Course Title	Content Area	Grade Level	Credit (if applicable)
PLTW Cybersecurity	CTE	10, 11, 12	1.0 BPS 3.0 University New Haven

Course Description

PLTW Cybersecurity is a full-year course implemented in 10th grade or above. The design of the course exposes high school students to the ever-growing and far-reaching field of cybersecurity. Students accomplish this through problem-based learning, where students role-play and train as cybersecurity experts.

PLTW Cybersecurity strongly connects to the National Cybersecurity Workforce Framework (also known as the NICE Framework or NCWF). Created by the National Institute of Standards and Technology (NIST), this framework identifies standards developed by numerous academic, industry, and government organizations. The framework objectives address topics that span K-12 education and guide learning progressions. The also incorporate many of the big ideas outlined by the College Board and addressed in AP CSP. In addition, the course integrates Computer Science Teachers Association (CSTA) standards.

PLTW Cybersecurity gives students a broad exposure to the many aspects of digital and information security, while encouraging socially responsible choices and ethical behavior. It inspires algorithmic thinking, computational thinking, and especially, “outside-the-box” thinking. Students explore the many educational and career paths available to cybersecurity experts, as well as other careers that comprise the field of information security. The course contains the following units of study.

Connection to the *BPS Vision of the Graduate*	PLTW Standards Aligned to BPS Vision of the Graduate
Collaboration	**COL.A Collaborate when processing information to gain insight and knowledge** COL.A.1 Collaboration is an important part of solving data-driven problems. COL.A.2 Collaboration facilitates solving computational problems by applying multiple perspectives, experiences, and skill sets. COL.A.3 Communication between participants working on data-driven problems gives rise to enhanced insights and knowledge. COL.A.4 Collaboration in developing hypotheses and questions, and in testing hypotheses and answering questions, about data helps participants gain insight and knowledge. COL.A.5 Collaborating face-to-face and using online collaborative tools can facilitate processing information to gain insight and knowledge. COL.A.6 Investigating large data sets collaboratively can lead to insight and knowledge not obtained when working alone. **COL.B Collaborate effectively as part of a team.** COL.B.1 A collaboratively created computational artifact reflects effort by more than one person. COL.B.2 Effective collaborative teams consider the use of online collaborative tools. COL.B.3 Effective collaborative teams practice interpersonal communication, consensus building, conflict resolution, and negotiation. COL.B.4 Effective collaboration strategies enhance performance. COL.B.5 Collaboration facilitates the application of multiple perspectives (including sociocultural perspectives) and diverse talents and skills in developing computational artifacts. COL.B.6 A collaboratively created computational artifact can reflect personal expressions of ideas. **COL.C Apply project management strategies effectively as part of a team.** COL.C.1 Select and use computational tools that enable collaboration. COL.C.2 Work with a group to establish team norms. COL.C.3 Establish clear responsibilities and split workloads equitably.
Communications and Technology Literacy	**COM.A Communicate ideas, processes, and products to optimize audience perception and understanding.** COM.A.1 Tailor and communicate information to diverse audiences. COM.A.2 Recognize and use the diverse skill sets of team members when solving problems. **ERM.D Evaluate online and print sources for appropriateness and credibility.**

	ERM.D.1 Evaluate the credibility of a source by considering the reputation and credentials of the author(s), publisher(s), site owner(s), and/or sponsor(s). ERM.D.2 Evaluate the relevance of information from a source and whether it supports an appropriate claim or the purpose of the investigation. **IOC.A Recognize that a digital presence affects future success, both personally and professionally** IOC.A.1 Evaluate the impact to yourself and others when sharing digital information online.
Information Literacy	**ERM.D Evaluate online and print sources for appropriateness and credibility.** ERM.D.1 Evaluate the credibility of a source by considering reputation and credentials of the author(s), publisher(s), site owner(s), and/or sponsor(s). ERM.D.2 Evaluate the relevancy of information from a source and whether it supports an appropriate claim or the purpose of the investigation.
Critical Thinking and Problem Solving	**CCP.A Apply creative and original thinking when confronted with a problem or new scenario.** CCP.A.1 Translate ideas into tangible solutions by employing an iterative and exploratory process. **CCP.D Describe moments within a process where curiosity, persistence, and the positive aspect of failure played an important role in gaining understanding about a problem or unexpected observation.** CCP.D.1 Describe difficulties and/or opportunities you encountered and how they were resolved or incorporated.
Social and Cross-Cultural Skills Global Awareness Empathy	**CAR.A Describe career paths within the computing specialties.** CAR.A.1 Describe a variety of careers within cybersecurity. CAR.A.2 Recognize the education and credentialing requirements for careers within cybersecurity. CAR.A.3 Demonstrate the initiative and independent learning required to stay current with evolving technology and career needs. **ERM.A Abide by professional, ethical, and legal standards when handling data or protecting data.** ERM.A.1 Develop a classroom code of conduct. ERM.A.2 Provide rationales for all ethical decisions. ERM.A.3 Engage others with respect and forethought. ERM.A.4 Weigh the ethical decisions and personal consequences when exploring and sharing digital information. ERM.A.6 Engage in debate with others to define ethical and unethical behavior. ERM.A.7 Identify the unique circumstances in which penetration testing is legal and ethical. ERM.A.8 Adhere to the rules of data privacy and the need to access information.
Civic Literacy	**ERM.B Discern how to use technology in ways that support community well-being.** ERM.B.1 Evaluate whether a particular cyber behavior is acceptable in a social context. ERM.B.2 Consider the impact of personal cyber behavior on others.

Aligned Core Resources	**Link to** ***Completed Equity Audit***	**Additional Course Information:** ***Knowledge/Skill Dependent courses/prerequisites***
PLTW Cybersecurity Online Modules https://my.pltw.org/	Equity Curriculum Review - Cybersecurity	N/A

Standard Matrix

Standards	Unit 1	Unit 2	Unit 3	Unit 4
CAR.A	☑ CAR.A.1 ☑ CAR.A.2 ☐ CAR.A.3	☑ CAR.A.1 ☐ CAR.A.2 ☐ CAR.A.3	☑ CAR.A.1 ☑ CAR.A.2 ☑ CAR.A.3	☐ CAR.A.1 ☐ CAR.A.2 ☐ CAR.A.3

COM.A	☑ COM.A.1 ☑ COM.A.2	☑ COM.A.1 ☑ COM.A.2	☑ COM.A.1 ☑ COM.A.2	☑ COM.A.1 ☑ COM.A.2
COM.B	☑ COM.B.1 □ COM.B.2	☑ COM.B.1 □ COM.B.2	☑ COM.B.1 □ COM.B.2	☑ COM.B.1 □ COM.B.2
COL.A	☑ COL.A 1 ☑ COL.A 2 ☑ COLA.3 □ COL.A.4 ☑ COL.A.5	☑ COL.A.1 ☑ COL.A.2 ☑ COL.A.3 ☑ COL.A.4 ☑ COL.A.5 ☑ COL.A.6	☑ COL.A.1 ☑ COL.A.2 ☑ COL.A.3 ☑ COL.A.4 ☑ COL.A.5 ☑ COL.A.6	☑ COL.A.1 ☑ COL.A.2 ☑ COL.A.3 ☑ COL.A.4 ☑ COL.A.5 ☑ COL.A.6
COL.B	□ COL.B.1 □ COL.B.2 □ COL.B.3 ☑ COL.B.4 ☑ COL.B.5 ☑ COL.B.6	☑ COL.B.1 ☑ COL.B.2 ☑ COL.B.3 ☑ COL.B.4 ☑ COL.B.5 ☑ COL.B.6	☑ COL.B.1 ☑ COL.B.2 ☑ COL.B.3 ☑ COL.B.4 ☑ COL.B.5 ☑ COL.B.6	☑ COL.B.1 ☑ COL.B.2 ☑ COL.B.3 ☑ COL.B.4 ☑ COL.B.5 ☑ COL.B.6
COL.C	☑ COL.C.1 ☑ COL.C.2 □ COL.C.3	☑ COL.C.1 ☑ COL.C.2 ☑ COL.C.3	☑ COL.C.1. ☑ COL.C.2 ☑ COL.C.3	☑ COL.C.1 ☑ COL.C.2 ☑ COL.C.3
ERM.A	☑ ERM.A.1 □ ERM.A.2 □ ERM.A.3 ☑ ERM.A.4 □ ERM.A.5 □ ERM.A.6 □ ERM.A.7 □ ERM.A.8	☑ ERM.A.1 ☑ ERM.A.2 ☑ ERM.A.3 ☑ ERM.A.4 □ ERM.A.5 ☑ ERM.A.6 ☑ ERM.A.7 ☑ ERM.A.8	□ ERM.A.1 ☑ ERM.A.2 ☑ ERM.A.3 ☑ ERM.A.4 ☑ ERM.A.5 ☑ ERM.A.6 ☑ ERM.A.7 ☑ ERM.A.8	□ ERM.A.1 □ ERM.A.2 ☑ ERM.A.3 ☑ ERM.A.4 ☑ ERM.A.5 □ ERM.A.6 □ ERM.A.7 ☑ ERM.A.8
ERM.B	☑ ERM.B.1 ☑ ERM.B.2	☑ ERM.B.1 ☑ ERM.B.2	☑ ERM.B.1 ☑ ERM.B.2	□ ERM.B.1 □ ERM.B.2
ERM.C	□ ERM.C.1 □ ERM.C.2	□ ERM.C.1 □ ERM.B.2	☑ ERM.C.1 □ ERM.C.2	□ ERM.C.1 □ ERM.C.2
ERM.D	☑ ERM.D.1 ☑ ERM.D.2	☑ ERM.D.1 ☑ ERM.D.2	☑ ERM.D.1 ☑ ERM.D.2	□ ERM.D.1 □ ERM.D.2
CCP.A	☑ CCP.A.1 □ CCP.A.2	☑ CCP.A.1 □ CCP.A.2	☑ CCP.A.1 □ CCP.A.2	☑ CCP.A.1 □ CCP.A.2
CCP.B	☑ CCP.B.1 □ CCP.B.2	☑ CCP.B.1 □ CCP.B.2	☑ CCP.B.1 □ CCP.B.2	☑ CCP.B.1 □ CCP.B.2
CCP.C	☑ CCP.C.1	☑ CCP.C.1	☑ CCP.C.1	☑ CCP.C.1
CCP.D	□ CCP.D.1	☑ CCP.D.1	☑ CCP.D.1	□ CCP.D.1
CCP.E	□ CCP.E.1 □ CCP.E.2 ☑ CCP.E.3	☑ CCP.E.1 ☑ CCP.E.2 ☑ CCP.E.3	☑ CCP.E.1 □ CCP.E.2 ☑ CCP.E.3	□ CCP.E.1 □ CCP.E.2 □ CCP.E.3
CCP.F	☑ CCP.F.1 ☑ CCP.F.2	☑ CCP.F.1 ☑ CCP.F.2	☑ CCP.F.1 ☑ CCP.F.2	☑ CCP.F.1 ☑ CCP.F.2
IARP.A	□ IARP.A.1	☑ IARP.A.1	□ IARP.A.1	☑ IARP.A.1

	☐ IARP.A.2 ☐ IARP.A.3 ☐ IARP.A.4	☐ IARP.A.2 ☐ IARP.A.3 ☐ IARP.A.4	☐ IARP.A.2 ☐ IARP.A.3 ☐ IARP.A.4	☑ IARP.A.2 ☑ IARP.A.3 ☑ IARP.A.4
IARP.B	☑ IARP.B.1 ☐ IARP.B.2	☑ IARP.B.1 ☑ IARP.B.2	☑ IARP.B.1 ☑ IARP.B.2	☑ IARP.B.1 ☐ IARP.B.2
IARP.C	☐ IARP.C.1 ☐ IARPC.2 ☑ IARPC.3	☑ IARP.C.1 ☑ IARPC.2 ☑ IARPC.3	☐ IARP.C.1 ☐ IARPC.2 ☑ IARPC.3	☑ IARP.C.1 ☐ IARPC.2 ☐ IARPC.3
IARP.D	☐ IARP.D.1 ☐ IARP.D.2 ☐ IARP.D.3	☑ IARP.D.1 ☑ IARP.D.2 ☑ IARP.D.3	☑ IARP.D.1 ☑ IARP.D.2 ☑ IARP.D.3	☑ IARP.D.1 ☐ IARP.D.2 ☐ IARP.D.3
IARP.E	☐ IARP.E.1 ☐ IARP.E.2 ☐ IARP.E.3	☑ IARP.E.1 ☐ IARP.E.2 ☐ IARP.E.3	☑ IARP.E.1 ☑ IARP.E.2 ☑ IARP.E.3	☑ IARP.E.1 ☐ IARP.E.2 ☐ IARP.E.3
DAT.A	☑ DAT.A.1 ☐ DAT.A.2 ☐ DAT.A.3 ☐ DAT.A.4	☑ DAT.A.1 ☑ DAT.A.2 ☑ DAT.A.3 ☑ DAT.A.4	☑ DAT.A.1 ☑ DAT.A.2 ☑ DAT.A.3 ☑ DAT.A.4	☑ DAT.A.1 ☐ DAT.A.2 ☐ DAT.A.3 ☑ DAT.A.4
DAT.B	☑ DAT.B.1 ☑ DAT.B.2 ☑ DAT.B.3 ☑ DAT.B.4 ☑ DAT.B.5	☑ DAT.B.1 ☐ DAT.B.2 ☐ DAT.B.3 ☐ DAT.B.4 ☐ DAT.B.5	☐ DAT.B.1 ☐ DAT.B.2 ☐ DAT.B.3 ☐ DAT.B.4 ☐ DAT.B.5	☑ DAT.B.1 ☑ DAT.B.2 ☐ DAT.B.3 ☑ DAT.B.4 ☐ DAT.B.5
DAT.C	☐ DAT.C.1 ☐ DAT.C.2	☑ DAT.C.1 ☑ DAT.C.2	☑ DAT.C.1 ☑ DAT.C.2	☑ DAT.C.1 ☑ DAT.C.2
IOC.A	☑ IOC.A.1 ☐ IOC.A.2	☑ IOC.A.1 ☐ IOC.A.2	☐ IOC.A.1 ☐ IOC.A.2	☐ IOC.A.1 ☐ IOC.A.2
IOC.B	☐ IOC.B.1 ☐ IOC.B.2 ☐ IOC.B.3 ☐ IOC.B.4	☑ IOC.B.1 ☑ IOC.B.2 ☑ IOC.B.3 ☑ IOC.B.4	☑ IOC.B.1 ☑ IOC.B.2 ☑ IOC.B.3 ☐ IOC.B.4	☐ IOC.B.1 ☐ IOC.B.2 ☐ IOC.B.3 ☐ IOC.B.4
CTT.A	☑ CTT.A.1 ☑ CTT.A.2	☑ CTT.A.1 ☑ CTT.A.2	☑ CTT.A.1 ☑ CTT.A.2	☑ CTT.A.1 ☐ CTT.A.2
CTT.B	☑ CCT.B.1 ☐ CCT.B.2	☑ CCT.B.1 ☑ CCT.B.2	☑ CCT.B.1 ☑ CCT.B.2	☑ CCT.B.1 ☑ CCT.B.2
CSN.A	☑ CSN.A.1 ☑ CSN.A.2	☐ CSN.A.1 ☑ CSN.A.2	☑ CSN.A.1 ☑ CSN.A.2	☑ CSN.A.1 ☑ CSN.A.2
CSN.B	☑ CSN.B.1 ☑ CSN.B.2 ☑ CSN.B.3 ☑ CSN.B.4 ☑ CSN.B.5 ☑ CSN.B.6	☑ CSN.B.1 ☑ CSN.B.2 ☐ CSN.B.3 ☐ CSN.B.4 ☑ CSN.B.5 ☐ CSN.B.6	☑ CSN.B.1 ☑ CSN.B.2 ☑ CSN.B.3 ☑ CSN.B.4 ☑ CSN.B.5 ☐ CSN.B.6	☑ CSN.B.1 ☐ CSN.B.2 ☐ CSN.B.3 ☑ CSN.B.4 ☑ CSN.B.5 ☐ CSN.B.6
CSN.C	☑ CSN.C.1 ☑ CSN.C.2	☑ CSN.C.1 ☑ CSN.C.2	☑ CSN.C.1 ☑ CSN.C.2	☐ CSN.C.1 ☐ CSN.C.2

