Boost up Your Certification Score

Huawei
H35-665
Huawei Certified ICT Professional-5G-Security Solution

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

An operator is building a slice for a bank's payment terminals beside its consumer slices on a shared RAN. The bank requires that PDU session management and user-plane traffic for its terminals are handled only by functions dedicated to its slice. It accepts sharing the RAN and the functions that handle registration and mobility, and the operator wants the lowest-cost design that meets the requirement. Which configuration should the operator choose?

A. A dedicated SMF and UPF for the bank's slice, with a shared AMF and RAN
B. A dedicated AMF for the bank's slice, with a shared SMF, UPF and RAN
C. A shared AMF, SMF, UPF and RAN, with a separate S-NSSAI for the bank
D. A dedicated AMF, SMF and UPF for the bank's slice, with a shared RAN

Answer: A

Question: 2

A security architect is ranking the impact of compromise for components of an operator's virtualized core. The candidates are a single UPF instance, one gNB, one subscriber's USIM, and the NFV orchestrator that instantiates, scales and terminates all core NFs.
Which compromise has the broadest impact?

A. The UPF instance, because it forwards user traffic for every slice in the network
B. The orchestrator, because it controls every NF's lifecycle
C. The USIM, because its long-term key lets an attacker act for all subscribers
D. The gNB, because it holds the long-term keys of every attached subscriber

Answer: B

Question: 3

An operator's incident response team has confirmed that a MEC application server is compromised. It has isolated the server from the network and captured forensic images of its memory and disk.
Which incident response activity should the team carry out next?

A. Recovery: return the server to production service immediately
B. Preparation: write and test the team's playbooks
C. Eradication: remove the attacker's malware and access
D. Detection: confirm once more that an incident has occurred

Visit us at: https://www.examsboost.com/test/h35-665

Answer: C

Question: 4

A car-parts factory connects its own programmable logic controllers and a supplier-built monitoring application to an operator-provided private 5G network. A penetration test finds an unauthenticated remote-control function in the monitoring application, reachable from the factory's devices over the 5G network.
Under the shared responsibility model, who owns remediation of this finding?

A. The operator, because the vulnerable application is reachable across its 5G network
B. The national regulator, because the factory counts as critical industrial infrastructure
C. The network equipment vendor, because its gNBs and UPF carry the application's traffic
D. The factory, because it owns that connected application

Answer: D

Question: 5

A utility deploys thousands of 5G smart-meter modules in unattended street cabinets. Its risk assessment notes that a thief could remove a module's USIM and insert it into attacker-controlled equipment to reach the network as that meter.
Controls inside the module that lock the USIM so it works only with its authorized mobile equipment belong to which security domain?

A. User domain security, because it protects access between the USIM and the mobile equipment
B. Network domain security, because the equipment connects through operator transport
C. Application domain security, because the meter application runs on the module
D. Network access security, because the network authenticates the subscription held in the USIM

Answer: A

Question: 6

An operator's security architects are mapping where each protection for a UE's traffic terminates on the network side.
Which protections terminate at the gNB?
(Choose two.)

A. De-concealment of the UE's SUCI
B. Ciphering of NAS signaling

C. Verification of the UE's authentication response
D. Integrity protection of RRC signaling
E. PDCP ciphering of user-plane data on radio bearers

Answer: D,E

Question: 7

A power grid operator connects legacy substation devices that have no 5G modem. Each substation uses an industrial 5G router whose SIM authenticates to the operator, with the devices plugged into the router's Ethernet ports. An audit finds that any laptop plugged into a spare port gets the same access as the devices.
Which control closes this gap?

A. Switching the router's primary authentication from 5G AKA to EAP-AKA'
B. Secondary authentication of the router's PDU sessions by the grid operator's AAA server
C. Authenticating wired devices at the router's ports before they use its 5G session
D. Allowing only the router's subscription onto the substation DNN and slice at the UDM

Answer: C

Question: 8

An operator splits its gNB-CU into a central CU-CP and CU-UP instances placed at edge sites near a stadium and a university campus. A design review asks which link carries the user-plane security keys from the CU-CP to the CU-UP.
Which interface is it?

A. E1, between the CU-CP and each CU-UP instance
B. N2, between the CU-CP and the AMF
C. N3, between each CU-UP and the UPF
D. F1-C, between the CU-CP and each gNB-DU

Answer: A

Question: 9

A wind farm operator moves from a design where turbine data crossed the operator's central core to one with a UPF and edge server at the substation, linked to the operator core over the wind farm's own transport network, which the operator does not manage. The change keeps turbine data local and cuts latency.
Which risk does the new design introduce that the central design largely avoided?

Visit us at: https://www.examsboost.com/test/h35-665

A. Exposure of the turbines' long-term keys held in the UDM
B. Interception of N3 and N4 on the site transport
C. Loss of NAS protection between turbines and the AMF
D. Abuse of roaming signaling across the N32 interface

Answer: B

Question: 10

On a port's private 5G network, analysis of registrations from several UEs near one quay shows that the network selected weaker algorithms for them than it assigns to identical UEs elsewhere. A rogue relay device was later found near the quay.
Which threat class was being attempted?

A. A replay of previously captured authentication vectors from the home network
B. A signaling storm caused by UEs repeating their registration attempts
C. A bidding-down attack
D. An extraction of the long-term key stored in each UE's USIM

Answer: C

Visit us at: https://www.examsboost.com/test/h35-665

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer