Maryland CTE Programs of Study

Cybersecurity III (2025)

General requirements. This course is recommended for students in Grades 9-12. Students shall be awarded one credit for successfully completing this course. 1

1 General requirements. This course is recommended for students in Grades 9-12. Students shall be awarded one credit for successfully completing this course. 1

Introduction. 2

A Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions. 2.A

B The Digital Technology (DT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to securing and protecting network systems. 2.B

C The Cybersecurity Career and Technical Education (CTE) Program of Study emphasizes pathways related to securing computer and information networks, including local area networks (LAN), wide area networks (WAN), intranets, extranets, and other data communication systems. 2.C

D The Cybersecurity III course emphasizes the use of security information and event management (SIEM) tools, network behavior analysis, and ethical hacking practices to protect against sophisticated cyber threats. Students will also gain experience in incident response and risk management, learning to apply cybersecurity frameworks and regulatory standards.. 2.D

E Students will participate in at least two Career-Connected Education and Work-Based Learning experiences in this course, which might include informational interviews or job shadowing relevant to the program of study. 2.E

F Students are encouraged to participate in extended learning experiences through aligned Career and Technical Student Organizations (CTSOs). CTSOs are a cocurricular requirement in the Carl D. Perkins Act, and alignment to CTSO activities is an expectation for CTE programs in the state of Maryland. 2.F

Kn Skip to main content **he student demonstrates the necessary skills for career development, naintenance of employability, and successful completion of course outcomes. The student is expected to:** 3.A

1 Identify and demonstrate positive work behaviors that enhance employability and job advancement, such as regular attendance, promptness, proper attire, maintenance of a clean and safe work environment, and pride in work. 3.A.1

2 Demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, active listening, and a willingness to learn. 3.A.2

3 Employ effective reading, writing, and technical documentation skills. 3.A.3

4 Solve problems using critical thinking techniques and structured troubleshooting methodologies. 3.A.4

5 Demonstrate leadership skills and collaborate effectively as a team member. 3.A.5

6 Implement safety procedures, including proper handling of hardware and following cybersecurity guidelines. 3.A.6

7 Exhibit an understanding of legal and ethical responsibilities in the IT field, following data privacy laws and best practices for security. 3.A.7

8 Demonstrate time-management skills and the ability to prioritize tasks in a technical setting. 3.A.8

B The student identifies various career pathways in the information technology field. The student is expected to: 3.B

1 Develop a career plan that includes the necessary education, certifications, job skills, and experience for specific roles in IT networking. 3.B.1

2 Create a professional resume and portfolio that reflect skills, projects, certifications, and recommendations. 3.B.2

3 Demonstrate effective interview skills for roles in IT and networking. 3.B.3

C The student develops technology and digital literacy skills. The student is expected to: 3.C

1 Use technology as a tool for research, organization, communication, and problem-solving. 3.C.1

2 Use digital tools, including computers, mobile devices, collaboration platforms, and cloud services, to access, manage, and create information. 3.C.2

3 Demonstrate proficiency in using emerging and industry-standard technologies, including virtualization tools, network management software, and cybersecurity applications. 3.C.3

4 Understand ethical and legal considerations for technology use, including the principles of data protection, copyright, and responsible technology use. 3.C.4

D The student integrates core academic skills into networking practices. The student is expected to: 3.D

1 Demonstrate the use of clear communication techniques, both written and verbal, that are consistent with industry standards. 3.D.1

Skip to main content

! Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting. 3.D.2

3 Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting. 3.D.3

E The student demonstrates the necessary skills to perform advanced network and system security monitoring. The student is expected to: 3.E

1 Implement and configure security information and event management (SIEM) tools to monitor and analyze network traffic for potential security threats. 3.E.1

2 Use network monitoring tools and techniques to detect, respond to, and investigate unusual or unauthorized activity. 3.E.2

3 Configure alerts and incident logging procedures to support security operations. 3.E.3

4 Perform network behavior analysis to identify anomalies and potential threats. 3.E.4

F The student demonstrates the necessary skills to conduct vulnerability assessments and penetration testing. The student is expected to: 3.F

1 Plan and execute vulnerability assessments using tools like Nessus, Nmap, or OpenVAS, documenting and reporting findings. 3.F.1

2 Explain and apply methodologies for penetration testing, including reconnaissance, scanning, and exploitation. 3.F.2

3 Develop skills in ethical hacking techniques to identify and mitigate security vulnerabilities. 3.F.3

4 Evaluate and implement remediation actions based on vulnerability assessment reports and best practices in cybersecurity. 3.F.4

G The student demonstrates the necessary skills to manage incident response and recovery procedures. The student is expected to: 3.G

1 Describe and apply incident response processes, including preparation, detection, containment, eradication, recovery, and post-incident analysis. 3.G.1

2 Utilize digital forensics tools to collect, analyze, and preserve evidence in response to cybersecurity incidents. 3.G.2

3 Coordinate and document incident handling procedures, creating post-incident reports with recommended improvements. 3.G.3

4 Apply disaster recovery and business continuity planning practices to ensure data integrity and operational resilience. 3.G.4

H The student demonstrates the necessary skills to assess and apply organizational security controls and compliance standards. The student is expected to: 3.H

1 Identify and interpret industry regulations and compliance standards, such as PCI-DSS, GDPR, and HIPAA, and apply appropriate security controls. 3.H.1

2 Implement security frameworks (such as NIST or ISO/IEC 27001) to establish organizational cybersecurity policies and procedures. 3.H.2

Skip to main content

3 Develop risk management strategies that assess and mitigate potential business impacts of security threats. 3.H.3

4 Conduct audits to ensure compliance with organizational policies and regulatory requirements, documenting any corrective actions. 3.H.4

I The student integrates core academic skills into advanced cybersecurity practices. The student is expected to: 3.I

1 Demonstrate advanced technical communication skills in documenting complex cybersecurity processes and protocols. 3.I.1

2 Apply statistical analysis to evaluate and interpret security data from logs, alerts, and other monitoring tools. 3.I.2

3 Use principles of digital forensics to analyze and reconstruct events related to security incidents. 3.I.3

J The student demonstrates the necessary skills to evaluate AI/ML artifacts during incident investigations. The student is expected to: 3.J

1 Identify indicators of deepfake media or AI-generated content relevant to social-engineering incidents. 3.J.1

2 Propose playbook steps for suspected AI-enabled attacks (collection, containment, notification). 3.J.2

K The student demonstrates the necessary skills in secure software fundamentals. The student is expected to: 3.K

1 Explain common web/application flaws (survey of OWASP Top 10) and simple input validation concepts. 3.K.1

2 Use basic static/dynamic analysis tools in a safe lab to spot low-risk issues. 3.K.2

3 Propose remediation and secure coding guidelines appropriate to a high-school level. 3.K.3

L The student demonstrates the necessary skills to conduct and improve incident response. The student is expected to: 3.L

1 Participate in a tabletop exercise that practices roles, communications, and decision- making for a simulated incident. 3.L.1

2 Document post-incident lessons learned and propose updates to playbooks, controls, and training. 3.L.2

3 Coordinate with continuity/recovery stakeholders to align recovery time and recovery point objectives at a conceptual level. 3.L.3