SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
TECHNICAL SKILLS & COMPETENCIES (TSC) REFERENCE DOCUMENT

TSC Category	Operations and User Support					
TSC Title	Threat Analysis and Defence					
TSC Description	Enable and conduct analysis of malicious threats, to examine their characteristics, behaviours, capabilities, intent and interactions with the environment as well as the development of defence and mitigation strategies and techniques to effectively combat such threats					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			ICT-OUS-3014-1.1	**ICT-OUS-4014-1.1**	**ICT-OUS-5014-1.1**	**ICT-OUS-6014-1.1**
			Perform static, dynamic or behavioural analysis on malicious codes and threats, debug malware and thwart malicious attacks	Examine malicious threat behaviour and capabilities, and circumvent anti-analysis mechanisms, recommending techniques to block malicious code and attacks	Establish an enterprise threat defence and mitigation strategy, incorporating new techniques to combat threats and attacks	Re-define analysis and defence strategies, techniques and tactics to combat new types and sources of threats and attacks.
Knowledge			• Types of threats or malware • Patterns of common malware characteristics • Mechanism of malware • Various file formats of malicious threat types • Programming languages which malware are created from • Types and usage of static, dynamic and behavioural analysis tools • Types and usage of anti-malware tools	• New and emerging threats • Range of malware analysis techniques • Core concepts for reverse-engineering malware at the code level • Anti-analysis mechanism in anti-disassembly, anti-debugging and obfuscations mechanisms • Techniques to circumvent anti-analysis mechanisms • Malware defence techniques	• Industry developments and trends in threat analysis and defence • New and emerging techniques in threat analysis • Different enterprise threat mitigation strategies, approaches and critical considerations	• Long term trends and evolution in the types and perpetrators of threats and attacks • Principles underlying threat defence and analysis strategies and methodologies
Abilities			• Create a safe hostile-code analysis environment • Correlate stages, actions or malicious commands in an attack • Perform static and dynamic analysis of malicious code and executables	• Use a combination of dynamic analysis techniques and reverse engineering techniques to determine threat characteristics and capabilities • Identify emerging and complex threats from	• Establish alliances with broader communities to keep updated on new and emerging threats, attacks and anti-detection mechanisms • Verify threat analysis outcomes and reports • Establish the organisation threat	• Chart direction to anticipate evolution of cybersecurity threats and attacks in the operating environment • Employ new methods or tools to analyse malicious software and attacks

			• Utilise behavioural analysis tools to understand the nature of the threat • Debug malware with debuggers and monitoring tools to gather information on malware • Document specimen's attack capabilities, propagation characteristics and threat signatures • Draft recommendations to mitigate malware, exploit kits and attacks • Use anti-malware and threat gateways to thwart malicious attacks	malicious software and codes • Conduct in-depth examination of malicious threats to understand the behaviour, capabilities, intent and interactions with the environment • Apply countermeasures to circumvent or subvert anti-analysis mechanisms • Unpack protected malicious executables • Recommend proactive steps to combat and mitigate malicious code, threats and attacks • Modify existing techniques or develop new ways to block malicious code and attacks	protection and defence strategy, balancing protection, capability, cost and performance	• Re-define threat defence techniques to combat emerging or new kinds of attacks
Range of Application	Threats may include but are not limited to: • Attacks (Buffer overflow) • Exploit kits (Sweet Orange; Nuclear; Neutrino; Fiesta; HanJuan; Angler) • Malware (Worm; Trojan dropper; Trojans; Rootkits; Remote Access Trojan; Rouge scanners; Ransomware; Point of Sale Infostealers; DNS hijacker; Distributed Denial of Service; Browser hijacker; Botnets) • Mobile (SMS Trojan; Mobile spyware; Mobile PUP; Mobile ransomware; Mobile Bank Trojan)					