

AP CYBERSECURITY

Course Outline - AP Career Kickstart / Cisco CyberOps Associate

School Year 2026-2027

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

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 Framework	College Board AP Cybersecurity Course and Exam Description, effective Fall 2026
Technical Curriculum	Cisco Networking Academy CyberOps Associate / CBROPS 200-201 v1.2 alignment

Course Purpose

Develop students who can analyze cyber risk, apply layered security controls, detect and investigate attacks, communicate findings, and perform ethical, authorized cybersecurity work. Cisco CyberOps Associate provides the principal technical operations context, while Operational Technology (OT) cybersecurity is embedded as an applied strand rather than taught as a separate course.

1. 1. Course Competencies

- Analyze vulnerabilities, threats, attack methods, likelihood, impact, and organizational risk with and without appropriate AI support.
- Select and explain physical, administrative, network, endpoint, application, data, identity, and cryptographic security controls.
- Detect attacks by monitoring systems and analyzing logs, packet captures, alerts, host evidence, firewall rules, permissions, and indicators of compromise.
- Differentiate malicious activity from benign activity and distinguish true positives, false positives, false negatives, and normal operational behavior.
- Apply Cisco CyberOps concepts in security monitoring, host-based analysis, network intrusion analysis, threat intelligence, incident response, SIEM/SOAR, and security policy.
- Use Windows, Linux, Wireshark, Packet Tracer, command-line tools, virtual machines, cyber ranges, and instructor-approved security tools in authorized environments.
- Preserve evidence, document findings, follow escalation procedures, and apply ethical, legal, privacy, and professional cybersecurity norms.
- Collaborate effectively with people and, when authorized, AI while retaining human judgment, verification, traceability, and accountability.
- Apply cybersecurity principles to OT and industrial environments where safety, availability, reliability, segmentation, asset visibility, and controlled change are critical.

2. 2. AP Unit-by-Unit Course Outline

The sequence below follows the five-unit AP Cybersecurity framework effective Fall 2026. Cisco CyberOps labs and technical competencies are integrated where they reinforce AP learning objectives. Timing is tentative and may

be adjusted for the MVROP calendar, student mastery, lab availability, AP requirements, and current cybersecurity events.

AP Unit	Core Content	CyberOps / Demonstrated Skills	Embedded OT / Applied Context	Tentative Pacing
1. Introduction to Security	Cybersecurity foundations; risk; threats; vulnerabilities; social engineering; suspicious website logins; public networks; AI-based attacks; AI in cyber defense	CIA triad; threat intelligence; threat actors; attack methods; behavioral/statistical detection; basic alert interpretation; ethical authorization	Credential theft, impersonation, remote access, and AI-enabled social engineering affecting industrial and manufacturing personnel	Weeks 1-3
2. Securing Spaces	Physical vulnerabilities and attacks; facility security; administrative and physical controls; physical attack detection; access management	Defense in depth; access control; policies and procedures; evidence handling; event documentation; physical security assessment	Plant-floor access, tailgating, removable media, exposed ports, control cabinets, safety zones, visitor/vendor access, and asset inventory	Weeks 4-7
3. Securing Networks	Network attacks; managerial controls; wireless security; segmentation; firewalls; network monitoring and attack detection	TCP/IP and 5-tuple analysis; packet capture; Wireshark; NetFlow; ACL/firewall interpretation; IDS/IPS; network intrusion analysis; alert triage	IT/OT segmentation, industrial DMZ concepts, secure remote access, passive monitoring, availability-conscious containment, and protected conduits	Weeks 8-15
4. Securing Devices	Device vulnerabilities and attacks; authentication; endpoint protection; operating-system security; detecting device compromise	Windows/Linux analysis; malware and ransomware; host logs; HIDS/HIPS; EDR concepts; process/file analysis; indicators of compromise; sandbox concepts	PLCs, HMIs, engineering workstations, controllers, sensors, legacy systems, constrained patching, safe hardening, and maintenance windows	Weeks 16-23
5. Securing Applications and Data	Application and data attacks; access controls; stored-data protection; cryptography; application security; attack detection; recovery	Web attacks; PKI/certificates; log correlation; SIEM/SOAR concepts; incident response; evidence; security policy; governance; recovery documentation	Protection of recipes/configurations, secure backups, vendor access, change control, data integrity, and recovery of physical processes	Weeks 24-31
Integration, Capstone, and AP Review	Cumulative scenarios; document-based analysis; technical writing; AP-style multiple-choice and free-response practice; exam preparation	SOC alert triage; host/network correlation; incident documentation; escalation; CyberOps certification review; cumulative investigations	IT/OT incident tabletop or capstone emphasizing safety, continuity, evidence preservation, containment, recovery, and lessons learned	Weeks 32-36

