CERTLABZ CERTIFICATION BOARD

Certified OT Security Engineer (COSE)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working OT security engineer would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1

Domain 3: Network Architecture and Segmentation

CONFIG

Emma Wilson reviews the rule set on the firewall between the industrial DMZ and the Level 2 control zone.

```
# DMZ <-> Control zone
1  allow  hist-l2:any      -> hist-dmz:5450    tcp   # historian replication
2  allow  jump-dmz:any     -> eng-ws:3389      tcp   # vendor sessions
3  allow  corp-net:any     -> 10.20.1.0/24:502 tcp   # "for the dashboards"
4  allow  any              -> any              any   # temporary, added 2024
5  deny   any              -> any              any   log
```

Listing 1.1 Conduit firewall policy as deployed.

Which two rules should be removed or rewritten first, and why?

A. Rules 1 and 2, because historian replication and vendor sessions must never cross the DMZ boundary in either direction.

B. Rules 3 and 4, because they let enterprise hosts write Modbus to every PLC and let anything through, defeating the conduit.

C. Rules 2 and 5, because vendor access should be a direct VPN to the PLCs and the final deny stops legitimate traffic.

D. Rules 1 and 5, because replication should run inbound from the DMZ and a logged deny fills the disk with events.

Correct answer: B
Rule 3 gives the whole corporate network Modbus access to the controller subnet, and rule 4 is an any/any allow that makes every other rule meaningless. Historian replication outbound to the DMZ and brokered jump-host sessions are exactly what a conduit should permit, and a logged default deny is correct.

Question 2

Domain 1: OT, ICS and Control System Fundamentals

DATA

James Carter inventories a water treatment site. Four assets are listed with the level the integrator assigned.

Asset	Function	Assigned level
Chlorine dosing PLC	Runs the dosing control loop	Level 1
Operator HMI	Supervisory display and setpoints	Level 2
Replicated historian	Read-only copy for enterprise users	Level 2
Flow transmitter	Measures flow into the works	Level 0

Table 2.1 Assets and assigned Purdue levels.

Which assignment is wrong, and where should that asset sit?

A. The chlorine dosing PLC is wrong; a controller that runs a loop belongs at Level 0 with the field devices.

B. The operator HMI is wrong; a supervisory display with setpoint control belongs at Level 3 site operations.

C. The replicated historian is wrong; a copy that enterprise users read belongs in the DMZ at Level 3.5.

D. The flow transmitter is wrong; a transmitter that feeds the PLC belongs at Level 1 with basic control.

Correct answer: C
A replicated historian exists so enterprise users can read plant data without touching the control network, which is the purpose of the industrial DMZ at Level 3.5. PLCs sit at Level 1, HMIs at Level 2 and transmitters at Level 0, so the other three assignments are correct.

Question 3

Domain 4: Asset, Vulnerability and Patch Management

DATA

Olivia Davis triages four ICS advisories against the asset inventory.

Advisory	CVSS	Affected asset	Exposure
A	9.8	Historian in DMZ	Reachable from enterprise
B	7.5	Safety controller	Isolated zone, key in run
C	8.1	Remote-access gateway	Internet facing
D	6.5	HMI	Control zone only

Table 3.1 Advisories, scores, assets and exposure.

Which advisory should be handled first?

A. Advisory A, because the highest CVSS score always determines the order of work regardless of where the asset sits.

B. Advisory B, because anything touching the safety controller must be patched before all other work is considered.

C. Advisory C, because an internet-facing gateway is the most reachable path to the plant whatever its base score.

D. Advisory D, because HMIs are the assets operators use most and their exposure to the control zone is total.

Correct answer: C

OT prioritisation weighs reachability and consequence, not CVSS alone. An internet-facing remote-access gateway is the most exposed path into the plant, so advisory C comes first. The historian is next because it is reachable from the enterprise. The safety controller is isolated with its key switch in run, so it is protected while a window is planned.

Question 4

Domain 5: Monitoring, Detection and Incident Response

DATA

Liam Anderson reviews the passive sensor alerts for one night shift, in order.

Time	Source	Alert
00:20	10.20.1.77	New host seen on the control VLAN
00:55	10.20.1.77	Logic read from six PLCs
02:10	10.20.1.77	Setpoint writes to PLC-03 and PLC-04
02:15	HMI-01	Displayed values unchanged
03:20	10.20.1.77	Host no longer seen

Table 4.1 Sensor alerts during the shift.

What does this sequence most likely indicate, and what is the correct first action?

A. Routine maintenance by a contractor; close the alerts as expected activity and log the host as a known device.

B. Reconnaissance then manipulation of control with view held normal; confirm process safety with operations now.

C A misconfigured historian polling PLCs; move the host into the DMZ and re-baseline the sensor for the shift.

D A sensor fault that duplicated alerts; restart the passive sensor and wait for a clean baseline before acting.

Correct answer: B
A new host enumerating and reading logic from many controllers, then writing setpoints while the HMI shows no change, is the classic pattern of reconnaissance followed by manipulation of control with manipulation of view. The first action in OT response is to confirm with operations that the process is safe, then preserve evidence and contain the host without stopping the controllers.

Question 5

Domain 3: Network Architecture and Segmentation

DATA

Ava Thompson compares four proposals for vendor remote access to a packaging line.

