

# Cybersecurity & Digital Forensics



**“With the current often borderless and constantly evolving nature of cyber threats, we believe that a new generation of highly skilled specialists is key to a secure future. With the lack of existing cyber security talents worldwide, courses such as this aim to bridge the gap by providing students with the expertise and opportunity to learn from thought leaders in the security industry, and be groomed as the next generation of leaders with cybersecurity knowledge and skills.”**

Stephan Neumeier  
Managing Director  
Kaspersky Lab Asia Pacific and Japan

Advanced persistent threat, ransomware and distributed denial of service attacks are things you will learn to understand. We will teach you about their workings and the potential damage they can cause. You will learn how to defend against them and acquire the professional skills to detect them when (not if) defences fail. In addition, you will learn the techniques to uncover hidden digital traces, analyse digital evidence, reconstruct a digital trail of events and unravel the mystery behind a cybercrime one byte at a time. The cyber world today needs highly trained professionals with a strong sense of righteousness and tenacity to give companies and organs of state a fighting chance against lurking hackers and criminals.

In the first year, you will master IT fundamentals that equip you with skills in areas such as software development, networking and data analytics. In your second year, you will acquire industry-specific competencies in areas such as network security, forensics in digital security and ethical hacking. You will learn how to conduct vulnerability assessments of computer and application systems, use ethical hacking tools and implement intrusion prevention solutions. In your final

year, you will be attached to local or overseas cyber security or forensics companies.

You will also gain hands-on training at the TP-IBM Security Operations Centre and the Temasek Advanced Learning, Nurturing & Testing Lab (a Cyber Range) set up in collaboration with the Ministry of Home Affairs.

You will attain sought-after professional certifications, such as the RedHat Certified System Administrator/Engineer (RHCSA/RHCE), Forensic Toolkit ACE, Palo Alto Networks (ACE) and Cellebrite Mobile Forensics Fundamentals. Upon graduating, you can pursue further studies through the Earn & Learn Programme to work and deepen your skills, or undertake a degree course.

## Career Opportunities

Our graduates have good employment opportunities with local and multinational businesses, governments, financial and banking institutions, and consulting firms as security penetration testers, security operations analysts, incident/forensic/threat investigators and IT security auditors.

## Graduation Requirements

Cumulative Grade Point Average : min 1.0

TP Fundamentals Subjects : 40 credit units

Diploma Subjects

Core Subjects : 72 credit units

Elective Subjects : min 8 credit units

Total Credit Units Completed : min 120 credit units

## Application

Apply during the Joint Admissions Exercise following the release of the GCE O Level results. For other categories of local applicants, please refer to the section on “Admission and Requirements”. For international students, please refer to the section on “Information for International Students”.

## Entry Requirements for Singapore-Cambridge GCE O Level Qualification Holders

To be eligible for consideration for admission, applicants must obtain 26 points or better for the net ELR2B2 aggregate score (i.e. English Language, 2 relevant subjects and best 2 other subjects, including CCA Bonus Points) and meet the minimum entry requirements of this course. CCA cannot be used to meet the minimum entry requirements.

For details on GCE O Level Minimum Entry Requirements, refer to page 214.

*Note: Applicants with complete colour vision deficiency are not eligible to apply for this course.*

## Course Structure

TP FUNDAMENTALS (TPFun) SUBJECTS				
SUBJECT CODE	SUBJECT	LEVEL	CREDIT UNITS	
CCS1006	Communication & Information Literacy	1	2	
CCS1007	Workplace Communication	1	2	
CCS1008	Persuasive Communication	1	2	
CGS1002	Global Studies	1	3	
CGS1003	Managing Diversity at Work*	1	3	
CGS1004	Global Citizenship & Community Development*	1	3	
CGS1005	Expressions of Culture*	1	3	
CIN1001	Innovation & Entrepreneurship	1	2	
GCC1001	Current Issues & Critical Thinking	1	2	
LEA1011	Leadership: Essential Attributes & Practice 1	1	1	
LEA1012	Leadership: Essential Attributes & Practice 2	1	1	
LEA1013	Leadership: Essential Attributes & Practice 3	1	1	
LSW1002	Sports & Wellness	1	2	
MCR1001	Career Readiness 1	1	1	
MCR1002	Career Readiness 2	1	1	
MCR1003	Career Readiness 3	1	1	
TGL1001	Guided Learning	1	3	
CSI3004	Student Internship Programme	3	16	

\* Students must choose one of these three subjects or TGL1001 Guided Learning.

## DIPLOMA SUBJECTS – CORE SUBJECTS

SUBJECT CODE	SUBJECT	LEVEL	CREDIT UNITS
CCF1C02	IT Systems Security Essentials	1	4
CIA1C06	Database Application Development	1	4
CIA1C07	Logic & Mathematics	1	3
CIA1C10	Data Analytics	1	4
CIT1C14	Data Structures & Algorithms	1	4
CIT1C18	Computational Thinking	1	4
CIT1C19	User Experience & Interface Design	1	3
CIT1C20	Coding & Development Project	1	4
CMC1C08	Network Technology	1	4
CCD2C03	Ethical Hacking & Intrusion Prevention	2	4
CCD2C04	Forensics in Digital Security	2	4
CCD2C05	IT Security Management & Audit	2	4
CCD2C06	Servers Administration & Security	2	4
CCD2C08	Secure Web Applications	2	4
CCF2C01	Network Security	2	4
CDF3C01	Incident Response & Management	3	4
CMP3602	Major Project	3	10

## DIPLOMA SUBJECTS – ELECTIVE SUBJECTS

SUBJECT CODE	SUBJECT	LEVEL	CREDIT UNITS
<u>Digital Forensics</u>			
CDF2C02	Digital Media Forensics	2	4
CDF2C04	Investigation Methodology & Techniques	2	4
CDF2C05	Application Forensics	2	4
CIG2C06	Data Security & Governance	2	4
<u>Enterprise Security</u>			
CCD2C09	Enterprise System Security & Assurance	2	4
CFI2C03	IT Project Management	2	4
CMC2P52	IoT Security & Privacy	2	4
CCD3C01	Security Technology & Innovation	3	4