AP Cybersecurity Syllabus

High School - One Year (130 hours)

Course Overview and Goals

AP Cybersecurity trains students in the field and aligns closely with standard first-year collegiate cybersecurity courses. Students explore defense-in-depth strategies and learn to address specific vulnerabilities, attacks, mitigations, and detection measures across a variety of domains, including physical spaces, computer networks, devices, applications, and data.

The CodeHS AP Cybersecurity course is a year-long course designed to help students master the basics of cybersecurity and equip them to successfully pass the College Board AP Cybersecurity Exam at the end of the school year. All learning materials and resources teachers and students need for a successful year-long AP Cybersecurity course can be found on the CodeHS website at codehs.com/course/27705/overview.

Course Background and Resources

Prerequisites

There are no specific course prerequisites for AP Cybersecurity. Students should be motivated and willing to work both individually and in teams on college-level projects. AP Cybersecurity is designed to serve as a foundational course that aligns with multiple programs of study within Career and Technical Education (CTE) Digital Technology Pathways.

This course is meant to be a first-time introduction to cybersecurity and does not require students to come in with any prior experience. However, we recommend that students take our Fundamentals of Cybersecurity course prior to this AP course (more info at codehs.com/course/21597/overview). Students who have completed our Fundamentals of Cybersecurity course will be able to apply knowledge of concepts covered in the introductory course to the more advanced setting of the AP courses.

Learning Environment

The course utilizes a blended classroom approach. The content is fully web-based, with students completing all activities in the browser. Teachers utilize tools and resources

provided by CodeHS to leverage time in the classroom and give focused 1-on-1 attention to students. Each unit of the course is broken down into lessons. Lessons consist of video tutorials, short quizzes, interactive simulations to explore, and written exercises, adding up to 120 hours of hands-on practice in total.

Technology Requirements

You can find the basic technology requirements for using the CodeHS platform in the Technical Set-Up Guide.

AP Alignment

The CodeHS AP Cybersecurity course aligns directly with the College Board AP Course and Exam Description (CED), with the CodeHS units and lessons following the order of the units and topics outlined in the CED. Each lesson in the course corresponds to a specific topic, and the lesson activities are designed to address the topic's Learning Objectives (LOs) and Essential Knowledge (EK) statements. By watching instructional videos, reading articles and notes pages, exploring examples, and completing simulation exercises throughout the lessons, students develop a strong understanding of all of the knowledge and skills outlined in the CED.

Detailed descriptions of each unit and its contents are provided in the Course Breakdown section of the syllabus.

AP Classroom and Assessment

Formative assessments are integrated throughout the CodeHS AP Cybersecurity course to monitor student progress, provide timely feedback, and guide instruction to ensure mastery of key concepts and skills. Each lesson includes multiple opportunities to gauge student understanding, such as multiple-choice quizzes and free-response questions.

In addition to the formative assessments within the course, teachers can also use the resources within AP Classroom (myap.collegeboard.org) to assess student understanding. It offers tools like progress checks, topic questions, and practice exams that align closely with the AP Exam content and structure.

The CodeHS Cybersecurity course maps 1:1 with the structure of AP Classroom, ensuring that you can seamlessly integrate resources from both platforms. For each lesson, there are corresponding resources available in AP Classroom, such as topic questions that reinforce specific concepts. For example, after completing the CodeHS lesson The Tricks

Behind Every Scam (Understanding Social Engineering), you can assign the topic questions for the Understanding Social Engineering topic in AP Classroom as formative assessments. These questions not only provide students with targeted practice and related AP Exam-style problems but also allow teachers to identify gaps in student understanding. Teachers can use the results of these assessments to inform their instruction by revisiting and reviewing concepts as needed to ensure students have a solid grasp of the material before moving forward.

When to Use AP Classroom

- **Topic Questions**: Assign topic questions after every lesson to provide formative assessments that target specific skills. These questions align with the material in each CodeHS lesson and give students additional practice with AP-style questions. Teachers can use the results of these assessments to identify gaps in student understanding and revisit or review concepts as needed, ensuring students build a strong foundation before progressing.
- **Progress Checks**: Use progress checks as more comprehensive formative assessments during mid-unit or end-of-unit reviews. These checks are designed to gauge students' understanding of broader topics and provide actionable insights for teachers. By analyzing the results, teachers can identify areas where further review might be needed and address gaps in understanding before moving on to practice exams or more summative assessments.
- **Practice Exams**: As the AP Exam approaches, utilize the full-length practice exams that are available on AP Classroom. These exams familiarize students with the test format, timing, and content, serving as valuable summative assessments that prepare them for exam day.

CodeHS Cyber Range

The CodeHS Cyber Range is an interactive, browser-based lab environment where students solve real cybersecurity challenges, run Linux commands, and practice skills in a safe virtual setting. These activities are supplemental and not required to meet College Board standards. They are designed to add real-world context and hands-on engagement to course concepts. You can find additional information at codehs.com/cyber-range.

Course Breakdown

Unit 1: Introduction to Security (3 weeks or 15 hours)

In this unit, students experience three distinct examples of how adversaries try to compromise systems: Students explore how adversaries use social engineering to influence the behavior of targets and the impacts of targets clicking on malicious links or downloading malicious files. Students see how adversaries compromise systems through weak authentication, and they learn how to strengthen authentication to protect themselves. Students learn about the hazards of public Wi-Fi, including how adversaries use it to attack victims, as well as how to protect themselves.

Building Cybersecurity Skills

In this first unit, students begin to explain how vulnerabilities in systems give rise to risk and learn to identify potential avenues of attack. Students learn how to identify ways they can protect themselves from potential cyberattacks by mitigating risks. Students also learn how to detect cyberattacks by analyzing log files and identifying signs of suspicious activity—often called indicators of compromise (IoCs).

Topics Covered	• Welcome to Cybersecurity • Understanding Social Engineering • Suspicious Website Logins • Best Practices for Public Networks • AI-Based Cybersecurity Attacks • Leveraging AI in Cyber Defense • End of Unit Assessment
Sample Projects, Activities & Assignments	• **Investigating Network Logs:** Students analyze real network log data to identify signs of a password attack in progress. By examining login patterns, timestamps, and failed authentication attempts, students practice the evidence-based detection skills used by security professionals to identify threats before damage occurs. (Skill 1.A) • **Gandalf Challenge:** Students interact directly with an AI tool and attempt to manipulate it into revealing protected information using prompt injection techniques. After completing the challenge, students reflect on what their experience reveals about the vulnerabilities of large language models and why LLM security is a growing concern in cybersecurity. (Skill 1.B) • **Complete Your Story:** Students use a randomized story-starter

	framework to write an original fictional cyberattack narrative, incorporating real adversary classifications and wireless attack methods covered in the unit. The activity requires students to apply technical concepts in context, demonstrating understanding of how attacks are planned and executed from an adversary's perspective. (Skill 1.A) • **Human-in-the-Loop:** Students review AI-generated security recommendations across a set of realistic scenarios and evaluate whether each recommendation is safe to implement as written or requires human expert review before action is taken. Students document their reasoning and submit a completed analysis explaining the appropriate role of human oversight in AI-assisted cybersecurity defense. (Skill 2.A)
Summative Assessments	• End of Unit Assessment (Lessons 1.1-1.9)

Unit 2: Securing Spaces (4 weeks or 20 hours)

In this unit, students focus on securing a physical location. Adversaries that can gain physical access to a device are often able to bypass many of the technical controls that protect the device and the data on it. Thus, securing the physical space is a critical first layer of defense and a concrete way for students to develop adversarial thinking skills and begin to identify vulnerabilities, threats, attacks, and mitigations. Students consider how physical spaces might be breached by adversaries, how to detect physical breaches, how to select devices to prevent or deter an adversary, and how to place those devices to maximize their usefulness.

Building Cybersecurity Skills

This unit focuses on an aspect of security that is concrete and is present in students' everyday lives. By leveraging the fact that students move through different spaces (e.g., their home, the school building, a bank) that are secured in a variety of ways, teachers can connect the concepts of vulnerabilities, threats, and risk to students' experiences. Students begin assessing and managing risk in this familiar domain while they practice selecting security controls based on the principles from Unit 1. Finally, students consider how to select controls to detect physical breaches and evaluate the impact of those controls.

Topics Covered	• Cyber Foundations • Physical Vulnerabilities and Attacks

	• Protecting Physical Spaces • Detecting Physical Spaces • End of Unit Assessment
Sample Projects, Activities & Assignments	• **Create a Phishing Email:** Students draft an original phishing email using at least four social engineering tactics covered in the lesson, annotating each tactic with an explanation of the psychological manipulation it employs. Students then reflect on which tactics they found most effective and why. (Skill 1.A) • **Capstone: Coffee Shop Consultant:** Students act as security consultants for a local coffee shop chain that has experienced two real-world security incidents involving password reuse and a suspected payment system compromise. Working through a four-part project, students conduct a full risk assessment, select risk management strategies, recommend and classify security controls by type and function, and build a layered defense-in-depth security plan that addresses the business's specific vulnerabilities. (Skill 1.A)(Skill 2.A)(Skill 2.B) • **Secure the Building:** Students act as security consultants for a regional bank branch, designing a complete physical detection strategy using a constrained set of controls including cameras, motion sensors, and security guards. Students determine optimal placement for each control based on traffic patterns and coverage gaps, train employees on suspicious activity protocols across five realistic scenarios, and write out full detection-to-response sequences for three security incidents including an after-hours badge anomaly and an unscheduled loading dock intrusion. (Skill 3.A)(Skill 3.B)
Summative Assessments	• End of Unit Assessment (Lessons 2.1-2.17)

