

Beyond IT Security Training.
We Train Differently

Hacking and Security Vulnerability Management



We assess your digital asset to find vulnerability	Train you to fix	Secure your digital asset
What is the uniqueness?	How will you learn?	How will it benefit you?
Pre-training	During the training	Post-training
<p>Security Assessment with Analysis Report No other training providers did this before and we are the first! Prior to the training, our security engineers will conduct a security assessment and provide a security analysis report on your digital asset.</p> <p>Understand Your Digital Asset You will get a clear understanding on the security and the hidden risks of your digital assets.</p>	<p>Hands-on Session You will learn and improve your technical skills to test and secure your digital asset.</p> <p>Solution-Driven You will have the opportunity to focus and get professional consultation from trainer based on the challenges you face in the security analysis report on your digital asset.</p> <p>Live Hacking and Penetration Testing You will practice and sharpen your skills by applying it in live platforms.</p>	<p>Skills Application You will be able to understand and fix the vulnerabilities of your digital asset listed in the security analysis report.</p> <p>Master Information Security You will be able to master advanced techniques to secure and conduct security assessment on digital assets.</p>

Course Description

This training covers a broad domains of security topics including network security, web application security and mobile application security.

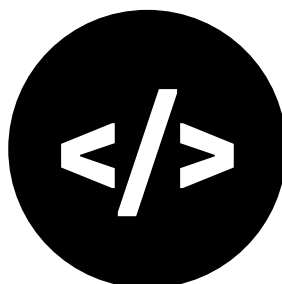
It begins by covering the basic concept of different security domain and move to the threats landscape and security assessment.

You will be able to assess the security posture of your digital assets and learn how to implement a defense-in-depth base on the findings.

This training is suitable for the industry newcomer or any IT professionals that would like to strengthen their knowledge and skills in these security domains.

Course Outline

- Web Application Arthitecture
- HTTP Basics
- Injection
- Cross Site Scripting (XSS)
- Cross Site Scripting Forgery (CSRF)
- Mastering Burp Suite
- File Inclusion Attacks
- Overview of Network Security
- Target Enumerations and Port
- Scanning
- Vulnerability Assessment
- Penetration Testing with Metasploit
- Sniffing
- Password Cracking
- Introduction to Android
- Android Arthitecture
- Android Security Model
- Android Application Assessment
- Automated Assessment with
- Drozzer
- Introduction to iOS
- iOS Security Model
- iOS Application Assessment
- iOS Application Cracking and Patching



Learning Outcomes

- Enable you to understand and demonstrate key concepts of information security
- Discover the security risks in different security domains
- Learn to perform vulnerability assessment and identify vulnerabilities of your digital assets
- Identify best practices that can be used to protect and enhance the security of your network, web application and mobile application
- Enable you to understand the types of security countermeasures available and how they should be applied

Duration

4 Days

Exam Details

Number of Questions: 50

Passing Score: 70%

Test Duration: 85 mins Exam + 5 mins NDA

Test Format: Multiple Choice

Test Delivery: PVTTC (Pearson VUE Test Center)

Exam Prefix: CZ 400



Who Should Attend

IT professionals, information security personnel,
network administrator, web application developer,
mobile application developers, penetration teater
and anyone who are responsible in
information security and data protection

Certified Information Security Specialist (CISS)



VISIONCORP
smart solutions for smart people

www.visioncorp.com.my
Tel: +6 03 7665 2021
Email: service@visioncorp.com.my