CYBERSECURITY & DIGITAL FORENSICS COURSE MODULES

Mitigate cyber threats Singapore faces in our quest to be a smart nation. IT security professionals are in high demand to help Singapore succeed in this quest. With rapid growth in the area of Financial Technology, information security will be even more critical to protect our financial institutions, Join the fight against cybercrime with our Diploma in Cybersecurity & Digital Forensics (CSF).

In your first year, you will build a strong foundation in basic IT and security through modules such as Programming, Cyber Security Fundamentals, Front-end Development, Databases, Cryptography and Operating Systems Fundamentals.

In your second year, you will develop skills in the areas of network security, software security and digital forensics. You will learn to set up secure web servers, develop secure software applications and investigate cybercrimes. You will also learn how to secure codes and processes that go into developing applications, so that they are protected from external threats right from the start. This is called the Security Development Lifecycle, and is a highly valued skill in the industry.

In your final year, you will put your skills into practice by performing penetration tests on software, systems and networks, conducting in-depth forensic investigations on digital devices and networks, and analyzing malicious software or malware. You will get to do all these as well as work on information security projects in cutting-edge CSF labs.

What's more, you will attend masterclasses by information security professionals, and hone your skills in the real world with internships at the Ministry of Home Affairs and leading IT security organisations, such as Palo Alto Networks, SecureAge, Microsoft, NCS, CrimsonLogic, KPMG, Ernst & Young, CSIT and Ensign Infosecurity. You can also attain the highly sought-after CompTIA Security+ professional certification.

LEVEL 2.1

Fundamentals for IT Professionals II

This module gives a course-based experience in which students can engage with the local community and industry. This includes participation in community service events or in Service-Learning projects that leverage students' discipline knowledge and skills to meet identified needs. Through iterative and guided reflection on the service experience, students gain a broader appreciation of their discipline and an enhanced sense of personal voice, empathy and civic responsibility. Industry talks and seminars are organised to keep students up-to-date on emerging trends so as to build up their interpersonal, team and networking skills with the community and industry.

Networking Infrastructure

This module covers basic Local Area Network (LAN) and Wide Area Network (WAN) infrastructures including physical cabling systems used for an enterprise network, and how hardware platforms such as switches, routers and servers are deployed in typical networks. The module also introduces students to major networking protocols such as Ethernet, RIP, PPP, OSPF and HDLC, network operating systems and applications that run on LANs/WANs. Students will learn to configure switches and routers, and will be taught the techniques to configure and troubleshoot LANs and WANs.

Reverse Engineering Malware

This module trains students in reverse engineering malicious software using system and network monitoring tools, a disassembler, and a debugger. The module focuses on teaching students the essential assembly language concepts, along with the use of an assembly language emulator, a disassembler, and a debugger. These assembly language concepts and tools are needed to examine malicious code and understand its execution flow, identify common assembly-level patterns in malicious code, identify suspicious API calls, and to bypass defensive mechanisms of the malware.

Secure Software Development

This module provides students with the knowledge of the secure software development lifecycle. It trains students to incorporate security throughout the entire process of software development. With the knowledge gained from this module, students would be able to design, code, test and deploy software with a security mindset. The module begins with training students on how to identify, gather and record security requirements for a software. Students will learn

secure software design, where various security frameworks, considerations and methodologies are taught. Students will understand how software vulnerabilities can be exploited and how to address the risks. Students are trained to write secure code that is resilient against critical web application attacks. Finally, students are trained in secure software testing and how to securely deploy software.

World Issues: A Singapore Perspective^

This module develops a student's ability to think critically on world issues. Students will discuss a wide range of social, political and cultural issues from the Singapore perspective. It also looks at how city-state Singapore defied the odds and witnessed close to half a century of rapid economic growth, strong political ties and social harmony.

LEVEL 2.2

Data Structures & Algorithms

This module aims to provide students with the knowledge and skills to analyse, design, implement, tests and document programs involving data structures. It teaches basic data structures and algorithms within the conceptual framework of abstract data types. The emphasis here is to use the class feature of an Object-oriented language platform to give the concrete implementation of various abstract data types.

