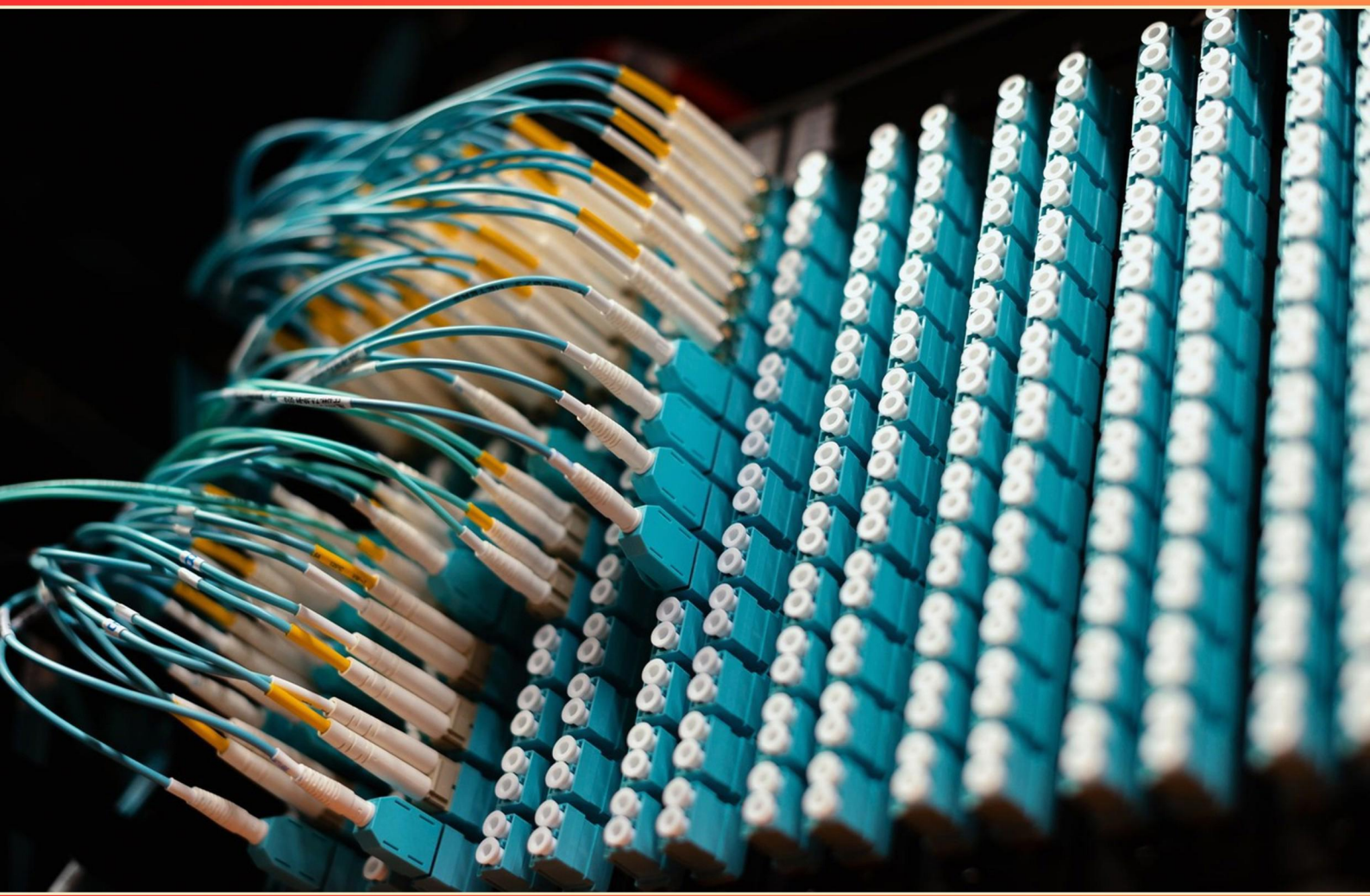
AIR FORCE CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://airforcecybersec.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1
Table of Contents 2
Introduction 3
How to Use This Guide 4
Questions 5
Answers 8
Explanations 10
Next Steps 15

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **Which platform is used to update the dynamic block list when interacting with viruses and other security threats?**

   A. Panorama (Palo Alto)

   B. Next Generation Firewall

   C. Splunk

   D. SolarWinds

2. **Which domain/layer focuses on organizational and operational aspects when architecting an enterprise network?**

   A. Business Layer

   B. Environment Layer

   C. Technology Layer

   D. Data Layer

3. **Which term is used to describe the plan outlining the desired effects and objectives of a cyber operation?**

   A. CONOPS

   B. SPINS

   C. CSCS

   D. Information Dominance Flight Plan

4. **Which term represents the golden age of network security, emphasizing firewalls, VPNs, and DMZs to control network access?**

