MICROWARE
Your Trusted Partner Since 1985

Course Title	Course Code
Internet of Things (IoT) lab (Onward)	**ITL-IOTL**

Background

HKSAR government promotes the innovation and information technology for secondary school. As it's high demands on how our society encourages Hong Kong teenagers to be the new force group in participation in the Information security industry sector. Security is critical to the success of businesses and Information technology and information security Industry adoption. The resilience of production processes strongly depends on the companies' awareness of the current threat landscape and the employed security framework for protecting against attacks. In Hong Kong, STEM education is promoted through Science, Technology and Mathematics Education. Hence, Technology is one of the important subjects for teenager to understand more about Cybersecurity. The introduction and fundamental knowledge of Cybersecurity definitively belongs to one of most important area that allow students and parent with additional considerations for the student's life planning within the study life of secondary school.

Intensive demand on IT professional

Due to international demand for information security professionals across educational institutes, NGO, Enterprises are high. How about if we can enable our Hong Kong teenager starting to look into one of the high demanding industries as one of the shortcuts to allow them to have earlier exposure on Information security. It can also validate the knowledge required for entry-level network security positions.

Source: Data Security Challenges 2021

According to the current report of (ISC)² (www.isc2.org) Cybersecurity Workforce Study 2020, the global Cybersecurity workforce is now in a shortage of 3.12 million professional.
Except for the mentioned APAC Countries, the United Kingdom is one of the countries in the world that focus on the development of teenagers' education in cyber security perspective. There is a scheme (CyberFirst) especially targeting age group 11-19 young peoples in order to develop the UK's next generation of cyber professionals through the student bursaries.

Young peoples in CyberFirst[2]

Apart from the CyberFirst schema, it's also has a competition targeting girls' sector, i.e. CyberFirst Girls Competition. It provides an interesting but challenging environment to inspire the next generation of young women to consider a career in cyber security.

Another organization, Youth Fed[3] is a youth charity that supports over 5,000 young people between the ages of 8 and 25, helping to improve the lives of young people through celebrating and delivering activities. We enable young people to thrive and achieve their full potential, regardless of background or circumstance. With the mission and vision that, promoting the Youth Fed Cyber Programme is an exciting initiative running in the North West of England.
The programme has two main focuses:
To inspire potential talent, creating a pipeline for the cyber security industry to respond to the skills gap.
To make people safer in the digital world.

The Cyber Programme is run from two fully equipped Security Operations Centre's (SOCs) – one based in Salford and one in Daresbury. At the SOCs, our Youth Fed operatives run a series of workshops starting with the Cyber Security Taster Session. Youth Fed with objectives are: To advance in life and help young people through the provision of recreational and curriculum enriching activities provided in the interest of social welfare, designed to improve their standard of living.

IT Innovation Lab

In Hong Kong, we do have a similar supporting scheme brought to us from the Hong Kong Government. The OGCIO of the Hong Kong government invites the majority of secondary schools to participate in the "IT Innovation Lab in Secondary Schools" [4] Programme. This schema aims to thereby promoting local popular science education and expanding the supply of innovation and technology talent and meet the needs of a technology-driven society.

Training courses providing

Our training course is teaching the teenagers understand what cybersecurity is. Though those cybersecurity related training courses, the students may raise their interest in cybersecurity related subjects in their tertiary education. By attending this course, secondary school could be much easier to promoting the aspects related to the cybersecurity. In order to allow more teenagers starting to understand what's cybersecurity about. It helps secondary school to enhance their students to participant worldwide cybersecurity competition and also increases their reputation so forth. Students may have chance to visit VTC (Cyber Range Security Lab) & HKIT (Cyber Security degree and diploma courses) or education seminar as well.

We are providing four courses that includes Introduction to CTF, Cybersecurity Essential, IoT security, IoT Lab (ONWARD).