Unit 3: Securing Networks (5 weeks or 25 hours)

Most digital devices are connected to other devices through a computer network. The transmission of data between devices creates new opportunities for adversaries, so defenders must think carefully about how networks are designed and how data is protected while in transit. In this unit, students learn about common network attacks and how to protect against them. Students study the benefits of network segmentation and learn how to place and configure firewalls to manage network traffic. They also learn how to analyze network log files to find possible indicators of compromise (IoCs).

Building Cybersecurity Skills

In this unit, students learn to apply their risk assessment skills in the domain of networking, identifying vulnerabilities and evaluating the likelihood and impact of a vulnerability being exploited to determine the risk. Students learn how to apply security controls to a network to help prevent and deter adversaries, and how to collect and analyze network data to detect attacks. Students also learn how automated tools, including AI, enable faster, more efficient detection of malicious activity on networks.

Topics Covered	• Network Vulnerabilities and Attacks • Protecting Networks: Managerial Controls and Wireless Security • Protecting Networks: Segmentation • Protecting Networks: Firewalls • End of Unit Assessment
Sample Projects, Activities & Assignments	• **What's Happening on the Network?:** Students analyze four network attack scenarios described by school IT staff and administrators, identifying the specific attack type in each case, including MAC flooding, DNS poisoning, ARP poisoning, and a smurf attack, based on observable symptoms reported. Students explain how each attack affects confidentiality, integrity, and availability to demonstrate understanding of how network attacks generate risk. (Skill 1.C) • **Locking Down the Airwaves:** Students work through a queue of flagged wireless access point tickets as a security technician, diagnosing the misconfiguration in each scenario and applying the correct fix using an interactive settings panel. Across three tickets, students disable beacon frame broadcasting on a restricted server room WAP, adjust signal strength to prevent the network from extending beyond physical boundaries, and configure wireless encryption. Students read an explanation of each fix before moving to the next scenario. (Skill 2.D) • **Create a Subnet Network:** Students design a segmented network for a high school by dividing a single assigned network address into five subnets sized for each department, calculating usable IP addresses, avoiding address overlaps, and producing a network diagram. Students then select one department and explain in writing how subnetting contains the damage if a device on that subnet is compromised, demonstrating understanding of segmentation as a security control. (Skill 2.A)

Summative Assessments	• End of Unit Assessment (Lessons 3.1-3.18)

Unit 4: Securing Devices (5 weeks or 25 hours)

Computer devices store, process, and transmit all the digital data in the world. Devices include computer systems and laptops, smartphones and tablets, and a range of items that have microcomputers installed in them, like washing machines and coffee makers—these are often called smart devices or IoT (Internet of Things) devices. In this unit, students learn about how systems authenticate users of devices and how adversaries attempt to impersonate legitimate users. Students come to understand how adversaries use malware to compromise devices and the importance of keeping devices updated and of using anti-malware software. Students also learn how to analyze log files for indicators of compromise (IoCs).

Building Cybersecurity Skills

As more everyday items incorporate embedded computers, device vulnerabilities and attacks are growing rapidly. In this unit, students learn to assess risk based on these new vulnerabilities. They learn how devices can be protected as another part of a defense-in-depth security strategy. Students also practice detecting attacks against devices by reviewing authentication logs for IoCs.

Topics Covered	• Device Vulnerabilities and Attacks • Authentication • Protecting Devices • Detecting Attacks on Devices • End of Unit Assessment
Sample Projects, Activities & Assignments	• **Open Doors:** Students explore how adversaries exploit three compounding device vulnerabilities including open ports, misconfigured firewalls, and missing anti-malware through an interactive notes activity that includes a live port scan simulation and firewall rule comparison. Students analyze how each vulnerability creates an attack surface, examine how a misconfigured firewall rule can expose a device despite appearing protected, and trace how all three vulnerabilities chain together to give an adversary a clear path from the network to full device control. (Skill 1.C) • **Capstone: The Riverside High Security Breach:** Students take on the role of a junior security analyst investigating a real

