Central Bucks School District
Math Department

AP Cybersecurity

Course Number:	2009
Course Level:	Advanced/College Bound
Grade:	9-12
Time/Credit:	83 minutes daily: Grades 9, 10, 11, and 12
	1 credit: 9^{th} – 12^{th} grade

Board Approval Date:

Central Bucks School District
20 Welden Drive
Doylestown, PA 18901

Table of Contents

Central Bucks School District
K-12 Computer Science Teaching and Learning Principles

1. Investigating, problem-solving, and communicating about computer science (speaking, reading, writing, representing, and listening) stimulates students' curiosity, builds confidence, and leads students toward deeper conceptual understanding.

2. Lessons should address students' strengths, interests, and learning styles through differentiated instruction.

3. All students can achieve excellence in computer science when:
    - instruction is appropriately paced
    - teachers set high expectations
    - students feel supported by their teachers, parents and administrators

4. Students must be actively engaged in learning experiences designed to connect to their prior knowledge.

5. For students to transfer and use knowledge meaningfully teachers need to:
    - present new ideas within rich and meaningful contexts
    - help students to make connections to their lives both within and outside of school

6. Computer Science instruction is more effective when teachers incorporate:
    - manipulatives
    - integrated development environments, both online and device based

7. Assessment should be ongoing, diagnostic, and aligned with instruction.

Documents Considered:

College Board (2019). AP Computer Science A: Course and Exam Description. Retrieved from https://apcentral.collegeboard.org/courses.

Computer Science Teachers Association (2017). CSTA K-12 Computer Science Standards, Revised 2017. Retrieved from http://www.csteachers.org/standards.

Kilpatrick, J., Swafford, J., & Findell, B. (2001). *Adding It Up: Helping Children Learn Mathematics.* Washington, DC: National Academy Press.

Marzano, R., & Pickering, D. (1997). *Dimensions of Learning.* Alexandria, VA: Association for Supervision and Curriculum Development; Aurora, CO: Mid-continent Regional Educational Laboratory.

Tomlinson, Carol Ann. (1999). *The Differentiated Classroom: Responding to the Needs of All Learners.* Alexandria, VA: Association for Supervision and Curriculum Development.

Zemelman, S., Daniels, H., & Hyde, A. (1998). *Best practice: New Standards for Teaching and Learning in America's Schools*. Portsmouth, NH: Heinemann.

Central Bucks School District
K-12 Computer Science Program Enduring Understandings

Students will understand that:

Computing Systems

- Abstractions hide the underlying implementation details of computing systems embedded in everyday objects.
- Levels of abstraction and interactions between application software, system software, and hardware layers can be compared.
- Guidelines that convey systematic troubleshooting strategies can be developed that others can use to identify and fix errors.

Networks and the Internet

- There is scalability and reliability of networks, in which the relationship between routers, switches, servers, topology, and addressing can be described.
- Sensitive data can be affected by malware and other attacks.
- Security measures can address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

Data and Analysis

- There are different bit representations of real-world phenomena, such as characters, numbers, and images.
- There are tradeoffs in how data elements are organized and where data is stored.

Algorithms and Programming

- Algorithms are used to solve computational problems by leveraging prior student knowledge and personal interests.
- Programmers must justify the selection of specific control structures when tradeoffs involve implementation, readability, and program performance, and explain the benefits and drawbacks of choices made.
- Problems can be decomposed into smaller components through systematic analysis, using constructs such as procedures, modules, and/or objects.
- Documentation of design decisions using text, graphics, presentations, and/or demonstrations is an integral part in the development of complex programs.

Impacts of Computing

- Computing affects personal, ethical, social, economic, and cultural practices.
- Computational artifacts must be tested and refined to reduce bias and equity deficits.

Central Bucks School District
K-12 Computer Science Program Essential Questions

Computing Systems

- What is an abstraction?
- How does abstraction manage complexity?

Networks and the Internet

- How do scalability and redundancy relate to reliability on the Internet?
- What is malware and how is sensitive data affected by it?
- How do efficiency, feasibility, and ethical impacts impact security measures?

Data and Analysis

- What are the tradeoffs in how data elements are organized and where data is stored?
- How do we collect, visualize, and store large amounts of data?
- Why do we create computational models and how does the data we use affect those models?
- What is the purpose of creating prototypes to solve computational problems?

Algorithms and Programming

- What is an algorithm?
- How do algorithms and programs differ?
- Why is the selection of specific control structures important when considering implementation, readability, and program performance?
- Why is the decomposition into smaller components in constructs such as procedures, modules, and/or objects important in the software development process?
- Why are documentation and design decisions an integral part in the development of complex programs?

Impacts of Computing

- What is the purpose of collecting data?
- How is data used or abused?
- What are the ways that computing affects personal, ethical, social, economic, and cultural practices?
- Why must we test and refine computational artifacts to reduce bias and equity deficits?

Central Bucks School District – Course of Study Overview

AP Cybersecurity Overview

Desired Results.

Course Description:

2009 AP Cybersecurity (18 weeks, 1 credit)
AP Cybersecurity introduces students to the principles, practices, and tools used to secure digital systems. Through a combination of hands-on labs, real-world scenarios, and project-based learning, students explore foundational topics such as network security, cryptography, risk assessment, system vulnerabilities, and ethical hacking. The course emphasizes both the technical and human aspects of cybersecurity and prepares students for further study or careers in the field. Up to one credit from computer science courses may be used to fulfill graduation requirements for mathematics.

Committee Members (Original)**:** Dustin Frey, Aaron Fromal, Anthony Paglione, Matt Quinn, Brian Novick: K – 12 Mathematics Supervisor

Acceptable Evidence.

Course Grading: The final course grade is calculated as follows:

- Each marking period grade counts for 45% of the students' course grade.
- The final exam counts for 10% of the students' course grade.

AP Cybersecurity Pacing Guide	
Unit 1: Introduction to Security	**15**
1.1 – Understanding Social Engineering 1.2 - Suspicious Wi-Fi Login 1.3 - The Dangers of Public Wi-Fi 1.4 - AI Based Cybersecurity Attacks 1.5 - Leveraging AI in Cyber Defense Formative Assessment	13
Remediation and Enrichment	1
Unit 1 Summative Assessment	1
Unit 2: Securing Spaces	**12**
2.1 – Cyber Foundations 2.2 - Physical Vulnerabilities and Attacks 2.3 - Protecting Physical Spaces 2.4 - Detecting Physical Attacks Formative Assessment	10
Remediation and Enrichment	1
Unit 2 Summative Assessment	1
Unit 3: Securing Networks	**15**
3.1 – Network Vulnerabilities and Attacks 3.2 - Protecting Networks: Managerial Controls and Wireless Security 3.3 - Protecting Networks: Segmentation 3.4 - Protecting Networks: Firewalls 3.5 - Detecting Network Attacks Formative Assessment	13
Remediation and Enrichment	1
Unit 3 Summative Assessment	1
Unit 4: Securing Devices	**12**
4.1 – Device Vulnerabilities and Attacks 4.2 - Authentication 4.3 - Protecting Devices 4.4 - Detecting Attacks on Devices Formative Assessment	10
Remediation and Enrichment	1
Unit 4 Summative Assessment	1
Unit 5: Securing Applications and Data	**18**
5.1 - Application and Data Vulnerabilities and Attacks 5.2 - Protecting Applications and Data: Managerial Controls and Access Controls 5.3 - Protecting Stored Data with Cryptography 5.4 - Asymmetric Cryptography 5.5 - Protecting Applications 5.6 - Detecting Attacks on Data and Applications Formative Assessment	16
Remediation and Enrichment	1

Unit 5 Summative Assessment	1
Projects, Review, and Final Exam	**8 - 12**
Projects	5-8
Review	2-3
Final Exam	1
Total Days for Course:	**80 - 84**

Required and Supplementary Technology and Texts

Required Technology

- Student Laptops
- College Board:
  - AP Classroom Progress Checks
  - AP Cybersecurity Labs
  - Released Multiple-Choice and Free Response Questions
- Suggested Online Resources
  - Cyber.org
  - web.mit.edu/mprat/Public/web/Terminus/Web/main.html

Supplemental Resources

- Code.org
- CodeHS.com
- CyberChef
- BleepingComputer | Cybersecurity, Technology News and Support

Desired Results

Essential Questions:

- What evidence could you use to convince a teacher that an email is not legitimate?
- What elements of an email might cause someone to act impulsively?
- What are some potential consequences for someone who clicked a malicious link in an email?
- What types of information does an authorization log contain?
- What patterns do you notice in an authorization log?
- What entries in an authorization log are suspicious and why?
- How could you avoid joining a malicious network?
- What other types of services or applications could be impacted while logged into a malicious network?
- Do you know all your online connections (on social media and gaming platforms) in real life?
- Do you know that all your online connections are who they claim to be?
- Have you heard of adversaries trying to impersonate someone to get money out of a relative?
- How could you help protect relatives from becoming victims of an impersonation scheme?
- What are some potential advantages and disadvantages of using an AI-powered tool to review application code?
- Why is it important for the software development team to review the changes to the application code before implementing them?
- Are there times when you use AI-powered tools to help you review your work?

Enduring Understandings:

Students will understand that…

- Social engineering attacks employ psychological tactics to manipulate users into revealing sensitive information (elicitation), downloading a malicious file, or clicking on a malicious link. Social engineering can be performed in person but is often done by email, by text message, or through social media messages.
- Adversaries often use psychological tactics like intimidation and urgency to achieve their goals. Intimidation is when an adversary threatens a target with negative consequences if they do not comply. Urgency is when an adversary creates reasons why a target should act quickly.
- Social engineering tactics rely on common psychological principles that influence human behavior.
- Intimidation leverages a natural human aversion to negative consequences. By drawing attention to possible negative consequences, adversaries use fear to incite targets to act.
- Urgency leverages a natural human response to react quickly to time-sensitive needs. When targets detect a sense of urgency in a message, they feel pressured to respond or act quickly, which can prevent them from taking the time to consider whether an action is reasonable or safe.
- Victims may give an adversary personal information that could lead to impersonation, such as name, phone number, address, workplace, pets' names, or birthdate. These types of information are often used on websites as challenge questions to verify a user's identity.

- Victims may give an adversary secure information like a one-time password (OTP) or authentication login code, which could allow an adversary to log in to a service as the victim.
- Victims may download malware or click a link that installs malware on their device, steals information from their web browser, or directs them to a website where their login credentials can be captured by an adversary.
- In an online password attack, adversaries try to log in to a device or service using common passwords, common password patterns, or stolen passwords.
- Signs of an online password attack include:
    - Many failed attempts to log in over a short duration
    - Login attempts at unusual times
    - Login attempts from unknown devices
- Many people use common patterns when creating passwords, such as:
    - Starting a password with one or two words, adding a two-digit number (often signifying a year), and putting a special character at the end
    - Including the names of family or pets in their passwords
    - Including personally significant dates in their passwords
- Adversaries often construct a dictionary of possible passwords based on personal information gathered about a target, such as birthday, anniversary, names of pets, and names of family members, and use an automated tool to submit potential passwords.
- Users should increase password complexity by using lowercase and uppercase letters, numbers, and special characters, and spreading the special characters and numbers throughout the password.
- When available, users should enable multifactor authentication (MFA), which will require the user to provide extra proof of identity—such as a one-time code—in addition to the password as an extra layer of security.
- Adversaries can be classified by their skill levels.
- Adversaries have a variety of motivations, including greed, desire for recognition, dedication to a cause, revenge, politics, or beliefs.
- In an evil twin attack, an adversary sets up their own wireless access point (WAP) with a service set identifier (SSID) similar or identical to a target network; the adversary's network is called the evil twin. Victims of this attack could select to unknowingly connect to the evil twin, allowing the adversary to capture their network traffic.
- In a jamming attack, an adversary floods an area with a strong electromagnetic (EM) signal in the same frequency range as the wireless network, which prevents legitimate traffic between the access point (AP) and users. This type of attack that prevents users from accessing resources is called a denial of service (DoS) attack.
- In a war driving attack, adversaries try to detect wireless network beacons while driving or walking around a target. If a wireless signal is detected, the adversary can gather information about the type of wireless network used and find areas where the wireless signal extends outside the physical building.
- Individuals should verify that the name of any wireless network they join exactly matches the name of the network they intend to join.
- Individuals should avoid joining unprotected wireless networks. Unprotected wireless networks do not require a password or authentication to join.
- Individuals may consider using a virtual private network (VPN), which encrypts all their traffic, so that any intercepted traffic would not be immediately readable.

- Adversaries can use AI-powered tools that leverage existing voice and image samples of a person to create a digital avatar of that person. The use of these technologies enables adversaries to impersonate someone over the phone or even on a video call, which can lead to financial loss or the sharing of sensitive or private information. As more organizations adopt voice-based authentication, the impact of voice-impersonation has a larger potential impact.
- Adversaries can use generative AI tools, like large language models (LLMs), to create convincing phishing messages in any target language. Because traditional phishing messages are sometimes written by non-native speakers of the target's language, unnatural language is a feature that has been used to distinguish phishing messages from legitimate messages. However, with AI tools, adversaries can now craft phishing messages in any language that read as though they were written by a native speaker.
- Adversaries can craft prompts that extract secure or sensitive information from LLMs. Secure or sensitive information in LLMs can come from user input and the large data sets used to train LLMs.
- Adversaries can publish websites or modify existing websites to contain false information so that the false information will be included in the training sets for LLMs, causing the LLMs to repeat the false information.
- Adversaries can perform reconnaissance on a target using AI-powered tools that scan the internet to gather information posted on social media and public websites.
- Adversaries can use AI-enhanced coding tools to help them write new malware, modify existing application code to perform malicious activities, or to find vulnerabilities in large code bases.
- Shared secrets with close friends and relatives that can be used to verify each other's identities should be established. A secret word or phrase known only to two parties can be used to authenticate identities in high stakes situations.
- Multifactor authentication (MFA) should be enabled. If an adversary clones a target's voice to access a system with voice authentication, requiring a second authentication factor could prevent an adversary from gaining access to accounts.
- Personal or sensitive data should not be entered into any AI-powered tools, such as chatbots or virtual assistants. Some AI-powered tools feed user input back into the model to provide continuous training. Adversaries could extract data that users have included in prompts.
- Output from AI-powered tools should be carefully evaluated. Information from AI-powered tools should be verified using reputable, stable, non-AI-based sources.
- AI tools can review current security configurations, like firewall rules and access controls, and recommend more secure options. Recommendations should always be checked by a knowledgeable security technician before being implemented.
- AI-powered tools can analyze application code to identify vulnerabilities and recommend mitigations. Recommendations should always be reviewed by a knowledgeable programmer before being implemented.
- AI-powered tools can suggest rules for automated detection systems. Detection rules should always be reviewed by a knowledgeable detection engineer before being added to a system.
- Of the millions of digital events that happen on networks daily, some likely represent an adversary conducting malicious activity. Humans cannot carefully examine all those events to identify the malicious activity.
- AI-powered tools can be trained to quickly analyze digital events and sort the events that are likely malicious activity from those that are harmless.

- AI-powered tools can be programmed to alert human cybersecurity personnel when likely malicious activity is detected or to take specific corrective actions based on the type of malicious activity detected.
- AI-powered tools enable threat-detection and response teams to catch malicious activity and intervene quickly to prevent loss, harm, damage, and destruction to digital infrastructure and data.

Knowledge:
Students will know…

- Definitions: Social engineering, elicitation, intimidation, urgency, impersonation, one-time password (OTP), authentication login code, multifactor authentication (MFA), shared secrets, malware, phishing, online password attack, denial of service (DoS) attack, evil twin attack, jamming attack, war driving, reconnaissance, password complexity, password patterns, dictionary attack, wireless access point (WAP), service set identifier (SSID), virtual private network (VPN), unprotected wireless network, voice impersonation, generative AI, large language models (LLMs), AI-powered tools, AI-enhanced coding tools.

Skills:
Students will be able to…

- Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.
- Identify security controls and explain how they mitigate risks.
- Identify methods for monitoring systems and explain how they detect attacks.

Computer Science Standards:

CSTA K-12 Computer Science Standards

- 2-NI-05 Explain how physical and digital security measures protect electronic information. (P7.2) 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
- 2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
- 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
- 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.
- 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
- 2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
- 3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
- 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

AP Cybersecurity Computational Thinking Practices

1.1.A Identify common indicators of social engineering tactics.
1.1.B Explain how social engineering tactics influence victims to perform a desired action
1.1.C Describe possible impacts for victims of social engineering attacks.

1.2.A Identify common signs of a password attack.
1.2.B Explain how adversaries take advantage of weak authentication.
1.2.C Explain how to make authentication stronger
1.3.A Identify the type of adversary conducting a cyberattack
1.3.B Identify types of wireless cyberattacks.
1.3.C Explain how individuals can protect themselves from some cyberattacks.
1.4.A Explain how adversaries use AI-powered tools to augment cyberattacks.
1.4.B Explain how to protect against some AI-augmented cyberattacks.
1.5.A Explain how cyber defenders can leverage AI-powered tools to protect networks, applications, and data.
1.5.B Explain how AI-powered tools are enabling faster and more accurate threat detection and response.

Acceptable Evidence.

Acceptable evidence of learning other than Performance Tasks:

Formative Assessment

- Warm-ups
- Check point assignments
- Class work
- Homework
- Exit slips
- Keep a notebook
- Current Event Reports
- Quizzes
- Canvas Quizzes
- Programming Assignments
- Unit Quiz

Summative Assessment

- Unit Test

Suggested learning experiences and instruction

Learning Experiences:

- AP Classroom: Progress Check for Unit 1.
- AP Classroom Scenario: Detecting Phishing Messages.
- AP Classroom Scenario: Detecting Unauthorized Logins.
- AP Classroom Scenario: Impacts of Using Public Wi-Fi.
- AP Classroom Scenario: AI-Powered Cyberattacks.
- AP Classroom Scenario: AI-Powered Cyber Defense.

Instructional Strategies:

- Use a presentation to demonstrate new material.
- Use PowerPoint slides to present concepts and terminology.
- Complete teacher-generated self-review questions, multiple-choice, true/false, and short answer problems.