Proposal	Design
1	Permanent site-to-site VPN from the vendor into the Level 2 network
2	Port forward on the plant firewall to the engineering workstation
3	Jump host in the DMZ, MFA, approval per session, recording, no inbound tunnel
4	Remote desktop tool installed on the HMI with the vendor's own account

Table 5.1 Proposed remote-access designs.

Which proposal is defensible?

A Proposal 1, because a site-to-site VPN encrypts the vendor traffic and the plant firewall still sees every packet.

B Proposal 2, because a single port forward exposes only one host and the engineering workstation is hardened.

C Proposal 4, because a remote desktop tool on the HMI keeps the vendor inside the operator view at all times.

D Proposal 3, because a brokered, approved, recorded session with no inbound tunnel contains a vendor compromise.

Correct answer: D
Brokered access through a DMZ jump host with MFA, per-session approval and recording, and no standing tunnel into the control network, is the design that keeps a compromised vendor from becoming a compromised plant. A permanent VPN, a port forward and a remote tool on the HMI each create a direct path to control assets.

Question 6

Domain 5: Monitoring, Detection and Incident Response

CONFIG

An operator reports that a mixing PLC is behaving oddly. The draft response plan below was written by the IT security team.

```
step 1: power off the PLC to stop the attacker
step 2: reflash the PLC with the vendor image
step 3: capture network traffic
step 4: tell operations what happened
```

Listing 6.1 Draft response steps for the mixing PLC.

What is wrong with this plan?

A. Nothing is wrong; removing power is the fastest containment and reflashing restores a clean, trusted controller.

B. It powers off and reflashes before operations confirm a safe state or any evidence is kept, which is unsafe and blind.

C. The only flaw is order: traffic capture should come first and the other three steps are correct as they stand.

D. The only flaw is scope: the whole control network should be powered off rather than one mixing PLC on its own.

Correct answer: B
Cutting power to a running controller can put the process in an unsafe state, and reflashing before an upload of the running logic and a network capture destroys the evidence needed to understand the attack. OT response starts by confirming safety with operations, preserves evidence, then contains without stopping the controller, and restores in a coordinated window.

Question 7

Domain 2: Threats, Risk and Standards

A site sets a target security level of SL 3 for its safety zone under IEC 62443. The assessment finds the zone currently achieves SL 1. What should the engineer do?

A. Lower the target to SL 1 so that the assessment closes with no gap and the zone can be reported as compliant.

B. Record the gap, treat the risk and strengthen the zone until the achieved level meets the target or it is re-justified.

C. Ignore the gap because the safety zone has never been attacked and the controllers are physically locked away.

D. Move the safety controller into the general control zone so that both zones can share one target level of SL 2.

Correct answer: B
The difference between the target and achieved level is the remediation plan. Lowering the target without justification, ignoring the gap, or merging the safety zone into a lower-security zone all defeat the purpose of setting a target for the highest-consequence assets.

Question 8

Domain 4: Asset, Vulnerability and Patch Management

An engineer proposes running the enterprise vulnerability scanner across the Level 1 controller network during production so the inventory is complete by Friday. What is the right response?

A. Approve it, because modern controllers handle unexpected traffic and a complete inventory is worth a small risk.

B. Approve it with a lower scan rate, because throttling removes the chance of a controller faulting under load.

C. Decline it and use passive discovery from a SPAN port, with any active queries done in a maintenance window.

D. Decline it and rely on the purchase records, because an inventory built from invoices is accurate enough.

Correct answer: C
Legacy embedded stacks can fault or reboot when they receive unexpected traffic, halting the process. Passive discovery identifies devices without transmitting to them, and any active or credentialed queries belong in a maintenance window with vendor guidance. Invoices do not tell you what is on the network today.

Question 9

Domain 6: Governance, Safety and Secure Operations

Operations objects that requiring multi-factor authentication on the control room HMI would slow response during an emergency. Which resolution is sound?

A. Remove MFA from every OT system, because the safety argument from operations outweighs any security control.

B. Keep a shared view account on the HMI without MFA, and require MFA and named accounts for engineering and remote access.

C. Force MFA on the HMI regardless, because a consistent policy matters more than the concerns of the operators.

D. Replace the HMI with an automated system so that no operator ever needs to log in during an emergency again.

Correct answer: B
Controls go where they reduce risk without harming safety. Operator view in a physically controlled room is a different risk from the ability to change logic or connect remotely, so MFA and individual accounts belong on engineering and remote access while the control room relies on physical access control.

Question 10

Domain 1: OT, ICS and Control System Fundamentals

A plant engineer asks why the safety controller's physical key switch matters to cybersecurity. Which answer is correct?

A. It does not matter; the key switch only selects the display language and has no effect on what the controller runs.

B. In program mode it blocks all network traffic, so leaving it there is the safest setting for normal operation.

C. In run mode it blocks program changes; leaving it in program mode is what let TRITON attempt to alter safety logic.

D. It matters only for warranty purposes, because vendors refuse support when the key has been turned by the customer.

Correct answer: C

Many safety controllers accept logic changes only when the key switch is in program mode. Leaving it there outside maintenance removes a physical barrier, which is exactly what the TRITON attackers relied on. Procedures should require the switch in run mode except during authorised, supervised changes.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document COSE-001. https://certlabz.com/certifications/certified-ot-security-engineer.html