AP® Cybersecurity Syllabus

Last Updated: May 2026

Teacher Profile

Teacher Name:
School Name:
School Website:
Contact Information:

Course Overview

AP Cybersecurity provides a broad introduction to cybersecurity, emphasizing how threats and vulnerabilities create risk, and how individuals and organizations manage and mitigate risk using a defense-in-depth approach across physical spaces, networks, devices, applications, and data. Students repeatedly evaluate how layered security controls work together to reduce vulnerabilities, strengthen resilience, and improve organizational security posture.

Students learn to think and work like an analyst: interpreting realistic scenarios, evaluating artifacts/evidence (e.g., network diagrams, logs, packet captures), and making evidence-based, context-aware security recommendations.

Students develop professional cybersecurity practices including technical communication, collaborative problem solving, incident documentation, evidence-based reasoning, and ethical decision-making.

Core Course Skills

College Board organizes the course around three repeated skill categories:

1. **Analyze Risk**
2. **Mitigate Risk**
3. **Detect Attacks**
4. **Collaborate**

Students will continuously practice:

- Identifying vulnerabilities, threats, and attack methods (including with/without AI support where appropriate)
- Selecting layered security controls that mitigate risk
- Detecting and interpreting indicators of compromise using realistic artifacts/evidence

Legal, ethical, and professional norms (required)

Because cybersecurity involves sensitive data and elevated access, students will operate under professional norms and legal expectations. Instruction will explicitly address ethical conduct and laws/regulations impacting data, systems, and privacy.

Class safety rule (non-negotiable):
All security testing, scanning, and investigation must occur only in approved classroom labs/simulations and only against systems the student has explicit permission to access.

Academic integrity and AI use

- Students may use AI tools only when explicitly permitted and must cite their use (tool name + what it contributed).
- Any AI output must be verified with course concepts and supporting evidence from provided artifacts.

- Unauthorized access, scanning, exploitation, or testing outside approved labs is prohibited.

Teaching Strategies

The AP Cybersecurity course is taught using a student-centered instructional model that emphasizes conceptual understanding, active engagement, collaboration, and real-world application of cybersecurity principles. Lessons begin with structured direct instruction that introduces core concepts through guided questioning, visual models, demonstrations, and analysis of authentic cybersecurity scenarios. Students regularly engage in collaborative discussions, problem-solving activities, simulations, and formative assessments designed to uncover misconceptions and encourage critical thinking before formal solutions are presented. Instruction scaffolds complex topics such as network security, cryptography, threat analysis, and ethical computing through incremental learning experiences that connect technical knowledge to practical applications and career pathways.

Throughout the course, students participate in hands-on investigations, labs, coding activities, case studies, and scenario-based challenges that mirror industry practices and workplace expectations. Frequent formative assessments, peer collaboration, reflection activities, and data-driven instructional adjustments are used to support student growth and mastery. Emphasis is placed on communication, computational thinking, digital ethics, and analytical reasoning while students explore contemporary cybersecurity threats, defensive strategies, and emerging technologies. The course also integrates career readiness practices by promoting teamwork, technical documentation, troubleshooting, professional communication, and problem-solving skills aligned with modern cybersecurity and technology fields.

Materials & tools

Required

- School-managed device or laptop capable of running a browser and classroom tools
- Headphones (for video labs/demos)
- Notebook (digital or paper)

Recommended lab environment (teacher provided/approved)

- A **Linux environment/range** (VM or cloud sandbox) for file permissions, access control, and command-line work (supports Unit 5 access controls and cryptography workflows).
- Packet capture/log viewing tools (teacher-approved) aligned to exam-style artifacts (e.g., logs, directories, packet captures).

Course Assessments

The teacher will have formative assessments to ensure students understand the material that has been taught. They are divided into two categories. The first category is ungraded and consists of student participation, student responses to questions, observed student--student interactions and unit scenarios. Questions are incorporated within each daily lesson, and students use a response device to submit answers anonymously. These results are used to spark discussion and debate between students in a social constructivist environment. These questions also provide teachers and students instant feedback to gauge the pace of instruction and the need for reteaching.

Throughout the course, students progressively analyze increasingly complex and authentic cybersecurity artifacts including authentication logs, firewall rules, network diagrams, packet captures, access records, vulnerability reports, and incident evidence aligned to AP-style free-response expectations.

