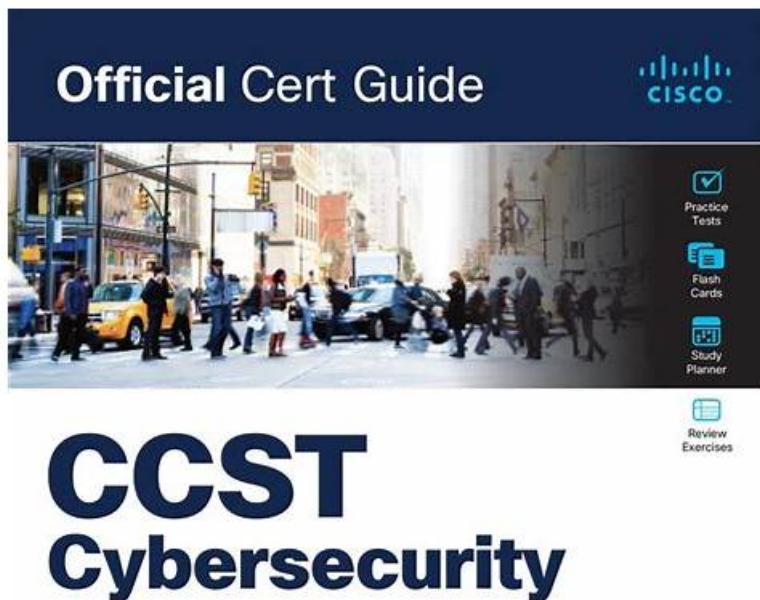


Free PDF 2026 100-160: Cisco Certified Support Technician (CCST) Cybersecurity Newest Interactive Practice Exam



Raymond Lacoste
Shane Sexton

ciscopress.com

BTW, DOWNLOAD part of Prep4cram 100-160 dumps from Cloud Storage: <https://drive.google.com/open?id=1nbYqbUmvHdR6ayAQqEkStbsd2g6smj>

As a worldwide leader in offering the best 100-160 Test Torrent, we are committed to providing comprehensive service to the majority of consumers and strive for constructing an integrated service. What's more, we have achieved breakthroughs in 100-160 certification training application as well as interactive sharing and after-sales service. As a matter of fact, our company takes account of every client's difficulties with fitting solutions. As long as you need help, we will offer instant support to deal with any of your problems about our Cisco Certified Support Technician (CCST) Cybersecurity guide torrent. Any time is available; our responsible staff will be pleased to answer your questions.

Cisco 100-160 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Basic Network Security Concepts: This section of the exam measures the skills of a Network Defender and focuses on understanding network-level protections, including firewalls, VPNs, and intrusion detection prevention systems, providing insight into how threats are mitigated within network environments.
Topic 2	<ul style="list-style-type: none">Vulnerability Assessment and Risk Management: This section of the exam measures the skills of a Risk Management Analyst and entails identifying and assessing vulnerabilities, understanding risk priorities, and applying mitigation strategies that help manage threats proactively within an organization's systems

Topic 3	<ul style="list-style-type: none"> Essential Security Principles: This section of the exam measures the skills of a Cybersecurity Technician and covers foundational cybersecurity concepts such as the CIA triad (confidentiality, integrity, availability), along with basic threat types and vulnerabilities, laying the conceptual groundwork for understanding how to protect information systems.
Topic 4	<ul style="list-style-type: none"> Incident Handling: This section of the exam measures the skills of an Incident Responder and centers on recognizing security incidents, responding appropriately, and containing threats—forming the essential foundation of incident response procedures.
Topic 5	<ul style="list-style-type: none"> Endpoint Security Concepts: This section of the exam measures the skills of an Endpoint Security Specialist and includes securing individual devices, understanding protections such as antivirus, patching, and access control at the endpoint level, essential for maintaining device integrity.

