CCOA Vorbereitung, CCOA Deutsche Prüfungsfragen

P.S. Kostenlose 2025 ISACA CCOA Prüfungsfragen sind auf Google Drive freigegeben von It-Pruefung verfügbar: https://drive.google.com/open?id=1CcKhj17mGViGSudDIo9vU1cBuRif_LD0

Jedem, der die Prüfungsunterlagen und Software zu ISACA CCOA （ISACA Certified Cybersecurity Operations Analyst） von It-Pruefung nutzt und die ISACA Zertifizierungsprüfungen nicht beim ersten Mal erfolgreich besteht, versprechen wir, die Kosten für das Prüfungsmaterial 100% zu erstatten.

ISACA CCOA Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Technology Essentials: This section of the exam measures skills of a Cybersecurity Specialist and covers the foundational technologies and principles that form the backbone of cybersecurity. It includes topics like hardware and software configurations, network protocols, cloud infrastructure, and essential tools. The focus is on understanding the technical landscape and how these elements interconnect to ensure secure operations.
Thema 2	• Cybersecurity Principles and Risk: This section of the exam measures the skills of a Cybersecurity Specialist and covers core cybersecurity principles and risk management strategies. It includes assessing vulnerabilities, threat analysis, and understanding regulatory compliance frameworks. The section emphasizes evaluating risks and applying appropriate measures to mitigate potential threats to organizational assets.
Thema 3	• Incident Detection and Response: This section of the exam measures the skills of a Cybersecurity Analyst and focuses on detecting security incidents and responding appropriately. It includes understanding security monitoring tools, analyzing logs, and identifying indicators of compromise. The section emphasizes how to react to security breaches quickly and efficiently to minimize damage and restore operations.
Thema 4	• Securing Assets: This section of the exam measures skills of a Cybersecurity Specialist and covers the methods and strategies used to secure organizational assets. It includes topics like endpoint security, data protection, encryption techniques, and securing network infrastructure. The goal is to ensure that sensitive information and resources are properly protected from external and internal threats.
Thema 5	• Adversarial Tactics, Techniques, and Procedures: This section of the exam measures the skills of a Cybersecurity Analyst and covers the tactics, techniques, and procedures used by adversaries to compromise systems. It includes identifying methods of attack, such as phishing, malware, and social engineering, and understanding how these techniques can be detected and thwarted.

>> CCOA Vorbereitung <<

Hilfsreiche Prüfungsunterlagen verwirklicht Ihren Wunsch nach der Zertifikat der ISACA Certified Cybersecurity Operations Analyst

Wenn Sie Ihre Position in der konkurrenzfähigen Gesellschaft durch die ISACA CCOA Zertifizierungsprüfung festigen und Ihre fachliche Fähigkeiten verbessern wollen, müssen Sie gute Fachkenntnisse besitzen und sich viel Mühe für die Prüfung geben. Aber es ist nicht so einfach, die ISACA CCOA Zertifizierungsprüfung zu bestehen. Vielleicht durch die ISACA CCOA Zertifizierungsprüfung können Sie Ihnen der IT-Branche vorstellen. Aber man braucht nicht unbedingt viel Zeit und Energie, die Fachkenntnisse kennenzulernen. Sie können die Schulungsunterlagen zur ISACA CCOA Zertifizierungsprüfung von It-Pruefung wählen. Sie werden zielgerichtet nach den IT-Zertifizierungsprüfungen entwickelt. Mit ihr können Sie mühelos die schwierige ISACA CCOA Zertifizierungsprüfung bestehen.