The second category is graded where students will demonstrate learning through:

- **Scenario-based performance tasks** (each unit) mirroring the course's real-world scenarios and job-role framing
- **AP-style multiple-choice** sets tied to realistic job scenarios
- **AP-style free-response** practice analyzing cybersecurity artifacts (e.g., logs, diagrams, directories, packet captures)
- Short written recommendations ("security memos") using claim-evidence-reasoning

These are all given in the same form as the AP exam: 70% multiple choice, 30% free response which includes error analysis and scenario-based questions. The multiple-choice questions are conceptual while the free response section involves solving multi-step problems or providing extended thinking answers; often similar to questions from prior AP exams.

Students complete a cumulative cybersecurity investigation requiring analysis of multiple artifacts, identification of vulnerabilities and attack methods, evaluation of risk, and development of layered mitigation recommendations.

Texts and Supplemental Materials

This syllabus corresponds to a digital curriculum: The New Jersey Center for Teaching and Learning (NJCTL) Progressive Science Initiative® (PSI®): AP Cybersecurity. Course resources including Presentations, Problem Sets, Quizzes, Tests, and Unit Plans can be accessed at https://njctl.org/materials/courses/ap-cybersecurity/.

NOTE: The course materials located on the NJCTL website are accepted as equivalent to a college textbook for many other AP courses.

Course Outline and Pacing

Unit 1: Introduction to Security *(25 days)*

Topics	Resources, Labs, & Assessments
● 1.1 What is Cybersecurity? ● 1.2 Understanding Social Engineering - Phishing & Other Social Engineering Attacks - Consequences of Phishing & Protection ● 1.3 Suspicious Wi-Fi Login - Mitigating & Detecting Account Compromise ● 1.4 Best Practices for Public Wi-Fi - Mitigating & Detecting Network Compromise ● 1.5 AI-Based Cybersecurity Attacks - Mitigating & Detecting AI Attacks ● 1.6 Leveraging AI in Cybersecurity - AI in Detection Systems	**Resources:** ● AP Classroom ● Materials can be found on NJCTL website at Unit 1 **Activities/Labs:** ● Weekly AP Classroom practice: short scenario MCQ and artifact analysis mini-FRQ ● Phishing and Account Compromise Investigation - evidence-based risk analysis and mitigation plan ● Students work collaboratively in teams to analyze cybersecurity evidence, evaluate mitigation strategies, and communicate evidence-based recommendations. **Assessments:** ● Formative Assessments ● Quizzes

	• Unit Scenario-based Activities • Unit Test
Unit Skills & Scenarios	
Learning Objectives: 1.1 A – C, 1.2 A – C, 1.3 A – C, 1.4 A – B, 1.5 A – B Scenarios: • **Phishing Investigation & Risk Analysis Activity** Students analyze simulated phishing emails to identify indicators of social engineering, evaluate attacker tactics, determine potential risks, and develop mitigation recommendations. This activity aligns to Analyze Risk skills 1.A–1.D and Detect Attacks skill 3.D. • **Suspicious Login Log Analysis Lab** Students examine authentication and login records to identify indicators of unauthorized access, recognize suspicious login behavior, and recommend stronger authentication controls. This activity aligns to learning objectives 1.2.A–1.2.C and skills 1.B, 2.A, and 3.D. • **Public Wi-Fi & Rogue Access Point Scenario Investigation** Students evaluate a simulated public Wi-Fi compromise scenario, identify vulnerabilities associated with rogue wireless networks, and create a layered security response plan to protect user accounts and sensitive information. This activity aligns to learning objectives 1.3.A–1.3.C and skills 2.B and 3.B.	

Unit 2: Securing Spaces *(30 days)*

Topics	**Resources, Labs, & Assessments**
• 2.1 Cyber Foundations • 2.2 Risk Assessment & Management • 2.3 Security Controls • 2.4 Physical Vulnerabilities and Attacks • 2.5 Protecting Physical Spaces • 2.6 Detecting Physical Attacks	**Resources:** • AP Classroom • Materials can be found on NJCTL website at Unit 2 **Activities/Labs:** • Weekly AP Classroom practice: short scenario MCQ and artifact analysis mini-FRQ • Physical Vulnerability Assessment -assesses layered controls and monitors placement recommendations. • Students work collaboratively in teams to analyze cybersecurity evidence, evaluate mitigation strategies, and communicate evidence-based recommendations. **Assessments:** • Formative Assessments • Quizzes • Unit Scenario-based Activities • Unit Test
Unit Skills & Scenarios	
Learning Objectives: 2.1 A – G, 2.2 A – C, 2.3 A – B, 2.4 A – C Scenarios:	