>> Interactive 100-160 Practice Exam <<

Free 100-160 Exam - 100-160 Latest Braindumps

With all of these 100-160 study materials, your success is 100% guaranteed. Moreover, we have Demos as freebies. The free demos give you a prove-evident and educated guess about the content of our practice materials. As long as you make up your mind on this exam, you can realize their profession is unquestionable. And their profession is expressed in our 100-160 training prep thoroughly. They are great help to catch on the real knowledge of 100-160 exam and give you an unforgettable experience. Do no miss this little benefit we offer.

Cisco Certified Support Technician (CCST) Cybersecurity Sample Questions (Q70-Q75):

NEW QUESTION # 70

Which technology is commonly used to monitor network data and identify security incidents?

- A. IDS (Intrusion Detection System)
- B. SOAR (Security Orchestration, Automation, and Response)
- C. SIEM (Security Information and Event Management)**
- D. Firewall

Answer: C

Explanation:

SIEM is a technology that focuses on monitoring network data to identify security incidents. It collects and analyzes security event logs from various sources, such as firewalls, intrusion detection systems (IDS), and antivirus software, to identify abnormal behavior or potential security incidents. SIEM solutions provide real-time monitoring, correlation, and alerting capabilities, enabling organizations to effectively detect and respond to security threats.

NEW QUESTION # 71

Which protocol is commonly used for remote user authentication and authorization?

- A. RADIUS**
- B. LDAP
- C. SSH
- D. TACACS+

Answer: A

Explanation:

RADIUS (Remote Authentication Dial-In User Service) is a widely-used protocol for remote user authentication and authorization. It provides centralized authentication, authorization, and accounting management for users who dial in or connect remotely to a network. RADIUS uses a client-server model where the client (network access server) forwards user authentication requests to the

RADIUS server for validation.

NEW QUESTION # 72

Which of the following is an example of a human-caused disaster?

- A. Flood
- B. Tornado
- C. Earthquake
- D. Cyberattack

Answer: D

Explanation:

Cyberattacks, such as hacking, malware, or ransomware attacks, are considered human-caused disasters. They are intentional actions carried out by individuals or groups with malicious intent and can result in significant disruption, data loss, and financial damage if proper cybersecurity measures are not in place.

NEW QUESTION # 73

Which of the following control types is focused on identifying vulnerabilities and weaknesses in systems and addressing them?

- A. Corrective controls
- B. Detective controls
- C. Compensating controls
- D. Preventive controls

Answer: A

Explanation:

Corrective controls are designed to identify and rectify vulnerabilities and weaknesses in systems. They aim to correct issues identified through assessments, audits, or incident response, and ensure that the necessary steps are taken to minimize the associated risks. Examples of corrective controls include patch management, vulnerability scanning, and system hardening procedures.

NEW QUESTION # 74

Which of the following is a limitation of vulnerability databases?

- A. They cover all known vulnerabilities in every software and hardware.
- B. They require minimal human effort for maintaining and updating.
- C. They provide real-time information on emerging threats.
- D. They may not include vulnerabilities discovered by malicious actors.

Answer: D

Explanation:

Vulnerability databases are an essential resource for cybersecurity professionals to stay informed about known vulnerabilities. However, these databases primarily rely on information shared by vendors, security researchers, and ethical hackers. Malicious actors, who may discover vulnerabilities independently, may not disclose them in such databases. Therefore, it is crucial to adopt a well-rounded approach to vulnerability management and consider potential undisclosed vulnerabilities.

NEW QUESTION # 75

.....

Do you want to obtain your 100-160 study materials as quickly as possible? If you do, then we will be your best choice. You can receive downloading link and password with ten minutes after buying. In addition, 100-160 exam dumps are high quality, because we have experienced experts to edit, and you can pass your exam by using 100-160 Exam Materials of us. In addition, we are pass guarantee and money back guarantee, if you fail to pass the exam by using 100-160 study materials of us, we will give you full refund. And the money will be returned to your payment account.

Free 100-160 Exam: https://www.prep4cram.com/100-160_exam-questions.html

What's more, part of that Prep4cram 100-160 dumps now are free: <https://drive.google.com/open?id=1nbYqbUmvHdR6ayAQqEkSttbsd2g6smj>