UTeach Computer Science

AP Cybersecurity
Syllabus and Planning Guide
(2026–2027)

Table of Contents

Curriculum Description

Developers

UTeach AP Cybersecurity was developed by the UTeach Institute (UTeach Computer Science) in collaboration with Teach Cyber through a partnership that brings together expert faculty from The University of Texas at Austin, successful secondary computer science teachers, and UTeach's more than 25 years of experience leading evidence-based teacher preparation nationwide.

UTeach Computer Science provides College Board-aligned, student-centered curricula that mirrors the evolving cybersecurity industry and AP requirements. Partner teachers receive comprehensive resources, including classroom-ready lesson plans, intentionally scaffolded activities and assignments, AP-style formative and summative assessments, auto grading, academic integrity features, and learner behavior insights. The customizable curriculum includes embedded teacher guidance, timely support videos, and on-demand coaching to empower educators with the instructional strategies needed to be successful in a variety of high school learning environments. UTeach CS continuously refines the program to enhance student learning experiences, build teacher capacity, address teachers' evolving needs, and broaden access to high-quality cybersecurity education.

Curriculum Overview

UTeach AP Cybersecurity is year-long high school curriculum that fully addresses the course content as specified by the College Board's AP Cybersecurity Course and Exam Description, including all topics, learning objectives, essential knowledge statements, computational thinking practices and skills, and sequenced curriculum units.

UTeach AP Cybersecurity introduces students to the principles and practices used to protect systems, networks, devices, applications, and data in today's connected world. Students examine how adversaries exploit vulnerabilities and how cybersecurity professionals use security controls, encryption, authentication, monitoring, and risk assessment to defend digital systems. Throughout the course, students explore topics including cyber threats and attacks, networking, device and application security, cryptography, and data protection while also considering the ethical, legal, and societal impacts of cybersecurity. Hands-on labs and real-world scenarios provide students with opportunities to analyze attacks, investigate vulnerabilities, and apply cybersecurity concepts in practical environments.

The lessons and materials used throughout this curriculum incorporate project-based learning (PBL), a pedagogical approach that actively engages students in the educational process, improves retention, and develops problem-solving, critical thinking, and group communication skills.

Textbook

The interactive online textbook is an essential component of the UTeach CS Cybersecurity curriculum for both students and teachers**. *It is required for students to have daily access to the internet*.** The textbook, assessments, assignments, and built-in lab environments are hosted on the cloud-based Codio platform, which can be integrated with most learning management systems. Codio is FERPA compliant, GDPR compliant, and meets the Web Content Accessibility Guidelines (WCAG) 2.1 Standard at Level AA. Codio is actively committed to maintaining and continuously improving the accessibility of the Codio experience.

Resources and Technical Requirements

Aside from the license, which may be purchased or provided through a grant, UTeach AP Cybersecurity does not require additional materials for implementation.

Websites Accessed Throughout the Curriculum

The websites below will be accessed in this curriculum. Please advise the school IT department about these websites prior to beginning the course. Always test site access from your device(s) and students' devices to ensure a smooth lesson.

**.codio.com, *.codio.io, https://uteachcs.github.io/Cyber-CSS/css/styles.css, youtube.com, *.googlevideo.com, *.ytimg.com, *.gstatic.com, acm.org/code-of-ethics, washingtonpost.com, *.nist.gov, education.cfr.org, khehy.com, cnn.com, *.wikipedia.org, scworld.com, fbi.gov, darkreading.com, itsecurityguru.org, csoonline.com, forbes.com, smartermsp.com, blog.gigamon.com, computerhistory.org, medium.com, web.mit.edu, test-ipv6.com, whatismyipaddress.com, nordvpn.com, iptrackeronline.com, wireshark.org, digiguardsecurity.org, chubb.com, typingdna.com, md5calc.com, crackstation.net*

Course Framework

The course framework consists of two components: 1) Course Skills and 2) Course Content, which includes topics, learning objectives, and essential knowledge statements.

(1) Course Skills

Cybersecurity skills, including collaboration, are critical to the deep understanding and application of cybersecurity knowledge and practice. Students should develop and use these skills throughout the course.