	☑ CSN.C.3	☑ CSN.C.3	☑ CSN.C.3	□ CSN.C.3
CSN.D	□ CSN.D.1 □ CSN.D.2 ☑ CSN.D.3 ☑ CSN.D.4 ☑ CSN.D.5 ☑ CSN.D.6	□ CSN.D.1 □ CSN.D.2 □ CSN.D.3 □ CSN.D.4 □ CSN.D.5 □ CSN.D.6	☑ CSN.D.1 ☑ CSN.D.2 ☑ CSN.D.3 ☑ CSN.D.4 ☑ CSN.D.5 ☑ CSN.D.6	□ CSN.D.1 □ CSN.D.2 □ CSN.D.3 □ CSN.D.4 □ CSN.D.5 ☑ CSN.D.6
CSN.F	□ CSN.F.1 □ CSN.F.2 ☑ CSN.F.3 □ CSN.F.4 □ CSN.F.5 ☑ CSN.F.6 ☑ CSN.F.7	□ CSN.F.1 ☑ CSN.F.2 ☑ CSN.F.3 □ CSN.F.4 □ CSN.F.5 ☑ CSN.F.6 ☑ CSN.F.7	☑ CSN.F.1 ☑ CSN.F.2 ☑ CSN.F.3 ☑ CSN.F.4 ☑ CSN.F.5 ☑ CSN.F.6 ☑ CSN.F.7	□ CSN.F.1 □ CSN.F.2 □ CSN.F.3 □ CSN.F.4 ☑ CSN.F.5 ☑ CSN.F.6 □ CSN.F.7
CSN.G	☑ CSN.G.1 □ CSN.G.2 □ CSN.G.3 ☑ CSN.G.4	☑ CSN.G.1 ☑ CSN.G.2 ☑ CSN.G.3 ☑ CSN.G.4	□ CSN.G.1 ☑ CSN.G.2 ☑ CSN.G.3 ☑ CSN.G.4	□ CSN.G.1 □ CSN.G.2 □ CSN.G.3 □ CSN.G.4
CSN.H	☑ CSN.H.1 ☑ CSN.H.2 □ CSN.H.3	☑ CSN.H.1 □ CSN.H.2 ☑ CSN.H.3	☑ CSN.H.1 ☑ CSN.H.2 ☑ CSN.H.3	□ CSN.H.1 □ CSN.H.2 □ CSN.H.3
CSN.I	□ CSN.I.1 □ CSN.I.2	☑ CSN.I.1 ☑ CSN.I.2	□ CSN.I.1 □ CSN.I.2	☑ CSN.I.1 □ CSN.I.2
CSN.J	□ CSN.J.1 □ CSN.J.2 ☑ CNS.J.3	☑ CSN.J.1 ☑ CSN.J.2 ☑ CNS.J.3	☑ CSN.J.1 ☑ CSN.J.2 ☑ CNS.J.3	□ CSN.J.1 ☑ CSN.J.2 □ CNS.J.3
SA.A	□ SA.A.1 □ SA.A.2 □ SA.A.3	□ SA.A1 □ SA.A2 □ SA.A.3	□ SA.A1 □ SA.A2 □ SA.A.3	☑ SA.A.1 ☑ SA.A.2 ☑ SA.A.3
SA.B	□ SA.B.1	□ SA.B.1	☑ SA.B.1	□ SA.B.1
SA.C	□ SA.C.1 □ SA.C.2 □ SA.C.3	□ SA.C.1 □ SA.C.2 □ SA.C.3	□ SA.C.1 □ SA.C.2 ☑ SA.C.3	☑ SA.C.1 ☑ SA.C.2 ☑ SA.C.3

Unit Links

Unit 1: Personal Security
Unit 2: System Security
Unit 3: Network Security
Unit 4: Applied Cybersecurity

Unit Title

Unit 1: Personal Security

Relevant Standards: Bold indicates priority

COM.B Recognize documentation as an indispensable part of the security process.

COM.B.1 Maintain a detailed record of the process and the steps used to solve a problem.

CCP.B Create a computational artifact for creative expression.

CCP.B.1 Identify a computational artifact as something created by a human using a computer and differentiate between a program, an image, audio, a video, a presentation, or a web page file.

CCP.C Deconstruct a complex problem into simpler parts.

CCP.C.1 Identify and apply solutions to subcomponents to achieve a system-wide solution.

CCP.E Engage stakeholders in a problem and use their perspectives to shape the course of your development.

CCP.E.3 Share meaningful insights about the context of an organization's threat environment that improve its risk management posture. (NICE A0120)

CCP.F Apply and describe the process based on user-centered research to solve a problem.

CCP.F.1 Apply and describe the process used during the development of a solution

CCP.F.2 Acknowledge that stages of failure and technical hurdles are typical in processes that produce positive outcomes.

IARP.B Analyze the evidence of an attack.

IARP.B.1 Identify common types of malware.

IARP.C Design the correct level of protection by implementing the appropriate safeguards.

IARP.C.3 Protect against future information threats.

DAT.A Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.

DAT.A.1 Identify systemic security issues based on the analysis of vulnerability and configuration data. (NICE A0001)

DAT.B Identify personal data sharing that places people at risk and evaluate risky personal data-sharing practices.

DAT.B.1 Understand that security and privacy concerns arise with data containing personal information.

DAT.B.2 Understand data mining techniques used to perform social engineering.

DAT.B.3 Create a risk assessment of personal data sharing and evaluate the potential for social engineering attacks.

DAT.B.4 Evaluate attacks that occur via email.

DAT.B.5 Manage browser security settings to facilitate safe browsing.

CTT.A Select and apply appropriate computational tools and techniques to solve a problem or create value for others.

CTT.A.1 Select collaboration tools for data collection, writing, or protecting data.

CTT.A.2 Navigate and use unfamiliar documentation and public information to extend the student's own knowledge and to achieve a computational approach to solve a problem.

CTT.B Apply tools with varying levels of abstraction within software, a computer, a network, and the internet.

CTT.B.1 Recognize and discern between different levels of abstraction while working with computational tools.

CSN.A Describe the modular components of a computer's hardware and software.

CSN.A.1 Identify the hardware components of a computer.

CSN.A.2 Identify the broad tasks that operating systems manage, such as process management and file management.

CSN.B Identify user actions that strengthen the security of information stored on a computer.

CSN.B.1 Navigate system files to locate files that are used to manage computer resources.

CSN.B.2 Manage system processes and user processes.

CSN.B.3 Create strong passphrases.

CSN.B.4 Install and manage protective software, including updates and removal.

CSN.B.5 Manage software using configuration tools and/or parameters.

CSN.B.6 Manage important data by establishing backup procedures.

CSN.C Monitor, analyze, and manage active processes on a computer or network of computers.

CSN.C.1 Differentiate between user and system processes.

CSN.C.2 Identify and analyze potentially malicious/foreign processes.

CSN.C.3 Install, analyze and remove processes.

CSN.D Gain understanding of how an operating system is structured and works by navigating the file system and

modifying files, extensions, rights, and visibility to better protect data.

CSN.D.3 Change file extensions and predict the effects of the change.
CSN.D.4 Manage file types, access rights, and visibility of files.
CSN.D.5 Organize a file system.
CSN.D.6 Search a file system.

CSN.F Identify the components (software, hardware, protocols) that allow computers to network and communicate.

CSN.F.3 Describe networking hardware.
CSN.F.6 Identify network system sub-components responsible for security.
CSN.F.7 Locate and solve security problem(s) within a network system's subcomponents.

CSN.G Analyze the evidence of web exploitations, both from front-end application and backend services perspective.

CSN.G.1 Identify websites that appear untrustworthy or dangerous to the end user.
CSN.G.4 Protect against web-based weaknesses.

CSN.I Identify user actions that strengthen the security of a networked system.

CSN.I.1 Recognize that the security of a network depends on the security of its individual components.
CSN.I.2 Manage settings and configuration files of software and/or drivers to maintain the security of the network.

CSN.J Use abstractions to manage and analyze information.

CSN.J.3 Identify the abstracted nature of network communication

Essential Question(s):	**Enduring Understanding(s):**

1.1 - Why do people engage in risky behavior in cyberspace?
People engage in risky behavior online due to a lack of awareness, convenience, or misplaced trust. Understanding human behavior is critical to promoting safer online practices.

1.3 - What are the consequences of inappropriate behavior in cyberspace?
Inappropriate behavior in cyberspace can lead to personal, legal, and societal consequences, including identity theft, reputational damage, and legal penalties. Respect and accountability are vital in the digital world.

2.1 - Why does information need protection?
Information needs protection to preserve its confidentiality, integrity, and availability. Securing data prevents misuse, theft, and unauthorized access, ensuring trust in digital systems.

2.2 - How do computers safely store information?
Computers use encryption, secure storage methods, and access controls to safely store information. These techniques reduce the risk of data breaches and unauthorized access.

4.1 - How can information be safely exchanged?
Information can be safely exchanged by using secure protocols, encryption, and authentication mechanisms, which protect data during transmission and ensure it reaches the intended recipient.

5.1 - How can malware be stopped?
Malware can be stopped through proactive defenses, such as antivirus software, firewalls, timely updates, and user education to recognize and avoid potential threats.

7.1 - What makes a good cyber team?
A good cyber team is collaborative, adaptive, and skilled in various cybersecurity disciplines. Effective communication, diverse expertise, and a shared commitment to ethical practices ensure successful outcomes in complex scenarios.

Demonstration of Learning:	
A hands-on, scenario-based cybersecurity project where students are tasked with addressing a simulated security breach or malware incident. Students prepare a **report or presentation** that documents: ● The steps they took to address the security incident. ● The tools and techniques they used for virus scanning, data recovery, and malware removal. ● A security improvement plan for the system, including backup and prevention strategies.	Students will demonstrate their learning by: ● Identifying safe and strong passwords ● Identifying suspicious content in email and on social media ● Identifying security improvements to social media accounts ● Conducting a thorough scan of the computer using antivirus software. ● Identifying and isolating suspicious processes or applications. ● Safely removing or quarantining identified malware

• The results of the file behavior analysis and the outcomes of the system scan.	to prevent further damage. • Utilizing data recovery techniques to attempt restoration of lost files. • Verifying integrity and completeness of restored files. • Providing guidance on data backup practices to prevent future data loss. • Performing a comprehensive scan of the system for suspicious files and directories. • Analyzing file attributes and behavior patterns to identify potential threats.
Family Overview	**Pacing for Unit**
[PLTW Cybersecurity Family Overview (2024)]()	28 Days (Traditional) 14 Days (Block)
Unit-specific Vocabulary:	**Integration of Technology and Aligned Unit Materials, Resources, and Technology**
1.1 Introduction to Cybersecurity: Digital footprint, Virtual machine, Crack, Python script, Brute force attack, Dictionary attack, Encrypted, Algorithm, File extension, Authorize, Authenticate, CAPTCHA, Turing Award, Social media, Spam, Phishing, Phisher, Email source, Top-Level domain, Cyber team, Team norms 1.2 Firewalls and Malware: Network topology, LAN, Switched topology, Router, Wireless, Services, Virus, Worm, Backdoor, Spyware, Trojan Horse, Adware, Pop-up, Operating system, Updated, Firewall, Server, Protocol, Port, Web Server, HTTP, Encrypt, Log files, Zip file, Wildcard, RAM, Environment variable, Process tree, URL, Cookies, Site certificate,	
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
Potential interdisciplinary connection may integrate ethical considerations in cybersecurity with principles of civic responsibility and democratic values. Students will explore how advancements in technology intersect with civil liberties, rights, and governance, fostering critical thinking and ethical reasoning	• Cybersecurity is only applicable to government-related organizations. • Individuals are not affected by and do not contribute to the security of cyberspace • A good password is something that can be easily remembered or has special meaning • Social networking is safe and everyone on social media can be trusted • All email content is safe and can be trusted. • Using the same password on all my accounts is a good and safe way for me to remember my passwords. • When a computer has low or non-existent security, it only poses a risk for the users of that computer. • Improving security of a network can only be done by experts. • Files, folders, applications, and processes are all different from another and their management tasks have little in common. • A brand new computer is automatically safe to use. • When someone browses the internet, the websites they visit don't track or store much information about them, their browser, or their devices.

	● Security experts already know everything they need to know to secure a computer. ● Security experts work in isolation all day ● Solving problems is a linear process and does not require any iteration.
Differentiation through *Universal Design for Learning*	
UDL Indicator	**Teacher Actions:**

1. I CAN describe the importance and scope of cyber security.

Engagement:

Real-World Scenarios: Begin by discussing recent news stories about cyberattacks or data breaches (e.g., social media hacks, ransomware attacks) to illustrate the importance of cybersecurity.

Discussion: Facilitate a class discussion on why cybersecurity is essential for individuals, businesses, and governments. Allow students to share their thoughts on how cybersecurity affects their personal lives and global events.

Representation:

Infographics and Visuals: Use visual aids like diagrams, charts, or infographics to show the scope of cybersecurity (e.g., the types of cyber threats, the difference between cybersecurity and IT security).

Videos/Documentaries: Show a short video or documentary that explains the global impact of cyberattacks on companies, governments, and individuals.

Action/Expression:

Group Project: Have students work in groups to create a presentation or infographic that outlines the importance of cybersecurity in different sectors (business, healthcare, education, government).

Reflective Writing: Ask students to write a brief reflection on how cybersecurity impacts their daily activities and what they do to protect themselves online.

2. I CAN analyze how various authentication strategies protect online information.

Engagement:

Interactive Demo: Use an interactive demonstration of various authentication methods (e.g., passwords, biometrics, two-factor authentication) and allow students to participate in securing a fictional online account.

Discussion/Brainstorming: Encourage students to brainstorm different types of authentication methods they've encountered, such as PIN codes, facial recognition, or hardware tokens.

Representation:

Visual Comparisons: Provide side-by-side comparisons of different authentication strategies (e.g., password vs. biometric authentication) with pros and cons.

Flowcharts/Diagrams: Use flowcharts or diagrams that show how authentication methods work step by step (e.g., how two-factor authentication enhances security).

Action/Expression:

Hands-on Practice: Have students test out different authentication methods on simulated platforms (e.g., logging into websites with different authentication strategies).

Create a Security Plan: Ask students to create a security plan for a fictional business or service, recommending appropriate authentication strategies to protect user data.

3. I CAN demonstrate the ability to protect myself and others from exposing personal information and social engineering attacks.

Engagement:

Social Engineering Scenario: Introduce students to social engineering attacks by role-playing a phishing scam or a pretexting scenario where a "hacker" tries to gain information from a student.

Discussion: Start a class discussion about the different types of social engineering attacks, such as phishing, baiting, or tailgating, and how they can occur both online and in physical settings.

Representation:

Case Studies and Examples: Provide real-world examples of social engineering attacks and their consequences (e.g., emails that mimic bank communications).

Video Examples: Show video clips or simulations of social engineering attacks to help students recognize red flags.

Action/Expression:

Role-Playing: Have students participate in role-playing exercises where they practice responding to phishing attempts or other social engineering attacks.