- **Facility Security Risk Assessment Activity**
  Students evaluate a simulated organization's building layout, assets, and vulnerabilities to identify physical security risks and recommend layered mitigation strategies. Students create a risk assessment report that prioritizes threats based on likelihood and impact. This activity aligns to Skills 1.C, 1.D, and 2.B.
- **Physical Security Controls Investigation Lab**
  Students analyze different physical and administrative security controls including badge access systems, surveillance cameras, barriers, and visitor policies. Students determine which controls best mitigate specific vulnerabilities and justify their recommendations using defense-in-depth principles. This activity aligns to Skills 2.A–2.C.
- **Physical Intrusion Detection Scenario Analysis**
  Students review surveillance footage descriptions, access logs, and incident reports to identify indicators of unauthorized access and determine how an attack occurred. Students classify the attack method and propose improved detection and response procedures. This activity aligns to Skills 3.A–3.D and collaborative problem-solving objectives.
- **Unauthorized Building Access Investigation**
  Students investigate how an adversary gained physical access to a restricted facility area through tailgating and poor badge verification procedures. Students analyze surveillance descriptions, visitor logs, and employee reports to identify vulnerabilities and recommend layered physical security improvements.

Unit 3: Securing Networks *(50 days)*

Topics	Resources, Labs, & Assessments
• 3.1 ARP Poisoning & Man-in-the-Middle Attacks • 3.2 Other Network Attacks • 3.3 Network Vulnerabilities and Attacks • 3.4 Protecting Networks: Managerial Controls and Wireless Security • 3.5 Protecting Networks: Segmentation • 3.6 Protecting Networks: Firewalls • 3.7 Detecting Network Attacks • 3.8 Choosing a Detection Method • 3.9 Detecting Attacks Using Log Files	**Resources:** • AP Classroom • Materials can be found on NJCTL website at Unit 3 **Activities/Labs:** • Weekly AP Classroom practice: short scenario MCQ and artifact analysis mini-FRQ • Secure Wireless/Network Design – students implement layered defense-in-depth network protections including wireless security controls, segmentation strategies, firewall rules, and detection methods while evaluating false positives and false negatives. • Students work collaboratively in teams to analyze cybersecurity evidence, evaluate mitigation strategies, and communicate evidence-based recommendations. **Assessments:** • Formative Assessments • Quizzes • Unit Scenario-based Activities • Unit Test

Unit Skills & Scenarios
Learning Objectives: 3.1 A – C, 3.2 A – B, 3.3 A – B, 3.4 A – D, 3.5 A – E Scenarios: ● **Network Traffic Investigation Lab** Students analyze simulated network traffic logs and packet activity to identify indicators of compromise (IoCs), malware communication, or unauthorized access attempts to classify network attacks. Students recommend mitigation strategies based on evidence collected during the investigation. This activity aligns to Skills 1.B, 3.B, and 3.D. ● **Wireless Security Configuration Activity** Students evaluate different wireless network configurations and determine which settings best protect against unauthorized access and wireless attacks. Students compare encryption methods, password policies, and authentication strategies while justifying recommendations using defense-in-depth principles. This activity aligns to Skills 2.A–2.C. ● **Firewall Rule Analysis & Network Segmentation Scenario** Students review a simulated organization's network diagram and firewall rule set to identify security weaknesses, unnecessary open ports, and segmentation issues. Students propose improved firewall configurations and defense-in-depth network segmentation strategies to reduce organizational risk and prevent lateral movement within the network. This activity aligns to Skills 1.C, 2.B, and 2.D. ● **Suspicious Network Traffic Analysis** Students analyze firewall logs, network diagrams, and unusual traffic patterns after a company experiences slow network performance and unauthorized outbound connections. Students identify indicators of compromise, classify the likely attack, and recommend segmentation and firewall improvements.

Unit 4: Securing Devices *(35 days)*

Topics	Resources, Labs, & Assessments
● 4.1 Types of Computing Devices & Malware ● 4.2 Device Vulnerabilities and Attacks ● 4.3 Password Security & Authentication ● 4.4 Protecting Devices with Defense-in-Depth Strategies ● 4.5 Detecting Attacks on Devices	**Resources:** ● AP Classroom ● Materials can be found on NJCTL website at Unit 4 **Activities/Labs:** ● Weekly AP Classroom practice: short scenario MCQ and artifact analysis mini-FRQ ● Device Threat Model - create authentication plan and detection strategy using device indicators ● Students work collaboratively in teams to analyze cybersecurity evidence, evaluate mitigation strategies, and communicate evidence-based recommendations. **Assessments:** ● Formative Assessments ● Quizzes ● Unit Scenario-based Activities

