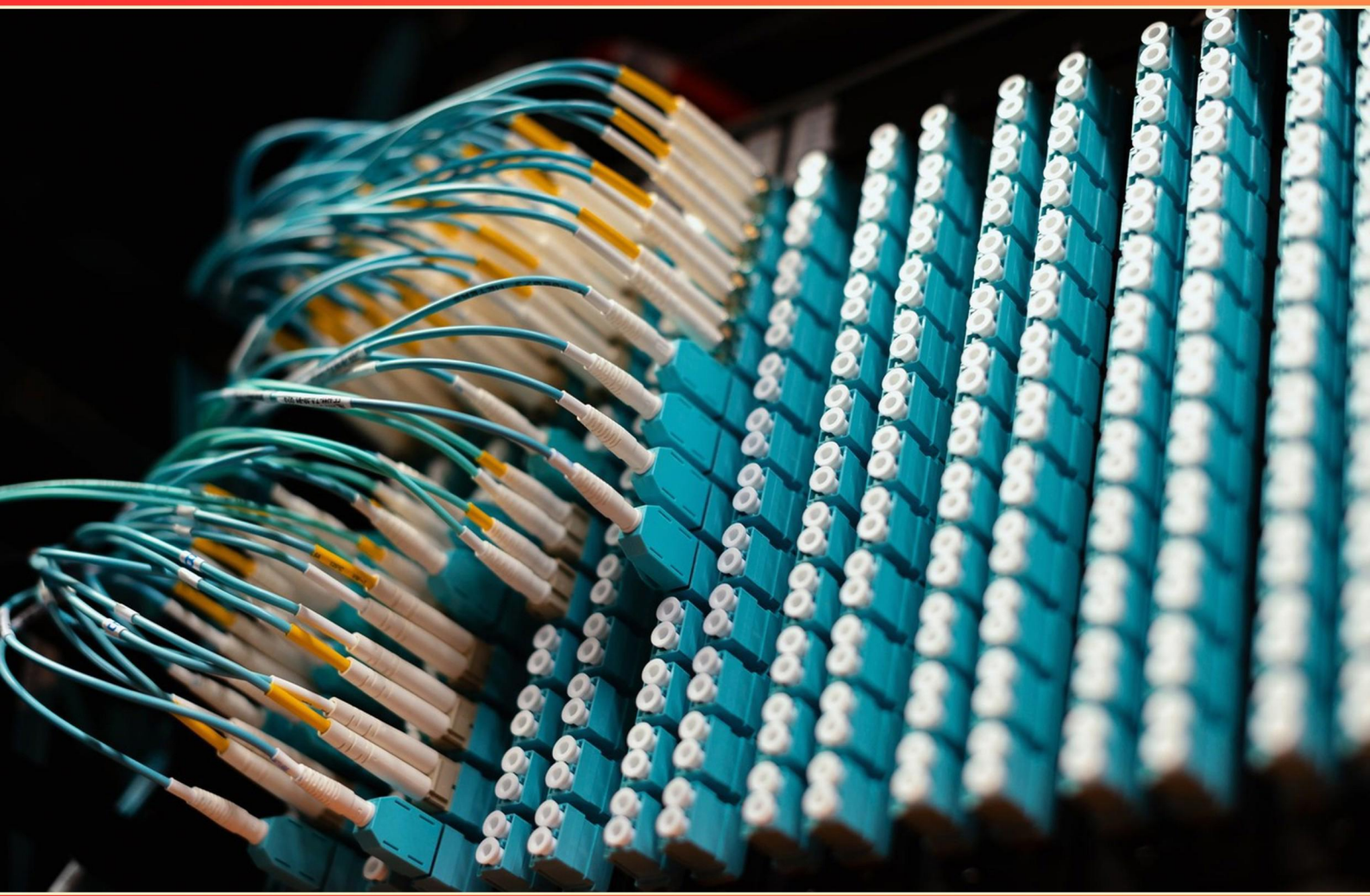
AIR FORCE CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://airforcecybersec.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **Which tool is used for searching, monitoring, visualizing, and analyzing machine data by the 26th Network Operations Squadron?**

   A. Splunk

   B. Microsoft Endpoint Configuration Manager (MECM)

   C. Redundant Array of Independent Disks (RAID)

   D. Mission Critical Mentality

2. **Which area/aspect of network management deals with repair and upkeep of network components?**

   A. Network Maintenance

   B. Administration/Accounts

   C. Layer 4 - Endpoint Security

   D. Layer 7 - The 'Human' or Physical Layer

3. **Which term provides the legal framework for the roles and organization of the U.S. military services and the Department of Defense?**

   A. Title 10, US Code (Armed Forces)

   B. Title 50

   C. Command Strategy

   D. Strategic guidance

4. **Which layer is specifically labeled as the 'Human' or Physical Layer?**

   A. Layer 1 - Mission Critical Assets/User Access Management

   B. Layer 4 - Endpoint Security

   C. Layer 7 - The 'Human' or Physical Layer

   D. Layer 2 - Data Security

5. **Which tool is used for managing vulnerabilities in cyber systems?**

   A. Microsoft Endpoint Configuration Manager (MECM)

   B. Splunk

   C. Active Directory (AD)

   D. Emergency Operating Procedures (EOPs)

6. What term describes the combined physical, virtual, or logical connectivity of an organization's users, devices, systems, and applications?

