

FBLA Collegiate Cybersecurity*

Security Fundamentals (10 test items)

1. Describe examples of confidentiality, integrity, and availability in cybersecurity operations
2. Discuss measures for establishing digital trust (e.g., identity proofing, non-repudiation, attestation)
3. Explain how authentication, authorization, and accounting are implemented in practice
4. Analyze principles of Zero Trust present in security architectures
5. Discuss examples of binary and hexadecimal in cybersecurity
6. Perform basic arithmetic involving binary and hexadecimal
7. Analyze examples of least privilege principles

Cyber Threats and Vulnerabilities (20 test items)

1. Analyze the causes of SQL injection and buffer overflow vulnerabilities (e.g., poor input validation, memory management)
2. Analyze the causes, mechanics, and consequences of race conditions (e.g., critical sections, information leak, crash)
3. Discuss attributes of threat actors and their goals (e.g., internal and external threats, financial gain, espionage, data theft)
4. Analyze how different viruses infiltrate systems and spread (e.g., boot sector, polymorphic, macro)
5. Analyze how backdoors, zero-days, and outdated software can lead to cybersecurity incidents
6. Discuss social engineering scams and attacks (e.g., phishing, phone scams, email scams)
7. Describe the purpose, methods, and mechanics of a DDoS attack
8. Analyze effects of and defense against types of malware (e.g., viruses, Trojans, worms)
9. Describe the consequences and mechanics of cryptographic attacks on enterprise systems
10. Evaluate the security of a wireless network

* Sources: These learning outcomes are based on content from the Cybersecurity Curricula 2017, Security+ Certification Exam Objectives, and K-12 Cybersecurity Learning Standards.

Security and Design (20 test items)

1. Analyze the security benefits and drawbacks of cloud infrastructure (e.g., IaaS, SaaS, PaaS)
2. Recommend changes to cybersecurity policies based on system architecture (e.g., microservice, cloud-based, hybrid)
3. Discuss use cases and examples of logical and physical segmentation (e.g., VLANs, subnets, air-gapped systems)
4. Analyze security use cases for containerization and virtualization in enterprise systems
5. Recommend a backup schedule based on an organization's needs (e.g., differential, incremental, full)
6. Recommend RAID levels based on an organization's needs (e.g., level 0, level 5)
7. Discuss types of testing used in cybersecurity
8. Analyze the impact of physical network design decisions on cybersecurity
9. Discuss key considerations in designing secure systems (e.g., availability, resilience, cost, responsiveness)
10. Discuss ways to increase resilience and recovery in design (e.g., load balancing, clustering, multi-cloud, platform diversity, backups)

Network and Data Security (20 test items)

1. Discuss the role of cryptography in ensuring confidentiality, integrity, authentication, and non-repudiation
2. Analyze the benefits and drawbacks of public and private key cryptography
3. Describe the mechanics of public and private key cryptography
4. Discuss types of ciphers (e.g., shift, Caesar, substitution)
5. Discuss logical access control methods (e.g., access control lists, group policies, passwords)
6. Analyze differences between access control models (e.g., MAC, DAC, RBAC)
7. Analyze network authentication methods (e.g., multifactor, certificates, tokens)
8. Describe the characteristics of effective and ineffective hash functions (e.g., collisions, distribution, efficiency)
9. Discuss the advantages and disadvantages of using blockchain for data integrity and authentication

Security Operations and Management (10 test items)

1. Discuss common security policies (e.g., acceptable use, information security, business continuity, disaster recovery)
2. Discuss elements of disaster prevention and recovery plans
3. Discuss the use cases of different types of firewalls (e.g., network-based, NGFW, WAF)
4. Evaluate messaging, email, and data security policies for risk management
5. Describe change management practices

Security Protocols and Threat Mitigation (20 test items)

1. Describe the purposes of SSH, HTTPS, TLS, and WPA protocols
2. Explain how intrusion detection and prevention systems work (e.g., signature-based, anomaly-based, NIDS)
3. Evaluate the effectiveness of policies and practices for preventing viruses, phishing, and email scams
4. Analyze different types of obfuscation (e.g., code, data, network)
5. Explain how digital certificates and Certificate Authorities (CAs) contribute to security
6. Explain how patches, updates, and version control prevent attacks
7. Discuss examples of penetration testing
8. Describe a VPN and its uses in cybersecurity
9. Describe security protocols used by VPNs and their characteristics (e.g., TLS, OpenVPN, L2TP, IPsec)

References

- Adelaide University. *Cyber security basics: Exploring the fundamentals of cyber security*.
<https://online.adelaide.edu.au/blog/cyber-security-fundamentals>
- Association for Computing Machinery. *Cybersecurity Curricula 2017*.
https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
- Codecademy. *Introduction to cybersecurity*. <https://www.codecademy.com/learn/introduction-to-cybersecurity>
- CompTIA. *Security+ Certification Exam Objectives*.
<https://assets.ctfassets.net/82ripq7fjls2/6TYWUym0Nudqa8nGEnegiG/0f9b974d3b1837fe85ab8e6553f4d623/CompTIA-Security-Plus-SY0-701-Exam-Objectives.pdf>
- Cybersecurity Guide. *Mastering the basics: A comprehensive guide to cybersecurity 101 for the digital age*. <https://cybersecurityguide.org/resources/cybersecurity-101/>
- The Academic Initiative of the Cyber Innovation Center. *K-12 Cybersecurity Learning Standards*.
https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf