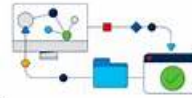


200-201 Schulungsmaterialien & 200-201 Dumps Prüfung & 200-201 Studienguide



200-201 CBROPS Exam Topics Customize Your Study Plan

To earn your CyberOps Associate certification, you must pass the **200-201 CBROPS** exam. This 120-minute exam tests your knowledge of security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

The following topics are likely to be included on the **200-201 CBROPS** exam. The topics are subject to change at any time to reflect the latest technologies aligned to Cisco's products.



Cisco Cert Prep Tip: Print out this document and use it as you assess your strengths and challenges in preparing your study plan.

Exam Topics:

Section: 1.0 Security Concepts

1.1 Describe the CIA triad	Need to Study?	Complete by:	Resource:	Completed
	Y / N			<input type="checkbox"/>
1.2 Compare security deployments	Need to Study?	Complete by:	Resource:	Completed
1.2.a Network, endpoint, and application security systems	Y / N			<input type="checkbox"/>
1.2.b Agentless and agent-based protections	Y / N			<input type="checkbox"/>
1.2.c Legacy antivirus and antimalware	Y / N			<input type="checkbox"/>
1.2.d SIEM, SOAR, and log management	Y / N			<input type="checkbox"/>
1.3 Describe security terms	Need to Study?	Complete by:	Resource:	Completed
1.3.a Threat intelligence (TI)	Y / N			<input type="checkbox"/>
1.3.b Threat hunting	Y / N			<input type="checkbox"/>
1.3.c Malware analysis	Y / N			<input type="checkbox"/>
1.3.d Threat actor	Y / N			<input type="checkbox"/>
1.3.e Run book automation (RBA)	Y / N			<input type="checkbox"/>

Übrigens, Sie können die vollständige Version der DeutschPrüfung 200-201 Prüfungsfragen aus dem Cloud-Speicher herunterladen: <https://drive.google.com/open?id=1cLrtZOEWSNLSheOhsCgqnOvgm6V9f0GQ>

Die Cisco 200-201 Zertifizierungsprüfung sind jedem IT-Fachmann sehr wichtig. Solange Sie das 200-201 Zertifikat bekommen, werden Sie im Beruf sicher nicht aussondert. Sie werden befördert und ein höheres Gehalt beziehen. Mit diesem Zertifikat können Sie alle bekommen, was Sie wünschen. Die Fragenpool zur Cisco 200-201Zertifizierungsprüfung von DeutschPrüfung sind die Ressourcen zum Erfolg. Mit diesen Schulungsmaterialien werden Sie den Schritt zum Erfolg beschleunigen. Sie werden sicher mehr selbstbewusster.

Um für die Cisco 200-201 Zertifizierungsprüfung zugelassen zu werden, sollten Kandidaten ein grundlegendes Verständnis von Netzwerkgrundlagen, Sicherheitskonzepten und Bedrohungsanalysen haben. Sie sollten auch Erfahrung in der Arbeit in einem Cybersecurity Operations Center (SOC) oder einer ähnlichen Umgebung haben. Die Prüfung besteht aus 100 Fragen und ist in mehreren Sprachen verfügbar.

Die Cisco 200-201 Prüfung ist eine wesentliche Zertifizierung für diejenigen, die ihre Karriere im Bereich der Cybersicherheit beginnen oder vorantreiben möchten. Es ist eine umfassende Prüfung, die eine breite Palette von Cybersicherheitsgrundlagen abdeckt und somit eine hervorragende Wahl für diejenigen ist, die ein tiefes Verständnis der Cybersicherheitsoperationen erlangen möchten. Das Bestehen dieser Prüfung führt zur Zertifizierung als Cisco Certified CyberOps Associate, die von Arbeitgebern weltweit anerkannt wird.

Cisco 200-201 Fragenkatalog - 200-201 Praxisprüfung

Wofür zögern Sie noch? Sie haben nur eine Chance. Jetzt können Sie die vollständige Version zur Cisco 200-201 Zertifizierungsprüfung bekommen. Sobald Sie die DeutschPrüfung klicken, wird Ihr kleiner Traum verwirklicht werden. Sie haben die besten Schulungsunterlagen zur Cisco 200-201 Zertifizierungsprüfung gekriegen. Benutzen Sie beruhigt unsere Cisco 200-201 Prüfungsfragen und Antworten, werden Sie sicher die Cisco 200-201 Prüfung bestehen.

Die Cisco 200-201 Prüfung ist eine anspruchsvolle Prüfung, die gründliche Vorbereitung und Studium erfordert. Es wird empfohlen, dass Kandidaten Kenntnisse in Netzwerkgrundlagen, Betriebssystemen und grundlegenden Sicherheitskonzepten haben, bevor sie diese Prüfung ablegen. Darüber hinaus sollten die Kandidaten mit verschiedenen Cybersecurity-Tools und -Technologien vertraut sein.

Cisco Understanding Cisco Cybersecurity Operations Fundamentals 200-201 Prüfungsfragen mit Lösungen (Q89-Q94):

89. Frage

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

- A. **nmap -sL 192.168.1.0/24**
- B. nmap -sP 192.168.1.0/24
- C. nmap --top-ports 192.168.1.0/24
- D. nmap -sV 192.168.1.0/24

Antwort: A

90. Frage

Syslog collecting software is installed on the server For the log containment, a disk with FAT type partition is used An engineer determined that log files are being corrupted when the 4 GB file size is exceeded. Which action resolves the issue?

- A. Add space to the existing partition and lower the retention period.
- B. **Use FAT32 to exceed the limit of 4 GB.**
- C. Use the Ext4 partition because it can hold files up to 16 TB.
- D. Use NTFS partition for log file containment

Antwort: B

Begründung:

FAT is a file system that organizes and stores data on a disk. However, FAT has a limitation of 4 GB for the maximum file size, which means that any file larger than that will be corrupted. To resolve this issue, the engineer can use FAT32, which is an improved version of FAT that supports files up to 32 GB. Alternatively, the engineer can use other file systems that have higher file size limits, such as Ext4 or NTFS. Reference= Cisco Cybersecurity Operations Fundamentals, Module 5: Security Policies and Procedures, Lesson 5.1: Data Retention, Topic 5.1.1: Data Retention Policies and Procedures

91. Frage

Which piece of information is needed for attribution in an investigation?

- A. **known threat actor behavior**
- B. 802.1x RADIUS authentication pass and fail logs
- C. proxy logs showing the source RFC 1918 IP addresses
- D. RDP allowed from the Internet

Antwort: A

Begründung:

Actually this is the most important thing: know who, what, how, why, etc.. attack the network.

92. Frage

Drag and drop the uses on the left onto the type of security system on the right.

ensures protection of individual devices	Endpoint
detects intrusion attempts	
monitors host for suspicious activity	
monitors incoming traffic and connections	Network

Antwort:

Begründung:

ensures protection of individual devices	Endpoint
detects intrusion attempts	ensures protection of individual devices
monitors host for suspicious activity	monitors incoming traffic and connections
monitors incoming traffic and connections	Network
	detects intrusion attempts
	monitors host for suspicious activity

Endpoint
ensures protection of individual devices
monitors incoming traffic and connections

Network
detects intrusion attempts
monitors host for suspicious activity

93. Frage

Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.

