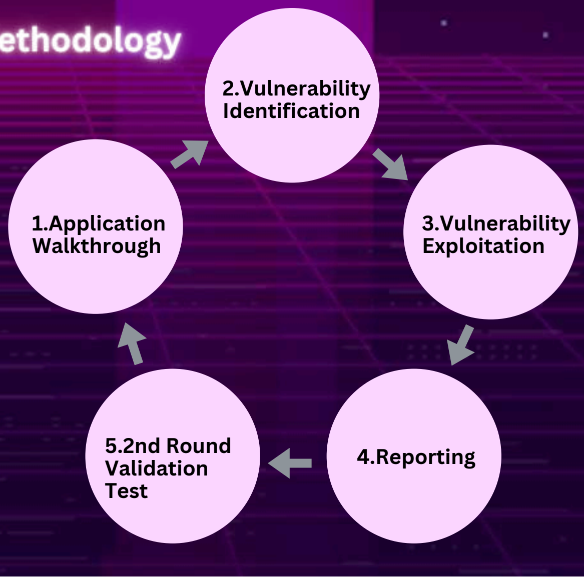
Today, most companies from small start-ups to international businesses see the importance of penetration testing.  Hazards from extremely refined hackers and cyber criminals mean that you cannot afford to be fully contented with your cyber security. As hackers are becoming increasingly proficient, business owners are also becoming increasingly concerned of system threats. One amongst the foremost vital tools that firms will use to defend themselves is penetration testing. Penetration testing is a cyber security skill that utilizes an equivalent technique as a criminal hacker to gain access to your IT systems. They use any methodology that a criminal would possibly use like parole cracking, viruses or maybe social engineering.

The usual case for businesses that run their own cyber security and in-house computer systems is that they seldom get a second opinion. Several business homeowners trust their IT professionals and believe that they have robust systems that are free from potential weaknesses. However, result of not obtaining a second professional opinion is that you may just be left with blind spots in your systems.

## HOW IT WORKS

Find any new vulnerabilities before hackers do. Have our ethical professionals conduct penetration tests on your system and have security gaps patched and sealed before hackers find them.

### Methodology


1.Application Walkthrough
2.Vulnerability Identification
3.Vulnerability Exploitation
4.Reporting
5.2nd Round Validation Test

CyberQuote
Financial Training
Information Technology

# PHISHING DRILL

## INTRODUCTION

Phishing drills are simulated exercises conducted to assess and enhance their resilience against phishing attacks. This is a deceptive technique where attackers attempt to trick individuals into divulging sensitive information, such as usernames, passwords, or financial details, by posing as trustworthy entities through fraudulent emails, messages, or websites. These drills help organisations educate their personnel, test their awareness, and evaluate the effectiveness of their defenses against these deceptive tactics.

The drills play a crucial role in building a human firewall within organisations. By regularly testing and refining employees' ability to recognise and resist phishing attempts, organisations can significantly reduce the risk of falling victim to real-world attacks. Additionally, these drills contribute to a culture of cybersecurity awareness and create an environment where employees are actively engaged in protecting the organisation's sensitive information.

## WE PROVIDE

- Email Phishing (Most Common)
- SMS Phishing
- Hybrid Phishing (Physical & Email)

CyberQuote
Financial Training
Information Technology

# CYBER-SAFEGUARD AWARENESS PROGRAMME

## INTRODUCTION

Commercial enterprises that rely extensively on their online databases cannot undermine the importance of Cyber Security. Unless you deploy a proven measure to safeguard sensitive data you will never know when hackers will attempt to access your information. Cyber-Safeguard Awareness Programme (C-SAP) training is essential for all corporate staff.

**This course includes the following:**

- E-Learning User Awareness
- Simulated Ethical Phishing Attack
- User Awareness Workshop
- Security Incident Updates

## FUNDING INFORMATION

**Contact us at support@cyberquote.com.sg**

## COURSE DURATION

***5 hours***

***This course contains assessments***
3 ***hour workshop,***
***1 hour e-learning***
1 ***hour phishing demonstration***

E-LEARNING USER AWARENESS

USER AWARENESS WORKSHOP

SECURITY INCIDENT UPDATES

CyberQuote
Financial Training
Information Technology

# SECURITY BASELINE CHECK & CONFIGURATION AUDIT

## INTRODUCTION

**Security baseline/configuration check refers to a compliance check of the configurations of operating systems, databases, software, and containers of a server against standard compliance setting. After that, stakeholders can harden the security of assessed assets, to reduce the risks of cyber attack, and meet the requirements for security compliance.**

## Some of the standards:

- ISO/IEC 27001:2013
- ISO/IEC 13335-1:2004
- ISO/IEC TR 15443-1:2005
- GB/Z 20986-2007
- ISACA
- CESG (CHECK) IT Health Check
- OWASP OWASP_Testing_Guide_v4
- OWASP OWASP_Top_10_2021

## Applicable targets:

- Server
- OS
- DB
- Firewall
- etc

CyberQuote

Financial Training
Information Technology

# SMART CONTRACT AUDIT

## INTRODUCTION

**A process of assessment on Blockchain smart code contract to identify security vulnerabilities and poor coding practices, and then come up with recommendations to remediate identified vulnerabilities. It can be either static audit on contract code, or dynamic audit to run contract on public chains to identify security issues.**

## KEY BENEFITS

- **Security Assurance:** Smart contract audit identifies and rectifies vulnerabilities, reducing the risk of fraud, or unauthorized financial transactions, etc.

- **Regulatory Compliance:** Smart contract audit ensures that smart contracts align with relevant regulations and compliance requirements.

- **Cost Efficiency:** Smart contract audit helps prevent financial losses due to vulnerabilities, saving resources in the long run.

- **Smooth Development:** A well-audited Smart Contract is less likely to encounter unexpected issues during deployment, minimizing downtime and ensuring a positive user experience.

CyberQuote

Financial Training
Information Technology

# CYBER SECURITY FORENSIC

## INTRODUCTION

Cybersecurity forensics serves as an invaluable tool in the ongoing battle against cyber threats, offering insights that enable organisations to fortify defenses, mitigate risks, and respond effectively to security incidents.

We leverage on advanced tools and techniques to collect, preserve, and analyse digital evidence. This evidence can span a wide range of sources, such as network logs, system configurations, and application data. The process involves scrutinising the digital landscape to reconstruct the sequence of events leading up to, during, and following the security incident.

The forensic examination seeks to answer critical questions, including how incidents occur, what vulnerabilities were exploited, and who may have been involved. This comprehensive approach aids in understanding the root causes of the incident and helps organisations enhance their security posture by implementing effective preventive measures.

## KEY BENEFITS

- Unveils the root cause of a security breach to prevent similar future breaches
- Postulate the motive behind the crime and identify the main culprit

CyberQuote

Financial Training
Information Technology

# RED TEAM DRILL EXERCISE

## INTRODUCTION

The term "red team" refers to a group of skilled cybersecurity professionals who simulate real-world cyber threats to evaluate the effectiveness of an organisation's defenses. The primary objective of a red team exercise is to identify vulnerabilities, weaknesses, and potential points of failure within the system, network, or overall cybersecurity infrastructure.

A red team cybersecurity drill is a comprehensive and proactive exercise designed to assess and enhance the security posture of an organisation.

We offer 2 types of exercise.

### Type 1 – Black Box Attack Drill

- **Objective:** Assess corporate's overall security defense against cyber attacks, to exploit defense loopholes by reconnaissance, phishing, and all kinds of cyber attack, etc.
- **Charge Mode:** Charge based on No. of detected vulnerabilities of different risk levels

### Type 2 – Script-Based Attack Drill

- **Objective:** Assess corporate's reaction/response/SOC against cyber attack.
- **Charge Mode:** Customised/to be negotiated by different case

CyberQuote
Financial Training
Information Technology

# DATA ASSET CARDING

## INTRODUCTION

**DAC is a process to sort data distribution and sensitive data use status by scanning, sniffing, traffic & log analysis, and data grading and classification. DAC helps customers with database discovery and sensitive data discovery in network, and classifies data assets according to its type and security classification, to achieve a targeted protection of sensitive data.**

## HOW IT WORKS

**Static carding:** DAC locates databases in current network environment. DAC searches database in its networks regularly to provides accurate basis for database security management.

**Dynamic carding:** DAC provides access to the popularity of the database, automatically monitors the sensitive data use status on the application side, operation side, and maintenance side, discovers data abuse, and provides the basis for core data security management and control

CQ
CyberQuote
Financial Training
Information Technology

# CONTACT US

cyberquote.com/sg/contact-us

support@cyberquote.com.sg

☎ + 65 6011 8921