	Skill Category 1	Skill Category 2	Skill Category 3	Skill Category 4
	Analyze Risk Evaluate risk to organizational assets.	**Mitigate Risk** Implement protective and deterrent security controls.	**Detect Attacks** Implement detection methods, monitor systems, and analyze evidence.	**Collaborate** Work with others and AI to accomplish a task.
Communicating concepts Explain key cybersecurity concepts.	1.A Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.	2.A Identify security controls and explain how they mitigate risks.	3.A Identify methods for monitoring systems and explain how they detect attacks.	4.A Develop clear, shared team objectives related to a cybersecurity task.
Investigating problems Explore the parameters of a problem to plan for solutions.	1.B Determine ways adversaries exploit vulnerabilities to compromise an asset.	2.B Determine layered security controls that address vulnerabilities.	3.B Determine strategies and methods to detect attacks.	4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.
Assessing impacts Evaluate impacts on systems.	1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.	2.C Evaluate, with and without the support of AI, the impact of protective risk-management strategies.	3.C Evaluate the impact of threat detection methods.	4.C Implement AI as a collaboration tool individually and as a group.
Enacting solutions Apply and communicate solutions.	1.D Document, with and without the support of AI, the likelihood and impact of risks.	2.D Implement and log mitigations with and without the support of AI.	3.D Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.	4.D Complete assigned work to accomplish a collaborative cybersecurity task.

(2) Course Content

The course content is organized into units that reflect key domains of cybersecurity knowledge and practice. These units comprise the content and skills colleges and universities typically expect students to be proficient in to qualify for college credit and/or placement. Units 1–5 introduce students to security, and present knowledge and skills needed to secure spaces, secure networks, secure devices, and secure applications and data.

Curriculum Unit Overviews
Unit 1: Introduction to Security Students are introduced to foundational cybersecurity concepts through real-world scenarios that explore cyberspace, common cyber threats, and the challenges of securing modern digital environments. Students examine topics such as social engineering, password attacks, public Wi-Fi risks, AI-powered cyberattacks, and the role of AI in cybersecurity defense while learning how attackers exploit both technology and human behavior. Throughout the unit, students analyze suspicious activity, identify vulnerabilities and indicators of compromise, evaluate layered defenses, and consider the ethical and societal impacts of cybersecurity decisions.
Unit 2: Securing Spaces In Unit 2 students explore how cybersecurity threats arise and how organizations defend against them. Students examine attacks, vulnerabilities, threats, and cybersecurity risk while learning about different types of adversaries, social engineering techniques, insider threats, and the phases of a cyberattack. The unit also introduces the CIA Triad, security controls, defense-in-depth strategies, and physical security concepts that help organizations protect systems and data. Through risk assessments, security investigations, and real-world scenarios, students identify vulnerabilities, evaluate risk, and recommend appropriate security controls.
Unit 3: Securing Networks Students explore how computing devices, operating systems, and networks support modern communication and data exchange. Students learn how devices connect and communicate across networks and the internet while examining key networking concepts, protocols, and network components. Building on this foundation, students investigate common network attacks and vulnerabilities, including wireless attacks, spoofing, denial-of-service attacks, and network misconfigurations. The unit also introduces network security practices such as wireless security configurations, network segmentation, firewalls, and access control lists, along with network monitoring and detection tools such as NIDS, NIPS, and SIEM systems. Through hands-on activities and log analysis, students identify suspicious network activity and evaluate methods used to protect and monitor networks.

Unit 4: Securing Devices The focus of Unit 4 is securing individual devices and understanding how adversaries target them. Students examine malware, device vulnerabilities, weak authentication practices, and misconfigurations that can be exploited to compromise systems and data. The unit explores password security concepts such as hashing, salting, and common password attacks, while also introducing authentication factors, multi-factor authentication (MFA), and secure login configurations. Students also learn how organizations protect and monitor devices using security policies, anti-malware tools, software updates, and host-based firewalls. Through log analysis and threat detection activities, students identify indicators of compromise and investigate potential device-level attacks.
Unit 5: Securing Applications and Data Applications, data protection, and secure software practices are the primary focus of this unit. Students examine common application and data attacks, assess cybersecurity risk, and explore methods used to protect information through data classification, managerial controls, and access control models. The unit also introduces cryptography, including symmetric and asymmetric encryption, secure communication, and key management concepts. Students learn secure application design practices such as input sanitization, verify file integrity using hashing, and analyze logs and indicators of compromise to detect potential attacks on applications and data.

Unit 1: Introduction to Security

In Unit 1, students explore several common ways adversaries attempt to compromise systems and users. Through real-world scenarios, students examine how social engineering attacks manipulate human behavior, how weak authentication can lead to unauthorized access, and how public Wi-Fi networks can expose users to cyber threats. Students also investigate how adversaries use AI-powered tools to enhance cyberattacks and how cybersecurity professionals leverage AI to improve threat detection, response, and network defense. Throughout the unit, students learn strategies for recognizing cyber risks and protecting themselves through stronger security practices and safer online behavior.

