

AP CYBERSECURITY

Cisco CyberOps Associate-Aligned Course Syllabus

School Year 2026-2027

Program	Mission Valley Regional Occupational Program (MVROP)
Instructor	Hector Albizo
Grade Level	Grades 11-12
Course Length	Full academic year; block schedule
Credits	10 high school credits, subject to MVROP policy
Course Type	Advanced Placement / Career Technical Education
Primary Curriculum	AP Cybersecurity CED and Cisco CyberOps Associate curriculum

Course Mission

Students will learn to analyze cyber risk, implement layered defenses, detect and classify attacks, communicate technical findings, and perform ethical, authorized cybersecurity work using modern tools, collaborative practices, and instructor-directed artificial intelligence.

"The only roadblock to your success rests between your ears."

1. Course Overview

AP Cybersecurity is a yearlong, college-level course that develops foundational cybersecurity knowledge and workforce-ready technical skills through real-world scenarios, hands-on investigations, and defense-in-depth problem solving. The course addresses security across physical spaces, computer networks, devices, applications, and data. Instruction uses the Cisco CyberOps Associate curriculum as the principal technical operations resource, extending AP learning into security monitoring, host-based analysis, network intrusion analysis, threat intelligence, incident response, and security policies and procedures.

2. Course Framework and Alignment

The syllabus integrates three complementary structures:

- AP Cybersecurity course content and the recurring skills of Analyze Risk, Mitigate Risk, Detect Attacks, and Collaborate with people and AI.
- Cisco CyberOps Associate technical competencies in security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.
- An embedded Operational Technology (OT) cybersecurity strand that applies traditional cybersecurity principles to industrial, manufacturing, robotics, facilities, and critical-infrastructure environments. OT is integrated into the coursework and is not a separate course.

3. Prerequisites and Student Readiness

- No formal prerequisite is required unless established by MVROP enrollment policy.
- Prior experience with computer hardware, operating systems, networking, or CCNA Introduction to Networks is recommended but not required.
- Students must be willing to read technical material, document evidence, troubleshoot methodically, collaborate professionally, and persist through complex problems.
- Heavy mathematics is not required; success depends primarily on logic, attention to detail, ethical judgment, communication, and consistent practice.

4. Student Learning Outcomes

- Identify threats, vulnerabilities, attack methods, and their effects on organizational risk.
- Evaluate likelihood, impact, and risk-reduction strategies with and without AI assistance.
- Select, implement, document, and evaluate layered security controls.
- Analyze network traffic, logs, alerts, packet captures, endpoint evidence, and indicators of compromise.
- Differentiate true positives, false positives, false negatives, and benign activity to avoid unnecessary escalation.
- Use Windows, Linux, Wireshark, Packet Tracer, command-line tools, SIEM/SOAR concepts, threat intelligence, and cyber-range resources in authorized environments.
- Explain authentication, access control, segmentation, firewalls, cryptography, PKI, malware, web attacks, and incident-response processes.
- Apply chain-of-custody, evidence preservation, documentation, legal, ethical, and professional standards.
- Recognize AI-enabled attacks and use AI responsibly as an instructor-directed collaboration and analysis tool.
- Explain how cybersecurity priorities change in OT environments, including safety, availability, reliability, asset visibility, segmentation, and secure remote access.
- Communicate findings clearly through reports, briefings, diagrams, incident tickets, and team-based exercises.

5. Course Content and Tentative Pacing

Pacing will be adjusted to the MVROP calendar, student needs, AP requirements, lab availability, and current cybersecurity events. All required AP topics will be taught. Cisco labs and OT applications are integrated where they strengthen the AP learning objectives.

