Cyber Security

Purpose: To evaluate each contestant's preparation for employment and to recognize outstanding students for excellence and professionalism with relation to the entry level skills within the field of Cyber Security.

Contest Location	▪ B-Hall ** Contest in A, B, C or D Hall will not be able to leave for lunch, please select "Contestant Plus" when registering or having contestant prepared to purchase lunch with credit card at vendors in the Exhibit Hall.
Special Notes	▪ Exhibit Halls do not open to observers until 12:00 pm. ▪ The contest is designed around Outcome and Competencies from the Career Field Technical Content Standards for Cybersecurity as defined by the Ohio Department of Education. These can be found at http://education.ohio.gov/getattachment/Topics/Career-Tech/Information-Technology-Career-Field/IT_Standards_No-DOK-20180810.pdf.aspx?lang=en-US. ▪ The following will not be tolerated and are grounds for disqualification from competition. o No smart watches and/or phones are permitted during the contest and/or in contest o No contact with anyone outside of the contest area once the contest begins o No inappropriate communication between contestants such as verbally degrading another contest o No cheating on any portion of the contest such as informing another contestant of the skills/test prior to competing.
Testing	▪ There will be a written knowledge test.
Eligibility	▪ Open to active Career Technical Student Organization students (Team of 2) enrolled in Cyber Security, Information Security, or System and Networking Security as the occupation objective.
Clothing	Class E: Contest specific – Business Casual ▪ Official SkillsUSA white polo shirt. ▪ Black dress slacks (accompanied by black dress socks or black or skin-tone seamless hose) or black dress skirt (knee-length, accompanied by black or skin-tone seamless hose). **OR**

	Men – Official red blazer, jacket, sweater; black dress slacks; white dress shirt; plain black tie with no pattern or SkillsUSA black tie; black socks and black dress shoes Woman – Official red blazer, jacket or sweater; black dress skirt (knee length) or slacks with businesslike white, collarless blouse or white blouse with small, plain collar that may not extend onto the lapels of the blazer; black sheer or skin-tone seamless hose and black dress shoes.
Provided by Contestant **(Tool List)**	▪ Hard copy of one (1) page personal resume ▪ Laptop computer ▪ Modern Web Browser (Firefox recommended) o Must be able to access the URL https://sandbox02.cech.uc.edu/vac and allow pop-ups for this site.
Competition Standards **(Not all will be tested but contestant should be knowledge of all)**	Please refer to the National Technical Standards
Resume	▪ In conjunction with National Standards, violations may result in student loss of contest. ▪ All SkillsUSA Ohio State Championship Contest will require a short interview component. Students should be prepared with basic job interview skills.

Equipment and Materials - Provided by the OCRI:

- All reference materials, diagrams, instructions will be provided.
- Access to virtual machines and software required to complete challenges in the contest will be provided. Participants should familiarize themselves with the following software and platforms.
- The Ohio Cyber Range (Training will be provided).
- Windows 10 & Server 2019
- Linux OSes (Kali and Ubuntu)
- Pfsense (Open Source Security OS https://www.pfsense.org/)
- Cisco Packet Tracer (Free download and training can be obtained here https://www.netacad.com/courses/packet-tracer)
- Wireshark (https://www.wireshark.org/)

Scope of the Contest

The contest is designed around Outcome and Competencies from the Career Field Technical Content Standards for Cybersecurity as defined by the Ohio Department of Education. These can be found at http://education.ohio.gov/getattachment/Topics/Career-Tech/Information-Technology-Career-Field/IT_Standards_No-DOK-20180810.pdf.aspx?lang=en-US.

The contest is focused on skills performance and consists of several scenario-based challenges requiring the provisioning, testing, deployment, configuration, maintenance, protection and defensive procedures with the end goals set by the technical committee.

Contestants must successfully complete assigned tasks at a number of independent virtual activity stations. The challenges are designed based on recommended best practices of the industry. Approximately 45 minutes are allowed at each station.

Contestants may complete the stations in any order they choose. Students are not required to complete all tasks in each scenario. Some tasks may have several steps that may have dependences or be judged independently. Points will be awarded for tasks and steps that are completed successfully. Scores from each station will be combined. Contestants must complete all tasks on their own without the use of outside resources. Some reference materials will be provided.

Contest Domains – End-Point Security

Given a scenario, contestants will apply knowledge of industry standard processes and procedures to secure a stand-alone workstation running Windows 10. Contestants will be asked to perform tasks in some or all the following areas:

1. Local user management
2. Access Control
3. Password policy management
4. Local user and computer policy management
5. Mange security services
6. Manage installed software and services
7. Malicious software removal

Secure Networking

Given a scenario, contestants will apply knowledge of security related activities and configurations to setup a secure network with both layer 2 and layer 3 devices. Cisco packet tracer will serve as a simulation platform. Contestants will be asked to perform tasks in some or all the following areas:

1. Configure switch/router security
2. Network segmentation
3. Mange port security
4. Access control lists
5. Establish secure connect to devices management environment

Server Hardening

Given a scenario, contestants will apply knowledge of industry standard processes and procedures to secure an Active Directory domain server running Windows Server 2019. Contestants will be asked to perform tasks in some or all the following areas:

1. User and group management
2. Apply appropriate role-based permissions, ACLs, and rights to network users and groups
3. Configure server security logging and auditing
4. Apply Group Policy
5. Secure network services and ports

Network Perimeter Security

Given a scenario, contestants will apply knowledge of network perimeter security to configure typical boundary devices and services. Pfsense will serve as the platform to configure effective network zones and edge security systems. Contestants will be asked to perform tasks in some or all of the following areas:

1. Configure device management security
2. Configure firewall rules to create a three-homed boundary between three network zones with different security levels.
3. Configure NAT and/or port forwarding
4. Create a VPN connection
5. Configure IPSec

Forensics

Given a scenario, contestants will apply knowledge of forensics activities associated with Incident Response Actions. Contestants will collect and analyze information from a variety of sources to identify and report events that have occurred on a system. Contestants will be asked to perform tasks in some or all of the following areas:

1. Packet (PCAP) analysis
2. Log analysis
3. Collect, process, and preserve computer-related evidence.

Pen Testing

Given a scenario, contestants will apply knowledge and skills related to the process of penetration testing. Contestants will plan, prepare, and execute tests of systems in order to identify, report, and/or exploit vulnerabilities in a system or network. Contestants will be asked to perform tasks in some or all of the following areas:

1. Port Scanning
2. Vulnerability Scanning
3. Packet capture (Man in the Middle)
4. Network discover (enumeration)
5. Perform a (TBD) attack
6. Exploit a known vulnerability to exfiltrate data (flag) from remote system
7. Establish a persistence in a compromised network or device.