Maryland CTE Programs of Study

Cybersecurity II (2025)

General requirements. This course is recommended for students in Grades 10-12. Students shall be awarded one credit for successfully completing this course. 1

1 General requirements. This course is recommended for students in Grades 10-12. 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 II course delves into advanced networking concepts, such as subnetting, routing, VPNs, and network security protocols, and students will learn to apply vulnerability scanning, risk assessment, and incident response strategies to protect against unauthorized access and data breaches. 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

Knowledge and Skills. 3

Skip to main content

A The student demonstrates the necessary skills for career development, naintenance of employability, and successful completion of course outcomes. The tudent 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

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

Skip to main content

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 configure, manage, and troubleshoot complex network infrastructures. The student is expected to: 3.E

1 Design and implement infrastructures, including LANs, WANs, and VPNs, to support secure and efficient data communication. 3.E.1

2 Configure and troubleshoot routing and switching devices, such as routers and managed switches, according to industry standards. 3.E.2

3 Utilize subnetting, IP addressing, and network protocols (TCP/IP, DNS, DHCP) to design secure network configurations. 3.E.3

4 Apply techniques for optimizing network performance and securing network traffic. 3.E.4

F The student demonstrates the necessary skills to secure network devices and manage network security protocols. The student is expected to: 3.F

1 Implement network security controls, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and secure network protocols (e.g., HTTPS TLS). 3.F.1

2 Configure and troubleshoot virtual private networks (VPNs) and other remote access solutions to protect data transmission. 3.F.2

3 Demonstrate knowledge of wireless security settings, including encryption standards (WPA2, WPA3) and access control. 3.F.3

4 Monitor network activity and logs to detect and respond to security threats. 3.F.4

G The student demonstrates the necessary skills to assess and mitigate cybersecurity threats and vulnerabilities. The student is expected to: 3.G

1 Identify and analyze security vulnerabilities in network systems using vulnerability scanning tools and penetration testing methods. 3.G.1

2 Conduct risk assessments and apply best practices for risk mitigation, including patch management, configuration management, and security policies. 3.G.2

3 Explain and implement access control models, such as role-based access control (RBAC), and multi-factor authentication (MFA). 3.G.3

4 Perform security audits and apply remediation strategies to strengthen the security posture of network environments. 3.G.4

H The student demonstrates the necessary skills to implement organizational security practices and procedures. The student is expected to: 3.H

1 Create and enforce security policies, procedures, and incident response plans based on organizational needs. 3.H.1

2 Explain and implement data protection strategies, including data classification, encryption, and secure disposal methods. 3.H.2

Skip to main content

3 Apply principles of social engineering awareness and conduct training to enhance security culture within an organization. 3.H.3

4 Demonstrate an understanding of regulatory compliance and privacy laws, such as GDPR and HIPAA, and their impact on cybersecurity practices. 3.H.4

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

1 Demonstrate effective communication skills in documenting and reporting security incidents and resolutions. 3.I.1

2 Apply advanced mathematical concepts, including probability and statistics, for analyzing network traffic patterns and threat data. 3.I.2

3 Use scientific and forensic principles to investigate and analyze security incidents in digital systems. 3.I.3

J The student demonstrates the necessary skills to differentiate IT and OT (industrial control) security and apply resiliency and secure-by-design principles. The student is expected to: 3.J

1 Compare IT vs. OT environments (safety/availability priorities, legacy systems, real-time constraints). 3.J.1

2 Describe the Purdue Model and recommend segmentation for ICS/IIoT networks. 3.J.2

3 Identify common OT threats (e.g., ransomware in manufacturing, insecure remote access) and basic mitigations (e.g., allow-listing, change control). 3.J.3

4 Apply secure-by-design concepts (threat modeling, SBOM awareness, default-deny) to simple OT scenarios. 3.J.4

5 Explain how incident response and business continuity differ in OT contexts (safety and recovery windows). 3.J.5

K The student demonstrates the necessary skills in cloud security fundamentals. The student is expected to: 3.K

1 Differentiate IaaS, PaaS, and SaaS and shared-responsibility models. 3.K.1

2 Configure identity, MFA, and baseline policies in a sandbox cloud tenant. 3.K.2

3 Interpret basic cloud service provider logs (e.g., sign-in, resource changes) to identify misconfigurations. 3.K.3

4 Describe risks of public storage, exposed keys, and over-permissive roles; propose remediations. 3.K.4

Skip to main content

L **The student demonstrates the necessary skills in identity and access management (IAM). The student is expected to:** 3.L

1. Map the identity lifecycle (provision, review, de-provision) and enforce least-privilege via roles. 3.L.1
2. Implement MFA choices and evaluate usability vs. security trade-offs. 3.L.2
3. Explain single sign-on (SSO) and federated identity at a conceptual level. 3.L.3

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

1. Explain common web/app flaws (OWASP Top 10 at a survey level) and simple input validation. 3.M.1
2. Use static/dynamic analysis tools in a safe lab to spot low-risk issues. 3.M.2
3. Propose remediation and secure coding guidelines appropriate to a high-school level. 3.M.3

N **The student demonstrates the necessary skills to participate in practical, challenge-based cybersecurity activities. The student is expected to:** 3.N

1. Complete beginner-to-intermediate CTF labs (e.g., privilege escalation basics, simple web exploitation) in a safe, isolated environment. 3.N.1
2. Produce brief write-ups capturing approach, tools used, and lessons learned. 3.N.2
3. Engage with recognized gamified platforms (e.g., SANS BootUp CTF, NetWars Skill Quest) or equivalent, as available and approved. 3.N.3

O **The student demonstrates the necessary skills to evaluate AI-assisted defense and adversarial use cases. The student is expected to:** 3.O

1. Describe how anomaly detection and clustering can support security operations center (SOC) workflows. 3.O.1
2. Recognize adversarial uses of AI (e.g., phishing at scale, deepfakes) and propose controls (e.g., content provenance, user education). 3.O.2