ISACA Certified Cybersecurity Operations Analyst CCOA Prüfungsfragen mit Lösungen (Q72-Q77):

72. Frage
Which of the following is the PRIMARY benefit of implementing logical access controls on a need-to-know basis?

- A. Limiting access to sensitive data and resources
- B. Providing a consistent user experience across different applications
- C. Ensuring users can access all resources on the network
- D. Reducing the complexity of access control policies and procedures

Antwort: A

Begründung:
The primary benefit of implementing logical access controls on aneed-to-know basisis tolimit access to sensitive data and resources. This principle ensures that users and processes have access only to the information necessary for their roles.
* Principle of Least Privilege:Minimizes the risk of data exposure by restricting access based on job responsibilities.
* Data Protection:Reduces the chance of internal data breaches by limiting who can view or modify sensitive information.
* Enhanced Security:Mitigates the risk of privilege misuse or insider threats.
Incorrect Options:
* B. Ensuring users can access all resources:This contradicts the need-to-know principle.
* C. Providing a consistent user experience:This is unrelated to access control.
* D. Reducing the complexity of access control policies:While it can simplify management, the primary goal is data protection.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 4, Section "Access Control Models," Subsection "Need-to-Know Principle" - Implementing need-to-know access reduces exposure of sensitive data by restricting access only to necessary users.

73. Frage
The user of the Accounting workstation reported thattheir calculator repeatedly opens without their input.
The following credentials are used for thisquestion.
Username:Accounting
Password:1x-4cc0unt1NG-x1
Using the provided credentials, SSH to the Accountingworkstation and generate a SHA256 checksum of the filethat triggered RuleName Suspicious PowerShell usingeither certutil or Get-FileHash of the file causing theissue. Copy the hash and paste it below.

Antwort:

Begründung:
See the solution in Explanation.
Explanation:
To generate theSHA256 checksumof the file that triggeredRuleName: Suspicious PowerShellon the Accounting workstation, follow these detailed steps:
Step 1: Establish an SSH Connection
* Open a terminal on your system.
* Use the provided credentials to connect to theAccounting workstation:
ssh Accounting@<Accounting_PC_IP>
* Replace <Accounting_PC_IP> with the actual IP address of the workstation.
* Enter the password when prompted:

1x-4cc0unt1NG-x1
Step 2: Locate the Malicious File
* Navigate to the typical directory where suspicious scripts are stored:
cd C:\Users\Accounting\AppData\Roaming
* List the contents to identify the suspicious file:
dir
* Look for a file related toPowerShell(e.g., calc.ps1), as the issue involved thecalculator opening repeatedly.
Step 3: Verify the Malicious File
* To ensure it is the problematic file, check for recent modifications:
powershell
Get-ChildItem -Path "C:\Users\Accounting\AppData\Roaming" -Recurse | Where-Object { $_.LastWriteTime
-ge (Get-Date).AddDays(-1) }
* This will list files modified within the last 24 hours.
* Check file properties:
powershell
Get-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" | Format-List *
* Confirm it matches the file flagged byRuleName: Suspicious PowerShell.
Step 4: Generate the SHA256 Checksum
Method 1: Using PowerShell (Recommended)
* Run the following command to generate the hash:
powershell
Get-FileHash "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Algorithm SHA256
* Output Example:
mathematica
Algorithm Hash Path
--------- ---- ----
SHA256 d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d C:
\Users\Accounting\AppData\Roaming\calc.ps1
Method 2: Using certutil (Alternative)
* Run the following command:
cmd
certutil -hashfile "C:\Users\Accounting\AppData\Roaming\calc.ps1" SHA256
* Example Output:
SHA256 hash of calc.ps1:
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
CertUtil: -hashfile command completed successfully.
Step 5: Copy and Paste the Hash
* Copy theSHA256 hashfrom the output and paste it as required.
Final Answer:
nginx
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
Step 6: Immediate Actions
* Terminate the Malicious Process:
powershell
Stop-Process -Name "powershell" -Force
* Delete the Malicious File:
powershell
Remove-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Force
* Disable Startup Entry:
* Check for any persistent scripts:
powershell
Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"
* Remove any entries related to calc.ps1.
Step 7: Document the Incident
* Record the following:
* Filename:calc.ps1
* File Path:C:\Users\Accounting\AppData\Roaming\
* SHA256 Hash:d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
* Date of Detection:(Today's date)

74. Frage
Which of the following is the PRIMARY benefit of using software-defined networking for network security?

- A. It simplifies network topology and reduces complexity.
- B. It Improves security monitoring and alerting capabilities.
- C. It provides greater scalability and flexibility for network devices.
- D. It allows for centralized security management and control.