AP Unit	Primary Topics	Cisco CyberOps Emphasis	Embedded OT Application	Tentative Timing
1. Introduction to Security	Social engineering; suspicious website logins; public networks; AI-based attacks; AI in cyber defense	CIA triad; risk, threat, vulnerability, exploit; threat actors; behavioral/statistical detection; generative-AI social engineering	AI-enabled impersonation and phishing against manufacturing personnel; protection of credentials and remote access	Weeks 1-3
2. Securing Spaces	Cyber foundations; physical vulnerabilities and attacks; physical controls; physical attack detection	Defense in depth; policies and procedures; evidence; access control; physical security	Plant-floor access, tailgating, removable media, exposed ports, control cabinets, safety zones, and asset inventory	Weeks 4-7
3. Securing Networks	Network attacks; managerial controls; wireless security; segmentation; firewalls; network detection	TCP/IP and 5-tuple analysis; NetFlow; packet capture; IDS/IPS; firewalls; ACLs; Wireshark; network intrusion analysis	IT/OT segmentation, industrial DMZs, secure remote access, passive monitoring, and availability-conscious containment	Weeks 8-15
4. Securing Devices	Device vulnerabilities and attacks; authentication; endpoint protection; detecting device attacks	Windows/Linux analysis; malware; ransomware; host logs; HIDS/HIPS; EDR concepts; sandbox analysis; indicators of compromise	PLCs, HMIs, engineering workstations, sensors, controllers, legacy systems, patch constraints, and safe hardening	Weeks 16-23
5. Securing Applications and Data	Application/data attacks; access controls; stored-data protection; cryptography; application security; attack detection	Web attacks; PKI and certificates; SIEM/SOAR logs; incident response; evidence; security policy and governance	Integrity of recipes/configurations, secure backups, vendor access, change control, and recovery of physical processes	Weeks 24-31
Integration and Review	AP-style scenarios; cumulative investigations; technical writing; exam preparation; capstone	SOC alert triage; host/network correlation; incident documentation; CyberOps certification review	IT/OT incident tabletop or capstone emphasizing safety, continuity, evidence, and escalation	Weeks 32-36

6. Embedded Operational Technology Cybersecurity Strand

- OT cybersecurity will be taught as a recurring application strand within the AP and Cisco coursework. It will not replace required AP content and will not be offered as a separate course within this syllabus. Students will apply core cybersecurity concepts to systems that monitor or control physical processes.
- Distinguishing IT assets from OT assets and understanding IT/OT convergence.
- Prioritizing safety, availability, reliability, process integrity, and controlled change.
- Recognizing common OT components such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), sensors, actuators, industrial networks, and supervisory systems.
- Applying asset inventory, network segmentation, least privilege, secure remote access, monitoring, backup, and incident-response concepts to industrial environments.
- Understanding that aggressive scanning, unplanned patching, or immediate shutdown may create operational or safety consequences in OT.
- Analyzing regional advanced-manufacturing scenarios relevant to Fremont and the greater Bay Area.

7. Instructional Methods

- Instructor demonstrations and guided technical practice.
- Cisco Networking Academy modules, assessments, Packet Tracer activities, and CyberOps labs.
- AP Cybersecurity scenarios, case studies, document-based analysis, and AP-style questions.
- Network and host investigations using logs, command-line output, packet captures, and simulated alerts.
- Cyber-range and sandbox exercises conducted only in authorized environments.
- Individual and team-based SOC simulations, tabletop exercises, briefings, and after-action reviews.
- Embedded AI-supported activities when specifically authorized by the instructor.
- OT cybersecurity applications woven into physical security, networking, endpoint, application, data, and incident-response lessons.

8. Primary Resources and Technology

- College Board AP Cybersecurity Course and Exam Description and AP Classroom resources.
- Cisco Networking Academy CyberOps Associate curriculum and related Cisco learning resources.
- School-managed Windows computers and approved Linux virtual machines.
- Cisco Packet Tracer, Wireshark, VirtualBox, Python, web browsers, and instructor-approved security tools.
- Cyber ranges, log datasets, PCAP files, case-study evidence, and lab network equipment.
- Instructor-provided readings, current-event materials, and regional workforce scenarios.

School-Managed Devices Only

Personal laptops and unapproved computing devices may not be connected to the classroom or lab network. Students will use school-managed systems and instructor-approved removable media only.

9. Assessment and Grading

The proposed grading categories below may be adjusted to conform to final MVROP grading policy and instructor implementation. Students are evaluated on both technical accuracy and professional practice.

