James Clemens High School
11307 County Line Road
Madison, Alabama 35756
Cybersecurity II

Cybersecurity II

Course Description

Cybersecurity II is aimed at providing students with an in-depth look into what it means to be a cybersecurity professional. Emphasis is placed on best practices for secure networking and computing, along with other practical exercises for developing security standards that govern organizational compliance, risk management, access control, and identity management. Students will have the opportunity to prepare for a core industry standard certification exam related to security and can use these techniques, tools, and methodologies to prepare for a career within the cybersecurity field.

Career and Technical Student Organizations are integral, co-curricular components of each career and technical education course. These organizations enhance classroom instruction while helping students to develop leadership abilities, expand workplace-readiness skills, and access opportunities for personal and professional growth. Students in the Information Technology cluster affiliate with SkillsUSA and/or TSA.

Foundational standards, shown in the table below, are an important part of every course. Through these standards, students learn and apply safety concepts, explore career opportunities and requirements, practice the skills needed to succeed in the workplace, develop leadership qualities and take advantage of the opportunities afforded by Career and Technical Student Organizations (CTSOs), and learn and practice essential digital literacy skills. The foundational standards are to be incorporated throughout the course.

Pre-requisites

Cybersecurity I

Instructional Delivery Plan *Students will:*

1. Learn and use standard safety practices.
2. Participate in a virtual design challenge
3. Study/take an industry Cybersecurity Certification Test (Security+)

Course Goals

Foundational Standards

1. Incorporate safety procedures in handling, operating, and maintaining tools and machinery; handling materials; utilizing personal protective equipment; maintaining a safe work area; and handling hazardous materials and forces.
2. Demonstrate effective workplace and employability skills, including communication, awareness of diversity, positive work ethic, problem-solving, time management, and teamwork.
3. Explore the range of careers available in the field and investigate their educational requirements, and demonstrate job-seeking skills including resume-writing and interviewing.
4. Advocate and practice safe, legal, responsible, and ethical use of information and technology tools specific to the industry pathway.
5. Participate in a Career and Technical Student Organization (CTSO) to increase knowledge and skills and to enhance leadership and teamwork.
6. Use technology to collaborate with peers and/or experts to create digital artifacts that can be published online for a target audience.
7. Formulate new ideas, solve problems, or create products through the design and engineering process by utilizing testing, prototypes, and user feedback.

Secure Networking

1. Identify and integrate secure protocols and services in a given scenario.
   Examples: SSH, tunnel and transport, IMAP, S/MIME, SFTP, FTPS
2. Differentiate among firewall technologies.
   Examples: stateful vs. stateless, web application firewall
3. Illustrate secure network designs, creating diagrams by hand or with networking software.
   Examples: load balancing, network segmentation, virtual private network, network based intrusion systems
4. Configure wireless security settings.
   Examples: WPA3, SAE, PEAP, RADIUS, site surveys, WAP, WPS, IEEE 802.1x
5. Apply secure mobile solutions in a given environment.
   Examples: NFC, mobile application management (MAM), BYOD, rooting, jailbreaking, sideloading
6. Describe the value of implementing security concepts in an enterprise environment.
   Examples: configuration and baseline management, IP schema, data loss prevention, honeypots
7. Identify and explain equalization and cloud computing concepts.
   Examples: platform as a service (PaaS), software-defined networking visibility (SDN), virtual machine (VM)
8. Compare and contrast cloud security controls.
   Examples: cloud native controls vs. third-party solutions, virtual networks

Security Principles

9. Compare and contrast secure application development, deployment, and automation concepts.
   Examples: server-side vs. client-side execution and validation, automation/scripting
10. Summarize types of authentication protocols and authorization design concepts used in network security.
    Examples: Kerberos, attribute-based access control (ABAC)
11. Explain the security vulnerabilities and constraints of embedded and specialized systems.
    Examples: system control and data acquisition (SCADA), industrial control system (ICS), Internet of Things (IoT), inability to patch
12. Explain penetration testing techniques and exercise types.
    Examples: white box, black box, red team, blue team
13. Explain the importance of having policies, processes, and procedures for carrying out incident response plans.
    Examples: attack frameworks, cyber kill chain, incident response process
14. Compare and contrast symmetric and asymmetric algorithms and their security uses.
15. Describe the primary components of public key infrastructure and explain why these structures are critical to organizations.
    Examples: Pretty Good Privacy (PGP), establishing confidentiality in email

Digital Forensics

16. Use the appropriate tool to assess organizational security in a given scenario.
    Examples: netstat, nmap, FTK imager, Nessus
17. Identify and utilize appropriate data sources to support an investigation of a given security incident.
    Examples: metadata, protocol analyzer output, syslog, rsyslog, syslog-ng
18. Explain the fundamental concepts of digital forensics.
    Examples: documentation and evidence, acquisition, on-premises versus cloud
19. Analyze risk management policies and procedures in a given organizational environment.
    Examples: risk management strategies, business impact analysis
20. Explain the procedures involved in creating a digital forensics investigation report and provide examples of report formats.
    Examples: Use word processing software to write reports which include the purpose of the investigation, the process of securing documents obtained as evidence, and conclusions.

Credentialing

Security+ Certification testing will be offered to those ready to take it after approximately 100-125 hours of seat time during this course or during a follow-up course afterwards.

Grading and Assessment

Not all assignments are graded. It is imperative that students are conscientious and complete ALL of the required work on time. Students are required to take notes (annotations), participate in lectures, watch tutorial videos, read selections, and respond with appropriate grammar. It is the student's responsibility to obtain the class notes from another student if absent. Assessment is given in all kinds of formats; written, verbal, performance products, skills demonstrated, knowledge gained and development of problem-solving.

- *Assessments 70%*

- *In-Class Work 30%*

Late Work

Any assignments that are turned in late without excuse will result in 10 points deducted from the final grade. After 3 days late the assignment can earn up to half credit.

Makeup Work

If you are absent, you will be expected to make up the work that was missed. All missed assignments and tests must be made up within three days of an EXCUSED absence. If it is not excused, you will not be allowed to make up the work (including exams).
On the day you return to class, please see the to-do list in Schoology immediately for any content that you missed or make an appointment for a make-up quiz or test. If you enter school after class or leave school before class, you are expected to see me to find out what you missed or will miss. You will be held accountable for work due that day or work assigned for homework that night.

TSA (Technology Student Association) CTSO Integration

TSA is a fundamental part of this course and is a national career and technical student organization of students engaged in science, technology, engineering, and mathematics (STEM). TSA's integrated into the program which includes competitions and leadership opportunities. TSA provides students with activities during their class time and after school with our local TSA Chapter.

Embedded Numeracy Anchor Assignment

Students will identify and formulate binary, decimal and hexadecimal numbers as it relates to Networking IP addresses, as well as using it for a network subnetting project.

This assignment will account for a test grade.

Embedded Literacy Anchor Assignment

Students will read and comprehend complex informational texts used to explain security, networking, and policies independently and proficiently. Students will write analysis and interpretation of text based on projects that they are working on by keeping a Cybersecurity Notebook of their work.

This assignment will account for a test grade.

Embedded Science Anchor Assignment

Students will use scientific methods for troubleshooting cyber security intrusion problems in a virtual lab environment to derive solutions.

This assignment will account for a test grade.

Culminating Project

Students will use their learned skills to take the Security+ outline and create a presentation to share with the class to help all prepare for the Security+ Exam.

Supplies

1. Folder or section in a binder for handouts.
2. Notebook will be electronic
3. Calculator
4. Shared Folder on Google Drive

Procedures

1. Once the bell has rung, the student is expected to be seated in class and ready to work.
2. Tardies are strictly enforced. James Clemens High School's tardy policy will be followed.
3. No hall passes for the **first or last 10** minutes of class
4. The hall pass binder is yellow. Students will be required to sign each time they leave/return to class.
5. You have three days to do makeup work and tests. It is up to you to look up the to-do list on schoology about the work missed. You can also review the latest posts on Schoology.
6. During fire drills we will exit the building to the correct exit of the building, and you are to walk with **PURPOSE**. You are to always stay with me and form a single file line once we are safely outside and be ready to be counted.
7. When the intercom sounds, you must immediately sustain all talking.
8. Raise your hand and wait to be called upon.
9. Listen without interrupting.
10. I employ the ***Ask 3 Before Me Principle***. This room is full of others that you can learn from or you can assist in their learning.
11. If we finish before the bell, you must remain seated at your desk. Take advantage of this time to work on homework, other class assignments, etc.

Computer/Internet Appropriate Usage Policies

1. You are required to bring your Chromebook, charged every day.
2. Please bring your charger every day to class.
3. Work on only software/apps for the class (or other classes).
4. DO NOT install any software/proxies/emulators on Lab PC's.
5. DO NOT copy, move, delete other's work sessions, files etc.

CTE Dual Enrollment

Students at James Clemens High School can attend Calhoun Community College, Drake State Technical Community College or University of Alabama at Huntsville to take dual enrollment courses:

Consent to Video Recording

Class Recordings: Instruction in this class might be recorded or streamed live. Any recordings will be available to students enrolled in this class. This is intended to supplement the classroom experience. Students are expected to follow appropriate school system and campus-wide policies and maintain the security of passwords used to access classroom recordings. Live streaming and recordings may not be captured or reproduced, shared with those not in the class, or uploaded to other online environments. Doing so would be a breach of the Baldwin County Public School System's Acceptable Use Policy. If I, or an administrator plan to use any recordings, beyond the classroom environment, students identifiable in the recordings will either be de-identified or will be notified prior to obtain proper consent prior to such use.

Career Pathway Program	**Cybersecurity and Infrastructure Program** **(Must teach three courses from this program list within two years.)** This pathway provides students with the skills necessary for protecting information technology infrastructure and networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Cybersecurity is an enormous and growing field as consumers and businesses share data through online shopping and social media applications.		
Course Number	**Career Pathway Program Courses**	**Career Readiness Indicator (CRI)**	**In Demand Occupations**
10997G1001	Career Pathway Project in Information Technology	• Certiport Information Technology Specialist (ITS) Cloud Computing • Certiport Information Technology Specialist (ITS) Cloud Computing • Certiport Information Technology Specialist (ITS) Cybersecurity • Certiport Information Technology Specialist (ITS) Networking • Cisco Certified Network Associate (CCNA) • CompTIA IT Fundamentals • CompTIA Linux+ • CompTIA Network+ • CompTIA Security+ • Microsoft 365 Fundamentals • Microsoft Azure Data Fundamentals • Microsoft Azure Fundamentals • Microsoft Dynamics 365 Fundamentals CRM • Microsoft Dynamics 365 Fundamentals ERP • Microsoft Power Platform Fundamentals • Microsoft Security, Compliance, and Identity Fundamentals • TestOut Network Pro • TestOut Security Pro	• Cloud Architect • Cloud Engineer • Cloud Infrastructure Engineer • Cloud System Administrator • Data Engineer • DevOps Cloud Engineer • UI Developer
10102G1014	Cloud and Virtualization		
10997G1002	CTE Lab in Information Technology		
10020G1011	Cybersecurity I		
10020G1012	Cybersecurity II		
10020G1013	Cybersecurity III		
10109G1001	Foundations of Operating Systems		
10001G1000	Information Technology Fundamentals		
10109G1000	Linux Fundamentals		
10112G1001	Network Fundamentals		
10112G1002	Network Systems Administration		
10152G1001	Programming Foundations		