Course Skills addressed:

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

Unit 1 Schedule (13 Days)

Assignment	AP Topic	# of Class Periods
1.1 The Student Tech Team Case File	1.1 Understanding Social Engineering 1.2 Suspicious Website Logins 1.3 Best Practices for Public Networks 1.4 AI-Based Cybersecurity Attacks 1.5 Leveraging AI in Cyber Defense Scenario Connections: 1A Detecting Phishing Messages 1B Detecting Unauthorized Logins 1C Impacts of Using Public Wi-Fi 1D AI-Powered Cyberattacks 1E AI-Powered Cyber Defense	2
1.2 Understanding Cyberspace and Cybersecurity	Foundational/pre-knowledge	2
1.3 Internet Security	Foundational/pre-knowledge	1
1.4 Understanding Social Engineering	1.1 Understanding Social Engineering	1
1.5 Suspicious Website Logins	1.2 Suspicious Website Logins	1
1.6 Best Practices for Public Networks	1.3 Best Practices for Public Networks	1
1.7 AI-Based Cybersecurity Attacks	1.4 AI-Based Cybersecurity Attacks	1

Assignment	AP Topic	# of Class Periods
1.8 Leveraging AI in Cyber Defense	1.5 Leveraging AI in Cyber Defense	1
1.9 Ethics and Cybersecurity	Foundational/pre-knowledge	1
1.10 Unit 1 Vocabulary Quiz		1
1.11 Unit 1 Test		1

Unit 2: Securing Spaces

In Unit 2, students examine how physical security serves as a critical first layer of cybersecurity defense. Students explore how adversaries can exploit physical access to bypass technical protections and compromise devices, systems, and data. Through analyzing vulnerabilities, threats, and attack methods, students develop adversarial thinking skills while learning how organizations secure physical spaces using layered security controls, monitoring systems, and detection methods. Students also evaluate how physical security devices and procedures can prevent, deter, and detect unauthorized access and breaches.

Course Skills addressed:

- 1.A Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.
- 1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.
- 1.D Document, with and without the support of AI, the likelihood and impact of risks.
- 2.A Identify security controls and explain how they mitigate risks.
- 2.B Determine layered security controls that address vulnerabilities.
- 3.A Identify methods for monitoring systems and explain how they detect attacks.
- 3.B Determine strategies and methods to detect attacks.

Unit 2 Schedule (22 Days)

Assignment	AP Topic	# of Class Periods
2.1.1 Unmasking Deception: Exploring Social Engineering Project Launch	Application	1
2.2 Attacks, Vulnerabilities, & Threats	Foundational/pre-knowledge	1
2.3 Social Engineering Attacks	2.1 Cyber Foundations	1
2.4 Social Engineering Lab	Reinforcement	1
2.1.2 Unmasking Deception: Exploring Social Engineering Project Workday 2	Application	1
2.5 Types of Adversaries	2.1 Cyber Foundations	1
2.6 Phases of a Cyberattack	2.1 Cyber Foundations	1
2.7 Cybersecurity Risk Assessment	2.1 Cyber Foundations	1
2.1.3 Unmasking Deception: Exploring Social Engineering Project Workday 3	Application	1
2.8 CIA Triad	2.1 Cyber Foundations	2
2.9 Security Controls	2.1 Cyber Foundations	1

Assignment	AP Topic	# of Class Periods
2.10 Physical Vulnerabilities	2.2 Physical Vulnerabilities and Attacks	1
2.11 Physical Security Risk Assessment	2.2 Physical Vulnerabilities and Attacks	1
2.12 Protecting Physical Spaces	2.3 Protecting Physical Spaces	1
2.13 Detecting Physical Attacks	2.4 Detecting Physical Attacks	1
2.14 Case Study: Securing Xtensr Labs	Scenario 2A Securing Xtensr Labs	2
2.1.4 Unmasking Deception: Exploring Social Engineering Project Workday 4	Application	1
2.15 Unit 2 Vocabulary Quiz		1
2.16 Unit 2 Test		1
Unmasking Deception: Exploring Social Engineering Project Presentations		1

Unit 3: Securing Networks

In Unit 3, students explore how computer networks enable communication between devices and how network connectivity creates opportunities for cyberattacks. Students investigate common network attacks, vulnerabilities, and methods adversaries use to intercept, manipulate, or disrupt data in transit. The unit emphasizes network defense strategies such as network segmentation, firewall placement and configuration, wireless security, and traffic management. Students also analyze network log files and monitoring data to identify indicators of compromise (IoCs) and investigate potential network threats.