Category	Weight	Examples
Hands-on labs and investigations	35%	Packet analysis, host analysis, configuration, logs, evidence, lab reports
Projects, scenarios, and collaborative work	25%	SOC cases, OT applications, tabletop exercises, capstone, briefings
Unit assessments and AP-style assessments	25%	Quizzes, tests, multiple-choice, free-response, source analysis
Cisco coursework and knowledge checks	10%	NetAcad modules, quizzes, skills practice, certification review
Professional practice	5%	Preparedness, safety, documentation, teamwork, equipment care, ethical conduct

10. Assignment Submission and Late-Work Policy

- Assignments are due by the date and time posted by the instructor. Students are responsible for checking the learning-management system and maintaining current work throughout the term.
- Students should communicate early when illness, an approved absence, an accommodation, or an emergency affects completion of work. Extensions are not automatic and must be arranged in accordance with MVROP policy.
- Technical work may require revision after feedback. Revision opportunities, when offered, must be completed by the published deadline.

ABSOLUTELY NO BULK END-OF-TERM SUBMISSIONS

Multiple missing assignments submitted during the final week of a semester or the year-end grading period will not be accepted or graded. Students must submit work by published deadlines and address missing work throughout the grading period. Waiting until the final week to turn in a collection of assignments is not an acceptable academic or workplace practice.

11. Artificial Intelligence Use for Coursework

- Artificial intelligence may be used for assignments only at the direction and under the guidance of the instructor. AI is a professional tool, not a substitute for student reasoning, evidence, or accountability.
- Use AI only when the instructor explicitly authorizes it for the assignment or activity.
- Follow the stated purpose, tool, account, prompt, data, and collaboration restrictions.
- Do not enter student records, passwords, personally identifiable information, medical information, confidential school information, proprietary data, or live security information into an AI system.
- Verify AI-generated claims, commands, configurations, code, citations, and recommendations before use.
- Disclose and document AI assistance when required, including prompts, outputs, revisions, and sources.
- Do not use AI to complete an assessment, generate an entire submission, conceal a lack of understanding, fabricate evidence, or misrepresent authorship.
- Students remain responsible for the accuracy, safety, legality, ethics, and quality of all submitted work, regardless of AI assistance.
- The instructor may require students to reproduce, explain, defend, or complete work without AI support.

12. Cybersecurity Ethics, Authorization, and Academic Integrity

- All cybersecurity activity must remain within instructor-approved systems, accounts, files, networks, simulations, cyber ranges, and lab boundaries.
- Students may not scan, probe, intercept, exploit, disrupt, bypass controls, obtain credentials for, or attempt unauthorized access to MVROP, school-district, public, private, or internet-connected systems.
- Techniques taught for defensive education may not be used against another person or organization without explicit written authorization.
- Students must preserve evidence, follow chain-of-custody directions, and report suspicious activity immediately rather than investigating beyond authorization.
- Account sharing, password sharing, plagiarism, unauthorized collaboration, copied configurations, fabricated evidence, and undisclosed AI-generated work are prohibited.
- Violations may result in loss of lab privileges, academic consequences, referral to administration, and other action under applicable policy or law.

13. Classroom and Laboratory Safety

NO FOOD OR DRINK

Food and beverages are not permitted in the classroom or laboratory. This prohibition protects students, electrical equipment, computers, network devices, evidence, and instructional materials. Only exceptions specifically authorized under MVROP policy or a documented accommodation will apply.

- Follow all instructor directions before powering, cabling, opening, moving, or configuring equipment.
- Maintain clear walkways and manage cables to prevent trip, electrical, and equipment hazards.
- Do not connect personal storage devices, adapters, cables, hotspots, or network equipment without permission.
- Report damaged equipment, exposed wiring, overheating, unusual odors, spills, safety concerns, and security incidents immediately.
- Do not remove equipment, media, evidence, components, or documents from the classroom or lab without authorization.
- Use safety equipment and electrostatic-discharge controls when directed.

14. MVROP Cell Phone & Electronic Device Policy

MVROP Cell Phone & Electronic Device Policy Tentative pending Board approval Fall of 2026

To prepare you for professional industry standards and comply with California state law (AB 3216 / CA Education Code § 48901.7), our class follows a “Workplace-First” device policy.

1. Expectation: Off & Away

Unless explicit permission is given, all personal devices (phones, smartwatches, earbuds) must be turned off or silenced and stored out of sight in your backpack or assigned caddy.

2. Academic & CTE Exceptions

Your phone is a professional tool when used appropriately. Devices are only permitted when authorized by the instructor for relevant coursework, such as:

Accessing digital blueprints, safety manuals, or specialized software.

