ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Cyber AB

Code: CMMC-CCA

Exam: Certified CMMC Assessor (CCA) Exam

https://www.examsnest.com/exam/cmmc-cca/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Topic 3, Assessing CMMC Level 2 Practices

Question: 1

You are assessing Conedge Ltd, a contractor that develops cryptographic algorithms for classified government networks. In reviewing their network architecture documents, you see they have implemented role-based access controls on their workstations using Active Directory group policies. Software developers are assigned to the "Dev_Roles" group which grants access to compile and test code modules. The "Admin_Roles" group with elevated privileges for system administration activities is restricted to the IT staff. However, when you examine the event logs on a developer workstation, you find evidence that a developer was able to enable debugging permissions to access protected kernel memory – a privileged function. How should execution of the debugging permission be handled to align with AC.L2-3.1.7 – Privileged Functions?

A. Require it to generate an email alert
B. Perform automatic termination of the action
C. Implement geo-IP blocking on the workstation
D. Ensure it is logged to the central SIEM system

Answer: D

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:
AC.L2-3.1.7 requires "preventing non-privileged users from executing privileged functions and logging such attempts." The developer's access to kernel memory (a privileged function) violates least privilege, and logging to a SIEM (D) ensures visibility and auditability, aligning with the practice. Alerts (A) are supplementary, termination (B) isn't required, and geo-IP blocking (C) is unrelated. The CMMC guide emphasizes logging for accountability.
Extract from Official CMMC Documentation:
CMMC Assessment Guide Level 2 (v2.0), AC.L2-3.1.7: "Log attempts by non-privileged users to execute privileged functions."
NIST SP 800-171A, 3.1.7: "Examine logs for privileged function attempts."
Resources:
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question: 2

While reviewing a contractor's Microsoft Active Directory authentication policies, you observe that the account lockout threshold is configured to allow 5 consecutive invalid login attempts before locking the account for 15 minutes. Additionally, the reset account lockout counter is set to 30 seconds after each unsuccessful login attempt. Based on this scenario, which of the following statements are TRUE about the contractor's implementation of CMMC practice AC.L2-3.1.8 – Unsuccessful Logon Attempts?
A. The contractor has successfully implemented practice AC.L2-3.1.8 – Unsuccessful Logon Attempts warranting a score of MET
B. The contractor's approach does not provide sufficient protection against unauthorized access attempts
C. Based on the current implementation, CMMC practice AC.L2-3.1.8 cannot be scored as MET
D. The contractor's approach does not adequately address the required assessment objectives

Answer: A

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:
AC.L2-3.1.8 requires "limiting unsuccessful logon attempts" by defining: [a] a threshold, and [b] a lockout duration or delay. The contractor’s settings (5 attempts, 15-minute lockout, 30-second reset) meet these objectives, providing reasonable protection against brute-force attacks. While stricter settings (e.g., fewer attempts) could enhance security, CMMC doesn’t mandate specific values, only that limits are enforced. This 1-point practice scores Met (+1), making A true. B, C, and D assume inadequacy without evidence of failure.
Extract from Official CMMC Documentation:
CMMC Assessment Guide Level 2 (v2.0), AC.L2-3.1.8: "Define and enforce [a] number of attempts, [b] lockout duration or delay."
DoD Scoring Methodology: "1-point practice: Met = +1."
Resources:
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question: 3

While examining a contractor's audit and accountability policy, you realize they have documented types of events to be logged and defined content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. After the logs are analyzed, the results are fed into a system that automatically generates audit records stored for 30 days. However, mechanisms implementing system audit logging are lacking after several tests because they produce audit logs that are too limited. You find that generated logs cannot be independently used to identify the event they resulted from because the defined content specified therein is too limited. Additionally, you realize the logs are retained for 24 hours before they are automatically deleted. Which of the following is a potential assessment method for AU.L2-3.3.1 – System Auditing?
A. Examine procedures addressing audit record generation
B. Testing procedures addressing control of audit records
C. Testing the system configuration settings and associated documentation
D. Examining the mechanisms for implementing system audit logging

Answer: A

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:
AU.L2-3.3.1 requires "creating and retaining audit records with sufficient content." Examining procedures (A) verifies if defined content meets requirements, addressing the scenario's deficiency (limited logs). Testing procedures (B) isn't standard, testing configs (C) is secondary, and examining mechanisms (D) isn't a method—testing them is. The CMMC guide lists procedural examination as key.
Extract from Official CMMC Documentation:
CMMC Assessment Guide Level 2 (v2.0), AU.L2-3.3.1: "Examine procedures addressing audit record generation."
NIST SP 800-171A, 3.3.1: "Examine documented processes for content sufficiency."
Resources:
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question: 4