Course Skills addressed:

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

Unit 3 Schedule (28 Days)

Assignment	AP Topic	# of Class Periods
3.1.1 Designing Tomorrow's Secure Network Today Project Launch	Application	1
3.2 Foundations of Computing Devices	4.1 Device Vulnerabilities and Attacks	1
3.3 Operating Systems	4.3 Protecting Devices	1
3.4 Introduction to Linux/Ubuntu OS Lab	Reinforcement	1
3.5 Introduction to Networks	Foundation/pre-knowledge	1
3.6 Components of a Network	Foundation/pre-knowledge	1
3.7 The Internet	Foundation/pre-knowledge	1
3.8 Introduction to Wireshark Lab	Reinforcement	1
3.1.2 Designing Tomorrow's Secure Network Today Project Workday 2	Application	1

Assignment	AP Topic	# of Class Periods
3.9 Common Network Attacks	3.1 Network Vulnerabilities and Attacks	1
3.10 Network Vulnerabilities	3.1 Network Vulnerabilities and Attacks	1
3.11 Network Risk Assessment	3.1 Network Vulnerabilities and Attacks	1
3.12 Linux Networking Commands Lab	Reinforcement	1
3.13 Network Managerial Controls	3.2 Protecting Networks: Managerial Controls and Wireless Security	1
3.14 Configuring Wireless Network Security	3.2 Protecting Networks: Managerial Controls and Wireless Security Scenario 3B Configuring a Secure Wireless Network	1
3.15 Network Segmentation	3.3 Protecting Networks: Segmentation Scenario 3C Protecting a Network on a Naval Submarine	2
3.1.3 Designing Tomorrow's Secure Network Today Project Workday 3	Application	1
3.16 Firewall Fundamentals	3.4 Protecting Networks: Firewalls	1
3.17 Firewall Rules and Access Control Lists	3.4 Protecting Networks: Firewalls	1
3.18 Firewall Placement and Network Protection	3.4 Protecting Networks: Firewalls Scenario 3A Protecting Patient Medical Data	1
3.19 Network Detection Tools	3.5 Detecting Network Attacks	1
3.20 Network Detection Methods	3.5 Detecting Network Attacks	1
3.21 Detecting Network Attacks	3.5 Detecting Network Attacks	1
3.1.4 Designing Tomorrow's Secure Network Today Project Workday 4	Application	1
3.22 Unit 3 Vocabulary Quiz		1
3.23 Unit 3 Test		1
Designing Tomorrow's Secure Network Today Project Presentations		1

Unit 4: Devices

In Unit 4, students examine how computing devices, smart devices, and IoT systems store, process, and transmit digital data and how adversaries target these devices to gain unauthorized access. Students learn how authentication systems verify users and how attackers attempt to impersonate legitimate users through password attacks and other techniques. The unit also explores malware, device vulnerabilities, software updates, anti-malware protections, and secure device configurations used to defend systems. Through log analysis and threat detection activities, students identify indicators of compromise (IoCs) and investigate potential device-level attacks.

Course Skills addressed:

- 1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.
- 1.D Document, with and without the support of AI, the likelihood and impact of risks.
- 2.A Identify security controls and explain how they mitigate risks.
- 2.B Determine layered security controls that address vulnerabilities.
- 2.C Evaluate, with and without the support of AI, the impact of protective risk-management strategies.
- 2.D Implement and log mitigations with and without the support of AI.
- 3.B Determine strategies and methods to detect attacks.

Unit 4 Schedule (24 Days)

Assignment	AP Topic	# of Class Periods
4.1.1 A Cybersecurity Plan for a Small Business Project Launch	Application	1
4.2 Identifying Malware Types	4.1 Device Vulnerabilities and Attacks	1
4.3 Keylogger Lab	Reinforcement	1
4.4 Device Vulnerabilities	4.1 Device Vulnerabilities and Attacks	1
4.5 Device Risk Assessment	4.1 Device Vulnerabilities and Attacks	1
4.1.2 A Cybersecurity Plan for a Small Business Project Workday 2	Application	1
4.6 Password Hashing	4.2 Authentication	1
4.7 Password Vulnerabilities	4.2 Authentication	1
4.8 Password Cracking Lab	Reinforcement	1
4.9 Authentication Factors	4.2 Authentication	1
4.10 Securing Device Login Settings	4.2 Authentication	1

Assignment	AP Topic	# of Class Periods
	Scenario 4B Configuring Authentication Settings	
4.11 Device Managerial Controls	4.3 Protecting Devices	1
4.12 Anti-Malware Protection	4.3 Protecting Devices	1
4.13 Configuring a Host-Based Firewall	4.3 Protecting Devices	1
4.1.3 A Cybersecurity Plan for a Small Business Project Workday 3	Application	1
4.14 Detecting Device Attacks	4.4 Detecting Attacks on Devices	1
4.15 Device Detection Methods	4.4 Detecting Attacks on Devices	1
4.1.4 A Cybersecurity Plan for a Small Business Project Workday 4	Application	1
4.16 Device Security Case Study: Smart Farm Equipment	Application Scenario 4A Designing Secure Connected Farm Equipment	1
4.17 Authentication Log Analysis	4.4 Detecting Attacks on Devices Scenario 4C Analyzing Log Files for Indicators of Compromise	1
4.1.5 A Cybersecurity Plan for a Small Business Project Workday 5	Application	1
4.18 Unit 4 Vocabulary Quiz		1
4.19 Unit 4 Test		1
A Cybersecurity Plan for a Small Business Project Presentations		1

Unit 5: Securing Applications and Data

In Unit 5, students explore how applications and digital data are protected and why data is often the primary target of cyberattacks. Students examine common attacks against applications and data, along with methods adversaries use to steal, alter, or disrupt access to information. The unit introduces access control concepts used to manage permissions and limit data access, as well as cryptography techniques that protect the confidentiality and integrity of data both in storage and during transmission. Students also investigate secure application practices, analyze logs for evidence of attacks, and evaluate mitigations that help prevent, detect, and respond to threats against applications and data.

Course Skills addressed:

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

Unit 5 Schedule (27 Days)

Assignment	AP Topic	# of Class Periods
5.1.1 Designing the Future of Secure Communication Project Launch	Application	1
5.2 Application Vulnerabilities	5.1 Application and Data Vulnerabilities and Attacks	1
5.3 Application Attacks	5.1 Application and Data Vulnerabilities and Attacks	1
5.4 SQL Injection Lab	Reinforcement	1
5.5 Buffer Overflow Lab	Reinforcement	1
5.6 Application Risk Assessment	5.1 Application and Data Vulnerabilities and Attacks	1
5.7 Data Classification and Protection	5.2 Protecting Applications and Data: Managerial Controls and Access Controls	1

Assignment	AP Topic	# of Class Periods
5.8 Application and Data Managerial Controls	5.2 Protecting Applications and Data: Managerial Controls and Access Controls	1
5.9 Access Control Models	5.2 Protecting Applications and Data: Managerial Controls and Access Controls	1
5.10 Configuring Access Controls in Linux	5.2 Protecting Applications and Data: Managerial Controls and Access Controls Scenario 5A. Protecting Sensitive Data	1
5.11 Cryptography Fundamentals	5.3 Protecting Stored Data with Cryptography	1
5.12 Symmetric Encryption	5.3 Protecting Stored Data with Cryptography	1
5.13 Asymmetric Encryption	5.4 Asymmetric Cryptography	1
5.14 Asymmetric Encryption Algorithms	5.4 Asymmetric Cryptography	1
5.15 Public Key Encryption Lab	Reinforcement - Scenario 5B: Sending Encrypted Messages	1
5.1.2 Designing the Future of Secure Communication Project Workday 2	Application	1
5.16 Secure Application Design	5.5 Protecting Applications	1
5.17 Protecting Applications	5.5 Protecting Applications	1
5.18 Detecting Data Attacks	5.6 Detecting Attacks on Data and Applications	1
5.19 Application and Data Detection Methods	5.6 Detecting Attacks on Data and Applications	1
5.1.3 Designing the Future of Secure Communication Project Workday 3	Application	1
5.20 File Integrity and Hash Verification	5.6 Detecting Attacks on Data and Applications	1
5.21 Analyzing Logs for Application Attacks	5.6 Detecting Attacks on Data and Applications	1
5.1.4 Designing the Future of Secure Communication Project Workday 4	Application	1
5.22 Unit 5 Vocabulary Quiz		1
5.23 Unit 5 Test		1
Designing the Future of Secure Communication Project Presentations		1

Pedagogical Approaches

The UTeach AP Cybersecurity curriculum uses project-based learning (PBL) and other research-backed methods to engage all students. PBL fosters critical thinking and problem-solving skills through real-world challenges. The curriculum emphasizes cultural context, teacher facilitation, and mediated instruction. Teachers unfamiliar with PBL can learn more at the Buck Institute for Education website.

Educators are encouraged to use various PBL strategies, including narrative anchoring videos, unit projects, clear rubrics, regular benchmarks, scaffolding activities, final products, and reflection. These tools enhance engagement and help increase comprehension and retention, problem-solving abilities, critical thinking, and group communication skills.

Instructional Sequencing

The yearlong curriculum consists of five instructional units carefully structured to introduce students to foundational cybersecurity concepts and practices through hands-on lessons focused on topics such as cyber threats and attacks, physical and network security, device and application security, authentication, cryptography, risk assessment, threat detection, and data protection. Students connect classroom learning to real-world application with unit projects, easy-to-understand videos, collaborative research activities, and hands-on labs.

Introduction

The first assignment of each instructional unit opens with an anchor video designed to introduce the driving questions, unit project, and key topics for the next few weeks of study. Students are expected to participate in small-group and/or whole-class discussion to identify areas of focus that will direct and drive learning throughout the unit.

Topic Lessons/Activities

Distributed throughout each unit, individual lessons, daily activities, research assignments, and discussions allow students to explore and practice applying relevant skills and concepts in greater detail.

Project Workdays

Each unit project has between four and five dedicated work periods for students to work on their deliverables. Project workdays are spread throughout the unit, strategically placed after relevant topics have been presented.

Assessments

In addition to informal formative assessments throughout each unit, student learning and progress is also assessed at the end of each unit through a formal summative assessment and evaluation of their independent and collaborative efforts on the unit project. Formal end-of-unit assessments are comprised of multiple-choice questions and free response questions.

Unit Projects

The narrative-driven curriculum immerses students in encounters with cunning adversaries who have intercepted the course with their own agenda. These adversaries challenge students to adopt an adversarial mindset, presenting real-world scenarios and dilemmas that test their skills and ethical boundaries. The students' mission is to resist their temptations, use their growing cybersecurity knowledge to counteract their tactics, and understand the importance of maintaining integrity in the face of cyber threats.

The opening module of each unit serves as a formal launch of the unit project—a product-oriented challenge for students to investigate, research, and solve over the course of the unit. The project launch starts with an anchor video that introduces the fundamental problem or challenge to be solved and is intended to spark the students' imaginations and inspire them to find a solution. Projects are designed to be collaborative, with students working together in groups.

Rubrics

Each unit project is accompanied by a clearly defined rubric that specifies the set of expectations for work throughout the unit, including an exhaustive list of assessment criteria for the artifacts that students will produce and detailed descriptors for each performance level that a student might demonstrate. Teachers should provide students with the rubric at the start of the unit as part of the initial discussion immediately following the anchor video. Giving the students the rubric at the time of the project launch is critical for setting clear expectations early in the research and learning process. Over the course of the unit, teachers should regularly refer to the goals and criteria of the rubric to ensure that students remain focused and on track to meet the stated requirements.

Benchmarks

Each unit provides the teacher with several benchmark activities, or subtasks, that feed into the larger unit project. Each of these subtasks contributes directly to the final product that the students create. Teachers can use these benchmarks as intermediate informal assessments to gauge the progress of each student and/or collaborative group in their mastery of the unit goals.

Scaffolding Activities

The bulk of each unit consists of a series of individual topic lessons, activities, discussions, and hands-on applications that allow the teacher to provide instruction, guidance, and support to students and collaborative groups as they design and implement the deliverables for the unit project. These scaffolding activities serve to introduce, explain, and encourage the use of the unit's core concepts and skills by providing students with structured opportunities and incentives to explore the material in greater depth.

Final Products and Student Portfolio

At the culmination of each unit, student groups are expected to present a final product that represents the body of their work and implementation on the unit project. Students demonstrate their mastery of the core content and skills for the unit by exhibiting the authentic and purposeful artifacts and completing a reflection piece. A key component of the project always includes a public presentation of each student's work before their peers as a way of providing motivation for each student and holding them accountable for their own learning.

Reflection

Students are provided time to reflect at the end of project workdays with thoughtful responses to specific questions about the topics covered in the unit project. This provides students an opportunity to reflect on the challenges and successes during the unit project.