   A. Perimeter Security

   B. FedRAMP

   C. Insider Threats

   D. Threat Intelligence

5. **Which term is described as the front line defense between the DoD and the Internet?**

   A. USAF Gateway Router - IP/MPLS

   B. IMS

   C. AFLCMC

   D. Cyber Mission Force

SAMPLE

6. What term describes a collection of computing environments under a single authority with secure access controls?

A. Enclave

B. APC

C. ECN

D. ERS

7. Which component is associated with OPCON (Operational Control) in cyberspace operations?

A. AFCYBER

B. 16th AF

C. JHQ-C

D. JRSS

8. Encompass Resolve, Identify, Protect, Detect, Respond, Recover, and Continuous Validation & Assessment, outlining the key operational focus areas in Air Force cybersecurity missions. Which term matches this description?

A. AFCYBER Mission Areas

B. Cyberspace Mission Types

C. Cyberspace Missions

D. Time-Sensitive Target (TST)

9. Which tool is designed to automatically identify and fix vulnerabilities in cyber systems?

A. Automated Remediation and Asset Discovery (ARAD)

B. Microsoft Endpoint Configuration Manager (MECM)

C. Active Directory (AD)

D. Emergency Drills

10. Which term best describes a security philosophy that requires verification of every access attempt, regardless of origin?

A. Zero Trust Security

B. Perimeter Defense

C. Access Control Lists

D. Patch Management

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which platform is used to update the dynamic block list when interacting with viruses and other security threats?

A. Panorama (Palo Alto)

B. Next Generation Firewall

C. Splunk

D. SolarWinds

Centralized distribution of threat intelligence to multiple devices is what this is about. Panorama acts as the centralized management plane for Palo Alto firewalls, collecting threat data and updates and pushing dynamic block lists and other threat signatures to all managed devices. That centralized push is what keeps protections in sync across the network so new viruses and security threats are blocked everywhere you rely on those firewalls. The other options don't serve this orchestration role: a single Next Generation Firewall handles protection on one device, Splunk is for log analysis, and SolarWinds is a general network management tool.

2. Which domain/layer focuses on organizational and operational aspects when architecting an enterprise network?

A. Business Layer

B. Environment Layer

C. Technology Layer

D. Data Layer

The Business Layer focuses on organizational and operational aspects when architecting an enterprise network. It translates business goals into network requirements, governs policies and compliance, defines service levels, roles, responsibilities, budgeting, and change management, and ensures the network enables day-to-day operations across the enterprise. This alignment with strategy, governance, and operations is what makes it the best fit for addressing how the network supports the organization as a whole. The other layers handle different concerns: the Environment Layer deals with physical hosting, facilities, and site-specific factors; the Technology Layer covers network devices, protocols, and configurations; the Data Layer focuses on data assets and how data moves and is stored.

3. Which term is used to describe the plan outlining the desired effects and objectives of a cyber operation?

A. CONOPS

B. SPINS

C. CSCS

D. Information Dominance Flight Plan

Concept of Operations explains how a cyber operation will be carried out to achieve the intended effects and objectives. It lays out the end state, the key actions, the sequencing, and who does what, providing a shared understanding for planners and operators. In cyber contexts, the CONOPS translates strategic goals into an actionable approach, defining the desired effects on the adversary or environment and guiding the development of more detailed plans and tasks. Other terms don't fit this role: SPINS are specialized instructions that modify or supplement standard procedures rather than describing the overall operation concept. CSCS isn't the established term for a cyber operation plan. Information Dominance Flight Plan tends to address broad information superiority initiatives rather than detailing the specific plan and effects of a cyber operation.

SAMPLE

4. Which term represents the golden age of network security, emphasizing firewalls, VPNs, and DMZs to control network access?

A. Perimeter Security

B. FedRAMP

C. Insider Threats

D. Threat Intelligence

Perimeter security describes the traditional boundary-based approach to protecting a network, where the main defenses sit at the edge: firewalls monitor and control traffic between networks, VPNs provide secure channels for remote access, and DMZs host public-facing services with restricted access to the internal network. This model emphasizes controlling who and what can cross the network boundary, forming a protective shield around the trusted environment. It's often called the golden age because these edge-based controls were the primary, most relied-upon defenses in many organizations. FedRAMP is about standardized security assessments for cloud services, not the boundary-focused edge protection described here. Insider threats refer to risks from people inside the organization rather than edge controls. Threat intelligence involves gathering information to anticipate attacks, not the network boundary defenses themselves.

5. Which term is described as the front line defense between the DoD and the Internet?

A. USAF Gateway Router - IP/MPLS

B. IMS

C. AFLCMC

D. Cyber Mission Force

The front line defense between the DoD and the Internet is the network boundary device that sits at the edge and enforces security before traffic enters or leaves the DoD networks. A gateway router at the edge handles traffic ingress and egress, applying access controls, routing decisions, and often VPN termination to ensure only authorized traffic crosses into the DoD environment. In the Air Force setup, the term that describes this role is the USAF Gateway Router - IP/MPLS, which serves as that boundary device and enforces policy at the edge of the network. The other options refer to a system or organization rather than a boundary device, so they don't fit the role of the frontline protector between DoD networks and the Internet. This gateway function is what provides the first line of defense by controlling and monitoring what can enter or leave the trusted network.

6. What term describes a collection of computing environments under a single authority with secure access controls?

A. Enclave

B. APC

C. ECN

D. ERS

An enclave is a secure boundary that groups multiple computing environments under one authority and enforces access controls across them. This setup ensures consistent authentication, authorization, and policy enforcement for everything inside the boundary, protecting resources and isolating them from outside domains. Because all systems within the enclave share a common security policy and control point, it's easier to manage who can access what and to audit activity. The other terms describe things that aren't a unified security domain of computing environments under central control, so they don't fit the description as well.

SAMPLE

7. Which component is associated with OPCON (Operational Control) in cyberspace operations?

A. AFCYBER

B. 16th AF

C. JHQ-C

D. JRSS

OPCON in cyberspace operations means the authority to direct and employ forces for a cyber mission. In the Air Force, the unit that centralizes and leads Air Force cyber forces—planning, tasking, and execution of cyber missions—is AFCYBER. This organization acts as the Air Force's cyber component and coordinates under the broader guidance of USCYBERCOM to carry out cyberspace operations on the required timeline. That makes AFCYBER the component associated with OPCON for Air Force cyberspace operations. The other options represent different parts of the structure or support functions: a larger cyber-focused field command would not itself hold the Air Force's OPCON; a joint cyber headquarters handles cross-service coordination rather than the Air Force's direct OPCON authority; and JRSS refers to a network security architecture rather than a command with OPCON responsibility.

8. Encompass Resolve, Identify, Protect, Detect, Respond, Recover, and Continuous Validation & Assessment, outlining the key operational focus areas in Air Force cybersecurity missions. Which term matches this description?

A. AFCYBER Mission Areas

B. Cyberspace Mission Types

C. Cyberspace Missions

D. Time-Sensitive Target (TST)

These Air Force cyber operations are organized into AFCYBER Mission Areas, a named framework that groups actions across the cyber lifecycle—Resolve, Identify, Protect, Detect, Respond, Recover—with Continuous Validation & Assessment. This term is the official label for that structured set of operational focus areas used to guide planning, execution, and assessment of cyber missions within the Air Force. The other options describe broader or unrelated concepts: Cyberspace Mission Types and Cyberspace Missions are general labels, not the formal designation for this grouped framework, and Time-Sensitive Target pertains to a different domain of operations entirely.

SAMPLE

9. Which tool is designed to automatically identify and fix vulnerabilities in cyber systems?

A. Automated Remediation and Asset Discovery (ARAD)

B. Microsoft Endpoint Configuration Manager (MECM)

C. Active Directory (AD)

D. Emergency Drills

Automated vulnerability management centers on continuously discovering assets, identifying weaknesses, and applying fixes with minimal human intervention. A tool that does both—identifying weaknesses across the network and automatically applying remediation actions—minimizes manual effort and speeds up response. Automated Remediation and Asset Discovery fits this role because it is designed to scan for vulnerabilities and automatically remediate them, such as deploying patches or adjusting configurations across affected systems. Microsoft Endpoint Configuration Manager focuses on managing devices—inventory, software deployment, and patch distribution—but it isn't built to automatically detect vulnerabilities across the environment and perform remediation without manual guidance. Active Directory is about managing identities and access, not vulnerability identification or automatic fixes. Emergency Drills are practice exercises and don't perform vulnerability scanning or remediation. So, the tool described is Automated Remediation and Asset Discovery.

10. Which term best describes a security philosophy that requires verification of every access attempt, regardless of origin?

A. Zero Trust Security

B. Perimeter Defense

C. Access Control Lists

D. Patch Management

Zero Trust Security is the approach where no user or device is trusted by default, regardless of whether the access request originates inside or outside the network. Every attempt to access a resource must be authenticated, authorized, and continuously evaluated, with the principle of least privilege guiding who can do what. This means even internal traffic is verified, and access decisions can adapt in real time based on context such as device health, user identity, and behavior. This philosophy contrasts with relying on a strong network perimeter alone. Perimeter Defense focuses on keeping threats out at the boundary, not on verifying every access request inside. Access Control Lists are policies that enforce who can access what, but they're a mechanism rather than the overarching philosophy. Patch Management deals with updating software to fix vulnerabilities, not with controlling access.

SAMPLE

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!

SAMPLE