A. Enterprise Network

B. Data Center

C. Cloud Infrastructure

D. Local Area Network

7. Replicating adversary tactics for cyber integrity is known as?

A. Threat Emulation and Continuous Validation Assessment

B. Reconnaissance / Strike Coordination & Reconnaissance and Recover

C. Legacy and Current Mission Types

D. Secure and Protect

8. Which term provides point-to-cloud, scalable, transport independent services?

A. IMS

B. AFLCMC

C. AFNGS

D. Proxy

9. Which term is established to standardize network operations and improve mission predictability across cyberspace operations?

A. Cyberspace Centers of Excellence (COEs)

B. Mission Critical Mentality

C. Emergency Operating Procedures (EOPs)

D. Redundant Array of Independent Disks (RAID)

10. Which role maintains mission even in the event of an emergency or an outage?

A. Continuity of Operations (COOP)

B. MECM and ARAD

C. Wireshark

D. DSO

Answers

1. A
2. A
3. A
4. C
5. A
6. A
7. A
8. A
9. A
10. A

Explanations

1. Which tool is used for searching, monitoring, visualizing, and analyzing machine data by the 26th Network Operations Squadron?

A. Splunk

B. Microsoft Endpoint Configuration Manager (MECM)

C. Redundant Array of Independent Disks (RAID)

D. Mission Critical Mentality

Splunk is built to search, monitor, visualize, and analyze machine data from a wide range of sources such as logs, metrics, and events across networks and applications. It ingests data, indexes it, and provides a powerful search language and dashboards that let you drill into incidents, track performance trends, and set up real-time alerts. This combination—collecting diverse machine data and turning it into actionable insights with searchable queries and visualizations—makes Splunk the go-to tool for understanding how systems behave and where issues are occurring. The other options don't fit this use. Microsoft Endpoint Configuration Manager focuses on managing software and settings on endpoints rather than analyzing machine data at scale. RAID is a storage setup that improves redundancy or performance, not data analysis. Mission Critical Mentality isn't a data-analysis tool.

2. Which area/aspect of network management deals with repair and upkeep of network components?

A. Network Maintenance

B. Administration/Accounts

C. Layer 4 - Endpoint Security

D. Layer 7 - The 'Human' or Physical Layer

Repair and upkeep of network components is addressed by network maintenance. This area covers keeping hardware, cabling, and devices functioning through preventive care, troubleshooting, replacing faulty parts, applying firmware and software updates, and coordinating planned downtime. All of these activities aim to preserve reliability and performance by addressing wear, failures, and degradation before they impact users. Administrative tasks focus on users and access controls, so they aren't about maintaining the hardware or links. Security at Layer 4 deals with protecting data in transit, not the ongoing repair and upkeep of components. The physical or "human" layer concerns the physical environment and human factors, rather than the ongoing maintenance of equipment.

3. Which term provides the legal framework for the roles and organization of the U.S. military services and the Department of Defense?

A. Title 10, US Code (Armed Forces)

B. Title 50

C. Command Strategy

D. Strategic guidance

The legal framework that defines how the U.S. military services are organized and how the Department of Defense operates is found in Title 10 of the United States Code. It codifies the missions and structure of the armed forces, assigns responsibilities to the services and the DoD, and sets the authorities for manpower, procurement, and the budget under the chain of command. This statute ensures civilian control of the military and provides the binding foundation for how the services are arranged and how they operate. Other options don't establish this primary organizational framework: Title 50 deals with national defense and intelligence activities rather than the internal organization of the armed forces; Command Strategy and Strategic guidance refer to planning and policy concepts rather than binding legal structures.

4. Which layer is specifically labeled as the 'Human' or Physical Layer?

A. Layer 1 - Mission Critical Assets/User Access Management

B. Layer 4 - Endpoint Security

C. Layer 7 - The 'Human' or Physical Layer

D. Layer 2 - Data Security

The main idea here is recognizing how this particular security model assigns responsibilities across layers, with human and physical aspects treated as a distinct outer domain. Layer 7 is explicitly labeled as the "Human" or Physical Layer, so selecting that option shows you understand that this framework places people and physical access controls at the top layer of defense, bridging policy, behavior, and physical protections with the rest of the security stack. In concrete terms, this layer focuses on how human factors (awareness, training, policy adherence) and physical safeguards (facility access, hardware protection) interact with cyber defenses. That's why the option describing Layer 7 as the Human/Physical Layer is the best choice. The other options describe different security domains (mission-critical assets/user access management, endpoint security, data security) which belong to other layers in the model and do not carry the Human/Physical label.