Digital Forensics

This module gives an insight into the process of forensics investigation. It covers the various types of computer related crimes, techniques of gathering electronic evidence, and the recovering of deleted, damaged or encrypted data. Students will also make use of advanced forensic tools to perform forensic investigation. Besides the tools and techniques of investigation, students will be taught sound forensic investigation methodology and the proper handling of evidence. The module will also cover aspects of law and policies applicable to digital forensics.

Malware Analysis Tools and Techniques

This module teaches a repeatable malware analysis methodology, which includes static analysis, code analysis, and behavioural analysis. Students are taught how to write a malware analysis report on a target malware. Students will be able to determine the malware's indicators of compromise needed to perform incident response triage. This module trains students to efficiently use network and system monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in an OS environment. Students are also trained to decrypt and analyse malicious script components of web pages, identify and examine the behaviour of malicious documents, and apply memory forensics techniques to analyse complex malware and rootkit infections. This module carries a pre-requisite: Reverse Engineering Malware (REM).

Server & Cloud Security

This module aims to teach students the concepts and knowledge related to securing web servers and cloud models. It covers topics such as how a web server is installed and optimized securely, the various methods of attacking web servers and the appropriate countermeasures. The specific tools used to test for vulnerabilities in web servers, their applications and databases will also be covered. Cloud security topics will cover introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS). Each of these delivery models presents an entirely separate set of security conditions to consider. An overview of security issues within each of these models will be covered with in-depth discussions of risks to consider.

Web Application Development

This module provides students with the knowledge and skills needed to develop web applications and web application protocol interface (API). Students will be introduced to an integrated development environment that will enable them to design and develop web applications and web API over the Internet. They will learn how to make use of web development technologies such as ASP.NET framework, jQuery for rich internet applications, data interchange formats such as JSON AJAX, source code version control systems such as GIT or SVN to develop effective web applications, and web API targeting both mobile web and unified web experience. This module aims to provide students with a good understanding of the web development architecture and service layer as well as the various issues related to Web Application Development.

Web Application Pen-Testing

This module provides a thorough understanding of major web application vulnerabilities and their potential impact on people and organisations. The module teaches a repeatable web pen-testing methodology, which includes reconnaissance, mapping, discovery, and exploitation of web application vulnerabilities and flaws. Students are taught how to write a web application pen-test report. The module teaches students the pen-tester's perspective of web applications. It trains students on building a profile of the machines that host the target web application and come up with a map of the web application's pages and features. Students are also trained in web application attack tools and interception proxies that are used to discover and exploit key web application vulnerabilities.

COURSE CURRICULUM

Module Name	Credit Units
YEAR 2	
Level 2.1 (22 hours per week)	
Career & Professional Preparation II	2
Fundamentals for IT Professionals II	2
Networking Infrastructure	4
Reverse Engineering Malware	4
Secure Software Development	4
Web Application Development#	4
World Issues: A Singapore Perspective ^	2
Level 1.2 (22 hours per week)	
Data Structures and Algorithms	4
Digital Forensics	4
Malware Analysis Tools and Techniques	4
Server & Cloud Security	4
Web Application Pen-Testing	4
Interdisciplinary Studies (IS) elective ^	2

Notes:

^ For more details on Interdisciplinary Studies (IS) electives, please log on to www.np.edu.sg/is/

IS Modules

The School of Interdisciplinary Studies (IS) delivers a broad-based curriculum, which nurtures a new generation of professionals with multidisciplinary skills and an innovative and entrepreneurial spirit to meet the challenges of a knowledge economy. IS offers both prescribed modules and electives to challenge boundaries. Prescribed modules develop students' competencies in core areas such as Communication, Innovation and Enterprise, Culture and Communication, and Personal Mastery and Development, while elective modules provide insights into Arts and Humanities, Business, Design, and Science and Technology.

The elective modules offered may change from year to year, depending on relevance and demand. They may also include modules available in other diplomas offered by the School.