3. 3. Hands-on Laboratory and Scenario Progression

- Security-risk and social-engineering analysis, including instructor-directed examination of AI-enabled impersonation and phishing.
- Physical-security survey and defense-in-depth exercise covering access points, removable media, visitor/vendor access, and evidence preservation.
- Network traffic analysis using Wireshark, packet captures, TCP/IP metadata, common protocols, firewall/ACL rules, and intrusion-detection evidence.
- SOC-style alert triage requiring students to distinguish suspicious activity from benign activity and avoid unnecessary escalation.
- Windows and Linux host investigations using processes, files, permissions, logs, authentication events, malware indicators, and endpoint evidence.
- Web/application, authentication, cryptography, PKI, and data-protection exercises emphasizing confidentiality, integrity, availability, and access control.
- SIEM/SOAR-oriented log correlation and incident-response scenarios requiring evidence, timeline development, containment recommendations, and reporting.
- OT cybersecurity applications embedded into appropriate labs, including segmentation, asset visibility, secure remote access, safe containment, and availability constraints.
- Cumulative AP-style capstone or tabletop investigation integrating physical, network, endpoint, application, data, policy, and communication requirements.

4. 4. Assessment Evidence

Evidence Type	Purpose	Typical Evidence
Hands-on labs and investigations	Demonstrate technical and analytical skill	Packet analysis, host analysis, configurations, logs, evidence, lab reports, instructor observation
AP-style scenario analysis	Apply AP skills to authentic evidence	Risk analysis, mitigation recommendations, attack detection, firewall/log/permission source analysis
Cisco CyberOps coursework	Reinforce SOC and certification-aligned knowledge	NetAcad modules, knowledge checks, labs, security-monitoring and incident-response tasks
Projects and collaborative exercises	Demonstrate professional teamwork and communication	SOC cases, tabletop exercises, OT applications, briefings, after-action reviews
Unit assessments	Measure required knowledge and AP/CyberOps transfer	Quizzes, tests, multiple-choice questions, free-response questions, technical explanations
Capstone	Integrate cybersecurity competencies	Cumulative investigation, evidence package, risk/mitigation analysis, incident report, presentation or briefing

AP Exam Preparation

The AP Cybersecurity Exam is fully digital. Current College Board guidance specifies 60 multiple-choice questions in 80 minutes (70% of the exam score) and one 50-minute free-response question (30%). The free-response task requires students to analyze multiple sources from the same device, such as firewall rules, system/application logs, file permissions, and device policy. Course assessments therefore emphasize evidence-based reasoning rather than memorization alone.

5. 5. Cisco CyberOps, AI, and OT Integration

- Cisco CyberOps: The Cisco curriculum strengthens AP learning through security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies/procedures.
- AI: Students learn to recognize AI-enabled threats and may use AI as an instructor-directed analysis and collaboration tool. All AI output must be verified; students retain responsibility for evidence, conclusions, safety, ethics, and authorship.
- Detection and automation: Students compare signature/rule-based approaches with behavioral and statistical approaches and examine SIEM/SOAR and automated-security workflows at an appropriate introductory level.
- OT strand: OT cybersecurity is woven into the AP units as an application of core cybersecurity principles. It is not a separate course and does not displace required AP content.
- Regional workforce relevance: Industrial and advanced-manufacturing examples connect cybersecurity to environments where digital systems interact with machines, facilities, robotics, controls, and physical processes.

6. 6. Professional and CTE Expectations

- Perform only instructor-authorized cybersecurity activities within approved systems, networks, accounts, files, simulations, and lab boundaries.
- Preserve evidence and document observations, hypotheses, actions, commands, sources, and results accurately.
- Protect credentials, student information, configurations, security data, and other privileged or restricted information.
- Communicate and collaborate professionally; distinguish facts, assumptions, and conclusions during technical investigations.
- Follow classroom/lab safety, equipment-handling, no-food/no-drink, personal-device, academic-integrity, and AI-use requirements stated in the companion syllabus.

- Maintain current coursework. Multiple missing assignments submitted during the final week of a semester or year-end grading period will not be accepted or graded, subject to legally required accommodations and approved exceptions.
- Apply responsible disclosure, authorization, privacy, chain-of-custody, and escalation principles expected in cybersecurity workplaces.

7. 7. Pathway Progression and Workforce Relevance

AP Cybersecurity serves as an advanced cybersecurity component within the MVROP ICT pathway. Networking and systems knowledge developed through courses such as CCNA Introduction to Networks and IT Essentials supports student success, while the AP/CyberOps combination advances students into security monitoring, threat analysis, incident response, and defensive operations. The embedded OT strand broadens this preparation for advanced manufacturing, industrial automation, utilities, transportation, smart infrastructure, robotics, and other environments where IT and physical systems converge.

8. 8. Reference Basis

College Board, AP Cybersecurity Course and Exam Description, effective Fall 2026.

College Board, AP Cybersecurity Course Audit curricular and resource requirements.

College Board, AP Cybersecurity Exam overview and current digital exam format.

Cisco Networking Academy, CyberOps Associate - current course catalog.

Cisco, 200-201 CBROPS v1.2 exam topics: security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

MVROP AP Cybersecurity companion syllabus for classroom, laboratory, grading, AI-use, academic-integrity, and electronic-device policies.

Document status: Sequence, pacing, labs, assessment timing, and instructional resources may be adjusted to meet the MVROP calendar, AP requirements, student mastery, equipment availability, current cyber threats, College Board updates, Cisco curriculum updates, and administrative direction.