	• Unit Test

Unit Skills & Scenarios
Learning Objectives: 4.1 A – D, 4.2 A – D, 4.3 A – D, 4.4 A – D Scenarios: • **Endpoint Compromise Investigation Lab** Students investigate endpoint indicators of compromise including suspicious processes, unauthorized logins, and abnormal device behavior. Students determine how the compromise occurred and recommend remediation and prevention strategies. This activity aligns to Skills 1.B, 3.B, and 3.D. • **Authentication Security Evaluation Activity** Students evaluate different authentication methods and security policies to determine how organizations can reduce the risk of credential-based attacks. Students compare password-only authentication to multifactor authentication and analyze the strengths and limitations of various identity verification methods. This activity aligns to Skills 2.A–2.C. • **Device Hardening & Security Configuration Scenario** Students review a device configuration checklist for a simulated organization and identify weaknesses related to patching, permissions, software installation, and endpoint protection settings. Students create a layered defense-in-depth device security plan designed to reduce vulnerabilities and improve overall endpoint security posture. This activity aligns to Skills 1.C, 2.B, and 2.D. • **Compromised Employee Laptop Investigation** An employee reports unusual pop-ups, slow performance, and unauthorized password reset notifications on a company laptop. Students analyze endpoint logs, installed software, and user behavior to determine how the compromise occurred and recommend remediation steps and improved device protections.

Unit 5: Securing Applications and Data *(40 days)*

Topics	**Resources, Labs, & Assessments**
• 5.1 Application and Data Vulnerabilities and Attacks • 5.2 Data States, Classification, & Managerial Controls • 5.3 Access Control Models & Linux Permissions • 5.4 Protecting Stored Data with Cryptography • 5.5 Asymmetric Cryptography • 5.6 Protecting Applications • 5.7 Detecting Attacks on Data and Applications	**Resources:** • AP Classroom • Materials can be found on NJCTL website at Unit 5 **Activities/Labs:** • Weekly AP Classroom practice: short scenario MCQ and artifact analysis mini-FRQ • Secure sensitive data using defense-in-depth strategies including layered access controls, cryptographic protections, monitoring systems, and attack detection indicators. • Students work collaboratively in teams to analyze cybersecurity evidence, evaluate mitigation strategies, and communicate evidence-based recommendations. **Assessments:** • Formative Assessments • Quizzes

	● Unit Scenario-based Activities ● Unit Test

Unit Skills & Scenarios

Learning Objectives: 5.1 A – C, 5.2 A – D, 5.3 A – B, 5.4 A – C, 5.5 A – B, 5.6 A – E
Scenarios:

- **Application Vulnerability Investigation Lab**
  Students analyze a simulated web application scenario to identify vulnerabilities related to insecure user input, weak authentication, or excessive permissions. Students identify application and database indicators of compromise to support incident analysis. Students explain how adversaries could exploit the weaknesses and recommend defense-in-depth secure coding and mitigation strategies. This activity aligns to Skills 1.B, 2.A, and 2.B.
- **Cryptography & Secure Communication Activity**
  Students compare symmetric and asymmetric encryption methods through guided scenarios involving secure data storage and secure communication between systems. Students evaluate which encryption methods are most appropriate for different cybersecurity situations and justify their reasoning using security principles. This activity aligns to Skills 2.B–2.D.
- **Database Attack Detection Scenario**
  Students review application logs, database activity reports, and access records to identify indicators of unauthorized access or malicious activity. Students classify the attack behavior, determine potential impacts to organizational data, and develop an incident response and mitigation plan. This activity aligns to Skills 3.A–3.D and collaborative cybersecurity problem-solving objectives.
- **Database Breach & Web Application Investigation**
  Students investigate a suspected data breach involving a vulnerable web application that improperly validates user input. Students analyze logs, user access records, and SQL query behavior to determine how the attack occurred and propose encryption, access control, and secure coding mitigations.

Student Evaluation

Students are evaluated on their ability to analyze evidence, classify attacks, and communicate evidence-based cybersecurity recommendations.

Category	Frequency	Approx. Point Value
Labs/Activities	1-2 per unit	40-60 points
Unit Scenarios/Quizzes	1-2 per week	10-30 points
Unit Tests	1 roughly every 2-3 weeks (end of each unit)	100 points
Final Exam	1, at the end of the course	100 points

Teacher Resources

AP Classroom and CollegeBoard Resources at https://apcentral.collegeboard.org/courses/ap-cybersecurity/course