Create Educational Materials: Ask students to create a poster, infographic, or video that educates others on how to recognize and protect against social engineering attacks.

4. I CAN configure a firewall to protect against malware.

Engagement:

Hands-On Lab Activity: Set up a hands-on activity where students configure a basic firewall on a virtual machine or network. Show them how to test and verify its effectiveness against malware.

Real-Life Application: Discuss scenarios where firewalls are essential, such as for protecting sensitive business data or securing a home network.

Representation:

Step-by-Step Tutorials: Provide a step-by-step visual guide or video on configuring a firewall and monitoring its performance.

Firewall Diagrams: Use diagrams to explain how firewalls function in a network, such as how they monitor and filter incoming and outgoing traffic.

Action/Expression:

Configure a Virtual Firewall: Students can configure firewalls on virtual machines or simulated systems and document their process.

Firewall Comparison: Have students compare different types of firewalls (e.g., hardware vs. software firewalls) and create a report on which is most effective for certain use cases.

5. I CAN apply safety measures for accessing and storing data.

Engagement:

Scenario-Based Learning: Present students with a variety of real-world scenarios (e.g., securing personal data on mobile devices, backing up company data, or protecting sensitive medical records) and ask them to discuss safety measures.

Discussion: Lead a discussion on common risks associated with accessing and storing data, such as unauthorized access, data loss, or identity theft.

Representation:

Checklists and Guidelines: Provide students with safety checklists or best practices for securely accessing and storing data (e.g., strong passwords, encryption, using cloud storage securely).

Visual Aids: Show diagrams of secure data storage practices (e.g., cloud encryption, physical storage devices with encryption, access control measures).

Action/Expression:

Data Protection Plan: Have students create a personal or business data protection plan, outlining steps they would take to access and store data securely.

Demonstration: Ask students to demonstrate how to apply safety measures for accessing and storing data, such as encrypting files or setting up secure cloud storage.

6. I CAN recognize and terminate suspicious processes.

Engagement:

Real-World Scenarios: Present a scenario where a computer might be infected with malware or running suspicious processes, and ask students to brainstorm how they would investigate the issue.

Interactive Demonstration: Walk through the process of identifying suspicious processes in Task Manager or Activity Monitor on a computer, explaining what each process does.

Representation:

Process Diagrams: Provide visual diagrams that show how to identify and interpret different system processes, including what typical system processes look like and how to recognize unusual activity.

Videos: Show a video that demonstrates the process of investigating and terminating suspicious processes safely.

Action/Expression:

Hands-On Investigation: Have students practice identifying and terminating suspicious processes in a virtual environment or using sandbox software.

Case Study Analysis: Ask students to analyze a case study of a system infection, identifying the suspicious processes involved and explaining how they would terminate them.

7. I CAN manage browser configuration including security settings, cookies, history, downloads, and access to resources.

Engagement:

Interactive Walkthrough: Guide students through a live demonstration of managing browser settings, including clearing history, disabling cookies, and adjusting security settings for various browsers.

Scenario-Based Learning: Ask students to consider a scenario where their browser is compromised (e.g., through tracking cookies or a malicious extension) and discuss how they would address it.

Representation:

Browser Configuration Diagrams: Provide diagrams or screenshots showing how to access and adjust different browser settings for security (e.g., blocking third-party cookies, adjusting privacy settings).

Step-by-Step Guides: Provide written or video guides for configuring browser security settings, clearing history, and managing cookies and downloads.

Action/Expression:

Hands-On Configuration: Have students individually adjust browser security settings on their own devices or virtual environments.

Browser Configuration Report: Ask students to write a report on how they would configure their browser to maximize security, explaining their reasoning for each setting.

Supporting Multilingual/English Learners

Related CELP standards:	**Learning Targets:**

Learning Target 1: I can describe the importance and scope of cyber security.

- **Level 1:** Can recognize basic terms related to cyber security (e.g., “computer safety,” “passwords”). May identify simple examples of cyber security, such as locking a device or using antivirus software.
- **Level 2:** Can describe the general purpose of cyber security, such as keeping personal information safe. Can identify basic cyber security threats (e.g., viruses, hackers).
- **Level 3:** Can explain the importance of cyber security in protecting personal data, sensitive business information, and online transactions. Can describe common types of cyber security threats (e.g., phishing, malware).
- **Level 4:** Can explain the scope of cyber security, discussing various aspects such as network security, data encryption, and threat detection. Can describe how cyber security practices impact individuals, businesses, and governments.
- **Level 5:** Can analyze the broader implications of cyber security on society and the global economy. Can assess the risks and strategies involved in protecting digital infrastructures, and explain the importance of staying up-to-date with evolving threats and best practices.

Learning Target 2: I can analyze how various authentication strategies protect online information.

- **Level 1:** Can recognize common authentication methods (e.g., “password,” “fingerprint”). May need support in understanding how they work to protect information.
- **Level 2:** Can describe basic authentication methods, such as passwords or PINs, and their role in protecting online accounts. Can identify the importance of keeping passwords secure.
- **Level 3:** Can explain different types of authentication strategies (e.g., two-factor authentication, biometrics, security questions) and how they enhance online security. Can describe the advantages and limitations of these methods.
- **Level 4:** Can analyze various authentication strategies, such as multi-factor authentication, and explain their effectiveness in protecting sensitive online information. Can discuss the role of encryption and secure communication protocols in authentication.
- **Level 5:** Can evaluate and compare the security of different authentication methods based on the context of use (e.g., personal accounts, corporate systems). Can recommend appropriate authentication strategies for different online environments.

Learning Target 3: I can demonstrate the ability to protect myself and others from exposing personal information and social engineering attacks.

- **Level 1:** Can recognize simple examples of social engineering (e.g., unsolicited emails or phone calls). May be able to identify basic ways to protect personal information.
- **Level 2:** Can describe common social engineering tactics, such as phishing or pretexting. Can identify actions that help protect personal information, like avoiding sharing passwords.
- **Level 3:** Can demonstrate awareness of social engineering attacks and how to avoid falling victim to them. Can explain how to protect personal information, such as using strong passwords and recognizing suspicious emails or phone calls.
- **Level 4:** Can identify specific social engineering techniques used in various online scams and describe proactive measures to prevent exposure. Can demonstrate how to secure personal information through privacy settings and cautious online behavior.

- **Level 5:** Can analyze and respond to complex social engineering scenarios, employing strategies to protect both personal and professional information. Can educate others on best practices for avoiding social engineering attacks and protecting sensitive data.

Learning Target 4: I can configure a firewall to protect against malware.

- **Level 1:** Can recognize the concept of a firewall and its basic purpose (e.g., "keeps bad stuff out"). May need assistance in understanding how to configure or use it.
- **Level 2:** Can describe what a firewall does (e.g., “blocks unwanted traffic”) and can identify basic settings or options. Can recognize the importance of using a firewall for malware protection.
- **Level 3:** Can explain how a firewall works to protect against malware and can configure basic firewall settings, such as allowing or blocking specific applications or ports.
- **Level 4:** Can configure a firewall with specific rules to block malware and unauthorized access. Can describe how firewalls work in conjunction with other security tools to enhance system protection.
- **Level 5:** Can set up advanced firewall configurations to protect against malware and other cyber threats. Can analyze and adjust firewall settings based on network needs and security threats, and ensure that the firewall is optimized for maximum protection.

Learning Target 5: I can apply safety measures for accessing and storing data.

- **Level 1:** Can recognize that data needs to be protected (e.g., “don’t share your passwords”). May need guidance on specific safety measures.
- **Level 2:** Can describe basic safety measures for accessing and storing data, such as using a password or encrypting files. Can identify simple ways to protect data from unauthorized access.
- **Level 3:** Can explain safety measures for securely accessing and storing data, such as using encryption, strong passwords, and multi-factor authentication. Can identify secure methods for transferring data.
- **Level 4:** Can apply safety measures to protect data while accessing it on various devices and platforms. Can securely store sensitive data using encryption, access controls, and backups.
- **Level 5:** Can design and implement comprehensive data protection strategies, including data access policies, secure storage protocols, and risk management practices. Can evaluate data security measures and make recommendations to improve data protection.

Learning Target 6: I can recognize and terminate suspicious processes.

- **Level 1:** Can recognize that suspicious processes may indicate a problem (e.g., “something isn’t right” when the computer slows down). May need help identifying what constitutes a suspicious process.
- **Level 2:** Can identify basic signs of suspicious processes, such as high CPU usage or unknown programs running. May need support to terminate or manage these processes.
- **Level 3:** Can recognize and explain what constitutes suspicious processes or malware running on a device (e.g., unusual processes, unfamiliar names). Can terminate processes using basic task management tools.
- **Level 4:** Can identify and explain the behavior of suspicious processes, such as those associated with malware or unauthorized applications. Can terminate processes using advanced tools and ensure that no damage is done to the system.
- **Level 5:** Can analyze system performance to detect suspicious activity, terminate harmful processes, and mitigate risks. Can use diagnostic tools and logs to identify the source of suspicious processes and recommend solutions to prevent future issues.

Learning Target 7: I can manage browser configuration including security settings, cookies, history, downloads, and access to resources.

- **Level 1:** Can recognize that a browser has settings to adjust. May need guidance on how to manage basic security features.
- **Level 2:** Can describe basic browser settings, such as clearing history or enabling a pop-up blocker. Can adjust basic security settings, such as enabling or disabling cookies.
- **Level 3:** Can explain the function of different browser settings related to security, such as controlling cookies, clearing history, and managing downloads. Can configure a browser to block potentially harmful resources or unauthorized access.
- **Level 4:** Can manage browser security settings comprehensively, adjusting configurations for cookies, history, downloads, and access to resources. Can enable and manage settings to maximize privacy and security while browsing.
- **Level 5:** Can optimize browser configurations for security, implementing advanced settings such as sandboxing, blocking tracking scripts, and managing multiple security layers. Can educate others on how to configure browsers securely and safely access resources online.

Lesson	**Learning Target**	**Success Criteria/Assessment/Resources**

Sequence		
1	I CAN describe the importance and scope of cyber security.	● I can define cybersecurity ● I can identify insecure data sharing practices ● I can describe the impact of your digital presence.
2	I CAN analyze how various authentication strategies protect online information	● I can protect my personal computer. ● I can differentiate between a strong and weak password. ● I can examine password cracking algorithms used in brute force attacks.
3	I CAN demonstrate the ability to protect myself and others from exposing personal information and social engineering attacks	● I can identify unsafe practices related to social media and email. ● I can protect a social media profile. ● I can protect against spam and phishing. ● I can learn to evaluate suspicious email or websites. ● I can learn how to protect against social engineering attacks.
4	I CAN configure a firewall to protect against malware	● I can discuss how network devices are connected ● I can identify types of malware
5	I CAN apply safety measures for accessing and storing data	● I can discuss files and file types ● I can access files safely and identify ownership ● I can identify suspicious data on my computer ● I can encrypted files
6	I CAN recognize and terminate suspicious processes	● I can manage processes and the files that launched them
7	I CAN manage browser configuration including security settings, cookies, history, downloads, and access to resources	● I can differentiate between HTTP and HTTPS ● I can examine site certificates ● I can use my Google Chrome browser to improve security features.

Unit Title:

Unit 2: System Security

Relevant Standards: Bold indicates priority

COM.B Recognize documentation as an indispensable part of the security process.

COM.B.1 Maintain a detailed record of the process and the steps used to solve a problem.

CCP.B Create a computational artifact for creative expression.

CCP.B.1 Identify a computational artifact as something created by a human using a computer and differentiate between a program, an image, audio, a video, a presentation, or a web page file.

CCP.C Deconstruct a complex problem into simpler parts.

CCP.C.1 Identify and apply solutions to subcomponents to achieve a system-wide solution.

CCP.D Describe moments within a process where curiosity, persistence, and the positive aspect of failure played an important role in gaining understanding about a problem or unexpected observation.

CCP.D.1 Describe difficulties and/or opportunities you encountered and how they were resolved or incorporated.

CCP.E Engage stakeholders in a problem and use their perspectives to shape the course of your development.

CCP.E.1 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, nonrepudiation). (NICE A0123)

CCP.E.2 Tailor technical and planning information to a customer's level of understanding. (NICE A0105)

CCP.E.3 Share meaningful insights about the context of an organization's threat environment that improve its risk management posture. (NICE A0120)

CCP.F Apply and describe the process based on user-centered research to solve a problem.

CCP.F.1 Apply and describe the process used during the development of a solution

CCP.F.2 Acknowledge that stages of failure and technical hurdles are typical in processes that produce positive outcomes.

IARP.A Use digital forensics investigative techniques to solve a cybercrime.

IARP.A.1 Define what constitutes a cybercrime.

IARP.B Analyze the evidence of an attack.

IARP.B.1 Identify common types of malware.

IARP.B.2 Use knowledge of historical malware attacks to evaluate modern threats.

IARP.C Design the correct level of protection by implementing the appropriate safeguards.

IARP.C.1 Describe the positive and negative outcomes of different solutions related to data confidentiality, integrity, and availability.

IARP.C.2 Compare the value of protecting information in terms of cost, levels of security, and ease of access to data.

IARP.C.3 Protect against future information threats.

IARP.D Detect and analyze the occurrence of a cybersecurity event.

IARP.D.1 Use pattern finding techniques to determine trends in attack data.

IARP.D.2 Identify malicious network traffic.

IARP.D.3 Analyze attack data to determine the source of the attack and the harmful effects it may have on the system.

IARP.E Respond to a detected cybersecurity event.

IARP.E.1 Communicate the event.

DAT.A Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.

DAT.A.1 Identify systemic security issues based on the analysis of vulnerability and configuration data. (NICE A0001)

DAT.A.2 Apply front-end collection systems, including traffic collection, filtering, and selection, to identify security threats. (NICE K0143)

DAT.A.3 Use Boolean operators to construct simple and complex queries. (NICE S0285)

DAT.A.4 Identify hidden patterns or relationships. (NICE S0109)

DAT.B Identify personal data sharing that places people at risk and evaluate risky personal data-sharing practices.

DAT.B.1 Understand that security and privacy concerns arise with data containing personal information.

DAT.B.5 Manage browser security settings to facilitate safe browsing.

DAT.C Describe the variety of abstractions used to represent data.

DAT.C.1 Digital data is represented by abstractions at different levels.

DAT.C.2 Data is represented using different number bases such as decimal and hexadecimal.

IOC.B Analyze the impact of cybersecurity on our national security, infrastructure, economy, and public health.

IOC.B.1 Identify the sectors of society that are at risk to cybersecurity breaches.

IOC.B.2 Weigh the outcomes of various types of computer “hacking”, including black, white, and gray.

IOC.B.3 Compare the motivations of different types of cybercrimes.

IOC.B.4 Describe the impact computer security (or lack thereof) has had on society.

CTT.A Select and apply appropriate computational tools and techniques to solve a problem or create value for others.

CTT.A.1 Select collaboration tools for data collection, writing, or protecting data.

CTT.A.2 Navigate and use unfamiliar documentation and public information to extend the student's own knowledge and to achieve a computational approach to solve a problem.

CTT.B Apply tools with varying levels of abstraction within software, a computer, a network, and the internet.

CTT.B.1 Recognize and discern between different levels of abstraction while working with computational tools.

CTT.B.2 Recognize the commonalities of command line tools and their automated, scripted versions.

CSN.A Describe the modular components of a computer’s hardware and software.

CSN.A.2 Identify the broad tasks that operating systems manage, such as process management and file management.

CSN.B Identify user actions that strengthen the security of information stored on a computer.

CSN.B.1 Navigate system files to locate files that are used to manage computer resources.

CSN.B.2 Manage system processes and user processes.

CSN.B.5 Manage software using configuration tools and/or parameters.

CSN.C Monitor, analyze, and manage active processes on a computer or network of computers.

