AP® Cybersecurity

Course Overview

About the Advanced Placement Program® (AP®)

The Advanced Placement Program® has enabled millions of students to take college-level courses and earn college credit, advanced placement, or both, while still in high school. AP Exams are given each year in May. Students who earn a qualifying score on an AP Exam are typically eligible, in college, to receive credit, placement into advanced courses, or both. Every aspect of AP course and exam development is the result of collaboration between AP teachers and college faculty. They work together to develop AP courses and exams, set scoring standards, and score the exams. College faculty review every AP teacher's course syllabus. We commit to supporting educators and communities in their efforts to make AP courses widely available, advancing students in their plans for college and careers.

AP Cybersecurity Course Overview

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. Developed in partnership with college faculty and industry leaders, this yearlong course aligns with the NICE Workforce Framework for Cybersecurity.

The AP Cybersecurity course is designed to be the equivalent of a one-semester college-level introduction to cybersecurity course.

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.

UNIT SCENARIOS

Unit scenarios for each unit in the cybersecurity framework offer authentic cybersecurity situations and are designed to connect the knowledge and skills students gain in each unit to relevant, real-world applications. These scenarios are offered to support hands-on, career-connected instruction.

AP Cybersecurity Course Content

The course content is organized into five units of study that provide a suggested sequence for the course. These units comprise the content and conceptual understandings in which colleges and universities typically expect students to be proficient to quality for college credit and/or placement.

- **Unit 1:** Introduction to Security
- **Unit 2:** Securing Spaces
- **Unit 3:** Securing Networks
- **Unit 4:** Securing Devices
- **Unit 5:** Securing Applications and Data

Each unit is broken down into teachable segments called topics.

AP Cybersecurity Course Skills

CYBERSECURITY SKILLS

- **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.

PROFESSIONAL SKILL DOMAINS

- **Communicating concepts:** Explain key cybersecurity concepts.
- **Investigating problems:** Explore the parameters of a problem to plan for solutions.
- **Assessing impacts:** Evaluate impacts on systems.
- **Enacting solutions:** Apply and communicate solutions.

AP Cybersecurity Exam Structure

AP CYBERSECURITY EXAM: 2 HOURS, 10 MINUTES

Assessment Overview

The AP Cybersecurity Exam assesses student understanding of the skills and learning objectives outlined in the course framework. The exam is 2 hours and 10 minutes long and includes 60 multiple-choice questions and 1 multi-part free-response question.

Format of Assessment

Section I: Multiple Choice | 60 Questions | 80 Minutes | 70% of Exam Score

- The multiple-choice section assess all five units and includes set-based questions.
- The assessment is organized around course skills with the following weighting: Skill Category 1: Analyze Risk–25-40%; Skill Category 2: Mitigate Risk–25-40%; Skill Category 3: Detect Attacks–25-40%

Section II: Free Response | 1 Question | 50 Minutes | 30% of Exam Score

- Section II of the AP Cybersecurity Exam includes one multi-part free-response question.
- The **Device Security Analysis** free-response question includes six sources about a single digital device.
- Students will be expected to cite evidence from the provided sources and explain their reasoning when describing attacks, permission settings, and the impact of policy and configuration modifications.

Exam Components

Sample Multiple-Choice Question

A school district wants to ensure that only the school principal (`kmurray`) can edit faculty evaluation reports and to limit permissions for everyone else. The district's system administrator wants to set the following permission for the file `Oak_Park_HS`, which contains the faculty evaluations.

```
-rw-r----- kmurray staff 2048 Sep 18 10:45 Oak_Park_HS
```

Which of the following commands can be used to set the permissions shown?

(A) `chmod 444 Oak_Park_HS`

(B) `chmod 640 Oak_Park_HS`

(C) `chmod 740 Oak_Park_HS`

(D) `chmod 777 Oak_Park_HS`

Correct Answer: B

Sample Free-Response Question

Device Security Analysis

- Requires students to answer a multi-part, free-response question based on analyzing multiple simulated sources from a single digital device. Students are asked to identify security issues; detect evidence of attacks; and describe the impact of changes to permission settings and firewall controls on network traffic, device behavior, and users. Provided sources may include security policies, firewall configurations, file-system permissions, and log files. Students are expected to cite evidence from the provided sources and explain their reasoning when describing attacks, permission settings, and the impact of policy or configuration changes.