5. Which tool is used for managing vulnerabilities in cyber systems?

A. Microsoft Endpoint Configuration Manager (MECM)

B. Splunk

C. Active Directory (AD)

D. Emergency Operating Procedures (EOPs)

Managing vulnerabilities relies on centralized patch and configuration management across all endpoints. Microsoft Endpoint Configuration Manager is designed for this role: it inventories devices, deploys and schedules patches and updates, and enforces security baselines and configurations. By actively pushing fixes and ensuring systems stay configured to secure standards, it directly reduces exposure from known vulnerabilities, making it the best fit among the options. Splunk, while excellent for collecting and analyzing logs to detect issues, isn't a patching or vulnerability remediation tool. Active Directory handles identity, access, and policy distribution but not the actual process of remediation across endpoints. Emergency Operating Procedures are steps for responding to incidents, not a tool for vulnerability management.

6. What term describes the combined physical, virtual, or logical connectivity of an organization's users, devices, systems, and applications?

A. Enterprise Network

B. Data Center

C. Cloud Infrastructure

D. Local Area Network

The concept being tested is the overall connectivity fabric that ties together all parts of an organization. An Enterprise Network describes how users, devices, systems, and applications are connected across physical, virtual, and logical layers—encompassing on premises networks, WANs, wireless, VPNs, SD WAN, and even connections to cloud services. It also includes the security policies, access controls, and management practices that govern that connectivity, spanning multiple sites and remote users. This makes it the best fit because it captures the entire spectrum of how everything in the organization communicates and is accessed, not just a single location or a specific type of resource. Other options don't cover the full scope. A data center is a facility housing servers and storage, focusing on centralized computing resources rather than the complete connectivity landscape of the organization. Cloud infrastructure refers to the cloud resources themselves (compute, storage, networking services) rather than the total network that unites users, devices, and applications across environments. A local area network describes the network within a single building or campus, which is only a portion of the enterprise's broader connectivity needs.

7. Replicating adversary tactics for cyber integrity is known as?

A. Threat Emulation and Continuous Validation Assessment

B. Reconnaissance / Strike Coordination & Reconnaissance and Recover

C. Legacy and Current Mission Types

D. Secure and Protect

Replicating adversary tactics for cyber integrity is about threat emulation combined with continuous validation assessment. Threat emulation involves simulating real attacker techniques to test how well defenses detect, respond, and recover from those tactics. Pairing this with continuous validation assessment means you're not just testing once; you're continuously verifying that security controls, configurations, and the overall system integrity hold up over time as the environment evolves and new threats appear. This approach provides practical insight into detection coverage and incident response readiness by replaying realistic attack scenarios. The other options don't capture this idea: they refer to reconnaissance or coordination terms, or are generic security phrases that don't convey actively mimicking attacker behavior or ongoing integrity verification.

8. Which term provides point-to-cloud, scalable, transport independent services?

A. IMS

B. AFLCMC

C. AFNGS

D. Proxy

Think of a service framework that lets applications offer multimedia and other services over any IP network without being tied to how the data is transported. IP Multimedia Subsystem embodies this. It defines a modular, service-centric architecture that sits between the application layer and the transport networks. By separating signaling and control from the transport, IMS can run over cellular, Wi Fi, or wired networks and supports roaming and interworking. Its components enable scalable deployment across many users and services, making it well-suited for cloud-based, carrier-grade environments. That combination—point-to-cloud capability, scalability, and transport independence—fits IMS best. The other options are not service frameworks: a proxy is a routing element rather than a full transport-agnostic service framework, and the remaining terms refer to organizations or systems rather than a concept that provides scalable, transport-independent services.

9. Which term is established to standardize network operations and improve mission predictability across cyberspace operations?

A. Cyberspace Centers of Excellence (COEs)

B. Mission Critical Mentality

C. Emergency Operating Procedures (EOPs)

D. Redundant Array of Independent Disks (RAID)

Standardizing how cyberspace operations are conducted across units is essential for reliable mission outcomes. Cyberspace Centers of Excellence are established to create and maintain common standards for operations, tools, training, and assessment. By centralizing doctrine, playbooks, and metrics, they ensure teams across the force execute cyber tasks in the same way, use compatible systems, and measure success against shared criteria. This common approach makes outcomes more predictable, speeds up readiness, and improves collaboration during joint missions and exercises. The other options don't serve this role: Emergency Operating Procedures focus on incident response in emergencies rather than cross-unit standardization; RAID is a storage technology; Mission Critical Mentality isn't a formal framework used for standardizing cyberspace operations.

10. Which role maintains mission even in the event of an emergency or an outage?

A. Continuity of Operations (COOP)

B. MECM and ARAD

C. Wireshark

D. DSO

This question tests how an organization preserves mission capability during emergencies or outages. Continuity of Operations, or COOP, focuses on keeping essential functions running when normal systems fail. It involves identifying mission-critical tasks, establishing alternate facilities and communication methods, ensuring key personnel can carry out those tasks, safeguarding data and resources, and regularly exercising the plan so responses are swift and effective. Because COOP is specifically centered on maintaining the mission under disruption, it best fits the scenario. The other options relate to IT management, a network analysis tool, and a role that isn't about continuity planning, so they don't address sustaining operations during an outage.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://airforcecybersec.examzify.com

We wish you the very best on your exam journey. You've got this!