CSN.C.1 Differentiate between user and system processes.

CSN.C.2 Identify and analyze potentially malicious/foreign processes.

CSN.C.3 Install, analyze and remove processes.

CSN.F Identify the components (software, hardware, protocols) that allow computers to network and communicate.

CSN.F.2 Diagram a network of computers.

CSN.F.3 Describe networking hardware.

CSN.F.6 Identify network system sub-components responsible for security.

CSN.F.7 Locate and solve security problem(s) within a network system's subcomponents.

CSN.G Analyze the evidence of web exploitations, both from front-end application and backend services perspective.

CSN.G.1 Identify websites that appear untrustworthy or dangerous to the end user.

CSN.G.2 Analyze security weaknesses in client-side (front-end) applications.

CSN.G.3 Analyze security weaknesses in server-side (back-end) web services.

CSN.G.4 Protect against web-based weaknesses.

CSN.H Perform ethical hacking to discover systems strengths and weaknesses.

CSN.H.1 Identify the risks and needs of ethical hacking.

CSN.H.3 Analyze system security to discover vulnerabilities and exploits.

CSN.I Identify user actions that strengthen the security of a networked system.

CSN.I.1 Recognize that the security of a network depends on the security of its individual components.

CSN.I.2 Manage settings and configuration files of software and/or drivers to maintain the security of the network.

CSN.J Use abstractions to manage and analyze information.

CSN.J.1 Use high- and/or low-level data analysis techniques to analyze network traffic.

CSN.J.2 Use a variety of data representations to help analyze large or complex data.

CSN.J.3 Identify the abstracted nature of network communication

Essential Question(s):	**Enduring Understanding(s):**

1.1: Why do people engage in risky behavior in cyberspace?

People engage in risky online behavior due to convenience, lack of awareness, curiosity, or overconfidence. Understanding human tendencies helps in developing strategies for safer online practices.

1.2: Is hacking ever appropriate?

While hacking is often associated with illegal activities, ethical hacking can be a legitimate and necessary practice to identify and fix vulnerabilities, ensuring stronger security systems.

1.3: What are the consequences of inappropriate behavior in cyberspace?

Inappropriate actions online can lead to personal, financial, legal, and societal repercussions. Responsible behavior helps maintain a safer and more respectful digital environment.

2.1: Why does information need protection?

Information requires protection to maintain its privacy, reliability, and accessibility. Safeguarding data ensures trust and prevents exploitation or unauthorized use.

2.2: How do computers safely store information?

Computers use encryption, access controls, and secure storage systems to protect data, ensuring its confidentiality and integrity while minimizing risks from unauthorized access or corruption.

3.1: How does past knowledge help with data analysis?

Analyzing past trends and patterns enables better predictions and decisions, helping to identify risks and opportunities in both cybersecurity and broader contexts.

4.1: How can information be safely exchanged?

Secure exchanges rely on encryption, authentication, and safe transmission protocols, ensuring that data remains private and reaches its intended recipient without being intercepted.

4.2: What makes a network vulnerable?

Networks are vulnerable due to weak passwords, outdated software, misconfigurations, or a lack of security protocols, making them susceptible to attacks.

4.3: How can we minimize network vulnerabilities?

Network vulnerabilities can be reduced by implementing firewalls, regular updates, strong authentication measures, and continuous monitoring for potential threats.

5.1: How can malware be stopped?

Malware can be stopped through a combination of proactive defenses like antivirus software, firewalls, and education about safe online practices, as well as swift response to detected threats.

6.1: Where and how are cybersecurity skills used?

Cybersecurity skills are applied in diverse fields, including finance, healthcare, government, and technology, to protect systems, data, and people from cyber threats.

Demonstration of Learning:

Students are tasked with securing an e-commerce website. The company is facing a series of cybersecurity challenges, and the students are responsible for designing the network, implementing security protocols, and ensuring the system is secure, efficient, and compliant with best practices.

Students submit a comprehensive security plan and presentation that includes:

- A network topology diagram with an explanation of how the design meets security needs.
- A list of security measures applied (encryption, access control, firewalls, etc.) with explanations of how they contribute to confidentiality, integrity, and availability.
- A report detailing how the vulnerabilities were identified and mitigated.
- A demonstration of the functioning website with security features such as MFA, encryption, and error message configurations.
- A summary of the backup and update strategy, including security protocols for data protection.

Students will demonstrate their learning by:

- Applying CIA levels of security to an e-commerce network.
- Identifying hardware necessary to create networks.
- Identifying network topology and creating a diagram to meet the security needs.
- Removing an unnecessary service (SMTP mail)
- Configuring error messages to be less revealing of system information.
- Classifying data based on sensitivity
- Implementing encryption protocols (e.g., SSL/TLS) to protect sensitive data during transmission.
- Utilizing strong access controls and authentication mechanisms to safeguard data access.
- Identifying potential vulnerabilities such as SQL injection, cross-site scripting (XSS), and inadequate authentication mechanisms.
- Implementing firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and block malicious activity.
- Regularly updating and patching software to protect against known vulnerabilities.
- Using multi-factor authentication (MFA) for employee access to sensitive systems and data.
- Ensuring secure backups of data to mitigate risks of data loss due to cyber incidents.
- Balancing security measures with user

	experience to ensure smooth website functionality. ● Optimizing website performance to handle high e-commerce traffic while maintaining security measures.
Family Overview	**Pacing for Unit**
PLTW Cybersecurity Family Overview (2024)	33 Days (Traditional) 17 Days (Block)
Unit-specific Vocabulary:	**Integration of Technology & Aligned Unit Materials, Resources, and Technology**
Section 2.1: E-Commerce, CIA Triad, Confidentiality, Availability, Integrity, Internet of Things, Passive Analysis, Protocol, host, URL, Web server, port, information architecture, domain name, IP Address, Security Baseline, Firewall, Topology Section 2.2: Unauthorized Hacking, Authorized Hacking, Ethical Hackers, Script Kiddie, Insider, Hacktivist, Cyber Syndicate, Warfare/Espionage, DDoS, Botnet, Keylogger, On Path Attack, Ransomware, Rootkit, Programming Errors, Ping Flood, Ping of Death, Smurf Attack, Mailbomb, Teardrop, site Certificate, Decrypt, Penetration test, Log Files, Forceful Browsing, Attack Surface, Loose-Lipped Error Section 2.3: Client, Abstracted, Exploits, Tag, Comment, Cross-site scripting, Linux, SQL Injection, Routing Table, Packet Sniffer, Packet Filtering, MAC Address, Front-end, Back-end, pcap File, Organizationally Unique Identifier, Network Interface Card, Broadcast, Transmission Control Protocol (TCP), TCP handshake, Transport Layer Security (TLS),	
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
Potential interdisciplinary connection may integrate ethical considerations in cybersecurity with principles of civic responsibility and democratic values. Students will explore how advancements in technology intersect with civil liberties, rights, and governance, fostering critical thinking and ethical reasoning	● Data on the internet is always secured with high confidentiality, high integrity, and is always available to its users. ● Websites do not share user information and browsing habits with other services. ● All data on a website is stored on one computer ● Data on the internet is always secured with high confidentiality, high integrity, and is always available to its users. ● All types of hacking are bad. ● Successful cyberattacks can only be carried out by sophisticated experts. ● Vulnerabilities of a website are only caused by poor programming techniques. ● Using default configurations is not a security risk. ● The more services a server provides the better. ● Using default configurations is not a security risk. ● The more services a server provides the better. ● Email service is necessary for all servers. ● Error messages are cryptic and do not provide useful information. ● Websites can only be exploited on the server level. ● It’s okay to exploit a website as long as you don’t

	intend to use any information you may come across in the process. ● When information is sent or received over the internet, it is transferred all at once. ● All malware is sophisticated and difficult to detect or stop. ● Log-in usernames and passwords are always hidden or kept secret when transferred around the internet, especially passwords because they're masked in the user interface, like *******. ● Once I am fully trained as a cybersecurity expert, my education will be complete. ● Security experts work in isolation all day. ● Solving problems is a linear process and does not require any iteration.
Differentiation through *Universal Design for Learning*	
UDL Indicator	**Teacher Actions:**

1. I CAN use the CIA triad to design a network security plan.

Engagement:

Real-World Examples: Start by discussing high-profile security breaches where the CIA triad (Confidentiality, Integrity, and Availability) could have been applied to prevent or mitigate the attack.

Scenario-Based Learning: Present a scenario (e.g., designing a security plan for an e-commerce site) and ask students how they would apply each element of the CIA triad.

Representation:

Infographics and Diagrams: Provide visual representations of the CIA triad and how each component relates to network security. Use simple diagrams to show the interplay between confidentiality, integrity, and availability in a network security plan.

Step-by-Step Guides: Offer a step-by-step guide on how to design a network security plan using the CIA triad, explaining key concepts like encryption (Confidentiality), checksums (Integrity), and backup systems (Availability).

Action/Expression:

Create a Network Security Plan: Have students use the CIA triad to design a network security plan for a hypothetical company, considering aspects like data encryption, user authentication, and network uptime.

Peer Review: Ask students to present their security plans to classmates, followed by peer feedback on how well they applied the CIA triad.

2. I CAN analyze computer systems while causing minimal impact.

Engagement:

Ethical Hacking Introduction: Begin with a discussion on ethical hacking, emphasizing the importance of conducting security analyses without disrupting system operations. Use real-world examples of ethical hackers performing security audits for companies.

Safety and Ethics Discussion: Have students discuss the ethical considerations of system analysis and the consequences of causing disruptions in a production environment.

Representation:

Simulation Tools: Provide access to simulation tools (e.g., virtual machines, penetration testing environments) where students can practice analyzing computer systems safely without impacting real systems.

Case Studies: Present case studies of ethical hacking, highlighting how attackers can exploit systems and how minimal-impact analysis tools were used to identify vulnerabilities.

Action/Expression:

Hands-On Practice: In a controlled environment (e.g., using virtual labs), have students perform penetration testing and vulnerability scanning with tools like Nmap or Nessus, ensuring minimal disruption.

Document Findings: Ask students to write a report on their findings from a system analysis, focusing on the security vulnerabilities they identified and how to fix them without causing system downtime.

3. I CAN identify network topology and create a diagram to meet the security needs.

Engagement:

Network Design Scenarios: Start with examples of different network topologies (e.g., star, bus, ring, mesh) and how they impact security. Discuss the benefits and challenges of each topology in securing a network.

Interactive Discussions: Engage students by discussing real-world network setups and how they are designed with security in mind (e.g., a corporate LAN vs. a home network).

Representation:

Network Diagrams: Provide students with pre-made network topology diagrams and explain how each component (routers, firewalls, switches) contributes to security.

Diagramming Tools: Introduce network diagramming software (e.g., Lucidchart, Microsoft Visio) and show how students can create and analyze security-focused network diagrams.

Action/Expression:

Create a Network Diagram: Have students design a network topology diagram that reflects security best practices (e.g., segmented networks, firewalls, DMZ) to meet specific needs (e.g., securing a financial institution).

Peer Review: Students can present their network diagrams to peers, explaining how their design addresses potential security vulnerabilities.

4. I CAN analyze a notorious malware attack called Stuxnet.

Engagement:

Real-World Case Study: Introduce the Stuxnet malware attack, a sophisticated cyberattack that targeted Iran's nuclear facilities, and discuss its impact on global cybersecurity.

Group Discussion: Facilitate a class discussion about the Stuxnet attack: how it was carried out, what vulnerabilities were exploited, and its implications for the future of cybersecurity.

Representation:

Documentaries/Case Studies: Show a video or documentary on Stuxnet to give students a deeper understanding of how the attack unfolded and how it was detected.

Timeline of Events: Provide a detailed timeline of the Stuxnet attack, breaking it down into phases (e.g., initial infection, spread, targeting, and discovery).

Action/Expression:

Research Assignment: Assign students to research the Stuxnet attack and write a report analyzing how it worked, the vulnerabilities it exploited, and the lessons learned.

Class Presentation: Students can present their findings on Stuxnet, proposing ways that similar attacks could be prevented in future systems.

5. I CAN exploit a website by uploading files to its root directory using anonymous FTP.

Engagement:

Ethical Hacking Discussion: Introduce the concept of anonymous FTP and its vulnerabilities. Discuss ethical considerations and the legal implications of exploiting website vulnerabilities.

Interactive Activity: Start with a demo or simulation that shows how FTP can be used to upload files and exploit websites.

Representation:

Step-by-Step Guide: Provide a detailed guide on how an attacker might exploit anonymous FTP access, and then explain how to protect against it (e.g., disabling anonymous FTP access).

Diagrams: Show diagrams of FTP file transfers and root directory structures to help students visualize how file uploads can lead to vulnerabilities.

Action/Expression:

Simulated Attack: In a controlled environment (e.g., virtual labs), allow students to perform an exploit by uploading files to a test server’s root directory and then ask them to demonstrate how to mitigate this risk.

Report on Mitigation: After completing the task, students should create a report explaining how they exploited the vulnerability and the steps necessary to prevent such an attack.

6. I CAN disable directory browsing from a client's web browser.

Engagement:

Security Scenarios: Begin with examples of how directory browsing can expose sensitive information on a website. Discuss how attackers can exploit this feature to gather files from a web server.

Discussion: Lead a class discussion on why disabling directory browsing is important and how it helps prevent unauthorized access to server files.

Representation:

Step-by-Step Tutorial: Provide a step-by-step guide on how to disable directory browsing in different web servers (e.g., Apache, Nginx).

Visual Examples: Show examples of a website's file structure with and without directory browsing enabled to help students understand the impact of this security setting.

Action/Expression:

Hands-On Configuration: Have students practice disabling directory browsing on a local or virtual web server.

Write a Report: After disabling directory browsing, students should document the process, explaining the importance of this setting in securing web applications.

7. I CAN manage and protect data from client-initiated attacks.

Engagement:

Real-World Attacks: Start with examples of client-initiated attacks such as SQL injection, cross-site scripting (XSS), or clickjacking, and explain how attackers target vulnerabilities in client systems.

Interactive Quiz: Use a quiz or game to test students' knowledge of common client-initiated attack techniques and the impact they can have on data protection.

Representation:

Visual Diagrams: Provide diagrams that show how client-initiated attacks work, including attack vectors and defense mechanisms.

Video Tutorials: Use videos to demonstrate how these attacks can be prevented, focusing on secure coding practices, input validation, and using firewalls to block malicious requests.

Action/Expression:

Simulate an Attack: Have students simulate a client-initiated attack on a test website and then work on implementing protections such as input validation or using prepared statements to prevent SQL injection.

Create a Data Protection Plan: Students can create a plan for protecting client data in an application, specifying security measures like encryption, secure sockets layer (SSL), and regular updates.

8. I CAN use Wireshark to identify attack data related to a common network tool.

Engagement:

Introduction to Wireshark: Introduce Wireshark as a tool for network analysis and packet sniffing. Start with a demonstration of how to use Wireshark to monitor network traffic.

Attack Scenarios: Present scenarios in which Wireshark can help detect common attacks (e.g., DDoS, MITM attacks, DNS poisoning).

Representation:

Wireshark Walkthrough: Provide a walkthrough of Wireshark's interface, explaining how to capture, filter, and analyze network packets. Show examples of attack data in the packet logs.

Attack Case Studies: Use case studies to demonstrate how Wireshark was used to identify and mitigate network attacks in real-world situations.

Action/Expression:

Hands-On Lab: Have students capture network traffic using Wireshark and analyze it for signs of attack (e.g., unusual traffic patterns or suspicious protocols).

Reporting Findings: Students should write a report detailing the attack data they identified, explaining the type of attack and how Wireshark helped detect it.

Supporting Multilingual/English Learners

Related *CELP standards:*	**Learning Targets:**

Learning Target 1: I can use the CIA triad to design a network security plan.

- **Level 1:** Can recognize the basic concepts of the CIA triad (Confidentiality, Integrity, Availability) with support. May be able to identify simple examples of network security.
- **Level 2:** Can describe the three components of the CIA triad and their role in network security (e.g., keeping data private, ensuring it's not altered, and accessible when needed).
- **Level 3:** Can explain how the CIA triad informs decisions in network security, including how to balance the three principles when designing a network security plan.
- **Level 4:** Can apply the CIA triad to design a basic network security plan, ensuring that confidentiality, integrity, and availability are addressed through access controls, encryption, and redundancy.
- **Level 5:** Can design a comprehensive network security plan incorporating the CIA triad principles, including advanced techniques like encryption protocols, secure access policies, and disaster recovery planning. Can analyze and adjust security measures based on real-world threats and business requirements.

Learning Target 2: I can analyze computer systems while causing minimal impact.

- **Level 1:** Can recognize that computer systems should be analyzed in a way that does not cause harm. May need support in understanding how to perform safe analysis.

- **Level 2:** Can describe basic methods for analyzing computer systems, such as using diagnostic tools or checking system performance, while minimizing impact (e.g., avoiding system crashes).
- **Level 3:** Can explain and apply techniques for analyzing computer systems without disrupting normal operations (e.g., using non-intrusive scanning tools or running tests in controlled environments).
- **Level 4:** Can perform detailed system analysis while minimizing risk and system downtime. Can use advanced tools (e.g., virtual machines or sandbox environments) to perform tests without impacting the production environment.
- **Level 5:** Can perform comprehensive system analysis with minimal impact on system functionality. Can identify and mitigate potential risks during analysis and use advanced methodologies (e.g., penetration testing, forensic analysis) to ensure systems remain secure during review.

Learning Target 3: I can identify network topology and create a diagram to meet the security needs.

- **Level 1:** Can recognize basic network components (e.g., routers, switches, devices). May need assistance in understanding network topology and security requirements.
- **Level 2:** Can describe simple network topologies (e.g., star, bus, mesh) and their basic components. Can identify some security needs in a basic network.
- **Level 3:** Can explain the concept of network topology and how different types of topologies influence security measures. Can create a simple network diagram that meets basic security requirements (e.g., firewalls, VPNs).
- **Level 4:** Can analyze the security needs of a network and create a detailed network diagram that incorporates security features such as access control lists (ACLs), firewalls, and intrusion detection/prevention systems (IDPS).
- **Level 5:** Can design and document advanced network topologies that address complex security needs, including multi-layer security, redundancy, and segmentation. Can create diagrams that balance both performance and security, ensuring scalability and fault tolerance.

Learning Target 4: I can analyze a notorious malware attack called Stuxnet.

- **Level 1:** Can recognize the term "Stuxnet" and understand it as a type of malware. May need assistance in grasping its impact.
- **Level 2:** Can describe the basics of the Stuxnet malware attack, such as it being a virus that targeted industrial systems. Can identify the affected systems (e.g., SCADA systems).
- **Level 3:** Can explain how Stuxnet was able to exploit vulnerabilities and spread across networks. Can describe the basic mechanism of how it caused damage to industrial control systems.
- **Level 4:** Can analyze the detailed functioning of Stuxnet, identifying specific vulnerabilities it exploited, such as zero-day exploits, and its impact on critical infrastructure. Can discuss its historical significance in the context of cyber warfare.
- **Level 5:** Can critically evaluate Stuxnet as a case study in cyber threats, discussing its implications on international cybersecurity policy, advanced malware tactics, and the future of industrial security. Can recommend security strategies to defend against similar attacks.

Learning Target 5: I can exploit a website by uploading files to its root directory using anonymous FTP.

- **Level 1:** Can recognize the concept of FTP (File Transfer Protocol) and understand the potential risks of improper configuration. May need support in understanding how anonymous FTP works.
- **Level 2:** Can describe what FTP is and how it can be used to upload files to a website. Can explain the potential vulnerabilities of anonymous FTP access.
- **Level 3:** Can demonstrate how improper FTP configuration can allow unauthorized file uploads to a website. Can describe the risks associated with anonymous FTP access.
- **Level 4:** Can exploit a website by uploading files to its root directory through anonymous FTP in a controlled, ethical hacking environment. Can identify vulnerabilities in FTP configuration that could allow this type of attack.
- **Level 5:** Can assess and exploit FTP misconfigurations to identify potential security flaws, while understanding the ethical implications. Can recommend corrective measures, such as disabling anonymous FTP, enforcing authentication, and securing FTP access to prevent such attacks.

Learning Target 6: I can disable directory browsing from a client's web browser.

- **Level 1:** Can recognize that directory browsing is a potential security risk. May need assistance in understanding how to disable it.
- **Level 2:** Can describe what directory browsing is and why it might be a security concern. Can explain the basic concept of restricting web server access to directories.
- **Level 3:** Can explain how to disable directory browsing in a web server configuration (e.g., through .htaccess

file or server settings). Can identify the risks of allowing directory browsing.

- **Level 4:** Can configure a web server to prevent directory browsing, enhancing security by limiting the visibility of directory contents. Can apply these settings across various types of web servers (e.g., Apache, Nginx).
- **Level 5:** Can implement and test directory browsing restrictions across a range of web applications, ensuring that server configurations are secure and robust against unauthorized access. Can educate clients on the risks of directory browsing and recommend security best practices.

Learning Target 7: I can manage and protect data from client-initiated attacks.

- **Level 1:** Can recognize that data protection is important when interacting with clients. May need assistance in understanding how client-initiated attacks work.
- **Level 2:** Can describe basic methods to protect data from attacks, such as using passwords or encrypting sensitive information. Can identify some types of client-initiated attacks (e.g., phishing, SQL injection).
- **Level 3:** Can explain how to protect data from client-initiated attacks by using techniques like encryption, input validation, and secure authentication. Can describe common attack vectors and how they target data.
- **Level 4:** Can implement strategies to protect data from client-initiated attacks, including secure communication protocols (e.g., HTTPS), data validation, and access control. Can monitor and respond to potential security incidents.
- **Level 5:** Can develop comprehensive security policies and procedures to safeguard data from client-initiated attacks. Can use advanced techniques like threat modeling, penetration testing, and security audits to identify and mitigate vulnerabilities before attacks occur.

Learning Target 8: I can use Wireshark to identify attack data related to a common network tool.

- **Level 1:** Can recognize the basic purpose of Wireshark (e.g., capturing network traffic). May need guidance in understanding how to use it to detect attacks.
- **Level 2:** Can describe how Wireshark captures network data and how it can be used to monitor network traffic. Can identify simple network traffic patterns.
- **Level 3:** Can use Wireshark to capture and analyze network traffic, identifying basic indicators of network attacks (e.g., unusual traffic spikes, unauthorized requests).
- **Level 4:** Can analyze network traffic in detail using Wireshark, identifying attack patterns (e.g., denial-of-service, man-in-the-middle). Can use filters to isolate relevant data related to a suspected attack.
- **Level 5:** Can use Wireshark to conduct in-depth network analysis, identifying complex attack data, such as advanced persistent threats or malware communication. Can apply expert-level knowledge to interpret traffic and identify sophisticated attack vectors.

Lesson Sequence	Learning Target	Success Criteria/Assessment/Resources
1	I CAN use the CIA triad to design a network security plan	• I can discuss data confidentiality, integrity, and availability • I can define the internet of things • I can protect against website tracking
2	I CAN analyze computer systems while causing minimal impact	• I can identify web ownership • I can observe website traffic • I can learn about domain names and IP addresses • I can identify ports and their services
3	I CAN identify network topology and create a diagram to meet the security needs.	• I can apply CIA levels of security to the e-commerce architecture of the Bikes, Boards, and Beyond network • I can identify hardware necessary to create the network
4	I CAN analyze a notorious malware attack called Stuxnet	• I can define malware • I can discuss motivations of malicious users • I can identify malware types and levels of sophistication
5	I CAN exploit a website by uploading files to its root directory using anonymous FTP.	• I can understand how web servers organize files • I can investigate a web server for directory browsing and log file location vulnerabilities

		● I can use anonymous FTP to update a web server.
6	I CAN disable directory browsing from a client's web browser	● I can mitigate web server vulnerabilities including directory browsing, default log file location, and anonymous FTP
7	I CAN manage and protect data from client-initiated attacks.	● I can identify client-server architecture. ● I can explore JavaScript programs. ● I can recognize and mitigated cross-site scripting exploits and SQL injection exploits
8	I CAN use Wireshark to identify attack data related to a common network tool	● I can learn basic network topology ● I can monitor and analyze data packets ● I can witness and mitigate a ping flood attack

Unit Title:

Unit 3: Network Security

Relevant Standards: Bold indicates priority

COM.B Recognize documentation as an indispensable part of the security process.

COM.B.1 Maintain a detailed record of the process and the steps used to solve a problem.

ERM.C Access safely, manage safely, and attribute information using effective and secure strategies.

ERM.C.1 Use advance search tools, Boolean logic, and key words to refine the search focus and/or limit search results based on a variety of factors (e.g., limiting by domain or site).

CCP.B Create a computational artifact for creative expression.

CCP.B.1 Identify a computational artifact as something created by a human using a computer and differentiate between a program, an image, audio, a video, a presentation, or a web page file.

CCP.C Deconstruct a complex problem into simpler parts.

CCP.C.1 Identify and apply solutions to subcomponents to achieve a system-wide solution.

CCP.E Engage stakeholder in a problem and use their perspectives to shape the course of your development.

CCP.E.1 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, nonrepudiation). (NICE A0123)

CCP.E.3 Share meaningful insights about the context of an organization's threat environment that improve its risk management posture. (NICE A0120)

CCP.F Apply and describe the process based on user-centered research to solve a problem.

CCP.F.1 Apply and describe the process used during the development of a solution

CCP.F.2 Acknowledge that stages of failure and technical hurdles are typical in processes that produce positive outcomes.

IARP.B Analyze the evidence of an attack.

IARP.B.1 Identify common types of malware.

IARP.B.2 Use knowledge of historical malware attacks to evaluate modern threats.

IARP.C Design the correct level of protection by implementing the appropriate safeguards.

IARP.C.3 Protect against future information threats.

IARP.D Detect and analyze the occurrence of a cybersecurity event.

IARP.D.1 Use pattern finding techniques to determine trends in attack data.

IARP.D.2 Identify malicious network traffic.

IARP.D.3 Analyze attack data to determine the source of the attack and the harmful effects it may have on the system.

IARP.E Respond to a detected cybersecurity event.

IARP.E.1 Communicate the event.

IARP.E.2 Discuss recovery methods for data, capabilities, or services that were impaired due to a cybersecurity event.

IARP.E.3 Remove threats and update protections.

DAT.A Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.

DAT.A.1 Identify systemic security issues based on the analysis of vulnerability and configuration data. (NICE A0001)

DAT.A.2 Apply front-end collection systems, including traffic collection, filtering, and selection, to identify security threats. (NICE K0143)

DAT.A.3 Use Boolean operators to construct simple and complex queries. (NICE S0285)

DAT.A.4 Identify hidden patterns or relationships. (NICE S0109)

DAT.C Describe the variety of abstractions used to represent data.

DAT.C.1 Digital data is represented by abstractions at different levels.

DAT.C.2 Data is represented using different number bases such as decimal and hexadecimal.

IOC.B Analyze the impact of cybersecurity on our national security, infrastructure, economy, and public health.

IOC.B.1 Identify the sectors of society that are at risk to cybersecurity breaches.

IOC.B.2 Weigh the outcomes of various types of computer "hacking", including black, white, and gray.

IOC.B.3 Compare the motivations of different types of cybercrimes.

CTT.A Select and apply appropriate computational tools and techniques to solve a problem or create value for others.

CTT.A.1 Select collaboration tools for data collection, writing, or protecting data.

CTT.A.2 Navigate and use unfamiliar documentation and public information to extend the student's own knowledge and to achieve a computational approach to solve a problem.

CTT.B Apply tools with varying levels of abstraction within software, a computer, a network, and the internet.

CTT.B.1 Recognize and discern between different levels of abstraction while working with computational tools.

CTT.B.2 Recognize the commonalities of command line tools and their automated, scripted versions.

SA.B Express an algorithm in a language.

SA.B.1 Analyze software algorithms and configuration files, including comments or pseudocode.

SA.C Use encryption algorithms to secure information.

SA.C.3 Apply encryption algorithms to encode or decode data digitally.

CSN.A Describe the modular components of a computer's hardware and software.

CSN.A.1 Identify the hardware components of a computer.

CSN.A.2 Identify the broad tasks that operating systems manage, such as process management and file management.

CSN.B Identify user actions that strengthen the security of information stored on a computer.

CSN.B.1 Navigate system files to locate files that are used to manage computer resources.

CSN.B.2 Manage system processes and user processes.

CSN.B.3 Create strong passphrases.

CSN.B.4 Install and manage protective software, including updates and removal.

CSN.B.5 Manage software using configuration tools and/or parameters.

CSN.C Monitor, analyze, and manage active processes on a computer or network of computers.

CSN.C.1 Differentiate between user and system processes.

CSN.C.2 Identify and analyze potentially malicious/foreign processes.

CSN.C.3 Install, analyze and remove processes.

CSN.D Gain understanding of how an operating system is structured and works by navigating the file system and modifying files, extensions, rights, and visibility to better protect data.

CSN.D.1 Traverse a file system using command lines.

CSN.D.2 Use ownership and permissions to analyze digital assets.

CSN.D.3 Change file extensions and predict the effects of the change.

CSN.D.4 Manage file types, access rights, and visibility of files.

CSN.D.5 Organize a file system.

CSN.D.6 Search a file system.

CSN.F Identify the components (software, hardware, protocols) that allow computers to network and communicate.

CSN.F.1 Define the boundary of a network (the network edge)

CSN.F.2 Diagram a network of computers.

CSN.F.3 Describe networking hardware.

CSN.F.4 Determine the security configurations of a wireless network.

CSN.F.6 Identify network system sub-components responsible for security.

CSN.F.7 Locate and solve security problem(s) within a network system's subcomponents.

CSN.G Analyze the evidence of web exploitations, both from front-end application and backend services perspective.

CSN.G.2 Analyze security weaknesses in client-side (front-end) applications.

CSN.G.3 Analyze security weaknesses in server-side (back-end) web services.

CSN.G.4 Protect against web-based weaknesses.

CSN.H Perform ethical hacking to discover systems strengths and weaknesses.

CSN.H.1 Identify the risks and needs of ethical hacking.

CSN.H.2 Identify the various stages of ethical hacking.

CSN.H.3 Analyze system security to discover vulnerabilities and exploits.

CSN.I Identify user actions that strengthen the security of a networked system.

CSN.I.1 Recognize that the security of a network depends on the security of its individual components.

CSN.I.2 Manage settings and configuration files of software and/or drivers to maintain the security of the network.

CSN.J Use abstractions to manage and analyze information.

CSN.J.1 Use high- and/or low-level data analysis techniques to analyze network traffic.

CSN.J.2 Use a variety of data representations to help analyze large or complex data.