Scanning diagnostic QR codes or photographing lab/portfolio projects.

Participating in class check-ins or quick assessments.

Note: Academic permission is never an allowance for social media, texting, gaming, or unauthorized photos/videos.

3. Safety & Professionalism

Zero Tolerance in Active Labs: Phones and earbuds are strictly prohibited near machinery, power tools, lifts, welding equipment, or during clinical procedures. Distraction is a major safety hazard.

Privacy: Unauthorized audio or visual recording in labs or changing areas is strictly forbidden.

4. Legal & Medical Exemptions

Per state law, devices may be accessed for documented medical monitoring (for example, glucose tracking), IEP/504 accommodations, or genuine emergency situations.

Implementation Notice

This syllabus language is tentative and must be conformed to the final MVROP Board-adopted policy, applicable sending-district requirements, student safety plans, and legally required accommodations.

15. Device-Policy Enforcement

- The instructor will use progressive classroom interventions consistent with the final MVROP policy and applicable student-discipline procedures.
- Unauthorized device use may result in the device being placed in the assigned storage location, loss of discretionary device privileges, parent/guardian contact, administrative referral, or other consequences authorized by policy.
- A student may not use a personal device to photograph, record, livestream, or distribute another person's image, voice, work, screen, credentials, or private information without authorization.
- Refusal to follow a safety-related direction may result in immediate removal from the active lab area.

16. Attendance, Participation, and Professional Standards

- Regular attendance is essential because many labs, team exercises, demonstrations, and cyber-range activities cannot be replicated independently.
- Students are expected to arrive on time, prepared to work, and ready to follow the daily lab status and safety briefing.
- Professional conduct includes respectful communication, accurate documentation, appropriate escalation, care of equipment, accountability for assigned roles, and constructive participation.
- Students who miss class are responsible for obtaining instructions and completing eligible make-up work within the permitted timeline.

17. Student Support, Accessibility, and Accommodations

MVROP will provide support and legally required accommodations in accordance with applicable law, Board policy, IEPs, Section 504 plans, English-learner supports, and documented student needs. Students should communicate with the instructor, counselor, case manager, or administrator as early as possible when support is needed. Accommodations do not waive safety, ethics, authorization, or academic-integrity requirements, but may change how a student accesses instruction or demonstrates learning.

18. AP Exam and Cisco Certification Preparation

- The course prepares students for the AP Cybersecurity Exam through continuous practice in analyzing risk, mitigating risk, detecting attacks, using evidence, and communicating solutions.
- Cisco CyberOps coursework provides additional preparation for the Cisco Cybersecurity Associate/CyberOps Associate certification objectives, including security monitoring, host analysis, network intrusion analysis, and policy/procedure domains.
- Completion of the course does not guarantee an AP score, college credit, placement, or Cisco certification. Exam registration, fees, eligibility, accommodations, and testing procedures are governed by College Board, Cisco, MVROP, and testing-center policies.

19. Student and Parent/Guardian Acknowledgment

By signing below, the student and parent/guardian acknowledge that they have reviewed this syllabus, understand the course expectations, and agree to support safe, ethical, professional, and timely participation. The signatures also acknowledge the following key requirements:

Cybersecurity activities are permitted only within instructor-authorized environments and boundaries.

AI may be used only when and how the instructor authorizes it.

Personal devices must comply with the Workplace-First device policy and active-lab safety restrictions.

Food and drink are prohibited in the classroom and laboratory, except as formally authorized.

Multiple missing assignments submitted during the final week of a semester or year-end grading period will not be graded.

The device-policy section remains tentative pending final Board action and will be updated to match adopted policy.

Student Name (print)		
Student Signature		Date
Parent/Guardian Name (print)		
Parent/Guardian Signature		Date
Best Contact Email/Phone		

Questions or concerns: Please contact the instructor through the official MVROP communication channel.

20. Framework References

[College Board, AP Cybersecurity Course and Exam Description, Effective Fall 2026](#)

[College Board, AP Cybersecurity Course Audit Requirements](#)

[Cisco, Understanding Cisco Cybersecurity Operations Fundamentals v1.2 \(200-201\) Exam Topics](#)

[California Education Code § 48901.7](#)