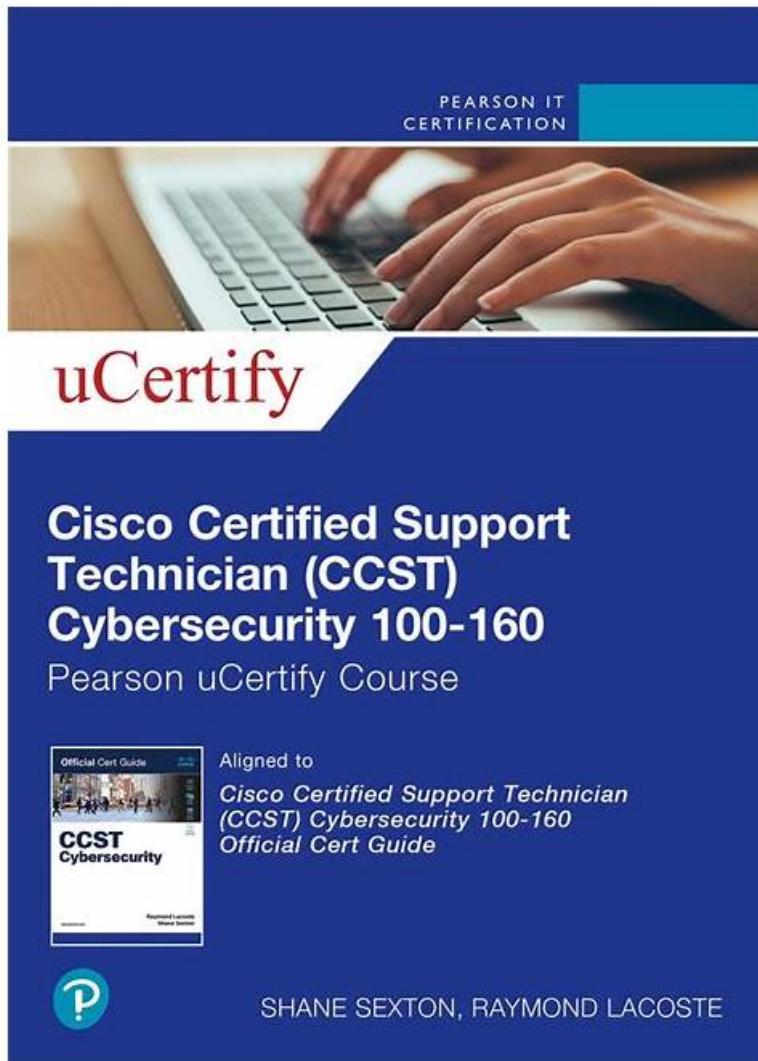


# 選擇100-160考古題介紹 -不用再擔心Cisco Certified Support Technician (CCST) Cybersecurity考試



PEARSON IT CERTIFICATION

uCertify

## Cisco Certified Support Technician (CCST) Cybersecurity 100-160

Pearson uCertify Course

Aligned to

*Cisco Certified Support Technician (CCST) Cybersecurity 100-160 Official Cert Guide*



SHANE SEXTON, RAYMOND LACOSTE

BONUS!!! 免費下載NewDumps 100-160考試題庫的完整版：<https://drive.google.com/open?id=1flnA8noE3a1wC3OXDTfwroSB2JA150ta>

為了不讓你得生活留下遺憾和後悔，我們應該盡可能抓住一切改變生活的機會。你做到了嗎？NewDumps Cisco的100-160考試培訓資料是幫助每個想成功的IT人士提供的培訓資料，幫助你們順利通過Cisco的100-160考試認證。為了不讓成功與你失之交臂，趕緊行動吧。

大家在準備考試的時候，可以結合本網站最新的Cisco 100-160 擬真試題去認真地做練習，這樣的話，可以為你的考試節省很多的時間。Cisco的100-160考試整體來說還是不算複雜的，只要事先將擬真試題看好就沒有問題了。還有，做實驗題是要一定要多想想，這樣的話，才能將自身的一些素質提高上去。我們的考題網剛更新100-160題庫能確保考生能順利通過100-160考試，獲得Cisco認證證照。

>> 100-160考古題介紹 <<

## 100%有保障的100-160考古題介紹，最好的學習資料幫助你快速通過100-160考試

對於NewDumps最近更新的Cisco 100-160考古題，我們知道，只有有效和最新的100-160題庫可以幫助大家通過考試，這是由眾多考生證明過的事實。請嘗試Cisco 100-160考古題最新的PDF和APP版本的題庫，由專家認證並覆蓋

考試各個方面，能充分有效的幫助您補充相關的100-160考試知識點。不放棄下一秒就是希望，趕緊抓住您的希望吧，選擇100-160考古題，助您順利通過考試！

## Cisco 100-160 考試大綱：

主題	簡介
主題 1	<ul style="list-style-type: none"><li>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</li></ul>
主題 2	<ul style="list-style-type: none"><li>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.</li></ul>
主題 3	<ul style="list-style-type: none"><li>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.</li></ul>
主題 4	<ul style="list-style-type: none"><li>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</li><li>prevention systems, providing insight into how threats are mitigated within network environments.</li></ul>
主題 5	<ul style="list-style-type: none"><li>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.</li></ul>

## 最新的 Cisco CCST 100-160 免費考試真題 (Q303-Q308):

### 問題 #303

Which encryption method uses two different keys, a public key and a private key?

- A. Symmetric encryption
- B. Asymmetric encryption**
- C. SSL/TLS
- D. Hashing

### 答案： B

#### 解題說明：

Asymmetric encryption, also known as public-key encryption, uses two different keys: a public key for encryption and a private key for decryption. The public key can be freely distributed, allowing anyone to encrypt messages that only the recipient with the corresponding private key can decrypt. This method is commonly used for secure communication and establishing secure connections.

### 問題 #304

What is the purpose of incident response planning in cybersecurity?

- A. To conduct forensic investigations after cybersecurity incidents
- B. To prevent cybersecurity incidents from occurring
- C. To recover from cybersecurity incidents and restore normal business operations
- D. To detect and respond to cybersecurity incidents in a timely and effective manner**

### 答案： D

#### 解題說明：

Incident response planning in cybersecurity focuses on establishing processes and procedures to detect, respond to, and mitigate the

impact of cybersecurity incidents. It ensures that organizations have the necessary measures in place to identify incidents promptly, contain them, and minimize the potential damage. The goal is to respond to incidents in a timely and effective manner to protect sensitive data and maintain business continuity.

#### 問題 #305

Which of the following is a primary goal of monitoring security events "as they occur"?

- A. To enforce security policies and access controls
- B. To meet regulatory compliance requirements
- C. To ensure zero incidents and vulnerabilities in the network
- D. **To detect and respond to security incidents in a timely manner**

答案: D

解題說明:

Monitoring security events "as they occur" is primarily aimed at quickly identifying and responding to security incidents. By continuously monitoring for potential threats and vulnerabilities, organizations can detect and mitigate security incidents in a timely manner, minimizing damage and reducing downtime.

#### 問題 #306

Which network security technology passively monitors network traffic and compares the captured packet stream with known malicious signatures?

- A. Honeypot
- B. IPS
- C. Proxy Server
- D. **IDS**

答案: D

解題說明:

The CCST Cybersecurity course states that an Intrusion Detection System (IDS) passively monitors network or system traffic and analyzes it against a database of known threat signatures or behavioral patterns.

"IDS devices inspect network traffic, compare it to known malicious signatures or anomalies, and generate alerts for suspicious activity without actively blocking traffic." (CCST Cybersecurity, Basic Network Security Concepts, IDS and IPS section, Cisco Networking Academy) A is correct: IDS is passive and signature-based.

B (IPS) is active and can block traffic.

C (Proxy Server) handles requests between clients and servers.

D (Honeypot) is a decoy system to attract attackers.

#### 問題 #307

Which of the following is the most secure and recommended method for storing sensitive user data in a database?

- A. Using asymmetric encryption
- B. Using symmetric encryption
- C. **Using hashing algorithms**
- D. Storing the data in plain text

答案: C

解題說明:

Option 1: Incorrect. Storing sensitive user data in plain text is highly insecure and not recommended. If a database breach occurs, all the data will be exposed without any protection.

Option 2: Incorrect. Using symmetric encryption would require storing the encryption key securely, which can be difficult.

Additionally, any access to the data would require the encryption key, adding complexity and potential vulnerabilities.

Option 3: Correct. Using hashing algorithms is the most secure and recommended method for storing sensitive user data in a database. Hashing algorithms convert the data into a fixed-size string, making it difficult to reverse-engineer and obtain the original data. This ensures that even if a breach occurs, the sensitive data remains protected.

Option 4: Incorrect. Using asymmetric encryption would also require storing the encryption keys securely and adds unnecessary complexity for data retrieval, making it less practical for storing sensitive user data in a database.

### 問題 #308

• • • • •

通過擁有技術含量的Cisco 100-160認證資格，可以使自己在一家新公司獲得不錯的工作機會，來提升你的IT技能，有一個更好的職業發展道路。我們的100-160考古題是可靠，經濟實惠，品質最高的題庫資料，以幫助考生解決如何通過Cisco 100-160考試的問題。我們還會不定期的更新所有考試的考古題，想獲得最新的100-160考古題就在我們的網站，確保你成功通過100-160考試，實現夢想！

100-160考試指南: <https://www.newdumpspdf.com/100-160-exam-new-dumps.html>

BONUS!!! 免費下載NewDumps 100-160考試題庫的完整版: <https://drive.google.com/open?id=1fLnA8noE3a1wC3OXDTfwroSB2JA150ta>