Antwort: D

Begründung:
Software-Defined Networking (SDN)centralizes network control by decoupling the control plane from the data plane, enabling:
* Centralized Management:Administrators can control the entire network from a single point.
* Dynamic Policy Enforcement:Security policies can be applied uniformly across the network.
* Real-Time Adjustments:Quickly adapt to emerging threats by reconfiguring policies from the central controller.
* Enhanced Visibility:Consolidated monitoring through centralized control improves security posture.
Incorrect Options:
* A. Simplifies network topology:This is a secondary benefit, not the primary security advantage.
* B. Greater scalability and flexibility:While true, it is not directly related to security.
* D. Improves monitoring and alerting:SDN primarily focuses on control, not monitoring.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Software-Defined Networks," Subsection "Security Benefits" - SDN's centralized control model significantly enhances network security management.

75. Frage
Cyber threat intelligence is MOST important for:

- A. revealing adversarial tactics, techniques, and procedures.
- B. performing root cause analysis for cyber attacks.
- C. configuring SIEM systems and endpoints.
- D. recommending best practices for database security.

Antwort: A

Begründung:
Cyber Threat Intelligence (CTI)is primarily focused onunderstanding the tactics, techniques, and procedures (TTPs)used by adversaries. The goal is to gain insights into:
* Attack Patterns:How cybercriminals or threat actors operate.
* Indicators of Compromise (IOCs):Data related to attacks, such as IP addresses or domain names.
* Threat Actor Profiles:Understanding motives and methods.
* Operational Threat Hunting:Using intelligence to proactively search for threats in an environment.
* Decision Support:Assisting SOC teams and management in making informed security decisions.
Other options analysis:
* A. Performing root cause analysis for cyber attacks:While CTI can inform such analysis, it is not the primary purpose.
* B. Configuring SIEM systems and endpoints:CTI cansupportconfiguration, but that is not its main function.
* C. Recommending best practices for database security:CTI is more focused on threat analysis rather than specific security configurations.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Threat Intelligence and Analysis:Explains how CTI is used to reveal adversarial TTPs.
* Chapter 9: Threat Intelligence in Incident Response:Highlights how CTI helps identify emerging threats.

76. Frage
Which of the followingBESTdescribes static application security testing (SAST)?

- A. Vulnerability scanning
- B. Codereview
- C. Attack simulation
- D. Configuration management

Antwort: B

Begründung:
Static Application Security Testing (SAST)involvesanalyzing source code or compiled codeto identify vulnerabilities without executing the program.
* Code Analysis:Identifies coding flaws, such asinjection, buffer overflows, or insecure function usage
.
* Early Detection:Can be integrated into the development pipeline to catch issues before deployment.
* Automation:Tools likeSonarQube, Checkmarx, and Fortifyare commonly used.
* Scope:Typically focuses on source code, bytecode, or binary code.
Other options analysis:
* A. Vulnerability scanning:Typically involves analyzing deployed applications or infrastructure.
* C. Attack simulation:Related to dynamic testing (e.g., DAST), not static analysis.
* D. Configuration management:Involves maintaining and controlling software configurations, not code analysis.
CCOA Official Review Manual, 1st Edition References:
* Chapter 9: Application Security Testing:Discusses SAST as a critical part of secure code development.
* Chapter 7: Secure Coding Practices:Highlights the importance of static analysis during the SDLC.

77. Frage
.....

Die ISACA CCOA Zertifizierungsprüfung ist schon eine der beliebten IT-Zertifizierungsprüfungen geworden. Aber für die Prüfung braucht man viel Zeit und Energie, um die Fachkenntnisse gut zu beherrschen. Im diesem Zeitalter, wo die Zeit sehr geschätzt wird, betrachtet man Zeit wie Geld. Das Schulungsprogramm zur ISACA CCOA Zertifizierungsprüfung von It-Pruefung dauert ungefähr 20 Stunden. Dann können Sie Ihre Fachkenntnisse konsolidierern und sich gut auf die ISACA CCOA Zertifizierungsprüfung vorbereiten.

Außerdem sind jetzt einige Teile dieser It-Pruefung CCOA Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1CcKhj17mGViGSudDIo9vU1cBuRif_LD0