WORLDSKILLS SINGAPORE 2025
TECHNICAL DESCRIPTION
CYBER SECURITY

Skill Competition

1. This competition includes the seven categories of cyber security functions as defined in the NIST NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework. (SP 800-181)

2. Conducted as a 2-person team event, competitors are given 24 hours over 3 days to complete the Test Projects for this competition.

Scope of Work

3. Competitors should be able to perform some of the roles as listed within the knowledge, skills and abilities adapted from the seven (7) categories stated in the NIST NICE Cybersecurity Workforce Framework:

   3.1. **Design and Development (DD)** – To design, develop and test secure technology systems, including on perimeter and cloud-based networks.

   3.2. **Implementation and Operation (IO)** – To provide implementation, administration, configuration, operation, and maintaining technology systems securely by way of handling daily operations, system updates, and user management.

   3.3. **Oversee and Governance (OG)** - To provide support, management, or development and advocacy so the organization may effectively conduct cybersecurity work.

   3.4. **Protect and Defend (PD)** - To protect against, identify and analyze risks to technology systems or networks. Includes investigation of cybersecurity events or attacks related to technology systems and networks.
   a) Perform vulnerability assessment and audit;
   b) Handle incidents via CSOC effectively.

   3.5. **Cybersecurity Intelligence (CI)** – To collect, process, analyse, and disseminate information regarding potential or existing cyber threats.

   3.6. **Cybersecurity Effects (CE)** – To plan, support and executes cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

WORLDSKILLS SINGAPORE 2025
TECHNICAL DESCRIPTION
CYBER SECURITY

3.7. **Investigation (IN)** - To conduct cybersecurity and cybercrime investigations, including the collection, management and analysis of digital evidence.

4. Competitors must also have a basic knowledge and understanding of cyber security in connection with information technology (IT) in the workplace (according to the NIST NICE Cybersecurity Workforce Framework).

5. Competitors will be expected to have relevant technical skills that enable them to set up, configure, operate, maintain, and manage servers, networks, and their firewalls, including hardware (e.g., Windows servers hosting network services, Windows clients. switches, routers, firewall) to support the security of information and information systems (please refer to industry certifications listed under point (5) above).

6. Competitors will be expected to have relevant technical skills that enable them to manage users' account, configure firewall rules, and updates OS and security patches. They are responsible for access control, passwords, and account creation and administration.

7. Competitors must be resourceful and able to work and collaborate in a team of 2 members. They may be presented with several cybersecurity-related problems that may not be fully defined.

Simulation and Scenario

8. The competition scenario may require the competitors to set up, install, configure, and harden computers, servers, firewalls, networking equipment, and associated software to meet the typical tasks of a network and systems security technician/consultant.

9. The competition scenario will be divided into three distinct tasks to be carried out over a spread of three (3) days of the competition:

9.1. Infrastructure Security Hardening and Vulnerability Assessment
9.2. Governance, Cybersecurity Incident Response, Digital Forensic Investigations and Application Security
9.3. Capture-The-Flag (CTF) Challenge.

WORLDSKILLS SINGAPORE 2025
TECHNICAL DESCRIPTION
CYBER SECURITY

10. Competitors will be assessed based on measurement (objective) marking only.

11. The assessment criteria and relative weighting of marks are as follows:

Criterion		Marks
A	Enterprise network, System protection and Oversees and Governance (PR, OV)	11.00
B	Securing Network Infrastructure (IO)	11.00
C	Linux and Windows (DD)	11.00
D	Oversee and Governance (OG)	3.00
E	Cybersecurity Intelligence (CI)	16.00
F	Investigation (IN, PR)	16.00
G	Cybersecurity Effects (CE)	16.00
H	Defend (IN, PR)	16.00
	Total	**100**

Major Tools & Materials

12. The following tools and materials will be used in the competition:

12.1. Materials

The following materials will be supplied to each competitor in the competition:

- Stationary for documentation purposes; and
- Consumables where required for the project(s).

12.2. Equipment

For hardware and software required, please refer to the hardware and software equipment list in ***Annex A – Infrastructure equipment list***.

WORLDSKILLS SINGAPORE 2025
TECHNICAL DESCRIPTION
CYBER SECURITY

Annex A – Infrastructure equipment list

The equipment used during the competition might include the following. Please note that the equipment is subject to change.

- Network switches CISCO 2960 (IOS version 15 or above)
- Router (with security feature) CISCO 1941
- NIDS/NIPS
- Wireshark
- Vulnerability scanners (Nessus)
- Nmap
- Kali Linux (Kernel 4.15.0 and above)
- Splunk Enterprise (9.0 and above)
- Web application firewall
- Microsoft Server OS (2012 R2 and above)
- Microsoft Active Directory
- Microsoft Remote Access Services
- Active Directory Certificate Services
- Linux Operating System (Kali / Ubuntu Desktop / CENTOS (22.04 and above)
- Windows Operating System
- MySQL
- IDA Free
- Radare (In Sandbox)
- OllyDbg / x64dbg
- Volatility (in Kali)
- Autopsy (in Kali)
- OSSEC
- VMWare
- Web Services
- FTP Services
- Digital Forensics tools (with features similar to Proof Finder)
- Putty
- Puttygen
- Bash (4.4 and above)
- Openssh-server_7.2p2-4ubuntu2.4_
- Openssh-server_7.2p2-4ubuntu2.4_