TIME	ITEMS		
	PRESENTATION AREA	**CHALLENGE AREA**	**BOOTH AREA**
1030-1130	Sharing on Career Upskilling by SSG *Discover Insights, Skills in Demand and Job Opportunities in Generative AI*	Singapore AI Safety Red Teaming Challenge (led by IMDA)	**Booths to be manned from 1000 – 1730** Booth 1 (GovTech) Prompt Injection mini CTF Challenge Booth 2 (IMDA) Moonshot Demo Booth 3 (SSG) Sharing of Skillsfuture Initiative Booth 4 (RedAlpha) Sharing on Cybersecurity Training and Development Programmes
1130-1200	Sharing by Dreadnode, SG AI CTF Vendor *Title Behind the scenes of creating AI CTF challenges*		
1200-1230	*Sharing by GovTech's Young Talent Programme Office*		
1230-1330	**LUNCH BREAK**		
1330-1400	Proposed CSG AI Security Presentation *Title Actionable Insights on AI Security: Risks, Controls, and Tools*	Singapore AI CTF (led by GovTech)	
1400-1500	Sharing on Career Upskilling by SSG *Discover Insights, Skills in Demand and Job Opportunities in Generative AI*		
1500-1530	Sharing by Dreadnode, SG AI CTF Vendor *Title Behind the scenes of creating AI CTF challenges*		
1530-1645	Sharing on navigating career transition into tech by WSG *Title: Planning your Career Transition into Tech*		
1645-1730	WSG Networking Session		
1730-1740	Guests Invited to take their seats	**END OF CTF**	**BOOTHS CLOSE**
1740-1750	Opening address by SMS		
1750-1810	Award Presentation to Top Teams		
1810-1830	Photo-taking and Networking		
	END OF EVENT		

Presentation Area (Talks and Synopsis) (1030-1830)			
	Item	**Title**	**Synopsis/Details**
Session 1: 1030–1130 Session 2: 1400-1500	Sharing on upskilling initiatives by SSG	**Discover Insights, Skills in Demand and Job Opportunities in Generative AI**	To educate the audience on the impact, tools, risks, and opportunities of Generative AI (GenAI) and its implications for the workforce. The workshop content is categorised into three sections: **1. Market Overview** • Define Artificial Intelligence • Introduce Generative AI and its applications in daily life • Examples of popular GenAI tools (e.g., ChatGPT, DALL-E) • Discuss potential risks such as misinformation and data privacy concerns • Provide guidelines for staying safe in a GenAI world **2. Impact on Jobs and Skills** • Highlight the rising demand for GenAI-related courses • Identify in-demand skills and job roles in the GenAI • Example of an in-demand job role related to GenAI (e.g. data analyst) **3. Realise Your Potential – Take the Next Steps Forward** • Introduce the SkillsFuture Career Transition Programme (SCTP) • Discuss critical core skills necessary for success in GenAI roles • Share career and skills resources for job seekers and professionals • Additional reading materials for deeper insights into GenAI

Presentation Area (Talks and Synopsis) (1030-1830)			
	Item	**Title**	**Synopsis/Details**
Session 1: 1130-1200 Session 2: 1500-1530	**Sharing by Dreadnode on CTF**	**Behind the scenes of creating AI CTF challenges**	Dreadnode, the vendor for Singapore AI CTF, will share the behind-the-scenes process of creating AI CTF challenges. The presentation will begin with the motivation, delve into technical details, and discuss lessons learnt from hosting and creating challenges for major cybersecurity events such as DEFCON and Black Hat. 1. Why AI CTF? a. How AI CTFs differs from traditional CTFs b. How AI challenges raise awareness of AI vulnerabilities 2. Choice of AI Domains a. Selection criteria for domains such as Prompt Injection, Model Fingerprinting, and Model Inversion b. Strategies for making challenges accessible 3. Storyboarding and Gamification a. Designing engaging narratives without compromising realism b. Methods to enhance participant engagement 4. Challenge Engineering Process a. Translating ideas into technical challenges b. Avoiding unintended vulnerabilities in challenges c. Designing anti-cheat mechanisms 5. Testing, Validation, and Launch a. Internal testing procedures b. Metrics for success 6. Lessons Learnt from Conducting CTFs a. Reflections on creating and hosting CTF challenges at international cybersecurity conferences (e.g., Black Hat, DEFCON) b. AI and cybersecurity trends shaping future challenges

Presentation Area (Talks and Synopsis) (1030-1830)			
	Item	**Title**	**Synopsis/Details**
1200-1230	**Sharing by GovTech POD on talent engagement programmes**	**Sharing by GovTech's Young Talent Programme Office**	The sharing will introduce GovTech and the talent engagement programmes by GovTech's Young Talent Programme Office. 1. A brief introduction to GovTech (e.g. featured projects, ABC values, life inside Govtech) 2. Young Talent programmes – Internship, GeekOut, TAP and Scholarships.
1330 –1400	**Proposed CSG AI Security Presentation**	**Actionable Insights on AI Security: Risks, Controls, and Tools**	CSG will present actionable insights derived from its efforts to ensure the confidentiality, integrity, and availability of Large Language Model (LLM) applications. These efforts include the following: 1. **AI red teaming project**, which pre-emptively identify risks in adversarial machine learning. This initiative provides assurance to the Government on the security of its LLM applications. 2. **Cybersecurity Playbook for Large Language Model Applications**, offering practical guidance to Agencies on securely procuring, developing (including training and fine-tuning), deploying (including integration), and using LLM applications. 3. **AI guardrails validation project**, which validates methods to benchmark and protect LLM applications against specific cybersecurity threats.