Differentiation:

- Work with students in flexible small groups to provide targeted intervention, reteaching, enrichment, or extension related to cybersecurity concepts and practices.
- Provide additional scaffolds such as guided notes, network diagrams, templates, structured lab procedures, and step by step protocols for students who need support.
- Provide opportunities for students ready for additional challenge to apply advanced concepts, evaluate emerging threats, and design secure solutions to authentic cybersecurity problems.

For Language Development:

- Create and maintain a student generated cybersecurity glossary that includes terminology, definitions, examples, and real world applications.
- Provide opportunities for students to explain cybersecurity concepts, threats, and mitigation strategies using appropriate technical vocabulary in both written and verbal formats.
- Use graphic organizers, diagrams, and visual models to connect terminology with concepts such as network security, encryption, authentication, risk management, and incident response.
- Develop study guides with clear definitions, case studies, and opportunities to practice cybersecurity communication and analysis.

For Enrichment:

- Meet in small groups with students who are ready for enrichment to provide instruction on advanced cybersecurity topics followed by challenging extension activities.
- Allow students to engage in more rigorous investigations, simulations, and problem-solving tasks that require deeper analysis of cybersecurity threats and defenses.
- Provide opportunities for students to explore specialized areas such as ethical hacking, digital forensics, cloud security, artificial intelligence security, cryptography, or security operations.
- Encourage students to complete enrichment projects involving security assessments, threat analysis, cyber defense strategies, policy development, or research on emerging cybersecurity issues that extend the core content while maintaining alignment with course objectives.

Central Bucks School District – Course of Study

Unit 2: Securing Spaces

Desired Results

Essential Questions:

- How do social engineers exploit psychological principles to manipulate individuals into compromising security?
- What motivates different types of adversaries, and how do their skill levels and goals influence the nature of their attacks?
- What are the phases of a cyberattack, and how do adversaries progress from reconnaissance to evasion?
- How do risk, vulnerabilities, and threats interact to compromise assets, and how can organizations assess and manage these risks?
- What are the principles of confidentiality, integrity, and availability, and how do security controls uphold these principles?
- How do physical security threats like tailgating, shoulder surfing, dumpster diving, and card cloning compromise cybersecurity?
- How do organizations use access control mechanisms and device restrictions to prevent unauthorized access and malware infections?
- How do natural disasters pose cybersecurity risks, and what strategies can mitigate their impact on digital infrastructure and data?
- How do organizations prioritize risk mitigation?

Enduring Understandings:

Students will understand that…

- Social engineers use psychological tactics to manipulate targets into taking a desired action.
- Pretexting is when adversaries create a believable reason to contact a target.
- Authority is when adversaries impersonate someone with power over a target or pretend to relay instructions from that person.
- Intimidation is when adversaries state negative consequences if demands are not met.
- Consensus is when adversaries create social pressure by making a target believe everyone else is doing a desired action.
- Scarcity is when adversaries create a sense of limited availability.
- Familiarity is when adversaries pretend to be or know someone close to a target to establish trust.
- Urgency is when adversaries create a deadline that requires quick action by a target to avert negative consequences.
- Script kiddies are low-skilled adversaries who use tools developed by others without understanding how the tools work. They are often motivated by greed or a desire for recognition.
- Hacktivists are motivated by social, political, or personal causes. They compromise computers and networks to support their cause or stop perceived harm, believing their goals justify their illegal methods.

- Cyberterrorists are motivated by politics or beliefs and seek to disrupt entire communities, regions, or nations through cyberattacks (e.g., attacking a power grid, water treatment plant, or other civil infrastructure). They can act independently or on behalf of governments or criminal organizations.
- Transnational criminal organizations seek financial gain primarily by deploying ransomware and stealing corporate intellectual property (IP) to sell in illegal markets.
- Cyberattacks aim to disrupt, harm, steal, or destroy devices, networks, or data. Adversaries work in phases, which may not all be used in every attack.
- In the reconnaissance phase of an attack, adversaries gather as much information as possible about their target, often using open source intelligence (OSINT), which is freely available information.
- In the initial-access phase of an attack, adversaries establish a foothold on the target's computer, often through social engineering or compromised or weak credentials.
- After gaining access during an attack, adversaries establish persistence to maintain access without needing to regain it. They may use a command and control (C2) protocol to send commands to the device and receive output, often through malware like a remote access trojan (RAT) or rootkit.
- In the lateral-movement phase of an attack, adversaries try to escalate their privileges by accessing computers and user accounts with elevated permissions to services and data.
- In the taking-action phase of an attack, adversaries act on their objectives by collecting targeted data, exfiltrating it, and disrupting services or destroying data.
- In the final phase of an attack, many adversaries try to evade detection by removing or editing log files and erasing other files they may have planted on devices (e.g., malware).
- Risk occurs when a threat can exploit a vulnerability to compromise an asset.
- An asset is anything valuable. Assets include financial resources, intellectual property, data, digital infrastructure, physical property, and reputation.
- The severity of an attack is often measured by financial cost, which can also include reputational and operational impacts.
- The result of a risk assessment can be quantitative or qualitative.
- Risk assessment documentation should include:
    - Vulnerable assets and their value
    - Descriptions of likely threats to the assets
    - Details of specific vulnerabilities for specific assets and how they would be exploited
    - An explanation of the severity of damage (financial, operational, reputational, etc.) if a specific asset were compromised, and the likelihood of that compromise occurring
    - A final rating, quantitative or qualitative, for each risk identified
- Once a risk has been identified and assessed, an organization has four options for managing that risk: avoid, transfer, mitigate, or accept.
- Residual risk is the risk that remains after an organization has gone through avoidance, transference, and mitigation. The residual risk is the level of risk that an organization is willing to accept. Risk acceptance acknowledges the fact that absolute security is unattainable.
- To conserve financial resources and employee capacity, an organization will often favor solutions that are cost effective and easy to implement and maintain.
- Security controls address at least one of the following principles:
    - Confidentiality ensures that only authorized individuals, systems, or processes can access data. Systems lacking confidentiality are vulnerable to data theft or destruction.

    - Integrity ensures that data is accurate and trustworthy. Systems lacking integrity are vulnerable to data manipulation.
    - Availability ensures that data and services are accessible to authorized individuals when needed. Systems lacking availability may experience unexpected downtime.
- Security controls can be classified by type.
    - Physical controls provide security in the physical space and include locks, fences, cameras, bollards, and security guards.
    - Technical controls provide security in the digital space and include firewalls, anti-malware software, and encryption.
    - Managerial controls provide rules, guidelines, policies, and procedures that specify what security should be in place and include password policies, regular access reviews, and incident response plans (IRPs).
- Security controls can be classified by function.
    - Preventive controls address potential vulnerabilities with the goal of stopping an adversary from attacking and include locks and encryption.
    - Detective controls help identify attacks when they occur and include intrusion detection systems (IDSs), cameras, security incidents, and event management (SIEM) systems.
    - Corrective controls fix problems and help restore systems to an operational state. Examples include vulnerability patching, repairing a broken card reader, and intrusion prevention systems (IPSs).
- A defense-in-depth strategy, or layered defense, uses multiple types of security controls to protect sensitive data and systems.
- A defense-in-depth strategy allows an organization to address different types of threats, each with a security control most suited to mitigate it.
- A defense-in-depth strategy allows for resilience in data protection, so when one security control is bypassed by an adversary, another security control may still prevent access to the data or system or limit the damage done to the data or system.
- Layers in a defense-in-depth strategy can include human, physical, network, device, application, and data.
- Adversaries often use social engineering when conducting a physical attack.
- Piggybacking is the name for an attack where an adversary uses social engineering to manipulate an authorized individual to grant the adversary access to a restricted area. Common piggybacking tactics include carrying something large to entice an authorized person to hold the door open, pretending to be an authorized person who has forgotten their access token, or pretending to be a maintenance person who needs to get into a certain area to perform an inspection or repair.
- Tailgating is the name for an attack where an adversary gains unauthorized access to a restricted area by following close behind an authorized individual without that individual's awareness or knowledge.
- Shoulder surfing is the name for an attack where an adversary watches as a user accesses sensitive information, so the adversary can use it later. Sometimes adversaries use a camera to record the target by accessing sensitive information for later analysis.
- Dumpster diving is the name for an attack where an adversary goes through a target's physical trash to look for information that could be used to help the adversary reach their goal.
- Card cloning is the name for an attack where an adversary makes a copy of an authorized user's access card so they can gain access to all the resources the user is authorized to access.

- Threats include human adversaries seeking to cause harm or disruption as well as natural disasters. Natural disasters can cause physical damage or destruction to computers and data as well as disruption of digital services provided by computers.
- Vulnerabilities are weaknesses or flaws that could allow an asset to be compromised.
- When adversaries gain access to an area with sensitive information, they can steal or copy sensitive information.
- When adversaries gain physical access to a device and its ports, they can plug in a keylogger or external drive containing malware, which could allow them to collect data from a user or possibly even to gain control of the device. With direct physical access, adversaries can also physically destroy a device, making the device itself, any data stored on it, and any services it provides unavailable.
- Physical access to devices can allow adversaries to bypass many technical controls and layers of security.
- Organizations should conduct employee security awareness training to educate employees about how they can contribute to the organization's security.
- Organizations should have a workstation security policy that outlines the measures necessary to protect a physical workplace. The policy may have tiers of workstation security based on the type of data handled at a workstation.
- To determine a relevant control, a cyber defender considers how an adversary could take advantage of a vulnerability to attack a system and how to prevent, detect, or correct the attack.
- Card readers can record which employee badges are being used to access different entries at specific times and deny access to unauthorized badges.
- Access control vestibules and turnstiles can prevent an authorized person from intentionally or accidentally admitting an unauthorized person into a restricted area.
- Organizations can disable USB ports to prevent external drives from loading malware onto a computer.
- An uninterruptible power supply (UPS) provides a backup power source for a device in the event of a power outage. Organizations can also use power generators to provide power at a larger scale to a building or set of critical devices.
- Organizations prioritize risk mitigations based on the severity of the risks and the cost of the recommended mitigations.
- Locks should be placed on all entries to areas containing sensitive information or systems. For areas with particularly sensitive information or systems, an organization could use an access control vestibule at the entry point to prevent piggybacking or tailgating.
- Security guards can be stationary or patrolling. Stationary guards can provide constant protection for a specific area, entrance, or high-value item. Patrolling guards are more difficult for an adversary to plan around and can create time pressure for an adversary. Placing stationary guards at places that funnel traffic (e.g., entry gates, main entrances or lobbies, and entrances to more secure access areas) can be highly effective, while patrolling guards are better suited for perimeters and exterior areas.
- Cameras provide visual monitoring and a visual record of activity within a designated space. Cameras can be paired with facial recognition software that can provide alerts when unauthorized individuals enter controlled areas. Once a physical breach has been detected, defenders can use live and recorded camera footage to track an adversary's path and actions.
- Motion detectors work best when paired with cameras. When a security alert is raised because a motion detector has been activated, defenders can use cameras to check the space visually and verify a physical security breach.

- When employees are required to use an electronic badge to unlock a door to a restricted area, a sensor can record how long the door was open. In reviewing entry logs for the door, potential piggybacking or tailgating can be detected by doors being open for longer than normal lengths of time.

Knowledge:

Students will know…

- Definitions: Social engineering, pretexting, authority, intimidation, consensus, scarcity, familiarity, urgency, script kiddies, hacktivists, insider adversaries, cyberterrorists, transnational criminal organizations, cyberattacks, reconnaissance, open source intelligence (OSINT), initial access, persistence, command and control (C2), remote access trojan (RAT), rootkit, lateral movement, taking action, data exfiltration, evasion, risk, threat, vulnerability, asset, risk assessment, quantitative assessment, qualitative assessment, risk avoidance, risk transference, risk mitigation, residual risk, risk acceptance, confidentiality, integrity, availability, security controls, physical controls, technical controls, tailgating, shoulder surfing, dumpster diving, card cloning, natural disasters, access control vestibules, turnstiles, USB port disabling, piggybacking, tailgating.

Skills:

Students will be able to…

- Identify vulnerabilities, threats, and attack methods, and explain how they generate risk.
- Identify security controls and explain how they mitigate risks.
- Evaluate the likelihood and impact of risks.
- Document the likelihood and impact of risks.
- Identify security controls and explain how they mitigate risks.
- Determine layered security controls that address vulnerabilities.
- Identify methods for monitoring systems and explain how they detect attacks.
- Determine strategies and methods to detect attacks.

Computer Science Standards:

CSTA K-12 Computer Science Standards

- 2-NI-05 Explain how physical and digital security measures protect electronic information. (P7.2) 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
- 2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
- 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
- 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.
- 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
- 2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
- 3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
- 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

AP Cybersecurity Computational Thinking Practices

2.1.A Identify social engineering attacks.
2.1.B Identify types of adversaries.
2.1.C Describe the phases of a cyberattack.
2.1.D Describe the risk assessment process.
2.1.E Identify strategies for managing risk.
2.1.F Identify types of security controls.
2.1.G Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.
2.2.A Identify common physical attacks.
2.2.B Explain how threats can exploit common physical vulnerabilities to cause loss, damage, disruption, or destruction to assets.
2.2.C Assess and document risks from physical vulnerabilities.
2.3.A Identify managerial controls related to physical security.
2.3.B Determine mitigation strategies for risks from physical vulnerabilities.
2.4.A Identify ways security controls can detect physical attacks.
2.4.B Determine effective placement of security controls for detecting physical attacks.
2.4.C Apply detection techniques to identify physical attacks.

Acceptable Evidence

Acceptable evidence of learning other than Performance Tasks:
Formative Assessment

- Warm-ups
- Check point assignments
- Class work
- Homework
- Exit slips
- Keep a notebook
- Current Event Reports
- Quizzes
- Canvas Quizzes
- Programming Assignments
- Unit Quiz

Summative Assessment

- Unit Test

Suggested learning experiences and instruction

Learning Experiences:

- AP Classroom: Progress Check for Unit 2.
- AP Classroom Scenario: Securing Xtensr Labs.
- AP Classroom Scenario Discussion: A server that stores customer data is in a room with no lock which is accessed via an unmonitored hallway.

- AP Classroom Scenario Discussion: Employees in an office that requires badge access have laptop computers that they leave on their desks unattended when they all go to lunch together. The computers do not contain any sensitive information, but there are no cables securing the devices to the desks.
- AP Classroom Scenario Discussion: A hacktivist is passionate about illegal fishing practices supported by a local food production company. The main webpage of this food production company would be a high value target for this hacktivist; defacing the webpage to expose the company's support of illegal fishing would provide no financial gain to the adversary but would allow them to raise awareness about an issue that motivates them.

Instructional Strategies:

- Use a presentation to demonstrate new material.
- Use PowerPoint slides to present concepts and terminology.
- Complete teacher-generated self-review questions, multiple-choice, true/false, and short answer problems.

Differentiation:

- Work with students in flexible small groups to provide targeted intervention, reteaching, enrichment, or extension related to cybersecurity concepts and practices.
- Provide additional scaffolds such as guided notes, network diagrams, templates, structured lab procedures, and step by step protocols for students who need support.
- Provide opportunities for students ready for additional challenge to apply advanced concepts, evaluate emerging threats, and design secure solutions to authentic cybersecurity problems.

For Language Development:

- Create and maintain a student generated cybersecurity glossary that includes terminology, definitions, examples, and real-world applications.
- Provide opportunities for students to explain cybersecurity concepts, threats, and mitigation strategies using appropriate technical vocabulary in both written and verbal formats.
- Use graphic organizers, diagrams, and visual models to connect terminology with concepts such as network security, encryption, authentication, risk management, and incident response.
- Develop study guides with clear definitions, case studies, and opportunities to practice cybersecurity communication and analysis.

For Enrichment:

- Meet in small groups with students who are ready for enrichment to provide instruction on advanced cybersecurity topics followed by challenging extension activities.
- Allow students to engage in more rigorous investigations, simulations, and problem-solving tasks that require deeper analysis of cybersecurity threats and defenses.
- Provide opportunities for students to explore specialized areas such as ethical hacking, digital forensics, cloud security, artificial intelligence security, cryptography, or security operations.
- Encourage students to complete enrichment projects involving security assessments, threat analysis, cyber defense strategies, policy development, or research on emerging cybersecurity issues that extend the core content while maintaining alignment with course objectives.

Desired Results

Essential Questions:

- How can cybersecurity professionals evaluate and document the likelihood and impact of risks, with and without AI support?
- What role does AI play in enhancing risk assessment and mitigation strategies in cybersecurity?
- How do protective risk management strategies reduce the impact of threats, and how can their effectiveness be evaluated?
- What are the key types of security controls, and how do they help mitigate specific cybersecurity risks?
- How can mitigations be implemented and logged effectively to support ongoing security operations?
- What methods are used to detect and classify cyberattacks, and how can digital evidence be analyzed to support this process?
- How do different threat detection methods (e.g., signature-based, anomaly-based, hybrid) impact the speed, accuracy, and cost of response?
- What are the benefits and limitations of using AI in threat detection and incident response?

Enduring Understandings:

Students will understand that…

- The address resolution protocol (ARP) is used by a default gateway on a network to establish a table that pairs internet protocol (IP) addresses with media access control (MAC) addresses. An ARP poisoning attack is when an adversary sends falsified ARP packets to the default gateway to modify the table so that the adversary's device receives traffic intended for the target by linking the target's IP address to the adversary's MAC address. Faking a MAC address is called MAC spoofing. This is an example of an on-path attack (or man-in-the middle attack), which is when an adversary interrupts a data stream between two parties, captures both parties' data, and copies or alters the data before sending them on. Both parties think they are communicating directly with each other, but instead they are each communicating with the adversary who is secretly intercepting their messages.
- A MAC flooding attack is when an adversary sends the target switch many Ethernet frames, each with a different MAC address. This can force the switch into broadcast mode, and the adversary can then collect all of the frames on the network (because they are being broadcast), which could allow the adversary to access sensitive information. This is an example of eavesdropping (or sniffing), which is when an adversary captures data in transit and can record and copy the data.
- A domain name system (DNS) poisoning attack is when an adversary pretends to be an authoritative name server (NS) and plants a fake DNS record on a DNS server to redirect browser traffic to a malicious website designed to steal credentials. This is an example of credential harvesting, which is when adversaries set up a fake login site that looks like a real one. Unsuspecting users enter their real credentials, which the adversaries capture and use.
- Adversaries can send malicious traffic into a network to flood it, create a DoS, map the internal structure of the network, or spoof a legitimate device. Networks without firewalls, or with improperly configured firewalls, are vulnerable to these types of attacks.

- Adversaries that have compromised a device often attempt to leverage their access to compromise other devices on the local area network (LAN).
- Adversaries that physically plug into a data port can gain access to a LAN through the switch port unless port security is enabled. This allows adversaries to launch DoS attacks or perform MAC flooding or MAC spoofing attacks.
- Adversaries standing outside of physically secure spaces can pick up the signals and beacon frames from a wireless access point that is broadcasting outside the physical space. This allows them to gather information about the wireless network and to attempt eavesdropping and cryptographic attacks on it.
- Adversaries can attempt to join networks to launch attacks from within the networks. Networks that do not authenticate devices and users make it easier for adversaries to join.
- If there is an open network port, an adversary can plug a wireless access point into the port creating a rogue access point. The adversary could use this rogue access point to access the internal network wirelessly (maybe even from outside the physical space). This allows the adversary direct access to the LAN, bypassing any firewalls.
- Vulnerabilities on a network can lead to adversaries being able to intercept and alter data in transit, launch DoS attacks, or move laterally on a network to gain access to more sensitive or critical systems. Network vulnerabilities can constitute a risk to confidentiality, integrity, and availability.
- There are automated vulnerability scanners that can check networks, devices, and applications for known vulnerabilities. These scanners produce a report that often includes the vulnerabilities detected, their severity, and mitigation recommendations.
- Successfully exploiting a network vulnerability often requires advanced technical ability and knowledge. This can impact the likelihood of an exploit.
- High risks from network vulnerabilities allow an adversary to easily have a significant impact by capturing network traffic, spoofing a legitimate device on the network, or launching a DoS attack.
- Moderate risks from network vulnerabilities could include vulnerabilities that might give adversaries the ability to gain information about systems or devices on a network.
- Low risks from network vulnerabilities include vulnerabilities that would be difficult to exploit and would likely have minimal negative impacts on an organization.
- A router security policy will set forth a minimum configuration standard for routers on an organization’s network.
- A switch security policy will set forth a minimum configuration standard for switches on an organization’s network.
- A virtual private network (VPN) policy will detail the minimum security requirements for employees using a VPN to access an organization’s internal network.
- A wireless security policy will establish the minimum security requirements for wireless networks within an organization.
- Organizations can disable beacon frame broadcasting on wireless access points (WAPs) to make it harder for adversaries to find their wireless network and learn its basic properties.
- Organizations can control the broadcast direction and signal strength of a WAP so the signal does not extend beyond the physical space the access point is meant to cover.
- Organizations should enable strong wireless encryption protocols to ensure wireless frames are not readable by adversaries who might intercept them.
- Organizations can require users to authenticate to join a network. Organizations can also enable MAC filtering to prevent unauthorized devices from accessing the network.

- Firewall zones and rules can be used to create a screened subnet (also known as a demilitarized zone, or DMZ)—a network segment that sits between public, external networks like the internet and internal, private networks. A screened subnet is typically a lower security zone than the internal, private networks, and it typically holds an organization's publicly facing resources, separating them from the internal network.
- Subnetting can be used to create different subnets based on IP addressing. If a device is compromised by an adversary, subnets can contain a security breach to reduce the number of exposed devices.
- Switches can be used to create VLANs, which logically separate devices physically connected to central switches.
- Network segmentation refers to the process of dividing a network into smaller, isolated segments or subnetworks (subnets).
- Dividing a network into smaller subnets isolates network traffic, which can prevent attacks on one subnet from impacting devices on other subnets.
- Network segmentation can allow for different security policies and controls to be applied to different segments of the network, allowing for higher security zones and lower security zones.
- Port security on a switch can prevent MAC flooding by limiting the number of addresses assignable to any single switch port.
- A firewall is used to allow or deny network traffic in or out of a network. The firewall itself is software that can be hosted on a standalone device or integrated into another network device, such as a router.
- A stateless firewall filters traffic based on information in packet headers, such as IP addresses, ports, and protocols.
- A stateful firewall (also known as dynamic packet filtering) tracks the state of network connections passing through the firewall and can filter according to connection-related rules in addition to the filtering done by a stateless firewall. This allows for more control over content allowed in and out of a network.
- A next-generation firewall (NGFW) has both the capabilities of typical stateless and stateful firewalls and additional advanced features, such as intrusion prevention, deep packet inspection, and filtering by application type.
- Network administrators create a set of rules, called an access control list (ACL), that a firewall uses to permit or deny inbound and outbound network traffic.
- The requirements for a firewall will specify what type of traffic from which sources or to which destinations should be allowed or denied.
- Automated detection tools analyze data collected from an organization's network and devices, such as switches and routers, servers, firewalls, and user computers. These data are often collected in a log file.
- A network intrusion detection system (NIDS) is an automated tool that analyzes data to determine if malicious activity is taking place on a network. When an attack is detected, it generates an alert.
- A network intrusion prevention system (NIPS) is an automated tool that, like an IDS, analyzes data to determine if malicious activity is taking place on a network. A NIPS can also mitigate or halt an attack by closing ports, blocking specific IP or MAC addresses, or rejecting specific protocols.
- A security information and event management (SIEM) system collects and analyzes data from multiple sources (including firewalls, NIDS/NIPS, device logs, and application logs) to detect patterns that may indicate a cyberattack and raises an alert if a potential attack is detected. Security analysts investigate the alert to determine whether it represents a true threat and follow standard operating procedures to resolve or escalate the alert.

- Computers log every action that users take. Firewalls, IDS, IPS, and other network sensors log all the traffic passing through various points in a network. A medium-sized organization's network is logging millions (or even tens of millions) of data points per day. Even a large team of humans is incapable of analyzing so much data.
- Threat detection teams are creating AI algorithms to analyze large amounts of data and classify the data patterns as malicious or normal.
- Volume of network traffic is a criterion for determining a detection method. Signature-based detection is more efficient for networks with high traffic volume. Signature-based detection compares detection data to a database of known indicators of compromise (IoCs), called signatures. Signature databases must be updated with IoCs for the latest attacks. Signature-based detection runs more quickly than anomaly-based detection.
- Cost is a factor in evaluating the impact of a network detection method. Detection tools and ongoing costs need to be within a budget. Anomaly-based detection systems require more expensive hardware to operate than signature-based systems. Hybrid detection is the most expensive option because it combines both anomaly-based and signature-based methods.
- Cost is a factor in evaluating the impact of a network detection method. Detection tools and ongoing costs need to be within a budget. Anomaly-based detection systems require more expensive hardware to operate than signature based. Hybrid detection is the most expensive option because it combines both anomaly and signature based methods.
- Evil-twin attacks can be detected by regularly scanning for service set identifiers (SSIDs) that look suspicious or similar to local legitimate SSIDs. Signal triangulation can be used to locate and disable an access point broadcasting an evil-twin network.
- Jamming attacks can be detected by recognizing that no wireless devices in a specific physical space are able to connect to a wireless network and by scanning for electromagnetic (EM) noise in the wireless range.
- ARP poisoning attacks can be detected by monitoring network traffic for unusual ARP messages (particularly duplicate MAC address ARP packets) and checking the ARP table on the default gateway.
- MAC flooding attacks can be detected by monitoring network traffic for an unexpected surge of Ethernet frames with different MAC addresses and checking the MAC address table on a switch.
- DNS poisoning attacks are difficult to detect. However, if an organization's website experiences an abrupt and otherwise inexplicable drop in traffic, DNS records should be examined as a potential cause.
- Smurf attacks can be detected by watching network traffic for a sudden increase in ICMP requests sent to the network's broadcast address.

Knowledge:
Students will know…

- Definitions: ARP, ARP poisoning, MAC address, MAC spoofing, MAC flooding, DNS poisoning, credential harvesting, DoS attack, firewall (stateless, stateful), access control list (ACL), port security, LAN, WAP, rogue access point, SSID, jamming attack, cryptographic attack, network segmentation, VLANs, subnetting, IP addressing, network vulnerabilities, lateral movement, confidentiality, integrity, availability, vulnerability scanner, detection tools (NIDS, NIPS, SIEM), threat detection, signature-based detection, anomaly-based detection, hybrid detection, indicators of compromise (IoCs), Smurf attack, ICMP requests, broadcast address, wireless encryption, MAC filtering, screened subnet (DMZ), router/switch/VPN/wireless security policies, beacon frames, signal triangulation, log files.

Skills:

Students will be able to…

- Evaluate, with and without the support of AI, the likelihood and impact of risks.
- Document, with and without the support of AI, the likelihood and impact of risks.
- Evaluate, with and without the support of AI, the impact of protective risk management strategies.
- Implement and log mitigations with and without the support of AI.
- Identify security controls and explain how they mitigate risks.
- Evaluate the impact of threat detection methods.
- Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

Computer Science Standards:

CSTA K-12 Computer Science Standards

- 2-NI-05 Explain how physical and digital security measures protect electronic information. (P7.2) 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
- 2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
- 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
- 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.
- 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
- 2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
- 3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
- 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

AP Cybersecurity Computational Thinking Practices

3.1.A Identify common network attacks.
3.1.B Explain how adversaries can exploit network vulnerabilities to steal, disrupt, or destroy network communication.
3.1.C Assess and document risks from network vulnerabilities.
3.2.A Identify managerial controls related to network security.
3.2.B Configure wireless network security features.
3.3.A Identify techniques for segmenting a network.
3.3.B Explain why network segmentation can increase network security.
3.4.A Identify types of network-based firewalls.
3.4.B Explain how a firewall uses an access control list to allow or deny traffic entering or leaving a network.
3.4.C Determine the effective placement of firewalls in a network.
3.4.D Configure a firewall to manage the flow of network traffic.
3.5.A Identify types of automated security tools used to detect network attacks.

3.5.B Explain how organizations can leverage artificial intelligence (AI) to enhance threat detection and response.
3.5.C Determine a network detection method.
3.5.D Evaluate the impact of a network detection method.
3.5.E Apply detection techniques to identify indicators of network attacks by analyzing log files.

Acceptable Evidence

Acceptable evidence of learning other than Performance Tasks:
Formative Assessment

- Warm-ups
- Check point assignments
- Class work
- Homework
- Exit slips
- Keep a notebook
- Current Event Reports
- Quizzes
- Canvas Quizzes
- Programming Assignments
- Unit Quiz

Summative Assessment

- Unit Test

Suggested learning experiences and instruction

Learning Experiences:

- AP Classroom: Progress Check for Unit 3.
- AP Classroom Scenario: Protecting Patient Medical Data
- AP Classroom Scenario: Protecting a Network on a Naval Submarine
- AP Classroom Scenario: Configuring a Secure Wireless Network

Instructional Strategies:

- Use a presentation to demonstrate new material.
- Use PowerPoint slides to present concepts and terminology.
- Complete teacher-generated self-review questions, multiple-choice, true/false, and short answer problems.

Differentiation:

- Work with students in flexible small groups to provide targeted intervention, reteaching, enrichment, or extension related to cybersecurity concepts and practices.
- Provide additional scaffolds such as guided notes, network diagrams, templates, structured lab procedures, and step by step protocols for students who need support.
- Provide opportunities for students ready for additional challenge to apply advanced concepts, evaluate emerging threats, and design secure solutions to authentic cybersecurity problems.

For Language Development:

- Create and maintain a student generated cybersecurity glossary that includes terminology, definitions, examples, and real world applications.
- Provide opportunities for students to explain cybersecurity concepts, threats, and mitigation strategies using appropriate technical vocabulary in both written and verbal formats.
- Use graphic organizers, diagrams, and visual models to connect terminology with concepts such as network security, encryption, authentication, risk management, and incident response.
- Develop study guides with clear definitions, case studies, and opportunities to practice cybersecurity communication and analysis.

For Enrichment:

- Meet in small groups with students who are ready for enrichment to provide instruction on advanced cybersecurity topics followed by challenging extension activities.
- Allow students to engage in more rigorous investigations, simulations, and problem-solving tasks that require deeper analysis of cybersecurity threats and defenses.
- Provide opportunities for students to explore specialized areas such as ethical hacking, digital forensics, cloud security, artificial intelligence security, cryptography, or security operations.
- Encourage students to complete enrichment projects involving security assessments, threat analysis, cyber defense strategies, policy development, or research on emerging cybersecurity issues that extend the core content while maintaining alignment with course objectives.

Desired Results

Essential Questions:

- How do different types of computing devices (servers, personal computers, handheld devices, and embedded systems) impact cybersecurity strategies?
- What unique security challenges do Internet of Things (IoT) devices and embedded systems present in critical infrastructure and everyday life?
- How can adversaries exploit common device vulnerabilities such as weak authentication, open ports, and unpatched software?
- What role does malware—including fileless malware—play in cyberattacks, and how can organizations defend against it?
- Why are cryptographic hash functions important for password security, and how do adversaries attempt to compromise them?
- How do authentication mechanisms, password complexity requirements, and multifactor authentication (MFA) strengthen security?
- What policies and technical controls (e.g., acceptable use policies, anti-malware software, host-based firewalls) help protect devices and networks?
- How do detection methods (signature-based, anomaly-based, hybrid) and system resource limitations influence cybersecurity performance and risk management?
- How do cost considerations, device sensitivity, and authentication practices influence the selection and implementation of threat detection methods in cybersecurity?

Enduring Understandings:

Students will understand that…

- Server computers are devices that provide one or more services to other computers (e.g., DNS, DHCP, FTP). Any computer can be a server, and in an enterprise environment servers typically have more processing power and storage than a personal computer.
- Personal computers are devices that are designed to be used by one person for work or recreational purposes (e.g., word processing, graphic design, web browsing, and media production or viewing). These include desktop, laptop, and notebook computers.
- Handheld computers (also called mobile computers or information appliances) are smaller than personal computers and run on battery power. These include tablets, smartphones, and wearable technology like smart watches.
- Embedded computers are devices that are part of a machine. Embedded devices have specific instruction sets for interfacing with the specialized components of the machine in which they are embedded. Embedded computers tend to be slower and cheaper than other computers and have minimal storage.
- Everyday devices with embedded computers are often called Internet of Things (IoT) devices. Embedded computers are found in transportation (e.g., cars, trains, and airplanes), devices that operate critical infrastructure (e.g., operating circuit breakers at electrical substations and pumps at water treatment plants), medical equipment (e.g., IV pumps, MRI scanners, pacemakers, and insulin pumps), and everyday devices like washing machines, coffee makers, and thermostats.

- Malware is often used as a tool to accomplish part of an adversary's plan to achieve their ultimate goal(s). There are many types of malware.
- Devices with unpatched software are vulnerable to these exploits, which could allow an adversary to crash a system, view user actions, enable or disable various services or components on the device, such as turning on a webcam or microphone, or even take control of the device to issue commands to steal or destroy information on the device.
- Adversaries can take advantage of weak authentication requirements by guessing a user's password or using social engineering to get a user to divulge their password.
- Adversaries can leverage open ports to connect to a device.
- Adversaries can send malicious data to devices to disrupt them or attempt to take control of them. Devices that have no firewall (or a misconfigured firewall) cannot filter out this malicious data.
- Adversaries often attempt to install malware on a device to disrupt or control it. Devices lacking anti-malware software are more vulnerable to this type of attack.
- Risk from device vulnerabilities can come from unauthorized access or malware that allows an adversary to impersonate an authorized user, remotely control a device, encrypt a device's drive to ransom the data, or wipe a device's memory, destroying data or rendering the device inoperable. The level of risk varies depending on the criticality of the device, the services the device provides, or the data it stores.
- A cryptographic hash function (also called a message digest function) is a mathematical algorithm that takes binary data of an arbitrary length, processes it according to a set of instructions, and outputs a fixed-length binary string called the hash (or checksum or message digest).
- Adversaries try to compromise hashing functions by forcing collisions in their output. If an efficient algorithm exists to force a collision for a specific hash function, then that hash function will be deprecated (no longer used in secure settings). MD5 and SHA1 are examples of deprecated hash functions.
- Password-based authentication services should not store passwords in plaintext, so that if an adversary gains access to the user:password directory they will not immediately know the passwords for all users. Instead, user passwords should be hashed and the hash stored in a database. When a user enters their password, it is hashed, and the hash is compared to the hash stored on file. If the hashes match, then the user is authenticated.
- If an adversary can compromise the password of a legitimate user, and that user's organization has not enabled MFA or other authentication protections, then the adversary can act within that organization with all the access and rights available to the user.
- Password attacks can be classified as online or offline.
- Many users reuse the same passwords (or variations of the same password) for all the services and accounts they have, despite warnings not to. When an organization's user database is stolen, the usernames, emails, and passwords are sold to adversaries or posted online. Adversaries often begin an attempt to compromise an account by trying stolen or leaked credentials for a target individual.
- Authentication mechanisms are technical controls that verify the identity of a user to ensure that only authorized users access a system. The proof the user provides to identify themselves is called a factor.
- Requiring complexity in passwords is a login setting that can be configured. When enabled, users setting a new password must include at least one character from each character set. Passwords

with characters from each character set are significantly harder for an adversary to crack than passwords that use characters from only one or two character sets.

- An acceptable use policy will describe the range of activities that are permissible, prohibited, or required by users on devices owned by an organization.
- Anti-malware software (sometimes called antivirus software) has tools to quarantine and remove malware that can corrupt, spy on, or destroy a system. Malware contains indicators that make it detectable; these indicators are called signatures.
- When vulnerabilities in operating systems and software are found, the vendor or organization that maintains the operating system software will fix it and send an update. A small update is called a patch.
- Host-based firewalls allow or deny traffic into or out of a single device. This provides an extra layer of security in case a host is connected to a compromised network.
- System processes and settings, login attempts, file download attempts, and user actions are logged by computing systems. These logs can be used to reconstruct circumstances leading up to and during a cyber incident.
- Performance is a criterion for determining a detection method. Detection tools use system memory and processing power and can impact the performance of a device. Anomaly-based detection tools use more system resources than signature-based tools. Signature-based detection is a better option for devices with less powerful system resources. Many embedded devices do not have enough system resources to run any detection tools on the device.
- Cost is a criterion for determining a detection method. Organizations that purchase detection software need to consider the cost of purchasing enough software licenses for the number of devices they need to monitor. Some organizations purchase an endpoint detection and response (EDR) service from a third-party vendor. Although these services are expensive, they provide a holistic, unified approach to threat detection for an organization's devices; they typically include a centralized alert platform for monitoring possible attacks on devices.
- Sensitivity or criticality of the device is a criterion for determining a detection method. Devices that store or process sensitive information or provide critical services are more likely to be targeted by adversaries and benefit from a hybrid-detection model to offer maximum protection, when possible.
- Online password attacks can be detected in authentication logs. A single user attempting many wrong passwords is an indicator of an online password attack. If a user:password hash database has been compromised, all the user passwords in the database should be considered insecure and all users should be forced to reset their passwords.

Knowledge:

Students will know…

- Definitions: Server, DNS, DHCP, FTP, personal computer, desktop, laptop, handheld computer, mobile computer, tablet, smartphone, wearable technology, embedded computer, Internet of Things (IoT), malware, patch, firewall, host-based firewall, anti-malware software, signature, cryptographic hash function, hash, collision, MD5, SHA1, password-based authentication, multifactor authentication (MFA), password attack, online password attack, offline password attack, authentication factor, acceptable use policy, system logs, anomaly-based detection, signature-based detection, endpoint detection and response (EDR), performance impact, cost analysis, authentication logs.

Skills:

Students will be able to…

- Evaluate, with and without the support of AI, the likelihood and impact of risks.
- Document, with and without the support of AI, the likelihood and impact of risks.
- Identify security controls, and explain how they mitigate risks.
- Determine layered security controls that address vulnerabilities.
- Evaluate, with and without the support of AI, the impact of protective risk management strategies.
- Implement and log mitigations with and without the support of AI.
- Determine strategies and methods to detect attacks.
- Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

Computer Science Standards:

CSTA K-12 Computer Science Standards

- 2-NI-05 Explain how physical and digital security measures protect electronic information. (P7.2) 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
- 2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
- 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
- 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.
- 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
- 2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
- 3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
- 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

AP Cybersecurity Computational Thinking Practices

4.1.A Identify types of computing devices.
4.1.B Identify the type of malware used in a cyberattack.
4.1.C Explain how adversaries can exploit common device vulnerabilities to cause loss, damage, disruption, or destruction.
4.1.D Assess and document risks from device vulnerabilities.
4.2.A Explain why hashes (also called hash outputs, checksums, message digests, or digests) are used to store passwords.
4.2.B Explain how password attacks exploit vulnerabilities.
4.2.C Determine the type of authentication used to verify the identity of a user.
4.2.D Configure login settings to make a device more secure.
4.3.A Identify managerial controls related to device security.
4.3.B Explain how anti-malware software can make a device more secure.
4.3.C Explain why keeping a device's operating system and software updated makes it more secure.
4.3.D Configure a host-based firewall.
4.4.A Explain how to detect attacks against devices.

4.4.B Determine controls for detecting attacks against a device.
4.4.C Evaluate the impact of a device detection method.
4.4.D Apply detection techniques to identify indicators of password attacks by analyzing log files.

Acceptable Evidence

Acceptable evidence of learning other than Performance Tasks:
Formative Assessment

- Warm-ups
- Check point assignments
- Class work
- Homework
- Exit slips
- Keep a notebook
- Current Event Reports
- Quizzes
- Canvas Quizzes
- Programming Assignments
- Unit Quiz

Summative Assessment

- Unit Test

Suggested learning experiences and instruction

Learning Experiences:

- AP Classroom: Personal Progress Check for Unit 4
- AP Classroom Scenario: Designing Secure Connected Farm Equipment
- AP Classroom Scenario: Configuring Authentication Settings
- AP Classroom Scenario: Analyzing Log Files for Indicators of Compromise

Instructional Strategies:

- Use a presentation to demonstrate new material.
- Use PowerPoint slides to present concepts and terminology.
- Complete teacher-generated self-review questions, multiple-choice, true/false, and short answer problems.

Differentiation:

- Work with students in flexible small groups to provide targeted intervention, reteaching, enrichment, or extension related to cybersecurity concepts and practices.
- Provide additional scaffolds such as guided notes, network diagrams, templates, structured lab procedures, and step by step protocols for students who need support.
- Provide opportunities for students ready for additional challenge to apply advanced concepts, evaluate emerging threats, and design secure solutions to authentic cybersecurity problems.

For Language Development:

- Create and maintain a student generated cybersecurity glossary that includes terminology, definitions, examples, and real-world applications.
- Provide opportunities for students to explain cybersecurity concepts, threats, and mitigation strategies using appropriate technical vocabulary in both written and verbal formats.
- Use graphic organizers, diagrams, and visual models to connect terminology with concepts such as network security, encryption, authentication, risk management, and incident response.
- Develop study guides with clear definitions, case studies, and opportunities to practice cybersecurity communication and analysis.

For Enrichment:

- Meet in small groups with students who are ready for enrichment to provide instruction on advanced cybersecurity topics followed by challenging extension activities.
- Allow students to engage in more rigorous investigations, simulations, and problem-solving tasks that require deeper analysis of cybersecurity threats and defenses.
- Provide opportunities for students to explore specialized areas such as ethical hacking, digital forensics, cloud security, artificial intelligence security, cryptography, or security operations.
- Encourage students to complete enrichment projects involving security assessments, threat analysis, cyber defense strategies, policy development, or research on emerging cybersecurity issues that extend the core content while maintaining alignment with course objectives.

Desired Results

Essential Questions:

- Why is encryption critical for protecting data stored on devices and drives, and what risks arise when files remain unencrypted?
- How can weak access control settings lead to security breaches, and what strategies can organizations use to prevent these vulnerabilities?
- What is the difference between local applications and web applications, and how does this distinction impact security risks?
- Why does accepting unvalidated or unsanitized user input pose a threat to database security, and how can developers mitigate this risk?
- How do SQL injection and cross-site scripting (XSS) attacks exploit application vulnerabilities, and what are the potential consequences for confidentiality, integrity, and availability?
- What is a buffer overflow, and why does exceeding a buffer's size create opportunities for adversaries to compromise a system?
- Why do organizations classify data and implement cryptography policies, and how do these measures help meet legal and regulatory requirements?
- How do access control models like RBAC and RuBAC enforce security, and why is the principle of least privilege essential for reducing risk?
- Why is encryption necessary for secure communication, and how do symmetric and asymmetric encryption differ in terms of key management and security strength?
- How do detective controls such as log analysis, honeypots, and cryptographic hash functions help identify and respond to malicious activity in real time?

Enduring Understandings:

Students will understand that…

- An adversary can read any unencrypted files if they have access to the device or drive storing the files.
- Computers have standard users and administrative users. Administrative users have access to control system settings and can typically access any files or applications on a system. If regular users are given administrative privileges on a computer, and an adversary can compromise a user's account, then the adversary will have elevated privileges on the system.
- When access control settings are weakly configured, many users often have permission to view and sometimes even edit files on a system. Adversaries can take advantage of weak access control settings to steal or destroy files or disrupt an application.
- Applications are programs that run instructions on computers; they are executable data. Some applications run locally on a user's computer, while other applications, like web applications, run on a server and are accessed by users through a network.
- Structured Query Language (SQL) is a computer language used to request information from databases and make changes to databases or entries in databases. Applications that query a database using unvalidated or unsanitized input from users are vulnerable.
- An SQL-injection attack places SQL commands and control characters into a user-input field in an application, which can lead to a breach of confidentiality by causing the application to return

more information than it should, or a breach of integrity by modifying or deleting data in the database.

- Websites are written using Hypertext Markup Language (HTML), and many websites use JavaScript to create dynamic content on websites or web applications. Because JavaScript commands run in the browser of the user visiting the website, those commands can access sensitive data stored in the browser, such as usernames, passwords, and cryptographic keys.
- A cross-site scripting (XSS) attack injects malicious code into a website that a user's browser then executes. The malicious code can be embedded in a link the user clicks (a Type I or Reflected XSS attack), or it can be inserted onto a website through a comment field, forum post, or visitor log, which would affect any user visiting that website (a Type II or Stored XSS attack).
- When applications take user input, that input is written to a buffer. A buffer is a designated section of computer memory with a fixed size. If the amount of data the user enters exceeds the size of the buffer, it can overflow into adjacent memory locations and overwrite other parts of the computer's memory.
- A buffer overflow attack feeds more data into memory than was allotted, which can cause a system to crash or to execute code outside the scope of a program's security policy, effectively allowing the adversary to perform unauthorized actions on a computer, such as accessing, modifying, or deleting files.
- Data security risks can involve a compromise of confidentiality when unauthorized persons can access sensitive data, integrity when data can be manipulated or altered from its intended state, and availability when data can be destroyed or encrypted to prevent others from accessing it.
- Organizations implement specific security controls to comply with legal requirements based on the types of data they collect, store, process, and transmit.
- Laws and regulations can require certain types of data to be stored, transmitted, and handled according to specific rules.
- Organizations that collect regulated data will label them and have policies that comply with the legal or regulatory requirements for the safe storage, transmission, and handling of these data.
- A cryptography policy describes the acceptable encryption protocols and key parameters for an organization.
- A web application security policy outlines the requirements and parameters for testing and mitigating web application vulnerabilities in an organization.
- Access control enforces which users or applications (called subjects) can access, modify, add, or remove (called operations) which files or applications (called objects). Access control models describe how to determine which subjects have what type of access to which objects.
- Role-based access control (RBAC) assigns every subject to a role and defines which roles have which types of access to which objects.
- Rule-based access control (RuBAC) checks a set of rules to determine what type of access a subject should have for a specific object and then allows or denies types of access based on the rules. This access control model is typically layered on top of another access control model.
- The principle of least privilege is the idea that entities should be given exactly as much access as they need to perform their function and no more.
- Authorization is when an entity is granted permission to have a certain type of access to a resource. Access controls are put in place to control which users have what types of access to which data.
- Linux commands can be used to set and change file access permissions.