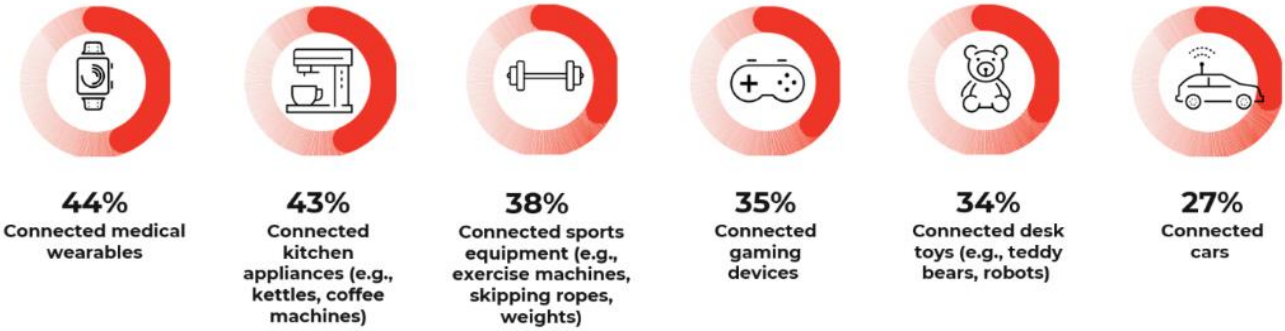
Courses Supporting Companies / Organizations

This course datasheet is about "**IoT Lab (Onward)**", for other courses please refer to correspondence course material.

****

What is IoT?
The Internet of Things (IoT) describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.
There is research result shown that are the strangest things connecting to corporate network. The top strangest connected devices respondents have seen on their networks are: Connected vehicles (27%) to connected toys (34%) and wearable medical devices (44%).

As everything becomes more connected, consumer IoT could easily become an entry route into industrial networks. Devices that employees innocently bring onto an organization's network are often not built with security in mind and can be easy gateways to a company's most important information and systems.



IoT is the soft underbelly of many businesses and an area they need to do more to protect. Failure to secure IoT poses a major threat to organisations. According to research conducted by Unit 42, well known security vendor threat intelligence research arm, 57% of IoT devices are vulnerable to attacks of medium to high severity. IoT is a business necessity that introduces risk: Massive increase in number of devices. Due to cheap IoT devices often shipped with vulnerabilities and difficult to patch yet have unfettered access.

Incredibly diverse devices: traditional IT security controls do not work. By 2022, IoT security attacks due to lack of insight into edge and third-party device providers will increase by 35%. Source: Gartner: Predicts 2019: Infrastructure Services. Updated on April 2020.

What we would like to promote is the Hong Kong young peoples' interest in Information technology especially in the aspect of Cyber security during their secondary schooling. Our teaching team is backed by multiple CTF international organizations such as Cyber Range training centre[6] trainer, Shenzen E-link(深圳易聆科), well-known industry in IT security service provider, Cyber Range training centre is the 1st education institute to introduce cybersecurity course by make use of blue team approach with defense technique. E-link is the experienced training institute that provides accredited training related to Information Security certificate of Mainland China Certified Information Security Professional (CISP). Onward Security is penetration testing and product security assessment solution provider. Onward stated that they are the only team in Taiwan who have done more than 200 network devices had been tested and 2,000+ vulnerabilities were discovered in the IoT, ICS/SCADA, automotive and medical devices. Their security assessment products specialize in evaluating and fulfil international standards to provide assurance for IoT product to reduce the possible vulnerabilities.

Cyber Range Training Centre[6]