Presentation Area (Talks and Synopsis) (1030-1830)			
	Item	**Title**	**Synopsis/Details**
1530 –1730	**Sharing on navigating career transition into tech**	**Planning your Career Transition into Tech**	This comprehensive session is designed to equip participants with the knowledge and tools necessary to navigate the dynamic landscape of ICT careers. **1. Planning Your Career Transition into Tech** Understand ICT Career Paths and Industry Trends • Gain awareness of ICT career pathways, job opportunities, reskilling options • Gain awareness of the impact industry trends have on ICT job roles and career pathways **2. Planning Your Career Development in Tech** • Develop your own career development plan • Take actions towards your career aspirations **3. Fireside Chat with industry experts from the Cybersecurity sector** • Gain clarity of self, circumstances and career aspirations • Explore available resources and support for individuals transitioning into tech **Group Photo-taking & Survey Dissemination** **Networking Session**

Challenge Area (0830-1730)		
Time	**Challenge**	**Synopsis**
0830-1230	**Singapore AI Safety Red Teaming Challenge (led by IMDA)**	The Singapore AI Safety Red Teaming Challenge will feature teams conducting red teaming for regional safety harms. The teams will comprise domain experts (e.g., cultural experts, linguists) from up to 10 countries across Asia. These domain experts will be selected by our partner institutes from the various countries*. Prior to the red teaming challenge on 5 Nov, there will be training workshops to familiarise participants with the red teaming platform. This is the first time that IMDA is organising such a red teaming challenge, which will build capability to support future safety evaluations. ** China (Beijing Academy of AI), India (IIT Madras), Japan (University of Tokyo/Japan AI Safety Institute), Korea (Naver AI Lab), Indonesia (Center for Digital Society), Philippines (Center for AI Research), Thailand (Electronic Transactions Development Agency), Vietnam (Hanoi University of Science and Technology), Singapore (AI Singapore).*
1330-1730	**Singapore AI CTF (led by GovTech)**	The Singapore AI CTF provides open challenges designed for security professionals and data scientists to learn about AI security in a competitive setting. The qualifying competition comprises 10 challenges of easy/medium difficulty across 7 domains (data analysis, model extraction, model fingerprinting, prompt injection, adversarial AI images, Adversarial Audio Generation and Model Inversion). Local and international teams will compete to solve these challenges in a virtual round held on 26 Oct 2024. The final round of the CTF comprises 8 challenges and will be held in hybrid format (both virtually and physically at MBS) on 5 Nov 2024.

Booth Area (Booths to be manned from 1000-1730)			
	Organiser	**Booth**	**Synopsis**
Booth 1	GovTech	**Prompt Injection mini CTF Challenge**	Participants can try a mini CTF challenge inspired by one of the challenges in the Preliminary round of the Singapore AI CTF. The goal of participants is to make an LLM reveal the ‘flag’ – in the form of a secret password. The purpose of the prompt injection challenge is to spread awareness of potential AI safety risks and remind public not to share sensitive information with LLM models.
Booth 2	IMDA	**Moonshot Demo**	Participants can view a demo of Project Moonshot. Project Moonshot reflects Singapore's commitment to addressing Artificial Intelligence (AI) risks through principled approaches, practical tools, and inclusive international engagement. It is one of the world’s first open-sourced tools to bring red-teaming, benchmarking, and baseline testing together in an easy-to-use platform – testament to Singapore’s commitment to harnessing the power of the global open-source community in addressing AI risks. The booth will demo the open beta Project Moonshot, which aims to provide intuitive results of the quality and safety of a model or application in an easily understood manner, even for a non-technical user. It was developed through working with partners such DataRobot, IBM, Singtel, and Temasek to ensure that the tool is useful and aligned with industry needs.
Booth 3	SSG	**Sharing of Skillsfuture Initiatives**	Participants will learn about SSG’s initiatives and resources, e.g. Skills and Training Advisory services (1 to 1 personalised advisory). SSG also aims to encourage the participants to sign up for virtual sessions, RIASEC profiling tool to identify their interests and SkillsFuture credit.
Booth 4	RedAlpha (Partner of WSG)	**Sharing on Cybersecurity Training and Development Programmes**	The booth by RedAlpha aims to share their full-time cybersecurity training programmes, targeting mid-careerists from non-technical disciplines for a full-time cybersecurity career.