	breach at a high school where 1,400 student records were stolen after an adversary successfully guessed an administrator's password using an automated tool. Working through a four-part analysis, students explain why plaintext password storage made the breach catastrophic, identify the attack type from actual login logs showing 4,852 failed attempts in under 17 minutes, evaluate the portal's single-factor authentication setup and recommend an improvement, and determine which two controls working together would have had the greatest impact on preventing the breach. (Skill 2.A)(Skill 2.B) ● **Why Device Updates Matter:** Students work through a 30-day scenario as the IT lead at a regional hospital, making real patch management decisions across three critical moments: a critical security patch arriving alongside lower-priority updates on Day 0, a public exploit disclosure on Day 7 while the patch sits undeployed, and a zero-day vulnerability with no vendor patch available on Day 21. Students use an interactive exposure window simulator to visualize how patch timing directly impacts risk, and determine what layered defenses to implement when a patch does not yet exist. (Skill 2.C)(Skill 2.D) ● **Guided Auth Log Analysis:** Students analyze a 70-minute authentication log from a credit union's security system containing three embedded attack patterns hidden within normal traffic. Working through a guided four-step process, students identify a brute force attack targeting a single account with 10 rapid attempts resulting in lockout, a password spraying attack hitting nine different accounts from the same IP within four seconds, and a credential stuffing attack testing default username and password pairs. Students explain what specific log evidence distinguishes each attack type from the others and describe how an analyst would respond to the findings. (Skill 3.D)
Summative Assessments	● End of Unit Assessment (Lessons 4.1-4.16)

Unit 5: Securing Applications and Data (6 weeks or 30 hours)

Most digital devices are connected to other devices through a computer network. The transmission of data between devices creates new opportunities for adversaries, so defenders must think carefully about how networks are designed and how data is protected while in transit. In this unit, students learn about common network attacks and how to protect against them. Students study the benefits of network segmentation and learn how to place and configure firewalls to manage network traffic. They also learn how to analyze network log files to find possible indicators of compromise (IoCs).

Building Cybersecurity Skills

In this unit, students learn to apply their risk assessment skills in the domain of networking, identifying vulnerabilities and evaluating the likelihood and impact of a vulnerability being exploited to determine the risk. Students learn how to apply security controls to a network to help prevent and deter adversaries, and how to collect and analyze network data to detect attacks. Students also learn how automated tools, including AI, enable faster, more efficient detection of malicious activity on networks.

Topics Covered	• Application and Data Vulnerabilities and Attacks • Protecting Applications and Data: Managerial Controls and Access Controls • Protecting Stored Data with Cryptography • Asymmetric Cryptography • Protecting Applications • Detecting Attacks on Data and Applications • End of Unit Assessment
Sample Projects, Activities & Assignments	• **Access Control Simulator**: Students work through three hospital access control scenarios in an interactive simulator, adjusting permission settings for staff accounts to apply the principle of least privilege. In the first scenario, a stolen laptop exposes admin-level access a nurse never needed; in the second, a receptionist's one-time admin access to system configuration was never revoked after a temporary task; in the third, both a nurse and receptionist have write access to billing records their roles don't require. Students adjust permissions, receive targeted feedback, and see in real time how each change reduces adversary reach if an account is compromised. (Skill 1.C) • **Capstone: Defending a Real System:** Students act as security consultants reviewing the launch plan for a telehealth startup that collects four categories of sensitive patient and billing

	data. Working through a three-part capstone, students classify each data type under the applicable legal framework including HIPAA, PCI-DSS, and the Privacy Act, recommend and justify an appropriate access control model for the organization, identify two gaps in a draft cryptography policy and explain the risk each gap creates, and write chmod commands to fix misconfigured file permissions on a shared server using both numeric and symbolic notation**.** (Skill 2.C)(Skill 2.D) ● **RSA Encryption Tool**: Students use a browser-based RSA simulation to generate a public and private key pair, encrypt a patient insurance record using the public key, and attempt to decrypt the ciphertext with both keys to observe that only the private key succeeds. Students then complete a simulated secure email workflow by loading a message, encrypting it, copying the ciphertext into an email to the billing team, and decrypting it as the recipient. Three reflection questions guide students to explain why no shared secret is needed in advance and what happens if the private key is stolen. (Skills 2.B)(Skill 2.D) ● **Hash It Out**: Students work through a three-step interactive simulation as an IT administrator at a county elections office, using SHA256 hash commands in PowerShell, bash, or zsh to verify file integrity. Students run a hash on an unchanged file and confirm it matches the stored digest, predict whether a single-character overnight alteration will change the digest before running the command, and compare two nearly identical note files differing by one word to observe that their digests share almost nothing. The activity demonstrates how hash-based detection catches tampering that would otherwise be invisible. (Skill 3.B)(Skill 3.D)
Summative Assessments	● End of Unit Assessment (Lessons 5.1-5.26)

Exam Review (2-3 weeks or 10-15 hours)

Students prepare for the AP Exam by practicing multiple-choice and free-response questions. Students should assess areas or topics that they need to practice.

Topics Covered

- Students know what to expect on the AP Exam
- Practice solving AP Exam type multiple choice questions
- Practice solving AP Exam type free response questions