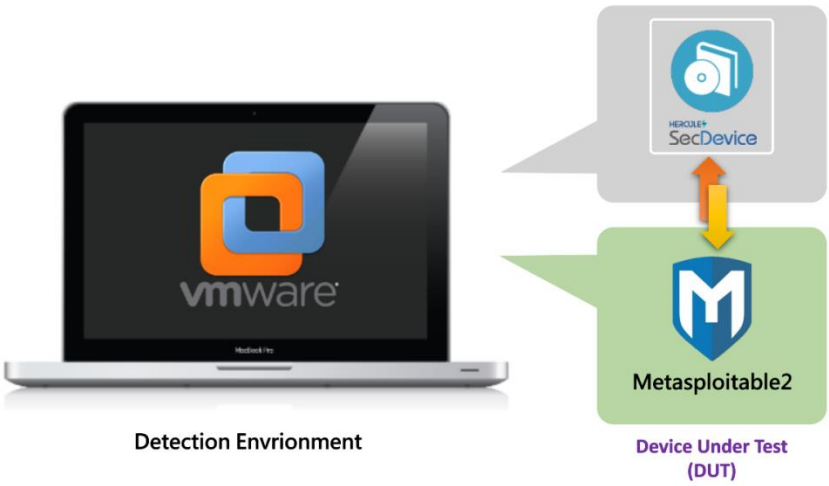
Course Objectives

In order to introduce what is IoT Lab, we will make use of this training course that helps you understand what IoT looks like, during the Cybersecurity training, secondary school students will be able to understand knowledge related to IoT devices especially with Hands on Lab exercises. This course is designed for students that are interested in validating comprehensive knowledge on current cybersecurity tenets.

What Can Be Learned

- Introduction to Basic network security
- What is IoT?
- Technique and Types of IoT.
- Fundamental of network security
- What is Wireless network security?
- Detection of vulnerability.
- Advanced Cybersecurity

Lab Class with equipment



The Internet of Things (IoT) device and basic operation concept on provided SecDevice. There are popular CTF challenge types related to Remote IoT that make use of SecDevie Hence, for the students who are interested in deeper study on how the IoT works in CTF, it's a good chance to have a more specific exposure of IoT. The IoT lab components consist of:

- SecDevice
- Metasploitable2

Upon this course, students will be able to demonstrate IoT & cybersecurity knowledge related to cyber security techniques in the manner of how to resolve technical problems with related lab components in hands-on exercises.

Further Study Path

After completing this course, students will be able to demonstrate basic IoT & cybersecurity knowledge related to cyber security techniques in the manner of how to resolve technical problems in Lab exercises. Students will be able to capable to participate further study on advance security topics, may be able to have higher chance to enroll VTC, University degree level courses.

Target Audience

- All young peoples that study in secondary school (recommended for F.3 to F.6 students)

Prerequisites

- Using Internet / email service experience
- A mobile smartphone with WIFI / internet connection, Notebook/Laptop for Lab lesson

Course Content Highlight

- Introduction to Basic Network Security - 2 lessons
  - Basic knowledge of network security
  - Network security detection concept
  - Network security detection methodology
- Detection of vulnerability - 4 lessons
  - Introduction to IoT security vulnerabilities
  - IoT vulnerability detection instructions
  - Case study
  - Test environment construction
  - Real machine operation
- Advanced Cybersecurity - 3 lessons
  - Test report interpretation
  - Vulnerability verification and misjudgment elimination
  - Vulnerability patching and security enhancement

Trainers

Frankie Leung
- CISSP, CISA, CISM, CRISC Certification holder
- Over 30 years' experience in IT, Security and Application Development

Paul Chow
- CISSP, CEH, OSWP Certification holder
- Over 30 years' experience in IT, Security and Application Development

Eric Moy
- CISSP, CEH, CISA, PRINCE2, ITIL and ISO20000 Certification holder
- Over 30 years' experience in IT, Security and Service Management

Michael Chow
- CISA, CISM, CRISC, PRINCE2 and ITIL Certification holder
- Over 20 years' experience in the Information technology and services industry.

Medium of Instruction
Cantonese (complemented with English terms) ***(English terms will be used where appropriate)***

Course format:

- 1 hour x 9 lessons (9 lessons classroom)
- Hands-on exercise (with IoT device and mobile device)
  - SecDevices, Metasploitable 2.

Key takeaway

- Completion certificate after passed dedicated assessments.

Class Size

10 persons per class

Award of Certificate

Candidates will be awarded four assessment certificates after they completed assessments.

Enquiries

Please call sales enquiry at (852) 2565-3030 or email to enquiry@microware.com.hk
Website: https://www.microware.com.hk/