You are assessing a contractor's implementation for CMMC practice MA.L2-3.7.4 – MediaInspection by examining their maintenance records. You realize the maintenance logs identify a repeating problem. A recently installed central server has been experiencing issues affecting the performance of the contractor's information systems. This is confirmed by your interview with the contractor's IT team. You requested to investigate the server, and the IT team agreed. On the server, there is a file named conf.zip that gets your attention. You decide to open the file in an isolated computer for further review. To your surprise, the file is a .exe used when testing the server for data exfiltration. How should this incident be handled?
A. By immediately reporting it to the FBI's Cyber Division
B. Decommissioning the server and installing a new one
C. In accordance with the incident response plan
D. By sandboxing the malicious code and continuing with business as usual

Answer: C

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:
CMMC practice MA.L2-3.7.4 – Media Inspection requires organizations to "inspect media containing diagnostic and test programs prior to maintenance to ensure no malicious code is present and handle incidents appropriately." The discovery of a .exe file used for data exfiltration testing on a production server indicates a potential security incident (malicious or unauthorized code). The practice's intent is to identify and manage such risks, and the CMMC framework mandates handling incidents per the organization's incident response plan (IR.L2-3.6.1), which should include steps like verification, containment, eradication, and reporting.
Option C: In accordance with the incident response plan– This is the correct approach, as it ensures a structured response (e.g., isolate the server, investigate the .exe's origin, remove it, and report if needed), aligning with CMMC's integrated security processes.
Option A: Reporting to the FBI immediately– Premature without internal verification and escalation per the IR plan; external reporting may follow but isn't the first step.
Option B: Decommissioning the server– Drastic and potentially unnecessary without analysis; it disrupts operations and skips investigation.
Option D: Sandboxing and continuing– Sandboxing is part of analysis, but continuing business as usual ignores the risk of active compromise.

Why C?The CMMC guide ties media inspection incidents to the IR process, ensuring a systematic response that balances security and operational needs. The assessor's role is to verify compliance, not dictate actions, but C reflects the required process.
Extract from Official CMMC Documentation:
CMMC Assessment Guide Level 2 (v2.0), MA.L2-3.7.4: "Handle identified malicious code in accordance with organizational incident response procedures."
CMMC Assessment Guide Level 2 (v2.0), IR.L2-3.6.1: "Establish an operational incident-handling capability to investigate, contain, and recover from incidents."
NIST SP 800-171A, 3.7.4: "Examine incident response plans for handling malicious code found during media inspection."
Resources:
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question: 5

A contractor allows for the use of mobile devices in contract performance. Some employees access designs and specifications classified as CUI on such devices like tablets and smartphones. After assessing AC.L2-3.1.18 – Mobile Device Connection, you find that the contractor maintains a meticulous record of mobile devices that connect to its information systems. AC.L2-3.1.19 – Encrypt CUI on Mobile requires that the contractor implements measures to encrypt CUI on mobile devices and mobile computing platforms. The contractor uses device-based encryption where all the data on a mobile device is encrypted. Which of the following is a reason why would you recommend container-based over full-device-based encryption?
A. Container-based encryption offers granular control over sensitive data, improves device performance by encrypting selectively, and enhances security in Bring-Your-Own-Device (BYOD) environments
B. Container-based encryption is more cost-effective
C. It is more user-friendly and easier to deploy on a large scale
D. Full-device encryption is not compatible with modern mobile operating systems

Answer: A

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:
AC.L2-3.1.19 requires "encrypting CUI on mobile devices." Full-device encryption secures all data, but container-based encryption (A) offers granularity (protecting only CUI), performance (less overhead), and BYOD compatibility (separating work/personal data), enhancing security and usability. Cost (B) and ease (C) aren't primary drivers, and full-device encryption (D) is compatible with modern OSes, per CMMC discussion.
Extract from Official CMMC Documentation:
CMMC Assessment Guide Level 2 (v2.0), AC.L2-3.1.19: "Container-based encryption provides granular control, performance, and BYOD support."
NIST SP 800-171A, 3.1.19: "Assess encryption methods for effectiveness."
Resources:
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Cyber AB

Code: CMMC-CCA

Exam: Certified CMMC Assessor (CCA) Exam

https://www.examsnest.com/exam/cmmc-cca/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation