Key Learning Outcomes for SG Cyber Odyssey

	Key Learning Outcomes		
Odyssey Stage	"Excite"	"Explore"	"Experience"
Target Audience	Pre-tertiary students with *no* cyber knowledge and may never heard of cybersecurity	Pre-tertiary students with *limited* cyber knowledge & curious to learn more	Pre-tertiary students with *some* cybersecurity knowledge; considering cyber as career/further career option
Focus	Overview	Blue Teaming	Red Teaming
Bloom's Level	Level 1 "Remember"	Level 2 "Understand"	Level 3 "Apply"
Examples of Activities	**School Assembly Talk, Visits to Companies**	**YCEP, Infocomm Club Activities**	**Advanced YCEP**
Typical Hands-on Exercises	Mobile device (most applicable and easiest to adapt in MOE schools)	Network Security (esp. WiFi)	Web App, IoT and Pent Testing (focus on HTML/Javascript)
Topics			
Fundamentals of Cybersecurity • Ethics • Identity & Access Management • Confidentiality, Integrity and Availability (CIA) • Cryptography • Career Prospects in Cybersecurity industry	**Cybersecurity Landscape** • Participants will develop an awareness of the global and local Cybersecurity and threat landscape **Job Prospects in Cybersecurity** • Participants will develop an understanding of the prospects of taking on a career in Cybersecurity, as well as be aware of the educational pathways to obtain the necessary skills and certification	**The Ethical Hacker** • Participants will develop an understanding of: 1. Ethical hacking and its implications 2. The relevant legislation behind ethical hacking (including Computer Misuse Act) **Understand Cybersecurity Job Roles** • Participants will develop an understanding of the job roles of various Cybersecurity professionals: 1. Cyber Risk Analyst 2. Security Penetration Tester 3. Forensic Investigation Manager	

	Basics of Authentication • Participants will: 1. Develop an awareness on the importance of strong credentials for authentication 2. Be able to implement strong passphrases to secure their online and offline accounts 3. Develop an understanding of the use of 2FA to secure critical transactions **Social Engineering** • Participants will develop an understanding of common Social Engineering and its associated attacks and preventive measures – Phishing/ Impersonation/Hoax. • Participant will develop an understanding of the principles of social engineering and their reasons for effectiveness: Authority/ Intimidation/Consensus/ Scarcity/ Familiarity/ Trust/ Urgency.	**Cybersecurity Essentials** • Participants will develop an understanding of: 1. The key principles behind Cybersecurity (e.g. CIA triad) 2. Cybersecurity and its associated terminologies 3. The differences between the various threat actors and their motivation (including script kiddies, cybercriminals, hacktivists and state actors) 4. Concept of Defense in Depth	**Cybersecurity Incident Management & Response Frameworks** • Participants will develop a basic understanding of: a. Need for Incident Response b. Stages of the Cybersecurity kill chain • Participants will develop a basic understanding of SIEM and use it to monitor incidents in a typical enterprise network

		Introduction to Cryptography • Participants will develop a broad level overview of the basics and use of cryptography. • Participants will be able to conduct a password brute force attack.	**Cryptography Fundamentals** • Participants will be able to: a. Describe basic cryptography concepts b. Understand difference between hashing, symmetric cryptographic algorithms and asymmetric cryptographic algorithms c. Use hashing and encryption to send/receive messages (e.g. using PGP)
Mobile Device Security	**Mobile Device Security** • Participants will: a. Develop basic understanding of common threats involving mobile computing devices (malware and use of mobile apps) b. Apply measures to prevent such attacks (update of App, OS, download only official App stores, backup of data, etc.)		**Mobile Device Security** • Participants will develop an understanding of and be able to perform basic penetration testing techniques such as: Rooting & Jailbreaking
Computer Networks & Network Security	**Networking Basics** • Participants will develop a broad, high-level overview of the structure of the Internet and how data is transmitted over networks. **Basics of Securing Wireless Networks** • Participants will develop an understanding of the workings of a	**Networking-in-depth** • Participants will develop a basic understanding of the following concepts: a. Network Protocols & Devices b. Network Access Control using MAC address c. VPN d. Security devices: IPS/IDS/Firewalls	**Network Reconnaissance** • Participants will develop an understanding on the use of the following: a. Protocol analyser b. Network scanners c. Wireless scanner/cracker

	wireless network and be able to secure wireless routers and access points, including MAC address filtering and WPA.	e. ARP and common network Man-In-The-Middle attacks	
Penetration Testing		**Introduction to Penetration Testing** • Participants will develop an understanding of the types of penetration testing and the ethics and legality issues of penetration testing.	**Penetration Testing Fundamentals** • Participants will be able to use common open source Pent Test tools (e.g. Metasploit) to perform penetration testing, such as SQL injection, water-hole attacks, buffer overflow, typo-squatting and ARP poisoning.
Web Technologies & Scripting			**JavaScript** • Participants will be able to: a. Understand the fundamentals of JavaScript b. Understand the use of and code with variables, constants, types, objects, arrays, functions, operators and control flows
			HTML • Participants will be able to: a. Understand the function and uses of HTML b. Understand the use of and code with block level and inline elements, simple frames and tables c. Understand the use of and code a simple HTML form

Computers, Operating Systems Internet of Things (IoT) devices, Threats & Malware	**Understanding Computers & Threats** • Participants will develop an understanding of: a. The anatomy of a computer and how a computer functions (CPU, RAM, Storage, Network Adapters) The common threats involving computing devices (eg. viruses and malware)	**Basics of Malware** • Participants will gain an understanding of the pathology of various types of malwares such as: a. Viruses, Worms, Trojans b. Ransomware c. Rootkits, Adware, Spyware, and Keyloggers d. Bots & Botnets	
		Operating Systems – Linux • Participants will be able to operate the Linux OS and perform command line functions such as: a. Basic Linux commands b. Files & Directories c. Users & Permissions d. Remote Access (e.g. SSH) e. File Security f. Scripting g. Processes h. User & Group Administration i. Web & File Service Protocols	**Operating Systems – Windows** • Participants will gain an understanding of the following Windows OS operations: a. Windows Server b. Windows Workgroup c. Windows Processes & Registry d. Windows PowerShell e. Files & Directories f. Users & Permissions
		Securing IoT Devices & Networks • Participants will gain an understanding of the pathology of common IoT attacks (such as DoS). • Participants will gain an understanding on how Cybersecurity principles can be applied to secure IoT devices and networks.	

Open-Source Intelligence (OSINT)		**OSINT** Participants will gain an understanding on gathering information and using publicly available sources such as: a. Search engines b. Social media accounts c. Metadata d. Geolocation	