CSN.J.3 Identify the abstracted nature of network communication

Essential Question(s):	**Enduring Understanding(s):**

1.2: Is hacking ever appropriate? Hacking can be ethical when used to identify and fix security vulnerabilities. This practice, known as ethical hacking, helps protect systems and data while promoting responsible and lawful behavior in cyberspace. 2.2: How do computers safely store information? Computers use encryption, secure storage practices, and access controls to protect data, ensuring it is kept private, accurate, and safe from unauthorized access or alteration. 3.1: How does past knowledge help with data analysis? Using historical data helps identify patterns, predict outcomes, and make informed decisions. In cybersecurity, understanding past events aids in recognizing potential threats and improving defenses. 4.1: How can information be safely exchanged? Safe information exchange relies on encryption, secure communication protocols, and authentication to prevent unauthorized access and protect data integrity during transmission. 4.2: What makes a network vulnerable? Networks are vulnerable due to weak security measures, outdated software, misconfigurations, and human error. Identifying and addressing these weaknesses is crucial to maintaining secure systems. 5.1: How can malware be stopped? Malware can be prevented and stopped through a combination of proactive measures like antivirus software, firewalls, education, regular updates, and swift responses to threats. 6.1: Where and how are cybersecurity skills used? Cybersecurity skills are essential across industries like healthcare, finance, government, and technology, where they protect sensitive information, maintain system integrity, and defend against cyberattacks. 7.1: What makes a good cyber team? A good cyber team is built on collaboration, diverse skills, effective communication, and professionalism. Team members must work together to solve problems, adapt to new challenges, and uphold ethical standards in cybersecurity.	
Demonstration of Learning:	
A comprehensive penetration testing and malware detection exercise on a Linux-based system. In this scenario, students will be tasked with detecting, analyzing, and responding to a series of simulated security incidents on a Linux system. Here's how you could break it down: Students submit the following documentation as part of their final demonstration: ● Malware Detection and Removal Report: Including a list of detected malware, processes, files, and steps taken to remove them. ● Pen Test Report: Detailing reconnaissance, vulnerabilities discovered, exploitation attempts, and remediation actions. ● Security Incident Response Report: Documenting the breach, response, and recovery efforts. ● Packet Analysis Report: Highlighting the differences between normal and malicious traffic and suggesting how such traffic can be detected. ● Log and Traffic Analysis Report: Explaining where the security breach occurred, how it was identified through log and traffic analysis, and recommendations for future monitoring.	Students will demonstrate their learning by: ● Detecting malware on a Linux®-based operating system. ● Identifying malicious files, processes, and users on the system. ● Securing a system by removing the detected malware. ● Using reconnaissance, scanning, compromise, and remediation to identify and remove system vulnerabilities. ● Creating a Pen Test report. ● Using packet analysis to compare safe, normal traffic to suspicious, malicious traffic. ● Creating a Security Incident Response Report. ● Analyzing network logs and traffic patterns to pinpoint where security breaches occur
Family Overview	**Pacing for Unit**
PLTW Cybersecurity Family Overview (2024)	46 Days (Traditional) 23 Days (Block)
Unit-specific Vocabulary:	**Integration of Technology &** **Aligned Unit Materials, Resources, and Technology**

3.1 Files and Processes: File system, Argument, Concatenate, Access control, AASCII, GNU, Open source, Shell, Pipe, Spawn, Background process, Root directory, 3.2 Attacks from the Net: Abstraction, Security baseline, Subnet, Ethical hacking, Reconnaissance, Scanning, Compromise, Remediation, Service, TCP handshake, Banner grabbing, Security framework, NIC 3.3 Analyzing the Net: Packet-switched, Address Resolution Protocol (ARP), ARP poisoning, Internet Control Messaging Protocol (ICMP), DoS, Maximum Transition Unit (MTU), Ethernet, Encryption, Spectrum analyzer, IEEE, Channels, WAP, WEP, Authentication protocol	
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
Potential interdisciplinary connection may integrate ethical considerations in cybersecurity with principles of civic responsibility and democratic values. Students will explore how advancements in technology intersect with civil liberties, rights, and governance, fostering critical thinking and ethical reasoning	● All operating systems are the same, they just have different names ● Cybersecurity careers are all technical. ● Cybersecurity educational paths always require a four-year college degree. ● Cybersecurity career opportunities are limited. ● Network traffic is always different so patterns of normal traffic cannot be determined. ● There is no way to detect unusual activity on a network ● Firewall rules are only configured on the physical pfSense firewall (the edge of the network). ● Hacking is always harmful to a network and only done by cyber attackers. ● It is completely acceptable to use scanning and compromise tools to investigate public hosts on the internet, as long as we don't intend to do major harm. ● Packets are too detailed to be used to analyze larger issues like exploits and malware. ● Malicious network traffic does not look anything like legitimate, healthy network traffic. ● Network traffic changes drastically between network configurations, and it is difficult to apply previous knowledge to new traffic. ● A slow network is always due to heavy traffic or low bandwidth.
Differentiation through *Universal Design for Learning*	
UDL Indicator	**Teacher Actions:**
1. I CAN use the command line to navigate the file system and to manage files and directories. *Engagement:* Start with an interactive demonstration of common command-line commands (e.g., `cd`, `ls`, `mkdir`, `rm`) in a terminal, allowing students to follow along. Present practical scenarios, such as organizing a project directory or cleaning up files, to show the relevance of mastering command-line navigation. *Representation:* Provide students with visual command-line cheat sheets or slides with syntax examples and common commands for file management. Show the command structure (e.g., `command [options] [arguments]`) with explanations of what each part does. *Action/Expression:* Have students practice by navigating the file system, creating directories, moving files, and deleting files using	

the command line. Assign a project where students must organize files in a directory structure and then manage or back up their files using specific commands.

2. I CAN utilize ownership and permission setting to analyze files.

Engagement:

Begin with an example of a company where sensitive files need restricted access. Ask students why setting ownership and permissions is important in such environments. Facilitate a class discussion on how misconfigured permissions can lead to security breaches or unauthorized access.

Representation:

Provide diagrams or charts showing how ownership and permissions work in Linux, including user, group, and other categories. Use a detailed step-by-step guide to show how to check and modify file permissions using commands like `chmod`, `chown`, and `chgrp`.

Action/Expression:

Have students practice changing file ownership and permissions using the `chown` and `chmod` commands to allow or deny access. Ask students to review a set of files with incorrectly set permissions and identify the problems, then fix the permissions according to best practices.

3. I CAN manage processes and services in a Linux®-based system.

Engagement:

Start with a scenario where managing services (e.g., a web server) is critical for system performance or security. Ask students how they think processes and services are managed on a server and why it's important to be able to start, stop, or monitor them.

Representation:

Use flowcharts to illustrate how processes are managed in Linux, showing parent-child relationships and process IDs (PIDs). Provide a list of useful commands like `ps`, `top`, `kill`, `systemctl`, and `service`, explaining their purpose and syntax.

Action/Expression:

Have students list running processes using `ps` and `top`, and stop or restart services using `systemctl` or `service`. Ask students to configure a service (e.g., Apache or SSH) to start at boot and then manually start and stop the service.

4. I CAN create an education/career plan.

Engagement:

Begin with a discussion on various careers in cybersecurity, networking, and IT, and how creating a plan can help students achieve their career goals. Invite professionals from the industry to discuss their career paths and provide advice on how to get started in the field.

Representation:

Provide students with a framework for setting long-term goals, such as SMART goals (Specific, Measurable, Achievable, Relevant, Time-bound). Provide examples of common career paths (e.g., cybersecurity analyst, network engineer) and certifications or degrees that help students advance.

Action/Expression:

Have students create a career plan that outlines their current skills, desired career, and the steps they will take (e.g., certifications, degrees, experience) to reach their goal. Have students share and provide feedback on each other’s career plans, offering suggestions and advice.

5. I CAN create a security baseline of network traffic.

Engagement:

Present a scenario where students need to establish a baseline of normal network traffic for a company. Discuss why this baseline is important for identifying malicious activity. Provide a simulated network environment where students can observe normal traffic patterns and discuss what constitutes "normal" vs. "abnormal."

Representation:

Use network diagrams to show what typical traffic should look like under normal conditions and how anomalies might be detected. Introduce traffic analysis tools like Wireshark and NetFlow, showing how they can be used to establish and monitor a baseline.

Action/Expression:

Have students use network monitoring tools to capture traffic data and establish a baseline of what normal traffic looks like for a test network. Ask students to document their findings, outlining what types of traffic are normal and what constitutes suspicious activity.

6. I CAN configure firewall rules to improve security.

Engagement:

Begin by discussing the role of firewalls in protecting a network and why configuring them properly is critical. Use case studies of real network attacks where poorly configured firewalls were a contributing factor to a security breach.

Representation:

Provide examples of firewall configuration rules (e.g., blocking certain ports, allowing specific IP addresses). Show firewall rule diagrams illustrating how traffic flows through different ports and how rules are applied to allow or deny traffic.

Action/Expression:

Have students configure firewall rules using `iptables` or `ufw` on a Linux system to control incoming and outgoing traffic based on specified criteria. Assign a lab where students must configure a firewall to allow necessary traffic (e.g., web traffic) while blocking unwanted traffic (e.g., HTTP on non-standard ports).

7. I CAN apply ethical hacking techniques to test and identify system vulnerabilities.

Engagement:

Introduce students to ethical hacking, highlighting the difference between ethical hacking (legal) and black-hat hacking (illegal). Present a scenario where students need to conduct a penetration test to identify system vulnerabilities in a controlled, ethical manner.

Representation:

Demonstrate the use of penetration testing tools like Kali Linux, Metasploit, and Nmap, and explain how each tool is used to find vulnerabilities. Show diagrams of common vulnerabilities (e.g., SQL injection, cross-site scripting) and explain how they are tested for in ethical hacking.

Action/Expression:

Have students perform a penetration test on a simulated vulnerable system, identifying and exploiting weaknesses in a controlled lab environment. After completing the test, ask students to write a detailed report on the vulnerabilities they discovered and how to mitigate them.

8. I CAN use Wireshark to perform an in-depth packet analysis on Address Resolution Protocol (ARP) data.

Engagement:

Start with an explanation of ARP (Address Resolution Protocol) and its role in mapping IP addresses to MAC addresses in a network. Show how ARP traffic can be captured in Wireshark and explain its role in network monitoring.

Representation:

Teach students how to use filters in Wireshark to isolate ARP packets for detailed analysis. Provide examples of ARP packets and explain the details of the captured data, such as ARP requests and responses.

Action/Expression:

Have students capture ARP packets in a controlled network environment using Wireshark and analyze the data to identify ARP requests and responses. Ask students to write a report on their analysis, identifying potential issues like ARP spoofing or unauthorized devices on the network.

9. I CAN analyze normal and malicious network traffic related to IP fragmentation.

Engagement:

Introduce the concept of IP fragmentation, explaining how large packets are broken into smaller fragments for transmission and why this can be exploited by attackers. Present examples of how IP fragmentation can be used for network attacks, such as fragment overlap attacks or DDoS amplification.

Representation:

Use diagrams to show how IP fragmentation works and how malicious traffic might exploit fragmented packets. Show how tools like Wireshark can be used to capture and analyze fragmented packets, with a focus on detecting unusual fragment patterns.

Action/Expression:

Have students capture and analyze fragmented packets in a network environment using Wireshark, distinguishing between normal and malicious fragmented traffic. Ask students to document their findings, identifying potential attacks using IP fragmentation and ways to mitigate them.

10. I CAN analyze normal and malicious network traffic related to user access and authentication to a wireless device.

Engagement:

Start with a discussion of how wireless networks use authentication protocols (e.g., WPA2) to secure access, and why analyzing authentication traffic is critical for network security. Present examples of common wireless attacks like WPA handshake cracking or rogue access points.

Representation:

Provide students with packet capture examples of normal vs. malicious wireless traffic, showing key elements like SSIDs, BSSIDs, and authentication frames. Explain the role of encryption and authentication in protecting wireless networks.

Action/Expression:

Have students capture wireless network traffic using tools like Wireshark or Aircrack-ng, analyzing authentication packets to identify potential vulnerabilities or attacks. Ask students to document their analysis, identifying legitimate and suspicious access attempts, and recommend security improvements.

Supporting Multilingual/English Learners

Related *CELP standards:*	**Learning Targets:**

Learning Target 1: I can use the command line to navigate the file system and to manage files and directories.

- **Level 1:** Can recognize basic command line concepts (e.g., "file," "folder") with support. May need help using simple commands.
- **Level 2:** Can use basic command line commands to navigate the file system (e.g., `cd`, `ls`) and perform simple file management tasks (e.g., creating, renaming files or directories).
- **Level 3:** Can effectively navigate directories, create and delete files and directories, and use more advanced commands (e.g., `cp`, `mv`, `rm`). Can explain the basic structure of a file system.
- **Level 4:** Can manage files and directories using advanced command line tools (e.g., `find`, `grep`, `chmod`) for searching, filtering, and modifying files. Can perform batch file management tasks with scripts.
- **Level 5:** Can navigate and manage complex file systems and automate file and directory management tasks using advanced command line techniques. Can troubleshoot file system issues and optimize system file structures.

Learning Target 2: I can utilize ownership and permission setting to analyze files.

- **Level 1:** Can recognize that files have owners and permissions. May need assistance understanding the concept of file ownership.
- **Level 2:** Can identify basic file permissions (e.g., read, write, execute) and understand file ownership. Can view file permissions using commands like `ls -l`.
- **Level 3:** Can explain how file ownership and permissions control access to files and directories. Can change file ownership and modify permissions using commands like `chown` and `chmod`.
- **Level 4:** Can analyze file ownership and permissions to determine potential security risks (e.g., files with weak permissions). Can configure access control lists (ACLs) for advanced permission management.
- **Level 5:** Can assess and manage file ownership and permissions at a system level to ensure secure and effective access control. Can automate permission auditing and troubleshoot complex permission issues in multi-user systems.

Learning Target 3: I can manage processes and services in a Linux®-based system.

- **Level 1:** Can recognize that a system runs processes and services. May need assistance in identifying running processes.
- **Level 2:** Can view basic system processes using commands like `ps` or `top`. Can start and stop simple services (e.g., using `systemctl` or `service` commands).
- **Level 3:** Can manage processes and services, including starting, stopping, and restarting services. Can monitor system performance and resource usage using commands like `htop` or `top`.
- **Level 4:** Can manage background processes (e.g., using `nohup`, `screen`, or `tmux`). Can troubleshoot and optimize service performance, ensuring services are running correctly and efficiently.
- **Level 5:** Can configure and automate processes and services for system optimization, security, and performance. Can analyze process dependencies, manage service failures, and automate service monitoring using scripts or tools like `systemd`.

Learning Target 4: I can create an education/career plan.

- **Level 1:** Can recognize the importance of planning for education and career development. May need guidance in creating specific goals.
- **Level 2:** Can describe their interests and career aspirations. Can set simple education or career goals (e.g., "I want to be a network administrator").
- **Level 3:** Can create a basic plan for education and career development, including short- and long-term goals. Can research potential career paths and the necessary education or certifications.
- **Level 4:** Can design a detailed education and career plan that includes specific courses, certifications, and

professional experience needed to achieve career goals. Can outline a timeline for achieving milestones.
- **Level 5:** Can develop a comprehensive and adaptable education/career plan, including backup strategies, ongoing professional development, and networking strategies. Can evaluate and adjust the plan as opportunities and challenges arise in the field.

Learning Target 5: I can create a security baseline of network traffic.

- **Level 1:** Can recognize that network traffic can be monitored for security purposes. May need guidance in identifying what constitutes normal vs. suspicious traffic.
- **Level 2:** Can describe the concept of network traffic baselines (e.g., expected volume, types of communication). Can use basic tools to capture network traffic.
- **Level 3:** Can establish a security baseline by capturing and analyzing network traffic. Can identify normal traffic patterns and baseline expectations for network activity.
- **Level 4:** Can create a comprehensive network traffic baseline using advanced tools (e.g., Wireshark, NetFlow). Can compare baseline data to identify potential anomalies or security threats.
- **Level 5:** Can continuously monitor and adjust network traffic baselines to detect emerging threats. Can recommend and implement changes to network configurations or security protocols based on baseline analysis.

Learning Target 6: I can configure firewall rules to improve security.

- **Level 1:** Can recognize the basic purpose of a firewall. May need assistance in understanding how to configure rules.
- **Level 2:** Can describe basic firewall concepts, such as allowing or blocking specific traffic. Can configure simple firewall rules for inbound and outbound traffic.
- **Level 3:** Can configure advanced firewall rules to secure a network, including rules for different ports and protocols. Can test firewall configurations and troubleshoot issues.
- **Level 4:** Can create and manage firewall policies for complex network environments. Can optimize firewall settings to prevent unauthorized access and ensure secure traffic flow.
- **Level 5:** Can design, implement, and audit firewall configurations for large-scale or multi-network environments. Can integrate firewalls with other security technologies (e.g., IDS/IPS) and monitor for security incidents.

Learning Target 7: I can apply ethical hacking techniques to test and identify system vulnerabilities.

- **Level 1:** Can recognize ethical hacking as a method for identifying vulnerabilities. May need support in understanding hacking techniques.
- **Level 2:** Can describe basic ethical hacking concepts, such as penetration testing or vulnerability scanning. Can identify simple vulnerabilities using basic tools.
- **Level 3:** Can apply ethical hacking techniques, such as penetration testing or network scanning, to identify vulnerabilities in systems. Can report findings to improve system security.
- **Level 4:** Can conduct detailed penetration tests on systems or networks, identifying vulnerabilities and recommending remediation strategies. Can use advanced tools (e.g., Metasploit, Nmap) to test for weaknesses.
- **Level 5:** Can design and execute comprehensive ethical hacking assessments, including social engineering, web application testing, and post-exploitation analysis. Can create and present detailed vulnerability reports and assist in remediation efforts.

Learning Target 8: I can use Wireshark to perform an in-depth packet analysis on Address Resolution Protocol (ARP) data.

- **Level 1:** Can recognize ARP as a protocol used in networking. May need assistance in using Wireshark for packet analysis.
- **Level 2:** Can describe the purpose of ARP in a network and the basic concepts of packet analysis. Can use Wireshark to capture basic ARP packets.
- **Level 3:** Can analyze ARP packets using Wireshark, identifying key fields such as MAC addresses and IP addresses. Can describe how ARP is used in network communication.
- **Level 4:** Can perform detailed ARP analysis with Wireshark, identifying ARP poisoning attacks or other network anomalies. Can use Wireshark filters to isolate ARP traffic.
- **Level 5:** Can conduct advanced packet analysis of ARP traffic using Wireshark, identifying malicious activities (e.g., ARP spoofing). Can recommend and implement countermeasures to secure ARP traffic on a network.

Learning Target 9: I can analyze normal and malicious network traffic related to IP fragmentation.

- **Level 1:** Can recognize that network traffic can be fragmented. May need guidance in understanding what constitutes normal vs. malicious fragmentation.

- **Level 2:** Can describe the concept of IP fragmentation and how it is used in network communication. Can identify basic examples of fragmented packets.
- **Level 3:** Can analyze fragmented network traffic to identify typical fragmentation patterns. Can explain how malicious actors might exploit fragmentation to bypass security filters.
- **Level 4:** Can identify and analyze fragmented packets that could indicate malicious activity, such as fragmented denial-of-service (DoS) attacks. Can use tools like Wireshark to capture and inspect fragmented traffic.
- **Level 5:** Can conduct in-depth analysis of fragmented IP traffic, identifying complex attack patterns and mitigating potential risks. Can implement measures to detect and block fragmented traffic designed for exploitation.

Learning Target 10: I can analyze normal and malicious network traffic related to user access and authentication to a wireless device.

- **Level 1:** Can recognize the importance of network security for wireless devices. May need help in identifying normal vs. malicious network traffic.
- **Level 2:** Can describe the basic concepts of user access and authentication in wireless networks (e.g., WPA, WPA2). Can identify basic network traffic related to user authentication.
- **Level 3:** Can analyze network traffic related to wireless authentication and user access. Can differentiate between legitimate and suspicious access attempts.
- **Level 4:** Can identify and analyze malicious wireless access attempts (e.g., brute-force, rogue AP) and recommend security measures to prevent unauthorized access.
- **Level 5:** Can conduct comprehensive analysis of wireless network traffic, identifying complex threats such as man-in-the-middle attacks, and implementing strategies to secure wireless networks.

Lesson Sequence	Learning Target	Success Criteria/Assessment/Resources
1	I CAN use the command line to navigate the file system and to manage files and directories.	● I can describe the Linux operating system ● I can document a variety of Linux commands
2	I CAN utilize ownership and permission setting to analyze files	● I can identify various file types ● I can utilize file hiding and encryption techniques
3	I CAN manage processes and services in a Linux®-based system.	● I can examine a process tree to identify parent/child processes ● I can use search techniques for identifying suspicious processes ● I can terminate processes
4	I CAN create an education/career plan	● I can discover the many ways to begin a career in cybersecurity
5	I CAN create a security baseline of network traffic.	● I can identify the layered nature of network architecture.
6	I CAN configure firewall rules to improve security	● I can mimic suspicious activity on the water treatment plant network ● I can capture suspicious network traffic for comparison to baseline traffic ● I can analyze suspicious network traffic using network topology documents and baseline traffic
7	I CAN apply ethical hacking techniques to test and identify system vulnerabilities	● I can learn the four phases of ethical hacking to identify system vulnerabilities ● I can use tools such as nmap, Nessus, Metasploit, and iptables
8	I CAN use Wireshark to perform an in-depth packet analysis on Address Resolution Protocol (ARP) data	● I can understand how packets and network communication should behave ● I can observe what network traffic looks like during an exploit

		● I can analyze normal packet activity and distinguish it from the abnormal/suspicious packet activity
9	I CAN analyze normal and malicious network traffic related to IP fragmentation	● I can understand how data moves through a network ● I can use Wireshark graphs to help see data trends in very large capture files ● I can apply IP fragmentation attack prevention methods
10	I CAN analyze normal and malicious network traffic related to user access and authentication to a wireless device	● I can discuss the dangers of using public Wi-Fi ● I can understand the normal and abnormal network traffic related to wireless networks. ● I can used a capture file that contains Wi-Fi traffic from a Cisco wireless router (or WAP) to crack an encrypted password

Unit Title:

Unit 4: Applied Cybersecurity

Relevant Standards: Bold indicates priority

CCP.B Create a computational artifact for creative expression.

CCP.B.1 Identify a computational artifact as something created by a human using a computer and differentiate between a program, an image, audio, a video, a presentation, or a web page file.

CCP.C Deconstruct a complex problem into simpler parts.

CCP.C.1 Identify and apply solutions to subcomponents to achieve a system-wide solution.

CCP.F Apply and describe the process based on user-centered research to solve a problem.

CCP.F.1 Apply and describe the process used during the development of a solution

CCP.F.2 Acknowledge that stages of failure and technical hurdles are typical in processes that produce positive outcomes.

IARP.A Use digital forensics investigative techniques to solve a cybercrime

IARP.A.1 Define what constitutes a cybercrime.

IARP.A.2 Acquire and maintain data in compliance with the digital forensics process.

IARP.A.3 Analyze data associated with a digital forensics investigation.

IARP.A.4 Describe the potential legal ramifications of cybercrimes.

IARP.B Analyze the evidence of an attack.

IARP.B.1 Identify common types of malware.

IARP.C Design the correct level of protection by implementing the appropriate safeguards.

IARP.C.1 Describe the positive and negative outcomes of different solutions related to data confidentiality, integrity, and availability.

IARP.D Detect and analyze the occurrence of a cybersecurity event.

IARP.D.1 Use pattern finding techniques to determine trends in attack data.

IARP.E Respond to a detected cybersecurity event.

IARP.E.1 Communicate the event.

DAT.A Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.

DAT.A.1 Identify systemic security issues based on the analysis of vulnerability and configuration data. (NICE A0001)

DAT.A.4 Identify hidden patterns or relationships. (NICE S0109)

DAT.B Identify personal data sharing that places people at risk and evaluate risky personal data-sharing practices.

DAT.B.1 Understand that security and privacy concerns arise with data containing personal information.

DAT.B.2 Understand data mining techniques used to perform social engineering.

DAT.B.4 Evaluate attacks that occur via email.

DAT.C Describe the variety of abstractions used to represent data.

DAT.C.1 Digital data is represented by abstractions at different levels

DAT.C.2 Data is represented using different number bases such as decimal and hexadecimal.

CTT.A Select and apply appropriate computational tools and techniques to solve a problem or create value for others.

CTT.A.1 Select collaboration tools for data collection, writing, or protecting data.

CTT.B Apply tools with varying levels of abstraction within software, a computer, a network, and the internet.

CTT.B.1 Recognize and discern between different levels of abstraction while working with computational tools.

CTT.B.2 Recognize the commonalities of command line tools and their automated, scripted versions.

SA.A Analyze an algorithm used to encrypt or decrypt data.

SA.A.1 Understand that in cryptography, ciphers are used to encrypt and decrypt data

SA.A.2 Evaluate the effectiveness of historical ciphers used to encrypt and decrypt data

SA.A.3 Describe how public key/private key encryption uses algorithms to secure data

SA.C Use encryption algorithms to secure information.

SA.C.1 Create historical algorithmic cyphers to encrypt and decrypt data.

SA.C.2 Apply encryption algorithms to encode or decode data manually or unplugged.

SA.C.3 Apply encryption algorithms to encode or decode data digitally

CSN.A Describe the modular components of a computer's hardware and software.

CSN.A.1 Identify the hardware components of a computer.

CSN.A.2 Identify the broad tasks that operating systems manage, such as process management and file management.

CSN.B Identify user actions that strengthen the security of information stored on a computer.

CSN.B.1 Navigate system files to locate files that are used to manage computer resources.

CSN.B.4 Install and manage protective software, including updates and removal.

CSN.B.5 Manage software using configuration tools and/or parameters.

CSN.D Gain understanding of how an operating system is structured and works by navigating the file system and modifying files, extensions, rights, and visibility to better protect data.

CSN.D.6 Search a file system.

CSN.F Identify the components (software, hardware, protocols) that allow computers to network and communicate.

CSN.F.5 Define network addressing including sub-netting.

CSN.F.6 Identify network system sub-components responsible for security.

CSN.I Identify user actions that strengthen the security of a networked system.

CSN.I.1 Recognize that the security of a network depends on the security of its individual components.

CSN.J Use abstractions to manage and analyze information.

CSN.J.2 Use a variety of data representations to help analyze large or complex data.

Essential Question(s):	**Enduring Understanding(s):**

1.1 Why do people engage in risky behavior in cyberspace?

People engage in risky behavior in cyberspace due to factors such as lack of awareness, peer pressure, convenience, or the illusion of anonymity. Understanding these motivations helps in designing strategies to reduce harmful online actions and increase digital responsibility.

1.2 Is hacking ever appropriate?

Hacking can be appropriate when done ethically, such as in the case of ethical hacking or penetration testing. These practices help identify and fix vulnerabilities in systems, preventing malicious attacks and improving overall security.

1.3 What are the consequences of inappropriate behavior in cyberspace?

Inappropriate behavior in cyberspace, such as cyberbullying, hacking, or data theft, can lead to legal penalties, loss of trust, damage to reputations, and emotional harm. It is important to understand the lasting effects of online actions on individuals, organizations, and communities.

2.1 Why does information need protection?

Information needs protection to ensure its privacy, accuracy, and availability. Without proper protection, sensitive data can be stolen, misused, or corrupted, leading to personal, financial, and societal harm. Secure information is critical to maintaining trust in digital systems.

2.2 How do computers safely store information?

Computers safely store information through encryption, secure access controls, and physical security measures. These techniques protect data from unauthorized access and ensure its integrity and confidentiality over time.

3.1 How does past knowledge help with data analysis?

Past knowledge, including historical data and previous incidents, provides context for analyzing current data trends. It helps in identifying patterns, predicting future outcomes, and making informed decisions, especially when assessing risks and vulnerabilities in cybersecurity.

4.1 How can information be safely exchanged?

Information can be safely exchanged by using secure protocols, encryption, and authentication measures. These tools ensure that data is transmitted privately and accurately, protecting it from interception and unauthorized access during exchange.

4.2 What makes a network vulnerable?

A network becomes vulnerable due to weak passwords, outdated software, misconfigurations, poor access controls, and lack of monitoring. Identifying and addressing these vulnerabilities is key to preventing unauthorized access and maintaining a secure network.

5.1 How can malware be stopped?

Malware can be stopped through a combination of proactive defenses, such as antivirus software, firewalls, regular software updates, and educating users about recognizing malicious threats. A multi-layered approach minimizes the risk and impact of malware.

6.1 Where and how are cybersecurity skills used?

Cybersecurity skills are used in various industries, including healthcare, finance, government, and technology. These skills protect sensitive data, defend against cyberattacks, and ensure the integrity of systems across diverse fields, making them crucial for safeguarding digital infrastructure. 7.1 What makes a good cyber team? A good cyber team is characterized by diverse skills, strong collaboration, clear communication, and professionalism. Team members must work together, adapt to new challenges, and adhere to ethical practices to effectively address cybersecurity issues and protect systems.	
Demonstration of Learning:	
A forensic investigation simulation where students are tasked with solving a complex cybercrime scenario. They would need to recover files, analyze encrypted data, trace stolen information, and apply forensic and cybersecurity protocols to uncover the full story. Students submit the following as part of their final demonstration: ● File Recovery Report: Detailing the evidence recovered from the suspect's USB drive, including any hidden or deleted files. ● Forensic Analysis Report: A comprehensive analysis of encrypted file systems, steganographic images, encrypted emails, and malware source files, including findings and decryption or extraction methods used. ● Suspect Involvement Report: A report identifying the primary suspect and any accomplices, with supporting evidence linking them to the crime. ● Exfiltration Report: A report tracing the exfiltration of the confidential spreadsheet, detailing how the data was accessed, moved, or shared. ● Stolen Data Tracking Report: Documentation of how the stolen data was traced across networks, emails, or other communication channels. ● Executive Innocence Verification Report: An analysis confirming or disproving the executive's claim of innocence based on forensic evidence. ● Security Breach Analysis and Remediation Report: A final report outlining how the breach occurred, identifying weaknesses, and recommending improvements to security protocols to prevent future incidents.	Students will demonstrate their learning by: ● Recovering files and evidence from a suspect's USB flash drive. ● Analyzing encrypted file systems, steganographic images, encrypted emails, and malware source files. ● Determining a suspect's involvement, uncover accomplices, and locate the missing diamond. ● Investigating the exfiltration of a confidential spreadsheet ● Tracing stolen data ● Verifying the executive's claim of innocence and identifying potential security breaches. ● Applying forensic techniques and cybersecurity protocols to solve the data breach.
Family Overview	**Pacing for Unit**
PLTW Cybersecurity Family Overview (2024)	42 Days (Traditional) 21 Days (Block)
Unit-specific Vocabulary:	**Integration of Technology** **Aligned Unit Materials, Resources, and Technology**
Section 4.1 Cipher, cryptography, plaintext, ciphertext, substitution cipher, encryption key, private key encryption, symmetric key encryption, public key encryption, asymmetric key encryption, one-way functions, Encrypted Drive, Recovery Key, Container, Encrypted Container, Mount, Dismount, Hash, Cryptocurrency, Steganography, Least Significant Bit, ASCII, Insertion Steganography,	

Generation Steganography, Digital Watermarking, Steganalysis, Digital Forensic Team, Consent Form, Chain of Custody Section 4.2 Hash Function, Hashing, Message, Digest, Brute-force, Algorithm, Disk Image, Identity, Subnet, Subpoena, open source,	
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
Potential interdisciplinary connection may integrate ethical considerations in cybersecurity with principles of civic responsibility and democratic values. Students will explore how advancements in technology intersect with civil liberties, rights, and governance, fostering critical thinking and ethical reasoning	● Cryptography is something that developed around advances in computing, and has not been around that long. ● Cryptography only relies on knowledge of computing systems. ● Information exchanged in public is very difficult to keep private. ● There is only one secure method to encrypt data stored on a computer. ● It is possible to decrypt data without knowing the recovery key or the password. ● Changing the data, the bits and bytes, that make up an image results in obvious changes to the way we see the image. ● In performing an investigation, you know or can predict most of the steps you will take ahead of time. ● Digital evidence (and computer data) isn't fragile. ● Browsing around a computer is the best way to go about an investigation. ● Just collecting and examining a computer is enough to prove where the evidence on it came from. ● Only police officers gather digital evidence. ● Minor changes are hard to detect on a file system. ● Files you get from another source (like the internet) are always safe and untampered with. ● Just copying data is good enough to perform an investigation. ● Looking around a drive doesn't modify its contents. ● People are easy to find or to discover "who" they are on the internet. ● Emails are anonymous. ● Digital evidence is always easy to find. ● Digital forensic tools do all the work for me; I don't have to understand or interpret the data.
Differentiation through *Universal Design for Learning*	
UDL Indicator	**Teacher Actions:**
1. I CAN create encrypted messages using various strategies. *Engagement:* Start by discussing the importance of encryption in protecting sensitive data and why it's essential for securing communication. Present real-world examples of encryption, such as secure messaging apps or email encryption, to make the concept relatable. *Representation:* Provide examples of various encryption techniques, such as symmetric encryption (AES) and asymmetric encryption (RSA). Visualize encryption processes through diagrams, showing how data is transformed into ciphertext.	

Action/Expression:

Have students practice creating encrypted messages using different strategies. Set up lab exercises where students encrypt and decrypt messages using tools like OpenSSL or GPG, reinforcing their understanding of the different encryption methods.

2. I CAN utilize public encryption while keeping information secret and private on the internet.

Engagement:

Begin by discussing how public encryption (e.g., RSA) is used to protect information on the internet, such as in secure email or website communication (HTTPS). Pose a question about how we can ensure our data stays private while communicating over untrusted networks.

Representation:

Provide a clear explanation of public-key cryptography and demonstrate how public and private keys work together to protect data. Use diagrams to show the encryption and decryption process, focusing on how private information remains confidential.

Action/Expression:

Have students generate public and private keys using encryption tools like OpenSSL, and then use them to send encrypted messages. Ask them to demonstrate how public-key encryption ensures privacy by encrypting messages with the recipient's public key and decrypting with their private key.

3. I CAN apply three strategies for data storage encryption.

Engagement:

Introduce the topic by explaining the importance of encrypting data at rest, such as protecting stored files on a hard drive or cloud storage. Discuss scenarios where data loss or theft can have serious consequences (e.g., financial data, medical records).

Representation:

Provide an overview of three common encryption strategies for data storage: full disk encryption (e.g., BitLocker), file-level encryption (e.g., EFS), and cloud storage encryption. Use diagrams or videos to show how each method protects data.

Action/Expression:

Have students implement each encryption method in a lab environment, such as enabling BitLocker on a Windows system or using VeraCrypt for file-level encryption. Have them compare the benefits and challenges of each method and write a report on their findings.

4. I CAN crack and extract hidden data.

Engagement:

Begin by discussing the concept of hidden or encrypted data, such as steganography or password-protected files. Pose a question about how attackers might extract data from seemingly secure environments.

Representation:

Explain common techniques used for hiding and cracking data, such as password cracking, steganography, and file decryption. Provide examples of tools like John the Ripper or Steghide that can help with cracking and extracting hidden data.

Action/Expression:

Have students practice cracking passwords or extracting hidden data using tools like John the Ripper for password cracking and Steghide for steganography. Assign a lab where students demonstrate how to uncover hidden data in a file or image and document the steps involved.

5. I CAN play the role of a digital forensics investigator, weighing the importance of evidence, considering the legality of gathering evidence, and documenting their work.

Engagement:

Start by discussing the role of digital forensics in criminal investigations and the importance of maintaining the integrity of evidence. Present real-world cases where digital evidence was key in solving crimes.

Representation:

Explain the principles of digital forensics, such as chain of custody, legal considerations (e.g., warrants), and documentation practices. Use case studies to illustrate the steps involved in collecting, preserving, and analyzing digital evidence.

Action/Expression:

Have students participate in a simulated digital forensics investigation, where they must identify, preserve, and document evidence from a compromised system. Students should follow proper legal procedures and document their findings as a professional forensics investigator would.

6. I CAN use hashing techniques to validate and authenticate data.

Engagement:

Introduce hashing by discussing its role in data integrity and authentication, such as how websites use hashing to store passwords securely. Present a scenario where data integrity is critical, such as verifying downloaded files or securing communications.

Representation:

Explain hashing algorithms (e.g., MD5, SHA-256) and their uses in validating data integrity and authenticating information. Provide examples of how hash values are used to ensure data has not been tampered with.

Action/Expression:

Have students use hashing tools like sha256sum or hashdeep to generate hashes for files and verify their integrity. Set up a lab where students compare the hash values of original and modified files to see how hashing can detect tampering.

7. I CAN image files and devices.

Engagement:

Begin with a discussion on the importance of creating an image of a device or storage medium, such as preserving a copy of data for forensics or backup purposes. Pose a question on why we might need to create an exact replica of a device or file system.

Representation:

Demonstrate the process of imaging a device or file system using tools like dd, FTK Imager, or Clonezilla. Use diagrams to show how imaging works, emphasizing how it ensures that no data is altered during the process.

Action/Expression:

Have students create a disk image of a virtual machine or a physical device using imaging software. Ask them to analyze the image to verify that it is an exact replica of the original device, documenting their process and any potential issues encountered.

8. I CAN establish identity in cyberspace.

Engagement:

Discuss the challenges and importance of establishing secure identities online, such as in online banking or social media. Present examples of identity theft and how attackers impersonate legitimate users.

Representation:

Explain methods of establishing identity in cyberspace, such as two-factor authentication (2FA), digital signatures, and biometrics. Use visual examples of each method, showing how they protect online identities.

Action/Expression:

Have students set up two-factor authentication for their accounts and generate digital signatures using encryption tools like PGP or GPG. Ask them to describe how these methods help establish and verify identities securely.

9. I CAN utilize forensic tools to create and analyze forensic images.

Engagement:

Start by discussing the role of forensic tools in digital investigations and how they help preserve and analyze evidence. Provide examples of famous forensic investigations that relied on forensic images.

Representation:

Introduce common forensic tools like FTK Imager, EnCase, or Autopsy, and explain how they can be used to create and analyze forensic images. Demonstrate the tools through a walkthrough video or guide.

Action/Expression:

Have students use forensic tools to create a forensic image of a device or storage medium. Then, have them analyze the image for potential evidence, identifying key artifacts such as deleted files or system logs. Students should document their analysis and discuss their findings in a written report.

Supporting Multilingual/English Learners

Related *CELP standards:*	**Learning Targets:**

Learning Target 1: I CAN create encrypted messages using various strategies

- **Level 1:** Can recognize basic encryption concepts and understand the purpose of encryption. Needs guidance to create simple encrypted messages.
- **Level 2:** Can apply basic encryption techniques (e.g., Caesar cipher, substitution cipher) to encrypt simple messages. Can explain the importance of encryption in protecting data.
- **Level 3:** Can use standard encryption methods (e.g., symmetric encryption) to encrypt messages securely. Can explain how different encryption techniques protect data from unauthorized access.
- **Level 4:** Can apply advanced encryption strategies (e.g., asymmetric encryption, public/private key pairs) to

encrypt messages securely. Can explain the strengths and weaknesses of different encryption algorithms.

- **Level 5:** Can create and implement complex encryption protocols and algorithms to secure messages in real-world scenarios. Can troubleshoot and analyze encryption issues in digital communication systems.

Learning Target 2: I CAN utilize public encryption while keeping information secret and private on the internet

- **Level 1:** Can recognize the concept of public encryption but may need help understanding its practical use in securing online communication.
- **Level 2:** Can describe how public encryption works and why it is important for securing data on the internet. Can apply basic public key encryption methods (e.g., RSA) for sending secret messages.
- **Level 3:** Can use public key encryption to secure information exchanged online, ensuring privacy and confidentiality. Can explain how the public/private key pair works in securing internet communications.
- **Level 4:** Can implement and manage secure online communication channels using advanced public encryption techniques (e.g., TLS/SSL). Can troubleshoot issues with encrypted communications and apply appropriate fixes.
- **Level 5:** Can design and implement secure online communication strategies using state-of-the-art encryption protocols. Can conduct security audits and risk assessments to ensure that encryption practices are effective in protecting privacy and data integrity.

Learning Target 3: I CAN apply three strategies for data storage encryption

- **Level 1:** Can identify the need for data storage encryption but may require help understanding different strategies.
- **Level 2:** Can describe basic encryption strategies for protecting data at rest, such as file-level encryption or folder encryption.
- **Level 3:** Can apply at least three different strategies for data storage encryption, such as full disk encryption, file-based encryption, and database encryption.
- **Level 4:** Can evaluate the strengths and weaknesses of different data storage encryption strategies and select the most appropriate strategy for a given use case.
- **Level 5:** Can design and implement robust encryption solutions for securing data across multiple storage platforms. Can integrate encryption with other security measures to create a comprehensive data protection system.

Learning Target 4: I CAN crack and extract hidden data

- **Level 1:** Can recognize that hidden data exists but may need assistance identifying methods for cracking or extracting it.
- **Level 2:** Can describe basic techniques for cracking encrypted data or extracting hidden information from files (e.g., steganography).
- **Level 3:** Can apply basic methods for cracking passwords or extracting hidden data from encrypted files using tools like hash crackers or steganography software.
- **Level 4:** Can employ advanced data recovery and decryption techniques to extract hidden information from encrypted or obfuscated data. Can explain the ethical considerations in cracking or recovering data.
- **Level 5:** Can conduct thorough forensic investigations to uncover hidden data in complex encrypted systems. Can design and implement methods to recover and extract data from a variety of digital storage formats.

Learning Target 5: I CAN play the role of a digital forensics investigator, weighing the importance of evidence, considering the legality of gathering evidence, and documenting their work

- **Level 1:** Can recognize the role of a digital forensics investigator but may need guidance in applying the legal and ethical aspects of the profession.
- **Level 2:** Can describe the role of a digital forensics investigator and the importance of evidence in an investigation. Can understand basic legal and ethical guidelines for gathering evidence.
- **Level 3:** Can perform basic digital forensics tasks, such as collecting and preserving evidence, while considering the legality and ethical implications. Can document findings clearly and systematically.
- **Level 4:** Can conduct full forensic investigations, evaluating evidence for its importance and legal admissibility. Can ensure that evidence is collected and documented according to legal standards.
- **Level 5:** Can lead complex forensic investigations, applying advanced techniques for data recovery and evidence analysis. Can ensure the integrity of evidence and provide expert testimony or reports that meet legal and ethical standards.

Learning Target 6: I CAN use hashing techniques to validate and authenticate data

- **Level 1:** Can recognize what a hash function is but may need help understanding its role in validating and authenticating data.

- **Level 2:** Can describe basic hashing techniques (e.g., MD5, SHA) and how they are used for data integrity checking.
- **Level 3:** Can use hashing techniques to validate data by comparing hashes, ensuring that data has not been altered. Can authenticate data by generating and comparing hash values.
- **Level 4:** Can apply advanced hashing techniques to secure data, ensuring that the data has not been tampered with during transmission or storage. Can use hash functions as part of an authentication system.
- **Level 5:** Can design and implement secure data validation and authentication systems using complex cryptographic hashing algorithms. Can integrate hashing with digital signatures and other security measures to protect data integrity.

Learning Target 7: I CAN image files and devices

- **Level 1:** Can recognize that imaging involves copying data but may need assistance with the process of creating and working with disk images.
- **Level 2:** Can describe the purpose of creating disk images and understand the concept of data duplication. Can create basic disk images of simple files or devices using imaging software.
- **Level 3:** Can create and manage disk images for forensic investigations, ensuring the integrity of the original data. Can use imaging tools to create and work with images of files or devices.
- **Level 4:** Can create disk images of complex systems (e.g., entire hard drives) and use specialized imaging software. Can ensure the image is an exact replica and document the imaging process for legal compliance.
- **Level 5:** Can create and analyze advanced disk images from various devices and file systems. Can troubleshoot and manage complex disk imaging tasks, ensuring data recovery, integrity, and compliance with legal standards.

Learning Target 8: I CAN establish identity in cyberspace

- **Level 1:** Can recognize the concept of identity in cyberspace but may need assistance understanding the various ways to establish and protect it.
- **Level 2:** Can describe methods for establishing identity online, such as using usernames and passwords. Can identify basic strategies for protecting online identity.
- **Level 3:** Can establish and verify identity in cyberspace using secure methods, such as multi-factor authentication (MFA) or biometric authentication.
- **Level 4:** Can implement and manage advanced identity protection strategies, such as digital certificates or identity management systems, to ensure secure online presence.
- **Level 5:** Can design and manage identity systems in cyberspace, ensuring secure, authenticated access to digital services. Can evaluate identity management systems for vulnerabilities and improve security protocols.

Learning Target 9: I CAN utilize forensic tools to create and analyze forensic images

- **Level 1:** Can recognize forensic tools but may need assistance understanding their role in creating and analyzing forensic images.
- **Level 2:** Can describe the basic purpose of forensic tools and understand how they can be used to create forensic images.
- **Level 3:** Can use basic forensic tools (e.g., FTK Imager, EnCase) to create and analyze forensic images of files and devices. Can ensure the image is a faithful copy of the original data.
- **Level 4:** Can use advanced forensic tools to create, analyze, and document forensic images, ensuring data integrity and legal admissibility. Can analyze images for hidden or deleted data.
- **Level 5:** Can design and execute complex forensic imaging tasks, using a wide range of forensic tools to handle sophisticated cases. Can ensure forensic imaging is performed according to legal and professional standards, documenting the entire process for evidence presentation.

Lesson Sequence	Learning Target	Success Criteria/Assessment/Resources
1	I CAN create encrypted messages using various strategies	• I can explore the history of cryptography • I can identify types of encryption
2	I CAN utilize public encryption while keeping information secret and private on the internet	• I can understand how data can be shared publicly and remain confidential. • I can validate who owns specific information. • I can exchange a message with paired key encryption

3	I CAN apply three strategies for data storage encryption	● I can explore uses of cryptography. ● I can identify different levels of cryptography in cybersecurity ● I can test the security of various cryptography methods (such as password cracking).
4	I CAN crack and extract hidden data	● I can explore the history of steganography. ● I can exercise the use and detection of steganography.
5	I CAN play the role of a digital forensics investigator, weighing the importance of evidence, considering the legality of gathering evidence, and documenting their work.	● I can understand the value of digital evidence. ● I can understand authority to search ● I can recognize different storage containers of digital evidence. ● I can practice proper collection techniques of digital evidence. ● I can use a chain of custody.
6	I CAN use hashing techniques to validate and authenticate data	● I can understand data authentication and validation ● I can practice hashing techniques ● I can validate and authenticate data using hashing
7	I CAN image files and devices.	● Understand the properties of a forensic image. ● Explore applicable scientific standards of forensic images. ● Practice creating a forensic image.
8	I CAN establish identity in cyberspace	● Understand identifying artifacts in digital forensics ● Explore methods to identify someone on the internet. ● Practice tracing email sources
9	I CAN utilize forensic tools to create and analyze forensic images.	● Understand the capabilities of a forensic tool suite ● Process a forensic image with a forensic tool suite ● Explore a forensic tool suite