- The purpose of cryptography is to hide information. A cryptographic algorithm defines a process for encrypting and decrypting information. Encryption is the process of hiding the information, and decryption is the process of reversing the encryption to retrieve the original information.
- An encryption algorithm defines a process for combining the information to be encrypted with a predefined key. The information to be encrypted is called the plaintext. The output of the encryption algorithm is called the ciphertext.
- Computer-based encryption algorithms operate on binary data. The most common symmetric encryption algorithm is the Advanced Encryption Standard (AES). AES encryption is used to secure Wi-Fi transmissions, internet browsing, file encryption on disks, and hardware-level encryption on processors.
- AES is a symmetric key block cipher that encrypts data in 128-bit blocks (16 bytes). AES can operate with keys of varying lengths. Longer keys produce more secure encryption but require more time to encrypt and decrypt.
- Symmetric encryption and decryption can be performed using the command line, specialized software, or web-based tools.
- Using OpenSSL in a CLI, a user can encrypt and decrypt a file.
- Asymmetric encryption allows users to communicate securely without prearranging a shared secret key.
- Longer keys result in larger keyspaces. For binary keys, an n-bit length key has a keyspace of 2n.
- Using an application to randomly guess an n-bit length encryption key means that on average an adversary will be able to guess the correct key in 2n /2 or 2n-1 guesses.
- Computational processing power and efficiency continue to improve, allowing software to guess keys faster. Key-length recommendations for both symmetric and asymmetric encryption algorithms are periodically increased to account for increased processing power.
- Common asymmetric encryption algorithms include RSA and elliptic curve cryptography (ECC). Asymmetric algorithms are used in many applications, including digital signatures and digital certificates.
- As with symmetric encryption, asymmetric encryption and decryption can be performed using the command line, specialized software, or web-based tools.
- Secure by design is an initiative that encourages companies to include security in all phases of product development including design. When organizations implement secure by design, security is a design principle not just a technical feature.
- When users enter input into an application, the application typically encases that input in special characters to process it. The characters that encase the user input are called control characters and include the single quote, the double quote, and the semicolon.
- Devices track and log when data are accessed and by whom. The process of recording and monitoring user activities is called accounting. Analysis of these logs can reveal malicious activity when an adversary attempts to access, copy, move, or delete data.
- Cost is a criterion in determining detective controls. Detective controls like honeypots and using hash values to check data integrity are inexpensive. Some organizations invest in third-party data loss prevention (DLP) services, which monitor data access, usage, and transmission by users throughout the organization to detect suspicious activity; DLP services provide strong detection capabilities at a higher cost.
- To operate at an effective speed, log analysis needs to be augmented with some automation. Honeypots offer near instantaneous detection capabilities.
- Cryptographic hash functions can help identify changes in a file because they are repeatable: the same input always produces the same output for a given hash function.

- SQL injection attacks can be detected by reviewing application and server logs of user input for SQL control words and symbols.
- XSS attacks can be detected by reviewing user input for suspicious tags.
- For web applications, buffer overflows can be detected by checking the amount of data the user is sending to the web application in their request.
- Directory traversal attacks can be detected by reviewing application and server logs. HTTP GET requests that include paths with sequences of ../ are indicators of an adversary attempting a directory traversal.

Knowledge:
Students will know…

- Definitions: Adversary, unencrypted files, access control, access control settings, weak access control, executable data, local application, web application, Structured Query Language (SQL), database, unvalidated input, unsanitized input, SQL injection, control characters, cross-site scripting (XSS), Reflected XSS (Type I), Stored XSS (Type II), buffer, buffer overflow, security controls, data classification, cryptography policy, web application security policy, access control model, Role-Based Access Control (RBAC), Rule-Based Access Control (RuBAC), principle of least privilege, authorization, Linux file permissions, cryptography, encryption, decryption, encryption algorithm, plaintext, ciphertext, Advanced Encryption Standard (AES), symmetric encryption, asymmetric encryption, key length, keyspace, RSA, Elliptic Curve Cryptography (ECC), digital signature, digital certificate, OpenSSL, accounting (in cybersecurity), log analysis, honeypot, Data Loss Prevention (DLP), cryptographic hash function, directory traversal attack, HTTP GET request.

Skills:
Students will be able to…

- Evaluate, with and without the support of AI, the likelihood and impact of risks.
- Document, with and without the support of AI, the likelihood and impact of risks.
- Evaluate, with and without the support of AI, the impact of protective risk management strategies.
- Implement and log mitigations with and without the support of AI.
- Determine layered security controls that address vulnerabilities.
- Identify security controls, and explain how they mitigate risks.
- Determine strategies and methods to detect attacks.
- Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

Computer Science Standards:

CSTA K-12 Computer Science Standards

- 2-NI-05 Explain how physical and digital security measures protect electronic information. (P7.2) 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
- 2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
- 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
- 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.

- 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
- 2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
- 3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
- 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

AP Cybersecurity Computational Thinking Practices

5.1.A Explain how adversaries can exploit application and file vulnerabilities to cause loss, damage, disruption, or destruction.
5.1.B Explain how application attacks exploit vulnerabilities.
5.1.C Assess and document risks from application and data vulnerabilities.
5.2.A Explain how the state or classification of data impacts the type and degree of security applied to that data.
5.2.B Identify managerial controls related to application and data security.
5.2.C Determine an appropriate access control model to protect applications and data.
5.2.D Configure access control settings on a Linux-based system.
5.3.A Explain how encryption can be used to protect files.
5.3.B Apply symmetric encryption algorithms to encrypt and decrypt data.
5.4.A Determine the appropriate asymmetric key to use when sending or receiving encrypted data.
5.4.B Explain why the length of a key impacts the security of encrypted data.
5.4.C Apply asymmetric encryption algorithms to encrypt and decrypt data.
5.5.A Identify the application security principles of secure by design and security by default.
5.5.B Explain how user input sanitization protects applications.
5.6.A Explain how to detect attacks on data.
5.6.B Determine controls for detecting attacks against applications or data.
5.6.C Evaluate the impact of a method for detecting attacks against an application or data.
5.6.D Identify whether a file has been altered by verifying its hash.
5.6.E Apply detection techniques to identify and report indicators of application attacks by analyzing log files.

Acceptable Evidence.

Acceptable evidence of learning other than Performance Tasks:
Formative Assessment

- Warm-ups
- Check point assignments
- Class work
- Homework
- Exit slips
- Keep a notebook
- Current Event Reports
- Quizzes
- Canvas Quizzes
- Programming Assignments
- Unit Quiz

Summative Assessment

- Unit Test

Suggested learning experiences and instruction

Learning Experiences:

- AP Classroom: Personal Progress Check for Unit 5
- AP Classroom Scenario: Protecting Sensitive Data
- AP Classroom Scenario: Sending Encrypted Messages

Instructional Strategies:

- Use a presentation to demonstrate new material.
- Use PowerPoint slides to present concepts and terminology.
- Complete teacher-generated self-review questions, multiple-choice, true/false, and short answer problems.

Differentiation:

- Work with students in flexible small groups to provide targeted intervention, reteaching, enrichment, or extension related to cybersecurity concepts and practices.
- Provide additional scaffolds such as guided notes, network diagrams, templates, structured lab procedures, and step by step protocols for students who need support.
- Provide opportunities for students ready for additional challenge to apply advanced concepts, evaluate emerging threats, and design secure solutions to authentic cybersecurity problems.

For Language Development:

- Create and maintain a student generated cybersecurity glossary that includes terminology, definitions, examples, and real-world applications.
- Provide opportunities for students to explain cybersecurity concepts, threats, and mitigation strategies using appropriate technical vocabulary in both written and verbal formats.
- Use graphic organizers, diagrams, and visual models to connect terminology with concepts such as network security, encryption, authentication, risk management, and incident response.
- Develop study guides with clear definitions, case studies, and opportunities to practice cybersecurity communication and analysis.

For Enrichment:

- Meet in small groups with students who are ready for enrichment to provide instruction on advanced cybersecurity topics followed by challenging extension activities.
- Allow students to engage in more rigorous investigations, simulations, and problem-solving tasks that require deeper analysis of cybersecurity threats and defenses.
- Provide opportunities for students to explore specialized areas such as ethical hacking, digital forensics, cloud security, artificial intelligence security, cryptography, or security operations.
- Encourage students to complete enrichment projects involving security assessments, threat analysis, cyber defense strategies, policy development, or research on emerging cybersecurity issues that extend the core content while maintaining alignment with course objectives.